جامعة النيلين
كلية الدراسات العليا

حماية الشبكات الرئيسة من الاختراق والبرامج الضارة

(دراسة لنيل درجة الماجستير في تقانة المعلومات)

إعداد: المهندس زكريا أحمد عمار
إشراف: الأستاذ الدكتور السمَّاني عبد المطلب أحمد

١٤٣٢هـ/٢٠١١م


بسم الله الرحمن الرحيم

(يرفع الله الذين آمنوا منكم والذين أوتوا العلم درجات)

الآية (١١) سورة المجادلة

مستلخص الدراسة

نظراً لانتشار الشبكات الحاسوبية واعتماد المؤسسات العامة والخاصة على كفاءتها وجودة عملها، فإن أي توقف لها أو تخريب فيها قد يؤدي إلى خسائر عظيمة وتعطيل لخدمات المواطنين، وبانتشار القراصنة والأخطار وإساءة الاستخدام كانت فكرة الدراسة للحد من الأضرار مسبقاً باتخاذ تدابير احتياطية من منظور أمني شامل، ومن خلال تحليل نتائج المسح الإحصائي توصلت الدراسة إلى أن مشكلات حماية وتأمين موارد شبكات الحاسب الآلي، لا تكمن في توريد وتثبيت الأجهزة والبرمجيات فقط، وإنما تكمن في توفير وإعداد الإنسان القادر على إدارة وتشغيل تلك الأجهزة والبرمجيات في إطار سياسات وإجراءات ضمن بيئة يسود فيها روح الفريق.

ولعدم وجود التوافق بين الهياكل التنظيمية وإجراءات ووظائف الموارد البشرية العاملة في مجال الحماية بالعينة المدروسة، فإن الوصول إلى حماية أفضل لشبكات الحاسب الآلي تتطلب إعادة تصميم الهياكل التنظيمية. وحتى يتم التمكن من التغلب على صعوبات الحماية لا بد من توفير أخصائيين في أمن المعلومات. وتوفير عدد كاف من موظفي أمن المعلومات، يحملون مؤهلات علمية تتناسب مع متطلبات أعمال الحماية وتوفير مسميات وظيفية مع بيان المهام والواجبات وخاصة للوظائف المتعلقة بالحماية والأمان.

ويتعين على متخذي القرار توفير الميزانيات اللازمة لتطوير العاملين وزيادة أعدادهم حسب التخصصات المطلوبة، وعمل ما يلزم لمطابقة الإجراءات مع المعايير العالمية ذات العلاقة بأمن المعلومات، وتوثيق إجراءات أعمال الحماية ومخططات الشبكات وتحديثها دورياً. وتوفير سياسات توظيف تؤدي إلى استقطاب الكوادر المؤهلة من ذوي الخبرة في مجال الحماية وتحفيزهم بالمكافآت المالية والمعنوية.

ولا بد من تعيين مدراء متخصصين لإدارة مراكز تقنية المعلومات بحيث يكون لديهم المؤهلات الكافية للتعامل مع متطلبات تطوير المختصين بالحماية وفهم الحاجة لتطويرهم

وتقدير أعمالهم. وإدراك أهمية إعادة تنظيم الهياكل التنظيمية للمؤسسات للتوافق مع الإجراءات والوظائف المستجدة في مجال امن المعلومات.

ولا بد من الاعتناء بأخلاقيات الموظفين، وإعطاء صفات النزاهة والصدق والإخلاص أولوية عالية وإدراجها في سياسات التوظيف، ولا بد من إعطائها درجات عالية في تقييمات المقابلات الشخصية، وتوظيف العناصر الموثوق بها، ومراجعة وتدقيق سلوك الموظفين من الناحية الأخلاقية وضرورة توفر الصدق والأمانة والضمير الحي على الدوام. وينبغي التأكد بشكل دوري من محافظة الموظفين على مستوياتهم الأخلاقية و زيادة حس المسؤولية كلما أمكن ذلك.

وحتى يتم التقليل من أخطار الاختراق وتلوث الحاسبات يجب أن تُبذل الجهود الكافية في توعية وتدريب مستخدمي الحاسبات الآلية بضرورة تثبيت تحديثات أنظمة التشغيل واتباع الطرائق الصحيحة لاستخدام البريد الالكتروني، وتمييز مواقع الانترنت غير الآمنة وتجنب زيارتها.

Abstract

Due to the spared of computer networks in all life fields, quality of business services for public and private organizations might be affected by any downtime or sabotage of computer networks, which may lead to great losses and disruption to citizen's services, the spread of the pirates and the dangers and misuse of the idea of the study to limit the damage already taking precautionary measures from the perspective of comprehensive security, and through the analysis of survey results The study found that the problems of protecting and securing resources for computer networks, does not only lie in the supply and installation of hardware and software, but also lies in the provision and preparation of human resources, they are capable of managing and operating hardware and software in the framework of the policies and procedures in an environment dominated by cooperation stuff.

And the lack of compatibility between the organizational structures, procedures and functions of human resources working in the field of protection of the studied sample networks, access to better protect computer networks require the redesign of organizational structures.

In order to be able to overcome the difficulties of protection must be provided to specialists in information security. Decision maker should provide budgets to develop staff , match procedures with international standards related to information security.

Appointment of managers specialized in the protection of the sections of information security.

Computer users should have attend required crocuses to enable them to consider protection parameters while they perform their work properly. And People who perform protection tasks should be appreciated by providing bonuses, allowances, and/or certificates of appreciation. Also the incomes of protection staff especially the experts should be increased to let them stay and not leave their jobs.

We must take care of the ethics of the staff, giving qualities of integrity, honesty and devotion to high priority and be included in employment policies. It should be ensured yearly that the ethical levels of staff is available, also it's better to increase the moral sense of responsibility whenever possible.

In order to reduce the risk from penetration and infection of computers, sufficient efforts should be made to aware and train users, to be able to install updates, to know right ways to open their e-mail, and avoid visiting unsafe Web sites.

الكلمات المفتاحية

أمن المعلومات، شبكات الحاسب الآلي، إدارة الأعمال، تقنية المعلومات، حماية مراكز المعلومات، مكافحة الفيروسات، إجراءات العمل ، وظائف تقنية المعلومات، أمن المنشآت المعلوماتية، شبكة الانترنت، حماية الشبكات الموزعة.

إهـــــــــداء

إلى والدي ووالدتي حبـــاً ووفـــــاء

إلى كل من ساعدني وشجعني

إلى أبنائي وبناتـــــــــي وزوجتي تشجيعاً على السير في دروب البحث العلمي

البـــــاحـــــــث

بسم الله الرحمن الرحيم

شكر وتقدير

الحمد لله رب العالمين والصلاة والسلام على أشرف الأنبياء والمرسلين نبينا محمد وعلى آله وصحبه أجمعين أما بعد.

فإنني أشكر الله سبحانه وتعالى على توفيقه بإتمام هذه الرسالة، وانطلاقاً من قولـــه عليه الصلاة والسلام "لا يشكر الله من لا يشكر الناس" فإنني أتوجه بالشكر والتقدير لمعالي الأستاذ الدكتور عبدالعزيز بن صقر الغامدي رئيس جامعة نايف العربية للعلوم الأمنية لتشجيعه، ودأبه المستمر لتطوير جامعة نايف العربية للعلوم الأمنية. كما أتوجه بالشكر لسعادة الدكتور محمد أسعد العالم عميد مركز المعلومات في جامعة نايف العربية للعلوم الأمنية على تشجيعه المستمر. كما أتقدم بوافر الشكر والتقدير لسعادة وكيل كلية التدريب الدكتور إبراهيم الماحي لتشجيعه المتواصل ومتابعته التي كانت السبب بعد الله في مواصلة دراستي رغم الظروف التي مررت بها فجزاه الله عني خير الجزاء وجعل ذلك في موازين حسناته إنه سميع مجيب. كما أشكر الدكتور سعيد بن عطية الشرم والدكتور عصام توفيق والأستاذ حسين الضرير لما قدموه من مساعدة وتشجيع وعون في مجال البحث العلمي. وأتوجه بخالص الشكر والتقدير لسعادة رئيس قسم التوثيق والإحصاء بمركز المعلومات بجامعة نايف العربية للعلوم الأمنية الدكتور أحمد عوده وفريقه الرائع محمود حامد وعبدالله المالكي لما قدموه من عون وتوجيه أثناء هذه الدراسة، والشكر موصول لجميع أعضاء الهيئة التدريسية بالجامعة لما قدموا من عون علمي بالتجاوب غير المنظور بالإجابة على تساؤلاتي، ولعددهم الوافر أذكر الفريق دكتور عباس أبو شامة والأستاذ الدكتور عبد العاطي الصياد والأستاذ الدكتور عبد الحفيظ مقدم و الدكتور محمود شاكر والدكتور أحسن طالب والدكتور محمد حمزاوي لما قدموا من علم وتوجيه.

وأتوجه بالشكر الجزيل للأستاذ الدكتور رئيس جامعة النيلين لمساعدته العلمية والإنسانية ولا أنسى بطل الجميع المشرف على هذه الدراسة سعادة الأستاذ الدكتور السماني عبدالمطلب أحمد حيث بفضل الله ثم بفضل جهده المتواصل وتوجيهاته السديدة ورحابة صدره أثناء فترة البحث تم إنجاز هذا العمل فله مني الوفاء وخالص التقدير .

كما أتوجه بخالص الشكر والتقدير لأعضاء لجنة المناقشة الموقرين سعادة الأستاذ الدكتور عوض حاج علي أحمد، وسعادة الأستاذ الدكتور عوض عبد الكريم محمد يوسف بقبول مناقشة هذه الرسالة

والحكم عليها رغم كثرة مشاغلهم وأعبائهم الأكاديمية والإدارية، سائلا الله عز وجل أن يديم عليهما موفور الصحة والعافية إنه سميع مجيب.

كما أتقدم بخالص الشكر إلى جميع الأساتذة اللذين قاموا بتحكيم استبانة هذه الرسالة بشكل عام وسعادة الأستاذ الدكتور عبد الحفيظ مقدم والأستاذ الدكتور محمد الأفندي والأستاذ الدكتور عبدالعاطي الصياد والأستاذ الدكتور أحمد عودة بشكل خاص على ما بذلوه من نصح وتوجيه فجزاهم الله عني خير الجزاء.

كما لا يفوتني أن أتقدم بالشكر الجزيل لأبنائي وبناتي وزوجتي الأبطال الذين أعطوني الكثير من وقتهم وما يزالون عونا ونبراساً ودافعاً لي في مسيرة حياتي.

وفي الختام أتقدم بالشكر الجزيل لكل من أسهم في إخراج هذا العمل الأكاديمي إلى النور.

وفق الله الجميع لما فيه خيري الدنيا والآخرة. إنه سميع مجيب، وآخر دعوانا أن الحمد لله رب العالمين.

الباحث

زكريا أحمد عمار

الفهـــــــرس

قائمة الجداول

قائمة الأشكال

الفصل الأول

الإطار العام للدراسة

١ ـ المقدمة.

١ ـ مشكلة الدراسة.

١ ـ تساؤلات الدراسة.

١ ـ فرضيات الدراسة.

١ ـ أهداف الدراسة.

١ ـ أهمية الدراسة.

١ ـ مصطلحات الدراسة.

الفصل الأول
الإطار العام للدراسة

١ ـ المقدمة

في عصرنا عصر المعلومات الذي يشهد نموا سريعا في المعلومات والمعارف حيث "تتضاعف كمية المعلومات كل خمس سنوات وتتضاعف قوة الحاسب الآلي كل سنتين"[١] وفي هذا العصر نشهد "ثورة في المعلومات الذي يقوم فيها الحاسب الآلي بالدور الأول حيث أصبح العلم قرية صغيرة تربطها شبكات المعلومات."[٢] في هذا العصر اعتمدت المؤسسات في تسيير أعمالها على تقنية المعلومات التي أثبتت أنها تسهم في إنجاز الأعمال بسرعة عالية وبدقة متناهية وحيث أن البيانات والمعلومات تخزن في مخازن معلومات مربوطة مع حاسبات المؤسسة من خلال شبكة الاتصال وغالبا ما تكون متاحة عبر شبكة الانترنت تسهيلا لإجراءات العمل واختصارا للوقت. ولهذا تطورت طرق معالجة البيانات للتوافق مع بيئة الحاسبات من طرق يدوية إلى طرق آلية منتجة نظم سير العمل الإلكترونية لتصل إلى مفهوم الحكومة الإلكترونية. وبذلك نجد أن تقنية المعلومات قد ساهمت في تسهيل الأعمال الطبية والهندسية والصناعية والمصرفية وأنظمة المكتبات وأعمال المؤسسات التعليمية بل إنها أصبحت سلاحاً في المؤسسات العسكرية يستخدم في الأعمال الحربية.

وشكلت شبكات الاتصال الوسط الذي تنساب فيه البيانات وتسكن فيه مخازن البيانات. إن هذه الشبكات تحتاج إلى حماية تضمن سلامة محتوياتها واستمرارية عملها. حيث وصل الأمر إلى أن الأعمال تتوقف في المؤسسات إذا تعطلت شبكات معلوماتها كشركات الطيران والشركات الكبيرة المنتشرة حول العالم بل إن التوقف القصير لتلك الشبكات يكبد أصحابها أو المستفيدون منها خسائر فادحة ، وإن التوقف القصير لشبكات المعلومات الحكومية والوطنية يؤدي إلى تعطيل أعمالها مما ينعكس على انخفاض مستوى الخدمات المقدمة للمواطنين وإرباك في مؤسسات الدولة ذات العلاقة بالشبكات المتعطلة. وتوقف شبكات المؤسسات التجارية يسبب خسائر مالية كبيرة قد تؤدي في كثير من الأحيان إلى الإفلاس. وغدت جودة الأعمال ونجاحها يعتمدان على جودة وأداء شبكات الاتصال واستمرارية عمل قواعد البيانات.

---

[١] مدحت أبو النصر قواعد ومراحل البحث العلمي ط١ (القاهرة: مجموعة النيل العربية،٢٠٠٤) ص٥٣

[٢] مدحت أبو النصر ٢٠٠٤ مرجع سابق ص٥٣

ونظراً لكثرة الأخطار التي تهدد سلامة البيانات التي تنساب في الشبكات أو البيانات المحتضنة في خزائنها وكثرة الأخطار التي تهدد استقرار تلك الشبكات وأمنها كالإصابة بالفيروسات والبرامج الضارة ومحاولات الاختراق لأغراض سرقة المعلومات أو التخريب أو التعديل والعبث، تأتي أهمية الحماية على مدار الساعة لمكوِّنات شبكات المعلومات المادية والبرمجية بتثبيت أجهزة وبرامج الحماية في بوابات الشبكات المحلية وداخل تلك الشبكات وإدارة تلك الأجهزة والبرمجيات من الزاوية الأمنية وسد الثغرات أولا بأول لتضييق فرص قراصنة المعلومات والمنافسين والأعداء من التمكن من اختراق أو سرقة أية بيانات من شبكات المعلومات. ومن هنا أتت فكرة هذا الدراسة الذي يبدؤها الباحث في هذا الفصل بتمهيد يستعرض فيه خلفية الدراسة ومشكلتها وأهميتها، وتساؤلاتها وفرضيتها، والتعريفات ذات الصلة بالدراسة.

بعد انتشار استخدام الحاسبات الآلية على جميع الأصعدة الاقتصادية والاجتماعية والسياسية واستخدام الأفراد لها، ناهيك عن المؤسسات والمنظمات فإن كمية المعلومات المتبادلة والمنقولة عبر شبكات الاتصال ازدادت بشكل مذهل، وانتشرت الشبكات في كل مكان مستخدمة لأشكال متعددة من الوسائط كالكابلات التي تربط المؤسسات والدول على الأرض، والهوائيات والأقمار الصناعية التي تنقل الإشارات اللاسلكية عبر الجو، وقد يكون وسط النقل هجينا يستخدم أكثر من نوع في آن واحد، كل ذلك لتسهيل انتقال المعلومات وتقصير المسافات. وفي هذا السياق جاءت شبكة الانترنت لتتيح لكل فرد أن يحصل على ما يشاء من المعلومات في مختلف أنحاء الدنيا وفي أي وقت وعلى مدار الساعة. ناهيك عن إتاحة الفرصة لمن يرغب لإضافة بيانات إلى قواعد المعلومات المتاحة في شبكة الانترنت.

إن تذكُّر خريطة العالم القديم يوحي بوجود حواف للعالم، "وفي عالم هذه الأيام المترابط ببعضه، يصحّ هذا التمثيل لفضاء الانترنت الحديث، فعندما يوصِل المرء شبكة منزله أو شركته بالإنترنت، فإن كل شيء ما بعد تلك الشبكة هو حرفياً حافة العالم وبداية شبكة الانترنت العالمية[٣]، وفيها توجد مصادر الخطر من قراصنة المعلومات الذين يسعون لاستغلال الثغرات ومواطن الضعف في شبكات الضحايا. إذ يمكن القول بأن كل مستخدم لهذه الشبكة هو طرف من هذا العالم، حيث تنتشر شبكات الحاسب الآلي في قطاعات الأعمال بكثافة شديدة وتزداد بتسارع قل نظيره في القطاعات الأخرى.

٣ توماس طوم : **الخطوة الأولى نحو أمان الشبكات** ، ترجمة مركز التعريب والترجمة ،(بيروت: الدار العربية للعلوم، ٢٠٠٤) ص١٩.

وقد أظهرت دراسة علمية في الولايات المتحدة أن نسبة (٧٠%) من قطاع الأعمال عام ٢٠٠٠م تعرضوا لعمليات إساءة استخدام الشبكات والحاسبات بزيادة عن عام ١٩٩٦م بلغت (٤٢%)، وقد تسببت حملات التخريب (Hacking) للأنظمة والشبكات والبرمجيات في أضرار كثيرة وزادت حوادث سرقة المعلومات وتخريب وتدمير مواقع الوِيب.[٤]

ونظراً لتنوع وسائط الربط والانتشار الواسع لتقنية المعلومات، حيث انتشرت الشبكات السلكية بمختلف أنواعها النحاسية والضوئية إلى جانب الشبكات اللاسلكية مما زاد الأخطار التي تهدد استقرار شبكات المعلومات وزادت الحاجة لتركيب برامج وتجهيزات الحماية وتطبيق نظم إدارة خاصة بأمن تقنية المعلومات لضمان الحماية القصوى بيقظة تامة على مدار الساعة وبمختلف مفاصل الشبكة بدءاً من بوابات الشبكات المحلية التي تتضمن جدران الحماية ومروراً بتأمين قواعد البيانات وأجهزة الخادم وانتهاء بتنفيذ جميع إجراءات الأمان في محطات العمل في الشبكة المحلية، ويترتب على ذلك إعداد تصميم محكم ودقيق لأجهزة الحماية من حيث ضبط صلاحيات الوصول والنفاذ إلى عتاد الشبكة مع توثيق جميع الأحداث والعمليات التي تجري على مكونات الشبكة ومواردها وأنظمة وأجهزة حمايتها والحفاظ على الاعتمادية العالية والاستمرارية والأداء وبحيث يتحقق التوازن بين إجراءات الأمان وجودة الأداء.

ويتعدى الأمر إلى إيجاد الاحتياطات اللازمة لتشغيل النظام بحالات الكوارث والأعطال الكبيرة بتوفير مراكز البيانات البديلة في أمكنة بعيدة وآمنة بل إن مراكز البيانات الاحتياطية التي تقوم بأخذ النسخ الاحتياطية بشكل آني (مباشر) غدت ضرورة للمنظمات أو المنشآت التي تصنف أعمالها بأنها عالية الأهمية كالبنوك ومراكز المعلومات الوطنية وشركات الانترنت العملاقة و بشكل يومي أو أسبوعي ويفضل أن تكون النُّسخ الاحتياطية في مدينة بعيدة بل في دولة أُخرى في إطار اتفاقية أمنية متبادلة.

يتواكب التطور في تقنية المعلومات مع تطوير الهياكل التنظيمية في المنظمات والمؤسسات حيث أُحدِثت مديريات وهيئات متخصصة بتقنية المعلومات والاتصالات وزيدت إدارات أو أقسام متخصصة بتقنية المعلومات تتضمن أقسام المساندة الفنية أو الدعم الفني للمستفيدين وتتضمن أقسام تتخصص بالأنظمة الآلية التي تعنى بالبرمجة والتحليل وتصميم البرمجيات وتشغيلها وتعليم المستفيدين طرق استخدامها بالإضافة لأقسام تشغيل نظم الشبكات وإدارة النسخ الاحتياطي وكذلك أقسام

---

[٤] انظر: فايز بن عبد الله الشهري ، **استخدامات شبكة الانترنت في مجال الإعلام الأمني العربي** ، مجلة البحوث الأمنية ، تصدر عن مركز الدراسات بكلية الملك فهد الأمنية ، الرياض، المجلد ١٠ العدد ١٩ نوفمبر ٢٠٠١ ص١٨٤

المعلومات ومواقع الانترنت وأقسام أمن المعلومات وتزيد التغيرات وتنقص حسب حجم المؤسسة أو المنظمة.

وأُحدثت وظائف جديدة تحتاجها تقنية المعلومات بمسميات لم تكن موجودة مثل مدير قواعد البيانات ومدير نظم التشغيل وفني المساندة ومبرمج ومحلل نظم أول وضابط امن المعلومات وفني تمديدات ومدقق السياسات الأمنية.

إضافة إلى ضرورة بذل كل الجهود الممكنة لدرء خطر الجريمة الإلكترونية وذلك بتأمين حماية قصوى لشبكات الحاسب الآلي واعتبارها قضية وطنية تتبناها الحكومات وتقوم بدور التوعية والدعم المادي والمعنوي لبقية القطاعات لمساعدتهم على تأمين الأمن المناسب لشبكات كل قطاع صغُر أم كبُر. فقد "ازدادت مخاطر الجرائم المتعلقة بالحاسب الآلي لأسباب متعددة منها تداخل الحاسب الآلي في بيئة الأعمال التجارية والمعاملات في القطاع العام والخاص، وانتشار ظاهرة سوء استخدام الحاسب الآلي مثل نشر الفيروسات وتعميم المعلومات الإرهابية وإفشاء أسرار أسلحة الدمار الشامل، وإمكانية النفاذ إلى أنظمة الدفاع والأمن ومعلومات التصنيع الحربي"[٥].

١-٢ مشكلة الدراسة.

لقد توسع مجتمع المعلومات وكثرت التعاملات الالكترونية في العالم حيث " بلغ عدد مستخدمي شبكة الانترنت 1,572,549,488 مستخدم في ٢٠٠٩/١/٦ وفق تقديرات بداية عام ٢٠٠٩ ويشكل ما نسبته ٢٣.٥% من تعداد السكان البالغ 6,676,120,288 نسمة في منتصف عام ٢٠٠٨ م. وقد بلغ تقدير عدد مستخدمي الانترنت في منتصف عام ٢٠٠٨ (قبل ستة شهور فقط) 1,463,632,361 مستخدماً للانترنت. بما نسبته 21.9% من تعداد سكان العالم في منتصف ٢٠٠٨ أي أن عدد مستخدمي الانترنت ازداد خلال النصف الثاني من ٢٠٠٨ فقط 106,817,925 مستخدما وهو ما يقابل فارق النسبة البالغ ١.٦% من مجموع سكان العالم في منتصف ٢٠٠٨م"[٦]. ولعل إلقاء نظرة على استخدام البريد الالكتروني الشائع يعطي صورة عن أهمية شبكة الانترنت وشبكات المعلومات عموماً حيث " تشير التقديرات في آذار /مارس ٢٠٠٧ تبعاً لـــ (Pew Internet and American Life Project data) أن (٩١%) من مستخدمي الانترنت في الولايات المتحدة يتعاملون بشكل مباشر on-line مع البريد الإلكتروني بإرسال أو قراءة البريد".[٧] ويشير تقرير أعدّته مجموعة شركة (Technology market research) بأن

---

[٥] انظر محمد أمين البشري ، التحقيق في الجرائم المستحدثة، (الرياض: مركز الدراسات والبحوث ، جامعة نايف العربية للعلوم الأمنية، ٢٠٠٤ ، طبعة ١) ، ص٨٦

[٦] متوفر على الرابط http://www.internetworldstats.com/blog.htm

[٧] http://www.pewinternet.org/trends.asp

عدد مستخدمي البريد الإلكتروني في تشرين أول/أكتوبر ٢٠٠٧ بلغ ١.٢ بليون مستخدم وتوقع التقرير ازدياد العدد إلى ١.٦ بليون عام ٢٠١١ .[٨] "ويقدر (Ferris Research) عدد مستخدمي البريد الالكتروني في مجال الأعمال في عام ٢٠٠٧ بما يقارب ٧٨٠ مليون مستخدم".[٩] من خلال هذه الإحصائيات يمكن استنتاج ضخامة التعاملات في وسط شبكات المعلومات وإدراك ضخامة الأخطار التي تزداد بازدياد مستخدمي الشبكات وتهدد هذه الأخطار استقرار شبكات المعلومات التي يجب أن تستمر بالعمل على مدار الساعة بحيث يتم تثبيت تجهيزات الحماية في بوابات الشبكات المحلية ويتم إعدادها بما يلزم لضمان عدم اختراقها وقرصنة محتويات مواردها، وتثبيت برمجيات الحماية داخل تلك الشبكات وإعدادها بما يلزم لضمان عدم إصابتها بالفيروسات والبرامج الضارة. وكل جهاز أو برنامج يحتاج مجموعة من الإعدادات والإجراءات لا بد من إتباعها باستمرار لتصفية حزم البيانات وكشف محاولات الاختراق ومنعها تلقائياً، وبسبب تعدد أنواع أجهزة الحماية وتعدد برمجياتها وكثرة قضايا أمن المعلومات.

ويترتب على ذلك إنجاز تصميم جيد لشبكات الاتصال الرئيسة وتأمين متطلبات الحماية الفيزيائية لها، ويتطلب الإعداد والضبط الدقيقين لتجهيزات الحماية من حيث إعداد لوائح التحكم بالوصول وضبط صلاحيات تسجيل الدخول والنفاذ إلى تجهيزات الشبكة ومواردها بالإضافة لعمليات تثبيت تحديثات مكونات شبكة المعلومات سواء كانت أجهزة أو برمجيات وترقية نظم التشغيل. إن حصر وتوثيق هذه الإجراءات والعمليات ومتابعتها فنيا وإداريا يحتاج لجهود فنية وإدارية تتكامل لتصبح قابلة للتطبيق وتصلح لأي منشأة تعتمد في أعمالها على تقنيات المعلومات بحيث يأخذ بالاعتبار الهيكل التنظيمي لإدارة تقنية المعلومات والمسميات الوظيفية لها والمؤهلات العلمية لشاغلي هذه الوظائف والإجراءات الإدارية والفنية اللازمة لضمان الحماية القصوى للشبكات الرئيسة بجميع مواردها.

إن المشكلات الأمنية التي أوجدتها شبكات الحاسب وبخاصة شبكة الانترنت والتي تتلخص بتعطيل وتدمير المواقع الحكومية والتجارية، والتسلل إلى الشبكات وسرقة أسرار الشركات والحكومات والمؤسسات الأمنية والدفاعية، وترويج برامج التخريب والتجسس والقرصنة، وسرقة المواقع وانتهاك حقوق الملكية الفكرية، بالإضافة إلى أن شبكة الانترنت صارت وسيلة اتصال فعالة للعصابات والمجرمين والمخالفين للقانون والأعراف الاجتماعية والأخلاقية السائدة، وتوفر بيئة خصبة للترويج للتجارة المحرمة وغسيل الأموال والجرائم المنظمة، وتشكل ميداناً حديثاً من ميادين الحرب الإلكترونية تتسابق فيه الجيوش ومراكز البحوث العسكرية لتطوير تقنيات الدفاع الالكترونية العالية،

[٨] متوفر على http:www.email-marketing-reports.com نقلا عن الرابط http://www.radicati.com/

[٩] متوفر على http:www.email-marketing-reports.com نقلا عن الرابط http://www.ferris.com/research-library/industry-statistics/

كما أنها تؤمن تربة مناسبة لنمو شبكات التجسس العالمية التي تمارس نشاطات جمع المعلومات وانتهاك الخصوصية على مدار الساعة.[١٠]

في هذه الدراسة يتناول الباحث شبكات الحاسب الآلي ومخازن المعلومات المتصلة بها وطرق حمايتها من الاختراق، ويتناول الفيروسات والبرامج الضارة وطرق الحماية منها، ويتعرض للهيكل التنظيمي للمؤسسات ويذكر ما ينبغي توفره من أقسام ليتناسب مع طبيعة شبكات الحاسب وصعوبة حمايتها بشكل شمولي وتنفيذ الإجراءات الأمنية التي تقود على أفضل حماية ممكنة.

١-٣ تساؤلات الدراسة

تهدف هذه الدراسة إلى تحديد وسائل وإجراءات حماية الشبكات الرئيسة ومصادر المعلومات الموجودة فيها أو المنقولة منها وذلك من خلال الإجابة على أسئلة الدراسة والتحقق من صحة فرضياتها.
وتطرح الدراسة تساؤلاً رئيساً يتمثل بالسؤال التالي: ما هي طرق ووسائل حماية موارد شبكات الحاسب الآلي الأمر الذي يقود إلى التساؤلات الفرعية التالية:

١. ما الأجهزة والبرامج المستخدمة لحماية الشبكات ومدى إعدادها وتحديثها.
٢. ما نقاط الضعف التي تُستغل لاختراق شبكات المعلومات وما التدابير الوقائية المتخذة لمنع استغلالها.
٣. ما الهياكل التنظيمية المناسبة لإدارات تقنية المعلومات وما مدى توافق الوظائف المستخدمة في مجال أمن شبكات المعلومات معها.
٤. ما إجراءات العمل المعتمدة لحماية شبكات المعلومات وما مدى إتباعها والعمل بها.
٥. ما التدابير الاحتياطية اللازمة لتجنب المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات المعلومات، وما التدابير الفعلية المتخذة للتغلب على تلك المخاطر.

١-٤ فرضيات الدراسة

١. لا توجد فروق ذات دلالة إحصائية بين كمية الأجهزة والبرامج المستخدمة لحماية الشبكات بإعداد وتحديث تلك الأجهزة والبرامج.
٢. لا توجد فروق ذات دلالة إحصائية بين نقاط الضعف التي تُستغل لاختراق شبكات المعلومات وبين التدابير الوقائية المتخذة لمنع استغلال تلك النقاط.

---

[١٠] انظر : فايز بن عبد الله الشهري ، **مرجع سابق**، ص ص١٨٤-١٨٦

٣. لا توجد علاقة ذات دلالة إحصائية بين الهياكل التنظيمية لإدارات تقنية المعلومات وبين توافق الوظائف المستخدمة في مجال حماية شبكات المعلومات.
٤. لا توجد علاقة ذات دلالة إحصائية بين إجراءات حماية شبكات المعلومات وبين إتباعها والعمل بها.
٥. لا توجد فروق ذات دلالة إحصائية بين التدابير الاحتياطية اللازمة لتجنب المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات المعلومات، وبين التدابير الفعلية المتخذة للتغلب على تلك المخاطر.

١-٥ أهداف الدراسة

١. حصر الأجهزة والبرامج المستخدمة لحماية الشبكات وطرق إعدادها وتحديثها.
٢. تحديد نقاط الضعف في الشبكات المدروسة وتدابير تقويمها.
٣. التعرف على مشكلات الهياكل التنظيمية في إدارات تقنية المعلومات، وعلاقتها بالوظائف الفنية والإدارية المطبقة في مجال الحماية، للوصول إلى إجراءات عمل مناسبة لتنفيذ سياسات الحماية.
٤. تحديد سياسات الحماية وإجراءات العمل اللازمة لتحقيق حماية عالية لشبكات المعلومات الرئيسة.
٥. حصر المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات المعلومات وحصر التدابير الاحتياطية اللازمة لتجنب تلك المخاطر.

١-٦ أهمية الدراسة

وفي هذه البيئة من شبكات المعلومات السريعة التغير تظهر في كل يوم فيروسات وبرامج ضارة جديدة، وفي كل يوم تطفو برمجيات وتغيب أخرى نتيجة عدم قدرة منتجيها على الاستمرار في التسابق والمنافسة، وفي هذا الموج تظهر الثغرات وتكثر مواطن الضعف وتبرز أهمية الحاجة لترقية التجهيزات وتحديث البرمجيات، وفي بحر التغيرات في تقنية المعلومات تجد قراصنة المعلومات الذين يستغلون ما يُكتشف من مواطن الضعف في التصميمات، وتوزيع التجهيزات وتركيب البرمجيات وإعداد كل ذلك في لوحة متناسقة يتم تحديثها باستمرار حتى تبقى متماسكة خالية من الثغرات لا يمكن خرقها واستغلالها بالاختراق والقرصنة أو التخريب مما يؤدي إلى خسائر معنوية ومادية لا حصر لها، وحتى القراصنة المبتدئون فإنهم يجدون هنا وهناك من خلال شبكة الانترنت كثيرا من الشبكات

غير المحصنة والتي تكثر فيها الثغرات الناتجة عن عدم التحديث وعدم اتخاذ التدابير اللازمة للحماية وعدم اختيار التصميمات المناسبة ويمكن بيان أهمية الدراسة كما يلي:

١. ستكون هذه الدراسة واحدة من المراجع المهمة للعاملين في مختلف القطاعات الأمنية عسكرية كانت أو مدنية والعاملين في المجالات الصناعية والتجارية حكومية كانت أم أهلية في مجال تقنية المعلومات بمختلف تخصصاتها كالشبكات وقواعد البيانات والمعلومات فيما يخص موضوع الحماية من زاوية الأمن والاحتياط للحفاظ على سلامة البيانات وتكاملها واعتماديتها والحفاظ على سرية المعلومات الموجودة في موارد الشبكات أو المنتقلة فيها والتقليل من إصابتها بالفيروسات والبرامج الضارة وتضييق احتمالات اختراق تجهيزاتها وبالتالي قرصنة مواردها وتجنب الوقوع في الأعطال والتوقف عن العمل وتكبد الخسائر الفادحة أو تعريض السمعة الوطنية والتجارية للضرر.

٢. تؤمن هذه الدراسة مصدرًا مهما للعاملين بمجال التحقيق في الجرائم المستحدثة حيث يستفاد منها بالتعرف على عناصر بناء نظم حماية الشبكات وتفاصيل تثبيتها ومخرجات أجهزتها من تسجيلات حركة البيانات اليومية التي تساعد في جمع الأدلة الجنائية في حالات التحقيق والتحري في مجال الجرائم الإلكترونية.[١١]

٣. ستكون مرجعاً مهماً لإدارات التخطيط والجودة والموارد البشرية فهي تطرح حلولا للهيكل التنظيمي المناسب للأعمال الفنية المطلوبة في إطار الهيكل التنظيمي للمنظمة وتحاول التوصل إلى إجراءات مناسبة تتداخل فيها المهام الفنية والأعمال الإدارية في إطار الهيكل التنظيمي لأقسام وإدارات تقنية المعلومات في المنظمة المدروسة.

٤. تقدم إجراءات تنظم عملية الحماية لجميع مكونات الشبكات ومواردها للمؤسسات محل الدراسة وتضبط عمليات إضافة أو إزالة مكونات الشبكة، و تنظم العلاقة بين الإدارات ذات الصلة في إطار الصلاحيات المعطاة لمنسوبي تلك الإدارات وتبين هذه الدراسة إجراءات أمن المعلومات المطبقة على الشبكات ومواردها مع توضيح مواطن الضعف ومواطن القوة فيها، وإيجاد التوصيات التي تفيد في تلافي نقاط الضعف وتحسين نقاط القوة بناء على نتائج التحليل.

٥. تقدم للعاملين في الأجهزة الأمنية مرجعاً أمنياً مهماً للوقاية من الجرائم الالكترونية.

٦. تقدم هذه الدراسة معلومات مفيدة جداً للراغبين في تصميم الشبكات ومراكز المعلومات آخذين بالاعتبار الاحتياطات الأمنية اللازمة لحماية شبكاتهم مختصرين الجهد والمال والوقت.

---

[١١] انظر محمد أمين البشري، مرجع سابق، ص٢٣

٧. تتفرد هذه الدراسة من بين الدراسات العربية السابقة بالجمع بين علوم الحاسب الآلي وبخاصة أمن المعلومات بتناولها موضوع الحماية الفنية للشبكات وعلوم إدارة الأعمال بتناولها موضوع الهيكل التنظيمي والموظفين والإجراءات والتوثيق.

١ ٧ مصطلحات الدراسة:

تستخدم الدراسة مفاهيم ومصطلحات علمية فيما يلي تحديد موجز لها:

١-الحاسب الآلي: "هو الجهاز الذي يقبل أو يعالج أو يخزن أو يسترجع البيانات من خلال برامج الحاسب الآلي، وهي سلسلة مشفرة من التعليمات أو النصوص يمكنها معالجة البيانات وإعطاء نتائج تلك المعالجة" [١٢]. وله تسميات أخرى كالحاسب المكتبي (Desktop) ومحطة العمل (Workstation) والحاسب المحمول (Laptop) ويمكن عدّ الحاسب الكفّي حاسبا آليا.
وعندما يكون الحاسب الآلي عضواً في شبكة يسمى محطة عمل (workstation) أو مضيف (Host)، وتبعاً لوظيفته في الشبكة يثبت عليه برنامج عميل (Client) أو خادم (Server).
وعند ارتباط الحاسب بشبكة الانترنت يعين له عنوان فريد من خلال بروتوكول عناوين الإنترنت (IP Address) يتم تعيينه بطريقة آلية أو يدوية والطريقة الآلية تستخدم بروتوكول (DHCP) [١٣] أما اليدوية فيقوم مستخدم الحاسب بإدخال العنوان يدوياً بعد حصوله على التعليمات المناسبة من مدير الشبكة أو من عناصر المساندة الفنية.
٢-**الجهاز الشبكي** (network node) هو أي جهاز مربوط بالشبكة ويأخذ عنوان شبكة فيزيائي (في طبقة ربط المعطيات (data link) وقد يكون طابعة أو حاسب آلي أو فاكس أو ثلاجة أو كاميرا رقمية أو خادم .. إلخ وكل مضيف أو حاسب في الشبكة يعد نقطة شبكة (network node) ولا يمكن عدّ كل نقطة شبكة (Node) حاسباً أو مضيفاً، حيث أن أجهزة المودم (modems) والمبدلات switches لا تحتاج عناوين شبكة (IP) بالحالة الافتراضية ولا تعدّ مضيفات شبكية، والأجهزة الشبكية كالطابعات وأجهزة التوجيه (hardware routers) يتم تعيين عناوين لها ولكن لا يمكن عدّها مضيفات أو حاسبات أعضاء بالشبكة. [١٤]

---

[١٢] عفاف شمدين، **الأبعاد القانونية لاستخدامات تكنولوجيا المعلومات**، (دمشق: بدون ، ٢٠٠٣) ص ١٢١
[١٣] الأحرف: (DHCP) اختصار من أوائل الكلمات بالعبارة Dynamic Host Configuration Protocol
[١٤] مترجم من ويكيبيديا ومتوفر على الرابط http://en.wikipedia.org/wiki/Host_computer

٣-الشَّبَكَة: لغةً هي شَرَكَةُ الصياد وجمعها شَبَكٌ وشِباك. شَبَكَهُ يَشْبِكُهُ فاشْتَبَكَ، وشَبَّكَهُ تشبيكاً فتَشَبَّك: أنشَب بعضه في بعض فنَشِبَ، وشَبَكَةِ الأمورُ واشْتَبَكَت وتشابكت: اختلطت والْتَبَسَت، وطريق شابِك: مُتداخل مُلتبِس، وأسدٌ شابِك: متشابِكُ الأنياب.[١٥]
الشبكة اصطلاحاً: هي مجموعة من الحاسبات تُعطى عناوين شبكية عمومية من قبل مسؤول الشبكة ويمكن ربط هذه الحاسبات في مجموعات حسب توضُّعها في المناطق الجغرافية.[١٦]

٤-الشبكة المحلية (LAN) : مجموعة من الحاسبات ترتبط فيما بينها وتتوضع على مساحة جغرافية محدودة كمبنى واحد أو مجموعة من المباني قريبة من بعضها بعضاً.

٥-الشبكة الواسعة (WAN) : مجموعة من الحاسبات ترتبط فيما بينها وتتوضَّع على مساحة جغرافية واسعة في إقليم أو مجموعة من الدول. وغالباً ما تكون الشبكة الواسعة مجموعة من الشبكات المحلية تنتشر في مناطق جغرافية مختلفة وترتبط فيما بينها.

٦-الشبكة الرئيسة: اصطلاحا هي مجموعة من الحاسبات مربوطة فيما بينها بوسط نقل، تحتوي أجهزة خادم لتخزين ومعالجة البيانات وتحوي على حدودها بوابات للتصفية والحماية، وخصوصاً تلك الحدود التي تتصل بالشبكات العامة كالانترنت. وتتكون الشبكات الرئيسة من مجموعة من الشبكات المحلية (LANs): وتُعد الشبكة المحلية والشبكة الواسعة من وُجهة نظر الباحث شبكاتٍ رئيسةً.

٧-الحِمَايَةُ لغةً: حَمَى الشيْءَ يَحمِيهِ حَمْياً وحِمايَةً، مَنَعَهُ، وقد حماهُ حَمياً وحَمية وحِماية وحَمْوَةً. وحَمى المريض ما يضُرُّره: مَنَعَهُ إيَّاه ، فالحِمَايةُ لُغَةً المنعُ. [١٧]

٨-الحماية (protection): **اصطلاحا:** بالنسبة لحماية طريق السفر يعني الأفعال والاحتياطات التي تؤدي لضمان مرور ووصول المسافرين بأمان، وبالنسبة لحماية المنتجين في بلد ما فهي مجموعة النظم والإجراءات التي تحمي المنتجين المحليين من المنافسين الأجانب. [١٨]

---

[١٥] **انظر**: الفيروز آبادي ، **القاموس المحيط** ، مؤسسة الرسالة دار الريان للتراث ، بيروت، ١٩٨٧ ط٢ ص١٢١٩

[16] **See:** Chris Brenton, Cameron Hunt, **Network Security** (Marian Village, Alameda: Sybex,2003) p42

[١٧] **انظر**: معجم القاموس المحيط ، مرجع سابق، ص١٦٤٧

[١٨] ترجمة بتصرف من answers.com متوفر على الرابط http://www.answers.com/protection#Dictionary_ans

٩-الحماية الأمنية لشبكة الحاسب الآلي: هي العملية التي يتم فيها حماية الأصول المعلوماتية الرقمية وهدفها هو حماية الخصوصية وصيانة التكامل وضمان الاستمرارية. وبهذه الأهداف تتم الحماية من جميع التهديدات والثغرات الأمنية للوصول إلى تحقيق أهداف المنظمة. ويُقصد بالتهديد الدخول غير المخول ويُقصد بالثغرات الأمنية نقاط الضعف الناتجة عن سوء إعداد البرمجيات ومكونات الأجهزة وضعف التصميم أو إهمال المستفيد وسوء استخدامه.[١٩]

١٠-شبكة الانترنت: اسم إنترنت في الإنجليزية (Internet) يتكون من البادئة (inter) التي تعني "بين" و كلمة (net) التي تعني "شبكة"، أي" الشبكة البينية "و الاسم يدل على بنية الإنترنت باعتبارها "شبكة ما بين الشبكات" أو شبكة من شبكات (network of networks) أو (interconnected networks)، و مع هذا فقد شاعت خطأ في وسائل الإعلام العربية تسمية الشبكة الدولية للمعلومات ظناً أن المقطع (inter) في الاسم هو اختصار كلمة (international)التي تعني دولي.

و كما يدل اسمها فإن شبكة الإنترنت هي شبكة ما بين عدة شبكات تدار كل منها بمعزل عن الأخرى بشكل غير مركزي ولا تعتمد أيا منها في تشغيلها على الأخريات، كما قد تستخدم في كل منها داخليا تقنيات شبكية مختلفة، وما يجمع بينها هو أن هذه الشبكات تتصل فيما بينها عن طريق بوابات تربطها مواصفات مشتركة قياسية. [٢٠]

ترد مصطلحات متعددة باللغة العربية يقصد بها شبكة الانترنت ومنها: الشبكة العالمية للمعلومات، شبكة النسيج العالمية، شبكة الانترنت وفي اللغة الانكليزية : (Net), (Web), (www), (Internet)) ووفق المفهوم العام المتداول تعرّف الانترنت بأنها" شبكة الشبكات". [٢١]

الانترنت وسيلة اتصال عالمية مهيمنة في كثير من بقاع العالم حيث أصبحت الانترنت أداة اتصال للوصول إلى ٥٠ مليون مستخدم خلال ٤ سنوات فقط بينما استغرق التلفزيون ١٣ سنة والحاسب ١٦ سنة والراديو ٣٨ سنة والهاتف ٧٤ سنة. وللانترنت خصائص اتصالية منها: سرعة انتقال

---

[19] **See:** Cisco systems inc. **Fundamentals of network security** (Indiana: Cisco press,2004) p5

[٢٠] متوفر على الموقع إنترنت http://ar.wikipedia.org/wiki/

[٢١] **انظر**: فايز بن عبد الله الشهري ، **مرجع سابق**، ص١٧٨

المعلومة والدقة العالية وخصوصية الاتصال بين المرسِل والمستقبِل وعالمية الحركة والمحتوى والاستخدام وقلة التكلفة.[٢٢]

والانترنت ظاهرة أمنية حيث يوجد تلازم بين انتشار استخدامات الشبكة كوسيلة جماهيرية وازدياد الآثار السلبية المتصاعدة لمختلف خدمات الانترنت، ويمكن أن تقدم الانترنت خدمات جمّة للعصابات الإجرامية والمنظمات الإرهابية تمكنهم من تبادل المعلومات بالأشكال المختلفة كالرسائل النصية أو رسائل الوسائط المتعددة أو بالمحادثة الفورية وتستطيع هذه العصابات أن تحمي اتصالاتها بنظم مشفرة وباستخدام حِيَل تُصَعّب سبُل كشفهم وملاحقتهم فيضعون الخطط بعيداً عن عيون الأمن، وعلى سبيل المثال أكدت تقارير إعلامية استخدام الإنترنت كوسيلة اتصال للتنسيق بين منفذي الهجوم على مبنى مركز التجارة العالمية في نيويورك ومبنى (البنتاغون) في ١١ سبتمبر عام ٢٠٠١م.[٢٣]

١١- معدل نقل البيانات (تدفق) (Bandwidth) : هو قياس كمية البيانات التي يمكنها الانتقال من مكان إلى آخر في فترة زمنية معطاة ويوجد استخدامان شائعان لهذا المصطلح الأول يتعامل مع الإشارات القياسية والثاني يتعامل مع الإشارات الرقمية ويقصد الباحث في هذا الدراسة الاستخدام الثاني. ويستخدم هذا المصطلح لوصف الشبكات المحلية والواسعة للدلالة على مقدرتها ولما كانت وحدة الأساسية للبيانات هي البِت (bit) والوحدة الأساسية للزمن هي الثانية (second) وإذا كان المراد وصف كمية البيانات المتدفقة في فترة زمنية محددة فيمكن استخدام الوحدة بِت بالثانية (bits per second) لوصف هذا التدفق وعليه وحدة قياس معدل انتقال البيانات هي بِت بالثانية ويعد هذا المعدل بطيء جداً ونظرا للتطور التقني الباهر فإن المعدل الشائع الاستخدام بوحدات الكيلو والميجا والجيجا حيث: 1 kbps = 1000 bps، 1 Mbps = 1000.000 bps، 1 Gbps = 1000.000.000 bps ويمكن تمثيل المعدل بمساحة سطح مقطع أنبوب نقل المياه، أو عدد مسارات طريق السيارات، وكلما كان المعدل أكبر كان أفضل.[٢٤]

١٢-البرمجيات الخبيثة (Malware) : جاءت هذه التسمية من الكلمتين (malicious software) وتعني البرمجية الماكرة أو الخبيثة، وهي برامج مخصصة للتسلل إلى أنظمة

[٢٢] **انظر**: فايز بن عبد الله الشهري ، مرجع سابق، ص ص ١٧٤-١٧٥
[٢٣] **انظر**: فايز بن عبد الله الشهري ، مرجع سابق، ص ١٨٢
[24] **See**: Cisco systems, inc: (Indiana, Cisco press, **Cisco networking academy program, first year companion guide** 2nd ed., 2001) PP 32-33.

الحاسب وتدميرها بدون معرفة المستخدم. وما إن يتم تثبيت البرمجية الخبيثة فإنه من الصعب جداً إزالتها. وبحسب درجة خطورة البرمجية من الممكن أن يتراوح أذاها من إزعاج بسيط إلى أذىً غير قابل للإصلاح يتطلب إعادة تهيئة القرص الصلب على سبيل المثال. ومن الأمثلة على البرمجيات الخبيثة الفيروسات، وأحصنة طروادة. ويجب أن لا يتم الخلط بين البرامج الخبيثة والبرامج المعيبة، حيث أن الأخيرة تكون برامج مكتوبة لأهداف مشروعة لكنها تحوي أخطاء. [٢٥]

١٣-الفيروسات: فيروس الحاسب الآلي (Virus) هو برنامج صغير له قدرة على العمل في الخفاء والتكاثر ويتم وضعه في الحاسب بواحدة من طرق الانتقال ليصيب الحاسب بالعدوى وفقا للأغراض التي صُمم من أجلها، وليس شرطاً أن تكون لبرنامج الفيروس أهداف تخريبية، ويتميز الفيروس عن البرامج الضارة التي تكرر نفسها مثل أحصنة طروادة (Trojans) والقنابل المنطقية (Bombs) [٢٦] . ويُعرف فيروس الحاسب الآلي بأنه برنامج ينفِّذ وينسخ نفسه دون معرفة المستخدم ويوصف الفيروس عموماً بأنه برنامج قادر على التكاثر، وتعدّ عملية النسخ بحد ذاتها غاية من غاياته، وبعض النُّسخ المولدة تكون فيروسات أيضاً ، ويلتصق الفيروس بمضيف ما بحيث يؤدي تنفيذ المضيف لعملية ما إلى تنفيذ الفيروس ضمناً [٢٧]. وحيث أن البرمجيات المضادة للفيروسات تقوم بعمل رائع في كشف وصد وإزالة الفيروسات الكامنة في الأقراص المرنة والأقراص الضوئية والذاكرات (الفلاش) وانتقال هذه الفيروسات بطيء نسبيا بالنسبة لنشر الفيروسات من خلال الانترنت والبريد الالكتروني حيث تطلب الأمر من مصنعي برمجيات الحماية إلى تحديث قواعد بيانات الفيروسات والبرامج الضارة الأخرى آنيا. لأن القراصنة يطورون بدورهم برمجيات القرصنة والتخريب مستغلين الثغرات الأمنية في أي شيء كنظم التشغيل أو أجهزة الشبكات بل حتى تصرفات الناس (الهندسة الاجتماعية) ونقص معلوماتهم.

١٤-البرامج الضارة: هي البرامج التي يمكن أن تؤثر سلباً على أداء الحاسبات الآلية وأهمها البرمجيات الخبيثة والفيروسات والبريد الدعائي وأحصنة طروادة والديدان.

١٥-البيانات والمعلومات: البيانات (Data) هي مجموعة من الحقائق الأولية أو الخام يتم تسجيلها بوساطة رموز معينة (كلمات، حروف، أشكال، أرقام ...) مثل عدد وأسماء العاملين، وعدد ساعات

---

[٢٥] متوفر على الرابط "برمجيات/http://ar.wikipedia.org/wiki/" في موقع ويكيبيديا
[٢٦] **انظر**: عبد الحميد بسيوني **الحروب الإلكترونية وقرصنة المعلومات (القاهرة:** دار الكتب العلمية للنشر والتوزيع، ٢٠٠٤) ص١٣
[٢٧] **انظر**: فادي حجار **تشريح الفيروسات (حلب:** شعاع للنشر والعلوم، ٢٠٠٣) ص٩

العمل في الأسبوع. وأما المعلومات فهي نتاج مجموعة من البيانات المنظمة بطريقة هادفة بما يجعل لها قيمة إضافية على قيمة البيانات نفسها. وهي مخرجات ناتجة من معالجة البيانات تسهل اتخاذ قرار أو إصدار حكم بشكل أفضل.[٢٨]

١٥-نظُم المعلومات: يُقصد بكلمة نظام (System) مجموعة من العناصر المتفاعلة معاً (المتساندة بنائياً والمتكاملة وظيفياً) لإنجاز هدف معيّن. ونظام المعلومات (Information System) هو مجموعة من العناصر والمكونات المترابطة معاً، تجمع البيانات وتعالجها وتخزنها وتُخرج المعلومات حسب الطلب. بمعنى أن نظام المعلومات هو مجموعة من القواعد والإجراءات المحددة والمصممة والمحتفظ بها تُستخدم بمساعدة تجهيزات المعلومات بغرض تقديم معلومات للإدارة وللبحوث الأساسية والتطبيقية. وتُعدّ نظم المعلومات بمثابة الشبكة العصبية التي تعمل من خلالها النظم الأخرى كنظام شؤون الموظفين والنظام المالي ونظام الاتصالات الإدارية ونظام القبول والتسجيل ونظام المستودعات، وبدونها يصعب تشغيل النظم الأخرى فهي تلعب دور الشرايين والأوردة التي تتدفق من خلالها المعلومات.[٢٩]

١٦-قاعدة البيانات (Data base): هي مجموعة متكاملة من البيانات تم تنظيمها على الصورة التي تمكن العديد من المستفيدين بالمؤسسة من التعامل معها [٣٠]. وتُبنى قواعد المعلومات بصورة أساسية على جداول مترابطة مع بعضها، وتتكون الجداول من أعمدة وصفوف وسجلات حيث أن **العمود** (Column): هو الوحدة الأساسية للجدول أو هو خاصة من خواص العنصر[٣١].
والصف (Row): هو مجموعة من القيم المفردة لأعمدة الجدول، فلكل عمود في الجدول توجد قيمة معينة ويضم الصف هذه القيم جميعها وهو ما يقابل السجل في الملفات.[٣٢]
والسجل (Record): هو ما يمثله الصف في جدول البيانات، فبالنسبة لجدول الموظفين يكون لكل موظف سجل (أي صف).[٣٣]

١٧-المنظمة المعلوماتية هي كل منشأة أو مؤسسة أو منظمة حكومية أو أهلية تعتمد في أعمالها على تقنية المعلومات بحيث يكون لديها قواعد بيانات وشبكة حاسب آلي ومحطات عمل وتتصل

[٢٨] مدحت أبو النصر مرجع سابق ص ص٥٤-٥٥
[٢٩] مدحت أبو النصر مرجع سابق ص ٦٥
[٣٠] حسن طاهر داود، الحاسب وأمن المعلومات، (الرياض: معهد الإدارة العامة، ٢٠٠٠) ص٢٧٢
[٣١] حسن طاهر ٢٠٠٠ مرجع سابق ص٢٧٣
[٣٢] حسن طاهر ٢٠٠٠ مرجع سابق ص٢٧٣
[٣٣] حسن طاهر ٢٠٠٠ مرجع سابق ص٢٧٣

بالانترنت، ويتوفر فيها مركز بيانات واحد على الأقل وحاسبات للمستفيدين وتتأثر سلباً بتوقف واحد أو أكثر من المكونات الحرجة لتقنية المعلومات.

١٨-الهيكل التنظيمي للمؤسسة/الشركة: يعتمد الهيكل التنظيمي على مبدأ التدرج الذي يحدد العلاقات نحو الاتجاهات الأربعة اليمين واليسار والأعلى والأسفل وقد يظهر على أساس التسلسل القيادي وقد يكون على أساس الوظائف ولا يبتعد عن المظهر الهرمي وفيه تتوسع السلطة والمسؤولية حسب التدرج في المستويات ولكل منصب في التنظيم دور يناسبه من حقوق وواجبات وامتيازات والالتزامات تحدد سلوك من يقوم بهذا الدور بشكل رسمي ويفيد الهيكل التنظيمي في توزيع النشاطات المحددة على أشخاص معينين وتحمل المسؤولية من كل عضو فيه والتنسيق بين هذه النشاطات ويعتمد تقسيم الوظائف والمهام في التنظيم على تقييم العمل التقني وبالتالي على تحليل الوظائف المختلفة في المؤسسة وتوفير الأشخاص المناسبين وهذا يدخل ضمن إطار تحليل الوظائف وتوظيف الموارد البشرية في المكان المناسب من أجل التقيد بإستراتيجية المؤسسة الرامية لتحقيق أهداف المؤسسة ضمن برامج وسياسات وأهداف المؤسسة من جهة والتكاليف الاقتصادية والاجتماعية من جهة أخرى العناصر المكونة للمؤسسة متعددة وبالتالي فان الهيكل الكلي هو في الحقيقة تركيب أمثل لمجموعة من الهياكل كالهيكل البشري الذي يحدد دور ومجال وعلاقات أعضاء المؤسسة، والهيكل المادي الذي يحدد أمكنة وحدات المؤسسة وأمكنة التجهيزات داخل هذه الوحدات، والهيكل القانوني الذي يحدد الشكل القانوني للمؤسسة، شركة أسهم، شركات قابضة أو فروع، والهيكل المالي: الذي يحدد مصدر رؤوس الأموال للمؤسسة وتوزيعها في أرض الواقع توجد خيارات أساسية أثناء تصميم هندسة هيكل تنظيمي للمؤسسة وتتمثل في كيفية التخصص في العمل، ومكان وضع السلطة، وإلى أي درجة يمكن وضع هيكل لا مركزي، وكيفية التنسيق.[٣٤]

١٩-إجراءات أمن المعلومات: الإجراء (Procedure): طريقة العمل، طريقة، أسلوب إنجاز أو تطبيق شيء ما. والإجراء القياسي بشكل عام هو سلسلة من الخطوات تُؤخذ لإنجاز شيء ما، وفي المنظمات هي مجموعة من الطرق أو النماذج المعدة لتنفيذ الأعمال الداخلية للمنظمة كالأعمال التجارية والنادي والحكومة، وفي علوم الحاسب الآلي هي مجموعة من التعليمات التي تُنجِز بموجبها مهام محددة مثل (الروتينات) الفرعية أو الوظائف [٣٥].

وإجراءات أمن المعلومات يقصد بها، سلسلة من العمليات مكتوبة ومعتمدة من قبل أعلى سلطة في المنظمة، تُنفذ باستمرار بغرض المحافظة على أمن معلومات المنظمة.

---

[٣٤] بتصرف من الرابط http://ar.wikipedia.org/wiki/الهيكل_التنظيمي في موقع ويكيبيديا

[٣٥] http://www.answers.com/topic/procedure

٢٠-الكفاءة (Efficiency): تشير الكفاءة إلى القدرة على إنتاج أكبر قدر من المخرجات بقدر ثابت من المجهود، أوالقدرة على بذل أقل مجهود لإنتاج قدر ثابت من المخرجات. كما تشير إلى أداء العمل المطلوب بأفضل طريقة، فالشخص الكفء هو الذي يحقق أفضل النتائج أو المخرجات بالمقارنة مع المدخلات المستخدمة في إنجازها، ويستطيع بالتالي خفض تكلفة الموارد المستخدمة في تحقيق تلك النتائج. والكفاءة هي الاستخدام الأمثل للموارد المتاحة لتحقيق حجم أو مستوى معين من النواتج بأقل التكاليف وهو من أهم مقاييس نجاح المؤسسات في تحقيق أهدافها.[٣٦]

٢١-مسمى الوظيفة: اسم يدل على وظيفة لعمل مجموعة من الواجبات والمهام في تقنية المعلومات هي المهن التي تختص بأعمال تقنية المعلومات مثل وظيفة أخصائي أمن معلومات ووظيفة مسؤول الشبكة المحلية،ووظيفة محلل نظم.

٢٢-سياسة أمن الشبكة: هي وثيقة عامة تحدد قواعد الوصول إلى شبكة الحاسب الآلي،وتحدد كيفية تنفيذ السياسات الأمنية وتضع الرسومات اللازمة لتوضيح توضُّع اللبنات الأساسية لشبكة الحاسب للوصول إلى بيئة معلوماتية آمنة. و تتكون الوثيقة من صفحات عديدة مكتوبة، وتُنشأ عادة من قبل لجنة متخصصة بحماية الشبكات.[٣٧]

٢٣-التحديث (Update): هو تثبيت الرقع البرمجية (التحديثات) لسد ثغرات أمنية أو عيوب برمجية وتتم عمليات التحديث بتنزيل تلك الرقع من موقع الشركة المنتجة على الانترنت وتثبيتها في المنتَج إما يدويا أو تلقائياً بطريقة الجدولة الآلية.

٢٤- **التحكم بالوصول** (Access Control): يحدد انسياب المعلومات من مصادر النظام إلى حسابات الأشخاص أو محطات العمل المرخص لهم فقط.[٣٨] من خلال لوائح التحكم بالوصول (Access Control Lists).

---

[٣٦] متوفر على الرابط http://ar.wikipedia.org/wiki/الكفاءة في موقع ويكيبيديا

[٣٧] متوفر على الرابط http://en.wikipedia.org/wiki/Network_security_policy في موقع ويكيبيديا

[38] **See:** Cisco systems inc. **Fundamentals of network security** (Indiana: Cisco press,2004) p727

٢٥- الاختراق (hacking): اختراق الشبكة هو محاولة الدخول إلى جهاز عضو في شبكة حاسب آلي من قبل شخص غير مصرح له بالدخول إلى ذلك الجهاز أو تلك الشبكة وذلك بغرض الإطلاع أو السرقة أو التخريب أو التعطيل أو زرع الفيروسات.

٢٦-التطبيقات: هي برمجيات جاهزة تستخدم من قبل المستفيد لأداء الأعمال المكتبية على جهازه المكتبي ومنها ما يثبت على الحاسب المكتبي وبعضها يثبت على حاسب مركزي ويتصل به المستفيدون عن طريق الشبكة مثل محررات النصوص والجداول الإلكترونية والعروض التقديمية وغالباً ما تكون بشكل حُزم برمجية.

٢٧-نظام التشغيل (Operating System): هو برنامج يقوم بتشغيل جهاز الحاسب الآلي ويشكل حلقة وصل بين المكونات المادية للحاسب من معالج وذواكر وأقراص تخزين من جهة، والمستفيد الذي يستخدم الحاسب الآلي من خلال برامج يفهمها كمحررات النصوص والجداول الإلكترونية والآلة الحاسبة وبرامج الرسم بالحاسب والألعاب وغيرها. ويمكن تصنيف أنظمة التشغيل تبعاً للجهاز الذي تشغله، فإذا كان الجهاز خادماً يكون نظام تشغيله نظام تشغيل خادم، وإذا كان الحاسب محطة عمل في شبكة يكون نظام التشغيل نظام تشغيل مخصص للأعمال، وإذا كان الجهاز منزلياً يكون نظام التشغيل مخصصاً للاستخدام المنزلي، وبالنسبة للأخير تكون ميزاته محددة فيما يخص التعامل مع الشبكات.

٢٨-مركز البيانات (Data Center): هو مجموعة من التجهيزات تتكون من أجهزة خادم وأجهزة تزويد الطاقة الكهربائية وأنظمة الإنذار والإطفاء وتتجمع في غرفة آمنة فيزيائياً، مزودة بأبواب متينة لها أقفال رقمية أو إلكترونية، ومزودة بنظام لتسجيل الداخلين إليها مع الوقت والتاريخ.

٢٩-الأنظمة الآلية: هي برامج مخصصة للأعمال مكونة من تطبيقات وقواعد بيانات ووظيفة هذه الأنظمة تحويل الأعمال اليدوية إلى أعمال قابلة للإنجاز عن طريق شبكة الحاسب الآلي مثل نظام الحسابات المالية ونظام المستودعات ونظام القبول والتسجيل.

الفصل الثاني

الإطار النظري والدراسات السابقة

٢-١ الإطار النظري

٢-٢ الدراسات السابقة

الفصل الثاني

الإطار النظري والدراسات السابقة

٢ ـ الإطار النظري

٢ ـ ١ تمهيد

تحاول هذه الدراسة التعرف على طرق ووسائل حماية الشبكات المستخدمة في المؤسسات التي تستخدم تقنية المعلومات والتعرف على إجراءات الأمان المستخدمة وأساليب إدارة أمن المعلومات ثم تحليلها وبناء على النتائج المستخلصة من التحليل يضع الباحث توصيات تفيد تلك المؤسسات في تحسين جودة الحماية لشبكاتها وترقية إجراءات الأمان المطبقة عليها، وتقديم توصيات خاصة بإدارة الحماية للوصول إلى أفضل حماية بظروف وصول مرنة لا تسبب تأخير في تعاملات المستفيدين.

وقد قسم الباحث هذا الفصل إلى مبحثين هما: الإطار النظري، والدراسات السابقة. ويتناول الباحث في الإطار النظري نظم المعلومات وأهمية حماية الشبكات وأهداف حماية الشبكات ثم ينتقل إلى معوقات الحماية.

٢ ـ ٢ نظم المعلومات

تكتسب شبكات المعلومات أهميتها من المحتوى الإلكتروني الذي يكون متوفرا في موارد الشبكات مثل أجهزة الخادم (Servers) ومخازن البيانات (Data Storages) وكذلك من أهمية البيانات المنسابة في خطوط الاتصال وعليه يرى الباحث ضرورة لاستعراض نظم المعلومات وبعض المفاهيم المتعلقة بها:

١ ـ **أنواع نظم المعلومات:** تقسم نظم المعلومات إلى نظم المعلومات التقليدية التي تُشَغَّل يدويا ونظم المعلومات المرتبطة بالحاسب الآلي والتي تعالج إلكترونيا والمهم هنا تلك النظم المرتبطة بالحاسب الآلي.

٢ -المكونات الأساسية لنظام المعلومات المرتبط بالحاسب الآلي:

يمكن تحديد هذه المكونات بالآتي:

أ - المدخلات (Inputs): وهي بيانات يتم إدخالها بالنظام بغرض معالجتها.

ب -المعالجة (Processing): وفيها يتم معالجة المدخلات وإنتاج معلومات ذات دلالة مفيدة باستخدام تقنية المعلومات والتي من عناصرها: أجهزة الحاسب الآلي (Hardware)، وبرمجيات الحاسب الآلي (software)، وقاعدة البيانات (Database)، وإجراءات النظام (procedures)، والأفراد (staff) .

ت -المخرجات (outputs): هي النتائج المرجوة من نظام المعلومات في إطار معالجة المدخلات.

ث -التغذية العكسية (Feedback): هي عملية إرجاع نتيجة تقييم المعلومات التي تم الحصول عليها من المخرجات، لاستخدامها في المدخلات بغرض تحسين نوعية المدخلات التي تعطي مخرجات أفضل.[٣٩]

٣ -المهام المنفذة بوساطة نظم المعلومات المعالجة إلكترونياً:

تُقسم نظم المعلومات المعالجة إلكترونياً إلى أربعة أنواع رئيسة هي:[٤٠]

أ - نظم دعم القرارات (DSS)

ب -نظم المعلومات الإدارية (MIS)

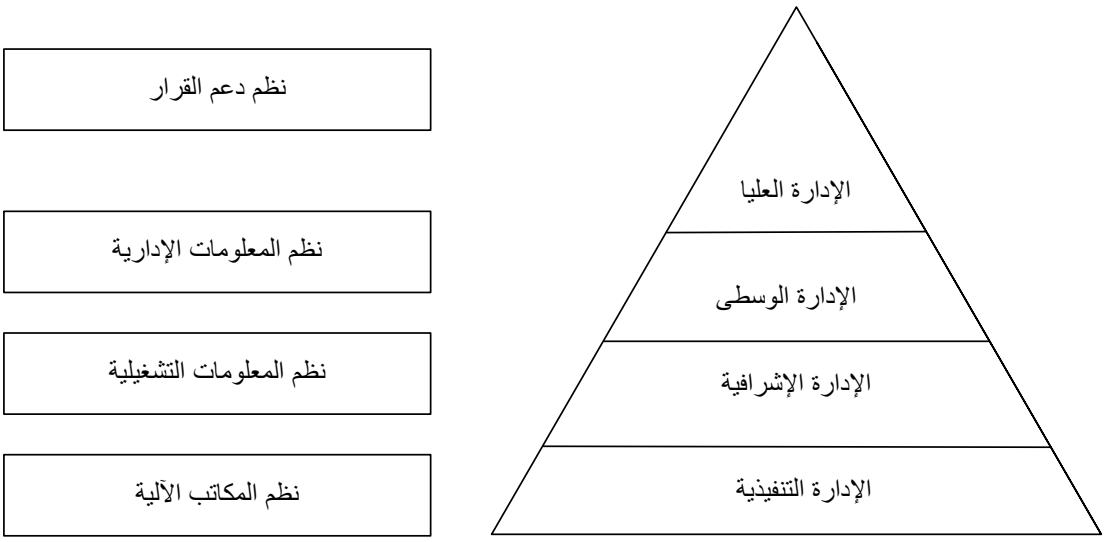
ت -نظم المعلومات التشغيلية (OIS)

ث -نظم المكاتب الآلية (AOS)

والشكل (١) يوضح المستويات الإدارية في أي منظمة معلوماتية وما يقابل كل مستوى من نظم المعلومات المناسبة له. يبين هذا الشكل مستوى الإدارة وما يقابلها من نظم معلوماتية، إن قاعدة الهرم ضرورية لكل ما فوقها فالإدارة التنفيذية ضرورية للإدارة الإشرافية والإدارة الإشرافية ضرورية للإدارة الوسطى والإدارة الوسطى هامة للإدارة العالية وعليه فإن نظم المكاتب الآلية تلزم لنظم المعلومات التشغيلية ونظم المعلومات التشغيلية تلزم نظم المعلومات الإدارية ونظم المعلومات الإدارية ضرورية لنظم دعم القرار.

[٣٩] انظر مدحت أبو النصر مرجع سابق ص ص ٦٦-٦٧

[٤٠] انظر مدحت أبو النصر مرجع سابق ص ص ٦٩-٧٠

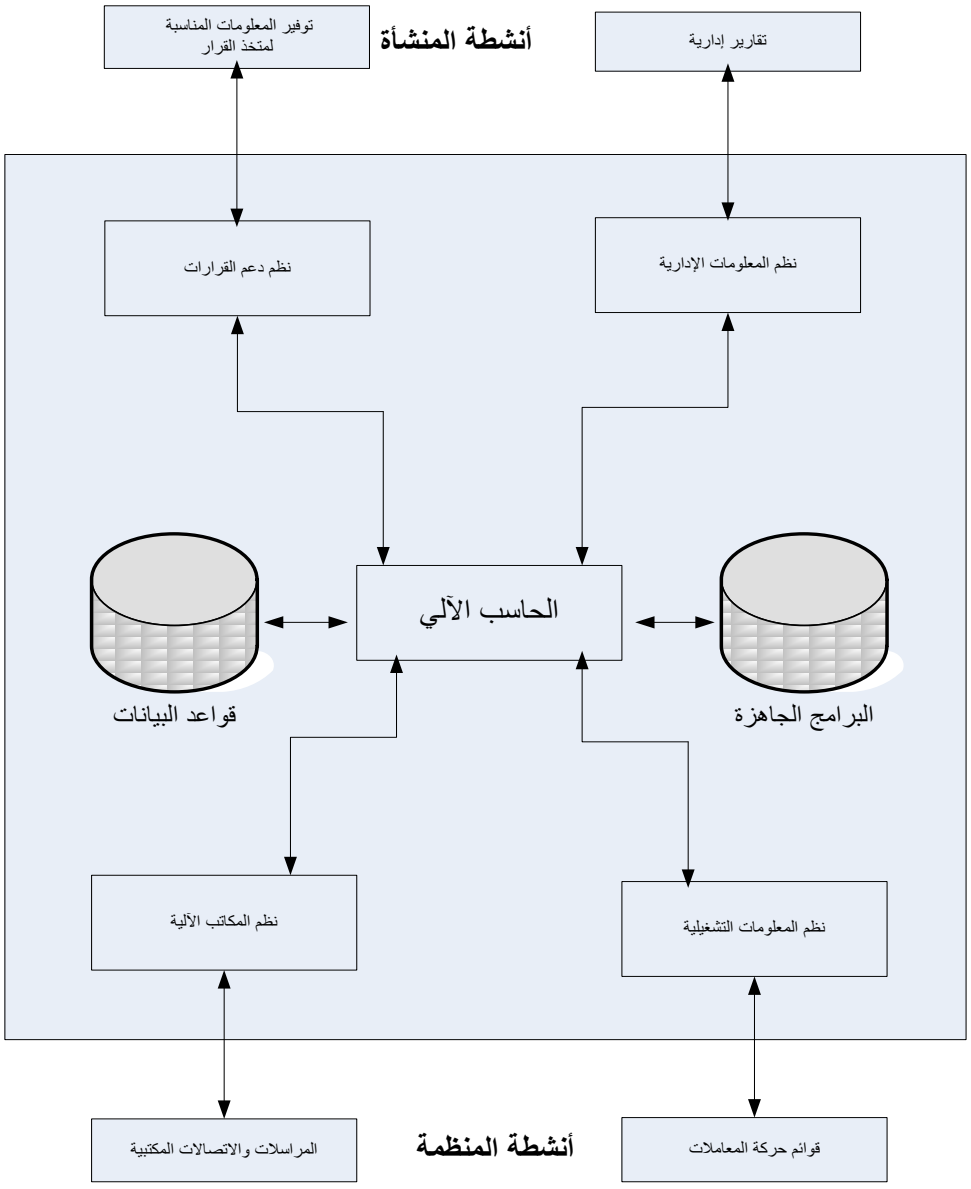


الشكل (١)

المستويات الإدارية في المنظمة المعلوماتية

ومن خلال معرفة المهام المنفذة بوساطة نظم المعلومات المرتبطة بالحاسب الآلي بالمنشأة [٤١] يتم معرفة العناصر التي تحتاج للحماية بما يتناسب مع قيمتها المادية أو المعنوية، حيث يوضح الشكل رقم (٢) أهم المهام التي يمكن تنفيذها بوساطة النظم المعالجة إلكترونياً داخل المنظمة، حيث تساعد نظم دعم القرارات الإستراتيجية الإدارة العليا في اتخاذ قرارات سديدة بمراجعة بيانات أقل. وتقوم نظم المعلومات الإدارية بتوفير المعلومات والتقارير الإدارية لأنشطة التخطيط و الرقابة و اتخاذ القرارات الاعتيادية. وتقوم نظم المعلومات التشغيلية بحصر وتجميع البيانات التي تعكس حركة المعاملات بالمنشأة، بينما تقوم نظم المعلومات الآلية بتنفيذ المهام المكتبية بطريقة آلية.

[٤١] انظر مدحت أبو النصر، مرجع سابق ص٧١



المهام المنفذة بوساطة نظم المعلومات
المرتبطة بالحاسب الآلي

الشكل (٢)

٢ ـ ٣ أهداف الحماية الأمنية لشبكات الحاسب الآلي:

إن الازدياد في اعتماد المؤسسات التجارية والمنشآت الوطنية والمنظمات الدولية على تطبيقات شبكات الحاسب والإنترنت بالتوافق مع التطور في تقنيات نقل الصوت مع البيانات، زاد من أهمية بقاء أنظمة المعلومات قيد التشغيل والعمل بصورة مستمرة (Availability) حيث أن توقفها يؤدي إلى خسائر كبيرة معنوية ومادية، ومهما اختلفت أسباب التوقف عن العمل فهي في النهاية نتيجة لضعف الحماية ضد ما يلي: سرقة المعلومات الخاصة والسرية، الخداع المالي ، الفيروسات، سوء الاستخدام من قبل المستفيدين داخل الشبكة، التلف والتخريب ، الوصول غير المرخص من قبل القراصنة، سرقة الحواسب المحمولة، هجمات رفض الخدمة، اختراق الأنظمة من خارج المنظمة أو المنشأة وغيرها. ويوجد ثلاثة أهداف رئيسة لحماية الشبكات وهي الخصوصية والتكاملية، والاستمرارية. (٤٢)

١- الخصوصية (Confidentiality): وتهتم بحماية البيانات من الكشف غير المرخّص والمسؤول عن حماية خصوصية وسرية البيانات المنشأة التي تمتلك تلك البيانات وبخاصة عندما تكون تلك البيانات خاصة بمستفيدين (عملاء) من خارج المنشأة، وعلى جميع العاملين بالمنظمة واجب الحفاظ على سرية بيانات منظمتهم ويعد هذا الواجب من المتطلبات القانونية. ومن المهم جداً عقد اتفاقيات حماية البيانات عند الاشتراك والتعاون في إنجاز الأعمال فيما بين المنظمات لحماية المعلومات المتبادلة وحماية معلومات كل منظمة من قبل الطرف الثاني ويدرج في تلك الاتفاقيات شرط ضرورة معالجة البيانات بطريقة آمنة تحميها من الكشف غير المرخص.

٢-السلامة (Integrity): تشير إلى ضمان كمال وسلامة البيانات بالمحافظة عليها من التعديل أو التخريب أو التدمير والتلف بطريقة غير مرخصة، على سبيل المثال: تكون السلامة مؤمنة عندما تكون الرسالة المستلمة يطابق الرسالة المرسلة، ولا بد من إجراء القياسات اللازمة للتأكد من سلامة كل البيانات بغض النظر عن خصوصيتها أو درجة سريتها.

٣-التوفّر (Availability): " تُعرَّف على أنها التشغيل المتواصل لأنظمة الحاسب الآلي، تحتاج التطبيقات مستوياتٍ مختلفة للتوفُّر، تبعاً لتأثُّر العمل (business) سلباً بفترة التوقف، وحتى يستمر تطبيق ما بالتوفر فيجب أن تكون جميع مكونات النظام متوفرة أيضاً بحيث تتضمن التطبيق وقاعدة البيانات والخادم وأجهزة التخزين وسلامة الشبكة من البداية إلى النهاية."(٤٣)

---

[42] **See**: Cisco systems, inc: (Indiana, Cisco press, **Cisco networking academy program, first year companion guide** 2nd ed., 2001) PP 32-33.

[43] **See**: Cisco systems, inc: (Indiana, Cisco press, **Cisco networking academy program, first year companion guide** 2nd ed., 2001) P 12.

ومصطلح التوفر (Availability) أيضا في الاتصالات يعني الدرجة التي يكون عندها النظام (أو الجهاز) قابلاً للعمل في حالة ملزمة عند بداية المهمة وعادة يُمثَّل التوفر بكسر عشري مثل ٠.٩٩٩٨ وأحياناَ بوحدة لوغاريتمية تدعى تسعات والتي تعتمد تقريبياً على عدد التسعات الموجودة بعد الفاصلة العشرية كأن يُقال خمسة تسعات عن التوفر 0.99999 . [٤٤]

و"التمثيل المبسط للتوفر A هو نسبة القيمة المتوقعة (Expected Value) لزمن بقاء النظام بحالة العمل (Uptime) إلى مجموع القيم المتوقعة لزمن بقائه بحالة العمل وزمن التوقفات (Down time) أو:

$$A = \frac{E[\text{Uptime}]}{E[\text{Uptime}] + E[\text{Downtime}]}$$

إذا عُرِّفت دالة الحالة X(t) بالشكل التالي:

$$X(t) = \begin{cases} 1, & \text{sys functions at time } t \\ 0, & \text{otherwise} \end{cases}$$

فإن التوفر يتمثل كما يلي:

$$A(t) = \Pr[X(t) = 1].$$
$$E[X(t)] = X.\Pr[X(t) = 1] \quad t > 0.$$

ويجب أن يعرّف متوسط التوفر في فترة على خط الزمن الحقيقي وباعتبار c ثابت عشوائي فإن متوسط التوفّر يعبَّر عنه بالشكل:

$$A_c = \frac{1}{c}\int_0^c A(t)\,dt, \quad c > 0.$$

وتُمثّل نهاية التوفّر (حالة الثبات) بالشكل:

$$A = \lim_{t\to\infty} A(t).$$

ويُعرّف متوسط التوفُّر أيضاً على فترة $[0, c]$ كالتالي:

[٤٤] انظر موقع مرجع الأسئلة على الرابط http://www.reference.com/browse/availability عن المصدر Federal Standard 1037C

$$A_\infty = \lim_{c\to\infty} A_c = \lim_{c\to\infty} \frac{1}{c}\int_0^c A(t)\,dt, \quad c > 0. \quad \text{(45)}$$

٢ ٤ التوازن في إجراءات الحماية والعناصر الضرورية لحماية الشبكات:

ولا بدّ من التعرف على مفاهيم ضرورية للتعامل مع حماية الشبكات بغرض الارتقاء لحماية متينة من دون تعقيد الوصول بالإضافة للعناصر الأساسية الضرورية لحماية الشبكات.

١-التوازن بين مرونة الوصول وصلابة الحماية:

إن الحماية الأمنية لشبكات المعلومات تصبح تحدّياً يحتاج كثيراً من الجهد والمال وخصوصاً عند أخذ مخاطر تضرر الأعمال من التوقفات. ويقع على كاهل مهندسي الشبكات مسؤولية إدارة سياسات الأمان للحفاظ على التوازن بين الوصول المرن وصلابة الحماية الأمنية. وعلى مدراء الشبكات أخذ القضايا التالية بالاعتبار بالنسبة للوصول الشفاف (Transparent Access):

أ - استمرارية الاتصال

ب - الأداء

ت - سهولة الاستخدام

ث - قابلية الإدارة

ج - التوفر

وعلى مسؤولي الشبكات أيضاً أخذ القضايا التالية بالاعتبار بالنسبة للحماية الأمنية (Security):

أ - إثبات الشخصية

ب - التخويل

ت - المسؤولية

ث - الضمان

ج - الخصوصية

ح - سلامة البيانات

٢-ومن العناصر الرئيسة لحماية الشبكة أمنياً[٤٦]:

---

[٤٥] ترجمة من الموقع answers.com متوفر على الرابط: http://www.answers.com/Availability

[٤٦] **See**: Cisco systems, inc: (Indiana, Cisco press, **Cisco networking academy program, first year companion guide** 2nd ed., 2001) P 13.

الاستخدام الناجح لتقنيات الشبكات يتطلب حماية البيانات ومصادر المعلومات في الشبكات من التلف ومن الانتهاك والاختراق، وتتضمن حلول حماية الشبكات خمسة حلول هي التعريف بالهوية، وحماية الحدود، وسرية البيانات، وإدارة الحماية، وإدارة السياسات.

أ – التعريف بالهوية (Identity):

يشير مفهوم التعريف بالهوية إلى التعريف الإيجابي الدقيق بهوية مستخدمي الشبكة ومضيفاتها وتطبيقاتها وخدماتها ومصادرها. وتوجد تقنيات معيارية تمكن من تنفيذ تعريف الهوية تتضمن بروتوكولات التخويل مثل خدمة الوصول للمستخدم الداخل من بعيد (RADIUS) [٤٧] ونظام التحكم بالوصول الطرفي المعدل (TACACS+) [٤٨]، وكيربيروس (Kerberos) [٤٩]، وأدوات كلمة المرور لمرة واحدة (OTP) [٥٠].

١– خدمة الوصول للمستخدم المتصل من بعيد (RADIUS):

تسمح هذه الخدمة لعدد من الأجهزة بالتشارك في قاعدة بيانات التحقق من أصالة هوية المتصل. وتقدم نقطة مركزية لإدارة الوصول البعيد لكل شبكة. وعند ورود طلب من عميل (RADIUS) سيُطلب منه اسم مستخدم وكلمة مرور ويتم تحويل هذه البيانات إلى خادم (RADIUS) فإذا كانت صحيحة يجيب الخادم بالموافقة ويسمح بوصول العميل إلى الشبكة، وإن لم تكن صحيحة يجيب الخادم بالرفض وبناءً عليه يتم إهمال طلب الوصول. استخدمت هذه الخدمة في بداية الأمر للاتصال البعيد عن طريق المودم وجدران الحماية ومن مساوئها أنها لا توفِّر خاصية التشفير ولذلك لابد عند اللزوم من توفير خاصية التشفير عن طريق خدمات إضافية.[٥١]

٢– نظام التحكم بالوصول الطرفي المعدل (TACACS+):

تقدم خدمة (TACACS+) طريقة بديلة عن خدمة (RADIUS) كأسلوب للوصول المركزي. كما في (RADIUS) فإن هذه الخدمة تجلب تصاريح الوصول من جدران الحماية إلى أجهزة الخادم الأخرى. وهي أيضا طريقة تحقق تستخدم أسماء المستفيدين وكلمات المرور، وبالمقابل فإن (TACACS+) تتوافق فقط مع بعض جدران الحماية بالمقارنة مع خدمة (RADIUS) الأكثر استخداماً. [٥٢]

---

47 RADIUS : Remote Access Dial-in User Service

48 TACACS+: Terminal Access Controller Access Control System +

49 The name comes from Greek mythology in which a three-headed dog guards the gates to Hades (Hades is the home of the dead beneath the earth, otherwise known as hell). ، An access control system

50 OTP: One-Time Password

51 **See:** Chris Brenton, Cameron Hunt, **Network Security** (Marian Village, Alameda: Sybex,2003) p٢٣١

52 **See:** Chris Brenton, Cameron Hunt, **Network Security** (Marian Village, Alameda: Sybex,2003) P١٤٨

٣ -كيربيروس (Kerberos):

أتى أصل تسمية كيربيروس من الأساطير اليونانية التي تروي أن كلباً ثلاثي الرؤوس يحرس بوابة مثوى الأموات الكائن تحت الأرض ويُعرف غير ذلك بالحُفرة.[٥٣] وفي مجال حماية الشبكات هو حلّ للتحقق من صحة الهوية وقد صُمِّم لتقديم تسجيل الدخول من خلال نقطة واحدة إلى بيئة متنوعة. تسمح هذه الخدمة بتحقق متبادل من الصحة مع إمكانية التشفير بين المستخدمين والخدمات. وتعتمد على كل مستخدم لتذكر اسم المستخدم الخاص به مع المحافظة على كلمة مرور فريدة. عندما يتم التحقق من صحة هوية مستخدم في نظام التشغيل المحلي يقوم عميل محلي بإرسال طلب تحقق إلى خادم (Kerberos)، يقوم الأخير بالاستجابة بإرسال الثبوتيات اللازمة مشفرة للمستخدم المعني، والعميل المحلي يحاول فك تشفير الثبوتيات مستخدماً كلمة المرور التي يمليها المستخدم، إذا كانت كلمة المرور صحيحة يكون المستخدم شرعياً ويُعطى بطاقة تصريح بالوصول تسمح بتشفير بيانات جميع جلسات الاتصال. وحالما يتم اعتماد شرعية المستخدم فلا يُطلب منه التحقق من الصحة عند محاولة وصوله لخدمات أخرى بالشبكة لأن البطاقة الصادرة بوساطة خادم (Kerberos) تقدم الثبوتيات اللازمة لدخول المستخدم إلى موارد إضافية بالشبكة. ومن أهم الدوافع لاستخدام هذه الخدمة أنها مجانية ويمكن تنزيل شفرة المصدر مجاناً واستخدامها.[٥٤]

ب -حماية حدود الشبكة (Perimeter Security)

تقدّم حماية الحدود الوسائل اللازمة لضبط الوصول للتطبيقات الحرجة في الشبكة والبيانات والخدمات للسماح فقط للمستفيدين الشرعيين بتمرير المعلومات عبر مكونات الشبكة، فيتم إعداد الموجهات والموزعات للقيام بتصفية الحزم (Packet filtering) وتثبيت جدران الحماية المتخصصة متعددة الوظائف (UTM) [٥٥] بالإضافة لبرامج الحماية من البرامج الضارة والفيروسات والبريد الدعائي، وتثبيت برامج إدارة الشبكة ومراقبة حركة حزم البيانات عند منافذ حدود الشبكة.

---

[٥٣] انظر موقع الأسئلة التجاري على الرابط http://www.answers.com/topic/kerberos-protocol-1

[54] **See:** Chris Brenton, Cameron Hunt, **Network Security** (Marian Village, Alameda: Sybex,2003) P٢٣٠

[55] UTM : Abbreviation of Unified Threat Management

ت –خصوصية البيانات (Data Privacy):

عندما تفرض ضرورة العمل حماية البيانات من التسريب يصبح التحقق من هوية المستخدم قضية حرجة ويتوجب على مسؤولي أمن الشبكات أن يفعّلوا خصائص التحقق من الهوية المتوفرة في أجهزة الاتصال الشبكية، ويمكن تفعيل خصائص التحقق من الهوية باستخدام تقنية الأنفاق (Tunneling) كتقنية التغليف العام (GRE) [٥٦] أو برتوكول أنفاق الطبقة الثانية (L2TP) [٥٧] التي تساعد على حماية خصوصية البيانات. وإلى جانب التحقق من الصحة تُستخدم تقنيات التشفير الرقمية كالحماية اعتماداً على عنوان بروتوكول الانترنت مثال ذلك (IPSec) وخصوصاً عند استخدام الشبكات الافتراضية الخاصة (VPNs) .

ث –إدارة الحماية الأمنية (Security Management) :

من المهم جداً تفقد حالة تدابير الحماية بالمراقبة الدورية للتأكد من بقاء الشبكة محمية بكل فعال، حيث تستطيع ماسحات مواطن الضعف تحديد النقاط الواجب مراعاة تدابير الوقاية لتعزيز الحماية، وتستطيع أنظمة كشف ومنع التلصص القيام بالمراقبة وتنفيذ ردود الأفعال المناسبة للحوادث المخالفة للقواعد المحددة في ملف الإعداد. وبذلك يمكن أن تحصل المنظمة على مشهد له معنى مفيد لكل من سيل البيانات وحالة حماية الشبكة.

ج –إدارة السياسات (Policy Management): [٥٨]

السياسة الأمنية تذهب بعيداً عن فكرة "إبقاء الأشخاص السيئين خارجاً" لتصبح وثيقة معقدة تعنى بضبط الوصول للبيانات وتصفح الانترنت واستخدام كلمات المرور والتشفير وملحقات البريد الالكتروني وغيرها. تصنف هذه القواعد حسب مجموعات أو أفراد في المنظمة. يجب أن تُبقي المستخدمين الماكرين خارجا ولا تأل جهدا في مراقبة وضبط الأشخاص المحتمل أن يكونوا خطرين ضمن المنظمة. والخطوة الأولى لإنشاء السياسة هي إدراك البيانات والخدمات القيِّمة (ولأي مستخدمين) ، ما احتمالات التعطل وهل يوجد أية حمايات متوفرة مسبقاً لمنع إساءة الاستخدام ، يجب أن تملي السياسة الأمنية سماحية الوصول بشكل هرمي بحيث تسمح للمستخدمين بالوصول للموارد الضرورية لإنجاز أعمالهم. وكبداية جيدة يمكن خلال كتابة وثيقة الأمن باستخدام نماذج من موقع معهد المعايير والتكنولوجية الدولي (National Institute for Standards and

[56] GRE: Abbreviation of Generic Routing Encapsulation
[57] L2TP: Abbreviation of Layer 2 Tunneling Protocol
[58] **See**: Cisco systems, inc: (Indiana, Cisco press, **Cisco networking academy program, first year companion guide** 2nd ed., 2001) P 14.

Technology) على الرابط http://www.nist.gov أو معهد (SANS) على الرابط http://www.sans.org/ وغيرهما. ويمكن أن تكون السياسات على شكل تعليمات يتم إعدادها على أجهزة شبكية مخصصة لحماية الشبكة.[٥٩]

بازدياد نمو الشبكات من حيث الحجم والتعقيد، يزداد الاحتياج لأدوات إدارة سياسات مركزية، أدوات معقدة يمكنها القيام بتحليل وتفسير وإعداد ومراقبة خصائص الحماية الضرورية. يمكن للأدوات المعتمدة على واجهة متصفح الويب أن تُسهِّل الاستخدام وتزيد من فعالية حلول حماية الشبكات.

٢ ٠ ٥ التوعية بالحماية الأمنية (Security Awareness)[٦٠]

عادةً لا يهتم المستخدم بحيثيات الحماية مما يتسبب بنتائج غير مرغوبة حيث تكون شبكات الحاسب الآلي بالنسبة له أداة تساعده لإنجاز متطلبات عمله الوظيفية وحسب، بل علاوة على ذلك غالباً ما يَعُدُّ إجراءات الحماية الأمنية ضرباً من الإزعاج أكثر منه مساعدة ووقاية. ولا بُدّ من إلزام كل منظمة بتقديم التدريب المناسب لموظفيها لتعليمهم ما يلزم حول أساسيات الحماية والكثير من المشكلات ذات الصلة بحماية المعلومات. ويجب أن يعتمد ذلك التدريب على سياسة الحماية الأمنية المتبعة في المنظمة. ويجب أن يشمل التدريب كلاً من الأفراد العاملين في تصميم أنظمة الشبكات وتركيبها وصيانتها. وتتضمن مناهج هذا التدريب المعلومات المتعلقة بالحماية وتقنيات الضبط الداخلية التي يمكن أن تتكامل مع تطوير أجهزة الشبكة و أنظمة تشغيلها وأساليب صيانتها.

ولابد من تدريب الأفراد المسؤولين عن أمن الشبكات تدريباً متعمقاً في المسائل التالية:

أ. تقنيات الحماية.

ب. منهجيات تقييم مواطن الضعف والتهديدات الأمنية.

ت. اختيار المعايير والتخطيط للتنفيذ الضوابط الأمنية.

ث. المخاطر الممكنة فيما لو لم يتم اتخاذ تدابير الحماية الأمنية المناسبة.

في المنظمات الكبيرة التي غالباً ما تكون منتشرة على مناطق جغرافية مختلفة تكون شبكة الحاسب كبيرة وتتكون من مجموعة من الشبكات المحلية (LANs) وعند ذلك يكون من الأفضل توظيف مدير شبكة محلية (LAN Administrator) لكل شبكة محلية (LAN) تُربط بالعمود الفقري

---

[٥٩] من ويكيبيديا على الرابط http://en.wikipedia.org/wiki/Network_security_policy

[60] **See**: Cisco systems, inc: (Indiana, Cisco press, **Cisco networking academy program, first year companion guide** 2nd ed., 2001) P 14.

لشبكة المنظمة ويكون هؤلاء المدراء للشبكات المحلية نقطة المركز لإتاحة ونشر المعلومات المتعلقة بنشاطات المنظمة في كل شبكة محلية.

ولا بُدّ من وجود قواعد لتنفيذ سياسات الحماية الأمنية قبل القيام بتوصيل الشبكة المحلية إلى العمود الفقري لشبكة المنظمة، ومن تلك القواعد:

أ. توفير سياسة للحماية الأمنية موحدة وموثقة بشكل جيد.

ب. توفير ضوابط تنزيل البرامج.

ت. توفير التدريب الكافي للمستخدمين.

ث. توفير خطة طوارئ الاستعادة عند الكوارث وتكون موثقة توثيقاً جيداً.

ويكون التدريب ضرورياً أيضاً للأفراد المسؤولين عن توزيع كلمات المرور فعلى هؤلاء الأفراد التأكد من تقديم المستفيد الذي يطلب كلمة مرور عند النسيان إثباتات كافية قبل إعادة تهيئة كلمة مرور جديدة. يوجد الكثير من الحوادث المنشورة تروي حصول أُناس على كلمات مرور جديدة بدون طلب الإثباتات اللازمة بسبب مجرد إظهار الغضب.

٢ ٦ ٦ التهديدات ومواطن الضعف في الشبكات

١. التهديدات والثغرات الأمنية (Security Threats and Vulnerabilities) [٦١]

يوجد ثلاثة مواطن ضعف أساسية تزيد من التهديدات الأمنية هي:

أ – نقاط ضعف تكنولوجية.

ب – نقاط ضعف الإعدادات كما في الجدول (٢/١).

ت – نقاط الضعف في سياسات الحماية كما في الجدول (٢/٢).

وتعد نقاط الضعف الثلاث مصدراً مهماً لأناس يبحثون عنها ويتلهفون للوصول إليها لاستغلالها بانتهاك خصوصية الشبكات والتلذذ بنشوة الانتصار باختراق الإجراءات الدفاعية لشبكات ضحاياهم.

---

[61] **See**: Cisco systems, inc: (Indiana, Cisco press, **Cisco networking academy program, first year companion guide** 2nd ed., 2001) P 15.

الجدول (٢/١)

نقاط ضعف الإعدادات

نقطة الضعف	كيفية استغلالها
حسابات المستخدمين غير المحمية	يمكن إرسال بيانات حساب المستخدم عبر الشبكة بشكل غير آمن، وبذلك يتم تعريض أسماء وكلمات مرور المستخدمين لأخطار التلصص.
حسابات النظام المزودة بكلمات مرور سهلة التخمين	عندما يستطيع المتلصصون تخمين كلمات المرور بسهولة ينجحون بدخول أنظمة المستخدمين الذين لديهم كلمات مرور سهلة.
الإعدادات غير الآمنة لمتصفحات الويب وخدمات الانترنت	المشكلة الشائعة لتشغيل "جافا" و"جافا سكربت" في متصفحات الويب أنها تسمح بوصول الاعتداءات من خلال "جافا أبليت".
إعدادات الحماية الافتراضية غير الآمنة	كثير من الأجهزة والبرمجيات مجهزة مسبقاً بإعدادات حماية افتراضية تنتج ثغرات أمنية عندما لا يتم تغييرها.
الإعدادات الضعيفة في أجهزة الشبكة	يمكن أن تؤدي الإعدادات الضعيفة في أجهزة الشبكات إلى مشكلات أمنية، فعلى سبيل المثال فقدان إعداد قوائم ضبط الوصول Access Control List أو كلمات مرور بروتوكول SNMP [٦٢] وبروتوكولات التوجيه يمكن أن تفتح ثغرات أمنية كبيرة.

[62] SNMP: simple network management protocol

جدول (٢/٢)

مواطن ضعف السياسات الأمنية

نقطة الضعف	كيفية استغلال الثغرات
النقص في توثيق سياسات الحماية	لا يمكن إلزام جميع المعنيين بسياسة ما إن لم تكن مكتوبة وموثقة ومعتمدة.
التنفيذ غير الكامل للسياسات الأمنية	الظروف الصعبة وبيئات العمل المليئة بالمشكلات تجعل من تنفيذ سياسات أمنية متماسكة أمراً صعباً.
كثرة تبديل الموظفين	يمكن أن يؤدي التبديل المستمر للموظفين إلى تعريض الشبكة لخطر الوصول غير المرخص من قبل الموظفين السابقين.
عدم تطبيق ضوابط الوصول المنطقية	يمكن أن يؤدي اختيار كلمات المرور الضعيفة أو سهلة الكسر أو الافتراضية للسماح بالوصول غير المرخص إلى الشبكة.
إهمال إدارة الحماية والمراقبة والمراجعة والتدقيق	عدم إنجاز التدقيق والمراجعة بالشكل المناسب يسمح بالوصول غير المرخص والهجمات التي تطال موارد الشبكة ضعيفة الحماية. وقد تؤدي هذه المشكلة إلى مشكلات قانونية مع الشركاء و العملاء وإدارة تقنية المعلومات.
تركيبات الأجهزة والبرامج والتعديلات غير المطابقة للسياسات المتبعة	أي تعديل غير مرخص في توصيلات الشبكة أو تركيب تطبيقات غير مرخصة ينشِئ ثغرات أمنية.
عدم وجود خطة طوارئ الكوارث	يسمح الافتقار إلى خطة الطوارئ لاستعادة النشاط عند الكوارث بحدوث الفوضى والخوف والتضارب عندما تُهاجم المنظمة.
الفشل في الالتزام في إرغام المعنيين بتنفيذ سياسة الحماية الأمنية	تكون السياسة الأمنية فعالة فقط إذا نُفّذت وتم الإعلام عنها بشكل واضح والإخفاق في توصيلها إلى المعنيين وتطبيقها يعرض المنظمة لزيادة في احتمالات حصول الهجمات على الشبكة.

٢. مواطن الضعف في حماية الشبكة (Network Security Weaknesses)

حتى يتم إكمال الاتصال من خلال الشبكة، يجب تمكين خدمات محددة وتشغيلها، وتتكون الشبكة النموذجية من بروتوكولات ونُظم تشغيل مكتبية وأجهزة شبكية تستخدم لتمرير البيانات

عبر الشبكة. وكل من مكونات الشبكة تحوي مواطن ضعيفة قابلة للاستغلال. ويمكن ذكر مواطن الضعف المشهورة التالية:

أ - نقاط ضعف بروتوكول (TCP/IP) وتشمل (HTTP) و (ICMP) و(SNMP) و (DoS).

ب -نقاط ضعف نظم التشغيل وتشمل (UNIX) و (MS-Windows) و (OS/2).

ت -نقاط ضعف عتاد الشبكة وتشمل حماية كلمات المرور وعدم وجود خصائص التحقق من الصحة وبروتوكولات التوجيه والإعداد السيئ لبروتوكولات التوجيه.

٣. التهديدات الرئيسة للشبكات (Primary Network Threats):

يمكن حصر تهديدات الشبكات في مجموعة من العناوين الكبيرة كالتالي:

أ - **تهديدات غير منظمة:** تتضمن بشكل رئيس أفراد غير متوقعين يستخدمون أدوات قرصنة سهلة تتوفر على شبكة الانترنت في مواقع كثيرة كأدوات كسر كلمات المرور (password crackers) والنصوص المغلفة (shell scripts) ، مع أن التهديدات غير المنظمة يمكن أن تحصل عند تشغيل أدوات القرصنة السهلة فإنها تظل مصدر خطر يمكن أن يؤذي الشبكة المعتدى عليها بأضرار خطيرة تزيد بازدياد مهارة هؤلاء الأفراد وقوة الأدوات المستخدمة. فعند اختراق موقع منظمة ما على الانترنت يكون ركن السلامة أحد أركان الحماية الأمنية غير محققاً، وحتى لو كان الموقع المخترق محمياً من الشبكات الخارجية بجدار حماية فعال فإن مصداقية المنظمة تنخفض لدى الأطراف الأخرى ويعدّون ذلك الموقع بيئة غير آمنة وبالتالي تتأثر أعمال المنظمة سلباً، ويكون الأثر أكثر سلبية إذا كان الموقع خاص بجهات وطنية دفاعية متصلة بقواعد بيانات عسكرية أو أمنية.

ب -**تهديدات منظمة:** تأتي من قراصنة مندفعين بشدة يحفزهم التنافس التقني، يعرفون ثغرات نظم التشغيل ويمكنهم فهم النصوص البرمجية والشفرات واستغلالها. يفهمون ويطورون ويستخدمون تقنيات القرصنة المعقدة في اختراق مواقع الشركات والمؤسسات غير المحمية عن جهل وقلة خبرة. هذه المجموعة من القراصنة غالباً ما تكون متورطة في معظم قضايا الاحتيال والسرقة التي يتم إخبار الجهات الأمنية عنها.

ت -**تهديدات خارجية:** هي تلك التهديدات التي يسببها أفراد أو منظمات يعملون من خارج المنظمة ولا يملكون حق الوصول إلى شبكة الحاسب العائدة لتلك المنظمة. تؤدي هذه المجموعة

من الأفراد أو المنظمات العمل عن طريق دخولها الشبكات بشكل رئيس من الإنترنت أو خطوط الهاتف من خلال خدمة الطلب الهاتفي (dialup).

ث -**تهديدات داخلية:** يمكن حصول هذا النوع من التهديدات عندما يكون لشخص ما حق الوصول لشبكة المنظمة سواء بحساب مسجل مسبقاً (اسم مستخدم وكلمة مرور) أو بالدخول الفيزيائي لأماكن وجود أجهزة ومعدات الشبكة. ووفقاً لوكالة (FBI) تشكل التهديدات نسبة من ٦٠ إلى ٨٠ بالمائة من التهديدات التي يتم الإخبار عنها.[٦٣]

٤. الهجمات الرئيسة:

بوجود العديد من نقاط الضعف تكون الشبكة معرضة للكثير من الهجمات ويتوفر ثلاثة أنواع رئيسة من الهجمات هي الاستطلاع والتنصت ورفض الخدمة.

أ. **الاستطلاع** (Reconnaissance):

يُقصد بالاستطلاع هنا جمع المعلومات بدون إذن أو تخويل، بقصد استكشاف شبكة منظمة ما ورسم مخططها ومعرفة الخدمات المستخدمة فيها واستنتاج نقاط ضعفها، وقد يرِد مصطلح الاستطلاع أحياناً باسم جمع المعلومات، وفي معظم الحالات تقود هذه العملية إلى تمكين الوصول غير المرخص ومن ثم تنفيذ هجمة رفض الخدمة. ويتم ذلك غالبا على مرحلتين بالشكل التالي:

المرحلة الأولى: يقوم القرصان الماكر بتنفيذ أوامر متعددة لكشف العناوين النشطة كالأمر (ping) بمسح جميع مكونات شبكة الضحية، ونتيجة هذه المرحلة تسجيل قائمة بالعناوين تدل كل منها على جهاز يقوم بخدمة أو مجموعة من الخدمات.

المرحلة الثانية: يستخدم القرصان أداة لمسح المنافذ ليستنتج المنافذ المفتوحة والخدمات العاملة في العناوين المستنتجة في المرحلة الأولى. ونتيجة هذه المرحلة تكون تحديد الخدمات والوظائف وبتوفيق العناوين والمنافذ يتوصل القرصان إلى معرفة التطبيقات المستخدمة وأنواعها وأسماء أنظمة التشغيل وإصداراتها التي تشغل حاسبات الشبكة الضحية. واعتماداً على هذه النتائج يقرر القرصان فيما إذا كانت نقاط الضعف قابلة للاستغلال أم لا. والاستطلاع يشبه تصرف السارق حينما يستكشف المبنى المراد سرقته فيدور حوله باحثاً عن نافذة مفتوحة أو نافذة سهلة الفتح أو باب مفتوح أو باب خلفي سهل الفتح أو نقطة ضعف في نظام الأقفال وغير ذلك.

---

[63] **See**: Cisco systems, inc: (Indiana, Cisco press, **Cisco networking academy program, first year companion guide** 2nd ed., 2001) P 20.

ويستخدِم القرصان على سبيل المثال أداة (NSLOOKUP) و أداة (WHOIS) لتحديد عناوين بروتوكولات الانترنت المسجلة للمنظمة الضحية. ثم يستخدم أداة (PING) ليقرر أية عناوين قيد التشغيل.

ب. **التنصت** (Eavesdropping): يُعرف التنصت بعبارات شائعة مثل استطلاع الشبكات واكتشاف الحُزم. يمكن أن يستخدم التنصت لاكتشاف الهجمات على الشبكات. ومن الأمثلة على البيانات القابلة للتأثر بالتنصت النسخة الأولى من بروتوكول (SNMP) الذي يرسل نص التعريف (Community string) بالنص الواضح غير المشفر، ويستطيع القرصان الماكر تشغيل أدوات تنصت على بروتوكول (SNMP) وجمع معلومات قيّمة عن معدات الشبكة وطرق إعداد كل منها. ومن البروتوكولات التي تقبل التصنت بروتوكول (TCP/IP) حيث يتم مراقبة الحُزم والتقاط كلمات المرور وأسماء المستخدمين عند مرورها بالشبكة وبيانات بطاقات الائتمان والبيانات الشخصية وكثير من البيانات المختلفة التي تقود لتسهيل الوصول إلى الشبكة الضحية ودخول أجهزة الخادم المتوفرة فيها.

والأدوات المستخدمة لتنفيذ التصنت تتضمن برامج تحليل الشبكات وبروتوكولاتها بالإضافة إلى أدوات التقاط الحُزم على شبكات الحاسب.

أما الطرق المستخدمة للحماية من هجمات التصنت فتتلخص بإصدار سياسة تقود إلى منع استخدام بروتوكولات قابلة للاختراق من قبل هجمات التنصت. واستخدام تشفير يتوافق مع متطلبات الحماية في المنظمة بحيث لا يُنقِص كفاءة موارد النظام أو رِضا المستفيدين.

ت. هجمة رفض الخدمة:

يتم في هذا النوع من الهجمات إرسال عدد كبير من الحزم من الشبكة الخارجية (عادة الانترنت) إلى الشبكة الداخلية [٦٤] (عادة خادم الويب) مما يؤدي إلى إيقاف خدمة الويب وبالتالي عدم استطاعة المستفيدين من تصفح موقع المنظمة المستهدفة. وغالباً ما يتم إرسال تلك الحزم من عدد كبير من الحاسبات من مواقع جغرافية مختلفة لتضييع مصدر الهجوم.

---

[64] **See**: Cisco systems, inc: (Indiana, Cisco press, **Cisco networking academy program, first year companion guide** 2nd ed., 2001) P 123.

٥. مواطن الضعف في طبقات نموذج طبقات الشبكة القياسي (OSI):

يتألف نظام طبقات الشبكة المفتوح (OSI) من سبعة طبقات لكل منها مجموعة من الوظائف ضرورية لانتقال البيانات من المصدر إلى الهدف عبر الشبكة. كل طبقة من هذه الطبقات تحوي مواطن ضعف تخصها وفيما يلي وصف مختصر لكل طبقة مع بيان موجز لأهم الهجمات الممكنة فيها:

أ - **الطبقة الفيزيائية** (Physical Layer): تتضمن وسائط التراسل الثنائي، والموصلات، والأجهزة وفيها يمكن التصنت على الكبلات،والوصول الكامل إلى الشبكة واستكشافها، بالإضافة إلى تأثر هذه الطبقة بالكوارث الطبيعية، وأعمال التخريب المادية، وانقطاعات الطاقة الكهربائية، وسرقة الأجهزة ووسائط التخزين وغيرها.

ب -**طبقة ربط البيانات** (Data Link Layer): وسائط الربط [٦٥] (LLC) وأيضاً (MAC) [٦٦] وفيهما يمكن التصنت والاستكشاف، بمعالجة أُطر البيانات، وكشف ضعف تأمين الشبكات الافتراضية (VLANs)، وكثرة إشارات الإعلان (Broadcast storms)،والتطفل وسوء إعداد بطاقات الشبكة (NICs)، والهجمات المؤتمتة (BOT)المستخدمة لذاكرة القراءة القابلة للبرمجة (EPROM) المثبتة على بطاقة الشبكة (NICs) .

ت -**طبقة الشبكة** (Network Layer) :وتتضمن بروتوكولات العناوين والمسار مثل: (ICMP) ,(IPX)[٦٧] , (IP) وفيها يمكن شن هجمات المسح بأداة (ping) واستكشاف الحُزم ، والاستكشاف يتم باستخدام (ARP)، (DDoS).

ث -**طبقة النقل** (Transport Layer) : تؤمن الاتصال من طرفية إلى أخرى وتستخدم بروتوكولات أهمها: (SPX),(UDP),(TCP) ويمكن استغلالها في مسح المنافذ، واستكشاف واختراق جلسات الاتصال، وبدء هجمات (DoS)،وفيض التزامن (SYN)، وقنابل (UDP)، والتجزئة (Fragmentation).

ج -**طبقة الجلسة** (Session Layer) : وتتشكل من الاتصالات الداخلية مثل (NFS), (SMB) , (Bind), (Xwindow), (RPC), (SQL) ويمكن استغلالها في مراقبة حركة البيانات ، ومشاركة مواطن الضعف والوصول إلى أصول المعلومات.

ح -**طبقة التمثيل** (Presentation Layer) وفيها يتم تمثيل البيانات مثل: (ASCII), (EBCDIC), (HTML), (Pict), (wav) ويمكن استغلال هذه الطبقة بسهولة

---

[65] MAC: Media Access Control

[66] LLC: Logical Link Control

[67] IPX: Internetwork Packet Exchange

لإظهار البيانات غير المشفرة، ويمكن للفيروسات والبرامج المضغوطة تجاوُز إجراءات الحماية، وتسهيل فك الشفرات للبيانات المشفرة تشفيراً ضعيفاً .

خ - **طبقة التطبيق** (Application Layer) : ويتم فيها معالجة التطبيقات الشبكية باستخدام بروتوكولات مختلفة مثل: (Mc OS), (Windows), (FTP), (Telnet), (Whois), (DNS), (SNMP), (HTTP), (UNIX) ويمكن استغلالها في إنشاء قنابل البريد الإلكتروني، وأحصنة طروادة، والفيروسات، والوصول غير المرخص إلى حاسبات ومعدات الشبكة، واستغلال الحاسبات المضيفة باستخدام ثغرات أنظمة التشغيل ومتصفحات الانترنت، والوصول إلى المعدات والسيطرة عليها، وإيقاف خدمة العناوين (DNS).

٢ ـ ٧ السياسات الأمنية والحماية (Security Framework and Policy)

كثيرا ما تحصل الحوادث الأمنية بسبب تقصير مسؤولي نظم التشغيل في الالتزام بتنفيذ سياسات الحماية حيث يتمكن القراصنة أو الموظفون ذوي الفضول من استغلال ذلك الإهمال. وعليه لا يكفي لتأمين الحماية معرفة نقاط الضعف وإغلاقها ولكن من الأهمية بمكان أيضاً لتوفير سياسات حماية مع الحرص على تطبيق هذه السياسات بشكل جدي وعلى كل المجال الذي تشمله ومنها:

أ - سياسة الاستخدام المقبول.

ب - سياسة أمن المعلومات (الحماية).

ت - سياسة النسخ الاحتياطي.

ث - سياسة التدريب في تخصصات تقنية المعلومات.

ج - سياسة الاسترجاع عند الكوارث.

ح - سياسية ضمان سلامة المعلومات.

٢ ـ ٨ عجلة الحماية الأمنية (The Security Wheel):

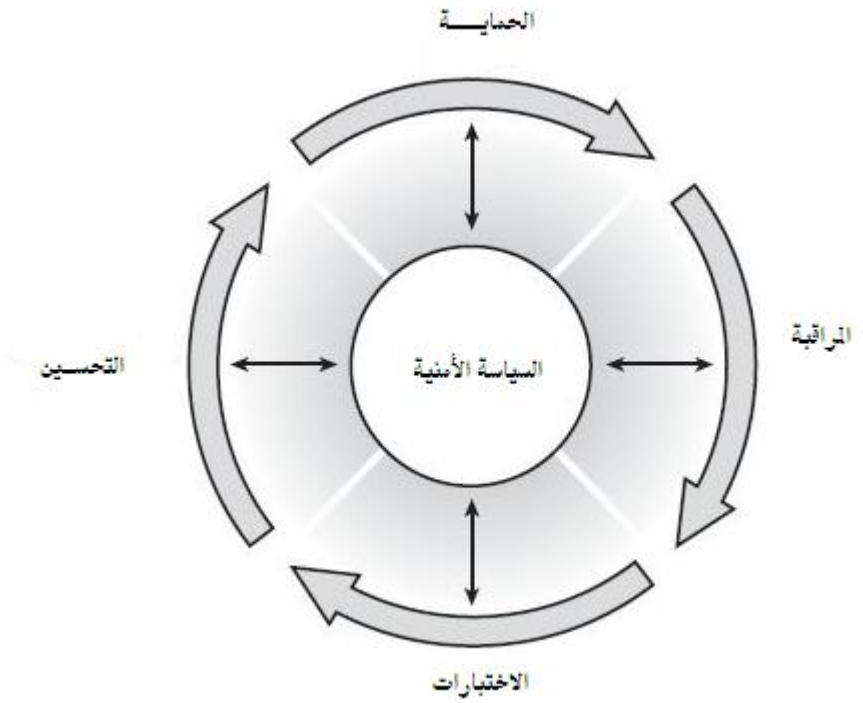
عجلة الحماية الأمنية عبارة عن عملية مستمرة تستخدم كطريقة فعالة للتأكد من وجود الإجراءات المناسبة للحماية من مواطن الضعف الأمنية والتأكد من عملها بشكل صحيح، وتلعب عجلة الحماية دورا مهما في تطبيق التشغيل التجريبي للتحديثات على بيئة التجربة ثم التشغيل النهائي على بيئة الإنتاج بحيث يتم ذلك باستمرار دون انقطاع. ويمكن من الشكل (٣) رؤية محور العجلة (السياسة الأمنية) والأقسام الأربعة على إطار العجلة وهي الحماية والمراقبة والاختبارات والتحسين، ولبدء دوران عجلة الحماية يتم أولا تطوير سياسة الحماية التي يجب أن تتناول على الأقل:

أ - تحديد أهداف الحماية في المؤسسة.

ب – تحديد وتوثيق الموارد المطلوب حمايتها.

ت – تحديد بنية الشبكة مع المخططات والمخازن.

ث – تحديد الموارد الحرجة التي تحتاج للحماية كموارد الأبحاث والموارد المالية والبشرية.



الشكل (٣) عجلة الحماية الأمنية

وبعد تطوير سياسة الحماية يتم جعلها محور لعجلة الحماية يدور حوله أربع تفريعات تتضمن الحماية والمراقبة والاختبارات التجريبية والتحسين. حيث تبدأ بالتخطيط للحماية الوقائية وتنفيذ تثبيت وإعداد تجهيزات الحماية ثم المراقبة ثم الاختبار التجريبي ثم التحسين ومن ثم يتم العودة إلى الحماية وهكذا دواليك.

١. **الحماية الوقائية:** لإيقاف الوصول والأنشطة غير المرخصة يتم حماية الشبكة بتفعيل سياسة الحماية وتطبيق حلول الحماية وأهم تلك الحلول:

أ – التحقق من الصحة (Authentication): إعطاء صلاحية الوصول للمصرح لهم فقط.

ب – جدران الحماية (Firewalls): تصفية حركة حُزم البيانات بالسماح بمرور الحُزم الواردة من المصادر المعروفة والموثوق بها ومنع الحُزم الواردة من جميع المصادر الأخرى وكذلك السماح بتشغيل الخدمات اللازمة لأعمال المؤسسة ومنع تشغيل الخدمات الأخرى.

ت -الشبكات الافتراضية (VPNs): تخفي المحتوى المنقول من البيانات بالتشفير بغرض عدم كشفها من قبل القراصنة والمنافسون والأعداء.

ث -سد الثغرات (Updates): تحديث أنظمة التشغيل لأجهزة الخادم والحاسبات المكتبية وأجهزة الشبكة كالموزعات والموجهات والنقاط اللاسلكية والبرمجيات لمنع استغلال مواطن الضعف الناتجة عن عدم التحديث.

٢. **المراقبة:** تتضمن المراقبة طرقاً يدوية وأخرى آلية لكشف انتهاكات الحماية الأمنية، ولابد من تركيب برمجيات تقوم بإظهار أداء أجهزة وبرامج الشبكة من حيث نسب استخدام موارد الجهاز كالمعالج والذاكرة ومساحة التخزين، وحالتها، بالإضافة لحركة البيانات في النقاط الشبكية الهامة، ومراقبة استخدام الانترنت وتسجيل المواقع غير المتوافقة مع سياسة الاستخدام، وإشعار القسم المختص عند وجود نقص بالموارد أو استخدام غير متوافق مع سياسة الاستخدام على سبيل المثال، وبما أن برامج المراقبة تحتاج إلى تراخيص محدودة العدد وتزداد تكلفتها بازدياد العدد المراقب ولا تستطيع بعض المؤسسات تطبيق المراقبة على جميع الأجهزة والبرمجيات بسبب التكلفة فلابد من أن تشمل المراقبة أجهزة وبرمجيات حسب الأهمية حيث تُعطى أجهزة الخادم الرئيسة مثل: (Active Directory), (DHCP), (DNS) أولوية عالية لتطبيق المراقبة عليها وكذلك تُعطى أولوية عالية لمراقبة قواعد البيانات والتطبيقات الهامة، بالإضافة لوجوب مراقب الموجهات وجدران الحماية وأجهزة الوسيط (Proxy).

وأما الإجراءات اليدوية فتقتضي تخصيص واحد أو أكثر من مسؤولي أمن الشبكات لمراجعة سجلات الأحداث يدويا مع تخصيص وقت كاف لفتح ومراجعة جميع أجهزة الخادم ومعدات الشبكة واقتراح ما يلزم لحل المشكلات وتحسين إجراءات حماية نظم التشغيل وتحليل تلك الملفات والخروج بنتائج تفيد في إصلاح الثغرات والتخطيط لحماية أفضل واقتراح ما يلزم لحل المشكلات.

والإجراءات الآلية (الفعالة) الأكثر استخداما تستخدم مراجعة وتدقيق ملفات عرض الأحداث (Logs) بشكل آلي، وكشف الانتهاكات يتم بشكل رئيس عن طريق مراجعة سجلات الأحداث واستخدام كاشف تجسس (IPS) [٦٨] حيث تتوفر أنظمة لكشف الانتهاكات في الزمن الحقيقي وقد تجد فيها خصائص لجمع الأحداث وتحليلها وإخراج نتائج على شكل تقارير جاهزة مسبقة الإعداد قابلة للتخصيص وتسَهّل على مسؤولي أمن الشبكات الوصول إلى الانتهاكات وإعداد التوصيات اللازمة لتحسين الحماية.

[68] IPS: Intrusion Protection System

٣. الاختبارات التجريبية:

في مرحلة الاختبار من عجلة الحماية يتم اختبار الحماية بشكل مستمر للتأكد من سلامة وظائف الحماية المنفذة في المرحلة الأولى (مرحلة الحماية الأمنية) والتأكد من سلامة نظام التدقيق والمراجعة ونظام كشف ومنع التجسس (IPS) المنفذة في المرحلة الثانية (المراقبة). ومن أدوات الاختبار المفيدة في قياس مواطن الضعف في هذه المرحلة أدوات المسح التالية: (SATAN) و (Nessus)و (Nmap) .

باجتماع نتائج تحليل المراجعة والتدقيق مع نتائج المسح لمواطن الضعف يمكن قياس فعالية إجراءات الحماية في المرحلتين السابقين (الحماية والمراقبة) والانتقال لمرحلة التحسين.

٤. **التحسين:** تتضمن مرحلة التحسين في عجلة الحماية تحليل البيانات المجمَّعة خلال مرحلتي المراقبة والاختبارات. يجب أن تستمر عجلة الحماية بالدوران بشكل دائم لأن الثغرات يمكن أن تتجدد بشكل يومي.

إن البيانات المجمّعة في الخطوات السابقة مع نتائج تحليلها وبيانات الثغرات المكتشفة يجب أن تؤدي إلى إنتاج توصيات وقرارات مناسبة لسد الثغرات المكتشفة وتفادي حصول مثلها مستقبلا ومن ثم تعديل أساليب الحماية تبعا لذلك.

٢ ـ ٩ سياسات الحماية الأمنية وإجراءات العمل:

إن سياسات الحماية ضرورية جداً لكي يتم تفصيل ثوب الحماية على حجمها حيث تنبثق سياسات الحماية أصلا من نشاطات المؤسسة أو المنظمة وتصمم بما يتناسب مع أهمية تلك النشاطات وصلاحيات الإطلاع والتعديل على بيانات تلك النشاطات وبما يتوافق مع أهداف تلك المنظمة ، وترافق السياسات إجراءات عمل تَحْكُم سير العمل من حيث التطبيق والتنفيذ وفقاً لمستويات سياسات الحماية المتمثلة بمستوى الاحتياجات ومستوى التنفيذ.

١. بناء وتطوير سياسات الحماية الأمنية:

لا بُد من تخصيص الوقت الكافي لبذل الجهود اللازمة لإعداد السياسات الأمنية التي تفيد في تقديم إجراء مراجعة وتدقيق الحماية الأمنية للشبكة، والإطار العام لتنفيذ حماية الشبكة، والسلوكيات المسموح بها وغير المسموح بها، وتبين البرامج التي تحتاجها المنشأة، وتساعد في ضبط الاتصالات فيما بين المدراء والمستفيدين وتحديد مسؤوليات كل منهم، وتحدد عملية معالجة الحوادث الأمنية، وتمكِّن من تنفيذ والدفع في تطبيق الحماية، وتنشئ أسس الأفعال المشروعة عند الضرورة. حيث أن حماية شبكات الحاسب غدت في أيامنا مشكلة عالمية.

ويمكن تعريف سياسة الحماية الأمنية بأنها "بيان رسمي للقواعد التي يجب أن يلتزم بها المستخدمون الذين لديهم صلاحيات الدخول إلى موارد الشبكة " [٦٩] ويمكن أن تكون سياسة الحماية الأمنية عبارة عن توضيحات موجزة عن الاستخدام المقبول لموارد الشبكة، ويمكن أن تكون عبارة عن مئات الصفحات تشرح بالتفصيل عن كل عنصر من عناصر شبكة الاتصال مرفقة بالسياسات ذات العلاقة. ومن المهم إدراك حقيقة أن الحماية الأمنية للشبكة لا يمكن أن تتحقق بمُنتج واحد، بل لا بُد من اتحاد مجموعة من الخدمات والمنتجات البرمجية والعتادية ترتبط بشكل وثيق مع سياسة الحماية.

وحتى تكون سياسة الحماية الأمنية فعالة تحتاج لقبول ودعم من وظائف مختلفة في المنظمة مثل:

أ – مسؤول إدارة أمن الموقع.

ب –الفريق الفني في تقنية المعلومات، كفريق الدعم الفني وفريق برمجة أنظمة المعلومات.

ت –مسؤولي إدارة المجموعات الكبيرة للمستخدمين في المنظمة كقسم الأعمال التجارية أو إدارة علوم الحاسب الآلي في جامعة.

ث –فريق التحقيق ومعالجة الحوادث الأمنية.

ج –مسؤولي مجموعات المستخدِمين المتأثرون بسياسة الحماية.

ح –الإدارة المسؤولة.

خ –مستشار قانوني عند الحاجة.

ولا بُد من توفر الدعم الكامل من إدارة المنظمة لسياسة الحماية الأمنية وبدونه فإن فرص الوصول إلى النتيجة المطلوبة ستكون قليلة.

ولا بُدّ من توفّر سياسة أمنية للتأكد من أن أصول الشبكة محمية من التخريب والوصول غير المرغوب. ويجب أن تكون جميع مواصفات حماية الشبكة معدّة بشكل يتوافق مع سياسة حماية المنظمة. وإذا لم تكن سياسة الحماية متوفرة أو كانت منتهية الصلاحية فلا بُد من إنشائها أو تحديثها قبل اتخاذ أي قرار حول إعدادات الحماية في أي عنصر من عناصر الشبكة.

ولا بد لكل سياسة حماية أن تتضمن:

أ –بيان الصلاحيات والمجال: ويحدد راعي سياسة الحماية والمناطق التي تغطيها.

ب –سياسة الاستخدام المقبول: وتحدد ما تسمح به المنظمة وما لا تسمح به تبعاً لطبيعة المعلومات فيها.

---

[69] **See**: Cisco systems, inc: (Indiana, Cisco press, **Cisco networking academy program, first year companion guide** 2nd ed., 2001) P 47.

ت -سياسة التعريف والتحقق من الصحة: تحدد هذه السياسة التقنيات والتجهيزات أو مزيج منهما حتى تستخدمهما المنظمة للتأكد من صحة هوية طالب الدخول والسماح فقط للمسموح لهم بدخول موارد الشبكة.

ث -سياسة الوصول للإنترنت: تحدد هذه السياسة الاستخدام المناسب والمقبول في المنشأة للإنترنت والاستخدام غير المناسب وغير المقبول.

ج -سياسة الوصول في حرم المنظمة: تحدد هذه السياسة طريقة دخول المستخدمين إلى موارد شبكة المعلومات في حرم المنظمة.

ح -سياسة الوصول عن بُعد: تحدد هذه السياسة طريقة وصول المستخدمين من خارج حرم المنشأة إلى موارد شبكة المعلومات بالمنشأة.

خ -إجراء معالجة حادث: تحدد هذه السياسة طريقة إنشاء فريق التحقيق في الحوادث الأمنية والإجراءات التي سيستخدمها خلال وبعد حصول أي حادث.

٢. بناء وتطوير إجراءات الحماية:

تنفِّذ إجراءات الحماية السياسات الخاصة بالحماية، وتبين الإعدادات وتسجيل الدخول والمراجعات وعمليات الصيانة، ويجب أن تكون إجراءات الحماية التي تخص المستفيدين ومسؤولي الشبكات ومسؤولي الحماية مكتوبة وموثقة، ويجب أن تحدد إجراءات الحماية كيفية معالجة الحوادث الأمنية، وتبين الإجراءات ما يجب عمله ومن يجب الاتصال بهم عند اكتشاف حالة تلصص أو اختراق. يمكن إيصال إجراءات الحماية للمستفيدين عن طريق الدورات التدريبية أو التعليم.

ولا بد من مراعاة التوازن بين مرونة الوصول وتحقيق الحد الأعلى من الحماية حيث ينبغي مراعاة التوازن بين الإنتاجية وقياسات الحماية وذلك في جميع سياسات الحماية حيث أن الهدف من أي تصميم حماية هو الحصول على الحد الأقصى من الحماية بأقل تأخير على زمن وصول المستفيد والإنتاجية.

إن بعضا من قياسات الحماية مثل تشفير بيانات الشبكة لا تقيِّد الوصول والإنتاجية. من جهة أخرى فإن أنظمة التحقق من الصحة الاحتياطية وغير الضرورية يمكن أن تحبط المستفيد وتحول دون وصوله إلى موارد الشبكة الهامة.

تحدد احتياجات العمل سياسة الحماية المستخدمة في المنظمة ويجب أن تقرر سياسة الحماية كيفية سير العمل في المنظمة. وبما أن المنظمات تتغير فإن سياسة الحماية لا بد أن تتحدث دوريا بما يتلاءم مع التغيرات الفنية في المنظمة والتغيرات في مواضع الموارد، وكذلك التغير في مسؤوليات الموظفين.

٣. مستويات سياسات الحماية: يمكن تحديد مستويات الحماية إلى مستويين اثنين هما:

أ – مستوى الاحتياجات: في هذا المستوى تحدد السياسة درجة الحماية المناسبة من الاختراق أو التخريب، وتقدِّر أيضاً التكلفة والعواقب والثغرات ومثال ذلك تحدد السياسة الأفراد الذين يحق لهم الوصول إلى سجلات شؤون الموظفين بمنسوبي إدارة شؤون الموظفين وتحدد الأفراد الذين يحق لهم إعداد وإدارة الموجه (Router) الرئيس بالمسؤول عن إدارة الموجهات وتحدد الأفراد الذين يحق لهم إعداد جدار الحماية بالمسؤول عن إدارة جدران الحماية وعتاد أمن الشبكة.[٧٠]

ب –مستوى التنفيذ: في هذا المستوى تبين السياسة الإرشادات اللازمة لتنفيذ مستوى الاحتياج، استخدام تقنية محددة بطريقة معرفة مسبقاً. ومثال ذلك قد يحتاج مستوى تنفيذ السياسية إلى إنشاء قائمة ضبط الوصول (Access Control List) وظيفتها السماح للحُزم القادمة من إدارة شؤون الموظفين بالوصول إلى الخادم الذي يحتضن سجلات الموظفين ومنع جميع الحُزم الأخرى. وعند إنشاء سياسة ما يجب تحديد احتياجات الحماية قبل تحديد التنفيذ.[٧١]

٤. **مكونات الشبكة:** تتكون الشبكة من معدات وأجهزة من جهة وبرمجيات تقوم ببث الحياة والحركة في تلك المعدات والأجهزة لتستطيع القيام بوظائفها الشبكية وتقسم إلى ساكنة ونشطة:

أ. **المكونات الساكنة** (Passive components): وتشمل الكابلات وموصلاتها سواء كانت ألياف ضوئية (Fiber Optec) أو كابلات نحاسية مجدولة (UTP) وتشمل لوحات ربط الكابلات(Patch Panels) وكبائن احتضان علب الربط وغرف التفتيش (Manholes) وجميع هذه المكونات يجب أن تكون في أمكنة آمنة محروسة ومراقبة بكاميرات ودوريات راجلة وجميع الغرف والكبائن يجب أن تكون مزودة بأقفال تُعطى مفاتيحها لمن يُصرح لهم فقط.

ب. **المكونات الفاعلة** (Active components): وتشمل الموزعات (Switches) والموجهات (Routers) وجدران الحماية (Firewalls) ونقاط الوصول اللاسلكية (Access Points) وأجهزة الخادم (Servers) التي تشمل خادمات قواعد البيانات (Data Base) وخادمات ترجمة العناوين (DNS) وخادمات توزيع العناوين (DHCP) وخادمات الويب وخادمات الحماية بأنواعها المختلفة كأجهزة

[70] **See**: Cisco systems, inc: (Indiana, Cisco press, **Cisco networking academy program, first year companion guide** 2nd ed., 2001) P ٤٩.

[71] **See**: Cisco systems, inc: (Indiana, Cisco press, **Cisco networking academy program, first year companion guide** 2nd ed., 2001) P ٥٠.

الخادم التي تستخدم برمجيات لتعمل بوظيفة جدار حماية أو مضاد للفيروسات أو حارس بوابة البريد الالكتروني أو خادم كشف الثغرات وتثبيت التحديثات وغيرها. وعلى مسؤول أمن الشبكة أن لا ينسى ضرورة تنفيذ إجراءات الحماية على البرمجيات والتطبيقات إضافة إلى نظم التشغيل.

٥. **أنماط سياسات الحماية للمكونات النشطة:**

يمكن تصنيف سياسات الحماية في المكونات النشطة إلى ثلاثة أنماط كنقطة بداية في تصميم الحماية وهي سياسة الحماية المفتوحة وسياسة الحماية المقيدة وسياسة الحماية المغلقة. وفي الواقع العملي تتدرج إعدادات المعدات النشطة بين المغلق والمفتوح حسب سياسة الحماية المعتمدة والتي تكون نتيجة لسياسة المنظمة.

تكون سياسة الحماية المفتوحة سهلة الإعداد والإدارة وكذلك سهلة الاستخدام من قبل المستفيدين وقليلة التكلفة. حيث يتم إعداد الأجهزة والبرمجيات بالشكل الافتراضي (إعدادات المصنع) مع قليل من التعديلات. وتناسب هذه السياسة المنظمات الخيرية، ومسؤولي أمن الشبكات قليلي الخبرة.

وتكون سياسة الحماية المقيَّدة بالمقارنة مع سياسة الحماية المفتوحة أكثر صعوبة من حيث الإعداد والإدارة من جانب مسؤولي أمن الشبكات وأكثر صعوبة من حيث الاستخدام من جانب المستفيد، وأكثر تكلفة ، وتناسب هذه السياسة الشبكات المحلية التي تحوي أصول معلوماتية ذات خصوصية، وتتصل بالإنترنت وتتنوع صلاحيات وصول المستفيدين فيها من الاطلاع إلى التعديل والإضافة والحذف. تؤمن هذه السياسة سهولة في الاستخدام من قبل المستفيدين.

وأما سياسة الحماية المغلقة فهي الأكثر صعوبة من حيث التنفيذ حيث يتم تفعيل جميع معايير الحماية الممكنة ، فيقوم مسؤولو أمن الشبكة بإعداد الأجهزة والبرمجيات بما يتوافق مع الحد الأقصى للحماية، ناهيك عن تثبيت أجهزة وبرمجيات ذات أداء عالٍ بتكلفة أكبر مثل جدران لحماية (Firewalls)، وكاشفات ومانعات التجسس (IPS)، وأجهزة الخادم المتخصصة. وبالمقارنة مع السياستين المفتوحة والمقيدة فإن سياسة الحماية المغلقة هي الأكثر صعوبة من جانب مسؤولي أمن الشبكات من حيث الإعداد والتنفيذ، وأكثر صعوبة من جانب المستفيدين من حيث الاستخدام، وأكثر تكلفة من كليهما. وتناسب هذه السياسة وجود أصول معلوماتية عالية القيمة في موارد الشبكة بافتراض أن جميع المستفيدين (المستخدمون) غير موثوق بهم وأن التهديد متكرر وأن الاستخدام صعب جداً من جانب المستفيدين.

ويحتاج المسؤولون عن أمن الشبكة إلى مهارات عالية ووقت أطول وبالتالي تحتاج المنظمات التي تطبق هذه السياسة إلى عدد أكبر من مسؤولي أمن الشبكات للمحافظة على حماية مُحكَمة متينة خالية من الثغرات. وتميل كثير من المؤسسات والمنظمات إلى اختيار مسؤولي أمن غير مشهورين وغير معروفين عند تنفيذ الحماية، وتقوم إدارة أمن الشبكة بتوضيح أنها تقوم بتنفيذ سياسة الحماية فقط ، وأن تلك السياسة موثقة كتابيا ومصادق عليها من قبل المنظمة.

٢ ـ ٢ـ١ وظائف الموارد البشرية العاملة في حماية شبكات الحاسب الآلي:

ظهرت وظائف لم تكن موجودة قبل دخول أنظمة المعلومات في شرايين مؤسسات وشركات الأعمال لتلبية احتياجات أداء مهام تشغيل وإدارة أنظمة الشبكات والمحافظة على سلامة البيانات وأهم هذه الوظائف:

١. مسؤول نظم تشغيل الشبكة (Network Operating Systems Administrator): يقوم مسؤول نظم تشغيل الشبكة بتشغيل أجهزة الخادم وصيانتها وإعداد الصلاحيات اللازمة لوصول المستخدمين بناء على السياسات المعطاة له من قبل مسؤول الأمان.

٢. مسؤول النسخ الاحتياطي والاسترجاع (Backup and Disaster Recovery Administrator): يقوم بتنفيذ سياسات النسخ الاحتياطي واسترجاع البيانات بتشغيل أجهزة النسخ الاحتياطي وتخزين الأشرطة بطريقة مؤرشفة يسهل الرجوع إليها بوقت قصير جداً ويسهل استرجاع البيانات منها باستخدام برمجيات وأجهزة النسخ الاحتياطي والاسترجاع.

٣. مسؤول أمن المعلومات (Information Security Officer): يشرف على جميع العاملين في مجال أمن المعلومات من السياسات إلى المراقبة وحتى التوصيات ومتابعة تشغيل منتجات الحماية.

٤. مسؤول أمن نظم التشغيل (Security Operator): يقوم بتنفيذ السياسات الأمنية المتعلقة بتحديث نظم التشغيل وتطبيق سياسات كلمات المرور ومراجعة سجلات الأحداث وتزويد مسؤول أمن المعلومات بتقارير دورية وإبلاغه فوراً عند وجود أحداث حرجة وخصوصاً في أجهزة الخادم.

٥. أخصائي أمن معلومات (Security supervisor): يقوم بإنشاء سياسات الحماية لجميع أجهزة الخادم وقواعد البيانات والحاسبات المكتبية وسياسات الاستخدام المقبول

لأصول تقنية المعلومات وسياسات استخدام الانترنت وسياسات توريد واستلام وتسليم وإتلاف أصول المعلومات وما شابه ذلك. ويعتمدها من صاحب القرار بالمنظمة وفق التسلسل الإداري المتبع فيها.

٦. مُراجِع سياسات الحماية (Security Policy Editor): يقوم بمراجعة وتدقيق تنفيذ السياسات الأمنية لجميع السياسات المعتمدة ويرفع تقرير النتائج إلى مسؤول أمن المعلومات. ويمكن أن يتعدد المراجعون حسب التخصص كأن يكون مراجع متخصص بحماية قواعد البيانات وآخر متخصص بحماية مواقع الويب.

٧. مسؤول إدارة نظم التشغيل (system admin): يقوم بإدارة أجهزة الخادم من حيث نظام التشغيل كتركيب النظام وإضافة وإزالة مكوناته البرمجية وإعداده بما يتناسب مع بيئة العمل وإدارة المستخدمين كإضافة وتعديل حسابات المستخدمين وإضافة وتعديل الصلاحيات على دخول أوعية المعلومات أو تنفيذ السياسة الأمنية فيما يتعلق بنظم التشغيل.

٨. مسؤول إدارة الشبكة (Network admin) : يقوم بإدارة عتاد الشبكة النشط (Active Components) كالموزعات (switches) بإعدادها بما يتوافق مع بيئة العمل وتعطيل الخدمات غير المستخدمة وإتاحة الخدمات الضرورية لحركة البيانات كإنشاء الشبكات المحلية الافتراضية (VLANs) وتقسيم الشبكة إلى أقسام افتراضية تصلح لتطبيق سياسة الحماية.

٩. مسؤول مساندة فنية (Technical support): يقوم بأعمال الصيانة والإصلاح اللازمة بعد حصول حادث أمني كحوادث الإصابة بفيروس أو برنامج خبيث أو حوادث الاختراق. وبالمؤسسات الصغيرة يمكن أن يُكلف بأعمال توصيل الكابلات وحمايتها بأغطية مناسبة وفق المعايير الموضوعة.

١٠. ضابط أمن معلومات (security officer): يقوم بالتنسيق بين إدارات تقنيات المعلومات والإدارات الأُخرى والمستخدمين في كل ما يتعلق بأمن المعلومات.

١١. مدير قاعدة البيانات (DBA): يقوم بإدارة قاعدة البيانات من حيث إنشاء المستخدمين وإعطائهم الصلاحيات المناسبة والإشراف على إعداد وتنفيذ عمليات النسخ الاحتياطي والاسترجاع لقواعد البيانات وينبغي أن يكون ملماً بنظام حماية قواعد البيانات المرفق معها بحيث يقوم بتنفيذ السياسة الأمنية الموضوعة لحماية قواعد البيانات.

١٢. مدير النظام : لكل نظام من الأنظمة الآلية ينبغي أن يعين مدير لهذا النظام كنظام شؤون الموظفين أو نظام القبول والتسجيل حيث يكون لكل واحد مدير يشرف على صيانته وتشغيله وتنفيذ إجراءات حمايته وجميع ما يلزم لاستمرار تشغيله على مدار الساعة.[٧٢]

١٣. مبرمج: يقوم المبرمج بتحويل خوارزميات البرنامج الواردة إليه من محلل النظم إلى (أكواد) وأسطر برمجية على شكل نصوص مكتوبة بإحدى لغات البرمجة ولا بد من تثقيف المبرمج بأساسيات أمن المعلومات لكي يقوم بإعداد البرنامج بشكل يتفادى الثغرات الممكنة والتي يفترض أن يعرفها أولا بأول.

١٤. مسؤول موقع (Web Master): يقوم مسؤول الموقع بالإشراف على كافة العمليات التصميمية والتعديلات التي تُجرى على الموقع ولا بد أن يكون ملماً بأساسيات حماية المواقع ومطلعاً بشكل مستمر على آخر الثغرات المكتشفة وسبل سدها. ويكون قادراً على التنسيق والتعاون مع مسؤولي حماية الشبكة ومدخلي البيانات في الموقع بحيث لا يتم إدخال معلومات تسمح باستخدامها لتنفيذ هجمات على الموقع.

٢ ـ ١٠ مكونات شبكة الحاسب الآلي:

في أواخر الثمانينيات من هذا القرن وبداية التسعينيات كثرت شبكات اتصال الكمبيوتر وتعدد مصنعوا الشبكات وتعددت الأجهزة والبرمجيات المكونة للشبكات بتعدد المصنعين واختلفت باختلافهم، وكنتيجة لذلك الاختلاف أضحت بعض الشبكات غير قادرة على التوافق مع بعضها الآخر وبالتالي لم تستطع تحقيق الاتصال فيما بينها، ولحل مشكلة عدم التوافق هذه ولتسهيل صناعة معايير واحدة للشبكات من قبل مصنعين مختلفين قامت منظمة المعايير الدولية (ISO) [٧٣] بإنشاء نموذج الطبقات السبعة لأية شبكة حاسب آلي وأصدرته كمرجع لجميع مصنِّعي عتاد وبرمجيات الشبكات عام ١٩٨٤. [٧٤] حيث تتضمن الطبقة الأولى (الطبقة الفيزيائية) مواصفات صناعة وسائط النقل مثل الكابلات النحاسية والألياف الضوئية ووسائط النقل اللاسلكية، وتتضمن الطبقة الثانية (طبقة ربط البيانات) مواصفات بطاقات الشبكة وبروتوكولات ربط البيانات ومواصفات الموزعات (switches). وتتضمن الطبقة الثالثة (طبقة الشبكة) بروتوكولات التوجيه ومواصفات الموجهات (Routers) وتتضمن الطبقة الرابعة (طبقة النقل) بروتوكولات النقل والخامسة (طبقة

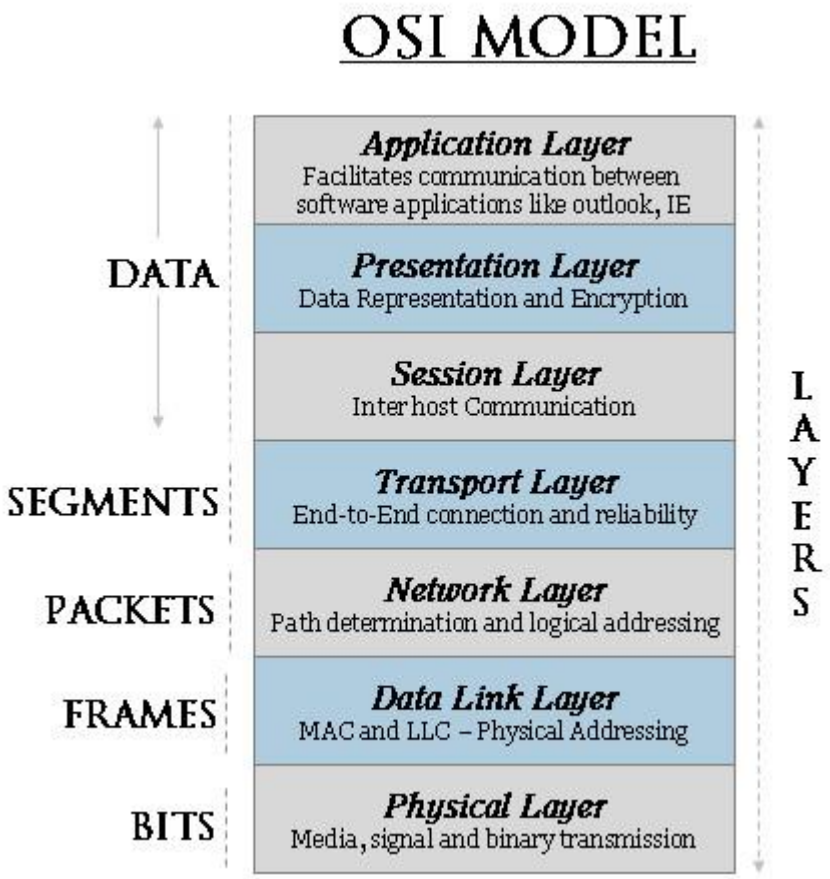
[٧٢] حسن طاهر داود ٢٠٠٠ مرجع سابق ص٢٨٥

[73] ISO: International Organization for Standardization

[74] Cisco System, Inc. Cisco Networking Academy Program: First – Year Companion Guide , Cico Press, Indianapolice, USA, 2001, Page 45.

الجلسة) تتناول جلسات الاتصال والسادسة (طبقة التمثيل) تختص بتمثيل البيانات والسابعة (طبقة التطبيقات) بالتطبيقات مثل البريد الإلكتروني ومحررات النصوص .

وسميت الوحدات على مستوى الطبقة الأولى بالبتات (Bits) والوحدات على مستوى الطبقة الثانية بالإطارات (Frames) . وسميت الوحدات على مستوى الطبقة الثالثة بالحزم (Packets) والرابعة المقطع (Segment) وسميت الوحدات على مستوى الطبقة الخامسة مع السادسة والسابعة بالمعطيات (Data). والشكل(٤) يبين نموذج (OSI) .



الشكل (٤) نموذج (OSI)

ويمكن التمييز بين ثلاث مجموعات رئيسة لمكونات شبكة الحاسب الآلي هي: مجموعة كابلات الربط ووسائط النقل التي تؤمن العمود الفقري للشبكة مع تفريعاته وأجهزة التوزيع مثل الموزعات (Switches) والتي تشمل المكونات الساكنة (Passive Components) والمكونات النشطة (Active Components) ، ومجموعة أجهزة الخادم (Servers) التي تؤمن برامج

تشغيل الشبكة وتمكّن من التشارك فيما بين موارد الشبكة، ومجموعة النهايات الطرفية التي يتم فيها إدخال البيانات وإخراج النتائج.

١. **العمود الفقري للشبكة (Backbone)**[٧٥] هو جزء من شبكة الحاسب يصل مختلف أجزاء الشبكة، قوامه وسائط نقل قد تكون كابلات ضوئية أو نحاسية عالية السرعة توصل ببطاقات الشبكة عالية السرعة العائدة لأجهزة الخادم. ولا يتم عادة توصيل محطات العمل إلى العمود الفقري بشكل مباشر وإنما عن طريق الموزعات (Switches)، ويكون طول العمود الفقري محدوداً وذلك في حالة ربط أجهزة الخادم مع بعضها في المكان الواحد وذلك لتسهيل السيطرة والإدارة. ويمكن استخدام كابلات طويلة في حالة الشبكة التي تربط أكثر من مبنى، وبالتالي يمكن القول بأن العمود الفقري للشبكة ما هو إلا كابل لتوصيل اثنين أو أكثر من خوادم الشبكات مع بعضها البعض وتجميع أجهزة الخادم في مكان واحد. ويمكن أن يقوم العمود الفقري بتقسيم الشبكة الكبيرة إلى شبكات صغيرة وذلك لتسهيل الإدارة وتحقيق أعلى معدل لانتقال البيانات. وعادة ما يُطلق اسم مركز البيانات (Data center) على المكان الذي يحوي أجهزة الخادم التي تحتضن قواعد البيانات (Data Base)، بالإضافة لأجهزة الخادم التي تشغل خدمات الشبكة مثل (DNS)، (Active Directory).

٢. **أجهزة التوزيع الشبكية**: وهي الأجهزة التي تقوم بتوزيع حزم البيانات وتربط بين الحاسبات بمختلف أنواعها عن طريق الكابلات، وتصنف إلى ثلاثة أصناف رئيسة هي الموزعات المكتبية وموزعات التفريع والموزعات المركزية. وجهاز التوزيع ما هو إلا جسر (Bridge) متعدد المنافذ، والجسر هو جهاز يستخدم لوصل شبكتين محليتين بحيث يسمح للمحطات الموجودة في كلا الشبكتين بالوصول إلى الموارد الموجودة بالشبكة الأخرى، ويمكن استخدام الجسور لزيادة طول أو عدد العقد الممكنة على الشبكة. وبوضع عدة جسور في جهاز واحد نحصل على الموزع (switch) الذي يعد نموذجاً محدثاً عن الجسر (Bridge).

أ - **الموزعات المكتبية**(Desktop switches): وتسمى أحياناً (Access Switches) وتعمل في مستوى طبقة ربط البيانات (Data Link Layer) في نموذج (OSI) [٧٦]. وتربط الحاسبات المكتبية والمحمولة والطابعات الشبكية وغيرها مما

---

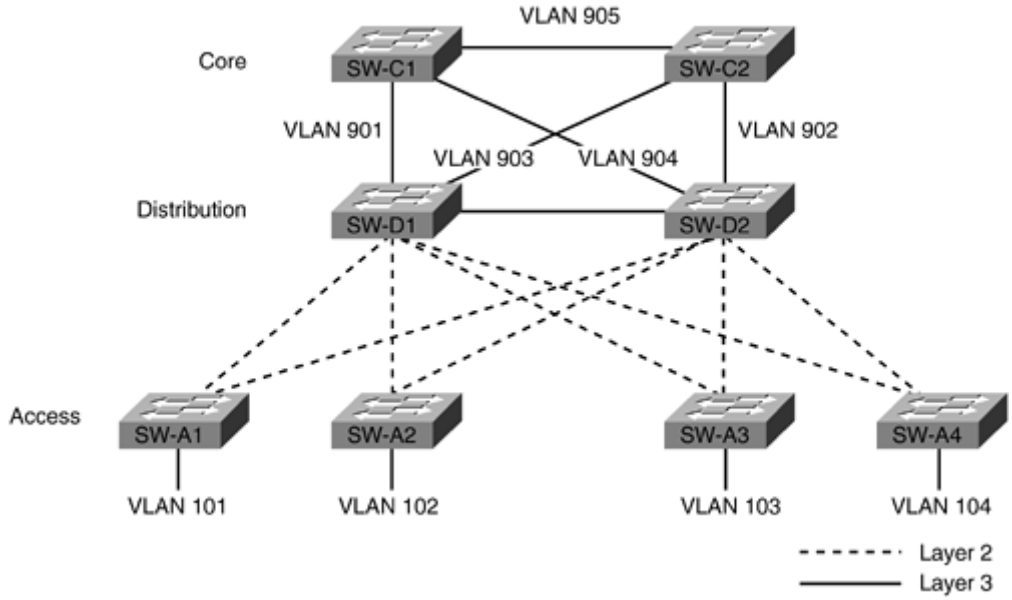
[٧٥] العمود_الفقري_للشبكة/http://ar.wikipedia.org/wiki موقع الموسوعة الحرة ويكيبيديا

[٧٦] **انظر:** جايمس سيميك ،**أساسيات شبكات الاتصال** ترجمة: مركز التعريب والترجمة (بيروت: الدار العربية للعلوم ١٩٩٩) ص٣٨٧

يُدعى بالنهايات الطرفية من جهة وبين الموزع المركزي من جهة أخرى. والشكل (٥) يوضح مكان الموزعات المكتبية في الشبكات الكبيرة.

ب -**الموزعات المركزية** (Core switches) : تكون منافذها عالية السرعة وغالباً ما تكون متعددة الجيجا بت بالثانية ويوصى باستخدامها في الشبكات المتوسطة والكبيرة حيث تتميز بوجود مزايا التوجيه (الطبقة ٣) إضافة لوظيفة التوزيع الأساسية (الطبقة٢) وتربط بين الموزعات الفرعية وأجهزة الخادم ويُنصح بتوفير موزع احتياطي لكل موزع مركزي بحيث يعملان معاً ويستلم أحدهما العمل إذا توقف الآخر لأي سبب كان. والشكل (٥) يوضح مكان الموزعات المركزية في الشبكات الكبيرة.

ت -الموزعات الفرعية (Distribution Switches): هي موزعات تعمل في الطبقة الثالثة والثانية وتربط بين الموزعات المركزية والموزعات المكتبية كما في الشكل (٥) ويُنصح باستخدامها في الشبكات الكبيرة.



الشكل (٥)

التصميم المفترض للموزعات في الشبكات الكبيرة

٣. **أجهزة الخادم** (Servers): هي أجهزة حاسب آلي تتميز بأن مكوناتها عالية الأداء بمواصفات خاصة من سرعة المعالج وسعة الذاكرة وتعدد الأقراص الصلبة لتوفير احتياطي في مساحة التخزين، الهدف منها تشغيل البرمجيات الخاصة بأجهزة الخادم والتي تسمى نظم تشغيل الخادم كعائلة نظام تشغيل الشبكات ويندوز (NT) الذي تطور إلى

(Windows2008) ونظام تشغيل الشبكات (يونكس) ونظام تشغيل الشبكات (لينوكس) ونظام تشغيل (Sun salaries)، وهذه النظم تستطيع تشغيل بروتوكولات الشبكة حسب الطلب كخدمة أسماء النطاق (DNS) وبروتوكول توزيع عناوين أعضاء الشبكة ديناميكيا (DHCP) وغيرهما. حيث يجب أن تعمل الخدمات الشبكية باستمرار ودون انقطاع لذلك هي تحتاج إلى أجهزة قادرة على التشغيل باعتمادية عالية.

إن كل هذه النظم تحتاج ما يضمن استمرارية وجودها وما يضمن خصوصية بياناتها وسرية معلوماتها. إن ذلك كله يحتاج نظم حماية أمنية لجميع المستويات السابقة فتكون نظم الحماية الأمنية وفق مستويات متدرجة حيث تبدأ بالحماية الفيزيائية (المادية) ثم حماية نظم الحاسبات المكتبية ثم حماية نظم تشغيل أجهزة الخادم وقواعد البيانات بحيث يتم حماية الشبكة المحلية، وكذلك حماية البيانات المخزونة، وحماية البيانات المنقولة ناهيك عن حماية البيانات أثناء المعالجة.

٢ ـ ٤ ـ ١ الحماية الأمنية في مكونات شبكة الحاسب الآلي:

١. الحماية الأمنية في أنظمة التشغيل:

تتلخص الحماية في أنظمة التشغيل كعائلة وندوز (NT) و وندوز (إكس بي) و وندوز (فيستا) ووندوز٧ و(لينوكس) و(يونكس) بالمحافظة على تحديث الترقيات الصادرة عن الشركة الصانعة أو المواقع الراعية للنظام المفتوح إذا كان من المصادر المفتوحة. والمحافظة على تنزيل التحديثات وتثبيتها باستمرار. بالإضافة لتركيب برامج الحماية من الفيروسات المحدثة أولاً بأول، وكذلك الحرص على تثبيت جدران الحماية البرمجية المناسبة، بالإضافة لتطبيق سياسات الحماية المتعلقة بكلمات المرور القوية وتنزيل البرمجيات المرخصة فقط، مع التأكيد على تعديل كلمات المرور الافتراضية التي قد تكون مسبقة الإعداد أينما وُجِدت.

٢. الحماية الأمنية في أجهزة التوزيع (Switches):

يقوم الموزع بوظيفة نقل إطارات البيانات اعتماداً على العنوان الفيزيائي المصنف بالطبقة الثانية، وفي الحقيقة أصبحت شركات صناعة الموزعات تنتج عائلات من الموزعات تعمل في الطبقة الثالثة إضافة إلى وظائفها في الطبقة الثانية، وغالباً ما توضع هذه الأخيرة في مركز الشبكة حيث تسعى لربط جميع المبدلات بنقطة مركزية تؤمن التوجيه اللازم للشبكات الافتراضية (VLANs) بالعمل بوظيفتين معاً هما التوزيع (طبقة ٢) والتوجيه (طبقة ٣) مما يقلل التكلفة ويُنقص الحجم ويخفض من الطاقة المستخدمة ولكن بالوقت نفسه يرفع من أخطار التوقف فتعطل جهاز واحد يوقف الوظيفتين معاً.

وتتلخص الحماية في أجهزة التوزيع سواء كانت أجهزة توزيع مصنفة في الطبقة الثانية (Layer2) من نموذج الطبقات السبع (OSI) أو كانت مصنفة في الطبقة الثالثة (Layer3) بالمحافظة على تحديث الترقيات الصادرة عن الشركة الصانعة لأنظمة تشغيلها، والمحافظة على تنزيل التحديثات وتثبيتها باستمرار. وإعداد هذه الموزعات إعداداً يتوافق مع سياسة الحماية المتبعة في المنظمة والتأكيد على تعديل كلمات المرور الافتراضية مسبقة الإعداد من المصنع. بالإضافة لتأمين الحماية الفيزيائية بتركيبها في غرف مزودة بأقفال ذات مفاتيح تعطى للعاملين المعنيين فقط بالإضافة لتأمين الظروف المحيطة المناسبة من حرارة ورطوبة حسب الشروط الفنية للتشغيل التي يُشار إليها في كُتيِّب التشغيل الذي يرفق مع كل جهاز عند التوريد بالشكل الورقي أو الإلكتروني أو كلاهما معاً وغالباً يتوفر في موقع الشركة الصانعة على الإنترنت.

٣. الحماية الأمنية في أجهزة التوجيه:

يتم استخدام الموجه للربط بين شبكتين أو أكثر كوظيفة شبكية ويمكن تزويد الموجه بوظائف أمنية بغرض الحماية وذلك بتصفية الحزم بإعداد قوائم التحكم بالوصول Access Control List (ACLs) لحركة البيانات الداخلة والخارجة وبذلك يتم تقليل الكثير من المخاطر الأمنية بالسماح بوصول الشبكات الموثوق بها ومنع وصول جميع الشبكات الأخرى ويمكن لمسؤولي أمن الشبكات السماح بالوصول لخدمات معينة فقط كخدمة تصفح الانترنت من خلال بروتوكول (HTTP) على المنفذ (8080) وخدمة تحويل العناوين (DNS) على المنفذ (٥٣) وهكذا.
ولضمان عمل الموجه بشكل سليم بوظائف الحماية المتكاملة لابد من التأكد من إعداد قوائم التحكم بالوصول (ACLs)، و تحديث نظام التشغيل أولا بأول من موقع الشركة الصانعة، ومراقبة أداء المعالج والذاكرة ومعالجة الخطأ عند ملاحظة زيادة الحمل على أحدهما، وتوفير موجه بديل جاهز بنفس الإعدادات لاستخدامه فور تعطل الأول. مع ضرورة الاهتمام باستخدام وتفعيل خصائص التحقق من الصحة باستخدام أسماء المستخدمين وكلمات مرور قوية، واستخدام خاصية تشفير كلمات المرور، واستخدام خاصية الشبكات الافتراضية عند الاحتياج مع تطبيق التشفير المناسب ، وتعطيل جميع الخدمات غير المستخدمة وتشغيل الخدمات الضرورية فقط وبالحد الأدنى اللازم لضمان الوصول بشكل جيد وسليم.

٤. الحماية الأمنية في أجهزة الوسيط (Proxy)

يُصمَّم الوسيط لإبقاء اتصال المستفيدين بوضع جيد، ويُثَبَّت بطريقتين مختلفتين الأولى الوضع الأمامي (Forward) ويكون وسيطا بين المستفيدين في شبكة منظمة ما وشبكة الإنترنت وفي هذه الحالة

يكون دوره حماية مستفيدي المنظمة من المشاهدة من قبل مستخدمي الإنترنت الموجودين خارج المنظمة بالإضافة لوظيفة التذكّر (Caching) حيث يقوم الوسيط بتخزين (تذكر) الصفحات التي يستعرضها المستفيدون لكي لا يتم جلبها من شبكة الانترنت في كل مرة بل يقوم الوسيط بتأمين الصفحات المختزنة لديه للمستفيد دون الحاجة لطلبها مرة ثانية من الانترنت. والطريقة الثانية عكسي (Reverse) ويكون وسيطا بين خادم ويب وجميع المستفيدين وفي هذه الحالة يحمي الوسيط خادم الويب من الاتصال المباشر مع المستفيدين بإخضاعهم لمجموعة من الإجراءات التي تُعرف في الوسيط بالإضافة لوظيفة التذكر حيث يستطيع الوسيط تأمين الصفحات المطلوبة سابقا من قبل المستفيدين من ذاكرته دون الحاجة للرجوع إلى خادم الويب وتسمى هذه الوظيفة في بعض المراجع (المسرِّع).

وفي كلتا الوضعيتين يمكن للوسيط الاحترافي القيام بحماية المنظمة بناء على إعدادات مسبقة يقوم بإعدادها مسؤول الأمن في الشبكة لتمييز طلبات المستفيدين المسموح بها وتمريرها وتمييز الطلبات الأخرى وإيقافها، وتمييز المحتوى المسموح وتمريره وإيقاف غير المسموح، وكشف وصد الفيروسات والبرامج الضارة ، وتصفية صفحات الإنترنت بناء على تصنيفات علمية لتسهيل حجب أصناف وتمرير أخرى.

ولابد من القيام بإجراءات دورية للمحافظة على سلامة الوسيط واستمرارية عمله ومنها القيام بأخذ نسخة احتياطية بشكل دوري عن إعدادات الوسيط وقبل أي تعديل، والقيام بتحديث نظام تشغيل الوسيط بالتحديثات الصادرة من الشركة المصنعة، وتوفير وسيط احتياطي معدّ بنفس الإعدادات ويعد ليعمل فور توقف الوسيط الأساسي آليا أو يدويا والطريقة الآلية أفضل.

يجب التأكد من أن أجهزة الحماية كجدران الحماية وأجهزة الخادم وأجهزة التوزيع محمية ولا يدخل إليها (فيزيائيا) سوى الأشخاص المخولين والمصرح لهم بالدخول حتى عمال النظافة ورجال الحراسة ينبغي أن يدخلوا بمعرفة إدارة أمن المعلومات وفي كل الأحوال لابد من القيام بتسجيل البيانات المطلوبة في سجلات خاصة بغرفة الخادم ومنها على الأقل: تسجيل أسماء جميع الداخلين مع مرجعية كل منهم وسبب الدخول، وتسجيل وقت الدخول، وتسجيل ما تم عمله في الغرفة، وتسجيل وقت الخروج .

حيث أن اختراق أي جهاز سواء كان خادم أو حاسب مكتبي أو وسيط إنترنت (Proxy) أو جدار حماية أو موجه (Router) سهل جداً بالنسبة للفنيين حيث يتطلب تعديل كلمة المرور في معظم الحالات إعادة التشغيل ثم قطع عملية الإقلاع بضغط زر (Break)، وتشغيل أمر أو تعديل كلمة المرور وحفظها في ذاكرة الإقلاع ومن ثم يتم إعادة التشغيل واستخدام كلمة المرور الجديدة، وتتاح طرق تعديل كلمات المرور (Recover) على شبكة الإنترنت من خلال مواقع صناعة

وتوريد تلك الأجهزة كخدمة من خدمات الدعم الفني. حيث تفترض جميع تلك الشركات أن مكان تركيب أجهزتها سيكون مكاناً آمنا ومحمياً.

٥. الحماية الأمنية باستخدام جدران الحماية:

تستخدم جدران الحماية على حدود الشبكات لحماية موارد تلك الشبكات والتي غالباً ما تكون قواعد بيانات، وتزداد أهمية حمايتها إذا كانت قواعد بيانات وطنية أو عسكرية أو تجارية، ولا بد أيضاً من الأخذ بالاعتبار حماية البرامج التي تشغلها والنظم التشغيلية والمحطات الطرفية وتوعية الأفراد المشغلين للنظام الشامل. ويُعد جدار الحماية "الجهاز الأكثر شهرة في عالم الشبكات المستخدم للحماية وترجمته الحرفية تعني جدار النار حيث يصنع جدار الحماية من الحريق في الأبنية من مواد غير قابلة للاحتراق ويوضع بحيث يقسم المكان لمنع انتشار الحريق من قسم إلى آخر وفي شبكات الحاسب الآلي يكون جدار الحماية نظاماً أو مجموعة من الأنظمة تقوم بالتطبيق الإلزامي لسياسة التحكم بالدخول بين شبكتين أو أكثر وتُصنف جدران الحماية الاحترافية في ثلاث أصناف رئيسة هي: جدران الحماية متخصصة وجدران الحماية المبنية على نظام الخادم وجدران الحماية الشخصية" [٧٧] .

و تصنف جدران الحماية المتخصصة إلى جدران حماية مبنية على البرمجيات وأخرى مبنية على أجهزة وتعدّ الجدران البرمجية أكثر شيوعاً لدى مستخدمي الحاسبات الشخصية. أما الجدران المبنية على الأجهزة فإنها تستخدم في الشركات والمؤسسات الكبيرة والمتوسطة، وما يهمنا في هذه الدراسة الاعتناء بالنوع الثاني الذي يُبنى على الأجهزة. ويمكن ذكر بعض أشكال أجهزة جدران الحماية كما يلي:

أ – أجهزة جدران الحماية المخصصة: وهي أجهزة حاسب آلي، تتميز بعدم تزويدها بمآخذ للوحة مفاتيح وشاشة ومأخذ تسلسلي عالمي وغيرها من المآخذ التي تزود بها عادة الحاسبات الشخصية والحاسبات المحمولة، وتقتصر على مخارج لربط الشبكات ومخرج للإعداد، ويوصل كل مخرج بشبكة معينة، ويمكن عزل الشبكات المتصلة بالمخارج تماماً بحيث لا يستطيع مسخدمو شبكة ما، الدخول إلى شبكة أخرى إلا بإنشاء أنفاق منطقية محددة داخل الجدار، ويعتمد هذا النوع في عمله على تقنية تحسس الحزم من خلال الدوائر الإلكترونية المتكاملة ASIC .

ب –جدران الحماية المدمجة: عندما تدمج وظائف جدار الحماية في موجه (router) أو موزع متعدد الطبقات (multilayer switch)، يسمى جدار الحماية بهذه الحالة

[77] Cisco systems inc. **Fundamentals of network security** (Indiana: Cisco press,2004) p 60

جدار حماية مدمج ، ويسمى في بعض المراجع جدار نقطة الاختناق (choke-point)، وعادة يقوم هذا النوع بتفتيش وفحص الحزم القادمة من مصادر غير موثوقة من خلال بروتوكول الإنترنت IP ويتميز هذا النوع بسرعته بالأداء ونقطة ضعفه أن إمكانية فك رموزه كبيرة من قبل المهاجمين الخبراء .

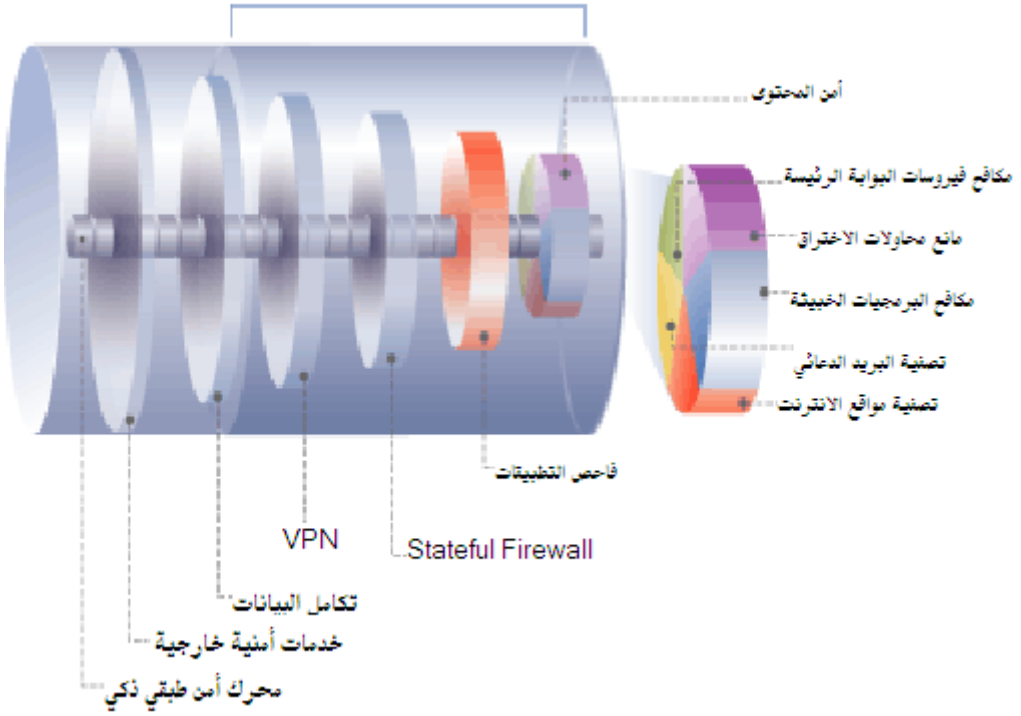
ت -بطاقات ذات وظيفة جدار حماية: تركب في موزع متعدد الطبقات (Multi Layer Switch) وغالباً ما يكون دوره كموزع مركزي (Core Switch) مثل Cisco Firewall Service Module (FWSM) .

ث -جدران الحماية الداعمة للشبكات الافتراضية الخاصة: بالإضافة لوظائف الحجب والتصفية للحزم الواردة ، فان هذا النوع يقوم بتأمين الشبكات الافتراضية الخاصة، بإضافة ميزة التشفير البيني، وقد دعيت خاصة لأنها تستخدم التشفير، وافتراضية لأنها تستخدم الشبكات العامة (الانترنت) لنقل معلومات خاصة. وعلى الرغم من أن ميزة الشبكات الافتراضية الخاصة كانت متوفرة قبل جدران الحماية باستخدام الموديمات وأجهزة التشفير فإنها أصبحت حالياً ميزة أساسية في جدران الحماية، وتستفيد المؤسسة التي لديها فروع من تقنية الشبكات الافتراضية الخاصة باستبدال خطوط الاتصالات الهاتفية المؤجرة بقنوات مشفرة عبر شبكة الإنترنت.

٦. أجهزة إدارة التهديدات الموحدة (UTM):

توفر تقنية المعلومات وسائل متنوعة لحماية الشبكات من أهمها جدران الحماية (firewalls) التي عرِفت في جدران الحماية التقليدية بالمصافي التي تطورت أخيراً لتصبح أجهزة حماية متعددة الخصائص (UTM) (الإدارة الموحدة للتهديدات) وهي جدران حماية لديها خصائص متعددة في صندوق واحد، وتتضمن تصفية البريد الإلكتروني الدعائي (Spam) وإمكانات الحماية من الفيروسات وكشف و منع التجسس (IDS/IPS)، وتصفية محتوى صفحات الوِيب بالإضافة لمهام جدران الحماية التقليدية. تصنف جدران الحماية هذه على أنها جدران حماية طبقة التطبيق (Application Layer)، لذلك يمكنها العمل بالنمط الشفاف (Transparent Mode) بحيث يتم إلغاء المستوى الأعلى من الفحص وبذلك تكون جدار الحماية أكثر بساطة من بوابة تحويل عنوان الشبكة NAT [٧٨] والشكل (٦) يوضح ذلك.

[٧٨] موقع ويكيبيديا



UTM Functions

الشكل (6)

وظائف جدران الحماية التي تستخدم مفهوم إدارة التهديدات

وقد اهتمت جدران الحماية في بداية ظهورها بالتصفية فقط (Filtering) ومن ثم أُلحِقت بها وظائف مختلفة مثل كشف محاولات الاختراق والتجسس (IDS) وكشف محاولات الاختراق والتصدي لها (IPS) وكشف ومكافحة الفيروسات ومنافذ تمكن من تأمين الاتصال النفقي الافتراضي عبر الإنترنت باستخدام التشفير ومن تلك الأجهزة جدران الحماية الحديثة (UTM) التي تمثل أوائل الكلمات في العبارة (Unified Threat Management) حيث تسعى لإدارة جميع التهديدات الممكنة من جهاز واحد يثبت في بوابة الشبكة المحلية،وتضم مكونات فرعية كتصفية مواقع الانترنت غير المرغوبة ومكافحة الفيروسات، وأحصنة طروادة، والبرمجيات الضارة، وعليه فإن كافة الشبكات الآمنة يجب أن تحمى بجدران حماية، فهي مطلوبة لتأمين الحماية بغض النظر عن اسم المُنتِج وجدران الحماية تقوم بإبقاء المستخدمين غير المرغوبين خارج شبكة المنظمة وخصوصاً عند إعدادها إعدادا سليماً.

٧. إعداد جدار الحماية:

عندما يقرر مسؤول أمن الشبكة في مؤسسة ما القرار الهام بتركيب جدار حماية للشبكة الداخلية، فلا بد من توكيل هذه المهمة لخبير بسياسة أمن المعلومات، فجدار الحماية لا يفيد في شيء إن لم يتم إعداده وتركيبه بالطريقة المناسبة. فلو كلف صاحب مبنى حارساً ووضعه عند باب المبنى بدون أن يوضح مهامه وبدون أن يخبره بالناس المسموح لهم بالدخول، بهذه الحالة فإن الحارس لن يمنع أحداً من الدخول، وبالتالي فلا فائدة من وجود هذا الحارس وتعتبر التكلفة المصروفة عليه ضياعاً ولا فائدة ترجى منها. ووجود جدار الحماية بدون إعداد يشبه أيضاً رجل الجمارك الذي يفتش بدقة ولكن ليس لديه قائمة بالممنوعات ولا بالمسموحات فيفتش ثم يمرر كل شيء مضيِّعا الوقت والمال. وهذا ينطبق على جدار الحماية، فهو لن يوقف أي حزمة قادمة من مصدر غير موثوق وهو لن يعترض أي حزمة مشبوهة ولذلك لا بد من إعداد جدار الحماية إعداداً صحيحاً ودقيقاً. ويعد تركيب وإعداد جدار الحماية ضرورياً وضرورياً جداً لكل شبكة حاسب آلي في أية منشأة تقرر الاتصال بالإنترنت، وفي حالة عدم تركيب جدار الحماية فإن العواقب ستكون بدون شك وخيمة جداً. ولحماية وتأمين الشبكات لا يكفي جدار الحماية وذلك للاعتبارات التالية:

أ – جدران الحماية ما هي إلا لبنة من لبنات السياسة الأمنية.

ب – يصبح جدار الحماية عديم الجدوى إذا لم يتم استخدامه بطريقة صحيحة.

ت – لا بد من تشغيل الخدمات المطلوبة وإيقاف الخدمات غير المطلوبة.

ث – تحديث نظام التشغيل كلما نصحت الشركة الموردة بذلك.

ج – يجب اختبار عمل جدار الحماية وذلك بمحاولة اختراقه من خارج المؤسسة، بصورة دورية والتأكد من سلامة عمله.

ح – جدران الحماية تركب لحماية الحدود فقط، ويجب مراعاة هذه الحقيقة.

خ – لا فائدة تُرجى من جدار الحماية عند وجود أبواب خلفية مثل الاتصال عن طريق المودم أو إدخال أقراص تخزين ملوثة في واحد أو أكثر من حاسبات الشبكة المحلية.

٨. تصميمات الحماية وفقاً لوظائف جدران الحماية:

يُعد جدار الحماية أساساً لتطبيق السياسة الأمنية لحماية الشبكة وذلك بوضع مخطط تظهر فيه أقسام الشبكة، حيث يقوم جدار الحماية بتقسيم الشبكة إلى شبكات منفصلة يتم التواصل فيما بينها من خلال وظيفة التوجيه (Routing) ومن خلال تطبيق السياسات التي يحددها مسؤول أمن الشبكة، وتتضمن جدران الحماية الحديثة وظائف مثل كشف ومنع الفيروسات والبرمجيات الضارة و تصفية

المواقع غير المرغوبة (Web Filtering)، وكشف ومنع التلصص ومحاولات الاختراق، ووظيفة تسجيل حركة الدخول والخروج من كل وجه (Interface) حسب الإعدادات المطلوبة، التي تحددها سياسات المؤسسة، بالإضافة لوظائف شبكية كتحديد معدل تدفق البيانات (bandwidth) والتوجيه (Routing)، والشبكات الافتراضية (VPN) وغيرها.

ولتنفيذ تلك الوظائف توضع جدران الحماية على حدود شبكة المؤسسة في بوابة الاتصال بالإنترنت والفروع، وقد صُنِعت جدران الحماية بحيث تتضمن عدة وظائف في جهاز واحد، توفيراً للمال والوقت وتسهيل إدارة جميع تلك الوظائف من نقطة واحدة، وفيما يلي تفصيل لأهم وظائف جدران الحماية الحديثة.

١. وظيفة تقسيم الشبكة (segmenting): يُزوَّد جدار الحماية بمنافذ (Ports) وتُدعى أحياناً واجهات (Interfaces) متعددة تزيد بازدياد إمكانيات الجهاز وعددها على الأقل منفذان وبالغالب تكون أربعة منافذ لجدران الحماية المتوسطة الحجم، ويُعَدّ المنفذ الأول (Int1) ليتصل بالشبكة الداخلية والمنفذ الثاني (Int2) ليتصل بالشبكة الحيادية والمنفذ الثالث بالشبكة الخارجية ويمكن أن تزيد الشبكات بحسب حجم الشبكة وحاجة الحماية الأمنية. حيث تقسم الشبكة إلى مناطق تكون الشبكة الداخلية موصولة بالمنفذ الأول (INT1) وتحتوي حاسبات المستفيدين وأجهزة الحماية من الفيروسات وأجهزة الخادم التي تؤمن التحقق من صحة المستفيدين كخادم (Active Directory) ، (RADIUS) ، (TACACS) . ويُعبَّر عن أقسام الشبكة بالمناطق لتبسيط المسألة وأهم المناطق هي:

أ –**المنطقة الآمنة:** غالبا ما تكون هي المنطقة الداخلية التي تتضمن حاسبات المستفيدين وخوادم قواعد البيانات وأجهزة الخادم التي تشغل خدمات الشبكة ,(DHCP) , (DNS) وخوادم الملفات وغيرها.

ب – **المنطقة غير الآمنة:** المنطقة العامة وغير الموثوق بها وغالبا ما تكون هي شبكة الإنترنت.

ت – المنطقة المعزولة(DMZ): تعد هذه المنطقة وسطاً بين المنطقة غير الآمنة (العامة) والمنطقة الآمنة (الشبكة الداخلية) وتوضع في المنطقة المعزولة عادة الخوادم التي تخدم المستفيدين الموجودين في المنطقة العامة (غير الآمنة) والمستفيدين الموجودين في المنطقة الآمنة (الداخلية) بالإضافة للمستفيدين الموجودين في المنطقة المعزولة نفسها. ويمكن أن يحتوي التصميم عدة مناطق معزولة حسب الحاجة.

ويعتمد توصيل جدار الحماية والموجهات على عدد المناطق حيث يجب توفير جدار حماية له وجهان (Interfaces) عندما يتوفر منطقتان داخلية وعامة حيث توصل الشبكة الداخلية إلى الوجه الداخلي (Internal Interface) وتوصل الشبكة العامة (التي تمثل المنطقة غير الآمنة) إلى الوجه الخارجي (Out Interface).

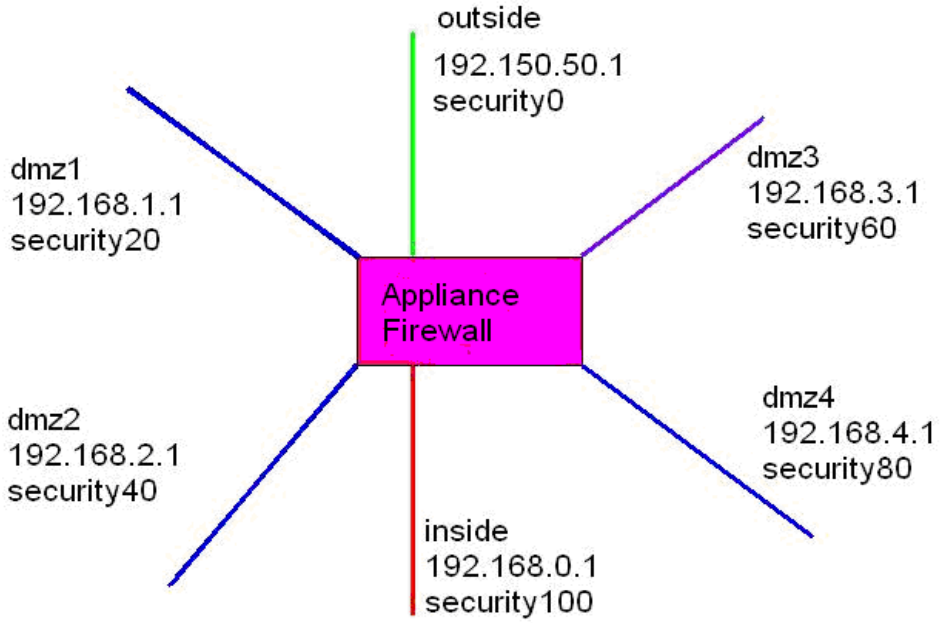
وعند وجود ثلاث مناطق يجب توفير جدار حماية له ثلاثة أوجه (Interfaces) وعندها يتوفر ثلاثة مناطق داخلية وعامة ومعزولة حيث توصل الشبكة الداخلية إلى الوجه الداخلي Internal (Interface) والشبكة العامة إلى الوجه الخارجي (Out Interface) والشبكة المعزولة إلى الوجه الثالث وغالبا ما يسمى (DMZ) وعند تعدد المناطق المعزولة تتعدد الوجوه الخاصة بها وتسمى ... , (DMZ2) ,(DMZ1) ويمكن إطلاق أي تسمية حسب الغرض المطلوب ولا ضرورة للتقيد بهذا العُرف.

٢-وظيفة تسجيل حركة البيانات: يقوم جدار الحماية بتسجيل كافة الأحداث التي يراها المهندس المسؤول جديرة بالاهتمام، كما يمكن له تحويل هذه الأحداث إلى خادم مخصص لتخزين وتحليل تلك الأحداث وغالباً ما يسمى نظام تسجيل الأحداث (SysLog) والغرض من ذلك القيام بتوثيقها في سجل يتضمن الطلبات القادمة مع مصدرها والهدف التي تقصده وكذلك الطلبات الصادرة والهدف الذي تقصده.

٣-التوفير في العناوين الخارجية والإخفاء للعناوين الداخلية: تقوم أجهزة جدران الحماية بتزويد المستفيدين بمئات العناوين الخاصة بشبكة المنشأة بينما يتصل جدار الحماية نفسه بعدد محدود من العناوين العامة على شبكة الانترنت. مثال ذلك عندما يتصل بالإنترنت ٢٤٠ مستخدم من داخل منشأة ما، فإنهم يحتاجون إلى ٢٤٠ عنوان إنترنت، وهذا أمر غير وارد بالنسبة لموردي خدمة الإنترنت، فمورد خدمة الإنترنت يعطي المؤسسة بحدود ٨ إلى ١٦ عنوان إنترنت بالغالب تُستهلك معظمها لخادم البريد الإلكتروني وخادم تفويض العناوين ومخارج جدار الحماية وغيرها، ويأتي جدار الحماية بالحل لهذه المعضلة بتحويل العناوين الداخلية إلى عناوين خارجية باستخدام جدول يضع فيه العناوين الخارجية وما يقابلها من العناوين الداخلية مرفقة بالمنفذ المستخدم، ويسمح لعشرات العناوين الداخلية باستخدام عنوان خارجي واحد بمساعدة المنافذ، والاستفادة من ذلك استفادة كبيرة، فمن جهة يتم إخفاء العناوين الداخلية بحيث لا يراها متصفحو الإنترنت الموجودون خارج شبكة المؤسسة مما يدعم حماية حاسبات المؤسسة، ومن جهة أخرى يتم توفير عناوين إنترنت عامة مما يوفر التكلفة المترتبة على تأمين عناوين إضافية.

٩. طريقة عمل جهاز جدار الحماية:

حيث أن أجهزة جدران الحماية تُزوَّد بمخرجين أو ثلاثة مخارج أو أربعة مخارج وهكذا، وتزداد قدرة الجدار كلما زادت مخارجه، فيكفي الشركات الصغيرة جدار بمخرجين، والشركات المتوسطة جدار بثلاثة، وتحتاج شبكات موردي الخدمة والشبكات الكبيرة أكثر من ثلاثة مخارج. والفكرة من المخارج هي أن كل مخرج يعطى اسم ودرجة سرية وكل مخرج يَرْبُط مقطع شبكي (منطقة)، وجميع المستفيدين الموجودين بشبكة مربوطة بمخرج ذي سرية عالية يمكنهم الاتصال بالمستفيدين المربوطين بمخرج ذي سرية أقل ولكن العكس غير ممكن إلا بإجراء الإعدادات المناسبة. والشكل رقم (٧) يبين جدار حماية بستة مخارج موضح عليه اسم المخرج ودرجة سريته وعنوانه وذلك على سبيل المثال.



الشكل (٧)

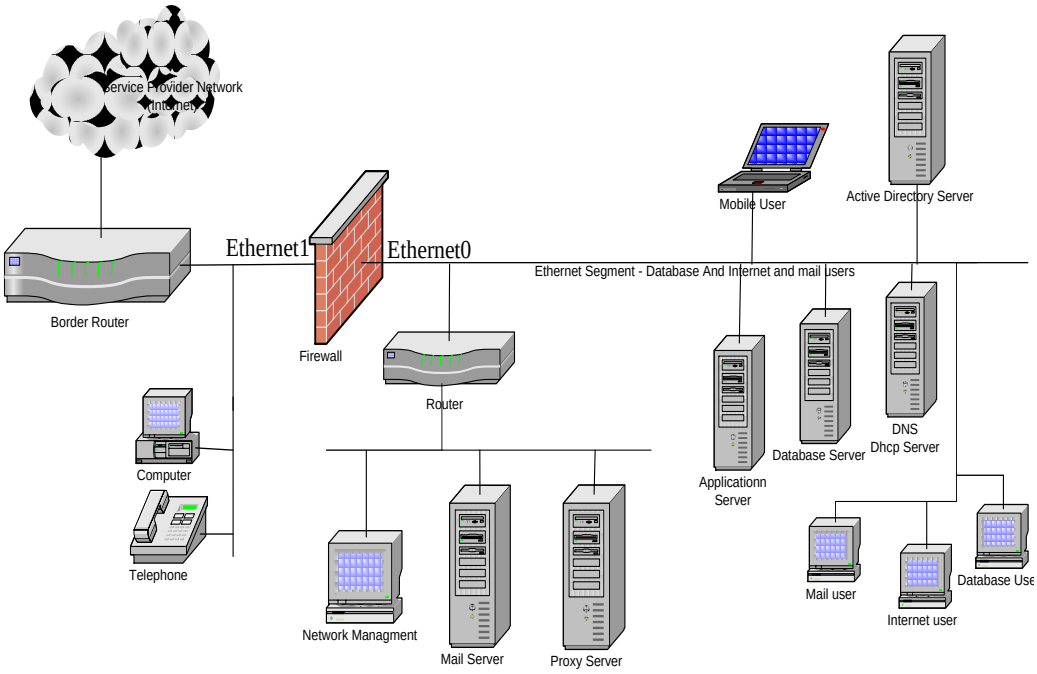
جدار حماية بستة مخارج

أمثلة على وصل أجهزة جدران الحماية على حدود الشبكات:

مثال ١: وصل جدار حماية يحوي مخرجين:

في الشكل (8) يُرى جدار حماية بمخرجين حيث أن المخرج الأول (Ethernet0) يوصل بموزع، وبهذا الموزع يتم وصل أجهزة الخادم الخاصة بخدمات الشبكة كخادم توزيع العناوين وخادم تحويل الأسماء (DNS)، وخادم قواعد البيانات (DB) وخادم المجال النشط (AD)، ويوصل خادم البريد الالكتروني ومفوض الانترنت بهذا المخرج ولكن من الأفضل عزله خلف موجِّه ووضعَه بقسم شبكي مختلف.

وأما المخرج الثاني (Ethernet1) فيتم وصله بموزع وتُربط بها أجهزة الهاتف الرقمية وأجهزة المراقبة وموجه بوابة الإنترنت، ولو اعتبرنا أن للجدار وجهين وكل وجه يمثل مخرج، فإن المخرج الثاني يعد بمثابة الوجه الخارجي للجدار، والمخرج الأول يعد الوجه الداخلي. والمستفيدين من الإنترنت الذين هم خارج المنشأة لا يرون الأجهزة الموجودة بالشبكة الداخلية.



الشكل (8)

شبكة محمية بجدار حماية بمخرجين

يسمى عادة المخرج (Ethernet0) المخرج الخارجي (Outside) أو (External) ويُعطى درجة السرية المنخفضة ويرمز للسرية المنخفضة بالرمز (security0)

ويسمى المخرج (Ethernet1) المخرج الداخلي (Inside) ويعطى درجة السرية العليا والتي يرمز لها بالرمز (Security100)، وفي الحقيقة فإن الأمر المستخدم لتسمية المخرج الأول والثاني كما في جدار حماية (Cisco) المبين بالشكل رقم (٨):

Nameif ethernet0 outside security0

Nameif ethernet1 inside security100

مثال ٢: وصل جدار حماية يحوي ثلاثة مخارج:

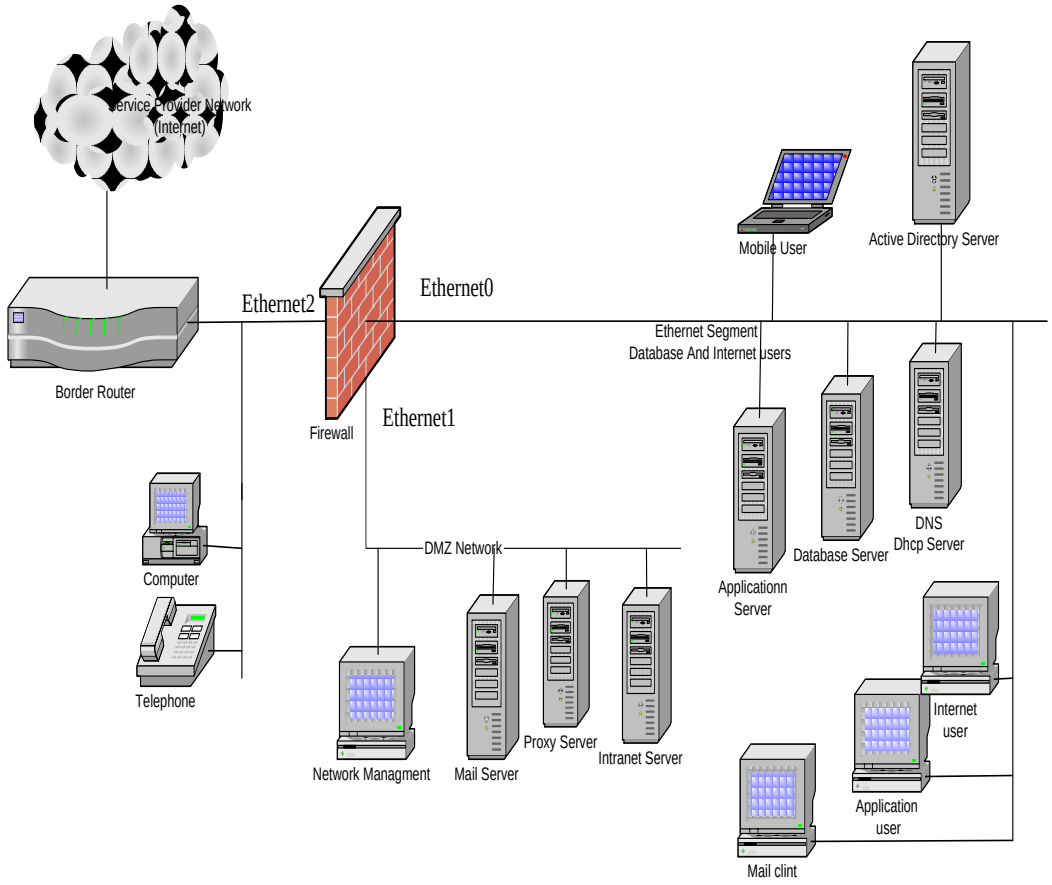
المخرج الأول (Ethernet0) يوصل بموزع وكما في المثال السابق يتم وصل أجهزة الخادم الخاصة بخدمات الشبكة، وخادم قواعد البيانات وخادم المجال النشط. ويسمى المخرج الخارجي (Outside) أو (External) ويعطى درجة السرية المنخفضة لها بالرمز(Security0) .

وأما المخرج الثاني (Ethernet1) فيتم وصله بموزع تُربط به أجهزة الهاتف الرقمية و خادم البريد الالكتروني ووسيط الانترنت، وأجهزة إدارة الشبكة والحاسبات الأقل أهمية أي التي لا تحتاج درجة حماية عالية، كحاسبات معامل التدريب والتي يفضل عزلها بموجِّهات (Routers) ويسمى هذا المخرج عادة المخرج بمخرج المنطقة منزوعة السلاح (DMZ) ويعطى درجة سرية متوسطة ويرمز لها بالرمز (Security40)، والرقم (٤٠) يمكن أن يكون أي رقم بين صفر ومائة في مثالنا هذا.

وأما المخرج الثالث (Ethernet2) كما في الشكل (9) فيوصل بموزع تلتقي فيه أجهزة الموجه الحدودي الذي سيؤمن توصيل الإنترنت من مورد خدمة الإنترنت مع أجهزة الهاتف الرقمية إن وجدت وأجهزة المراقبة، يعطى المخرج الثالث اسم (outside) ودرجة سرية منخفضة.والأوامر المستخدمة لتسمية المخارج وإعطاء درجات سريتها عادة ما تكون: كما في جدار الحماية من نوع (Cisco):

```
Nameif ethernet0 outside security0
Nameif ethernet1 outside security40
Nameif ethernet2 inside security100
```

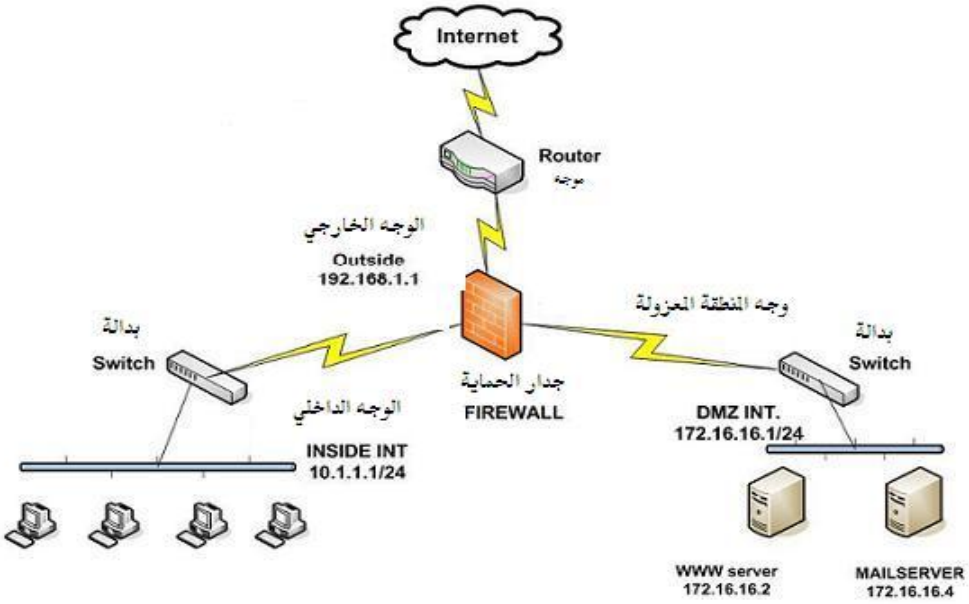
والفكرة من وجود ثلاثة مخارج هي إيجاد ثلاث مناطق واحدة عالية السرية وأخرى متوسطة السرية والثالثة منخفضة السرية، بحيث لا يمكن لمستفيد موجود بمنطقة أقل سرية الاتصال بمستفيد موجود بمنطقة أعلى سرية والعكس صحيح وهذه القاعدة تُعدَّل عند الحاجة عن طريق فتح أنفاق بين المناطق بالأوامر المتوفرة بأنظمة تشغيل جدران الحماية مثل ...., (conduit) ,(Access-list) وفقاً للسياسة الأمنية المحددة مسبقاً.



الشكل (9)

شبكة مزودة بجدار حماية بثلاثة مخارج

مثال٣ : يُرى في تصميم الشكل (١٠) المنطقة غير الموثوقة هي المتفرعة من الوجه الخارجي لجدار الحماية وتحوي الموجه و كل الشبكات الموصولة به. والمنطقة الموصولة الوجه الداخلي (Inside Interface) تعدّ منطقة موثوق بها (Trusted area) وتحوي الشبكة ١٠.١.١.١ بقناع ٢٥٥.٢٥٥.٢٥٥.٠ حيث يمكن أن يستوعب ٢٥٤ مضيف. والمنطقة الموصولة بالوجه المعزول (DMZ Interface) تعدّ منطقة موثوق بها وتحوي الشبكة ١٧٢.١٦.١٦.١ بقناع ٢٥٥.٢٥٥.٢٥٥.٠ حيث يمكن أن يستوعب ٢٥٤ مضيف.



الشكل (١٠) جدار حماية بثلاثة وجوه

هذا التصميم يناسب المنظمة التي تتوضع منشآتها على مساحة جغرافية صغيرة كالجامعة أو المشفى ولا يوجد لها فروع. أما المنظمات التي لها فروع تفصل بينها مسافات جغرافية فيكون التصميم مكوناً من مناطق موثوق بها تفصل بينها مناطق غير الموثوق بها كأن يكون منطقة شبكة مبنى الإدارة الرئيسة موثوقاً بها.

١٠ - محاسن ومساوئ أجهزة جدران الحماية:

١ محاسن أجهزة جدران الحماية:

بسبب حسنات هذا النوع من الأجهزة ينصح بشدة بتركيبها في شبكات المؤسسات الكبيرة، وتفيد جداً في الشركات المتوسطة وخصوصاً تلك التي لا يتوفر فيها خبير أمن معلومات، ومن هذه الحسنات:

أ - سهولة التركيب حيث تستغرق وقتاً طويلاً في الإعداد.

ب -واجهة استخدام سهلة مع سياسات أمنية جاهزة.

ت – وظائف حماية كثيرة في جهاز واحد.

ث – التوافق مع كافة خطوط الاتصال.

ج – التعامل مع الشبكات الافتراضية.

ح – تتمتع بوظائف تصفية الحزم .

خ – تتمتع بوظائف خادم الوسيط (proxy).

د – تتصف بقدرتها العالية على إخفاء العناوين الداخلية واستبدالها بأخرى خارجية بمساعدة منافذ بروتوكول TCP/IP.

٢ -مساوئ أجهزة جدران الحماية:

أ – بساطتها فهي لا تستطيع اكتشاف الاختراقات المعقدة.

ب –كونها أجهزة فلا تتصف بالقدر الكافي من المرونة التي يمكن أن تقدمها البرامج فتتحدث قواعد بياناتها وأنظمة تشغيلها وتبقى الأجهزة على حالها.

ت –لكل جهاز خصائصه التي تختلف عن مثيلاته حتى لو كان من إنتاج الشركة نفسها، فمن الضروري الانتباه للمواصفات بدقة عند التوريد.

ث –في الغالب تقوم جدران الحماية بإبطاء حركة الحزم عند البوابة وذلك عندما تطبق وظائف كثيرة كالحماية من الفيروسات والتصفية وكشف الاختراق وتسجيل الأحداث وتصبح حركة الحزم بطيئة في حالة كون جهاز الحماية أقل سعة من المطلوب كـــأن يُركب جهاز جدار حماية مخصص لخمسين مستخدم على حدود شبكة فيها مائة مستخدم.

١١ –**جدار الحماية الاحتياطي:** من المناسب تشغيل جدارين معاً أحدهما رئيسي والأخر احتياطي فعند تعطل الأول يقوم الثاني بالعمل مكانه، ويوجد في أنظمة تشغيل جدران الحماية تعليمات يجب إعدادها بعناية لتحديد الوقت الذي يجب أن ينتظره الجدار الاحتياطي حتى يستلم العمل، وفي حالة تشغيل جدار واحد لا بد من إشعاره بذلك بالأمر (No failover) وفي المنشآت الكبيرة يجب أن يتوفر في جدار الحماية منفذ لربط جهاز حماية آخر مماثل لكي يعملا بطريقة (Active–Active) وعادة ما يطلق هذا المنفذ

اسم (HA) اختصاراً للعبارة (High Availability) حيث يتم وصل الجهازين معا وفي حالة تعطل أحدهما يستلم الآخر العمل عنه مباشرة. وتوجد طريقة أخرى للوصل ولكن تحتاج لتدخل من قبل مسؤول الحماية وهي (Active–Standby) وفيها عند تعطل الجدار الرئيس المشار إليه بعبارة (Active) يقوم المسؤول بتشغيل الجدار الثاني (Standby)، وهذه الطريقة أقل تكلفة من الأولى ولكنها تحتاج لتدخل من قبل المهندس المسؤول.

١٢ – اختيار جدار الحماية:

الجدار الأفضل هو الذي يمكنه تطبيق احتياجات السياسة الأمنية ومن هذه الاحتياجات: حماية الشبكة الداخلية من الاختراق وحماية الشبكة الافتراضية، بالإضافة للمحافظة على سرعة الأداء. ولتحقيق هذه الأهداف فإن أفضل جدار حماية هو ذلك الجدار الذي يحقق أكبر عدد من النقاط التالية:

أ – أن يحوي الوظائف المطلوبة .

ب –أن يكون فنيو المنشأة قادرين على إعداده بشكل جيد، وإن لم يكن فعلى الأقل أن تتوفر إمكانية التدرب عليه.

ت –أن يتوفر دعم فني بالمدينة التي تتواجد فيها المنشأة.

ث –تتوفر فيه إمكانية تحديث نظام تشغيله وقاعدة بياناته بصورة دورية بشكل يومي.

١٣ – مكملات الحماية مع جدران الحماية:

يمثل تركيب جدار الحماية الخطوة الأولى على طريق تحقيق أمن شبكة المؤسسة، ولا تستطيع جدران الحماية المخصصة للشركات الصغيرة أو المتوسطة حماية شبكة المنشأة بشكل كامل، بل تحتاج لدراسة شاملة للمَواضِع المعرضة للهجوم، وعند حصول هذه الدراسة لا بد أن يصدر عنها قرارات توجب تنفيذ إجراءات هامة منها:

أ – تفحص أنظمة التشغيل والتطبيقات وقواعد البيانات وكلمات المرور والتي تقع خلف جدران الحماية، واكتشاف كافة الثغرات الأمنية المحتملة فيها وسدها باتخاذ الإجراءات الملائمة لذلك.

ب –توعية المستفيدين من البريد الإلكتروني بأساليب الخداع للبرامج الخطرة المرسلة مع البريد الالكتروني واتخاذ كافة الإجراءات الضرورية للحد من البرامج الضارة ومنها تركيب مضادات للفيروسات.

ت -توفير نظام الكشف عن الاختراق و التطفل Intrusion Detection and Prevention System (IPS) حيث تقوم هذه الأنظمة بكشف محاولات الاعتداء واتخاذ التدابير المناسبة آلياً بالإضافة لمهمات أخرى منها تتبع نشاطات المستخدم كدخوله وخروجه وحراسة الشبكة ضد أنواع معروفة من الهجمات والكشف عن حدوث مخالفات للسياسة الأمنية المتبعة.

ث -التحقق من هوية المستخدمين: التحقق من الهوية يعني التأكد من صحة هوية المستخدم بشكل يتجاوز مجرد التحقق من اسم المستخدم والكلمات السرية والتي لا تعتبر بحد ذاتها وسيلة قوية للتحقق من هوية المستخدمين، ويضاف إليها أساليب قوية للتحقق من هوية المستخدمين كالتشفير باستخدام الشهادات الرقمية، وبوساطة الشهادات الرقمية يمكن تفادي هجمات إعادة الاستخدام .

ج - مراقبة المحتوى: لقد أضيفت هذه الميزة في الأعوام الثلاثة الأخيرة مما زاد من قدرة جدران الحماية كأدوات لمراقبة المحتوى الوارد إلى الشبكة.

ح - الحماية من البرامج الضارة كالحماية من الفيروسات، ومراقبة عناوين الإنترنت، ومنع برمجيات جافا، وبرمجيات مسح كلمات سرية.

خ - لا بد من توفير بيئة التجربة (Test Environment) لتجربة التحديثات قبل تثبيتها. وتجربة التعديلات قبل تركيبها في بيئة الإنتاج (production Environment) وهي بيئة العمل الفعلية.

د - لا بد من توفير بيئة للتطوير (Development Environment): يستخدمها المبرمجون والمطورون في برمجة التطبيقات الجديدة، وتعديل التطبيقات.

٢-١-١٣ برامج الحماية من الفيروسات داخل الشبكة الواحدة:

برامج تركب على خادم ويثبت لها مساعدات في جميع الحاسبات الأعضاء في الشبكة، يتم تحديث الخادم يومياً من الشركة الصانعة ويتم تحديث المساعدات من خلال الخادم داخل الشبكة تبعا للسياسة الأمنية الموضوعة في المؤسسة، ويتم تنفيذ فحص دوري (يومي غالباً) لجميع الحاسبات. ومن أمثلتها: (Trend Micro Office Scan)، (Norton)، (Sophos)، (Avir-AntiVir)، (Kasper Sky)، (MacAfee)، (E-Trust)، (Avast) ، (E-trust).

٢-١-١٤ أمن المعلومات (Information Security):

تحتاج المنشآت عامة والمنشآت ذات الطبيعة التنافسية والعسكرية والأمنية خاصة لتأمين عنصر السرية للمعلومات التي تتطلب توفير السرية وعدم الإفشاء أو حمايتها من الانتهاك ومن الإجراءات المتبعة عادة توقيع الموظفين من داخل المنشأة والمتعاونين من خارجها على سن تعهد رسمي يتضمن في بنوده بندا بوجوب الالتزام بعدم إفشاء الأسرار التي يطلع عليها بحكم واجباته الوظيفية. وإجراءات المحافظة على أمن المعلومات تُتبع في المنشآت التي تستخدم شبكات الحاسب لحماية المعلومات من التهديد بالإزالة أو النقل أو الحذف أو التعديل أو التوقف عن الخدمة.

وللحفاظ على أمن المعلومات ذات الخصوصية يجب أن تتضمن الإجراءات ذات الصلة ما يلي:

١. بيان درجة السرية (سري للغاية، سري جداً، سري) وطرق تأمين كل درجة.
٢. حفظ الوثائق الهامة بوسائط حفظ الملفات الالكترونية المؤرشفة.
٣. حُسن اختيار الأفراد العاملين في حقل تقنية المعلومات حسن تدريبهم.
٤. ضمان أمن المعلومات المخزنة داخل أجهزة الحاسب الآلي بإجراءات ضرورية منها:
   أ. استخدام أقفال وتسلم مفاتيحها للأفراد المخولين فقط.
   ب. استخدام كلمات المرور القوية للدخول إلى جهاز خزن المعلومات.
   ت. استخدام شفرة (Code) لفتح البرامج.
   ث. استخدام بطاقات ممغنطة للدخول إلى غرف الحاسب الآلي.
   ج. استخدام بطاقة خاصة للدخول إلى أجهزة الخادم.
   ح. حصر وتحديد الأفراد الذين لهم الحق بالتعامل مع أجهزة الخادم.

٢-١-١٥ الحماية الأمنية لنظم التشغيل

تعد الحماية الأمنية في أنظمة التشغيل مسألة حيوية لأي نظام معلومات فاعل، وهي في غاية الأهمية، وخصوصاً عندما يتعلق الأمر ببعض الأنظمة الهامة مثل أنظمة معالجة القضايا العسكرية حيث يجب أن تقاوم أنظمة التشغيل أي نشاط غير شرعي كالوصول غير المخول، وانتحال شخصية مستفيد شرعي نتيجة إهمال وجهل المستفيد الشرعي بقواعد أمن المعلومات كأن يفشي بيانات حسابه أو يضع كلمة مرور بسيطة أو يهمل تحديث نظام التشغيل فيستغل المهاجم واحدة أو أكثر من تلك الثغرات فيقوم بواحد أو أكثر من الهجمات التالية:

أ - زرع أحصنة طروادة ثم جمع المعلومات من خلالها.

ب - يحصل على كلمة المرور بمراجعة إشارات ضربات المفاتيح عند قيام الضحية بتسجيل الدخول ويحصل على كلمات المرور ويعطي نفسه صلاحيات غير شرعية.

ت - يقوم المهاجم بتنفيذ الهجوم التنكري (Masquerade Attack).

١. التحكم بالوصول في أنظمة الحاسبات:

لكل نظام من أنظمة الحاسبات مجموعتين من المكونات، الأولى مكونات خاملة (Passive) لا تنتقل إلى أنظمة أخرى ويجب تأمين حمايتها فيزيائياً والأخرى مكونات نشطة (Active) يمكن أن تصل إلى مكونات حاسبات أخرى ولضمان ضبط الوصول إليها ظهرت مصفوفة الوصول.

أ - مصفوفة الوصول (Access Matrix) :

تمثل واقع الحماية الحالية في نظام التشغيل وعلى شكل مصفوفة من صفوف وأعمدة حيث تمثل الصفوف عادة العناصر التي لها حق الوصول وتمثل الأعمدة الموارد التي يحق الوصول إليها من قبل العناصر ومن الأمثلة على مصفوفة التحكم بالوصول المثال بالجدول رقم (٢/٣):

جدول رقم (٢/٣)

مثال مصفوفة تحكم بالوصول

	O1=S1	O2=S2	O3=S3	Q4	Q5
S1		انتظار		قراءة	قراءة، كتابة
S2	إشارة	تنفيذ	إرسال، استلام	حذف	كتابة
S3	تحكم	إشارة ، انتظار	تحكم	تنفيذ	قراءة

ب -مصفوفة الوصول الحركية (Dynamic Access Control):

تعكس مصفوفة الوصول الحالة الآنية لصلاحيات الوصول في نظام التشغيل، لذلك من الضروري تغييرها كلما تم تعديل الصلاحيات سواء بمنح صلاحيات جديدة أو سحب صلاحيات ممنوحة مسبقاً، باستخدام أوامر نقل الصلاحية، ومنح الامتياز، وحذف الامتياز، وقراءة محتويات مصفوفة الوصول، وإنشاء صلاحية، وحذف صلاحية، إنشاء مستخدم، حذف مستخدم.

ت -المشاركة وما يقابلها من حماية (Sharing versus protection)

توجد ثلاثة مستويات مشاركة تعتمد على أوامر الحماية وهي:

١. عدم وجود المشاركة (العزل الكامل).
٢. مشاركة لبيانات كينونات الخدمة (objects).
٣. مشاركة لبيانات المستفيدين (Subjects).

ث -استخدامات أنظمة التحكم بالوصول (Implementation of Access Control Systems).

يمكن أن تأخذ الاستخدامات المباشرة لمصفوفة الوصول صيغتين:

١. قدرة موجهة (مخصصة).
٢. قائمة تحكم بالوصول موجهة.

ج -نظام القدرة (Capability System):

وُضعت آلية تحكم بالوصول مخصصة للقدرة من قبل "سكرودر" و سالتزر" (Schroder, Saltzer) وفي هذه الآلية لكل مستفيد زوج مؤلف من اسم وكلمة مرور (الاسم، كلمة المرور) يوجد ضمن جدول تعريف المستفيد. ويقوم المشرف (Administrator) باختيار صلاحيات المستخدم من قائمة الصلاحيات باستخدام معالج الصلاحيات، وتكون جميع أوامر الحماية أو مصفوفة الوصول تحت سيطرة المشرف فقط وتخزن في منطقة محمية تقبل الوصول إليها من قبل المشرف فقط أيضاً.

ح - نظام قائمة التحكم بالوصول (Access Control List System):

يحتوي النظام كينونات امتياز تزود كل منها بقائمة بأسماء المستفيدين ذوي صلاحية الوصول تتطلب مصادقة المشرف الذي يقوم بفحص القائمة والتأكد من وجود صلاحية الوصول للمستخدم عند الطلب. ولزيادة سرعة الأداء تضاف سجلات التعقب (Shadow Registers) لتسجيل إشارات الطلب وعدم إعادة فحص المكونات التي سبق فحصها في القائمة وبذلك ينقص زمن المعالجة ويُستخدم نظام التحكم بالوصول في نظام تشغيل (Unix).

خ - تصميمات نموذج التحكم بالوصول:

وضع العالمان "سلتزر" و "سكرودر" (Schroeder, Saltzer) مجموعة من المبادئ تُراعى عند تصميم آلية التحكم بالوصول أهمها:

١. مبدأ التصميم المفتوح: ويتلخص بوجوب عدم اعتماد الحماية الأمنية للتحكم بالوصول على آلية التحكم بالوصول.
٢. مبدأ التفكير العميق التام: وينص على وجوب تدقيق الوصول المنفرد لخدمة معينة من قبل آليات التحكم بالوصول قبل السماح بالوصول.

٣. مبدأ الصلاحية الأقل: وفيه يجب إعطاء الحد الأدنى من الصلاحيات التي تؤمن إكمال واجبات العمل.

٤. مبدأ اقتصاد الآلية: يجب أن تكون الآلية سهلة ما أمكن.

٥. مبدأ القبول: وينص على أن الآليات صعبة التطبيق قد يُساء استعمالها بالوصول غير الشرعي إلى الخدمات.[٧٩]

٢-١-١٦ الحماية الأمنية لقواعد البيانات:

تعدّ قواعد البيانات في أي منظمة معلوماتية من أثمن الأصول التي تمتلكها لذلك كان من الضروري إعطاء صلاحيات الوصول إليها وفق الاحتياج الضروري للمستفيدين أو المشغلين بل حتى المبرمجين وحماية المكونات التي لا يحتاجها كل منهم. بسبب أخطاء الاستخدام وعدم ضبط الصلاحيات بالشكل المناسب يمكن أن تقع نسخ من أجزاء القاعدة في أيدي أفراد غير مرغوب فيهم ولحل هذه المشكلة تستخدم الحماية التشفيرية لقواعد البيانات باستخدام دالة "هاشية" ذات اتجاه واحد وخوارزمية تشفير تناظرية حيث أن كل قيد في قاعدة البيانات يملك حقلين يكون الأول للفهرسة والثاني للمفتاح.

١. تطبيق التشفير في قواعد البيانات (Application of Cryptography in Data Base):

قبل الغوص في موضوع تطبيق التشفير يرى الباحث ضرورة لذكر مفاهيم أساسية في التشفير:

أ - التشفير (cryptography) [٨٠]: هو مجموعة من التقنيات تستخدم لتحويل المعلومات إلى معلومات بديلة يمكن عكسها لاحقاً. يُشار إلى هذه المعلومات البديلة بالنص الواضح ونموذجياً تُنشأ باستخدام خوارزمية تشفير ومفتاح تشفير. وتسمى العملية المعاكسة للتشفير عملية فك التشفير.

ب -التحقق من الصحة (Authentication): هو عملية التأكد من أن كلا من النهايتين لوصلة الاتصال هما بالفعل من يقوم بالاتصال[٨١].

ت -خوارزمية التشفير (Crypto Algorithm): [٨٢] هي ببساطة صيغة رياضية تطبق على المعلومات المرغوب في تشفيرها.

---

[٧٩] انظر: عوض حاج علي أحمد، و آخرون، أمنية نظم التشغيل والشبكات الموزعة (الخرطوم: مطبعة جامعة النيلين ٢٠٠٢) طبعة١. ص ص ١-١٢

[80] See: Brenton Chress and Others: (Mariana Village Parkway, Alameda: Syb ex inc, **Mastering Network Security**, 2nd ed., 2003) PP 220.

81 .Ibid., p215

ث -مفتاح التشفير (crypto key):[٨٣] هو متغير إضافي يُدخل في الخوارزمية للتأكد من أن النص الواضح لا يشتق باستخدام نفس عملية الحساب كل مرة تُعالج فيها المعلومات باستخدام الخوارزمية.

تتعرض قواعد البيانات للتعديل من قبل مدخلي البيانات والمبرمجين والعاملين على صيانتها وتطويرها وبذلك تكون عرضة للتغيير غير المرغوب وقد يحصل هذا التغيير غير المرغوب فيه نتيجة لسوء استخدام غير مقصود من مستفيد شرعي، أو من قبل مستفيد غير شرعي، أو تصرف مخالف من مستفيد شرعي.

وبما أن قواعد البيانات التي هي تجمع لمجاميع معلومات مخزنة في مساحات تخزينية في الحاسب الآلي تعدّ جزءاً داخلياً من مكونات الحاسب الآلي (أجهزة الخادم) وللوصول إليها لا بد من تخطي الحواجز الأمنية المعدَّة لدخول الحاسب ومنها خط دفاع جدران الحماية وخط دفاع نظام التشغيل الذي يعوّل عليه كثيرا في حماية قواعد البيانات .

وبسبب وجود الثغرات الأمنية في نظم التشغيل على الرغم من التحديث المستمر من المطورين لنظم التشغيل واحتمالات استغلالها من قبل القراصنة والمستخدمين غير الشرعيين كان من الطبيعي عدم الاعتماد اعتماداً كلياً على إعدادات الحماية الخاصة بنظم التشغيل.[٨٤] حتى لو بلغت أنظمة التشغيل أعلى درجات الحماية.

ولا بد من الاعتماد على جملة من المعايير الأمنية في وقت واحد وخصوصاً عندما تتعلق الحماية بقواعد البيانات حيث يشرف نظام التشغيل على وصول المستفيد إلى قواعد البيانات النشطة في ذاكرة الحاسب الآلي. ويمكن استخدام التشفير لحماية سجل البيانات المخزن في الذاكرة. وبذلك يتم التغلب على سلبيات ثغرات نظام التشغيل الأمنية ففي حالة حصول وصول غير شرعي لسجلات قاعدة البيانات فيتوجب على القائم بذلك الوصول حصوله على المفتاح التشفيري المناسب. ولا يستطيع الاستفادة من وصوله كون البيانات مشفرة (غير قابلة للقراءة) وخصوصا أن تناقل البيانات بين مساحات التخزين والذاكرة في الحاسب الآلي تتم بالنص المشفر داخل نظام الحاسب وبإشراف النظام التشغيل.

---

82 Loc. Cit

83 Loc. Cit

٨٤ الحماية الأمنية لنظم التشغيل تعد على مستويات وباستخدام مصفوفة التحكم بالوصول ، انظر الفصل ٢ فقرة الحماية الأمنية لنظم التشغيل.

وبالتالي إن أي نسخ لمحتويات الذاكرة من قبل من لا يملك المفتاح التشفيري غير مفيد له لأن هذه النسخ تحتوي على النص المشفر (غير الواضح).[٨٥]

٢. التحويلات التشفيرية الحافظة لقواعد البيانات: (Cryptographic Transformations Preserving Data Structure)

بافتراض أن مجموعات البيانات بصيغة النص الواضح تمثل مستوى أول (Level 1) وأن مجموعات البيانات بالصيغة المشفرة تمثل المستوى الثاني (Level 2)، وبافتراض رمز المستوى (L) وقاعدة البيانات (DB) والتحويل التشفيري (E) والمفتاح التشفيري (K) يمكن الوصول إلى التعبير

$$E_k(LDB^{(1)}) = LDB^{(2)}$$

ويعني أن قاعدة البيانات في المستوى الثاني هي تحويل لقاعدة البيانات في المستوى الأول وفق المفتاح التشفيري (k) وفي الواقع تكون (E) مجموعة من التحويلات التشفيرية معرفة لعناصر محددة من قاعدة البيانات وتكون (k) مجموعة المفاتيح للتحويلات التشفيرية المقابلة.

وتبقى التحويلات التشفيرية (النصوص التشفيرية) محافظة على هيكل البيانات، وتبقى عناصر في قاعدة البيانات إلى جانب عناصر قاعدة البيانات الأخرى، وهي عناصر البيانات وقيود فيزيائية وحقول وقيود منطقية.

ومن التحويلات التشفيرية التي تطبق لحماية قواعد البيانات ما يلي:

أ -إحلال عناصر البيانات (Substituation of Data Items)

إن النصوص الواضحة والبيانات المشفرة عناصر بيانات توضع في حقول وفي تحويل الإحلال تتوفر حالتان الأولى لتغيير مواضع البيانات في الحقول قبل وبعد التحويل وبذلك يتم خداع غير المخولين لعدم إدراكهم إن كانت البيانات مشفرة أم لا. والحالة الثانية تكون عناصر البيانات قبل التحويل وبعده تتبع حقول مختلفة وعندها تكون صيغ عناصر البيانات الممثلة للنصوص المشفرة سلاسل من أرقام وحروف وليس من الضرورة أن تكون قابلة للقراءة.

ب - تقليص عناصر البيانات (Reduction of Data Item)

هو تحويل تشفيري له الصيغة التالية:

$$D^{(2)} = E_k\ (d1^{(1)} \ldots\ldots\ldots\ dp^{(1)})$$

[٨٥] لا بد هنا من التنويه إلى أن الحصول على النص المشفر قد يفيد العدو عند امتلاكه تقنيات كسر الشفرة باستخدام المسح والقواميس والمعالجات الرياضية المناسبة وقبل كل ذلك الوقت الكافي للقيام بعمليات كسر الشفرة ويساعد العدو على كسر التشفير عدم التقيد بإجراءات الأمان القاضية بضرورة تغيير المفتاح التشفيري وضرورة استخدام مفتاح تشفيري يحتاج وقت طويل ليتم فكه وبحيث يكون النص الواضح غير مفيد بعد الوقت المطلوب لفك التشفير وكشف النص الواضح.

التقليص لعدد p من عناصر البيانات في المستوى الأول لقاعدة البيانات يشير إلى عنصر بيانات مفرد في المستوى الثاني لقاعدة البيانات وتعتمد صيغة النص المشفر لعناصر البيانات على المفتاح التشفيري المستخدم. ويمكن أن ينجز تحويل التقليص في خطوتين: تعتمد الخطوة الأولى على لصق لعناصر البيانات المحددة وتستفيد الخطوة الثانية تحويل تشفيري معين. ومن عيوب هذا التحويل التشفيري أن الوصول إلى عناصر البيانات في المستوى الثاني لقاعدة البيانات لا يسمح باسترجاع عناصر البيانات الأصلية.

ت - توسيع عناصر البيانات (Expantion of Data Items):

تحويل التوسيع يعرّف كعملية معاكسة لتحويل تقليص العناصر والصيغة التالية تعرّف هذا التحويل:

$$(d_1^{(2)}, \ldots\ldots d_q^{(2)}) = E_k(d^{(1)})$$

وبذلك يخضع عنصر البيانات المفرد في المستوى الأول إلى عملية تشفير وبعد ذلك يقسم عنصر البيانات المشفر إلى q من العناصر المختلفة. ولا يتم تعريف عناصر البيانات في المستوى الثاني لذلك تكون عناصر البيانات محمية من الوصول غير الشرعي.

ث - تشفير عنوان الوصول (Encipherment of Access Address):

يتعامل تحويل عنوان الوصول التشفيري مع القيود المنطقية [٨٦] فإذا كان LR قيداً منطقياً في المستوى الأول لقاعدة البيانات وله الصيغة:

$$LR^{(1)} = i\ (\ F_1\ ,\ F_2\ ,\ldots\ldots,\ F_n\ )$$

وبعد تطبيق تحويل عنوان الوصول يتم الحصول على قيدين منطقيين $LR_1^{(2)}$ و $LR_2^{(2)}$

ج -التحويل التشفيري ومستويات قاعدة البيانات المقابلة (Cryptographyic transformation versus data base levels):

بغرض حماية قاعدة البيانات يُؤخذ بالاعتبار كل من المستفيد ومستويات صنف المستفيد، وحيث أن أي مستفيد يعمل في مساحة عمله ويملك الوصول إلى جزء قاعدة البيانات، وهو صنف المستفيد. وبفرض أن عناصر قاعدة البيانات لمستوى صنف المستفيد يتم تشفيرها بحيث يستطيع المستفيد معالجة

---

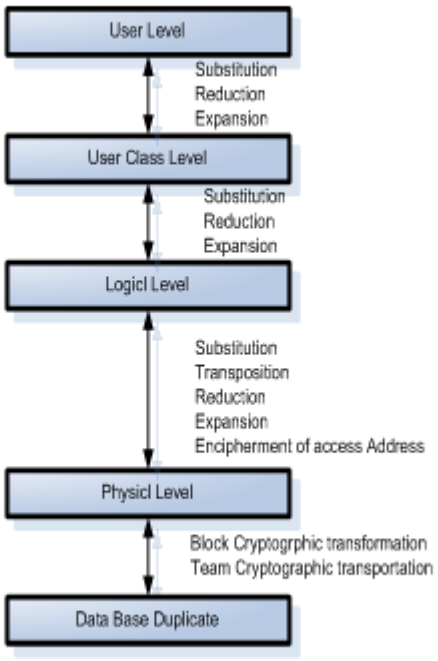
[٨٦] القيود فيزيائية ومنطقية والقيد الفيزيائي Physical Record هو قيد تكون فيه العناصر مرتبة ومترابطة بشكل تسلسلي فإذا كان PR قيداً فيزيائياً لقاعدة البيانات في المستوى i فإنه يعرّف كالآتي: $PR^{(i)} = (d^{(i)}, \ldots\ldots, d_n^{(n)})$ ، ويظهر هذا القيد على شكل جدول توجد فيه عناصر البيانات في حقول موزعة على بشكل أسطر وأعمدة يكون السطر قيد فيزيائي مفرد ويكون العمود مكوناً من مجموعات من بيانات متجانسة. والقيد المنطقي LR (Logical Record) هو الجدول الكلي مع اسم مميز وإذا كان $F^{(i)}$ الحقل في المستوى i لقاعدة بيانات هو مجموعة لكل عناصر البيانات لصفة مناسبة فإن القيد المنطقي في المستوى i يعرف كالتالي: $LR^{(i)} = I\ (F_1, F_2, \ldots\ldots F_k)$ و قاعدة البيانات المنطقية LDB في المستوى i تتكون من تجمع لكل القيود المنطقية مع مفسراتها وتعرف كالتالي: $LDB^{(i)} = \{LR_1^{(i)}, \ldots\ldots LR_m^{(i)}\}$ + INTEREPRETATION ، انظر عوض حاج علي أحمد أمنية التشغيل والشبكات الموزعة ص ص ٢١-٢٢ .

البيانات بصورة صحيحة إذا ضمنت المفاتيح التشفيرية المناسبة وتوجد ثلاث تحويلات تشفيرية يمكن تطبيقها طالما تم تأمين انتقال البيانات بين مستوى المستفيد ومستوى صنف المستفيد وهي:

أ - الإحلال (Substitution)

ب - التقليص (Reduction)

ت - التوسع (Expansion)



شكل (١١)

تطبيقات التحويل التشفيري بين مستويات قاعدة البيانات DB المتجاورة

يمكن استخدام التحويلات الثلاث السابقة المستخدمة بين مستوى المستفيد ومستوى صنف المستفيد أيضاً بين صنف المستفيد والمستويات المنطقية. و أما التحويلات بين المستوى المنطقي والمستوى الفيزيائي فهي:

أ – الإحلال (Substitution)

ب –الانتقال (Transposition)

ت –التقليص (Reduction)

ث –التوسع (Expansion)

ج –تشفير عنوان الوصول (Encipherment of Access Address):

وبذلك يمكن أن تخضع عناصر البيانات لنفس المستوى الفيزيائي للتشفير عدة مرات وكل التحويلات تحفظ هيكل البيانات بحيث يكون بالإمكان إدارة واسترجاع البيانات. وفي التشفير متعدد المستوى تكون ضمانة الحماية لقاعدة البيانات أكبر ولكن بنفس الوقت تزداد مخاطر تخريب البيانات وضياعها لذلك من الضروري العمل على تخزين نسخة احتياطية مطابقة لقاعدة البيانات، تخزن بهدف حماية قاعدة البيانات عند تعطل أو تدمير القاعدة الأصلية.

وعادة تخزن البيانات بصيغة النص الواضح وهذا يزيد من مخاطر الوصول من قبل الخصوم أو المستخدمين غير الشرعيين، وعادة يتم معالجة إدارة المفتاح وعمليات التشفير (التشفير وفتح الشفرة) من قبل نظام إدارة قاعدة البيانات (DBMS) وأفضل حل هو الحماية التشفيرية التي تتم فيها المعالجة من قبل مالكي البيانات المستقلين (Individual Owner of Data) حيث يجب أن يسلم المستفيد المفتاح التشفيري المناسب خلال إدخال البيانات في القاعدة وفي هذه الحالة يكون المستفيد هو المسؤول عن خزن المفتاح ويُستخدم المفتاح من قبل نظام إدارة قاعدة البيانات (DBMS) بطريقة تمنع التسرب أو الكشف أو التشويه.

٣. تهديدات قواعد البيانات:

يُستفاد من قواعد البيانات بإخراج التقارير الإحصائية باستخدام التساؤلات (Queries) وعندما تجيب قاعدة البيانات على تلك التساؤلات فإنها تستدعي محتويات السجلات المعنية في القاعدة وقد تكون بعض تلك السجلات سريةً، حيث تكون إجابات كل تساؤل محققة لمجموعة من الشروط، ولحماية السجلات السرية ينبغي تخصيص شروط التساؤل عليها، حيث تدعى الشروط المطبقة على السجلات السرية بفئة التساؤل أو فئة الاستفسار، وتوجد طرق متعددة لاستخراج المعلومات السرية من قاعدة البيانات ومنها:

أ – فئة تساؤل صغيرة

ب –فئة تساؤل كبيرة

ت –إضافة سجلات تمويهية (Dummy)

ث –اقتفاء الأثر (Tracking)

ج – استخدام المعادلات الآنية لتحليل الإجابات.

٤. تطبيق التشفير لحماية البيانات أثناء المعالجة:

يتم توفير الحماية بالتشفير أثناء المعالجة من قبل أنظمة تشغيل مصممة بشكل يناسب الإشراف على معالجة بيانات أي مستخدم. ومن مواصفات تلك الأنظمة وقف أي انسياب غير مخول بين مجموعتين من المستخدمين. وفي ظروف كثيرة كالتطبيقات المصرفية والتطبيقات الدفاعية والعسكرية يتوجب على المستخدم تطبيق التشفير أثناء المعالجة حيث يحتاج لحماية إضافية فبدلاً من أن يستخدم النص الواضح يختار تنفيذ معالجة برمجية للبيانات المدخلة وهي بصيغة النص المشفر.

ويتم تأمين البيانات بطرق مختلفة هي التحكم في الدخول والتحكم في تدفق البيانات والتحكم بمحاولات الاستنتاج والتشفير واستخدام هذه الطرق يقلل من تهديد البيانات ولكن لا يضمن منعها بالمطلق، حيث أن التحكم في الدخول يتم باستخدام كلمات المرور، والتحكم في تدفق البيانات يستخدم لمنع تسرب المعلومات، والتحكم في محاولات الاستنتاج يستخدم مع قواعد البيانات الإحصائية لمنع القراصنة من تنفيذ الاستفسار، واستنتاج بعضٍ من المعلومات السرية. ويستخدم التشفير عند توقع فشل طرق التحكم السابقة في توفير الحماية الأمنية التامة وتعتمد كفاءة التشفير على التوزيع الأمني لمفتاح الشفرة.

٥. الحماية الفيزيائية:

تتضمن الحماية الفيزيائية حماية جميع التجهيزات المادية اللازمة لتأمين الاتصال فيما بين أجهزة الحاسب وأهم ما يرى الباحث ذكره في هذا المجال:

أ. حماية الألياف الضوئية والأسلاك النحاسية حيث توضع في مواسير خاصة وتمدد تحت الأرض وتزود بغرف تفتيش توضع على مسافات تناسب عمليات الصيانة والإصلاح.

ب. حماية غرف التفتيش بتركيب أقفال للأغطية وحمايتها بحراسة دورية مع التصوير المرئي عند الضرورة.

ت. تزويد غرف الموزعات وغرف أجهزة الخادم التي تُعرف أيضاً بمراكز البيانات (Data Centers) بأقفال رقمية مع آلية لتسجيل الأفراد الداخلين والخارجين.

٢-١-١٧ الحماية الشاملة لشبكات الاتصال الحاسوبية:

يمكن تصور شبكة اتصال الحاسب الآلي كحاسب آلي واحد عملاق تتوزع مكوناته المادية على مساحات جغرافية مختلفة. والمكونات الأساسية لهذا الحاسب هي شبكات الاتصال التي تربط

أجهزة الخادم ببعضها من جهة وحاسبات المستفيدين مع أجهزة الخادم من جهة ثانية حيث تحتضن أجهزة الخادم قواعد البيانات ومواقع الويب وقوائم المستفيدين المخولين.

وفي هذه البيئة الواسعة المعقدة يتواجد الأصدقاء والخصوم ويتواجد المستخدمون الصالحون وآخرون غير صالحين ذوي نفوس ضعيفة ويسعون للقرصنة وممارسة الجريمة الإلكترونية وعلى مصممي الشبكات وواضعي حلول الحماية الأمنية أن يفترضوا دوماً إمكانية وصول الخصوم والقراصنة للبيانات المنقولة من خلال خطوط الاتصال أو الشبكات العامة كالإنترنت وبالتالي تطبيق التشفير المناسب، حيث يصعب حماية خطوط الاتصال التي تنتشر خارج أسوار المنشأة بالطرق التقليدية كالحراسة البشرية والأقفال والأبواب والأسوار ولذلك تكون طريقة الحماية بالتشفير هي الطريقة الأنسب.

١. **التشفير في شبكات الحاسب الآلي** (Cryptography in Computer Networks)

عند تطبيق التشفير بغرض حماية مكونات ومحتويات شبكة الاتصال يتم إبعاد الأنشطة غير الشرعية وبالتالي إبعاد الآثار والنتائج المحتملة من وجود المستخدمين غير الشرعيين.

أول ما استخدم التشفير كان يطبق لأغراض إخفاء النص الواضح بجعله غير قابل للقراءة ولكن تم تطوير استخدامه لأغراض أخرى فغدا يستخدم لأغراض كشف المعلومات غير الشرعية المدخلة، وكشف المعلومات المحذوفة وكشف المعلومات المعدلة. ويمكن استخدام طرق التشفير لحماية قنوات الانتقال (Transmission Channels) ومنها القنوات التي تربط المحطات الطرفية (Terminals) مع الحاسبات المضيفة (Host Computers) أو العُقد (Nodes) وقنوات ربط حاسبات المستفيدين المكتبية أو المحمولة مع أجهزة الخادم ومعدات شبكات الاتصال كالموجهات وجدران الحماية والبدالات. وتعتمد جودة الحماية الأمنية التي تستخدم طرق التشفير على سعة قناة الاتصال (Channel Capacity) .

إن من أهم المشكلات التي تنشأ عند تطبيق طرق التشفير في حماية شبكات الاتصال هي توزيع المفاتيح التشفيرية بين العُقد ودمج بروتوكولات التشفير في نظام إدارة شبكة الاتصال كمساعد في تنفيذ العمليات التشفيرية. [٨٧]

١ + **توزيع المفاتيح التشفيرية في الشبكات:** تتشكل قناة الاتصال من ارتباط حاسبين لمستفيدين A و B حيث يشكل الحاسبان شبكة، يرغب المستفيدان في حماية هذه الشبكة من

[٨٧] عوض حاج علي أحمد مرجع سابق ص٥٠

محاولات اعتداء الخصوم والمتطفلين. بافتراض أن الخصوم والمتطفلين يستطيعون الوصول إلى شبكة الاتصال بطرق مختلفة والتنصت على قناة الاتصال، فإن الحل الأمثل في هذه الحالة هو بناء درع حماية يأخذ في الحسبان جميع احتمالات الاعتداء الممكنة، باستخدام التشفير لمرات متعددة على مستويات مختلفة لتنظيم تدفق البيانات في قناة الاتصال. ومن أنواع الحماية التشفيرية لقناة الاتصال يمكن ذكر مايلي:

١ ـ ١ تشفير نهاية إلى نهاية (ربط محطة طرفية بأخرى): يضمن إبقاء المعلومات المتدفقة في قناة الاتصال بالشكل غير المقروء فيما بين النهايتين الطرفيتين. تعامل شبكة الاتصال الرابطة بين مستفيدين اثنين فقط كقناة اتصال مفردة ولا حاجة لمعالجة البيانات العائدة للمستفيدين الاثنين، ويمكن تطبيق هذا النوع عند الاستفادة المتبادلة بين موارد حاسب واحد مع آخر.

١ ـ ٢ تشفير محطة طرفية إلى حاسب مضيف: يمكن تطبيق هذا النوع عند استفادة محطة طرفية من موارد مختلفة موجودة في الحاسب المضيف بغرض حماية الملفات المستفاد منها في الحاسب المضيف والقابلة للمعالجة من قبل مستخدم المحطة الطرفية.

١ ـ ٣ تشفير حاسب مضيف إلى حاسب مضيف أو خادم إلى خادم .

وجميع طرق التشفير هذه تحتاج إلى مفاتيح وهذه المفاتيح تحتاج إلى التوزيع إلى المستفيدين المشتركين في قنوات الاتصال المشفرة. وتوجد وسائل مختلفة لتوزيع المفاتيح منها ما يعتمد على استخدام شبكة اتصال منفصلة تستخدم لتوزيع المفتاح فقط، ومنها ما يستخدم نفس شبكة الاتصال لغرض نقل البيانات والمفتاح بحيث تشفر المفاتيح وترسل إلى الأطراف المعنية بشكل نص مشفر باستخدام محطة طرفية إضافية.

ويتم تناقل المفاتيح سرياً بأن يقوم أحد المشتركين بتوليد المفتاح بطريقة عشوائية ثم إعطائه للطرف الثاني بطريقة آمنة كمقابلة الطرفين في غرفة (بدون نوافذ) وتسليم المفتاح أو إرسال المفتاح عن طريق مراسل موثوق ويمكن تمييز نوعين من المفاتيح الأول مفتاح تشفير المفتاح ويوزع إلى المشتركين بشكل سري. والثاني مفتاح تشفير البيانات وفيها يتم تشفير البيانات والنصوص المرسلة. و لما كان من الصعوبة بمكان إرسال مفاتيح التشفير فيزيائيا بسبب التأخير، فإنه يتم تجزئة المفتاح الواحد إلى عدة أجزاء وإرسال كل جزء في قناة اتصال مختلفة كاستخدام الهاتف لجزء والبريد الإلكتروني لجزء ثاني ورسائل SMS للجزء الثالث وإشارة راديو للجزء الآخر وهكذا. ويحتاج توزيع المفاتيح التشفيرية في الشبكات الكبيرة إلى تبادل المفاتيح بين كل زوج من المشتركين قبل البدء باستخدام قناة

الاتصال لتبادل البيانات والمعلومات وإن العدد الكلي لتبادلات المفتاح يحتاج في شبكة n فرد هو $n(n-1)/2$.[٨٨]

٢-١-١٨ الهيكل التنظيمي:

حيث أن شبكة اتصال الحاسب الآلي تربط مكونات المنشأة فإن الضرورة تقتضي من الباحث أن يقوم بوضع تصور لهيكل إداري يمثل الهيكل الإداري للمنشأة المفترضة ويستخدم لاحقا كنموذج تثبت فيه المسميات الوظيفية للموظفين لتحديد دور كل منهم فيما يخص الإجراءات اللازمة لحماية شبكة الاتصال الأمر الذي يمكن من فهم حركة المراسلات فيما بين الأقسام والإدارات المعنية. التي ستقوم عمليا بتنفيذ إجراءات حماية المعلومات المقترحة فيها، ولا بد للمؤسسة التي تستخدم تقنية الحاسب الآلي في تسيير أعمالها أن تراعي في هيكلها التنظيمي وجود إدارة بمسمى مركز تقنية المعلومات أو مركز التعليمي الالكتروني أو مركز الحاسب الآلي يأخذ الصفة التشغيلية لإجراءات وسياسات العمل.

في الواقع توجد خيارات أثناء تصميم الهيكل التنظيمي للمؤسسة تتمثل في كيفية التخصص في العمل، ومكان وضع السلطة، وإلى أي درجة يمكن وضع هيكل لا مركزي، وكيفية التنسيق بين التخصصات العمل وسلطات المسؤولين. ولذلك يتم بناء الهيكل التنظيمي للمؤسسة على مبادئ مختلفة منها مبدأ التدرج الذي يحدد العلاقات نحو الاتجاهات الأربعة اليمين واليسار والأعلى والأسفل ومنها التسلسل القيادي وقد يُبنى على أساس الوظائف.

ويأخذ الهيكل التنظيمي الشكل الهرمي حيث تتوسع السلطة والمسؤولية حسب التدرج في المستويات. ويتم تسمية المناصب في الهيكل التنظيمي حيث يوضح في دليل ملحق لكل منصب في التنظيم دور يناسبه من حقوق وواجبات، وامتيازات والتزامات تحدد سلوك من يقوم بهذا الدور بشكل رسمي.

يفيد الهيكل التنظيمي في توزيع النشاطات المحددة على أشخاص معينين وتحمل المسؤولية من كل عضو فيه والتنسيق بين هذه النشاطات بغرض الوصول لتحقيق الأهداف التي تصبو إليها المؤسسة من خلال رؤيتها الموضوعة مسبقاً.

ويعتمد تقسيم الوظائف والمهام في التنظيم على تقييم العمل التقني وبالتالي على تحليل الوظائف المختلفة في المؤسسة وتوفير الأشخاص المناسبين وهذا يدخل ضمن إطار تحليل الوظائف وتوظيف الموارد البشرية في المكان المناسب في إطار إستراتيجية المؤسسة الرامية لتحقيق أهداف المؤسسة ضمن برامج وسياسات وأهداف المؤسسة من جهة والتكاليف الاقتصادية والاجتماعية من جهة أخرى

[٨٨] عوض حاج علي أحمد ، مرجع سابق ص ص ٥٢-٥٥

العناصر المكونة للمؤسسة متعددة وبالتالي فان الهيكل الكلي هو في الحقيقة تركيب أمثل لمجموعة من الهياكل ومنها:

أ -الهيكل البشري و يحدد دور ومجال وعلاقات أعضاء المؤسسة.

ب الهيكل المادي و يحدد أمكنة وحدات المؤسسة وأمكنة التجهيزات داخل هذه الوحدات.

ت الهيكل القانوني الذي يحدد الشكل القانوني للمؤسسة، شركة أسهم، شركات قابضة أو فروع.

ث الهيكل المالي و يحدد مصدر رؤوس الأموال للمؤسسة وتوزيعها.

ولا بد لأي مؤسسة تعتمد في أعمالها على تقنية المعلومات أن تخصص مكاناً في هيكلها التنظيمي مخصص لتقنية المعلومات قد يأخذ مسميات مختلفة منها: إدارة التعليم الإلكتروني، مركز المعلومات، مركز تقنية المعلومات، إدارة الحاسب الآلي، إدارة. الحوسبة. وقد يكون المسمى مركز أو إدارة أو قسم أو وحدة حسب صغر وكبر المؤسسة.

ومن خلال زيارات الباحث الميدانية للمؤسسات التعليمية فإن بعض المؤسسات تُضمِّن وظائف تقنية المعلومات في مركز المعلومات والأخرى تضمن وظائف المعلومات في مركز تقنية المعلومات مضيقين المسافة بين مركز المعلومات ومركز تقنية المعلومات نظراً لصغر تلك المؤسسات و عدم أتمتة جميع أعمالها. وعلى كل حال فلا بد من إدراج أقسام متعددة تحت أي مسمى من المسميات السابقة (مركز، إدارة) وهي:

أ - قسم الشبكات: يختص بتمديدات شبكة المؤسسة من كابلات ضوئية أو نحاسية. بالإضافة لصيانة الشبكة دورياً وإصلاح المشكلات الفنية المتعلقة بالربط، ووضع الخطط اللازمة لتوسيع الشبكات أو تعديلها.

ب -قسم أمن المعلومات: يختص بوضع الخطط اللازمة لحماية الشبكة وإدارة برامج الحماية من الفيروسات وكذلك إدارة أجهزة الحماية وتفعيل خصائص الحماية في الموزعات والموجهات، بالإضافة لوضع الخطط اللازمة لتحديث وسائل الحماية، ووضع سياسات الحماية وتدقيق تنفيذها وكذلك وضع خطط الطوارئ واعتمادها من إدارة المؤسسة وتدريب المعنيين على تنفيذها.

ت -قسم الموقع الإلكتروني: يختص بإنشاء موقع إلكتروني للمؤسسة وجمع المعلومات المناسبة بالتنسيق مع جميع إدارات المؤسسة وإدخال تلك البيانات في الموقع بالإضافة لوضع الخطط اللازمة لتطوير الموقع وتنفيذها.

ث –قسم البريد الإلكتروني: يختص بإنشاء خادم للبريد الإلكتروني مخصص للمؤسسة وإنشاء حسابات بريد إلكترونية وتوزيعها على منسوبي المؤسسة وحثهم على استخدامها بالإضافة لوضع الخطط اللازمة لتحديث وتطوير نظام البريد الإلكتروني التابع للمؤسسة.

ج –قسم النظم الآلية: ويختص في تصميم وتطوير أنظمة آلية تحول سير الأعمال من طريقة تستخدم الأوراق إلى طريقة تستخدم المستندات الالكترونية من خلال البرمجيات وشبكة الحاسب الآلي وكذلك وضع الخطط اللازمة لتطوير برامج النظم الآلية لتلبية الاحتياجات الخاصة بأعمال المؤسسة.

ح –قسم التعليم الإلكتروني: ويختص بوضع حلول مناسبة للتعليم الإلكتروني وذلك ببناء موقع داخلي يؤمن التواصل بين المدرسين والطلاب ويتضمن مواد علمية تصلح للدخول عليها عبر الانترنت أو الشبكة الداخلية بحيث تقبل التفاعل بين الطلاب والأساتذة. ويضع الخطط اللازمة لتطوير حلول التعليم الإلكتروني بما يتناسب مع احتياجات المؤسسة.

خ –قسم التشغيل: ويختص في تشغيل أجهزة الخادم والأجهزة التي تساعد على إبقائها مستمرة بالعمل دون انقطاع مثل وحدات التغذية الكهربائية الاحتياطية وأجهزة النسخ الاحتياطي، وكل ما يلزم للمحافظة على المعلومات وصيانتها، وتنفيذ أوامر التشغيل حسب متطلبات العمل وقد يسمى هذا القسم قسم عمليات الحاسب.

د – قسم الصيانة والإصلاح أبرز مهامه إصلاح المشكلات الفنية لدى المستفيدين من خلال تلبية طلبات المساعدة التي ترد من قسم المساندة الفنية

ذ – قسم الجودة من أبرز مهامه وضع وتطوير معايير لإجراءات سير العمل في مركز المعلومات وتطوير عمليات التشغيل والسعي لتطبيق المعايير الدولية ذات العلاقة بمركز المعلومات وأهمها مركز البيانات (Data Center) وموقع الانترنت ومطابقة إجراءات العمل مع معايير دولية ذات علاقة بمراكز المعلومات وخصوصاً ما يتعلق بالحماية.

ر – قسم المساندة الفنية ويسمى أحيانا مكتب المساندة أو مكتب المساعدة أو الدعم الفني أو قسم دعم المستفيدين أو إدارة خدمات المستفيدين: ويختص بمساعدة منسوبي المؤسسة من موظفين وطلاب وباحثين ومراجعين الذين يستفيدون من خدمات تقنية المعلومات وتقديم الدعم الفني لهم.

ز – قسم البرامج التطبيقية: ويختص بتصميم وتنفيذ أعمال وبرامج المؤسسة عن طريق معالجتها آلياً وتطوير الأنظمة التي تلبي الاحتياجات المعلوماتية والإحصائية للمؤسسة.

س –قسم التدريب: ويختص في تدريب منسوبي مركز تقنية المعلومات ورفع كفاءات المتدربين منهم بما يتناسب مع التطور السريع في تقنية المعلومات، وإنشاء مسار تدريبي لكل تخصص من

تخصصات تقنية المعلومات وتخصيص ملف تدريبي لكل موظف في مركز تقنية المعلومات وترشيح الموظف للدورات وفقاً للمسار التدريبي لتخصصه. بالإضافة لتدريب جميع منسوبي المؤسسة بما يتناسب مع احتياجاتهم لاستخدام تقنية المعلومات من تعليم إلكتروني وبريد إلكتروني وكذلك استخدام الأنظمة الآلية ذات العلاقة.

٢ ـ ١٩ إجراءات أمن المعلومات:

حيث أن إجراء أمن المعلومات يكون سلسلة من العمليات مكتوبة ومعتمدة من قبل أعلى سلطة في المؤسسة، تُنفذ باستمرار بغرض المحافظة على أمن معلومات المنظمة. وأن الكفاءة تشير إلى أداء العمل المطلوب بأفضل طريقة بأقل التكاليف وهو من أهم مقاييس نجاح المؤسسات في تحقيق أهدافها. فإن الباحث تناول الهيكل التنظيمي لمراكز المعلومات، وتطرق إلى الوظائف المتداولة في أمن شبكات المعلومات، ليستطيع الربط بين الهيكل التنظيمي والوظائف ذات العلاقة بحماية موارد شبكة المعلومات، ومن ثم يستطيع قياس مدى كفاءة الإجراءات التي تنساب من خلال الهيكل التنظيمي.

١ -**وظائف تقنية المعلومات:** من أهم الوظائف التي ظهرت في مراكز تقنية المعلومات وتكون ضرورية لتنفيذ الإجراءات ما يلي:

أ - مسؤول نظم تشغيل الشبكة (Network Operating Systems Administrator).

ب -مسؤول النسخ الاحتياطي والاسترجاع (Backup and Disaster Recovery Administrator) .

ت -مسؤول أمن المعلومات (Information Security Officer) .

ث -مسؤول حماية نظم التشغيل (Security Operator) .

ج - أخصائي أمن معلومات (Security supervisor).

ح - مُراجِع سياسات الحماية (Security Policy Editor) .

خ - مسؤول إدارة نظم التشغيل (system admin).

د - مسؤول إدارة الشبكة (Network admin) .

ذ - مسؤول مساندة فنية (Technical support).

ر - ضابط أمن معلومات (security officer) .

ز - مدير قاعدة البيانات (DBA) .

س -مبرمج (Programmer).

ش -محلل نظم (System Analyst).

ص -مسؤول موقع (Web Master).

ض -مسؤول النسخ الاحتياطي (Backup Admin).

ط - منسق مشاريع.

ظ - أخصائي جودة.

ومن تلك الوظائف لا بد من تشكيل مجموعة من اللجان التي تختص بأداء أعمال تتصف بعلاقتها بأكثر من مجال واحد من مجالات تقنية المعلومات كالبرمجة والحماية والشبكات والتوثيق. وأهمها لجنة إدارة التعديل وهي لجنة تتكون من مجموعة من الأفراد يتم تشكيلها من قبل مدير إدارة تقنية المعلومات وتتكون من خبراء في الحماية والشبكات والبرمجة، ويكون من أهم أعمالها مراجعة أي تعديل في العمليات أو الإجراءات أو السياسات المتعلقة بالحماية وإضافات أجهزة وبرمجيات إلى الشبكة، ومن ثم توافق على التعديل أو تقترح تصحيحه أو ترفضه.

٢ -**أركان الإجراء:**

يتم توثيق الإجراء على شكل وثيقة نصية قد تكون صفحتين أو ثلاث وقد تمتد إلى عدد كبير من الصفحات بحسب طبيعة الإجراء وفي كل الأحوال تتضمن وثيقة الإجراء ما يلي:

أ. عنوان الإجراء واسم المؤسسة مالكة الإجراء ودرجة السرية وشعار المؤسسه.

ب. تصنيف البيانات من حيث درجة السرية.

ت. المؤلفون والمراجعون والمعتمدون للوثيقة.

ث. إصدارات الوثيقة مع بيان رقم الإصدار، من قام بالإصدار، مع بيان بالتعديلات.

ج. جدول المحتويات.

ح. وصف الإجراء (العملية).

خ. الغرض.

د. المجال.

ذ. معايير البدء.

ر. المدخلات.

ز. المسؤولين عن تنفيذ الإجراء.

س. مخطط الانسياب (شكل رسومي يوضح تسلسل الإجراء).

ش. شرح الإجراء.

ص. دلالات الرموز.

ض. المخرجات.

ط. الاعتماد/الموافقة.

ظ. معايير الانتهاء.

ع. السجلات/النماذج وتشمل: المراجع العلمية ،و المصطلحات الفنية .

غ. الملاحق.

ف. تحديث الوثيقة.

٣ -الإجراءات في مراكز تقنية المعلومات

من أهم الإجراءات في مراكز تقنية المعلومات الإجراءات التالية:

أ. إجراء إتلاف الأصول المعلوماتية(Information Assets) المنتهية الصلاحية.

ب. إجراء تركيب أو تطوير جهاز شبكة جديد (موزع أو موجه أو جدار حماية).

ت. إجراء إدارة تحديثات خادم قواعد البيانات.

ث. إجراء تثبيت التحديثات.

ج. إجراء تشغيل مضاد الفيروسات.

ح. إجراء تثبيت تحديثات أجهزة الحماية (جدران الحماية).

خ. إجراء تثبيت تحديثات أجهزة الشبكة (الموزعات والموجهات).

د. إجراء إعطاء صلاحيات لمستفيد جديد.

ذ. إجراء إعداد وتشغيل عمليات النسخ الاحتياطي والاسترجاع.

ر. إجراء عمليات التعديل في أجهزة وبرامج الحماية وقواعد البيانات.

ز. إجراء تسمية الأصول المعلوماتية (Information Assets) وتسجيلها على الوسائط المعلوماتية.

٢ + -٢ المخاطر التي تتعرض لها شبكات الحاسب:

تتعدد الأخطار التي يمكن أن تتعرض لها شبكات الحاسب الآلي منها ما يهدد البيانات خلال مرورها بالشبكات سواء في الكابلات أو الأثير أو أثناء نقل النسخ الاحتياطية ومنها يهدد فقدان البيانات أو تخريبها في أجهزة الخادم.[٨٩] وتكون نتائج التهديدات مختلفة كفقد البيانات المرسلة، ووصول البيانات إلى جهة أخرى،وحدوث خطأ أو تحريف في البيانات خلال انتقالها ويمكن تصنيف تلك المخاطر إلى تبعاً لمصدرها كما يلي:

[٨٩] حسن طاهر داود، الحاسب وأمن المعلومات، (الرياض: معهد الادارة العامة، ٢٠٠٠) ص٣٠٥

١ -مخاطر خارجية:

أ. التعدي على الكابلات وتخريبها.
ب. اندلاع الحريق.
ت. حصول إغراق بالمياه بسبب الفيضانات.
ث. اختراق لتعديل البيانات وتغيرها أو إتلافها.
ج. التعرض لهجوم إرهابي.

٢ -مخاطر داخلية:

أ. اختراق أجهزة الخادم من داخل المؤسسة (عبث،إساءة استخدام...).
ب. استخدام برامج بغرض التجسس من قبل المستفيدين من داخل المؤسسة.
ت. زيارة مواقع إنترنت غير موثوقة تسمح بتنزيل البرمجيات الضارة.
ث. الإصابة بفيروسات مصدرها الانترنت.
ج. الإصابة بفيروسات مصدرها وسائط التخزين وذواكر (الفلاش).
ح. تنزيل برامج غير مصرح بها.
خ. سرقة الأجهزة ووسائط التخزين.
د. الدخول غير المصرح إلى مركز البيانات وتعطيل عمل أجهزته.
ذ. تعديل إعدادات أجهزة الشبكة بطريقة يصعب تعقبها لإطالة فترة الانقطاع.

٣ -التدابير الوقائية (الاحتياطية) اللازمة لتجنب مخاطر الشبكات:

أ. توفير حراسة عند بوابات مركز البيانات على مدار الساعة.
ب. تجهيز مركز البيانات بحساسات الحرارة والحركة ونظام الإطفاء والإنذار.
ت. قفل مركز البيانات (غرفة أجهزة الخادم وأجهزة الشبكة) بحيث لا يدخلها إلا المتخصصون ممن لديهم ترخيص بالدخول.
ث. تجهيز مركز البيانات بآلية تسجيل للداخلين بالاسم والوقت وسبب الدخول.
ج. توفير مراقبة داخلية باستخدام كاميرات تلفزيونية مع التسجيل.
ح. تشغيل نظام للنسخ الاحتياطي والاسترجاع الآلي يومياً.

خ. وضع وسائط النسخ الاحتياطي في خزائن مضادة للصدمات والحريق.

د. تطبيق التشفير على وسائط النسخ الاحتياطي.

ذ. إبعاد وسائط النسخ لاحتياطي ووسائط التخزين عن أماكن تسرب المياه.

ر. إتلاف وسائط التخزين والنسخ الاحتياطي المنتهية الصلاحية.

ز. تركيب برامج مخصصة لمراقبة استخدام الشبكة.

س. توفير خطة طوارئ واضحة ومعتمدة واختبارها كل ثلاثة أشهر.

ش. إعداد خطة للتراجع (Rollback) تطبق في عند فشل خطة الطوارئ.

ص. توعية جميع الموظفين على أمن المعلومات كل حسب واجباته الوظيفية.

ض. اعتماد ميزانية خاصة بخطة الطوارئ.

ط. مطابقة إجراءات العمل لتتوافق مع معايير دولية (آيزو) تتعلق بالحماية.

ظ. عقد اتفاقيات تعاون مع المتخصصين في الحماية.

ع. تنفيذ اختبار دوري لنقاط الضعف انطلاقا من داخل وخارج الشبكة.

غ. تفعيل خصائص التشفير لقواعد البيانات.

ف. استخدام التشفير على اتصالات الشبكة الافتراضية (VPN).

ق. استخدام نظام لإدارة الأحداث (Logs) في جميع خوادم وأجهزة الشبكة.

ك. توفير مركز بيانات (Data Center) بديل لاستخدامه عند الطوارئ.

ل. تجهيز الوسيط (Proxy) بخدمة توليد التقارير وتحليلها.

م. توفير إجراءات مكتوبة ومعتمدة توضح ما يلزم لتنفيذ أعمال الحماية.

ن. توفير موظف واحد على الأقل يقوم بإدارة أجهزة الحماية وتحديثها.

ه. توفير موظف واحد على الأقل يقوم بإدارة برامج الحماية وتحديثها.

و. تأمين بديل واحد على الأقل لكل موظف يعمل في مجال الحماية.

ي. توظيف الأفراد المناسبين من حيث المؤهل والخبرة في أعمال الحماية.

أأ. توفير برنامج إدارة الحماية من جميع جوانبها.

بب. تأمين أجهزة احتياطية لجدار الحماية والموجه والوسيط و أجهزة الخادم.

تت. توفير إدارة خاصة بأمن المعلومات.

ثث. ربط إدارة أمن المعلومات مباشرة برئيس أو مدير المؤسسة.

جج. اشتراط توفر المهارات المناسبة لمستخدمي الحاسب الآلي.

حح. عقد دورات تدريب للتوعية في أمن المعلومات والحماية.

خخ. توفير خدمة الاتصال البعيد فقط للأفراد المعتمدين من الإدارة.

دد. توفير نظام لحماية البريد الالكتروني من الفيروسات والبريد الدعائي.

ذذ. تحديث نظام تشغيل أجهزة الشبكة بشكل دوري.

رر. إتاحة استخدام خاصية التحقق من الصحة في جدار الحماية.

زز. توفير سياسة خاصة بكلمات المرور وتطبيقها.

سس. توفير نظام لمراقبة حركة البيانات والتحكم بمنافذ الحاسبات ومشغلات الوسائط القابلة للإزالة.

شش. زيادة الاعتماد على أنظمة تشغيل أقل تأثرا بالفيروسات، وتقليل الاعتماد على أنظمة التشغيل الأكثر تأثرا بالفيروسات.

٤ معوقات الحماية:

توجد معوقات تساهم في صعوبة الوصول إلى حماية متكاملة منها ما يتعلق بالموارد البشرية ومنها يتعلق بالموارد المالية ومنها يتعلق بالتدريب وظهور تقنيات جديدة ويمكن تعداد أهمها كما يلي:

أ. ترك الموظفين المتخصصين بالحماية لوظائفهم بسبب الحصول على فرص أفضل.

ب. التدريب عالي التكلفة والحاجة إليه مستمرة وخصوصاً أن التقنيات المعلوماتية والبرامج تتجدد بصورة مستمرة وعلى البرامج التدريبية مواكبة ذلك التجدد وفي خضم هذه الدائرة تجد بعض المؤسسات صعوبة في صرف مبالغ كبيرة على الدورات التدريبية أو تحمل غياب موظفيها فترة حضور التدريب.

ت. ارتفاع تكلفة تراخيص البرمجيات وأنظمة التشغيل وسرعة إصدار نسخ جديدة تحتاج لتراخيص جديدة، مما يدعو بعض المؤسسات إلى تشغيل نسخ غير مرخصة.

ث. كثرة الفيروسات والبرمجيات الخبيثة وسرعة ظهور فيروسات جديدة وضرورة تحديث البرامج المضادة.

ج. صعوبة تطبيق السياسات بدون الدعم الإداري الواضح لعدم استيعاب التغيير السريع من قبل بعض الرؤساء القدامى في العمل.

ح. عدم وجود إدارة متخصصة في إدارة المخاطر وعدم توفر خطط طوارئ.

خ. ضعف الميزانيات المرصودة للتقنية المعلومات.

د. سرعة ظهور تقنيات جديدة وضرورة التوافق معها. وعدم اقتناع بعض إدارات المؤسسات بأهمية التواكب مع التقنية الحديثة ويظهر ذلك بمعارضة تخصيص الميزانيات الضرورية للتطوير.

ذ. عدم تثبيت تحديثات أنظمة تشغيل أجهزة الخادم والحاسبات المكتبية بانتظام و عدم تحديث أنظمة تشغيل جدران الحماية بانتظام.

ر. التكلفة العالية لجدران الحماية ذات الوظائف المتعددة (UTM) والتي توفر خاصية تصفية المواقع غير المرغوبة وخاصية الحماية من الفيروسات، وخاصية الحماية من البريد الدعائي (Spam) وخاصية كشف ومنع التلصص (IPS).

ز. عدم تحديث مكونات أجهزة الوسيط (Proxy) بانتظام.

س. قلة الكفاءة المهنية عند المستفيدين من موارد الشبكة.

ش. قلة الخبرة لدى العاملين بالحماية القادرين على إنشاء السياسات الأمنية وتدقيقها وتنفيذها.

ص. سرعة نمو البرامج ونظم التشغيل وازدياد حاجتها لسرعة معالجة أعلى وذاكرة أكبر الأمر الذي يتطلب تجديد الحاسبات الآلية وفي المؤسسات التعليمية تكون هوامش الربح غالباً بسيطة لا تسمح بتأمين أجهزة جديدة تتوافق مع البرمجيات الحديثة.

٥ تدابير حماية الشبكة والوقاية من الفيروسات والتغلب على نقاط الضعف:[٩٠]

أ. ينبغي اتخاذ تدابير عديدة لحماية أنظمة التشغيل والتطبيقات البرمجية من أخطار التعطل الناتجة عن الثغرات الأمنية والأخطاء التصنيعية بتثبيت التحديثات التصحيحية والأمنية التي تصدرها الشركات الصانعة وذلك بتخصيص بيئة مشابهة لبيئة الإنتاج لتجربة التحديثات قبل القيام بتثبيت تلك التحديثات في بيئة الإنتاج.

ب. تركيب جدران الحماية الحديثة ذات الوظائف المتعددة (UTM) على حدود الشبكات وإعداد تلك الجدران إعداداً يتناسب مع السياسات الأمنية المتبع في المؤسسة، وتحديثها بشكل مستمر.

ت. تركيب أنظمة الحماية من الفيروسات على بوابات البريد الإلكتروني وإعدادها الإعداد السليم وتحديثها بشكل مستمر.

ث. تدريب العاملين في الشبكات وحمايتها تدريباً متواصلاً من خلال مسار تدريب مخصص لكل موظف وبما يتناسب مع مهامه.

---

[٩٠] حسن طاهر داود، الحاسب وأمن المعلومات، مرجع سابق ، ص٣٢٥

ج. تخصيص خادم لتحديث نظم تشغيل الحاسبات المكتبية وأجهزة الخادم.

ح. تفعيل التحديث الآلي لجدران وبرامج الحماية.

خ. استخدام أدوات قياس أداء أجهزة الشبكة.

د. تزويد وتفعيل خاصية كشف ومنع الاختراق (IPS) و الحماية من الفيروسات وتصفية المواقع غير المرغوب فيها و الحماية من الفيروسات في جدران الحماية.

ذ. استخدام قائمة تتضمن المهام اليومية لأعمال الحماية (Check list) .

ر. تنفيذ اختبار دوري لكشف نقاط الضعف من داخل الشبكة ومن خارجها.

ز. مراجعة محاولات الدخول إلى النظام وخصوصا من داخل الشبكة.

س. تأمين عقود دعم فني لجدران الحماية وبرامج مضادات الفيروسات تجدد سنوياً.

ش. توفير نظام مخصص لمراقبة استخدام الإنترنت.

ص. توفير نظام احترافي للنسخ الاحتياطي وتشغيله بناء على سياسة نسخ احتياطي واسترجاع واضحة وموثقة.

ض. توفير مخطط واضح لجدران الحماية والخوادم والموجهات وتحديثه شهرياً.

ط. توفير نظام مخصص لمكافحة الفيروسات داخل الشبكة. وكذلك نظام مخصص لحماية البريد من الفيروسات والبريد الدعائي (Spams).

ظ. توفير نظام لإدارة تسجيلات الأحداث (Events /logs).

ع. توفير نظام متكامل مخصص لإدارة قضايا حماية الشبكة والحفاظ على أمنها من جميع الجوانب المادية والمنطقية.

غ. استخدام كلمة مرور بطول ٨ محارف على الأقل لحماية اتصالات (VPN).

ف. تحديث نظم تشغيل جدار الحماية والموجهات والموزعات والوسيط (Proxy) ونقاط الشبكة اللاسلكية كل ثلاثة أشهر على الأقل.

ق. إعداد لوائح التحكم بالوصول (access control list) في الموجهات (Routers).

ك. مراجعة تقارير استخدام الانترنت يومياً. و اتخاذ إجراء تأديبي لمن يسيء استخدام الانترنت.

ل. إعداد مفاتيح النقاط اللاسلكية بطول ٦٤ بت على الأقل.

م. إعداد الموزعات (Switches) لعزل حاسبات المتدربين عن موارد الشبكة.

ن. استخدام بيئة تطوير لبناء وتجربة التطبيقات الجديدة قبل نقلها إلى بيئة الإنتاج.

ه. إعداد نظم تشغيل الشبكة بحيث لا يتمكن المستخدمون داخل المؤسسة من تثبيت وإزالة أي برنامج في حاسباتهم المكتبية.

و. إعداد صلاحيات الوصول إعداد صلاحيات الوصول إلى موارد الشبكة حسب الاحتياج.

٢- الدراسات السابقة

٢-٢-١ المقدمة

من مراجعة الرسائل الجامعية والدوريات العلمية المحكمة في مكتبات كل من جامعة نايف العربية للعلوم الأمنية وكلية الملك فهد الأمنية وجامعة الملك سعود ومكتبة مركز الملك فيصل للبحوث والدراسات الإسلامية ومعهد الادارة العامة وقاعدة بيانات (Ebscohost) [٩١] على الانترنت، ومكتبة مدينة الملك عبدالعزيز للعلوم والتقنية، باستخدام أنظمة البحث الآلية في تلك المكتبات بالاضافة للدراسة في المواقع المتخصصة على شبكة الإنترنت التي تختص بأمن المعلومات وشبكات الحاسب الآلي تبين للباحث عدم وجود دراسة موضوعها حماية الشبكات من الاختراق والفيروسات والبرامج الضارة أو أجري على نفس مجتمع الدراسة ، وقد اختار الباحث دراسات ذات علاقة بموضوع الدراسة أو بجزء من أجزائه.

٢-٢-٢ الدراسات العربية

عرض الباحث ستة دراسات عربية وقد بدأ ببحوث أجريت (٢٠٠٧م) وانتهى ببحوث أجريت في عام (١٩٩٦م) كما يأتي:

١ -دراسة (عبد الرحيم، ١٤٢٨هـ/٢٠٠٧م):

دراسة مقدمة في ندوة "المجتمع والأمن " في دورتها الخامسة بعنوان "الجرائم الإلكترونية الملامح والأبعاد" بكلية الملك فهد الأمنية بالرياض وقد عرف فيها الأخطار والتهديدات التي تتعرض لها النظم المعلوماتية، وأعطى الحلول الواجب اتخاذها للتصدي لها وأكد أن التصدي للأخطار والتهديدات بمختلف أنواعها يشكل جزءاً من الأمن المعلوماتي وأشار إلى ضرورة وضع سياسة أمنية شاملة على مستوى المنظمة تأخذ بالاعتبار تحديد الاحتياجات الأمنية وفق المخاطر والتهديدات ـــ ووضع قواعد وإجراءات للعمل بها، ومراقبة الثغرات على مستوى النظم المعلوماتية ومواكبة عمليات تحديث وتعديل التطبيقات والتجهيزات المستخدمة، وأكد على أن السياسة الأمنية يجب أن تكون مبنية على التزام المستخدمين بالإجراءات والقواعد الأمنية، وعلى نظام أمني مادي ومنطقي يتلاءم مع احتياجات المنظمة والمستخدمين، وعلى إجراءات خاصة بإدارة عمليات تحديث البرمجيات والتطبيقات، وعلى استراتيجية واضحة تتعلق بعمليات حفظ وتخزين المعلومات، وعلى نظام مكتبي توثيقي يتم تحديثه باستمرار. ويتفق فيما أوصى به مع الباحث في توصيات هذه الدراسة، وأضاف الباحث في هذه الدراسة توصيات تخص ضرورة وجود هيكل تنظيمي واضح يتلاءم مع إجراءات

[٩١] مكتبة إلكترونية مخصصة للبحث العلمي على الموقع http://search.ebscohost.com

الحماية وكذلك وظائف تتناسب مع بيئة العمل المعلوماتية ووضع خطط طوارئ واضحة والتدرب المستمر على تنفيذها وقت الحاجة.

٢ -دراسة (عسيري ٢٠٠٤):

أجريت هذه الدراسة حول"الآثار الأمنية لاستخدامات الشباب للانترنت" وقد اتبعت الدراسة المنهج الوصفي و كان من أبرز توصياتها تدعيم البنية التحتية للانترنت وتدريب الشباب عليها. ووضع ضوابط لمقاهي الانترنت لتنظيم عملها، ورسم سياسات واضحة لأمن الانترنت والمعلومات في الوطن العربي ووضع خطط طوارئ لمواجهة الأزمات، وضرورة التكامل بين كافة القطاعات العامة والخاصة لضمان أمن الإنترنت. وحيث أن دراسة عسيري تقتصر على الآثار الأمنية لاستخدامات الانترنت من قبل الشباب فإنها تناولت الحماية من زاوية المستخدمين الشباب للإنترنت، و لم تتناول الحماية من زاوية كاملة (٣٦٠°) كما هو حال هذه الدراسة التي تناولت حماية الشبكات المحلية والموزعة من خلال حمايتها بالبرمجيات والأجهزة اعتماداً على سياسات أمنية وإجراءات عمل يقوم بها موظفون محترفون لهم مسميات وظيفية وواجبات واضحة في إطار هيكل تنظيمي واضح ومعتمد يتلاءم مع سير إجراءات العمل.

٣ -دراسة (العنزي، ٢٠٠٣):

أجريت هذه الدراسة حول جرائم نظم المعلومات وتوصلت الدراسة إلى أن حجم استخدام منفذ شبكة الانترنت وبرامج الاختراق الموجودة بها (٤.٢٥%) من مؤسسات عينة الدراسة كمنفذ خارجي أعلى من المنافذ الداخلية والخارجية الأخرى كإفشاء الرقم السري من قبل الموظفين (٤.١٦%) من مؤسسات عينة الدراسة، وبالنسبة لتكلفة جرائم نظم المعلومات توصلت الدراسة بأن جرائم نظم المعلومات تسببت لما نسبته (٤٢.٦%) من مؤسسات عينة الدراسة بخسائر مادية تبلغ أقل من (٥%) من نسبة إجمالي مصروفات المؤسسة. كما بأن ما نسبته (٤٢.٦%) من عينة الدراسة أكدوا بأن تكلفة جرائم نظم المعلومات في المؤسسات التي يعملون بها في عام ٢٠٠١ لا يتجاوز (٥%)، وما نسبته (١٤.٧%) منهم أكدوا أن تكلفتها من (١٠%) إلى أقل من (٣٠%)، وتوصلت الدراسة أيضاً إلى أن برامج الحماية تعد وسيلة ضبط وتحقيق هامة بشكل دائم، وتساعد بما نسبته (٩٤.٢%) في تحديد نوع الجريمة، وما نسبته (٩٥.١%) في تحديد توقيت ارتكاب الجريمة. وكشفت الدراسة عن أنه بالإمكان الاعتماد على عنوان (IP) بما نسبته (٩٤.٢%) وعلى برامج الحماية (٩١.٤%) ووسائل تتبع المخترقين (٧٤.٩%). وتبرز دراسة (العنزي) أهمية وسائل الحماية في ضبط الجريمة الإلكترونية وهي تتوافق مع دراسة الباحث عمار في دراسته هذه حماية الشبكات الرئيسة التي

أكدت على ضرورة تركيب برامج وأجهزة الحماية وإعدادها الإعداد المناسب والقيام بالتحديث المستمر لتقوم بصد جميع الهجمات وتسجيلها من خلال تفعيل خصائص تسجيل الأحداث وتسجيلها (Logs).

٤ -دراسة (الشهري ، ٢٠٠١):

أجريت هذه الدراسة حول "استخدامات الانترنت في مجال الإعلام الأمني العربي" وقد اتبعت المنهج الوصفي و استخلص الباحث من قراءة نتائج الدراسة الميدانية للمواقع العربية الأمنية على شبكة الانترنت توصيات أهمها تبادل الخبرات والاستشارات العلمية في مجالات توظيف الانترنت في حقل الإعلام. ورأى الباحث أن ميزة ومشكلة الانترنت أنها (وسيلة) تعليم وإعلام، وترفيه وتسوق، وهي بنفس الوقت (أداة) لجرائم محتملة مادية ومعنوية. ويكمن التحدي في أن الأمن (ضبط) والإنترنت (حرية)، وأوصت الدراسة بتشكيل لجنة متخصصة ممن يجمعون الخبرة الأمنية والإعلامية لمراجعة وتقديم المشورة والدعم للأجهزة الأمنية. وأوصت بتشجيع إنشاء جمعيات أصدقاء الشرطة، المرور، إلخ ومساعدتهم في إنشاء مواقع على الانترنت تهتم بالتوعية والتثقيف الأمني بشكل عام.[٩٢]

٥ -دراسة (عبدالحميد ، ٢٠٠١): [٩٣]

أجريت هذه الدراسة حول "البحث الجنائي المعاصر" وهو عنوان البحث، ومشكلة الدراسة تكمن في تطور الجريمة وظهور أشكال جديدة من الجريمة ترتكب بأساليب علمية وتقنية متقدمة. وجاء في الدراسة مكافحة الجريمة تتطلب الاعتماد على وسائل النقل السريعة وشبكات الاتصال السلكية واللاسلكية ذات الكفاءة العالية ونظم المعلومات المتطورة لمواجهة الجماعات المنظمة التي وصلت إلى درجة عالية من المهارة في استخدام المعلومات عن طريق الانترنت وشبكات الاتصال. ومن نتائج الدراسة تطوير أجهزة الشرطة وتدعيمها بالقدرات والكفاءات العلمية والوسائل التقنية المتاحة لمواجهة التحديات الأمنية، وتنمية العنصر البشري حتى يصبح قادراً على التعامل بفاعلية مع الجرائم المتطورة، والتعامل مع الأجهزة الحديثة، وتطوير مصادر الحصول على

[٩٢] دراسة فايز بن عبد الله الشهري ، **استخدامات شبكة الانترنت في مجال الإعلام الأمني العربي** ، مجلة البحوث الأمنية ، تصدر عن مركز الدراسات بكلية الملك فهد الأمنية ، الرياض، المجلد ١٠ العدد ١٩ نوفمبر ٢٠٠١

[٩٣] دراسة حسني بن درويش عبدالحميد ، **البحث الجنائي المعاصر (المعطيات والمتطلبات)**، مجلة البحوث الأمنية ، تصدر عن مركز الدراسات بكلية الملك فهد الأمنية ، الرياض، المجلد ١٠ العدد ١٩ نوفمبر ٢٠٠١

المعلومات بغرض إثراء الوقاية من الجريمة وإلى كشف غموضها وضبط مرتكبيها، كما أوصت الدراسة بتنمية أساليب الوقاية من الجريمة وزيادة فعاليتها للتعامل مع مشكلات الجريمة المتطورة.

٦ -دراسة (السحيباني، ١٩٩٦):

أجرى عبدالله بن محمد ناصر السحيباني عام ١٩٩٦م – جامعة نايف العربية للعلوم الأمنية بالرياض دراسة بعنوان "كفاءة الإجراءت الإدارية في المحافظة على أمن المعلومات" بإشراف الدكتور عبد الرحمن بن عبدالعزيز الشنيفي، وقد تناول في دراسته بشكل رئيس الإجراءات الإدارية المتعلقة بأمن المعلومات في المصارف من زوايا مختلفة ومنها إجراءات الدخول إلى المصرف وإجراءات التوظيف وإتلاف الوثائق والمطبوعات وإجراءات إدخال وإخراج الأجهزة المعلوماتية وإجراءات حماية النظام بعد انتهاء الدوام الرسمي والإجراءات المتخذة مع الموظف الذي يتم إنهاء خدماته، والإجراءات الإدارية والقانونية التي يجب أن تتخذ بحق الأفراد الذين يقومون بتسريب المعلومات. وتناول أيضاً تصميم برامج شبكة الاتصال والبرامج التطبيقية في المصارف. وأشار إلى أهمية وجود نظام أمني في المصرف ضد التسلل والسرقة والتخريب بالإضافة لأهمية وجود أنظمة للنسخ الاحتياطي وتجهيز مبنى المصرف ضد الكوارث والحريق. وأوصى (السحيباني) من خلال نتائج دراسته الكثير من التوصيات ومن أهمها ضرورة قيام المصارف التجارية بزيادة التركيز على استخدام الرقم السري لدخول المباني وغرف الحاسب الآلي، وإشعار العاملين بوجود مراقبة مستمرة عليهم، وصيانة أجهزة الحاسب الآلي داخل المصرف، وإجراء تجارب لاختبار طرق الاستجابة عند حدوث طارئ أو كارثة، وضرورة إصدار سياسات لأمن المعلومات، وضرورة توظيف متخصصين في أمن المعلومات، وضرورة اتخاذ إجراءات تأديبية صارمة بحق مسرّبي المعلومات ، وضرورة توعية منسوبي المصارف بأمن المعلومات والاطلاع على أحدث طرق المحافظة على أمن وسلامة المعلومات والاشتراك في الدوريات ذات العلاقة بأمن المعلومات. وتضيف هذه الدراسة على دراسة السحيباني تفصيل لإعدادات أجهزة وبرمجيات الحماية، وتتفق معها في جميع ما ورد فيها مع اختلاف عينة الدراسة.

٢-٢-٣ الدراسات الأجنبية:

١ -دراسة (علي سامان توسون Ali Saman Tosun ٢٠٠٣)، وهي دراسة بعنوان "Security Mechanisms for Multimedia Networking"، وتدور هذه الدراسة حول آليات حماية الوسائط المتعددة المتاحة على شبكات الحاسب الآلي، وقد أجريت في جامعة ولاية أوهايو وتناول فيها الباحث تحديات حماية تدفق بيانات

الفيديو باستخدام الوسيط (proxy)، وصعوبة معالجة الأحجام الكبيرة لبيانات أفلام الفيديو ، وتناول الهجمات النشطة على جريان حزم الفيديو وآليات حمايتها. وتحديات منع الهجمات النشطة وأداء ضغط بيانات الفيديو وآليات التشفير وأثرها على سرعة النقل ومن آليات حماية دوائر الفيديو عبر الانترنت. ومنها حماية نقل ملفات الفيديو باستخدام أجهزة الوسيط (Proxies) واستخدام التشفير من طرف إلى طرف (End to End) وتوفيق جودة النقل وسرعة التشفير وفك التشفير بالإضافة لآليات حماية نقل إشارات الفيديو لاسلكياً، وتوصل في توصياته إلى ضرورة استخدام التشفير في دوائر نقل الفيديو، وأوصى باستخدام أسلوب التحقق من صحة هوية المستخدم المدعوم بالتوقيع الرقمي في الاتصال بين نهايتين طرفيتين ، ومن توصيات هذه الدراسة تخفيض مستوى التشفير في دائرة نقل الفيديو لتجنب فقدان الحزم حيث أن فقدان أية حزمة تحتوي على بيانات تشفيرية يؤدي لفقدان البيانات المنقولة، وبخصوص تطبيقات ضغط البيانات المنقولة أوصى بتقسيمها إلى طبقيتين يتم تطبيق التشفير على أحدهما وتطبيق التحقق من صحة هوية المستخدم على الأخرى.

٢ -دراسة (عمارة ، ٢٠٠٧)[٩٤] قام شيخ فاروق عمارة بتقديم دراسة بعنوان " The Control of Firewalls using Active Networks" حول ضبط جدران الحماية باستخدام الشبكات النشطة وتتمحور حول مشكلة تغيير إعدادات أجهزة الشبكة (جدران الحماية والموجهات) المبنية على تصفية حزم البيانات بوضع برامج صغيرة مسبقة التعريف داخل تلك الأجهزة التي تمكِّن من تعديل أو إعادة توجيه حزم البيانات بفتح أو إغلاق المنافذ تبعاً لمحتوى الحزم باستخدام تقنيات الشبكة النشطة (Active Network) وهي من وجهة نظر الباحث ليست شبكات مادية تحمل (بتات) فقط بل إنها نموذج لأكثر من ذلك حيث يتم فيها معالجات عامة وهي طريقة (نوفل) للوصول إلى معمارية الشبكة حيث تنجز موزعات الشبكة معالجات مخصصة على الرسائل المارة من خلالها والتي تنجز تحكم من قبل المستفيد بمعالجات نقاط الشبكة كالموزع في شبكات اليوم. ومن توصياته التوجه نحو نموذج عام لبرمجة الشبكة يتمتع خصائص ذكية أهمها: خاصية التنقل وهي قابلية نقل البرامج وتشغيلها في مجال من منصات العمل، وخاصية الحماية وهي قابلية تقييد الموارد التي يمكن للبرامج أن تدخلها،

[٩٤] دراسة مقدمة في مؤتمر تقنية المعلومات والأمن الوطني في الرياض في ٢٠٠٧/١٢/١م.

وخاصية الفعالية وهي تمكين كل من خاصيتي التنقل والحماية من دون التأثير على أداء الشبكة.

٣ -دراسة (إدريس ، ٢٠٠٧)[٩٥]:

قام كل من "نور بك باشا إدريس" رئيس شركة سكان الماليزية المتخصصة بأمن المعلومات و"بحراني دهران شانموجان"، بتقديم دراسة بعنوان "Hybrid Intelligent Intrusion Detection" حول نظام هجين للكشف الذكي عن التجسس على شبكات الحاسب، وقد طرح الباحثان مشكلة عدم كفاية نظام كشف التجسس (IDS) [٩٦] لمنع التجسس على شبكات الحاسب الآلي كونها محدودة الإمكانات وتتركز قدرتها على المراقبة وتحتاج للتحديث اليومي لظهور بُرَيْمجات تجسس يومياً، وأكد الباحثان على ضرورة جمع وظائف أخرى لوظيفة المراقبة ومن أهم هذه الوظائف تحليل الأحداث وفحص البيانات المشفرة، واستخدام الشهادات الرقمية للهجمات المعروفة، واستخدام منطق الحلقات المتسلسلة (Fuzzy Logic) لوصف الصفات (Attributes) لتقليل كمية البيانات المعالجة ، ومن أهم توصيات دراستهما: ضرورة استخدام النظام الهجين (المركب) لأنه يساعد على كشف التلصص ومنعه أيضاً. واستخدام جهاز عالي الأداء من حيث المعالجة (Processing) للتوافق مع تشغيل الوظائف المتعددة التي يؤمنها النظام الهجين.

وتتوافق دراسة إدريس مع ما ذكر الباحث في دراسته هذه في أهمية جدران الحماية الذكية المعروفة بالاختصار (UTM)[٩٧] ، وتعني الإدارة الموحدة للتهديدات، وضرورة استخدامها على بوابات شبكات الحاسب الآلي، واختلفت دراسة إدريس عن هذه الدراسة في اقتصارها على جدران الحماية التي تستخدم نظام هجين وعدم تطرقها إلى نواحي الحماية الأخرى التي غطتها هذه الدراسة من منظور شامل لحماية شبكات الحاسب.

[٩٥] دراسة مقدمة في مؤتمر تقنية المعلومات والأمن الوطني في الرياض في ٢٠٠٧/١٢/١م.

[96] IDS: Intrusion Detection System

[97] UTM: Unified Threat Management

الفصل الثالث

(الإطار المنهجي للدراسة)

٣ ١ منهج الدراسة

٣ ٢ مجتمع وعينة الدراسة

٣ ٣ حدود الدراسة

٣ ٤ الاستبانة

٣ ٥ إجراءات تطبيق الدراسة

٣ ٦ الأساليب الإحصائية لمعالجة البيانات

الفصل الثالث

٣ ـ ١ منهج الدراسة

اعتمد الباحث في دراسته هذه على المنهج الوصفي الذي يناسب دراسة الظاهرة كما توجد في الواقع حيث أن الباحث وضع تساؤلات تكونت من خمسة محاور وكل محور من هذه المحاور يحاكي واقع الحماية في المؤسسات التعليمية والواقع المعرفي للعاملين في مجال الحماية بتلك المؤسسات، ويتميز المنهج الوصفي بوصف الظاهرة وصفاً دقيقاً ويعبر عنها تعبيراً كمياً أو كيفياً بالإضافة إلى تصنيف المعلومات بطريقة تساهم في ربط العلاقات بين المتغيرات المراد قياسها من خلال الدراسة.

٣ ـ ٢ حدود الدراسة

تهتم الدراسة بالحماية الأمنية لشبكات الحاسب الآلي العائدة للمؤسسات التعليمية الحكومية والخاصة الموجودة في مدينة الرياض بالمملكة العربية السعودية وفي الفترة من توزيع الاستبانة إلى وقت جمعها، وتبعاً لأهداف الدراسة والمجتمع الإحصائي المختار فإن الدراسة تتحدد بالحدود التالية:

١ ـ **الحدود الموضوعية:**

تقتصر الدراسة على موضوع محدد هو حماية الشبكات الرئيسة من الاختراق والفيروسات والبرامج الضارة.

٢ ـ **الحدود البشرية:**

تقتصر الدراسة على العاملين في شبكات الحاسب الآلي وحمايتها من حيث الإعداد والتحديث والتطوير. بالإضافة لمدراء أقسام أو مراكز تقنية المعلومات، في المؤسسات التعليمية.

٣ ـ **الحدود الزمنية:**

حدد المجال الزمني بفترة تطبيق الدراسة المسحية وهو الأشهر الستة الأخيرة من عام ٢٠٠٩م.

٤ ـ **الحدود المكانية:**

اقتصرت الدراسة على عينة عشوائية من المؤسسات التعليمية الموجودة في مدينة الرياض بالمملكة العربية السعودية.

٣ ٣ مجتمع وعينة الدراسة

استفاد الباحث من المنهج الوصفي بإجراء المسح الميداني لمجتمع الدراسة الذي تكون من مجموعة من المؤسسات التعليمية الخاصة والحكومية والمشتركة في مدينة الرياض عام ٢٠٠٩م وقد بلغ عدد المؤسسات التعليمية التي خضعت للبحث (٧٥) مؤسسة تعليمية أخذت كعينة عشوائية من أصل (٤٢٩) مؤسسة تعليمية في مدينة الرياض منها (٦٥) جامعة ومعهد [١]، والأخرى (٤٠٨) مدرسة[٢]. وقد تم اختيار المؤسسات التي تعتمد على تقنيات الحاسب الآلي في تسيير الكثير من أعمالها الأكاديمية والمالية معتمدة على برامج وأدوات تقنية المعلومات،وقد تم الاكتفاء بهذه العينة نظراً لكبر مجتمع الدراسة، وصعوبة الوصول إلى جميع المؤسسات التعليمية بسبب ضعف الإمكانات اللازمة للوصول إلى هذا العدد الكبير من المؤسسات المنتشرة على منطقة جغرافية واسعة في مدينة الرياض، ولصعوبة إقناع بعض المبحوثين بتعبئة الاستبانة حيث اعتذر الكثيرون منهم لأسباب تراوحت بين الانشغال وعدم وجود والوقت وبين سرية البيانات. وبلغ عدد أفراد العينة (١٠٥) فرداً، مكونين من مهندسين وإداريين وفنيين يعملون في إدارة وتشغيل أجهزة وبرمجيات حماية شبكات الحاسب الآلي في مراكز تقنية المعلومات الموجودة في المؤسسات التي خضعت للدراسة وقد اختلفت تسمية القسم المتخصص بتقنية المعلومات بين مركز المعلومات ومركز تقنية المعلومات وأحياناً الحاسب الآلي و أخذ في بعض المؤسسات اسم إدارة التعليم الإلكتروني، ويبدو للوهلة الأولى أن عدد أفراد عينة الدراسة قليل غير أن عدد المختصين في الشبكات والحماية في المؤسسة الواحدة لا يتجاوز اثنان في الغالب وفي معظم المؤسسات كان عدد المختصين بالحماية واحداً فقط وقليلة هي المؤسسات التي تجاوز فيها عددهم الاثنين.

٣ ٤ أداة الدراسة (الاستبانة):

اختار الباحث الاستبانة كأداة لقياس متغيرات الدراسة وذلك لمناسبتها لطبيعة الدراسة والمنهج الوصفي المستخدم فيها، بغرض تحقيق أهداف الدراسة والإجابة على تساؤلاتها واختار الاستبانة لأنها أكثر كفاءة في جمع أكبر قدر من البيانات من مجتمع متباعد من الصعب الوصول إلى أفراده بوقت قصير واختارها لأنها ذات تكلفة أقل وكونها أسهل من المقابلة، وقد صاغ الباحث الاستبانة في خمسة محاور بصورة تتناسب مع تساؤلات الدراسة كما هي في الملحق رقم (٣) ومرّ بناؤها بالمراحل التالية:

١. استفاد الباحث من مصادر البيانات من الكتب والمراجع والمقالات والدوريات العلمية والدراسات المشابهة لموضوع الدراسة وذلك في مرحلة

[١] دليل الصفحات الصفراء، شركة الاتصالات السعودية، الوحدة اكسبريس السعودية ش ذ.م.م الرياض٢٠٠٧-٢٠٠٨ ، ص ١٥٦
[٢] دليل الصفحات الصفراء، مرجع سابق ، ص ص ٤٠١-٤٠٨

إعداد الجانب النظري لتصميم أداة الدراسة، التي تمثلت بالاستبانة التي تم توزيعها على عينة البحث كأداة لجمع البيانات .

٢. بناء أداة الدراسة: تم تصميم الاستبانة في عباراتها الأولى بعد الرجوع إلى مصادر البيانات الأولية من الكتب والمراجع والدراسات العلمية والتي من خلالها تم إعداد المسودة الأولى للاستبانه المبينة في الملحق رقم (١) وكانت على النحو التالي :

أولاً : البيانات الشخصية والوظيفية لأفراد عينة الدراسة واشتملت على متغيرات الجنس، والوظيفة، والمؤهل العلمي، والتخصص، وسنوات الخبرة، والعمر، والشهادات الدولية التي نالها المبحوث، ونوع القطاع الذي تنتمي إليه المؤسسة التي يعمل فيها المبحوث، ومرحلة التعليم التي تعنى بها مؤسسة المبحوث، والنشاط العلمي الذي حضره المبحوث، وشهادات (الآيزو) التي نالتها المؤسسة التعليمية التي يعمل فيها المبحوث.

ثانياً : الأسئلة الخاصة بموضوع الدراسة واشتملت على المحاور التالية :

المحور الأول : ويشمل عدداً من العبارات حول الأجهزة والبرامج المستخدمة لحماية الشبكات للتعرف على مدى استخدام المؤسسة التعليمية لتلك الأجهزة والبرامج ومدى إعدادها وتحديثها ، وهي من العبارة رقم (١) إلى العبارة رقم (٤٧) كما وردت في الاستبانة تحت هذا العنوان.

المحور الثاني : ويشمل عدداً من العبارات حول درجة خطورة نقاط الضعف التي يمكن أن تُستغل لاختراق شبكات الحاسب الآلي، وكذلك درجة الأولوية للتدابير الوقائية الواجب اتخاذها للتخلص من نقاط الضعف، وهي من العبارة رقم (١) إلى العبارة رقم (٢٦) كما وردت في الاستبانة تحت هذا العنوان.

المحور الثالث: ويشمل عدداً من العبارات حول الهياكل التنظيمية لمراكز أو إدارات تقنية المعلومات في المؤسسات التعليمية ومدى توافقه مع الوظائف المتعلقة بأمن شبكة الحاسب الآلي. وهي من العبارة رقم (١) إلى العبارة رقم (٢٨) كما وردت في الاستبانة تحت عنوان.

المحور الرابع : ويشمل عدداً من العبارات حول إجراءات عمل حماية شبكات الحاسب الآلي، ومدى توفرها في المؤسسات التعليمية وكذلك مدى تطبيقها، وهي من العبارة رقم (١) إلى العبارة رقم (٢٦) .

المحور الخامس : ويشمل عدداً من العبارات حول المخاطر التي يمكن أن تؤثر سلباً على أمنية شبكات الحاسب الآلي وكذلك التدابير الاحتياطية اللازمة لتجنب تلك المخاطر، وبيان درجة أولوية تلك التدابير، وهي من العبارة رقم (١) إلى العبارة رقم (٥٩).

وقد تم صياغة عبارات المحاور الأول والثالث والرابع بإتاحة الفرصة للمبحوثين بالإجابة بواحد من ثلاث إجابات هي: نعم، إلى حد ما، لا. حيث (نعم) تعني موافق و(إلى حد ما) تعني موافق إلى حد ما و(لا) تعني غير موافق. وأعطيت الأوزان ٣ (نعم) ، ٢ (إلى حد ما ، ٣ (لا).
وتم صياغة عبارات المحورين الثاني والخامس بإتاحة الفرصة للمبحوثين بالإجابة وفقاً لمقياس خماسي لدرجة الخطورة حيث أعطيت الأوزان من (١) إلى (٥) حيث تبدأ بالرقم (١) الأقل خطورة وتنتهي بالرقم (٥) وهي الأعلى خطورة، وتعني ١ (عديم الخطورة) ، ٢ (قليل الخطورة) ، ٣ (متوسط الخطورة) ٤(خطِر) ، ٥ (خطِر جداً).
وكذلك درجة أولوية التدابير حيث أعطيت خمسة أوزان تبدأ بالرقم (١) الأقل أولوية وتنتهي بالرقم (٥) الأعلى أولوية. وتعني ١ (عديم الأولوية) ، ٢ (قليل الأولوية) ، ٣ (متوسط الأولوية) ٤(أولوية عالية) ، ٥ (الأولوية عالية جداً).

٣. الصدق الظاهري : عرضت الاستبانة على مجموعة من المحكمين وعددهم عشرة محكمين منهم المتخصص في مجال الحماية وأمن المعلومات وآخرون متخصصون في شبكات الحاسب الآلي ومنهم المتخصص في العلوم الإدارية وآخرون متخصصون في الإحصاء والبحث العلمي وقد تكرموا بإبداء ملاحظاتهم حول وضوح عبارات الاستبانة ومناسبة كل عبارة للمحور ومدى أهمية العبارة في كل محور حيث تم الأخذ بما اتفقت علية آراء المحكمين ومن ثم تم إعداد الاستبانة في صورتها النهائية المبينة في الملحق رقم (٣).

٤. الصدق البنائي وثبات أداة الدراسة: استكمالاً لإجراء صدق أداة الدراسة فقد طبقت الاستبانة على عينة استطلاعية قوامها (عشرة) أفراد من عينة الدراسة خلال فترتين متباعدتين وذلك للتأكد من مناسبة عبارات الاستبانة لعينة الدراسة والإطلاع على الآراء والمقترحات حول مدى وضوح محتوى الأداة، وتم حساب معامل ثبات أداة الدراسة للعينة (١٠٥) بمقياس كرونباخ

ألفـــا، وذلـــك باســـتخدام برنـــامج (SPSS) لمعالجـــة البيانـــات في الحاســـب الآلي. وقد أسفرت النتائج عن ما يلي:

أ - معامل ثبات عبارات المحور الأول

الجزء الأول من المحور الأول: الأجهزة والبرامج المستخدمة لحماية الشبكات والطـــرق المتبعة في إعدادها وتحديثها= 0.9317

الجزء الثاني من المحور الأول: مدى تطبيق الإعدادات والتحـــديثات اللازمـــة لأجهـــزة وبرامج الحماية = 0.8768

ب -معامل ثبات عبارات المحور الثاني:

الجزء الأول من المحور الثاني: نقاط الضعف التي يمكن أن تُستغل لاختـــراق شـــبكات الحاسب= 0.8184

الجزء الثاني من المحور الثاني: التدابير اللازمة لسد نقاط الضعف التي يمكـــن أن تُســـتغل لاختراق شبكات الحاسب= 0.9089

ت -معامل ثبات عبارات المحور الثالث: الهياكل التنظيمية المناسبة لمراكز تقنية المعلومات ومـــدى توافق الوظائف المستخدمة في مجال أمن شبكات المعلومات معها = 0.8665

ث -معامل ثبات عبارات المحور الرابع: إجراءات العمل في حماية شبكات المعلومـــات و مـــدى تطبيقها والعمل بها = 0.9121

ج -معامل ثبات عبارات المحور الخامس: المخاطر التي يمكن أن تؤثر سلباً على أمـــن شـــبكات الحاسب والتدابير الاحتياطية اللازمة لتجنبها، ودرجة خطورة المخاطر ودرجة الأولويـــة لاتخاذ التدابير الوقائية لتجنب تلك المخاطر.

الجزء الأول من المحور الخامس: المخاطر الخارجيـــة= 0.8260،المخـــاطر الداخليـــة= 0.8349

الجزء الثاني من المحور الخامس: تدابير الحماية مـــن المخـــاطر الداخليـــة والخارجيـــة= 0.9558

وبالرجوع إلى قيم معاملات الارتباط لجميع المحاور وجد الباحث أنهـــا تتـــراوح بـــين 0.8184 و 0.9558، وجميعها دالة إحصائياً عند مستوى ٠.١ ، وهي قيم مرتفعة تدل على قوة الارتباط بـــين العبارات والمحاور العائدة لها.

٣ ٥ إجراءات تطبيق أداة الدراسة:

بعد تأكد الباحث من الصدق الظاهري والبنائي ومن ثبات عبارات أداة الدراسة قام الباحث بإتمام الإجراءات التالية:

أ - تطبيق الدراسة وجمع البيانات الميدانية من خلال توزيع أداة الدراسة (الاستبانة) على العينة التي اختارها في مجتمع الدراسة وهو العاملون في حماية شبكات الحاسب الآلي في عينة عشوائية من المؤسسات التعليمية بالرياض، خلال الفترة من ٢٠٠٩/٧/١م إلى ٢٠٠٩/١٢/٣١م.

ب - توزيع أداة الدراسة على العينة التي شملت (٧٥) مؤسسة تعليمية من بينها مدارس كبيرة ومعاهد،وجامعات. وبلغ عدد الاستبانات الموزعة (٢٠٠) استبانة.

ت - استلام الاستبانات الموزعة على أفراد العينة حيث تم استعادة (١٣٠) استبانة وبلغت نسبة الاستبانات المعادة (٦٥%) من الاستبانات الموزعة، وبمراجعة الباحث للاستبانات المستعادة وتدقيقها تبين له وجود (٢٥) استبانة فيها إجابات غير مكتملة. وبذلك تكون الاستبانات التي خضعت للتحليل في هذه الدراسة (١٠٥) استبانة. وبنسبة (٥٣%) من أفراد العينة المختارة.

٣ ٦ أساليب المعالجة الإحصائية :

بعد حساب معامل ارتباط بيرسون لقياس الصدق البنائي وكذلك تحديد معامل ثبات الدراسة باستخدام معامل كرونباخ ألفا وبعد ذلك تم استخدام المقاييس الإحصائية التالية:

أ. التوزيعات التكرارية والنسب المئوية لوصف البيانات .

ب. المتوسط الحسابي الموزون، لعبارات المحاور الأول والثالث والرابع ذلك أن لكل عبارة ثلاثة مقاييس ، وهي من رقم (٣) إلى رقم (١) ، كما تم إيضاحها في الفقرة الخاصة بأداة الدراسة بحيث تقاس درجات المتوسط كما يلي:

المتوسط من (١) إلى أقل من (١.٦٧) يشير إلى غير موافق.

المتوسط من (١.٦٧) إلى أقل من (٢.٣٣) يشير إلى موافق إلى حد ما.

المتوسط من (٢.٣٣) إلى (٣) يشير إلى موافق.

ت. المتوسط الحسابي الموزون، لعبارات المحورين الثاني والخامس ذلك أن لكل عبارة خمسة مقاييس ، وهي من رقم (٥) إلى رقم (١) ، كما تم إيضاحها في الفقرة الخاصة بأداة

الدراسة. هذا يحدد مدى ارتفاع أو انخفاض استجابات المبحوثين لكل عبارة واردة بهذين المحورين بحيث تقاس درجات المتوسط كما يلي:

المتوسط من (١) إلى (١.٨٠) يشير إلى أن موضوع العبارة عديم الأهمية.

المتوسط من (١.٨١) إلى أقل من (٢.٦٠) يشير إلى أن موضوع العبارة قليل الأهمية.

المتوسط من (٢.٦١) إلى (٣.٤٠) يشير إلى أن موضوع العبارة متوسط الأهمية.

المتوسط من (٣.٤١) إلى (٤.٢٠) يشير إلى أن موضوع العبارة مهم.

المتوسط من (٤.٢١) إلى (٥) يشير إلى أن موضوع العبارة مهم جداً.

ث. الانحراف المعياري لتحديد مقدار التشتت في إجابات المبحوثين لكل عبارة عن المتوسط والذي يوضح مدى تشتت إجابات المبحوثين كما يفيد في ترتيب المتوسطات عند تساوي بعضها.

ج. معامل ارتباط بيرسون لتوضيح العلاقات بين متغيرات عناصر محاور الدراسة وذلك على النحو التالي :

الارتباط من + ١.٠٠ إلى يشير إلى + ٠.٧ يشير إلى أن الارتباط عالي.

الارتباط أقل من+ ٠.٧ إلى + ٠.٤ يشير إلى أن الارتباط متوسط.

الارتباط أقل من+ ٠.٤ يشير إلى أن الارتباط منخفض أو ضعيف .

ح. اختبار (ت) T-test للفرق بين متوسطين. واختبار LSD البُعدي للتعرف على مصادر الفروق الدالة إحصائياً وذلك بين المتغيرات التابعة والمتغيرات المستقلة.

٥. الصعوبات التي واجهت الباحث: واجه الباحث عدد من المشكلات خلال دراسته كان من أهمها:

أ. تطلب تحكيم الاستبانة زيارة عدد من الجامعات لمقابلة الأساتذة الأفاضل المتخصصين بموضوع الاستبانة واقتطاع قدر ثمين من أوقاتهم لإبداء رأيهم إزاء وضوح ومناسبة العبارات الواردة في محاور الاستبانة وقد صمم الباحث نموذج خاص للتحكيم كما في الملحق رقم (٢) وقد قام المحكمون مشكورين بتعبئته.

ب. توزيع الاستبانة وإعادتها استغرق وقت أكثر من اللازم بسبب توزع المؤسسات على مناطق متباعدة وانشغال المبحوثين وضيق وقتهم مما اضطر الباحث لزيارة معظمهم لأكثر من ثلاث مرات و أدى ذلك إلى أن تستغرق الدراسة وقت أكثر من الوقت المخصص.

ت. ضيق مجال العينة حيث أن عدد العاملين في مجال الحماية قليل مما قاد الباحث إلى زيارة عـــدد من المؤسسات يساوي تقريبا نصف أفراد العينة.

ث. عدم استجابة عدد من الموظفين المتخصصين بالحماية بدعوى الانشغال وضيق الوقت وسرية المعلومات.

ج. بعض المستجيبين لم يملؤوا الاستبانة على الوجه المطلوب، وقد استُبعدت اســـتباناتهم حيـــث ظهر تناقض في ملء البيانات، أو نقص في الحقول المطلوب تعبئتها.

ح. وجد الباحث صعوبة في الحصول على مراجع حديثة في موضـــوع الدراســـة وخصوصـــاً الدراسات السابقة التي تتناول نفس الموضوع.

الفصل الرابع

عرض وتحليل الدراسة الميدانية

٤-١ البيانات الديموغرافية (الأولية والشخصية) لعينة الدراسة

٤-٢ عرض وتحليل النتائج المتعلقة بأسئلة محاور الدراسة

٤-٣ الفروق والدلالات الإحصائية

الفصل الرابع
عرض نتائج الدراسة وتحليلها

يتناول الباحث في هذا الفصل عرض نتائج الدراسة وتحليلها وتفسيرها وذلك تحقيقاً لأهداف الدراسة في تحديد وسائل وإجراءات حماية شبكات الحاسب الآلي في المؤسسات التعليمية بمدينة الرياض بالمملكة العربية السعودية، حيث قام الباحث بتطبيق دراسته المسحية على العاملين في إدارة التشغيل والحماية لتلك الشبكات ، واستعراض نتائج البيانات الميدانية المدخلة بالحاسب الآلي من واقع الاستبيان الموزع على عينة المجتمع الإحصائي، وتطبيق أساليب التحليل الإحصائي عليها وتفسيرها بشكل مفصل بدءاً من خصائص عينة الدراسة مروراً بإفادات هذه العينة حول محاور الدراسة وانتهاء بعرض أهم الآراء التي وردت في إجابات أفراد عينة الدراسة حول الأجهزة والبرامج المستخدمة لحماية الشبكات ومدى إعدادها وتحديثها، و نقاط الضعف التي تُستغل لاختراق شبكات المعلومات والتدابير الوقائية المتخذة لمنع استغلالها، و الهياكل التنظيمية المناسبة لإدارات تقنية المعلومات وما مدى توافق الوظائف المستخدمة في مجال أمن شبكات المعلومات معها، وإجراءات العمل المعتمدة لحماية شبكات المعلومات و مدى إتباعها والعمل بها، والتدابير المتخذة لتجنب المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات المعلومات.

٤-١ البيانات الديموغرافية لعينة الدراسة:

اتصفت عينة الدراسة بعدد من السمات التي حددتها الخصائص الديموغرافية (الخصائص الشخصية) لأفرادها وتشمل: الجنس، العمر، الوظيفة، المؤهل العلمي، التخصص، عدد سنوات الخبرة، قطاع المؤسسة حكومي أو أهلي أو مشترك، مرحلة التعليم التي تختص بها المؤسسة، الدورات التدريبية، شهادات الآيزو. وتكمن أهمية هذه المتغيرات في تأثيرها على استجابات أفراد عينة الدراسة، وذلك من خلال الجداول وعرض النتائج المتعلقة بها والتي تتمثل في إجابات أفراد عينة الدراسة على الجزء الخاص بالبيانات الشخصية من الاستبانة على النحو التالي:

٤-١-١ توزيع عينة الدراسة وفقاً للجنس:

يوضح الجدول رقم (٤/١) أدناه توزيع عينة الدراسة وفقا للجنس

الجدول رقم (٤/١)

توزيع عينة الدراسة وفقا للجنس

الجنس	العدد	النسبة المئوية
ذكر	٩٠	%٨٥.٧١
أنثى	١٥	%١٤.٢٩
المجموع	١٠٥	%١٠٠

يوضح الجدول رقم (٤/١) توزيع عينة الدراسة وفقا لجنسهم حيث بلغت نسبة الذكور في عينة الدراسة ٨٥.٧١% وبلغت نسبة الإناث ١٤.٢٩% ويعود ذلك إلى أن غالبية المؤسسات التعليمية في الرياض تحوي أقسام مخصصة للذكور وأخرى مخصصة للإناث وتستفيد جميع تلك الأقسام من شبكة حاسب آلي واحدة تكون فيها مهام الحماية الرئيسة ملقاة على أقسام الذكور، هذا من جهة ومن جهة ثانية فإن زيارة الباحث للمؤسسات التي تختص بتعليم الذكور كانت أكبر لسهولة التواصل.

٤-١-٢ توزيع أفراد عينة الدراسة وفقا للعمر :

يوضح الجدول رقم (٤/٢) توزيع أفراد عينة الدراسة وفقا لأعمارهم

جدول رقم (٤/٢)

توزيع أفراد عينة الدراسة وفقا للعمر

العمر	العدد	النسبة المئوية
أقل من ٣٠ سنة	٤٤	%٤١.٩٠
من ٣٠ إلى أقل من ٤٠	٤٠	%٣٨.١٠
من ٤٠ سنة فأكثر	١٩	%١٨.١٠
لم سيتجيب	٢	%١.٩٠
المجموع	١٠٥	%١٠٠

أقل عمر = ٢٢ سنة ، أكبر عمر = ٧٠ سنة ، متوسط الأعمار = ٣٣.١٥ سنة ، الانحراف المعياري = ٩.٢١

ويتضح من الجدول رقم (٤/٢) أن المستجيبين الذين أعمارهم أقل من ٣٠ سنة تصل نسبتهم إلى ٤١.٩٠% ، وأن المستجيبين الذين أعمارهم من ٣٠ إلى أقل من ٤٠ سنة تصل نسبتهم إلى ٣٨.١٠ % . وأن الذين تبلغ أعمارهم ٤٠ سنة فأكثر تصل نسبتهم إلى ١٨.١٠ % . مما يشير الى أن العاملين في حقل حماية شبكات الحاسب الآلي وأمن المعلومات هم من الشباب وهذا أمر طبيعي جدا حيث أن تقنيات حماية شبكات الحاسب الآلي ظهرت في السنوات الخمس عشرة الأخيرة بعد دخول الإنترنت في المملكة العربية السعودية أواخر التسعينات من القرن الماضي . ولهذا فمن الطبيعي أن تجد أن نسبة العاملين في حماية شبكات الحاسب الآلي وأمن المعلومات هم من الشباب.

٤-١-٣ توزيع أفراد عينة الدراسة وفقاً للوظيفة:

يوضح الجدول رقم (٤/٣) توزيع أفراد عينة الدراسة وفقا لوظائفهم

جدول رقم (٤/٣)

توزيع أفراد عينة الدراسة وفقا للوظيفة

الوظيفة	العدد	النسبة المئوية
إدارية	١٠	%٩.٥٢
فنية	٤٩	%٤٦.٦٧
إدارية و فنية	٤٤	%٤١.٩٠
لم سيتجيب	٢	%١.٩٠
المجموع	١٠٥	%١٠٠

ويتضح من الجدول رقم (٤/٣) أن المستجيبين الذين يعملون بوظائف فنية وصلت نسبتهم إلى ٤٦.٦٧% ، وأن المستجيبين الذين يعملون بوظائف إدارية وفنية تصل نسبتهم إلى ٤١.٩٠% . وأن الذين يعملون بوظائف إدارية تصل نسبتهم إلى ٩.٥٢% مما يشير الى أن الوظائف الفنية في حقل حماية شبكات الحاسب الآلي وأمن المعلومات هي الأكثر احتياجاً (٤٦.٦٧%) تليها الوظائف الإدارية المشغولة من قبل أفراد لديهم مؤهلات فنية (٤١.٩٠%) وهذا أمر طبيعي جدا حيث أن تقنيات حماية شبكات الحاسب الآلي تتضمن تخصصات فنية متعددة وبذلك تكون وظائف الفنيين أكبر من وظائف الإداريين في مجال حماية شبكات الحاسب الآلي وأمن المعلومات.

٤-١-٤ توزيع أفراد عينة الدراسة وفقاً للمؤهل العلمي:

يوضح الجدول رقم (٤/٤) توزيع أفراد عينة الدراسة وفقا لمؤهلاتهم العلمية:

جدول رقم (٤/٤)

توزيع أفراد عينة الدراسة وفقا للمؤهل العلمي

المؤهل العلمي	العدد	النسبة المئوية
ثانوية عامة وما دون	٢	%١.٩٠
دبلوم سنتين بعد الثانوية	١٦	%١٥.٢٤
بكاروليوس	٧٠	%٦٦.٦٧
ماجستير	٨	%٧.٦٢
دكتوراه	٩	%٨.٥٧
المجموع	١٠٥	%١٠٠

ويتضح من الجدول رقم (٤/٤) أن المستجيبين الذين يحملون مؤهل الثانوية العامة وما دون وصلت نسبتهم إلى ١.٩٠% ، وأن المستجيبين الذين يحملون مؤهل دبلوم سنتين بعد الثانوية تصل نسبتهم إلى ١٥.٢٤% . وأن الذين يحملون مؤهل بكالوريوس تصل نسبتهم إلى ٦٦.٦٧% وأن الذين يحملون مؤهل ماجستير تصل نسبتهم إلى ٧.٦٢% وأن الذين يحملون مؤهل دكتوراه تصل نسبتهم ٨.٥٧% ويُلاحظ من هذه النسب أن حاملي شهادة البكاروليوس هم الأكثر وجوداً وحاملي شهادة الثانوية العامة هم الأقل وجوداً مع وجود نسبة معقولة من حاملي شهادتي الماجستير والدكتوراه ويرى الباحث أن هذه النسب متوافقة مع احتياج حقل حماية شبكات الحاسب الآلي وأمن المعلومات لمؤهلات عالية نظراً لأهميتها وصعوبة العمل بها من قبل غير المتخصصين.

٤-١-٥ توزيع أفراد عينة الدراسة وفقاً للتخصص:

يوضح الجدول رقم (٤/٥) توزيع أفراد عينة الدراسة وفقا لمؤهلاتهم العلمية:

جدول رقم(٤/٥)

توزيع أفراد عينة الدراسة تبعاً للتخصص

التخصص	العدد	النسبة المئوية
شبكات	٦١	%٥٨.١٠
برمجة	١٤	%١٣.٣٣
نظم معلومات إدارية	٢٦	%٢٤.٧٦
أخرى (تقنية معلومات)	٣	%٢.٨٦
لم سيتجيب	١	%٠.٩٥
المجموع	١٠٥	%١٠٠

ويتضح من الجدول رقم (٤/٥) أن المستجيبين من ذوي تخصص الشبكات بلغت نسبتهم إلى ٥٨.١٠% ، وأن المستجيبين من ذوي تخصص البرمجة وصلت نسبتهم إلى ١٣.٣٣% ، وأن المستجيبين من ذوي تخصص نظم المعلومات الإدارية وصلت نسبتهم إلى ٢٤.٧٦% ، وأن المستجيبين من ذوي تخصص تقنية المعلومات وصلت نسبتهم إلى ٢.٨٦%، ويُلاحظ من هذه النسب أن حاملي تخصص الشبكات هم الأكثر وجوداً تليها نسبة المتخصصين بنظم المعلومات الإدارية، و ذوي تخصص تقنية المعلومات هم الأقل وجوداً مع وجود نسبة معقولة من المتخصصين بالبرمجة، ويرى الباحث أن هذه النسب معقولة وتتناسب مع أحجام المؤسسات التعليمية حيث يتم تكليف المتخصصين بالبرمجة وتقنية المعلومات بالإشراف على مهام الحماية في المدارس والمعاهد صغيرة الحجم إضافة إلى مهامهم الرئيسة في البرمجة والدعم الفني، أما في الجامعات فتوكل مهام الحماية وأمن المعلومات لمتخصصين في الشبكات وهم النسبة الأكبر.

٤-١-٦ توزيع أفراد عينة الدراسة وفقاً لسنوات الخبرة:

ويوضح الجدول رقم (٤/٦) أدناه توزيع عينة الدراسة وفقا لسنوات الخبرة على الشكل التالي :

جدول رقم (٤/٦)

توزيع أفراد عينة الدراسة وفقا لسنوات الخبرة

سنوات الخبرة	العدد	النسبة المئوية
أقل من ٥ سنوات	٤٣	%٤٠.٩٥
من ٥ سنوات إلى أقل من ١٠ سنوات	٣٩	%٣٧.١٤
من ١٠ سنوات فأكثر	٢٣	%٢١.٩١
المجموع	١٠٥	%١٠٠

ويتضح من الجدول (٤/٦) أن نسبة فئة ذوي الخبرة من ١ إلى خمسة سنوات قد بلغت ٤٠.٩٥% ، ونسبة فئة الذين لديهم خبرة من خمسة سنوات إلى أقل من عشرة سنوات بلغت ٣٧.١٤% ، ونسبة فئة الذين لديهم خبرة عشر سنوات فأكثر بلغت ٢١.٩٢% . وإن هذه الاستجابات هي استجابات معقولة لأن سنوات الخبرة من ١- ٥ سنوات التي اتصفت بالنسبة الأكبر بين فئات الخبرة هي السنوات المتوافقة مع ظهور التقنيات الحديثة في مجال حماية شبكات الحاسب الآلي ودخولها إلى المؤسسات التعليمية في السنوات الخمسة الأخيرة.

٤-١-٧ توزيع أفراد عينة الدراسة وفقاً للقطاع الذي تنتمي إليه المؤسسة:

ويوضح الجدول رقم (٤/٧) أدناه توزيع عينة الدراسة وفقا للقطاع على الشكل التالي:

جدول رقم (٤/٧)

توزيع أفراد عينة الدراسة تبعاً للقطاع الذي تنتمي إليه المؤسسة

القطاع	العدد	النسبة المئوية
الحكومي	٣٧	%٣٥.٢٤
الأهلي	٥٤	%٥١.٤٣
المشترك	١٤	%١٣.٣٣
المجموع	١٠٥	%١٠٠

ويتضح من الجدول (٤/٧) أن نسبة فئة المؤسسات الأهلية بلغت ٥١.٤٣%، ونسبة فئة المؤسسات الحكومية بلغت ٣٥.٢٤%، ونسبة فئة المؤسسات ذات القطاع المشترك بلغت

١٣.٣٣%. ويُلاحظ من هذه النسب أن النسبة الأكبر هي المؤسسات التعليمية الأهلية وتليها نسبة المؤسسات التعليمية الحكومية والنسبة الأقل هي المؤسسات التعليمية المشتركة.

وإن هذه الاستجابات هي استجابات متوافقة مع بيئة التعليم في الرياض وتكثر المؤسسات التعليمية الأهلية، حيث تلقى الدعم والرعاية من الهيئات الحكومية المعنية بالتعليم.

٤-١-٨ توزيع أفراد عينة الدراسة وفقاً للمرحلة التعليمية التي تختص بها المؤسسة:

يوضح الجدول رقم (٤/٨) أدناه توزيع عينة الدراسة وفقا للمرحلة التعليمية التي تختص بها المؤسسة على الشكل التالي :

جدول رقم (٤/٨)

توزيع أفراد عينة الدراسة تبعاً للمرحلة التعليمية

المرحلة التعليمية	العدد	النسبة المئوية
ثانوية وما دون	٢٤	%٢٢.٨٦
معهد	٩	%٨.٥٧
جامعة	٤٨	%٤٥.٧١
مراحل مختلفة	٢٤	%٢٢.٨٦
المجموع	١٠٥	%١٠٠

ويتضح من الجدول (٤/٨) أن نسبة فئة المؤسسات التي تختص بمرحلة التعليم الثانوي وما دون بلغت ٢٢.٨٦% ، و نسبة فئة المعاهد التعليمية بلغت ٨.٥٧% ونسبة الجامعات بلغت ٤٥.٧١% ونسبة المؤسسات التي تختص بالمراحل المختلفة بلغت ٢٢.٨٦%. ويُلاحظ من هذه النسب أن النسبة الأكبر هي الجامعات وتليها نسبة الثانوية العامة والمراحل المختلفة وأقلها نسبة المعاهد. وإن هذه الاستجابات هي استجابات متوافقة مع العينة التي اختارها الباحث من عينة الدراسة بحيث تحقق شرط استخدام شبكات الحاسب الآلي وكانت الجامعات هي الأكثر توافقاً مع هذا الشرط تليها المدارس الثانوية كبيرة الحجم ومراكز التدريب التي تعنى بالمراحل التعليمية المختلفة وتليها المعاهد التعليمة.

٤-١-٩ توزيع أفراد عينة الدراسة وفقاً لحضور الدورات التدريبية:

يوضح الجدول رقم (٤/٩) أدناه توزيع أفراد عينة الدراسة وفقا للمرحلة التعليمية التي تختص بها المؤسسة على الشكل التالي :

جدول رقم(٤/٩)

توزيع أفراد عينة الدراسة تبعاً لحضور الدورات التدريبية

الدورة التدريبية	العدد	النسبة المئوية من أصل ١٠٥
التوعية في أمن المعلومات	٥٨	%٥٥.٢٤
برامج الحماية من الفيروسات	٤١	%٣٩.٠٥
جدران الحماية	٣٨	%٣٦.١٩
إدارة مراكز المعلومات	٣٤	%٣٢.٣٨
الأخطار المحتملة وخطط الطوارئ	٢٨	%٣٢.٣٨
مجموع الدورات	١٩٩	بدون مجموع للنسبة المئوية

ويتضح من الجدول (٤/٩) أن نسبة دورات التوعية في أمن المعلومات بلغت ٥٥.٢٤% ونسبة دورات برامج الحماية من الفيروسات بلغت ٣٩.٠٥% ونسبة دورات جدران الحماية بلغت ٣٦.١٩% ونسبة دورات إدارة مراكز المعلومات بلغت ٣٢.٣٨% ونسبة دورات الأخطار المحتملة وخطط الطوارئ بلغت ٣٢.٣٨%. وإن هذه الاستجابات هي استجابات متوافقة مع مهام أعمال الحماية في شبكات الحاسب الآلي ويُلاحظ أن دورات التوعية في أمن المعلومات هي الأكثر وذلك يعود إلى أهميتها واشتمالها على جميع الموظفين، تليها دورات برامج الحماية من الفيروسات، تليها دورات جدران الحماية، ثم دورات إدارة مراكز المعلومات، وكانت الجامعات هي الأكثر توافقاً مع هذا الشرط تليها دورات إدارة مراكز المعلومات ثم دورات الأخطار المحتملة وخطط الطوارئ ويعلل الباحث هذا التسلسل باحتياج المسؤولين عن أعمال الحماية حيث أن أعداد الفنيين المسؤولين عن الدعم الفني والتوعية هم الأكثر وجوداً يليهم عدد المسؤولين عن تشغيل برامج الحماية من الفيروسات يليهم أعداد المسؤولين عن إدارة جدران الحماية ويأتي بعدهم مدراء مراكز المعلومات وأقسام تقنية المعلومات ثم المسؤولين عن إعداد خطط الطوارئ.

٤-١-١٠ توزيع مؤسسات الدراسة وفقاً للتوافق مع شهادات (الآيزو):

يوضح الجدول رقم (٤/١٠) أدناه توزيع مؤسسات عينة الدراسة تبعاً للتوافق مع شهادات (الآيزو) على الشكل التالي :

جدول رقم (٤/١٠)

توزيع مؤسسات عينة الدراسة تبعاً للتوافق مع شهادات (الآيزو)

شهادات (الآيزو)	العدد	النسبة المئوية
المؤسسات التي نالت شهادات (آيزو)	٨	%٧.٦٢
المؤسسات التي لم تنل شهادات (آيزو)	٩٧	%٩٢.٣٨
مجموع أفراد العينة	١٠٥	%١٠٠

ويتضح من الجدول (٤/١٠) أن نسبة الأفراد الذين نالت مؤسساتهم شهادة في (الآيزو) ٧.٦٢% ونسبة الأفراد الذين لم تنل مؤسساتهم شهادة في (الآيزو) ٩٢.٣٨% . وإن هذه الاستجابات هي استجابات تتوافق مع وجود صعوبات إدارية ومالية وبشرية تعيق الوصول إلى مطابقة (الآيزو).

٤-٢ عرض وتحليل النتائج المتعلقة بأسئلة محاور الدراسة:

يتناول هذا الفصل عرض النتائج التي توصلت إليها الدراسة وتحليلها وتفسيرها، ويتضمن أيضاً خمسة محاور تضم كل واحدة منها تساؤلاً، ويتفرع من كل تساؤل مجموعة من عبارات تقوم هذه العبارات بقياس متغيرات المحاور الخمسة.

١. **تساؤل المحور الأول:** ما الأجهزة والبرامج المستخدمة لحماية الشبكات وما مدى استخدام تلك الأجهزة والبرامج ومدى إعدادها وتحديثها؟ وللحصول على النتائج المرجوة من هذا التساؤل قام الباحث بتقسيمه إلى جزأين:

الأول: ما الأجهزة والبرامج المستخدمة لحماية الشبكات؟ والثاني: ما مدى تطبيق الإعدادات والتحديثات اللازمة لأجهزة وبرامج الحماية ؟ حيث أن توفير الجهاز والبرنامج لا يكفي بل يجب إتباعه بإعداد سليم ومتابعة فنية و للإجابة على هذا التساؤل قام الباحث من خلال تحليل أداة الدراسة بحساب التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية ووضح الترتيب لعبارات المحور بجزأيه كالتالي:

الجزء الأول: ما الأجهزة والبرامج المستخدمة لحماية الشبكات والطرق المتبعة في إعدادها وتحديثها.

تفرع من هذا السؤال ٢٢ عبارة تقيس متغيرات توفر أجهزة الحماية، وللإجابة على هذا السؤال فقد تم تحليل استجابات أفراد عينة الدراسة وإيضاح ترتيبها حسب أهميتها وفق الجدول رقم (٤/١١) كما يلي:

جدول رقم (٤/١١)

استجابات أفراد عينة الدراسة إزاء الأجهزة والبرامج المستخدمة لحماية الشبكات

م	العبارة		الاستجابة			المتوسط	الانحراف المعياري	الترتيب حسب المتوسط
			لا	إلى حد ما	نعم	المجموع			
١	تستخدم مؤسستي واحد أو أكثر من جدران الحماية (FireWalls) عند بوابات الشبكة المحلية.	ك	١٧	١٤	٧٤	١٠٥	٢.٥٤	٠.٧٦	٦
		%	١٦.١٩	١٣.٣٣	٧٠.٤٨	%١٠٠			
٢	تتوفر في جدران الحماية التي تستخدمها مؤسستي منافذ كافية لتقسيم الشبكة إلى ثلاثة شبكات فرعية أو أكثر (داخلية و DMZ وخارجية).	ك	٢٦	٢٧	٥٢	١٠٥	٢.٢٥	٠.٨٣	١٥
		%	٢٤.٧٦	٢٥.٧٢	٤٩.٥٢	%١٠٠			
٣	جدران الحماية المستخدمة في مؤسستي تقبل التحديث الآلي.	ك	١٧	٢٨	٦٠	١٠٥	٢.٤١	٠.٧٦	٨
		%	١٦.١٩	٢٦.٦٧	٥٧.١٤	%١٠٠			
٤	تتوفر خاصية تصفية البريد الدعائي (Spam) في جداران الحماية المستخدمة.	ك	٢٨	٢٠	٥٧	١٠٥	٢.٢٨	٠.٨٦	١٤
		%	٢٦.٦٦	١٩.٠٥	٥٤.٢٩	%١٠٠			
٥	جدران الحماية المستخدمة في مؤسستي مزودة بخاصية كشف محاولات الاختراق (IDS) فقط.	ك	٥٧	٣٣	١٤	١٠٤	١.٥٩	٠.٧٢	٢٢
		%	٥٤.٢٩	٣١.٤٣	١٣.٣٣	%٩٩.٠٥			
٦	جدران الحماية المستخدمة في مؤسستي مزودة بخاصية كشف ومنع الاختراق (IPS) معاً.	ك	٢٩	٢٨	٤٨	١٠٥	٢.١٨	٠.٨٤	١٧
		%	٢٧.٦٢	٢٦.٦٧	٤٥.٧١	%١٠٠			
٧	جدران الحماية المستخدمة في مؤسستي مزودة بخاصية تصفية المواقع غير المرغوبة.	ك	٢٥	٢١	٥٩	١٠٥	٢.٣٢	٠.٨٤	١٠
		%	٢٣.٨١	٢٠.٠٠	٥٦.١٩	%١٠٠			
٨	تتوفر خاصية اتصال الشبكة الافتراضية VPN في معظم جدران الحماية المستخدمة.	ك	٤٠	٨	٥٧	١٠٥	٢.١٦	٠.٩٥	١٨
		%	٣٨.١٠	٧.٦١	٥٤.٢٩	%١٠٠			
٩	توفر إدارة مؤسستي عقد دعم فني لجدران الحماية يجدد سنويا من الشركة الصانعة.	ك	٣٢	٢٥	٤٨	١٠٥	٢.١٥	٠.٨٦	١٩
		%	٣٠.٤٨	٢٣.٨١	٤٥.٧١	%١٠٠			
١٠	يوجد في مؤسستي وسيط (proxy) لتوزيع خدمة الإنترنت على المستفيدين.	ك	٩	١٤	٨٢	١٠٥	٢.٧٠	٠.٦٢	١

		%	٨.٥٧	١٣.٣٣	٧٨.١٠	%١٠٠		
١١	يوجد نظام مخصص لمراقبة استخدام الإنترنت داخل مؤسستي.	ك	١٩	٣٤	٥٢	١٠٥	٢.٣١	٠.٧٦	١١
		%	١٨.١٠	٣٢.٣٨	٤٩.٥٢	%١٠٠		
١٢	في شبكة مؤسستي يوجد مبدل مركزي Core Switch واحد على الأقل.	ك	١٢	٢٣	٧٠	١٠٥	٢.٥٥	٠.٦٩	٥
		%	١١.٤٣	٢١.٩٠	٦٦.٦٧	%١٠٠		
١٣	توجد نقاط شبكة لاسلكية Access) (Points مثبتة داخل الشبكة المحلية.	ك	٨	١٨	٧٩	١٠٥	٢.٦٨	٠.٦١	٢
		%	٧.٦٢	١٧.١٤	٧٥.٢٤	%١٠٠		
١٤	تستخدم مؤسستي نظام احترافي للنسخ الاحتياطي.	ك	١٥	٣٦	٥٤	١٠٥	٢.٣٧	٠.٧٢	٩
		%	١٤.٢٩	٣٤.٢٩	٥١.٤٢	%١٠٠		
١٥	يوجد في مؤسستي مخطط واضح لجدران الحماية والخوادم والموجهات.	ك	٢٦	٢٣	٥٦	١٠٥	٢.٢٩	٠.٨٤	١٣
		%	٢٤.٧٦	٢١.٩٠	٥٣.٣٤	%١٠٠		
١٦	يوجد نظام مخصص لمكافحة الفيروسات داخل الشبكة.	ك	١٣	١٤	٧٨	١٠٥	٢.٦٢	٠.٧	٣
		%	١٢.٣٨	١٣.٣٣	٧٤.٢٩	%١٠٠		
١٧	يوجد نظام مخصص لحماية البريد من الفيروسات والبريد الدعائي (Spams).	ك	١٣	٢٤	٦٨	١٠٥	٢.٥٢	٠.٧١	٧
		%	١٢.٣٨	٢٢.٨٦	٦٤.٧٦	%١٠٠		
١٨	توفر مؤسستي عقد دعم فني لنظام الحماية من الفيروسات يجدد سنويا.	ك	٢٤	٢٤	٥٧	١٠٥	٢.٣١	٠.٨٢	١٢
		%	٢٢.٨٦	٢٢.٨٦	٥٤.٢٨	%١٠٠		
١٩	تستخدم مؤسستي موجه (Router) واحد على الأقل.	ك	١٠	٢٥	٦٩	١٠٥	٢.٥٧	٠.٦٦	٤
		%	٩.٥٢	٢٣.٨١	٦٥.٧١	%١٠٠		
٢٠	موقع مؤسستي على الإنترنت محتضن في شبكة المؤسسة.	ك	٥٠	١٩	٣٦	١٠٥	١.٨٧	٠.٩	٢٠
		%	٤٧.٦٢	١٨.١٠	٣٤.٢٨	%١٠٠		
٢١	توفر مؤسستي نظام لإدارة تسجيلات الأحداث (Events /logs).	ك	٢٣	٣٦	٤٦	١٠٥	٢.٢٢	٠.٧٨	١٦
		%	٢١.٩٠	٣٤.٢٩	٤٣.٨١	%١٠٠		
٢٢	توفر مؤسستي نظام متكامل مخصص لإدارة قضايا أمن المعلومات من جميع الجوانب.	ك	٥٣	٣٠	٢٢	١٠٥	١.٧٠	٠.٨	٢١
		%	٥٠.٤٨	٢٨.٥٧	٢٠.٩٥	%١٠٠		
المتوسط العام للجزء الأول من المحور الأول							٢.٢٩	٠.٥١	

يوضح الجدول رقم (٤/١١) الأجهزة والبرامج المستخدمة لحماية الشبكات ومدى استخدامها ويتضمن الجدول اثنان وعشرون عبارة توضح الأجهزة والبرامج التي تستخدمها المؤسسات عينة الدراسة وفقاً لاستجابات منسوبيها، ويُلاحظ أن المتوسط العام قد بلغ ٢.٢٩ بانحراف معياري ٠.٥١ وحيث أن الاستجابة (لا) أعطيت الوزن (١)، والاستجابة (إلى حد ما) أعطيت الوزن (٢)، و الاستجابة (نعم) أُعطيت الوزن (٣). وبناء على ذلك فإن المتوسطات التي تنتمي إلى المجال من ١ إلى ١.٦٧ تعني غير موافق، والمتوسطات التي تنتمي إلى المجال من ١.٦٧ إلى ٢.٣٣ تعني موافق إلى حد ما، والمتوسطات التي تنتمي إلى المجال من ٢.٣٣ إلى ٣ تعني موافق. من ذلك يُلاحظ أن المتوسط العام لجميع عبارات هذا الجدول تنتمي إلى المجال من١.٦٧ إلى ٢.٣٣ فهي تعني موافق إلى حد ما. ويُستنتج من ذلك أن أفراد عينة الدراسة يوافقون إلى حد ما على توفر الأجهزة والبرامج. ويمكن إبراز أهم النتائج في نقاط مرتبة حسب الأهمية كما يلي:

١ - توضح نسب العبارة التي جاءت في الترتيب رقم (١) وهي " يوجد في مؤسستي وسيط (proxy) لتوزيع خدمة الإنترنت على المستفيدين" أن (٧٠.٤٨%) من عينة الدراسة لديهم وسيط (بروكسي)، وقد حصلت تلك العبارة على متوسط حسابي (٢.٧٠)، وانحراف معياري (٠.٦٢).

٢ - توضح نسب العبارة التي جاءت في الترتيب رقم (٢) وهي " توجد نقاط شبكة لاسلكية (Access Points) مثبتة داخل الشبكة المحلية " أن (٧٥.٢٤%) من عينة الدراسة لديهم نقاط شبكة لاسلكية، وقد حصلت تلك العبارة على متوسط حسابي (٢.٦٨)، وانحراف معياري (٠.٦١).

٣ - توضح نسب العبارة التي جاءت في الترتيب رقم (٣) وهي " يوجد نظام مخصص لمكافحة الفيروسات داخل الشبكة" أن (٧٤.٢٩%) من عينة الدراسة لديهم نظام مخصص لمكافحة الفيروسات داخل الشبكة، وقد حصلت تلك العبارة على متوسط حسابي (٢.٦٢)، وانحراف معياري (٠.٧).

٤ - توضح نسب العبارة التي جاءت في الترتيب رقم (٤) وهي " تستخدم مؤسستي موجه (Router) واحد على الأقل." أن (٦٥.٧١%) من عينة الدراسة لديهم موجه (Router) واحد على الأقل ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٥٧)، وانحراف معياري (٠.٦٦).

٥ – توضح نسب العبارة التي جاءت في الترتيب رقم (٥) وهي " في شبكة مؤسستي يوجد مبدل مركزي Core Switch واحد على الأقل." أن (٦٦.٦٧%) من عينة الدراسة لديهم موزع شبكة مركزي، وقد حصلت تلك العبارة على متوسط حسابي (٢.٥٥)، وانحراف معياري (٠.٦٩).

٦ – توضح نسب العبارة التي جاءت في الترتيب رقم (٦) وهي " تستخدم مؤسستي واحد أو أكثر من جدران الحماية (FireWalls) عند بوابات الشبكة المحلية." أن (٧٠.٤٨%) من عينة الدراسة لديهم جدار حماية واحد على الأقل، وقد حصلت تلك العبارة على متوسط حسابي (٢.٥٤)، وانحراف معياري (٠.٧٦).

٧ – توضح نسب العبارة التي جاءت في الترتيب رقم (٧) وهي " يوجد نظام مخصص لحماية البريد من الفيروسات والبريد الدعائي (Spams)." أن (٦٤.٧٦%) من عينة الدراسة يوجد نظام مخصص لحماية البريد من الفيروسات والبريد الدعائي، وقد حصلت تلك العبارة على متوسط حسابي (٢.٥٢)، وانحراف معياري (٠.٧١).

٨ – توضح نسب العبارة التي جاءت في الترتيب رقم (٨) وهي " جدران الحماية المستخدمة في مؤسستي تقبل التحديث الآلي" أن (٥٧.١٤%) من عينة الدراسة يوجد جدران حماية تقبل التحديث الآلي ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٤١)، وانحراف معياري (٠.٧٦).

٩ – توضح نسب العبارة التي جاءت في الترتيب رقم (٩) وهي " تستخدم مؤسستي نظام احترافي للنسخ الاحتياطي. " أن (٥١.٤٢%) من عينة الدراسة يستخدمون نظام احترافي للنسخ الاحتياطي، وقد حصلت تلك العبارة على متوسط حسابي (٢.٣٧)، وانحراف معياري (٠.٧٢).

١٠ –توضح نسب العبارة التي جاءت في الترتيب رقم (١٠) وهي " جدران الحماية المستخدمة في مؤسستي مزودة بخاصية تصفية المواقع غير المرغوبة " أن (٥٦.١٩%) من عينة الدراسة يوجد لديهم جدران مزودة بخاصية تصفية المواقع غير المرغوبة، وقد حصلت تلك العبارة على متوسط حسابي (٢.٣٢)، وانحراف معياري (٠.٨٤).

١١ –توضح نسب العبارة التي جاءت في الترتيب رقم (١١) وهي " يوجد نظام مخصص لمراقبة استخدام الإنترنت داخل مؤسستي." أن (٤٩.٥٢%) من عينة الدراسة يوجد لديهم نظام

مخصص لمراقبة استخدام الإنترنت ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٣١)، وانحراف معياري (٠.٧٦).

١٢ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٢) وهي " توفر مؤسستي عقد دعم فني لنظام الحماية من الفيروسات يجدد سنويا " أن (٥٤.٢٨%) من عينة الدراسة يوفرون عقداً للدعم الفني خاص بنظام الحماية من الفيروسات ويجدد سنوياً، وقد حصلت تلك العبارة على متوسط حسابي (٢.٣١)، وانحراف معياري (٠.٨٢).

١٣ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٣) وهي " يوجد في مؤسستي مخطط واضح لجدران الحماية والخوادم والموجهات" أن (٥٣.٣٤%) من عينة الدراسة يوجد لديهم مخطط واضح لجدران الحماية والخوادم والموجهات ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٢٩)، وانحراف معياري (٠.٧٤).

١٤ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٤) وهي " تتوفر خاصية تصفية البريد الدعائي (Spam) في جداران الحماية المستخدمة " أن (٥٤.٢٩ %) من عينة الدراسة يوجد لديهم جدران حماية يتوفر فيها خاصية لتصفية البريد الدعائي، وقد حصلت تلك العبارة على متوسط حسابي (٢.٨٢)، وانحراف معياري (٠.٧٦).

١٥ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٥) وهي " تتوفر في جدران الحماية التي تستخدمها مؤسستي منافذ كافية لتقسيم الشبكة إلى ثلاثة شبكات فرعية أو أكثر (داخلية و DMZ وخارجية)" أن (٤٩.٥٢%) من عينة الدراسة يوجد لديهم جدران حماية فيها منافذ كافية لتقسيم الشبكة إلى ثلاثة شبكات فرعية على الأقل، وقد حصلت تلك العبارة على متوسط حسابي (٢.٢٥)، وانحراف معياري (٠.٨٣).

١٦ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٦) وهي " توفر مؤسستي نظام لإدارة تسجيلات الأحداث (Events /logs)" أن (٤٣.٨١%) من عينة الدراسة يوجد لديهم نظام لإدارة تسجيلات الأحداث ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٢٢)، وانحراف معياري (٠.٧٨).

١٧ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٧) وهي " جدران الحماية المستخدمة في مؤسستي مزودة بخاصية كشف ومنع الاختراق (IPS) معاً " أن (٤٥.٧١%) من عينة الدراسة يستخدمون جدران حماية مزودة بخاصيتي كشف ومنع الاختراق (IPS) بآن واحد ، وقد حصلت تلك العبارة على متوسط حسابي (٢.١٨)، وانحراف معياري (٠.٨٤).

١٨ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٨) وهي " تتوفر خاصية اتصال الشبكة الافتراضية VPN في معظم جدران الحماية المستخدمة " أن (٥٤.٢٩%) من عينة الدراسة يوجد لديهم جدران حماية تمتلك خاصية الاتصال الافتراضي VPN ، وقد حصلت تلك العبارة على متوسط حسابي (٢.١٧)، وانحراف معياري (٠.٩٥).

١٩ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٩) وهي " توفر إدارة مؤسستي عقد دعم فني لجدران الحماية يجدد سنويا من الشركة الصانعة " أن (٤٥.٧١%) من عينة الدراسة يوفرون عقداً للدعم الفني يخص جدران الحماية ويجدد سنوياً، وقد حصلت تلك العبارة على متوسط حسابي (٢.١٥)، وانحراف معياري (٠.٨٦).

٢٠ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢٠) وهي " موقع مؤسستي على الإنترنت محتضن في شبكة المؤسسة " أن (٣٤.٢٨ %) من عينة الدراسة يوجد لديهم موقع على الإنترنت ومحتضن في شبكة المؤسسة ، وقد حصلت تلك العبارة على متوسط حسابي (١.٨٧)، وانحراف معياري (٠.٩).

٢١ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢١) وهي " توفر مؤسستي نظام متكامل مخصص لإدارة قضايا أمن المعلومات من جميع الجوانب " أن (٢٠.٩٥ %) من عينة الدراسة يوجد لديهم نظام متكامل مخصص لإدارة قضايا أمن المعلومات من جميع الجوانب ، وقد حصلت تلك العبارة على متوسط حسابي (١.٧٠)، وانحراف معياري (٠.٨٠).

٢٢ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢٢) وهي " جدران الحماية المستخدمة في مؤسستي مزودة بخاصية كشف محاولات الاختراق (IDS) فقط " أن جدران الحماية المستخدمة لدى (١٣.٣٣ %) من عينة الدراسة مزودة بخاصية كشف محاولات الاختراق (IDS) فقط ، وقد حصلت تلك العبارة على متوسط حسابي (١.٥٩)، وانحراف معياري (٠.٧٢).

الجزء الثاني: مدى تطبيق الإعدادات والتحديثات اللازمة لأجهزة وبرامج الحماية.

تفرع من هذا السؤال ٢٣ عبارة تقيس متغيرات الإعداد والتحديث وللإجابة على هذا السؤال فقد تم تحليل استجابات أفراد عينة الدراسة وإيضاح ترتيبها حسب أهميتها وفق الجدول رقم (٤/١٢) كما يلي:

جدول رقم (٤/١٢)

استجابات أفراد عينة الدراسة إزاء مدى تطبيق الإعدادات والتحديثات اللازمة لأجهزة وبرامج الحماية

م	العبارة		الاستجابة				المتوسط	الانحراف المعياري	الترتيب
			لا	إلى حد ما	نعم	المجموع			
٢٣	يتم تحديث مخطط الشبكة دورياً.	ك	٨	٥٣	٤٤	١٠٥	٢.٣٤	٠.٦٢	٢
		%	٧.٦٢	٥٠.٤٨	٤١.٩٠	%١٠٠			
٢٤	يتم تفعيل خاصية الحماية من البريد الدعائي Spam في جدار الحماية.	ك	٣٠	٢٩	٤٥	١٠٤	٢.١٤	٠.٨٤	٩
		%	٢٨.٥٧	٢٧.٦٢	٤٢.٨٦	%٩٩.٠٥			
٢٥	يتم تحديث خاصية الحماية من الفيروسات في جدار الحماية بشكل آلي.	ك	٢٣	٣٢	٥٠	١٠٥	٢.٢٦	٠.٨٠	٤
		%	٢١.٩٠	٣٠.٤٨	٤٧.٦٢	%١٠٠			
٢٦	يتم استخدام كلمة مرور بطول ٨ محارف على الأقل لحماية اتصالات (VPN).	ك	٣٣	٣٩	٣٣	١٠٥	٢.٠٠	٠.٨٠	١٤
		%	٣١.٣٤	٣٧.١٨	٣١.٤٨	%١٠٠			
٢٧	يتم تفعيل خاصية تصفية المواقع غير المرغوبة في جدران الحماية في مؤسستي.	ك	٢٦	٣٧	٤١	١٠٤	٢.١٤	٠.٧٩	٨
		%	٢٤.٧٦	٣٥.٢٤	٣٩.٠٥	%٩٩.٠٥			
٢٨	يتم تحديث نظام تشغيل جدار الحماية بشكل أسبوعي على الأقل.	ك	٣٥	٥٧	١٣	١٠٥	١.٧٩	٠.٦٥	٢٠
		%	٣٣.٣٣	٥٤.٢٩	١٢.٣٨	%١٠٠			
٢٩	يتم تحديث نظام تشغيل الموجهات (Router Image) بشكل شهري على الأقل.	ك	٣٣	٥٢	٢٠	١٠٥	١.٨٨	٠.٧٠	١٦
		%	٣١.٤	٤٩.١	١٩.٥	%١٠٠			
٣٠	يتم إعداد لوائح التحكم بالوصول (access control list) في الموجهات.	ك	٣١	٤٠	٣٤	١٠٥	٢.٠٣	٠.٧٩	١٢
		%	٢٩.٥٢	٣٨.١٠	٣٢.٣٨	%١٠٠			
٣١	يتم تحديث نظام تشغيل الوسيط (Proxy) بشكل أسبوعي على الأقل.	ك	٢٢	٦٠	٢٣	١٠٥	٢.٠١	٠.٦٦	١٣
		%	٢٠.٩٥	٥٧.١٥	٢١.٩٠	%١٠٠			

٣٢	يتم تثبيت التحديثات الأمنية للوسيط (proxy) بشكل أسبوعي على الأقل.	ك	٣٥	٥١	١٩	١٠٥	١.٨٥	٠.٧٠	١٩
		%	٣٣.٣٣	٤٨.٥٧	١٨.١٠	%١٠٠			
٣٣	يتم مراجعة تقارير استخدام الانترنت يومياً.	ك	٤٠	٥٢	١٣	١٠٥	١.٧٤	٠.٦٧	٢٢
		%	٣٨.١٠	٤٩.٥٢	١٢.٣٨	%١٠٠			
.٣٤	يتم إعداد نظام النسخ الاحتياطي لأخذ النُّسخ الاحتياطية بشكل يومي.	ك	٩	٥٩	٣٧	١٠٥	٢.٢٧	٠.٦١	٣
		%	٨.٦	٥٦.٢	٣٥.٢	%١٠٠			
.٣٥	يتم تحديث أنظمة تشغيل المبدلات المركزية ومبدلات التوزيع (Switch Image) دورياً.	ك	٣٩	٤٢	٢٤	١٠٥	١.٨٦	٠.٧٧	١٨
		%	٣٧.١٤	٤٠.٠٠	٢٢.٨٦	%١٠٠			
.٣٦	يتم تثبيت تحديثات أجهزة نقاط شبكة لاسلكية (Access Points) دورياً.	ك	٤٠	٤٩	١٦	١٠٥	١.٧٧	٠.٧٠	٢١
		%	٣٨.١٠	٤٦.٦٦	١٥.٢٤	%١٠٠			
.٣٧	يتم إعداد مفاتيح النقاط اللاسلكية بطول ٦٤ بت على الأقل.	ك	٣١	٥٠	٢٤	١٠٥	١.٩٣	٠.٧٢	١٥
		%	٢٩.٦٥	٤٧.٦٧	٢٢.٦٨	%١٠٠			
.٣٨	يتم إعداد مفاتيح النقاط اللاسلكية بطول ١٢٨ بت على الأقل	ك	٣٥	٤٨	٢٢	١٠٥	١.٨٨	٠.٧٣	١٧
		%	٣٣.٣٣	٤٥.٧٢	٢٠.٩٥	%١٠٠			
.٣٩	يتم في مؤسستي إعداد المبدلات (Switches) لعزل حاسبات المتدربين عن موارد الشبكة.	ك	٩	٤٠	٥٦	١٠٥	٢.٤٥	٠.٦٥	١
		%	٨.٥٧	٣٨.١٠	٥٣.٣٣	%١٠٠			
.٤٠	تستخدم مؤسستي بيئة تجربة لتثبيت التحديثات قبل اعتمادها في بيئة الإنتاج.	ك	٢١	٤٥	٣٨	١٠٤	٢.١٦	٠.٧٤	٧
		%	٢٠.٠٠	٤٢.٨٦	٣٦.١٩	%٩٩.٠٥			
.٤١	تستخدم مؤسستي بيئة تطوير لبناء وتجربة التطبيقات الجديدة قبل نقلها إلى بيئة الإنتاج.	ك	٢٥	٤٣	٣٦	١٠٤	٢.١١	٠.٧٦	١٠
		%	٢٣.٨١	٤٠.٩٥	٣٤.٢٩	%٩٩.٠٥			
.٤٢	لا يستطيع المستخدمون بمؤسستي تثبيت وإزالة أي برنامج في حاسباتهم المكتبية.	ك	٣٣	٣٦	٣٦	١٠٥	٢.٠٣	٠.٨١	١١
		%	٣١.٤٢	٣٤.٢٩	٣٤.٢٩	%١٠٠			
.٤٣	لا يستطيع مستخدمو	ك	٢٤	٣٨	٤٣	١٠٥	٢.١٨	٠.٧٨	٥

	حاسبات المعامل الوصول إلى موارد شبكة المؤسسة.	%	٢٢.٨٦	٣٦.١٩	٤٠.٩٥	%١٠٠		
.٤٤	لا يستطيع المبرمجون الدخول إلى جميع التطبيقات بصلاحيات كاملة.	ك	٢٨	٣١	٤٦	١٠٥	٢.١٧	٠.٨٣	٦
		%	٢٦.٦٧	٢٩.٥٢	٤٣.٨١	%١٠٠			
.٤٥	لا يستطيع مدير نظام تشغيل الشبكة الدخول إلى جميع موارد الشبكة بصلاحيات كاملة.	ك	٥٩	٢٤	٢٢	١٠٥	١.٦٥	٠.٨١	٢٣
		%	٥٦.٣٩	٢٢.٦٦	٢٠.٩٥	%١٠٠			
المتوسط العام للجزء الثاني منن المحور الأول							٢.٠٣	٠.٣٩	

يوضح الجدول رقم (٤/١٢) مدى تطبيق الإعدادات والتحديثات اللازمة لأجهزة وبرامج الحماية المتوفرة في عينة الدراسة ويتضمن الجدول ثلاث وعشرون عبارة توضح مدى تطبيق إعدادات الأجهزة والبرامج وتحديثها وفقاً لاستجابات أفراد عينة الدراسة، ويُلاحظ أن المتوسط العام قد بلغ ٢.٠٣ بانحراف معياري ٠.٣٩ وحيث أن الاستجابة (لا) أعطيت الوزن (١) ، والاستجابة (إلى حد ما) أعطيت الوزن (٢) ، و الاستجابة نعم أُعطيت (٣). وبناء على ذلك فإن المتوسطات التي تنتمي إلى المجال من ١ إلى ١.٦٧ تعني غير موافق، والمتوسطات التي تنتمي إلى المجال من ١.٦٧ إلى ٢.٣٣ تعني موافق إلى حد ما، والمتوسطات التي تنتمي إلى المجال من ٢.٣٣ إلى ٣ تعني موافق. من ذلك يُلاحظ أن المتوسط العام لجميع عبارات هذا الجدول تنتمي إلى المجال من١.٦٧ إلى ٢.٣٣ فهي تعني موافق إلى حد ما. ويُستنتج من ذلك أن أفراد عينة الدراسة يوافقون إلى حد ما على الإعدادات والتحديثات التي تتم على الأجهزة والبرامج المتوفرة. ويمكن إبراز أهم النتائج في نقاط مرتبة حسب الأهمية كما يلي:

١ – توضح نسب العبارة التي جاءت في الترتيب رقم (١) وهي " يتم في مؤسستي إعداد المبدلات (Switches) لعزل حاسبات المتدربين عن موارد الشبكة " أن (٣٣.٣٥%) من عينة الدراسة يقومون بإعداد المبدلات بحيث يتم عزل معامل التدريب عن الشبكة المحلية، وقد حصلت تلك العبارة على متوسط حسابي (٢.٤٥)، وانحراف معياري (٠.٦٥).

٢ – توضح نسب العبارة التي جاءت في الترتيب رقم (٢) وهي " يتم تحديث مخطط الشبكة دورياً " أن (٤١.٩٠%) من عينة الدراسة يقومون بتحديث مخطط الشبكة بشكل دوري، وقد حصلت تلك العبارة على متوسط حسابي (٢.٣٤)، وانحراف معياري (٠.٦٢).

٣ – توضح نسب العبارة التي جاءت في الترتيب رقم (٣) وهي " يتم إعداد نظام النسخ الاحتياطي لأخذ النُّسخ الاحتياطية بشكل يومي " أن (٣٥.٢%) من عينة الدراسة يقومون بإعداد نظام النسخ الاحتياطي بحيث يتم أخذ النُّسخ الاحتياطية بشكل يومي ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٢٧)، وانحراف معياري (٠.٦١).

٤ – توضح نسب العبارة التي جاءت في الترتيب رقم (٤) وهي " يتم تحديث خاصية الحماية من الفيروسات في جدار الحماية بشكل آلي " أن (٤٧.٦٢%) من عينة الدراسة يقومون بتحديث خاصية الحماية من الفيروسات في جدار الحماية بشكل آلي ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٢٦)، وانحراف معياري (٠.٨٠).

٥ – توضح نسب العبارة التي جاءت في الترتيب رقم (٥) وهي " لا يستطيع مستخدمو حاسبات المعامل الوصول إلى موارد شبكة المؤسسة " أن (٤٠.٩٥%) من عينة الدراسة يقومون بإعداد الشبكة بحيث لا يتمكن مستخدمو المعامل من الوصول إلى موارد شبكة المؤسسة، وقد حصلت تلك العبارة على متوسط حسابي (٢.١٨)، وانحراف معياري (٠.٧٨).

٦ – توضح نسب العبارة التي جاءت في الترتيب رقم (٦) وهي " لا يستطيع المبرمجون الدخول إلى جميع التطبيقات بصلاحيات كاملة " أن (٤٣.٨١%) من عينة الدراسة يقومون بإعداد الشبكة بحيث لا يتمكن المبرمجون من الدخول إلى جميع التطبيقات بصلاحيات كاملة، وقد حصلت تلك العبارة على متوسط حسابي (٢.١٧)، وانحراف معياري (٠.٨٣).

٧ – توضح نسب العبارة التي جاءت في الترتيب رقم (٧) وهي " تستخدم مؤسستي بيئة تجربة لتثبيت التحديثات قبل اعتمادها في بيئة الإنتاج " أن (٣٦.١٩%) من عينة الدراسة يقومون بتحديث مخطط الشبكة بشكل دوري ، وقد حصلت تلك العبارة على متوسط حسابي (٢.١٦)، وانحراف معياري (٠.٧٤).

٨ – توضح نسب العبارة التي جاءت في الترتيب رقم (٨) وهي " يتم تفعيل خاصية تصفية المواقع غير المرغوبة في جدران الحماية في مؤسستي " أن (٣٩.٠٥%) من عينة الدراسة يقومون بتفعيل خاصية تصفية المواقع غير المرغوبة في جدران الحماية في مؤسساتهم ، وقد حصلت تلك العبارة على متوسط حسابي (٢.١٤)، وانحراف معياري (٠.٧٩).

٩ – توضح نسب العبارة التي جاءت في الترتيب رقم (٩) وهي " يتم تفعيل خاصية الحماية من البريد الدعائي Spam في جدار الحماية " أن (٤٢.٨٦%) من عينة الدراسة يقومون بتفعيل

خاصية الحماية من البريد الدعائي Spam في جدار الحماية ، وقد حصلت تلك العبارة على متوسط حسابي (٢.١٤)، وانحراف معياري (٠.٨٤).

١٠ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٠) وهي " تستخدم مؤسستي بيئة تطوير لبناء وتجربة التطبيقات الجديدة قبل نقلها إلى بيئة الإنتاج " أن (٣٤.٢٩%) من عينة الدراسة يستخدمون في مؤسساتهم بيئة تطوير لبناء وتجربة التطبيقات الجديدة قبل نقلها إلى بيئة الإنتاج ، وقد حصلت تلك العبارة على متوسط حسابي (٢.١١)، وانحراف معياري (٠.٧٦).

١١ -توضح نسب العبارة التي جاءت في الترتيب رقم (١١) وهي " لا يستطيع المستخدمون بمؤسستي تثبيت وإزالة أي برنامج في حاسباتهم المكتبية " أن (٣٤.٢٩%) من عينة الدراسة يقومون بإعداد شبكاتهم بحيث لا يستطيع المستخدمون تثبيت وإزالة أي برنامج في حاسباتهم المكتبية ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٠٣)، وانحراف معياري (٠.٨١).

١٢ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٢) وهي " يتم إعداد لوائح التحكم بالوصول (access control list) في الموجهات " أن (٣٢.٣٨%) من عينة الدراسة يقومون بإعداد لوائح التحكم بالوصول (access control list) في الموجهات، وقد حصلت تلك العبارة على متوسط حسابي (٢.٠٣)، وانحراف معياري (٠.٧٩).

١٣ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٣) وهي " يتم تحديث نظام تشغيل الوسيط (Proxy) بشكل أسبوعي على الأقل " أن (٢١.٩٠%) من عينة الدراسة يقومون بتحديث نظام تشغيل الوسيط (Proxy) بشكل أسبوعي على الأقل، وقد حصلت تلك العبارة على متوسط حسابي (٢.٠١)، وانحراف معياري (٠.٦٦).

١٤ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٤) وهي " يتم استخدام كلمة مرور بطول ٨ محارف على الأقل لحماية اتصالات (VPN) " أن (٣١.٤٨%) من عينة الدراسة يقومون بتحديث مخطط الشبكة بشكل دوري ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٠٠)، وانحراف معياري (٠.٨٠).

١٥ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٥) وهي " يتم إعداد مفاتيح النقاط اللاسلكية بطول ٦٤ بت على الأقل " أن (٢٢.٦٨%) من عينة الدراسة يقومون بإعداد

مفاتيح النقاط اللاسلكية بطول ٦٤ بت على الأقل ، وقد حصلت تلك العبارة على متوسط حسابي (١.٦٣)، وانحراف معياري (٠.٧٢).

١٦ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٦) وهي " يتم تحديث نظام تشغيل الموجهات (Router Image) بشكل شهري على الأقل " أن (١٩.٥٠%) من عينة الدراسة يقومون بتحديث نظام تشغيل الموجهات (Router Image) بشكل شهري على الأقل ، وقد حصلت تلك العبارة على متوسط حسابي (١.٨٨)، وانحراف معياري (٠.٧٠).

١٧ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٧) وهي " يتم إعداد مفاتيح النقاط اللاسلكية بطول ١٢٨ بت على الأقل " أن (٢٠.٩٥%) من عينة الدراسة يقومون بإعداد مفاتيح النقاط اللاسلكية بطول ١٢٨ بت على الأقل ، وقد حصلت تلك العبارة على متوسط حسابي (١.٨٨)، وانحراف معياري (٠.٧٣).

١٨ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٨) وهي " يتم تحديث أنظمة تشغيل المبدلات المركزية ومبدلات التوزيع(Switch Image) دورياً " أن (٢٢.٨٦%) من عينة الدراسة يقومون بتحديث أنظمة تشغيل المبدلات المركزية ومبدلات التوزيع (Switch Image) دورياً ، وقد حصلت تلك العبارة على متوسط حسابي (١.٨٦)، وانحراف معياري (٠.٧٧).

١٩ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٩) وهي " يتم تثبيت التحديثات الأمنية للوسيط (proxy) بشكل أسبوعي على الأقل " أن (١٨.١٠%) من عينة الدراسة يقومون بتثبيت التحديثات الأمنية للوسيط (proxy) بشكل أسبوعي على الأقل ، وقد حصلت تلك العبارة على متوسط حسابي (١.٨٥)، وانحراف معياري (٠.٧٠).

٢٠ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢٠) وهي " يتم تحديث نظام تشغيل جدار الحماية بشكل أسبوعي على الأقل " أن (١٢.٣٨%) من عينة الدراسة يقومون بتحديث نظام تشغيل جدار الحماية بشكل أسبوعي على الأقل ، وقد حصلت تلك العبارة على متوسط حسابي (١.٧٩)، وانحراف معياري (٠.٦٥).

٢١ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢١) وهي " يتم تثبيت تحديثات أجهزة نقاط شبكة لاسلكية (Access Points) دورياً " أن (١٥.٢٤%) من عينة الدراسة

يقومون بتثبيت تحديثات أجهزة نقاط شبكة لاسلكية (Access Points) دورياً ، وقد حصلت تلك العبارة على متوسط حسابي (١.٧٧)، وانحراف معياري (٠.٧٠).

٢٢ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢٢) وهي " يتم مراجعة تقارير استخدام الانترنت يومياً " أن (١٢.٣٨%) من عينة الدراسة يقومون بمراجعة تقارير استخدام الانترنت يومياً ، وقد حصلت تلك العبارة على متوسط حسابي (١.٤٧)، وانحراف معياري (٠.٦٧).

٢٣ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢٣) وهي " لا يستطيع مدير نظام تشغيل الشبكة الدخول إلى جميع موارد الشبكة بصلاحيات كاملة " أن (٢٠.٩٥%) من عينة الدراسة يقومون بإعداد شبكاتهم بحديث لا يستطيع مدير نظام تشغيل الشبكة الدخول إلى جميع موارد الشبكة بصلاحيات كاملة ، وقد حصلت تلك العبارة على متوسط حسابي (١.٦٥)، وانحراف معياري (٠.٨١).

تساؤل المحور الثاني: ما درجة خطورة نقاط الضعف التي يمكن أن تُستغل لاختراق شبكة الحاسب وما درجات الأولوية للتدابير الوقائية؟

للحصول على النتائج المرجوة من هذا التساؤل قام الباحث بتقسيمه إلى جزأين:

الجزء الأول: ما نقاط الضعف التي يمكن أن تُستغل لاختراق شبكات الحاسب.

الجزء الثاني: ما التدابير اللازمة لسد نقاط الضعف التي يمكن أن تُستغل لاختراق شبكات الحاسب.

حيث أن نقاط الضعف لا تكفي بل يجب تنفيذ تدابير مناسبة لتلافي نقاط الضعف تلك.

الجزء الأول: ما درجة خطورة نقاط الضعف التي يمكن أن تُستغل لاختراق شبكات الحاسب.

للإجابة على هذا التساؤل قام الباحث من خلال تحليل أداة الدراسة بحساب التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية ووضح الترتيب لعبارات هذا الجزء كالتالي:

جدول رقم (٤/١٣)

استجابات أفراد عينة الدراسة إزاء درجة خطورة نقاط الضعف التي يمكن أن تُستغل لاختراق شبكات الحاسب

م	العبارة		الاستجابة					المتوسط	الانحراف المعياري	الترتيب
			درجة خطورة نقاط الضعف (١) أقل خطورة، (٥) أعلى خطورة				المجموع			
			(٥)	(٤)	(٣)	(٢)	(١)			
١.	عدم تثبيت تحديثات أنظمة تشغيل أجهزة الخادم والحاسبات المكتبية بانتظام.	ك	٥١	٣٨	١٦	–	–	١٠٥	٤.٣٣	٠.٧٣	٣
		%	٤٨.٥٧	٣٦.١٩	١٥.٢٤	–	–	%١٠٠			
٢.	عدم تحديث أنظمة تشغيل جدران الحماية بانتظام.	ك	٧٦	١٥	٧	٥	٢	١٠٥	٤.٥٠	٠.٩٥	١
		%	٧٢.٣٨	١٤.٢٩	٦.٦٧	٤.٧٦	١.٩٠	%١٠٠			
٣.	عدم تحديث خاصية تصفية المواقع غير المرغوبة في جدران الحماية بانتظام.	ك	١٥	٥٦	٢٩	٢	٣	١٠٥	٣.٧٤	٠.٨٣	١٢
		%	١٤.٢٩	٥٣.٣٣	٢٧.٦٢	١.٩٠	٢.٨٦	%١٠٠			
٤.	عدم تحديث خاصية الحماية من الفيروسات في جدران الحماية بانتظام.	ك	٤٩	٣٦	١٦	٤	–	١٠٥	٤.٢٤	٠.٨٥	٥
		%	٤٦.٦٦	٣٤.٢٩	١٥.٢٤	٣.٨١	–	%١٠٠			
٥.	عدم تحديث خاصية الحماية من البريد الدعائي Spam في جدران الحماية.	ك	٣٣	٣٦	٢٧	٧	٢	١٠٥	٣.٨٧	١.٠٠	١٠
		%	٣١.٤٣	٣٤.٢٩	٢٥.٧١	٦.٦٧	١.٩٠	%١٠٠			
٦.	عدم وجود خاصية كشف ومنع التلصص IPS في جدران الحماية المستخدمة.	ك	٥٤	١٨	٣٠	٢	١	١٠٥	٤.١٦	٠.٩٧	٦
		%	٥١.٤٣	١٧.١٤	٢٨.٥٧	١.٩١	٠.٩٥	%١٠٠			
٧.	عدم تحديث مكونات أجهزة الوسيط (Proxy) بانتظام.	ك	٣٥	١٧	٤٣	٢	٧	١٠٤	٣.٦٨	١.١٦	١٣
		%	٣٣.٣٣	١٦.١٩	٤٠.٩٥	١.٩٠	٦.٦٧	%٩٩			
٨.	وجود نظم تشغيل غير مرخصة تعمل في الشبكة.	ك	٥٨	٥	١٧	١٣	١٢	١٠٥	٣.٨٠	١.٤٩	١١
		%	٥٥.٢	٤.٨	١٦.٢	١٢.٤	١١.٤	%١٠٠			

٩.	قلة الكفاءة المهنية عند المستفيدين من موارد الشبكة.	ك	٤٣	٢١	٣٦	٣	٢	١٠٥	٣.٩٥	١.٠٢	٩
		%	٤٠.٩٥	٢٠.٠٠	٣٤.٢٩	٢.٨٦	١.٩٠	%١٠٠			
١٠.	قلة الخبرة لدى العاملين بالحماية.	ك	٥٧	٢٣	٢٢	٣	–	١٠٥	٤.٢٨	٠.٨٩	٤
		%	٥٤.٢٩	٢١.٩٠	٢٠.٩٥	٢.٨٦	–	%١٠٠			
١١.	وجود كلمات مرور افتراضية في بعض الأجهزة والبرمجيات العاملة بالشبكة.	ك	٤٤	٢٧	٢٤	٧	٣	١٠٥	٣.٨٧	١.٠٩	٨
		%	٤١.٩٠	٢٥.٧١	٢٢.٨٦	٦.٦٧	٢.٨٦	%١٠٠			
١٢.	عدم وجود سياسة للحماية.	ك	٦٦	٢١	١٨	–	–	١٠٥	٤.٨٦	٠.٧٧	٢
		%	٦٢.٨٦	٢٠.٠٠	١٧.١٤	–	–	%١٠٠			
١٣.	أداء بعض الأجهزة ضعيف ولا تستطيع تشغيل مكافح الفيروسات.	ك	٥٠	٢٦	٢٤	٣	٢	١٠٥	٤.١٣	٠.٩٩	٧
		%	٤٧.٦٢	٢٤.٧٦	٢٢.٨٦	٢.٨٦	١.٩٠	%١٠٠			
المتوسط العام للجزء الأول من المحور الثاني									٤.١٨	٠.٦٦	

يوضح الجدول رقم (٤/١٣) خطورة نقاط الضعف التي يمكن أن تُستغل لاختراق شبكات الحاسب ويتضمن الجدول ثلاث عشرة عبارة توضح درجة خطورة نقاط الضعف التي يمكن أن تُستغل لاختراق شبكات الحاسب الآلي وفقاً لاستجابات أفراد عينة الدراسة، يتضح من هذا الجدول أن قيمة المتوسط العام لهذا الجزء هي (٤.١٨) وانحرافه المعياري (٠.٦٦)، وحيث أن المقياس المستخدم خماسي وفيه (١) تعني موضوع العبارة عديم الخطورة و(٢) تعني قليل الخطورة و (٣) تعني متوسط الخطورة، و(٤) تعني خطر و(٥) تعني خطر جداً. وبناء على ذلك فإن المتوسطات التي تنتمي إلى المجال من (١) إلى (١.٨٠) تشير إلى عديم الخطورة، و المتوسطات التي تنتمي إلى المجال من (١.٨١) إلى أقل من (٢.٦٠) تشير إلى قليل الخطورة و المتوسطات التي تنتمي إلى المجال من (٢.٦١) إلى (٣.٤٠) تشير إلى متوسطة الخطورة، و المتوسطات التي تنتمي إلى المجال من (٣.٤١) إلى (٤.٢٠) تشير إلى خطر و المتوسطات التي تنتمي إلى المجال من (٤.٢١) إلى (٥) تشير إلى خطر جداً.

من ذلك يُلاحظ أن المتوسط العام لجميع عبارات هذا الجدول تنتمي إلى المجال من (٣.٤١) إلى (٤.٢٠) فهي تعني خطر. ويُستنتج من ذلك أن أفراد عينة الدراسة يوافقون على أن نقاط الضعف في شبكاتهم خطرة. ويمكن إبراز أهم النتائج في نقاط مرتبة حسب الأهمية كما يلي:

١ – بلغ متوسط العبارة التي جاءت في الترتيب رقم (١) وهي " عدم تحديث أنظمة تشغيل جدران الحماية بانتظام " (٤.٥٠) بانحراف معياري (٠.٩٥).

٢ – بلغ متوسط العبارة التي جاءت في الترتيب رقم (٢) وهي " عدم وجود سياسة للحماية " (٤.٨٦) بانحراف معياري (٠.٧٧).

٣ – بلغ متوسط العبارة التي جاءت في الترتيب رقم (٣) وهي " عدم تثبيت تحديثات أنظمة تشغيل أجهزة الخادم والحاسبات المكتبية بانتظام " (٤.٣٣) بانحراف معياري (٠.٧٣).

٤ – بلغ متوسط العبارة التي جاءت في الترتيب رقم (٤) وهي " قلة الخبرة لدى العاملين بالحماية " (٤.٢٨) بانحراف معياري (٠.٨٩).

٥ – بلغ متوسط العبارة التي جاءت في الترتيب رقم (٥) وهي " عدم تحديث خاصية الحماية من الفيروسات في جدران الحماية بانتظام " (٤.٢٤) بانحراف معياري (٠.٨٥).

٦ – بلغ متوسط العبارة التي جاءت في الترتيب رقم (٦) وهي " عدم وجود خاصية كشف ومنع التلصص IPS في جدران الحماية المستخدمة " (٤.١٦) بانحراف معياري (٠.٩٧).

٧ – بلغ متوسط العبارة التي جاءت في الترتيب رقم (٧) وهي " أداء بعض الأجهزة ضعيف ولا تستطيع تشغيل مكافح الفيروسات " (٤.١٣) بانحراف معياري (٠.٩٩).

٨ – بلغ متوسط العبارة التي جاءت في الترتيب رقم (٨) وهي " وجود كلمات مرور افتراضية في بعض الأجهزة والبرمجيات العاملة بالشبكة " (٣.٨٧) بانحراف معياري (١.٠٩).

٩ – بلغ متوسط العبارة التي جاءت في الترتيب رقم (٩) وهي " قلة الكفاءة المهنية عند المستفيدين من موارد الشبكة " (٣.٩٥) بانحراف معياري (١.٠٢).

١٠ –بلغ متوسط العبارة التي جاءت في الترتيب رقم (١٠) وهي " عدم تحديث خاصية الحماية من البريد الدعائي Spam في جدران الحماية " (٣.٨٧) بانحراف معياري (١.٠٠).

١١ –بلغ متوسط العبارة التي جاءت في الترتيب رقم (١١) وهي " وجود نظم تشغيل غير مرخصة تعمل في أجهزة الشبكة " (٣.٨٠) بانحراف معياري (١.٤٩).

١٢ –بلغ متوسط العبارة التي جاءت في الترتيب رقم (١٢) وهي " عدم تحديث خاصية تصفية المواقع غير المرغوبة في جدران الحماية بانتظام" (٣.٧٤) بانحراف معياري (٠.٨٣).

١٣ –بلغ متوسط العبارة التي جاءت في الترتيب رقم (١٣) وهي " عدم تحديث مكونات أجهزة الوسيط (Proxy) بانتظام " (٣.٦٨) بانحراف معياري (١.١٦).

الجزء الثاني: ما التدابير الوقائية المتخذة لتلافي نقاط الضعف؟

للإجابة على هذا التساؤل قام الباحث من خلال تحليل أداة الدراسة بحساب التكـــرارات والنســـب المئوية والمتوسطات الحسابية والانحرافات المعيارية ووضح الترتيب لعبارات هذا الجزء كالتالي:

جدول رقم (١٤/٤)

التدابير الوقائية المتخذة لتلافي نقاط الضعف

م	العبارة		الاستجابة						المتوسط	الانحراف المعياري	الترتيب
			درجة الأولوية لسد نقاط الضعف (١) أقل أولوية ، (٥) أعلى أولوية					المجموع			
			(٥)	(٤)	(٣)	(٢)	(١)				
١٤	تخصيص خادم لتحديث نظم تشغيل الحاسبات المكتبية وأجهزة الخادم.	ك	٥٩	٣٤	١٢	–	–	١٠٥	٤.٤٥	٠.٦٩	٣
		%	٥٦.٢	٣٢.٤	١١.٤	–	–	%١٠٠			
١٥	تفعيل التحديث الآلي لجدران الحماية.	ك	٦٨	٢٤	١٣	–	–	١٠٥	٤.٥٢	٠.٧١	٢
		%	٦٤.٨	٢٢.٨	١٢.٤	–	–	%١٠٠			
١٦	تفعيل التحديث الآلي لبرامج الحماية.	ك	٨٣	١٨	٤	–	–	١٠٥	٤.٧٥	٠.٥٢	١
		%	٧٩.٠	١٧.٢	٣.٨	–	–	%١٠٠			
١٧	استخدام أدوات قياس أداء أجهزة الشبكة.	ك	٣٣	٤٠	٢٦	٤	٢	١٠٥	٣.٩٣	٠.٩٤	٩
		%	٣١.٤	٣٨.١	٢٤.٨	٣.٨	١.٩	%١٠٠			
١٨	تزويد وتفعيل خاصية كشف ومنع الاختراق (IPS) في جدران الحماية.	ك	٦٨	٢١	٧	٩	–	١٠٥	٤.٣٨	٠.٩٢	٥
		%	٦٤.٨	١٢.٤	١٩.٠	٣.٨	–	%١٠٠			
١٩	تزويد وتفعيل خاصية الحماية من الفيروسات في جدران الحماية.	ك	٦٨	٢١	٧	٩	–	١٠٥	٤.٤١	٠.٩٥	٤
		%	٦٤.٧	٢٠.٠	٦.٧	٨.٦	–	%١٠٠			

٢٠	تزويد وتفعيل خاصية تصفية المواقع غير المرغوب فيها في جدران الحماية.	ك	٣٤	٣٢	٢١	١١	٧	١٠٥	٣.٧١	١.٢٢	١١
		%	٣٢.٣	٣٠.٥	٢٠.٠	١٠.٥	٦.٧	%١٠٠			
٢١	تزويد وتفعيل خاصية الحماية من البريد الدعائي (Spam) في جدار الحماية.	ك	٤٢	٣٢	١٥	٥	١١	١٠٥	٣.٨٥	١.٢٩	١٠
		%	٤٠.٠	٣٠.٥	١٤.٣	٤.٧	١٠.٥	%١٠٠			
٢٢	استخدام قائمة تتضمن المهام اليومية لأعمال الحماية (Check list) .	ك	٢٦	٢٧	٤٣	٨	١	١٠٥	٣.٦٦	٠.٩٧	١٢
		%	٢٤.٧	٢٥.٧	٤١.٠	٧.٦	١.٠	%١٠٠			
٢٣	تنفيذ اختبار دوري لكشف نقاط الضعف من داخل الشبكة.	ك	٤١	٣٢	٢٧	٢	٣	١٠٥	٤.٠١	٠.٩٩	٨
		%	٣٩.٠	٣٠.٥	٢٥.٧	١.٩	٢.٩	%١٠٠			
٢٤	تنفيذ اختبار دوري لكشف نقاط الضعف بدءا من خارج الشبكة.	ك	٥٤	٣٠	١٥	٥	١	١٠٥	٤.٢٥	٠.٩٤	٧
		%	٥١.٤	٢٨.٦	١٤.٣	٤.٧	١.٠	%١٠٠			
٢٥	مراجعة محاولات الدخول إلى النظام وخصوصا من داخل الشبكة.	ك	٥٥	٢٤	٢٤	٢	–	١٠٥	٤.٢٦	٠.٨٨	٦
		%	٥٢.٤	٢٢.٩	٢٢.٩	١.٨	–	%١٠٠			
	المتوسط العام للجزء الثاني من المحور الثاني								٤.٠٩	٠.٥٥	

يوضح الجدول رقم (٤/١٤) درجة الأولوية لسد نقاط الضعف بخمسة درجات حيث (١) تدل على أقل أولوية و (٥) تدل أعلى أولوية ويتضمن الجدول اثنا عشرة عبارة توضح درجة الأولوية لسد نقاط الضعف وفقاً لاستجابات أفراد عينة الدراسة،

وحيث أن المقياس المستخدم خماسي وفيه (١) تعني موضوع العبارة عديم الأولوية و(٢) تعني قليل الأولوية و (٣) تعني متوسط الأولوية، و(٤) تعني أولوية عالية و(٥) تعني أولوية عالية جداً. وبناء على ذلك فإن المتوسطات التي تنتمي إلى المجال من (١) إلى (١.٨٠) تشير إلى عديم الأولوية، و المتوسطات التي تنتمي إلى المجال من (١.٨١) إلى أقل من (٢.٦٠) تشير إلى قليل الأولوية و المتوسطات التي تنتمي إلى المجال من (٢.٦١) إلى (٣.٤٠) تشير إلى متوسطة الأولوية ، و

المتوسطات التي تنتمي إلى المجال من (٣.٤١) إلى (٤.٢٠) تشير إلى أولوية عالية و المتوسطات التي تنتمي إلى المجال من (٤.٢١) إلى (٥) تشير إلى أولوية عالية جداً.

ويتضح من المتوسط العام لعبارات هذا المحور والذي بلغ (٤.٠٩) بانحراف معياري (٠.٥٥) أن أفراد عينة الدراسة يوافقون على أن إزالة نقاط الضعف في شبكات مؤسساتهم تحتاج إلى أولوية عالية.

ويمكن إبراز أهم النتائج في نقاط مرتبة حسب الأهمية كما يلي:

١ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (١) وهي " تفعيل التحديث الآلي لبرامج الحماية "(٤.٧٥) بانحراف معياري (٠.٥٢).

٢ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٢) وهي " تفعيل التحديث الآلي لجدران الحماية " (٤.٥٢) بانحراف معياري (٠.٧١).

٣ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٣) وهي " تخصيص خادم لتحديث نظم تشغيل الحاسبات المكتبية وأجهزة الخادم " (٤.٤٥) بانحراف معياري (٠.٦٩).

٤ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٤) وهي " تزويد وتفعيل خاصية الحماية من الفيروسات في جدران الحماية " (٤.٤١) بانحراف معياري (٠.٩٥٩).

٥ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٥) وهي " تزويد وتفعيل خاصية كشف ومنع الاختراق (IPS) في جدران الحماية " (٤.٣٨) بانحراف معياري (٠.٩٢).

٦ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٦) وهي " مراجعة محاولات الدخول إلى النظام وخصوصا من داخل الشبكة" (٤.٢٦) بانحراف معياري (٠.٨٨).

٧ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٧) وهي " تنفيذ اختبار دوري لكشف نقاط الضعف بدءا من خارج الشبكة" (٤.٢٥) بانحراف معياري (٠.٩٤٢).

٨ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٨) وهي " تنفيذ اختبار دوري لكشف نقاط الضعف من داخل الشبكة" (٤.٠١) بانحراف معياري (٠.٩٩).

٩ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٩) وهي " استخدام أدوات قياس أداء أجهزة الشبكة" (٣.٩٣) بانحراف معياري (٠.٩٤).

١٠ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (١٠) وهي " تزويد وتفعيل خاصية الحماية من البريد الدعائي (Spam) في جدار الحماية " (٣.٨٥) بانحراف معياري (١.٢٩).

١١ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (١١) وهي " تزويد وتفعيل خاصية تصفية المواقع غير المرغوب فيها في جدران الحماية " (٣.٧١) بانحراف معياري (١.٢٢).

١٢ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (١٢) وهي " استخدام قائمة تتضمن المهام اليومية لأعمال الحماية (Check list) " (٣.٦٦) بانحراف معياري (٠.٩٧).

تساؤل المحور الثالث: ما الهياكل التنظيمية المناسبة لمراكز تقنية المعلومات وما مدى توافق الوظائف المستخدمة في مجال أمن شبكات المعلومات معها؟

وتفرع من هذا السؤال ٢٨ عبارة تقيس متغيرات الهياكل التنظيمية وللإجابة على هذا التساؤل قام الباحث من خلال تحليل أداة الدراسة بحساب التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية ووضح الترتيب لعبارات المحور حسب أهميتها وفق الجدول رقم (٤/١٥) كالتالي:

جدول رقم (٤/١٥)

استجابات أفراد عينة الدراسة إزاء الهياكل التنظيمية المناسبة لمراكز تقنية المعلومات ومدى توافق الوظائف المستخدمة في مجال أمن شبكات المعلومات

م	العبارة		الاستجابة				المتوسط	الانحراف المعياري	الترتيب
			لا	إلى حد ما	نعم	المجموع			
١	يوجد في مؤسستي هيكل تنظيمي معتمد ومعمم، يتضمن الإدارة/القسم الذي أعمل فيه.	ك	٨	٣٠	٦٧	١٠٥	٢.٥٦	٠.٦٣	١
		%	٧.٦	٢٨.٦	٦٣.٨	%١٠٠			
٢	أرى أن الهيكل التنظيمي لإدارة/مركز تقنية المعلومات الذي أعمل فيه مناسب و مواكِب للتطور السريع في تقنية المعلومات.	ك	٢٢	٤٩	٣٤	١٠٥	٢.١١	٠.٧٣	١١
		%	٢١.٠	٤٦.٦	٣٢.٤	%١٠٠			
٣	يتم مراعاة التسلسل الإداري	ك	١١	٦٢	٣٢	١٠٥	٢.٢٠	٠.٦١	١٠

	في المعاملات الفنية.	%	١٠.٥	٥٩.٠	٣٠.٥	%١٠٠		
٤	يتم مراعاة التسلسل الإداري في المعاملات الإدارية والمالية.	ك	٤	٦٠	٤١	١٠٥	٢.٣٥	٠.٥٥	٥
		%	٣.٨	٥٧.٢	٣٩	%١٠٠		
٥	يوجد لجنة لإدارة التعديلات (شبكات وقواعد بيانات وموقع الانترنت..).	ك	٣٧	٤٩	١٩	١٠٤	١.٨٣	٠.٧١	١٩
		%	٣٥.٢	٤٦.٧	١٨.١	%٩٩.٠٥		
٦	يوجد قسم/إدارة/وحدة تحت مسمى أمن المعلومات أو أمن الشبكة أو ما شابه ذلك	ك	٥٨	٢٦	٢١	١٠٥	١.٦٥	٠.٨٠	٢٤
		%	٥٥.٢	٢٤.٨	٢٠	%١٠٠			
٧	يوجد في مؤسستي مسميات وظيفية للوظائف المتعلقة بالحماية في إدارة تقنية المعلومات مرفق بالمهام والواجبات والمسؤوليات والصلاحيات لكل وظيفة.	ك	٤٦	٤٦	١٣	١٠٥	١.٦٩	٠.٦٨	٢٢
		%	٤٣.٨	٤٣.٨	١٢.٤	%١٠٠			
٨	يتم تبديل الموظفين العاملين بالحماية باستمرار بمبادرة من الإدارة	ك	٥٨	٣٧	١٠	١٠٥	١.٥٤	٠.٦٧	٢٧
		%	٥٥.٢	٣٥.٣	٩.٥	%١٠٠			
٩	تتكرر مغادرة الموظفين في مجال الحماية والشبكات لوظائفهم رغبة بفرص أفضل.	ك	٣٥	٥١	١٩	١٠٥	١.٨٥	٠.٧٠	١٧
		%	٣٣.٣	٤٨.٦	١٨.١	%١٠٠			
١٠	المؤهل العلمي للعاملين في مجال الحماية في مؤسستي يناسب لمسميات وظائفهم.	ك	٣٥	٥٤	١٦	١٠٥	١.٨٢	٠.٦٨	٢٠
		%	٣٣.٣	٥١.٥	١٥.٢	%١٠٠			
١١	يوجد مدقق (Security Auditor) واحد على الأقل يراجع تنفيذ السياسات الأمنية.	ك	٥٩	٣٧	٩	١٠٥	١.٥٢	٠.٦٥	٢٨
		%	٥٦.٢	٣٥.٢	٨.٦	%١٠٠			
١٢	يوجد مسؤول (Network Admin) واحد على الأقل لأعمال الكابلات والمبدلات.	ك	١٢	٤٧	٤٦	١٠٥	٢.٣٢	٠.٦٧	٦
		%	١١.٤	٤٤.٨	٤٣.٨	%١٠٠			
١٣	يوجد موظف واحد على الأقل بمسمى ضابط أمن المعلومات	ك	٥٢	٤٥	٨	١٠٥	١.٥٨	٠.٦٣	٢٦
		%	٤٩.٥	٤٢.٩	٧.٦	%١٠٠			

١٤	يوجد موظف واحد على الأقل يقوم إدارة أجهزة الحماية.	ك	١٨	٤١	٤٦	١٠٥	٢.٢٧	٠.٧٤	٧
		%	١٧.١	٣٩.٠	٤٣.٩	%١٠٠			
١٥	يوجد موظف واحد على الأقل يقوم بإدارة برامج الحماية (برامج مكافحة الفيروسات والبريد الدعائي ومراجعة سجلات الأحداث (Events) لأجهزة الشبكة...).	ك	١٦	٣٦	٥٣	١٠٥	٢.٣٥	٠.٧٣	٤
		%	١٥.٢	٣٤.٣	٥٠.٥	%١٠٠			
١٦	عدد الموظفين الذين يعملون في مجال الحماية في مؤسستي غير كاف.	ك	١٥	٣٢	٥٨	١٠٥	٢.٤١	٠.٧٣	٣
		%	١٤.٣	٣٠.٥	٥٥.٢	%١٠٠			
١٧	أعاني من ضغط في العمل وأحتاج لوقت إضافي لإنجاز جميع واجباتي.	ك	٧	٤١	٥٧	١٠٥	٢.٤٨	٠.٦٢	٢
		%	٦.٧	٣٩.٠	٥٤.٣	%١٠٠			
١٨	تثمن مؤسستي أعمال الحماية بتقديم المكافآت أو العلاوات أو شهادات التقدير.	ك	٥٤	٣٧	١٤	١٠٥	١.٦٢	٠.٧١	٢٥
		%	٥١.٤	٣٥.٣	١٣.٣	%١٠٠			
١٩	مديري المباشر متخصص في إحدى مجالات تقنية المعلومات.	ك	٤٦	١٤	٤٥	١٠٥	١.٩٩	٠.٩٤	١٥
		%	٤٣.٨	١٣.٣	٤٢.٩	%١٠٠			
٢٠	مدير إدارة تقنية المعلومات متخصص في إحدى مجالات تقنية المعلومات.	ك	٤٠	٢٦	٣٩	١٠٥	١.٩٩	٠.٨٧	١٤
		%	٣٨.١	٢٤.٨	٣٧.١	%١٠٠			
٢١	أرى أن الدخل الذي أتقاضاه غير مناسب كموظف في مجال الحماية.	ك	١٤	٥٥	٣٦	١٠٥	٢.٢١	٠.٦٦	٨
		%	١٣.٣	٥٢.٤	٣٤.٣	%١٠٠			
٢٢	تقوم إدارة المؤسسة التي أعمل فيها بتخصيص ميزانية جيدة لتحسين الحماية.	ك	٢٩	٦١	١٥	١٠٥	١.٨٧	٠.٦٤	١٦
		%	٢٧.٦	٥٨.١	١٤.٣	%١٠٠			
٢٣	أرى أن التدريب الذي أحصل عليه من مؤسستي كاف لتأدية عملي.	ك	٥٠	٤١	١٤	١٠٥	١.٦٦	٠.٧١	٢٣
		%	٤٧.٦	٣٩.٠	١٣.٤	%١٠٠			
٢٤	توفر مؤسستي عقداً لتأمين الدعم الفني لأجهزة الحماية يشمل تبديل الجهاز.	ك	٣٤	٢٩	٤٢	١٠٥	٢.٠٨	٠.٨٥	١٢
		%	٣٢.٤	٢٧.٦	٤٠.٠	%١٠٠			

٢٥	أرى أن الدعم الفني الخاص بجدار الحماية الذي تستخدمه مؤسستي جيد.	ك	٣٥	٥٢	١٨	١٠٥	١.٨٤	٠.٧٠	١٨
		%	٣٣.٣	٤٩.٥	١٧.٢	%١٠٠			
٢٦	توفر مؤسستي عقداً لتأمين الدعم الفني لبرامج الحماية يشمل الحضور لموقع المؤسسة لإصلاح المشكلات عند طلب ذلك.	ك	٢٧	٥٢	٢٦	١٠٥	١.٩٩	٠.٧١	١٣
		%	٢٥.٧	٤٩.٥	٢٤.٨	%١٠٠			
٢٧	أرى أن الدعم الفني لبرامج الحماية من الفيروسات التي تستخدمها مؤسستي جيدة.	ك	١٧	٤٩	٣٩	١٠٥	٢.٢١	٠.٧٠	٩
		%	١٦.٢	٤٦.٧	٣٧.١	%١٠٠			
٢٨	تقوم مؤسستي بابتعاثي لحضور ندوات/مؤتمرات تتعلق بالحماية وأمن المعلومات.	ك	٥٢	٣١	٢٢	١٠٥	١.٧١	٠.٧٩	٢١
		%	٤٩.٥	٢٩.٥	٢١.٠	%١٠٠			
	المتوسط العام المحور الثالث						١.٩٢	٠.٣٣	

يوضح الجدول رقم (٤/١٥) الهياكل التنظيمية المناسبة لمراكز تقنية المعلومات وما مدى توافق الوظائف المستخدمة في مجال أمن شبكات المعلومات وذلك في المؤسسات التي تنتمي إليها عينة الدراسة ويتضمن الجدول ثمان وعشرون عبارة توضح مدى مناسبة الهياكل التنظيمية ومدى توافق الوظائف لأعمال الحماية وفقاً لاستجابات أفراد عينة الدراسة.

ويُلاحظ أن المتوسط العام قد بلغ ١.٩٢ بانحراف معياري ٠.٣٣ وحيث أن الاستجابة (لا) أعطيت الوزن (١) ، والاستجابة (إلى حد ما) أعطيت الوزن (٢) ، و الاستجابة نعم أُعطيت (٣). وبناء على ذلك فإن المتوسطات التي تنتمي إلى المجال من ١ إلى ١.٦٧ تعني غير موافق، والمتوسطات التي تنتمي إلى المجال من ١.٦٧ إلى ٢.٣٣ تعني موافق إلى حد ما، والمتوسطات التي تنتمي إلى المجال من ٢.٣٣ إلى ٣ تعني موافق. من ذلك يُلاحظ أن المتوسط العام لجميع عبارات هذا المحور تنتمي إلى المجال من١.٦٧ إلى ٢.٣٣ فهي تعني موافق إلى حد ما. ويُستنتج من ذلك أن أفراد عينة الدراسة يوافقون إلى حد ما على مناسبة الهياكل التنظيمية والوظائف المتوفرة في مؤسساتهم لأعمال حماية الشبكات. ويمكن إبراز أهم النتائج في نقاط مرتبة حسب الأهمية كما يلي:

١ – توضح نسب العبارة التي جاءت في الترتيب رقم (١) وهي " يوجد في مؤسستي هيكل تنظيمي معتمد ومعمم، يتضمن الإدارة/القسم الذي أعمل فيه " أن (٦٣.٨%) من عينة

الدراسة يتوفر لديهم هيكل تنظيمي معتمد ومعمم ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٥٦)، وانحراف معياري (٠.٦٣).

٢ - توضح نسب العبارة التي جاءت في الترتيب رقم (٢) وهي " أعاني من ضغط في العمل وأحتاج لوقت إضافي لإنجاز جميع واجباتي " أن (٥٤.٣%) من عينة يعانون من ضغط في العمل ويحتاجون لوقت إضافي لإنجاز جميع واجباتهم ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٤٨)، وانحراف معياري (٠.٦٢).

٣ - توضح نسب العبارة التي جاءت في الترتيب رقم (٣) وهي " عدد الموظفين الذين يعملون في مجال الحماية في مؤسستي غير كاف " أن (٥٨%) من عينة الدراسة لا يتوفر لديهم عدد كاف من الموظفين الذين يعملون في مجال الحماية، وقد حصلت تلك العبارة على متوسط حسابي (٢.٤١)، وانحراف معياري (٠.٧٣).

٤ - توضح نسب العبارة التي جاءت في الترتيب رقم (٤) وهي " يوجد موظف واحد على الأقل يقوم بإدارة برامج الحماية (برامج مكافحة الفيروسات والبريد الدعائي ومراجعة سجلات الأحداث (Events) لأجهزة الشبكة " أن (٥٠.٥%) من عينة الدراسة يتوفر لديهم يوجد موظف واحد على الأقل يقوم بإدارة برامج الحماية ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٣٥)، وانحراف معياري (٠.٧٣).

٥ - توضح نسب العبارة التي جاءت في الترتيب رقم (٥) وهي " يتم مراعاة التسلسل الإداري في المعاملات الإدارية والمالية " أن (٣٩%) من عينة الدراسة يتوفر لديهم يراعون التسلسل الإداري في المعاملات الإدارية والمالية ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٣٥)، وانحراف معياري (٠.٥٥).

٦ - توضح نسب العبارة التي جاءت في الترتيب رقم (٦) وهي " يوجد مسؤول (Network Admin) واحد على الأقل لأعمال الكابلات والمبدلات " أن (٤٣.٨%) من عينة الدراسة يتوفر لديهم مسؤول واحد على الأقل لأعمال الكابلات والمبدلات ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٣٢)، وانحراف معياري (٠.٦٧).

٧ - توضح نسب العبارة التي جاءت في الترتيب رقم (٧) وهي " يوجد موظف واحد على الأقل يقوم إدارة أجهزة الحماية " أن (٤٣.٩%) من عينة الدراسة يتوفر لديهم موظف واحد على الأقل يقوم إدارة أجهزة الحماية ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٢٧)، وانحراف معياري (٠.٧٤).

٨ - توضح نسب العبارة التي جاءت في الترتيب رقم (٨) وهي " أرى أن الدخل الذي أتقاضاه غير مناسب كموظف في مجال الحماية " أن (٣٤.٣%) من عينة الدراسة يرون أن الدخل الذي يتقاضونه غير مناسب كموظفين في مجال الحماية ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٢١)، وانحراف معياري (٠.٦٦).

٩ - توضح نسب العبارة التي جاءت في الترتيب رقم (٩) وهي " أرى أن الدعم الفني لبرامج الحماية من الفيروسات التي تستخدمها مؤسستي جيدة " أن (٣٧.١%) من عينة الدراسة يرون أن الدعم الفني لبرامج الحماية من الفيروسات التي تستخدمها مؤسساتهم جيدة ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٢١)، وانحراف معياري (٠.٧٠).

١٠ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٠) وهي " يتم مراعاة التسلسل الإداري في المعاملات الفنية " أن (٣٠.٥%) من عينة الدراسة يراعون التسلسل الإداري في المعاملات ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٢٠)، وانحراف معياري (٠.٦١).

١١ -توضح نسب العبارة التي جاءت في الترتيب رقم (١١) وهي " أرى أن الهيكل التنظيمي لإدارة/مركز تقنية المعلومات الذي أعمل فيه مناسب و مواكِب للتطور السريع في تقنية المعلومات " أن (٣٢.٤%) من عينة الدراسة يرون أن الهيكل التنظيمي لإدارة/مركز تقنية المعلومات الذي يعملون فيه مناسب و مواكِب للتطور السريع في تقنية المعلومات ، وقد حصلت تلك العبارة على متوسط حسابي (٢.١١)، وانحراف معياري (٠.٧٣).

١٢ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٢) وهي " توفر مؤسستي عقداً لتأمين الدعم الفني لأجهزة الحماية يشمل تبديل الجهاز " أن (٤٠.٠%) من عينة الدراسة توفر مؤسساتهم عقوداً لتأمين الدعم الفني لأجهزة الحماية يشمل تبديل الجهاز ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٠٨)، وانحراف معياري (٠.٨٥).

١٣ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٣) وهي " توفر مؤسستي عقداً لتأمين الدعم الفني لبرامج الحماية يشمل الحضور لموقع المؤسسة " أن (٢٤.٨%) من عينة الدراسة توفر مؤسساتهم عقوداً لتأمين الدعم الفني لبرامج الحماية يشمل الحضور لمواقع تلك المؤسسات ، وقد حصلت تلك العبارة على متوسط حسابي (١.٩٩)، وانحراف معياري (٠.٧١).

١٤ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٤) وهي " مدير إدارة تقنية المعلومات متخصص في إحدى مجالات تقنية المعلومات " أن (٣٧.١%) من عينة الدراسة يوجد لديهم

مدراء لإدارات تقنية المعلومات متخصصون في إحدى مجالات تقنية المعلومات ، وقد حصلت تلك العبارة على متوسط حسابي (١.٩٩)، وانحراف معياري (٠.٨٧).

١٥ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٥) وهي " مديري المباشر متخصص في إحدى مجالات تقنية المعلومات " أن (٤٢.٩%) من عينة الدراسة مدراؤهم المباشرون متخصصون في إحدى مجالات تقنية المعلومات ، وقد حصلت تلك العبارة على متوسط حسابي (١.٩٩)، وانحراف معياري (٠.٩٤).

١٦ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٦) وهي " تقوم إدارة المؤسسة التي أعمل فيها بتخصيص ميزانية جيدة لتحسين الحماية " أن (١٤.٣%) من عينة الدراسة تقوم إدارة مؤسساتهم التي يعملون فيها بتخصيص ميزانية جيدة لتحسين الحماية، وقد حصلت تلك العبارة على متوسط حسابي (١.٨٧)، وانحراف معياري (٠.٦٤).

١٧ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٧) وهي " المؤهل العلمي للعاملين في مجال الحماية في مؤسستي يناسب لمسميات وظائفهم " أن (١٨.١%) من عينة الدراسة المؤهل العلمي للعاملين في مجال الحماية في مؤسساتهم يناسب لمسميات وظائفهم، وقد حصلت تلك العبارة على متوسط حسابي (١.٨٥)، وانحراف معياري (٠.٧٠).

١٨ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٨) وهي " أرى أن الدعم الفني الخاص بجدار الحماية الذي تستخدمه مؤسستي جيد " أن (١٧.٢%) من عينة الدراسة يرون أن الدعم الفني الخاص بجدار الحماية الذي تستخدمه مؤسساتهم، وقد حصلت تلك العبارة على متوسط حسابي (١.٨٤)، وانحراف معياري (٠.٧٠).

١٩ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٩) وهي " يوجد لجنة لإدارة التعديلات (شبكات وقواعد بيانات وموقع الانترنت) " أن (١٨.١%) من عينة الدراسة يوجد لديهم لجان لإدارة التعديلات (شبكات وقواعد بيانات وموقع الانترنت)، وقد حصلت تلك العبارة على متوسط حسابي (١.٨٣)، وانحراف معياري (٠.٧١).

٢٠ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢٠) وهي " المؤهل العلمي للعاملين في مجال الحماية في مؤسستي يناسب لمسميات وظائفهم " أن (١٥.٢%) من عينة الدراسة تتناسب مؤهلاتهم العلمية في مجال الحماية مع مسميات وظائفهم ، وقد حصلت تلك العبارة على متوسط حسابي (١.٨٢)، وانحراف معياري (٠.٦٨).

٢١ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢١) وهي " تقوم مؤسستي بابتعاثي لحضور ندوات/مؤتمرات تتعلق بالحماية وأمن المعلومات " أن (٢١.٠%) من عينة الدراسة تقوم مؤسساتهم بابتعاثهم لحضور ندوات/مؤتمرات تتعلق بالحماية وأمن المعلومات ، وقد حصلت تلك العبارة على متوسط حسابي (١.٧١)، وانحراف معياري (٠.٧٩).

٢٢ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢٢) وهي يوجد في مؤسستي مسميات وظيفية للوظائف المتعلقة بالحماية في إدارة تقنية المعلومات مرفق بالمهام والواجبات والمسؤوليات والصلاحيات لكل وظيفة " أن (١٢.٤%) من عينة الدراسة يوجد في مؤسساتهم مسميات وظيفية للوظائف المتعلقة بالحماية في إدارة تقنية المعلومات مرفقة بالمهام والواجبات والمسؤوليات والصلاحيات لكل وظيفة ، وقد حصلت تلك العبارة على متوسط حسابي (١.٦٩)، وانحراف معياري (٠.٦٨).

٢٣ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢٣) " أرى أن التدريب الذي أحصل عليه من مؤسستي كاف لتأدية عملي" أن (١٣.٤%) من عينة الدراسة يرون أن التدريب الذي يحصلون عليه من مؤسساتهم كاف لتأدية أعمالهم، وقد حصلت تلك العبارة على متوسط حسابي (١.٦٦)، وانحراف معياري (٠.٧١).

٢٤ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢٤) "يوجد قسم/إدارة/وحدة تحت مسمى أمن المعلومات أو أمن الشبكة أو ما شابه ذلك " أن (٢٤.٨%) من عينة الدراسة يوجد لدى مؤسساتهم أقسام/إدارات/وحدات تحت مسمى أمن المعلومات أو أمن الشبكة أو ما شابه ذلك، وقد حصلت تلك العبارة على متوسط حسابي (١.٦٥)، وانحراف معياري (٠.٨٠).

٢٥ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢٥) " تثمن مؤسستي أعمال الحماية بتقديم المكافآت أو العلاوات أو شهادات التقدير " أن (١٣.٣%) من عينة الدراسة تثمن مؤسساتهم أعمال الحماية بتقديم المكافآت أو العلاوات أو شهادات التقدير، وقد حصلت تلك العبارة على متوسط حسابي (١.٦٢)، وانحراف معياري (٠.٧١).

٢٦ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢٦) " يوجد موظف واحد على الأقل بمسمى ضابط أمن المعلومات (Security Officer) " أن (٧.٦%) من عينة الدراسة يوجد لديهم موظف واحد على الأقل بمسمى ضابط أمن المعلومات ، وقد حصلت تلك العبارة على متوسط حسابي (١.٥٨)، وانحراف معياري (٠.٦٣).

٢٧ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢٧) " يتم تبديل الموظفين العاملين بالحماية باستمرار بمبادرة من الإدارة " أن (٩٠٥%) من عينة الدراسة يتم لديهم تبديل الموظفين العاملين بالحماية باستمرار بمبادرة من الإدارة ، وقد حصلت تلك العبارة على متوسط حسابي (١.٥٤)، وانحراف معياري (٠.٦٧).

٢٨ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢٨) " يوجد مدقق Security) (Auditor واحد على الأقل يراجع تنفيذ السياسات الأمنية " أن (٨٠٦%) من عينة الدراسة يوجد لديهم مدقق أمن معلومات واحد على الأقل يراجع تنفيذ السياسات الأمنية، وقد حصلت تلك العبارة على متوسط حسابي (١.٥٢)، وانحراف معياري (٠.٦٥).

تساؤل المحور الرابع: ما إجراءات العمل في حماية شبكات المعلومات وما مدى تطبيقها والعمل بها؟

للإجابة على هذا التساؤل قام الباحث من خلال تحليل أداة الدراسة بحساب التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية ووضح الترتيب لعبارات المحور حسب أهميتها وفق الجدول (٤/١٦) كالتالي:

جدول رقم (٤/١٦)

استجابات أفراد عينة الدراسة إزاء إجراءات العمل في حماية شبكات المعلومات ومدى تطبيقها والعمل بها

م	العبارة		الاستجابة				المتوسط	الانحراف المعياري	الترتيب
			لا	إلى حد ما	نعم	المجموع			
١	يوجد وثيقة توضح طريقة تحديث جدران الحماية.	ك	٤٨	٣٧	٢٠	١٠٥	١.٧٣	٠.٧٦	١٨
		%	٤٥.٧	٣٥.٣	١٩.٠	%١٠٠			
٢	يوجد وثيقة توضح طريقة تحديث نظام الحماية من الفيروسات والبرامج الضارة.	ك	٣٦	٣١	٣٨	١٠٥	٢.٠٢	٠.٨٤	٧
		%	٣٤.٣	٢٩.٥	٣٦.٢	%١٠٠			
٣	يوجد وثيقة توضح خطوات إعداد وتشغيل عمليات النسخ الاحتياطي	ك	٤٤	٢٢	٣٩	١٠٥	١.٩٥	٠.٨٩	١١
		%	٤١.٩	٢١.٠	٣٧.١	%١٠٠			

	والاسترجاع.							
٤	يتم أخذ موافقة لجنة التعديل قبل إجراء أي تعديل في أجهزة وبرامج الحماية.	ك	٣٦	٤٨	٢١	١٠٥	١.٨٦	٠.٧٣	١٣
		%	٣٤.٣	٤٥.٧	٢٠.٠	%١٠٠			
٥	يوجد وثيقة توضح أمكنة توضع أجهزة وبرامج الحماية.	ك	٣٧	٣٣	٣٥	١٠٥	١.٩٨	٠.٨٣	٩
		%	٣٥.٣	٣١.٤	٣٣.٣	%١٠٠			
٦	يوجد موظف واحد على الأقل يقوم بإدارة الإجراءات (إنشاءها ، تحديثها، توثيقها، ...).	ك	١٤	٦١	٣٠	١٠٥	٢.١٥	٠.٦٣	٣
		%	١٣.٣	٥٨.١	٢٨.٦	%١٠٠			
٧	يوجد إجراءات عمل خاصة بإدارة عمليات تحديث التطبيقات والبرمجيات.	ك	١٢	٦٢	٣١	١٠٥	٢.١٨	٠.٦٢	٢
		%	١١.٤	٥٩.٠	٢٩.٦	%١٠٠			
٨	توجد خطة تم تدريب المعنيين على تطبيقها لاسترداد النظام في الحالات الطارئة.	ك	٤٥	٣٥	٢٥	١٠٥	١.٨١	٠.٨٠	١٦
		%	٤٢.٩	٣٣.٣	٢٣.٨	%١٠٠			
٩	يوجد نظام لإدارة وثائق الإجراءات يتم تحديثه باستمرار.	ك	٥٥	٣٨	١٢	١٠٥	١.٥٩	٠.٦٩	٢٣
		%	٥٢.٤	٣٦.٢	١١.٤	%١٠٠			
١٠	يوجد صعوبات إدارية تعترض تنفيذ إجراءات حماية شبكة الحاسب.	ك	٢٠	٥٥	٣٠	١٠٥	٢.١٠	٠.٦٩	٥
		%	١٩.٠	٥٢.٤	٢٨.٦	%١٠٠			
١١	يوجد صعوبات مالية تعترض تنفيذ إجراءات حماية شبكة الحاسب.	ك	٢٤	٥٧	٢٤	١٠٥	٢.٠٠	٠.٦٨	٨
		%	٢٢.٩	٥٤.٢	٢٢.٩	%١٠٠			
١٢	يوجد صعوبات تدريبية تعترض تنفيذ إجراءات إدارة نظم أمن المعلومات.	ك	١٦	٥٨	٣١	١٠٥	٢.١٤	٠.٦٦	٤
		%	١٥.٢	٥٥.٣	٢٩.٥	%١٠٠			
١٣	تتوفر في مؤسستي سياسة (policy) للنسخ الاحتياطي والاسترجاع.	ك	٣٠	٤٢	٣٣	١٠٥	٢.٠٣	٠.٧٨	٦
		%	٢٨.٦	٤٠.٠	٣١.٤	%١٠٠			
١٤	تتوفر وثيقة مكتوبة تتضمن خطة طوارئ خاصة بتقنية المعلومات.	ك	٥٥	٣٣	١٧	١٠٥	١.٦٤	٠.٧٥	٢٢
		%	٥٢.٤	٣١.٤	١٦.٢	%١٠٠			

١٥	تخصص مؤسستي ميزانية لخطة الطوارئ.	ك	٥٨	٤٥	٢	١٠٥	١.٤٧	٠.٥٤	٢٦
		%	٥٥.٢	٤٢.٩	١.٩	%١٠٠			
١٦	يوجد مدة زمنية تبين الحد الزمني الأدنى لإعادة تشغيل النظام.	ك	٦٠	٣٥	١٠	١٠٥	١.٥٢	٠.٦٧	٢٥
		%	٥٧.١	٣٣.٤	٩.٥	%١٠٠			
١٧	يوجد في خطة الطوارئ بيان واضح للأنظمة الحرجة.	ك	٤٤	٤١	٢٠	١٠٥	١.٧٧	٠.٧٥	١٧
		%	٤١.٩	٣٩.٠	١٩.١	%١٠٠			
١٨	تتوفر في مؤسستي سياسة للاستخدام المقبول لتجهيزات تقنية المعلومات.	ك	٣٢	٥٨	١٥	١٠٥	١.٨٤	٠.٦٥	١٥
		%	٣٠.٥	٥٥.٢	١٤.٣	%١٠٠			
١٩	تتوفر في مؤسستي سياسة للتدريب في تخصصات تقنية المعلومات.	ك	٤١	٥٧	٧	١٠٥	١.٦٨	٠.٦٠	٢٠
		%	٣٩.٠	٥٤.٣	٦.٧	%١٠٠			
٢٠	تتوفر في مؤسستي سياسة توظيف الأفراد المناسبين في إدارة تقنية المعلومات.	ك	٣٢	٥٥	١٨	١٠٥	١.٨٧	٠.٦٨	١٢
		%	٣٠.٥	٥٢.٤	١٧.١	%١٠٠			
٢١	تتوفر في مؤسستي سياسة التوريد وتأمين الخدمات من خارج المنظمة (Outsourcing)	ك	٢٩	٤٩	٢٧	١٠٥	١.٩٨	٠.٧٣	١٠
		%	٢٧.٦	٤٦.٧	٢٥.٧	%١٠٠			
٢٢	تتوفر في مؤسستي سياسة لتقييم درجة سرية المعلومات.	ك	٤٤	٤٧	١٤	١٠٥	١.٧١	٠.٦٩	١٩
		%	٤١.٩	٤٤.٨	١٣.٣	%١٠٠			
٢٣	تتوفر في مؤسستي سياسة أرشفة وسائط حفظ البيانات.	ك	٣٨	٤٤	٢٢	١٠٤	١.٨٥	٠.٧٥	١٤
		%	٣٦.٢	٤١.٩	٢١.٠	%٩٩.١			
٢٤	تتوفر في مؤسستي إجراء إتلاف الأصول المعلوماتية Information (Assets) المنتهية الصلاحية.	ك	٥٨	٣٧	١٠	١٠٥	١.٥٤	٠.٦٧	٢٤
		%	٥٥.٣	٣٥.٢	٩.٥	%١٠٠			
٢٥	يتوفر في مؤسستي إجراء تسمية الأصول المعلوماتية وتسجيله على الوسائط	ك	٥٤	٣٣	١٨	١٠٥	١.٦٦	٠.٧٦	٢١
		%	٥١.٤	٣١.٤	١٧.٢	%١٠٠			

	المعلوماتية.								
٢٦	يتوفر في مؤسستي إجراء تحديث أنظمة التشغيل.	ك	١٤	٣٨	٥٣	١٠٥	٢.٣٧	٠.٧١	١
		%	١٣.٣	٣٦.٢	٥٠.٥	%١٠٠			
٢٧	المتوسط العام المحور الرابع						١.٨٤	٠.٠٤	

يوضح الجدول رقم (٤/١٦) إجراءات العمل في حماية شبكات المعلومات و مدى تطبيقها والعمل بها، في عينة الدراسة ويتضمن الجدول ست وعشرون عبارة توضح متغيرات الإجراءات وتطبيقها وفقاً لاستجابات أفراد عينة الدراسة،

ويُلاحظ أن المتوسط العام قد بلغ ١.٨٤ بانحراف معياري ٠.٠٤ وحيث أن الاستجابة لا أعطيت الوزن (١) ، والاستجابة (إلى حد ما) أعطيت الوزن (٢) ، والاستجابة (نعم) أُعطيت (٣). وبناء على ذلك فإن المتوسطات التي تنتمي إلى المجال من ١ إلى ١.٦٧ تعني غير موافق، والمتوسطات التي تنتمي إلى المجال من ١.٦٧ إلى ٢.٣٣ تعني موافق إلى حد ما، والمتوسطات التي تنتمي إلى المجال من ٢.٣٣ إلى ٣ تعني موافق. من ذلك يُلاحظ أن المتوسط العام لجميع عبارات هذا الجدول تنتمي إلى المجال من١.٦٧ إلى ٢.٣٣ تعني موافق إلى حد ما. ويُستنتج من ذلك أن أفراد عينة الدراسة يوافقون إلى حد ما على مناسبة إجراءات العمل في حماية شبكات المعلومات و تطبيقها والعمل بها في مؤسساتهم لأعمال حماية الشبكات.

ويمكن إبراز أهم النتائج في نقاط مرتبة حسب الأهمية كما يلي:

١ - توضح نسب العبارة التي جاءت في الترتيب رقم (١) وهي " يتوفر في مؤسستي إجراء تحديث أنظمة التشغيل " أن (٥٠.٥%) من عينة الدراسة يتوفر في مؤسساتهم إجراء تحديث أنظمة التشغيل ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٣٧)، وانحراف معياري (٠.٧١).

٢ - توضح نسب العبارة التي جاءت في الترتيب رقم (٢) وهي " يوجد إجراءات عمل خاصة بإدارة عمليات تحديث التطبيقات والبرمجيات " أن (٢٩.٦%) من عينة الدراسة لديهم إجراءات عمل خاصة بإدارة عمليات تحديث التطبيقات والبرمجيات ، وقد حصلت تلك العبارة على متوسط حسابي (٢.١٨)، وانحراف معياري (٠.٦٢).

٣ - توضح نسب العبارة التي جاءت في الترتيب رقم (٣) وهي " يوجد موظف واحد على الأقل يقوم بإدارة الإجراءات (إنشاءها ، تحديثها، توثيقها) " أن (٢٨.٦%) من عينة الدراسة يوجد لديهم موظف واحد على الأقل يقوم بإدارة الإجراءات (إنشاءها ، تحديثها، توثيقها) ، وقد حصلت تلك العبارة على متوسط حسابي (٢.١٥)، وانحراف معياري (٠.٦٣).

٤ – توضح نسب العبارة التي جاءت في الترتيب رقم (٤) وهي " يوجد صعوبات تدريبية تعترض تنفيذ إجراءات إدارة نظم أمن المعلومات " أن (٢٩.٥%) من عينة الدراسة يوجد لديهم صعوبات تدريبية تعترض تنفيذ إجراءات إدارة نظم أمن المعلومات ، وقد حصلت تلك العبارة على متوسط حسابي (٢.١٤)، وانحراف معياري (٠.٦٦).

٥ – توضح نسب العبارة التي جاءت في الترتيب رقم (٥) وهي " يوجد صعوبات إدارية تعترض تنفيذ إجراءات حماية شبكة الحاسب " أن (٢٩.٥%) من عينة الدراسة يوجد لديهم صعوبات إدارية تعترض تنفيذ إجراءات حماية شبكة الحاسب ، وقد حصلت تلك العبارة على متوسط حسابي (٢.١٠)، وانحراف معياري (٠.٦٩).

٦ – توضح نسب العبارة التي جاءت في الترتيب رقم (٦) وهي " تتوفر في مؤسستي سياسة (policy) للنسخ الاحتياطي والاسترجاع " أن (٢٨.٦%) من عينة الدراسة يتوفر في مؤسساتهم سياسة للنسخ الاحتياطي والاسترجاع ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٠٣)، وانحراف معياري (٠.٧٨).

٧ – توضح نسب العبارة التي جاءت في الترتيب رقم (٧) وهي " يوجد وثيقة توضح طريقة تحديث نظام الحماية من الفيروسات والبرامج الضارة " أن (٣١.٤%) من عينة الدراسة يوجد لديهم وثيقة توضح طريقة تحديث نظام الحماية من الفيروسات والبرامج الضارة ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٠٢)، وانحراف معياري (٠.٨٤).

٨ – توضح نسب العبارة التي جاءت في الترتيب رقم (٨) وهي " يوجد صعوبات مالية تعترض تنفيذ إجراءات حماية شبكة الحاسب " أن (٢٢.٩%) من عينة الدراسة يوجد لديهم صعوبات مالية تعترض تنفيذ إجراءات حماية شبكة الحاسب ، وقد حصلت تلك العبارة على متوسط حسابي (٢.٠٠)، وانحراف معياري (٠.٦٨).

٩ – توضح نسب العبارة التي جاءت في الترتيب رقم (٩) وهي " يوجد وثيقة توضح أمكنة توضع أجهزة وبرامج الحماية " أن (٣٣.٣%) من عينة الدراسة يوجد لديهم وثيقة توضح أمكنة توضع أجهزة وبرامج الحماية ، وقد حصلت تلك العبارة على متوسط حسابي (١.٩٨)، وانحراف معياري (٠.٨٣).

١٠ –توضح نسب العبارة التي جاءت في الترتيب رقم (١٠) وهي " تتوفر في مؤسستي سياسة التوريد وتأمين الخدمات من خارج المنظمة (Outsourcing) " أن (٢٥.٧%) من عينة

الدراسة يتوفر في مؤسساتهم سياسة التوريد وتأمين الخدمات من خـــارج المنظمـــة ، وقـــد حصلت تلك العبارة على متوسط حسابي (١.٩٨)، وانحراف معياري (٠.٧٣).

١١ -توضح نسب العبارة التي جاءت في الترتيب رقم (١١) وهي " يوجد وثيقة توضح خطوات إعداد وتشغيل عمليات النسخ الاحتياطي والاسترجاع " أن (٣٧.١%) من عينة الدراســـة يوجد لديهم وثيقة توضح خطوات إعداد وتشغيل عمليات النسخ الاحتياطي والاسترجاع ، وقد حصلت تلك العبارة على متوسط حسابي (١.٩٥)، وانحراف معياري (٠.٨٩).

١٢ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٢) وهي " تتوفر في مؤسســـتي سياســـة توظيف الأفراد المناسبين في إدارة تقنية المعلومات " أن (١٧.١%) من عينة الدراسة " تتوفر في مؤسساتهم سياسة توظيف الأفراد المناسبين في إدارة تقنية المعلومات ، وقد حصلت تلـــك العبارة على متوسط حسابي (١.٨٧)، وانحراف معياري (٠.٦٨).

١٣ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٣) وهي " يتم أخذ موافقة لجنة التعديل قبل إجراء أي تعديل في أجهزة وبرامج الحماية " أن (٢٠.٠%) من عينة الدراسة يأخـــذون موافقة لجنة التعديل قبل إجراء أي تعديل في أجهزة وبرامج الحماية ، وقد حصـــلت تلـــك العبارة على متوسط حسابي (١.٨٦)، وانحراف معياري (٠.٧٣).

١٤ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٤) وهي " تتوفر في مؤسســـتي سياســـة أرشفة وسائط حفظ البيانات " أن (٢١.٠%) من عينة الدراسة تتوفر في مؤسساتهم سياسة أرشفة وسائط حفظ البيانات ، وقد حصلت تلك العبارة على متوســـط حســـابي (١.٨٥)، وانحراف معياري (٠.٧٥).

١٥ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٥) وهي " تتوفر في مؤسســـتي سياســـة أرشفة وسائط حفظ البيانات " أن (١٤.٣%) من عينة الدراسة تتوفر في مؤسساتهم سياسة أرشفة وسائط حفظ البيانات، وقد حصلت تلك العبارة على متوســـط حســـابي (١.٨٤)، وانحراف معياري (٠.٦٥).

١٦ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٦) وهي " توجـــد خطـــة تم تـــدريب المعنيين على تطبيقها لاسترداد النظام في الحالات الطارئة " أن (٢٣.٨%) من عينة الدراســـة يوجد لديهم خطة تم تدريب المعنيين على تطبيقها لاسترداد النظام في الحالات الطارئة ، وقد حصلت تلك العبارة على متوسط حسابي (١.٨١)، وانحراف معياري (٠.٨٠).

١٧ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٧) وهي " يوجد في خطة الطوارئ بيان واضح للأنظمة الحرجة " أن (١٩.١%) من عينة الدراسة يضمنون خطة الطوارئ بياناً واضحاً للأنظمة الحرجة ، وقد حصلت تلك العبارة على متوسط حسابي (١.٧٧)، وانحراف معياري (٠.٧٥).

١٨ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٨) وهي " يوجد وثيقة توضح طريقة تحديث جدران الحماية " أن (١٩.٠%) من عينة الدراسة يوجد لديهم وثيقة توضح طريقة تحديث جدران الحماية، وقد حصلت تلك العبارة على متوسط حسابي (١.٧٣)، وانحراف معياري (٠.٧٦).

١٩ -توضح نسب العبارة التي جاءت في الترتيب رقم (١٩) وهي " تتوفر في مؤسستي سياسة لتقييم درجة سرية المعلومات " أن (١٣.٣%) من عينة الدراسة تتوفر في مؤسساتهم سياسة لتقييم درجة سرية المعلومات، وقد حصلت تلك العبارة على متوسط حسابي (١.٧١)، وانحراف معياري (٠.٦٩).

٢٠ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢٠) وهي " تتوفر في مؤسستي سياسة للتدريب في تخصصات تقنية المعلومات " أن (٦.٧%) من عينة الدراسة تتوفر في مؤسساتهم سياسة للتدريب في تخصصات تقنية المعلومات، وقد حصلت تلك العبارة على متوسط حسابي (١.٦٨)، وانحراف معياري (٠.٦٠).

٢١ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢١) وهي "يتوفر في مؤسستي إجراء تسمية الأصول المعلوماتية (Information Assets) وتسجيله على الوسائط المعلوماتية " أن (١٧.٢%) من عينة الدراسة يتوفر في مؤسساتهم إجراء لتسمية الأصول المعلوماتية وتسجيله على الوسائط المعلوماتية ، وقد حصلت تلك العبارة على متوسط حسابي (١.٦٦)، وانحراف معياري (٠.٧٦).

٢٢ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢٢) وهي "تتوفر وثيقة مكتوبة تتضمن خطة طوارئ خاصة بتقنية المعلومات " أن (١٦.٢%) من عينة الدراسة تتوفر لديهم وثيقة مكتوبة تتضمن خطة طوارئ خاصة بتقنية المعلومات ، وقد حصلت تلك العبارة على متوسط حسابي (١.٦٤)، وانحراف معياري (٠.٧٥).

٢٣ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢٣) وهي " يوجد نظام لإدارة وثائق الإجراءات يتم تحديثه باستمرار " أن (١١.٤%) من عينة الدراسة يوجد لديهم نظام لإدارة

وثائق الإجراءات يتم تحديثه باستمرار ، وقد حصلت تلك العبارة على متوسط حسابي (١.٥٩)، وانحراف معياري (٠.٦٩).

٢٤ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢٤) وهي " تتوفر في مؤسستي إجراء إتلاف الأصول المعلوماتية (Information Assets) المنتهية الصلاحية " أن (٩.٥%) من عينة الدراسة يتوفر في مؤسساتهم إجراء إتلاف الأصول المعلوماتية المنتهية الصلاحية ، وقد حصلت تلك العبارة على متوسط حسابي (١.٥٤)، وانحراف معياري (٠.٦٧).

٢٥ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢٥) وهي " يوجد مدة زمنية تبين الحد الزمني الأدنى لإعادة تشغيل النظام " أن (٩.٥%) من عينة الدراسة يوجد في خطة الطوارئ لديهم مدة زمنية تبين الحد الزمني الأدنى لإعادة تشغيل النظام ، وقد حصلت تلك العبارة على متوسط حسابي (١.٥٢)، وانحراف معياري (٠.٦٧).

٢٦ -توضح نسب العبارة التي جاءت في الترتيب رقم (٢٦) وهي " تخصص مؤسستي ميزانية لخطة الطوارئ " أن (١.٩%) من عينة الدراسة تخصص مؤسساتهم ميزانية لخطة الطوارئ ، وقد حصلت تلك العبارة على متوسط حسابي (١.٤٧)، وانحراف معياري (٠.٥٤).

تساؤل المحور الخامس: ما المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات الحاسب وما التدابير الاحتياطية اللازمة لتجنبها، وما درجة خطورة تلك المخاطر وما درجة الأولوية لاتخاذ التدابير الوقائية لتجنب تلك المخاطر.

للحصول على النتائج المرجوة من هذا التساؤل قام الباحث بتقسيمه إلى جزأين:

الجزء الأول: المخاطر الخارجية والمخاطر الداخلية

الجزء الثاني: تدابير الحماية من المخاطر الداخلية والخارجية

حيث أن معرفة المخاطر الداخلية والمخاطر الخارجية لا يكفي بل يجب تنفيذ تدابير مناسبة للحماية من تلك المخاطر. وللإجابة على هذا التساؤل قام الباحث من خلال تحليل أداة الدراسة بحساب التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية ووضح الترتيب لعبارات الجزء الأول من هذا المحور كالتالي:

جدول رقم (٤/١٧)

المخاطر الخارجية والداخلية

م	العبارة		الاستجابة						المتوسط	الانحراف المعياري	الترتيب
			درجة خطورة المخاطر الخارجية والداخلية (١) أقل خطوره ، (٥) أعلى خطورة					المجموع			
			(٥)	(٤)	(٣)	(٢)	(١)				
١.	التعدي على الكابلات وتخريبها.	ك	٧٣	٢٤	٧	١	–	١٠٥	٤.٦١	٠.٦٧	٣
		%	٦٩.٥	٢٢.٩	٦.٨	١.٠	–	%١٠٠			
٢.	اندلاع الحريق.	ك	٧٨	١٦	٩	١	–	١٠٤	٤.٦٣	٠.٧٣	٢
		%	٧٤.٣	١٥.٢	٨.٦	١.٠	–	%٩٩.١			
٣.	حصول إغراق بالمياه بسبب الفيضانات.	ك	٦٢	٣٢	٥	٣	١	١٠٣	٤.٤٧	٠.٨٠	٥
		%	٥٩.٠	٣٠.٥	٤.٨	٢.٩	١.٠	%٩٨.٢			
٤.	اختراق لتعديل البيانات وتغيرها أو إتلافها.	ك	٧٥	٢٧	٢	١	–	١٠٥	٤.٦٨	٠.٥٦	١
		%	٧١.٤	٢٥.٧	١.٩	١.٠	–	%١٠٠			
٥.	التعرض لهجوم إرهابي.	ك	٦٦	٢٠	١٤	٥	–	١٠٥	٤.٤٠	٠.٨٩	٧
		%	٦٢.٩	١٩.٠	١٣.٣	٤.٨	–	%١٠٠			
٦.	اختراق أجهزة الخادم من داخل المؤسسة (عبث،إساءة استخدام...).	ك	٦٥	٢٦	١١	١	٢	١٠٥	٤.٤٤	٠.٨٦	٦
		%	٦١.٩	٢٤.٨	١٠.٤	١.٠	١.٩	%١٠٠			
٧.	استخدام برامج بغرض التجسس من قبل المستفيدين من داخل المؤسسة.	ك	٦٠	٣٠	١٠	٤	–	١٠٤	٤.٣٧	٠.٩٥	٨
		%	٥٧.١	٢٨.٦	٩.٥	٣.٨	–	%٩٩			
٨.	زيارة مواقع إنترنت غير موثوقة تسمح بتنزيل البرمجيات الضارة.	ك	٣٨	٤٠	٢٣	٢	٢	١٠٥	٤.٠٥	٠.٩١	١٢
		%	٣٦.٢	٣٨.١	٢١.٩	١.٩	١.٩	%١٠٠			
٩.	الإصابة بفيروسات مصدرها الانترنت.	ك	٣٩	٣٥	٢٩	٢	–	١٠٥	٤.٠٦	٠.٨٥	١١
		%	٣٧.١	٣٣.٣	٢٧.٧	١.٩	–	%١٠٠			

.١٠	الإصابة بفيروسات مصدرها وسائط التخزين وذواكر الفلاش.	ك	٤٣	٣٨	١٨	٦	–	١٠٥	٤.١٢	٠.٨٩	١٠
		%	٤١.٠	٣٦.٢	١٧.١	٥.٧	–	%١٠٠			
.١١	تنزيل برامج غير مصرح بها.	ك	٢٢	٤٣	٢١	١٦	٣	١٠٥	٣.٦٢	١.٠٧	١٤
		%	٢١.٠	٤١.٠	٢٠.٠	١٥.١	٢.٩	%١٠٠			
.١٢	سرقة الأجهزة ووسائط التخزين.	ك	٤٥	٢٩	١٦	١٠	٥	١٠٥	٣.٩٤	١.١٨	١٣
		%	٤٢.٩	٢٧.٦	١٥.٢	٩.٥	٤.٨	%١٠٠			
.١٣	الدخول غير المصرح إلى مركز البيانات وتعطيل عمل أجهزته.	ك	٦٢	٢٢	١٥	٢	٤	١٠٥	٤.٣٠	١.٠٤	٩
		%	٥٩.٠	٢١.٠	١٤.٣	١.٩	٣.٨	%١٠٠			
.١٤	تعديل إعدادات أجهزة الشبكة بطريقة يصعب تعقبها لإطالة فترة الانقطاع.	ك	٧١	٢٣	٧	٢	٢	١٠٥	٤.٥١	٠.٨٦	٤
		%	٦٧.٦	٢١.٩	٦.٧	١.٩	١.٩	%١٠٠			
	المتوسط العام للجزء الأول من المحور الخامس								٤.٢٩	٠.٥٦	

يوضح الجدول رقم (٤/١٧) المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات الحاسب ويتضمن أربع عشرة عبارة توضح المخاطر الداخلية والخارجية وفقاً لاستجابات أفراد عينة الدراسة، يتضح من هذا الجدول أن قيمة المتوسط العام لهذا الجزء هي (٤.٢٩) وانحرافه المعياري (٠.٥٦)، وحيث أن المقياس المستخدم خماسي وفيه (١) تعني موضوع العبارة عديم الخطورة و(٢) تعني قليل الخطورة و(٣) تعني متوسط الخطورة، و(٤) تعني خطر و(٥) تعني خطر جداً. وبناء على ذلك فإن المتوسطات التي تنتمي إلى المجال من (١) إلى (١.٨٠) تشير إلى عديم الخطورة، و المتوسطات التي تنتمي إلى المجال من (١.٨١) إلى أقل من (٢.٦٠) تشير إلى قليل الخطورة و المتوسطات التي تنتمي إلى المجال من (٢.٦١) إلى (٣.٤٠) تشير إلى متوسطة الخطورة، و المتوسطات التي تنتمي إلى المجال من (٣.٤١) إلى (٤.٢٠) تشير إلى خطر و المتوسطات التي تنتمي إلى المجال من (٤.٢١) إلى (٥) تشير إلى خطر جداً.

من ذلك يُلاحظ أن المتوسط العام لجميع عبارات هذا الجدول ينتمي إلى المجال من(٤.٢٩) إلى (٥) فهي تعني خطر جداً. ويُستنتج من ذلك أن أفراد عينة الدراسة يوافقون على أن المخاطر الداخلية

والخارجية التي يمكن أن تتعرض لها شبكات مؤسساتهم خطرة جداً. ويمكن إبراز أهم النتائج في نقاط مرتبة حسب الأهمية كما يلي:

١ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (١) وهي " اختراق لتعديل البيانات وتغيرها أو إتلافها " (٤.٦٨) بانحراف معياري (٠.٥٦).

٢ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٢) وهي اندلاع الحريق " (٤.٦٣) بانحراف معياري (٠.٧٣).

٣ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٣) وهي " التعدي على الكابلات وتخريبها " (٤.٦١) بانحراف معياري (٠.٦٧).

٤ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٣) وهي " تعديل إعدادات أجهزة الشبكة بطريقة يصعب تعقبها لإطالة فترة الانقطاع" (٤.٥١) بانحراف معياري (٠.٨٦).

٥ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٥) وهي " حصول إغراق بالمياه بسبب الفيضانات." (٤.٤٧) بانحراف معياري (٠.٨٠).

٦ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٦) وهي " اختراق أجهزة الخادم من داخل المؤسسة (عبث،إساءة استخدام...)." (٤.٤٤) بانحراف معياري (٠.٨٦).

٧ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٧) وهي " التعرض لهجوم إرهابي " (٤.٤٠) بانحراف معياري (٠.٨٩).

٨ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٨) وهي " استخدام برامج بغرض التجسس من قبل المستفيدين من داخل المؤسسة " (٤.٣٧) بانحراف معياري (٠.٩٥).

٩ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٩) وهي " الدخول غير المصرح إلى مركز البيانات وتعطيل عمل أجهزته " (٤.٣٠) بانحراف معياري (١.٠٤).

١٠ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (١٠) وهي " الإصابة بفيروسات مصدرها وسائط التخزين وذواكر الفلاش " (٤.١٢) وانحراف معياري (٠.٨٩) .

١١ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (١١) وهي " الإصابة بفيروسات مصدرها الانترنت " (٤.٠٦) بانحراف معياري (٠.٨٥).

١٢ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (١٢) وهي " زيارة مواقع إنترنت غير موثوقة تسمح بتنزيل البرمجيات الضارة " (٤.٠٥) بانحراف معياري (٠.٩١).

١٣ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (١٣) وهي " سـرقة الأجهـزة ووسـائط التخزين" (٣.٩٤) بانحراف معياري (١.١٨).

١٤ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (١٤) وهي " تنزيل برامج غير مصرح بهـا " (٣.٦٢) بانحراف معياري (١.٠٧).

الجزء الثاني: تدابير الحماية من المخاطر الداخلية والخارجية

جدول رقم (١٨/٤)

التدابير الوقائية من المخاطر الداخلية والخارجية

م	العبارة		الاستجابة						المتوسط	الانحراف المعياري	الترتيب
			درجة الأولوية (١) أقل أولوية ، (٥) أعلى أولوية					المجموع			
			(٥)	(٤)	(٣)	(٢)	(١)				
١٥.	توفير حراسة عند بوابات مركز البيانات على مدار الساعة.	ك	٤٥	١٥	٢٧	١٢	٦	١٠٥	٣.٧٧	١.٢٧	٤٣
		%	٤٢.٩	١٤.٣	٢٥.٧	١١.٤	٥.٧	%١٠٠			
١٦.	تجهيز مركز البيانات بحساسات الحرارة والحركة ونظام الإطفاء والإنذار.	ك	٦٣	٢١	١٢	٩		١٠٥	٤.٣١	٠.٩٨	٤
		%	٦٠.٠	٢٠.٠	١١.٤	٨.٦		%١٠٠			
١٧.	قفل مركز البيانات (غرفة أجهزة الخادم وأجهزة الشبكة) بحيث لا يدخلها إلا المتخصصون ممن لديهم ترخيص بالدخول.	ك	٧٣	٢٢	٨	٢		١٠٥	٤.٥٦	٠.٨٠	١
		%	٦٩.٥	٢١.٠	٧.٦	١.٩		%١٠٠			
١٨.	تجهيز مركز البيانات بآلية تسجيل للداخلين بالاسم والوقت وسبب الدخول.	ك	٤١	٤٠	١٨	٢	٤	١٠٥	٤.٠٧	١.٠٠	٢٦
		%	٣٩.٠	٣٨.٢	١٧.١	١.٩	٣.٨	%١٠٠			
١٩.	توفير مراقبة داخلية باستخدام كاميرات تلفزيونية مع التسجيل.	ك	٤٣	٣٥	١٧	٩	١	١٠٥	٤.٠٥	١.٠٠	٢٩
		%	٤١.٠	٣٣.٢	١٦.٢	٨.٦	١.٠	%١٠٠			
٢٠.	عمل النسخ الاحتياطي	ك	٥٢	٣٠	٢١	٢	-	١٠٥	٤.٢٦	٠.٨٤	٨

	والاسترجاع الآلي يومياً.	%	٤٩.٥	٢٨.٦	٢٠.٠	١.٩	–	%١٠٠			
.٢١	وضع وسائط النسخ الاحتياطي في خزائن مضادة للصدمات والحريق.	ك	٥٦	٢٣	٢٠	٦	–	١٠٥	٤.٢٣	٠.٩٥	٩
		%	٥٣.٤	٢١.٩	١٩.٠	٥.٧	–	%١٠٠			
.٢٢	تطبيق التشفير على وسائط النسخ الاحتياطي.	ك	٤٤	٢٤	٢٥	١٠	٢	١٠٥	٣.٩٣	١.١٠	٤١
		%	٤١.٩	٢٢.٩	٢٣.٨	٩.٥	١.٩	%١٠٠			
.٢٣	إبعاد وسائط النسخ لاحتياطي ووسائط التخزين عن أماكن تسرب المياه.	ك	٥٧	٢٧	١٥	٦	–	١٠٥	٤.٢٩	٠.٩٢	٧
		%	٥٤.٣	٢٥.٧	١٤.٣	٥.٧	–	%١٠٠			
.٢٤	إتلاف وسائط التخزين والنسخ الاحتياطي المنتهية الصلاحية.	ك	٤٥	٢٣	٢٦	٩	٢	١٠٥	٣.٩٥	١.٠٩	٤٠
		%	٤٢.٩	٢١.٩	٢٤.٧	٨.٦	١.٩	%١٠٠			
.٢٥	تركيب برامج مخصصة لمراقبة استخدام المستفيدين.	ك	٤٤	٣١	٢٨	٢		١٠٥	٤.١١	٠.٨٧	١٩
		%	٤١.٩	٢٩.٥	٢٦.٧	١.٩		%١٠٠			
.٢٦	توفير خطة طوارئ واضحة ومعتمدة.	ك	٥٤	١٣	٣٠	٦	٢	١٠٥	٤.٠٦	١.١٠	٢٧
		%	٥١.٤	١٢.٤	٢٨.٦	٥.٧	١.٩	%١٠٠			
.٢٧	إعداد خطة للتراجع (Rollback) تطبق في حالة عدم نجاح خطة الطوارئ.	ك	٤٣	٢٧	٢٤	٧	٤	١٠٥	٣.٩٣	١.٢٠	٤٢
		%	٤١.٠	٢٥.٧	٢٢.٨	٦.٧	٣.٨	%١٠٠			
.٢٨	تدريب كل الموظفين على أمن المعلومات كل حسب واجباته الوظيفية.	ك	٤٥	٣٤	٢٣	٣		١٠٥	٤.١٥	٠.٨٦	١٦
		%	٤٢.٩	٣٢.٤	٢١.٨	٢.٩		%١٠٠			
.٢٩	اختبار خطة الطوارئ.	ك	٣٥	٣٨	٣١	١		١٠٥	٤.٠٢	٠.٨٢	٣٤
		%	٣٣.٣	٣٦.٢	٢٩.٥	١.٠		%١٠٠			
.٣٠	اعتماد ميزانية خاصة بخطة الطوارئ.	ك	٣٧	٣٦	٢٤	٨		١٠٥	٣.٩٧	٠.٩٥	٣٧
		%	٣٥.٢	٣٤.٣	٢٢.٩	٧.٦		%١٠٠			
.٣١	السعي لمطابقة إجراءات العمل لتتوافق مع معايير دولية (آيزو) تتعلق بالحماية.	ك	٤٠	٣٢	٢١	١١		١٠٤	٣.٩٧	١.٠١	٣٨
		%	٣٨.١	٣٠.٥	٢٠.٠	١٠.٥		%٩٩.١			
.٣٢	السعي للتوصل إلى اتفاقيات تعاون مع	ك	٤٣	٢٦	٣٢	٤		١٠٥	٤.٠٣	٠.٩٤	٣٢
		%	٤١.٠	٢٤.٧	٣٠.٥	٣.٨		%١٠٠			

	المتخصصين في الحماية.									
٣٣.	تنفيذ اختبارات دورية لنقاط الضعف انطلاقا من داخل الشبكة.	ك	٥١	٣٣	٢١			١٠٥	٤.٢٩	٠.٧٨	٦
		%	٤٨.٦	٣١.٤	٢٠.٠			%١٠٠			
٣٤.	تنفيذ اختبارات دورية لنقاط الضعف انطلاقا من خارج الشبكة.	ك	٣٢	٤١	٢٨	٤		١٠٥	٣.٩٦	٠.٨٤	٣٩
		%	٣٠.٥	٣٩.٠	٢٦.٧	٣.٨		%١٠٠			
٣٥.	استخدام تشفير لقواعد البيانات.	ك	٤٠	٤٦	١٨	١		١٠٥	٤.١٩	٠.٧٥	١٢
		%	٣٨.١	٤٣.٨	١٧.١	١		%١٠٠			
٣٦.	استخدام خاصية اتصال الشبكة الافتراضية (VPN).	ك	٤٨	٣١	٢٦			١٠٥	٤.٢١	٠.٨٢	١١
		%	٤٥.٧	٢٩.٥	٢٤.٨			%١٠٠			
٣٧.	استخدام نظام لإدارة الأحداث (Logs) في جميع خوادم وأجهزة الشبكة.	ك	٣٣	٤٩	٢٣			١٠٥	٤.١٠	٠.٧٣	٢٠
		%	٣١.٤	٤٦.٧	٢١.٩			%١٠٠			
٣٨.	توفير مركز بيانات (Data Center) بديل لاستخدامه عند الطوارئ.	ك	٤٤	٣٠	٢٦	٥		١٠٥	٤.٠٨	٠.٩٣	٢٤
		%	٤١.٨	٢٨.٦	٢٤.٨	٤.٨		%١٠٠			
٣٩.	تجهيز الوسيط (Proxy) بخدمة توليد التقارير وتحليلها.	ك	٣٠	٥٧	١٦	٢	-	١٠٥	٤.٠٨	٠.٧٨	٢٣
		%	٢٨.٦	٥٤.٣	١٥.٢	١.٩		%١٠٠			
٤٠.	توفير إجراءات مكتوبة ومعتمدة توضح ما يلزم لتنفيذ أعمال الحماية.	ك	٤٢	٣٦	٢٥	٢		١٠٥	٤.١٢	٠.٨٤	١٧
		%	٤٠.٠	٣٤.٣	٢٣.٨	١.٩		%١٠٠			
٤١.	توفير موظف واحد على الأقل يقوم بإدارة أجهزة الحماية وتحديثها.	ك	٤٣	٣٣	٢٣	٦		١٠٥	٤.٠٨	٠.٩٣	٢٢
		%	٤١.٠	٣١.٤	٢١.٩	٥.٧		%١٠٠			
٤٢.	توفير موظف واحد على الأقل يقوم بإدارة برامج الحماية وتحديثها.	ك	٤٣	٢٩	٢٣	٨		١٠٣	٤.٠٤	٠.٩٨	٣٠
		%	٤١.٠	٢٧.٦	٢١.٩	٧.٦		%٩٨.١			
٤٣.	تأمين بديل واحد على الأقل لكل موظف يعمل في مجال الحماية.	ك	٤٦	٢٩	٢١	٨		١٠٤	٤.٠٩	٠.٩٨	٢١
		%	٤٣.٨	٢٧.٦	٢٠.٠	٧.٦		%٩٩			
٤٤.	توظيف أشخاص مناسبين من حيث المؤهل والخبرة بنسبة ٩٠% على الأقل.	ك	٣٨	٣٨	٢١	٨		١٠٥	٤.٠١	٠.٩٤	٣٥
		%	٣٦.٢	٣٦.٢	٢٠.٠	٧.٦		%١٠٠			

٤٥.	تصميم أو توفير برنامج إدارة الحماية من جميع جوانبها.	ك	٤٦	٣٦	٢٠	٣		١٠٥	٤.١٩	٠.٨٥	١٣
		%	٤٣.٨	٣٤.٣	١٩.٠	٢.٩		%١٠٠			
٤٦.	تأمين جهاز احتياطي لجدار الحماية والموجه والوسيط و أجهزة الخادم.	ك	٦٠	٢٧	١٣	٥		١٠٥	٤.٣٥	٠.٨٨	٣
		%	٥٧.١	٢٥.٧	١٢.٤	٤.٨		%١٠٠			
٤٧.	توفير إدارة خاصة بأمن المعلومات.	ك	٥٦	١٥	١٩	٥	٩	١٠٤	٤.٠٠	١.٣١	٣٦
		%	٥٣.٣	١٤.٣	١٨.١	٤.٨	٨.٦	%٩٩.١			
٤٨.	جعل إدارة أمن المعلومات تابعة مباشرة لرئيس أو مدير المؤسسة.	ك	٤٦	٣١	١٧	٩	٢	١٠٥	٤.٠٥	١.٠٦	٢٨
		%	٤٣.٨	٢٩.٥	١٦.٢	٨.٦	١.٩	%١٠٠			
٤٩.	اشتراط توفر المهارات المناسبة لمستخدمي الحاسب الآلي.	ك	٤٢	٣٣	٢٣	٦	١	١٠٥	٤.٠٤	٠.٩٧	٣١
		%	٤٠.٠	٣١.٤	٢١.٩	٥.٧	١.٠	%١٠٠			
٥٠.	عقد دورات تدريب للتوعية في أمن المعلومات والحماية.	ك	٤٢	٣٥	٢٥	٣	–	١٠٥	٤.٠٨	٠.٩٥	٢٥
		%	٤٠.٠	٣٣.٣	٢٣.٨	٢.٩	–	%١٠٠			
٥١.	توفير خدمة الاتصال البعيد فقط للأفراد المعتمدين من الإدارة.	ك	٤٢	٣٧	٢٣	٢	١	١٠٥	٤.١١	٠.٨٨	١٨
		%	٤٠.٠	٣٥.٢	٢١.٩	١.٩	١.٠	%١٠٠			
٥٢.	توفير نظام لحماية البريد الالكتروني من الفيروسات والبريد الدعائي (Spam).	ك	٥٢	٣٦	١٢	٥	–	١٠٥	٤.٢٩	٠.٨٥	٥
		%	٤٩.٥	٣٤.٣	١١.٤	٤.٨	–	%١٠٠			
٥٣.	تحديث نظام تشغيل أجهزة الشبكة بشكل دوري.	ك	٥٩	١٩	١٨	٩	–	١٠٥	٤.٢٢	١.٠٢	١٠
		%	٥٦.٢	١٨.١	١٧.١	٨.٦	–	%١٠٠			
٥٤.	إتاحة استخدام خاصية التحقق من الصحة في جدار الحماية.	ك	٤٣	٤٠	١٨	٣	١	١٠٥	٤.١٥	٠.٨٧	١٥
		%	٤١.٠	٣٨.١	١٧.١	٢.٨	١.٠	%١٠٠			
٥٥.	توفير سياسة خاصة بكلمات المرور وتطبيقها.	ك	٥٥	٣٦	١٢	٢	–	١٠٥	٤.٣٧	٠.٧٦	٢
		%	٥٢.٤	٣٤.٣	١١.٤	١.٩	–	%١٠٠			
٥٦.	تدريب المستفيدين من موارد شبكة المعلومات.	ك	٤٧	٣٦	١٦	٤	٢	١٠٥	٤.١٦	٠.٩٥	١٤
		%	٤٤.٨	٣٤.٣	١٥.٢	٣.٨	١.٩	%١٠٠			
٥٧.	توفير برنامج للتحكم بمنافذ الحاسبات ومشغلات الوسائط القابلة	ك	٣٨	٤٣	١٥	٧	٢	١٠٥	٤.٠٣	٠.٩٨	٣٣
		%	٣٦.٢	٤١.٠	١٤.٢	٦.٧	١.٩	%١٠٠			

	للإزالة .										
.٥٨	زيادة الاعتماد على أنظمة تشغيل أقل تأثرا بالفيروسات (يونكس، لينوكس..)	ك	٢٤	٣٦	٣٠	٩	٦	١٠٥	٣.٦٠	١.١١	٤٤
		%	٢٢.٩	٣٤.٢	٢٨.٦	٨.٦	٥.٧	%١٠٠			
.٥٩	تقليل الاعتماد على نظام تشغيل مايكروسوفت كونه الأكثر تأثرا بالفيروسات.	ك	٢٧	٣٢	١٩	٢١	٦	١٠٥	٣.٥٠	١.٢٣	٤٥
		%	٢٥.٧	٣٠.٥	١٨.١	٢٠.٠	٥.٧	%١٠٠			
	المتوسط العام للجزء الثاني من المحور الخامس								٤.٠٩	٠.٥٥	

يوضح الجدول (٤/١٨) درجات الأولوية للتدابير الوقائية من المخاطر الداخلية والخارجية بخمسة درجات حيث (١) تدل على أقل أولوية و (٥) تدل أعلى أولوية، ويتضمن خمس وأربعون عبارة، توضح درجة الأولوية لتنفيذ التدابير الوقائية من المخاطر الداخلية والخارجية وفقاً لاستجابات أفراد عينة الدراسة.

وحيث أن المقياس المستخدم خماسي وفيه (١) تعني موضوع العبارة عديم الأولوية و(٢) تعني قليل الأولوية و (٣) تعني متوسط الأولوية، و(٤) تعني أولوية عالية و(٥) تعني أولوية عالية جداً. وبناء على ذلك فإن المتوسطات التي تنتمي إلى المجال من (١) إلى (١.٨٠) تشير إلى عديم الأولوية، و المتوسطات التي تنتمي إلى المجال من (١.٨) إلى أقل من (٢.٦٠) تشير إلى قليل الأولوية و المتوسطات التي تنتمي إلى المجال من (٢.٦١) إلى (٣.٤٠) تشير إلى متوسطة الأولوية ، و المتوسطات التي تنتمي إلى المجال من (٣.٤١) إلى (٤.٢٠) تشير إلى أولوية عالية و المتوسطات التي تنتمي إلى المجال من (٤.٢١) إلى (٥) تشير إلى أولوية عالية جداً.

ويتضح من المتوسط العام لعبارات هذا المحور والذي بلغ (٤.٠٩) بانحراف معياري (٠.٥٥) أن أفراد عينة الدراسة يوافقون على أن أولوية اتخاذ التدابير اللازمة لتجنب المخاطر الداخلية والخارجية التي يمكن أن تتعرض لها شبكات مؤسساتهم تحتاج إلى أولوية عالية.

ويمكن إبراز أهم النتائج في نقاط مرتبة حسب الأهمية كما يلي:

١ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (١) وهي " قفل مركز البيانات (غرفة أجهزة الخادم وأجهزة الشبكة) بحيث لا يدخلها إلا المتخصصون ممن لديهم ترخيص بالدخول " (٤.٥٦) بانحراف معياري (٠.٨٠).

٢ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٢) وهي " توفير سياسة خاصة بكلمات المرور وتطبيقها " (٤.٣٧) بانحراف معياري (٠.٧٦).

٣ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٣) وهي " تأمين جهاز احتياطي لجدار الحماية والموجه والوسيط و أجهزة الخادم " (٤.٣٥) بانحراف معياري (٠.٨٨).

٤ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٤) وهي " تجهيز مركز البيانات بحساسات الحرارة والحركة ونظام الإطفاء والإنذار " (٤.٣١) بانحراف معياري (٠.٩٨).

٥ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٥) وهي " توفير نظام لحماية البريد الالكتروني من الفيروسات والبريد الدعائي (Spam)." (٤.٢٩) بانحراف معياري (٠.٨٥).

٦ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٦) وهي " تنفيذ اختبارات دورية لنقاط الضعف انطلاقا من داخل الشبكة " (٤.٢٩) بانحراف معياري (٠.٩٢).

٧ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٧) وهي " إبعاد وسائط النسخ لاحتياطي ووسائط التخزين عن أماكن تسرب المياه " (٤.٢٩) بانحراف معياري (٠.٧٨).

٨ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٨) وهي " عمل النسخ الاحتياطي والاسترجاع الآلي يومياً " (٤.٢٦) بانحراف معياري (٠.٨٤).

٩ - بلغ متوسط العبارة التي جاءت في الترتيب رقم (٩) وهي " وضع وسائط النسخ الاحتياطي في خزائن مضادة للصدمات والحريق " (٤.٢٣) بانحراف معياري (٠.٩٥).

١٠ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (١٠) وهي " تحديث نظام تشغيل أجهزة الشبكة بشكل دوري " (٤.٢٢) بانحراف معياري (١.٠٢).

١١ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (١١) وهي " استخدام خاصية اتصال الشبكة الافتراضية (VPN)." (٤.٢١) بانحراف معياري (٠.٨٢).

١٢ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (١٢) وهي " تنفيذ اختبارات دورية لنقاط الضعف انطلاقا من خارج الشبكة " (٤.١٩) بانحراف معياري (٠.٧٥).

١٣ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (١٣) وهي " تصميم أو توفير برنامج إدارة الحماية من جميع جوانبها " (٤.١٩) بانحراف معياري (٠.٨٥).

١٤ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (١٤) وهي " تدريب المستفيدين من موارد شبكة المعلومات " (٤.١٦) بانحراف معياري (٠.٩٥).

١٥ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (١٥) وهي " إتاحة استخدام خاصية التحقق من الصحة في جدار الحماية " (٤.١٥) بانحراف معياري (٠.٨٧).

١٦ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (١٦) وهي " تدريب كل الموظفين على أمن المعلومات كل حسب واجباته الوظيفية " (٤.١٥) بانحراف معياري (٠.٨٦).

١٧ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (١٧) وهي " توفير إجراءات مكتوبة ومعتمدة توضح ما يلزم لتنفيذ أعمال الحماية" (٤.١٢) بانحراف معياري (٠.٨٤).

١٨ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (١٨) وهي " توفير خدمة الاتصال البعيد فقط للأفراد المعتمدين من الإدارة " (٤.١١) بانحراف معياري (٠.٨٨).

١٩ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (١٩) وهي " تركيب برامج مخصصة لمراقبة استخدام المستفيدين " (٤.١١) بانحراف معياري (٠.٨٧).

٢٠ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٢٠) وهي " استخدام نظام لإدارة الأحداث (Logs) في جميع خوادم وأجهزة الشبكة " (٤.١٠) بانحراف معياري (٠.٧٣).

٢١ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٢١) وهي " تأمين بديل واحد على الأقل لكل موظف يعمل في مجال الحماية " (٤.٠٩) بانحراف معياري (٠.٩٨).

٢٢ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٢٢) وهي " توفير موظف واحد على الأقل يقوم بإدارة أجهزة الحماية وتحديثها " (٤.٠٨) بانحراف معياري (٠.٩٣).

٢٣ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٢٣) وهي " تجهيز الوسيط (Proxy) بخدمة توليد التقارير وتحليلها " (٤.٠٨) بانحراف معياري (٠.٧٨).

٢٤ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٢٤) وهي " استخدام توفير مركز بيانات (Data Center) بديل لاستخدامه عند الطوارئ " (٤.٠٨) بانحراف معياري (٠.٩٣).

٢٥ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٢٥) وهي " عقد دورات تدريب للتوعية في أمن المعلومات والحماية " (٤.٠٨) بانحراف معياري (٠.٩٥).

٢٦ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٢٦) وهي " تجهيز مركز البيانات بآلية تسجيل للداخلين بالاسم والوقت وسبب الدخول " (٤.٠٧) بانحراف معياري (١.٠٠).

٢٧ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٢٧) وهي " توفير خطة طوارئ واضحة ومعتمدة " (٤.٠٦) بانحراف معياري (١.١٠).

٢٨ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٢٨) وهي جعل إدارة أمن المعلومات تابعة مباشرة لرئيس أو مدير المؤسسة" (٤.٠٥) بانحراف معياري (١.٠٦).

٢٩ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٢٩) وهي " توفير مراقبة داخلية باستخدام كاميرات تلفزيونية مع التسجيل " (٤.٠٥) بانحراف معياري (١.٠٠).

٣٠ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٣٠) وهي " توفير موظف واحد على الأقل يقوم بإدارة برامج الحماية وتحديثها " (٤.٠٤) بانحراف معياري (٠.٩٨).

٣١ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٣١) وهي " اشتراط توفر المهارات المناسبة لمستخدمي الحاسب الآلي " (٤.٠٤) بانحراف معياري (٠.٩٧).

٣٢ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٣٢) وهي " السعي للتوصل إلى اتفاقيات تعاون مع المتخصصين في الحماية " (٤.٠٣) بانحراف معياري (٠.٩٤).

٣٣ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٣٣) وهي " توفير برنامج للتحكم بمنافذ الحاسبات ومشغلات الوسائط القابلة للإزالة " (٤.٠٣) بانحراف معياري (١.١١).

٣٤ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٣٤) وهي " اختبار خطة الطوارئ " (٤.٠٢) بانحراف معياري (٠.٨٢).

٣٥ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٣٥) وهي " توظيف أشخاص مناسبين من حيث المؤهل والخبرة بنسبة ٩٠% على الأقل " (٤.٠١) بانحراف معياري (٠.٩٤).

٣٦ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٣٦) وهي " توفير إدارة خاصة بأمن المعلومات " (٤.٠٠) بانحراف معياري (١.٣١).

٣٧ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٣٧) وهي " اعتماد ميزانية خاصة بخطة الطوارئ " (٣.٩٧) بانحراف معياري (٠.٩٥).

٣٨ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٣٨) وهي " السعي لمطابقة إجراءات العمل لتتوافق مع معايير دولية (آيزو) تتعلق بالحماية " (٣.٩٧) بانحراف معياري (١.٠١).

٣٩ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٣٩) وهي " تنفيذ اختبارات دورية لنقاط الضعف انطلاقا من خارج الشبكة " (٣.٩٦) بانحراف معياري (٠.٨٤).

٤٠ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٤٠) وهي " إتلاف وسائط التخزين والنسخ الاحتياطي المنتهية الصلاحية " (٣.٩٥) بانحراف معياري (١.٠٩).

٤١ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٤١) وهي " تطبيق التشفير على وسائط النسخ الاحتياطي" (٣.٩٣) بانحراف معياري (١.١٠).

٤٢ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٤٢) وهي " إعداد خطة للتراجع (Rollback) تطبق في حالة عدم نجاح خطة الطوارئ " (٣.٩٣) بانحراف معياري (١.٢٠).

٤٣ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٤٣) وهي توفير حراسة عند بوابات مركز البيانات على مدار الساعة" (٣.٧٧) بانحراف معياري (٠.٩٨).

٤٤ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٤٤) وهي "زيادة الاعتماد على أنظمة تشغيل أقل تأثرا بالفيروسات (يونكس، لينوكس..) " (٣.٦٠) بانحراف معياري (١.١١).

٤٥ -بلغ متوسط العبارة التي جاءت في الترتيب رقم (٤٥) وهي " تقليل الاعتماد على نظام تشغيل مايكروسوفت كونه الأكثر تأثرا بالفيروسات " (٣.٥٠) بانحراف معياري (١.٢٣).

٤-٣ الفروق والدلالات الإحصائية

٤-٣-١ الفروق والدلالات الإحصائية لتوفر الأجهزة والبرامج ومدى تطبيق الإعدادات والتحديثات.

قام الباحث بحساب الفروق في المتوسطات بين توفر الأجهزة والبرامج المستخدمة لحماية الشبكات لعينة الدراسة وبين مدى تطبيق الإعدادات والتحديثات المناسبة على تلك الأجهزة والبرامج. وفق الجدول رقم (٤/١٩) كما يلي:

الجدول رقم (٤/١٩)

الفروق في المتوسطات بين توفر الأجهزة وبين مدى تطبيق الإعدادات والتحديثات

المتغير	المتوسط	الانحراف المعياري	n	قيمة (T)	درجة الحرية	قيمة (P) **
توفر الأجهزة والبرامج المستخدمة	٢.٢٩٧	٠.٥٠١	١٠٥	٧.٤٢٢	١٠٤	٠.٠٠٠١

مدى تطبيق الإعدادات والتحديثات	٢.٠٢٦	٠.٣٨٦				

** دال عندما تكون قيمة P أقل من ٠.٠١

يتضح من الجدول (٤/١٩) أن P=0.0001 ويدل ذلك على وجود فروق ذات دلالة إحصائية بين توفر الأجهزة والبرامج التي تستخدم في حماية الشبكات وبين تطبيق الإعدادات وتثبيت التحديثات لتلك الأجهزة والبرامج، حيث بلغ متوسط توفر الأجهزة والبرامج ٢.٢٩٧ ومتوسط تطبيق الإعدادات وتثبيت التحديثات ٢.٠٢٦ وذلك لصالح توفر الأجهزة والبرامج ويدل ذلك على عدم اكتمال الإعداد والتحديث للأجهزة والبرامج التي توفرها المؤسسات ويعود ذلك إلى عوامل متعددة أهمها كما في الجدول (٤/١٥):

أ. عدم توفير مراجع يقوم بتدقيق السياسات الأمنية حيث أن ٥٦.٢% من أفراد عينة الدراسة لا يوجد مدقق (Security Auditor) واحد على الأقل يراجع تنفيذ السياسات الأمنية.

ب. عدم وجود تقدير لأعمال الحماية حيث أن ٥١.٤% من أفراد عينة الدراسة لا تثمن مؤسساتهم أعمال الحماية بتقديم المكافآت أو العلاوات أو شهادات التقدير.

ت. النقص في تدريب القائمين على إدارة تلك الأجهزة حيث أن ٤٩.٥% من أفراد العينة لا تقوم مؤسستي بابتعاثهم لحضور ندوات/مؤتمرات تتعلق بالحماية وأمن المعلومات.

ث. عدم توفير أخصائي أمن معلومات حيث أن ٤٩.٥% من أفراد العينة لا تحوي مؤسساتهم وظيفة بمسمى ضابط أمن المعلومات (Security Officer).

ج. عدم كفاية التدريب حيث يرى ٤٧.٦% من أفراد العينة أن التدريب الذي أحصل عليه من مؤسستي كاف لتأدية عملهم.

ح. عدم وجود مسميات وظيفية مرفقة بمهام وواجبات حيث أن ٤٣.٨% من أفراد العينة لا يوجد في مؤسساتهم مسميات وظيفية للوظائف المتعلقة بالحماية في إدارة تقنية المعلومات مرفق بالمهام والواجبات والمسؤوليات والصلاحيات لكل وظيفة.

خ. عدم تعيين مدراء متخصصون حيث أن ٤٣.٨% من أفراد العينة يرأسهم مدراء غير متخصصين في إحدى مجالات تقنية المعلومات.

د. تعيين مدراء غير متخصصين لإدارات تقنية المعلومات حيث أن ٣٨.١% من أفراد عينة الدراسة لديهم مدير إدارة تقنية المعلومات غير متخصص في إحدى مجالات تقنية المعلومات

ذ. عدم توافق المؤهلات العلمية مع متطلبات أعمال الحماية حيث أن ٣٣.٣% من أفراد العينة لا يتناسب المؤهل العلمي للعاملين في مجال الحماية في مؤسساتهم مع مسميات وظائفهم.

ر. كثرة مغادرة موظفي الحماية لوظائفهم حيث أن ٣٣.٣% من أفراد العينة تتكرر مغادرة الموظفين في مجال الحماية والشبكات لوظائفهم رغبة بفرص أفضل.

٤-٣-٢ الفروق والدلالات الإحصائية لنقاط الضعف وأولويات تدابير إزالتها.

وقد قام الباحث بحساب الفروق في المتوسطات بين درجة خطورة نقاط الضعف التي يمكن أن تُستغل لاختراق شبكات الحاسب لعينة الدراسة وبين التدابير الوقائية المتخذة لتلافي نقاط الضعف. وفق الجدول رقم (٤/٢٠) كما يلي:

الجدول رقم (٤/٢٠)

الفروق في المتوسطات بين درجة خطورة نقاط الضعف وبين التدابير الوقائية لتلافي نقاط الضعف

المتغير	المتوسط	الانحراف المعياري	n	قيمة (T)	درجة الحرية	قيمة (P) *
درجة خطورة نقاط الضعف	٤.١٨	٠.٦٦	١٠٥	٢.٤٧٤	١٠٤	٠.٠١٥
التدابير الوقائية لتلافي نقاط الضعف	٤.٠٨	٠.٥٥				

* دال عندما تكون قيمة P أقل من ٠.٠٥

يتضح من الجدول (٤/٢٠) أن P=0.015 هي أقل من ٠,٠٥ ويدل ذلك على وجود فروق ذات دلالة إحصائية بين درجة خطورة نقاط الضعف التي يمكن أن تُستغل لاختراق شبكات الحاسب وبين التدابير الوقائية المتخذة لتلافي نقاط الضعف، حيث بلغ متوسط درجة خطورة نقاط الضعف ٤.١٨ ومتوسط تدابير تلافي نقاط الضعف، ٤.٠٨ وذلك لصالح درجة خطورة نقاط الضعف ويدل ذلك على عدم اكتمال التدابير الوقائية التي تتخذها المؤسسات التعليمية لتلافي نقاط الضعف ويعود ذلك إلى عوامل متعددة أهمها :

أ. عدم توفير مراجع يقوم بتدقيق السياسات الأمنية حيث أن ٥٦.٢% من أفراد عينة الدراسة لا يوجد مدقق (Security Auditor) واحد على الأقل يراجع تنفيذ السياسات الأمنية.

ب. النقص في تدريب القائمين على إدارة تلك الأجهزة حيث أن ٤٩.٥% من أفراد العينة لا تقوم مؤسستي بابتعاثهم لحضور ندوات/مؤتمرات تتعلق بالحماية وأمن المعلومات.

ت. عدم توفير أخصائي أمن معلومات حيث أن ٤٩.٥% من أفراد العينة لا تحوي مؤسساتهم وظيفة بمسمى ضابط أمن المعلومات (Security Officer).

ث. عدم كفاية التدريب حيث يرى ٤٧.٦% من أفراد العينة أن التدريب الذي أحصل عليه من مؤسستي كاف لتأدية عملهم.

ج. عدم وجود مسميات وظيفية مرفقة بمهام وواجبات حيث أن ٤٣.٨% من أفراد العينة لا يوجد في مؤسساتهم مسميات وظيفية للوظائف المتعلقة بالحماية في إدارة تقنية المعلومات مرفق بالمهام والواجبات والمسؤوليات والصلاحيات لكل وظيفة.

ح. عدم تعيين مدراء متخصصون حيث أن ٤٣.٨% من أفراد العينة يرأسهم مدراء غير متخصصين في إحدى مجالات تقنية المعلومات.

خ. تعيين مدراء غير متخصصين لإدارات تقنية المعلومات حيث أن ٣٨.١% من أفراد عينة الدراسة لديهم مدير إدارة تقنية المعلومات غير متخصص في إحدى مجالات تقنية المعلومات

د. عدم توافق المؤهلات العلمية مع متطلبات أعمال الحماية حيث أن ٣٣.٣% من أفراد العينة لا يتناسب المؤهل العلمي للعاملين في مجال الحماية في مؤسساتهم مع مسميات وظائفهم.

ذ. عدم تخصص جميع العاملين بالحماية التخصص بالشبكات حيث يشير الجدول ٤/٥ أن ٤٠% من أفراد العينة متخصصون بالشبكات.

ر. عدم المطابقة مع معايير (الآيزو) حيث يشير الجدول ٤/١٠ أن ٩٢.٣٨% من عينة الدراسة التي لم تنل شهادات مطابقة (آيزو).

٤-٣-٣ الفروق والدلالات الإحصائية للمخاطر الداخلية والخارجية وأولويات منع حدوثها.

قام الباحث بحساب الفروق في المتوسطات بين المخاطر الداخلية والمخاطر الخارجية حسب استجابات عينة الدراسة وبين التدابير المتخذة لتجنب تلك المخاطر وفق الجدول رقم (٤/٢١) كما يلي:

الجدول رقم (٤/٢١)

الفروق في المتوسطات بين المخاطر الداخلية والمخاطر الخارجية

وبين التدابير المتخذة لتجنب تلك المخاطر

المتغير	المتوسط	الانحراف المعياري	n	قيمة (T)	درجة الحرية	قيمة (P) *
المخاطر الداخلية والخارجية	٤.٢٩	٠.٥٥٧	١٠٥	٣.٣٨	١٠٤	٠.٠٠١

التدابير المتخذة لتجنب تلك المخاطر	٤.٠٩	٠.٥٥٤				

* دال عندما تكون قيمة P أقل من ٠.٠١

يتضح من الجدول (٤/٢١) أن P=0.001 هي أقل من ٠,٠١ ويدل ذلك على وجود فروق ذات دلالة إحصائية بين المخاطر الداخلية والخارجية وبين التدابير المتخذة لتجنب تلك المخاطر ، حيث بلغ متوسط المخاطر الداخلية مع المخاطر الخارجية ٤.٢٩ ومتوسط تدابير تجنب تلك المخاطر ، ٤.٠٩ وذلك لصالح المخاطر الداخلية والخارجية ويدل ذلك على عدم اكتمال التدابير الوقائية التي تتخذها المؤسسات التعليمية لتجنب المخاطر الداخلية والمخاطر الخارجية ويعود ذلك إلى عوامل متعددة أهمها:

أ. ٩٢.٣٨% من عينة الدراسة المؤسسات التي لم تنل شهادات آيزو حسب الاستجابات المبينة بالجدول رقم (٤/١٠) .

ب. ٥٠.٤٨% من عينة الدراسة لا توفر مؤسساتهم نظام متكامل مخصص لإدارة قضايا أمن المعلومات من جميع الجوانب حسب الاستجابات المبينة بالجدول رقم (٤/١١) .

ت. ٥٦.٣٩% من عينة الدراسة يستطيع مدير نظام تشغيل الشبكة لديهم الدخول إلى جميع موارد الشبكة بصلاحيات كاملة الاستجابات المبينة بالجدول رقم (٤/١٢).

ث. ٦٢.٨٦% من عينة الدراسة لا يتوفر لديهم سياسة للحماية حسب الاستجابات المبينة بالجدول رقم (٤/١٤).

ج. ٥٤.٢٩% من عينة الدراسة خبرتهم قليلة بالحماية حسب الاستجابات المبينة بالجدول رقم (٤/١٤).

ح. ٥١.٤% من عينة الدراسة لا يقومون بتنفيذ اختبار دوري لكشف نقاط الضعف بدءا من خارج الشبكة حسب الاستجابات المبينة بالجدول رقم (٤/١٤).

خ. ٥٢.٤% من عينة الدراسة لا يقومون بمراجعة محاولات الدخول إلى النظام وخصوصا من داخل الشبكة حسب الاستجابات المبينة بالجدول رقم (٤/١٤).

د. ٥٥.٢% من عينة الدراسة لا يوجد في مؤسساتهم قسم/إدارة/وحدة تحت مسمى أمن المعلومات أو أمن الشبكة أو ما شابه ذلك حسب الاستجابات المبينة بالجدول رقم (٤/١٥).

ذ. ٥٥.٢% من عينة الدراسة يتم في مؤسساتهم تبديل الموظفين العاملين بالحماية باستمرار بمبادرة من الإدارة حسب الاستجابات المبينة بالجدول رقم (٤/١٥).

ر. ٥٦.٢% من عينة الدراسة لا يوجد لديهم مدقق (Security Auditor) واحد على الأقل يراجع تنفيذ السياسات الأمنية حسب الاستجابات المبينة بالجدول رقم (٤/١٥).

ز. ٥١.٤% من عينة الدراسة لا تثمن مؤسساتهم أعمال الحماية بتقديم المكافآت أو العلاوات أو شهادات التقدير حسب الاستجابات المبينة بالجدول رقم (٤/١٥).

س. ٥١.٤% من عينة الدراسة لا يتوفر في مؤسساتهم إجراء تسمية الأصول المعلوماتية (Information Assets) وتسجيله على الوسائط المعلوماتية حسب الاستجابات المبينة بالجدول رقم (٤/١٦).

ش. ٥٢.٤% من عينة الدراسة لا يوجد لديهم نظام لإدارة وثائق الإجراءات يتم تحديثه باستمرار.

ص. ٢٩.٥% من عينة الدراسة يوجد لديهم صعوبات تدريبية تعترض تنفيذ إجراءات إدارة نظم أمن المعلومات.

ض. ٢٢.٩% من عينة الدراسة يوجد لديهم صعوبات مالية تعترض تنفيذ إجراءات حماية شبكة الحاسب.

ط. ٢٨.٦% من عينة الدراسة يوجد لديهم صعوبات إدارية تعترض تنفيذ إجراءات حماية شبكة الحاسب.

ظ. ٥٨% من عينة الدراسة لا يتوفر في مؤسساتهم إجراء إتلاف الأصول المعلوماتية (Information Assets) المنتهية الصلاحية.

ع. ٥٢.٤% من عينة الدراسة لا تتوفر لديهم وثيقة مكتوبة تتضمن خطة طوارئ خاصة بتقنية المعلومات.

غ. ٥٥.٢% من عينة الدراسة لا تخصص مؤسساتهم ميزانية لخطة الطوارئ.

ف. ٥٧.١% من عينة الدراسة لا يحددون في خطة الطوارئ مدة زمنية تبين الحد الـــزمني الأدنى لإعادة تشغيل النظام.

٤-٣-٤ الفروق والدلالات الإحصائية بين محاور الدراسة وفقاً للمتغيرات الشخصية والوظيفية

١ الفروق وفق الجنس:

هل هناك فروق ذات دلالة إحصائية في محاور الدراسة تبعاً لاختلاف الجنس؟

للإجابة على هذا السؤال تم تنفيذ اختبار (ت) T-Test ويظهر فيه المتغيرات التابعة وهي نقاط الضعف وتدابير إزالتها، والهياكل التنظيمية ، والإجراءات ، والمخاطر الداخلية والخارجية وتدابير إزالتها. والمتغير المستقل (الجنس) وله حالتان ذكر وأنثى.

جدول رقم (٤/٢٢)

اختبار (t) للفروق وفق الجنس

المتغير التابع	المتغير المستقل	n	المتوسط	الانحراف المعياري	قيمة (T)*	درجات الحرية	قيمة (P) **
نقاط الضعف	ذكر	٩٠	٤.١٦٦	٠.٧٠٥	-٠.٦٠٣	١٠٣	٠.٥٤٨
	أنثى	١٥	٤.٢٧٨	٠.٣٢٩			
تدابير إزالة نقاط الضعف	ذكر	٩٠	٤.٠٧٦	٠.٥٩٣	-٠.٤٦٤	١٠٣	٠.٦٤٤
	أنثى	١٥	٤.١٤٨	٠.٢٥٥			
الهياكل التنظيمية	ذكر	٩٠	١.٩٦٢	٠.٣٤٢	٢.٨٨	١٠٣	٠.٠٠٥
	أنثى	١٥	١.٧٠٤	٠.١١٨			
الإجراءات	ذكر	٩٠	١.٩٧٦	٠.٤١٨	٢.٠٢٠	١٠٣	٠.٠٤٦
	أنثى	١٥	١.٦٥٣	٠.١٩١			
المخاطر الداخلية والخارجية	ذكر	٩٠	٤.٢٧٩	٠.٥٩٤	-٠.٩٣١	١٠٣	٠.٣٥٤
	أنثى	١٥	٤.٤٢٣	٠.١٩٣			
تدابير تجنب المخاطر	ذكر	٩٠	٤.٠٧٦	٠.٥٩٣	-٠.٥٥٩	١٠٣	٠.٥٧٧
	أنثى	١٥	٤.١٤٨	٠.٢٥٦			

** دال عندما تكون قيمة P أقل من ٠.٠٥

ويظهر من بيانات الجدول رقم (٤/٢٢) أن متوسط استجابات الذكور قد وصل إلى (١.٩٦٢) فيما وصل متوسط استجابات الإناث (١.٧٠٤) مما يعني وجود فروق جوهرية في الهياكل التنظيمية لصالح الذكور.

ويظهر من بيانات الجدول رقم (٤/٢٢) أيضاً أن متوسط استجابات الذكور قد وصل إلى (١.٩٧٦) فيما وصل متوسط استجابات الإناث (١.٦٥٣) مما يعني وجود فروق جوهرية في الإجراءات لصالح الذكور.

٢ تحليل التباين الأحادي (الأنوفا) للمتغيرات الشخصية مع المحاور المختلفة

الجدول رقم (٤/٢٣)

فروق المتوسطات في محاور الدراسة تبعا لاختلاف الخبرة

المحور	مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة ف	قيمة p (*)
الهياكل التنظيمية	بين المجموعات	٠.١٠١	٢	٠.٠٥٠	٠.٤٥٢	٠.٦٣٨
	داخل المجموعات	١١.٣٦٣	١٠٢	٠.١١١		
	المجموع	١١.٤٦٤	١٠٤			
الإجراءات	بين المجموعات	٠.٢٤١	٢	٠.١٢٠	٠.٧٤٦	٠.٤٧٧
	داخل المجموعات	١٦.٤٧٨	١٠٢	٠.١٦٢		
	المجموع	١٦.٧١٩	١٠٤			
المخاطر الداخلية والخارجية	بين المجموعات	٠.٤٨٨	٢	٠.٠٧١	٠.٢٢٥	٠.٧٩٩
	داخل المجموعات	٣٢.٤٦٣	١٠٢	٠.٣١٥		
	المجموع	٣٢.٩٥١	١٠٤			
تدابير تجنب المخاطر	بين المجموعات	٢.٥١٤	٢	١.٢٥٧	٤.٣٤٤	٠.٠١٥ *
	داخل المجموعات	٢٩.٥١٢	١٠٢	٠.٢٨٩		
	المجموع	٣٢.٠٢٥	١٠٤			
نقاط الضعف	بين المجموعات	١.٧٧٦	٢	٠.٨٨٨	٢.٠٥١	٠.١٣٤
	داخل المجموعات	٤٤.١٦٦	١٠٢	٠.٤٣٣		
	المجموع	٤٥.٩٤١	١٠٤			
تدابير إزالة نقاط الضعف	بين المجموعات	١.٤١٤	٢	٠.٧٠٧	٢.٣٣٦	٠.١٠٢
	داخل المجموعات	٣٠.٨٦٧	١٠٢	٠.٣٠٣		
	المجموع	٣٢.٢٨١	١٠٤			

(*) دال عندما تكون قيمة p أقل من ٠.٠٥

يتضح من الجدول رقم (٤/٢٣) بأنه لا توجد فروق ذات دلالة إحصائية تبعاً للخبرة في محاور الهياكل التنظيمية و الإجراءات والمخاطر الداخلية والخارجية ونقاط الضعف وتدابير إزالة نقاط الضعف ما عدا محور تدابير تجنب المخاطر الداخلية والخارجية حيث أنه دال إحصائياً عند مستوى ٠.٠٥ وللتعرف على مصادر الفروق الدالة إحصائياً تم استخدام اختبار (LSD) البُعدي كما يلي:

الجدول رقم (٤/٢٤)

مصادر الفروق في تدابير تجنب المخاطر والتي ترجع إلى اختلاف الخبرة

المحور	الخبرة	n	المتوسط	١	٢	٣
التدابير	١- أقل من ٥ سنوات	٤٣	٤.٢١٨	-	-	-
	٢- من ٥ سنوات إلى أقل من ١٠ سنوات	٣٩	٣.٨٨٩	**	-	-
	٣- من ١٠ سنوات فأكثر	٢٣	٤.١٩١	*	-	-

(*) دال عندما تكون قيمة p أقل من ٠.٠٥

(**) دال عندما تكون قيمة p أقل من ٠.٠١

يظهر من بيانات رقم (٤/٢٤) أنه توجد فروق جوهرية في التدابير لصالح ذوي الخبرة من ٥ سنوات إلى أقل من ١٠ سنوات دالة عند مستوى أقل من ٠.٠٠١، وتوجد فروق جوهرية في التدابير لصالح ذوي الخبرة من ١٠ سنوات فأكثر دالة عند مستوى أقل من ٠.٠٠٥.

الجدول رقم (٤/٢٥)

فروق المتوسطات في محاور الدراسة تبعا لاختلاف الوظيفة

المحور	مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة ف	قيمة p (*)
الهياكل التنظيمية	بين المجموعات	٠.١٤٣	٢	٠.٠٧١	٠.٦٥٥	٠.٥٢٢
	داخل المجموعات	١٠.٨٨٤	١٠٠	٠.١٠٩		
	المجموع	١١.٠٢٧	١٠٢			
الإجراءات	بين المجموعات	٠.١٩٧	٢	٠.٠٩٨	٠.٦١٢	٠.٥٤٤
	داخل المجموعات	١٦.٠٥٣	١٠٠	٠.١٦١		
	المجموع	١٦.٢٥٠	١٠٢			
المخاطر الداخلية والخارجية	بين المجموعات	٠.٠٢٦	٢	٠.٠١٣	٠.٠٤٠	٠.٩٦٠
	داخل المجموعات	٣١.٨٣٥	١٠٠	٠.٣١٨		
	المجموع	٣١.٨٦١	١٠٢			
تدابير تجنب المخاطر	بين المجموعات	٢.٢٧٢	٢	١.١٨٦	٤.١٦٢	٠.٠١٨ *
	داخل المجموعات	٢٨.٤٩٢	١٠٠	٠.٢٨٥		
	المجموع	٣٠.٨٦٤	١٠٢			

نقاط الضعف	بين المجموعات	٤.١٤٩	٢	٢.٠٧٥	٥.٠٩٨	٠.٠٠٨ *
	داخل المجموعات	٤٠.٦٩١	١٠٠	٠.٤٠٧		
	المجموع	٤٤.٨٤٠	١٠٢			
تدابير إزالة نقاط الضعف	بين المجموعات	٤.٣١٤	٢	٢.١٥٧	٨.١٢٧	٠.٠٠١ *
	داخل المجموعات	٢٦.٥٤٠	١٠٠	٠.٢٦٥		
	المجموع	٣٠.٨٤٥	١٠٢			

(*) دال عندما تكون قيمة p أقل من ٠.٠٥

يتضح من الجدول رقم (٤/٢٥) بأنه لا توجد فروق ذات دلالة إحصائية في محاور الهياكل التنظيمية والإجراءات والمخاطر الداخلية والخارجية، وتوجد فروق ذات دلالة إحصائية عند مستوى ٠.٠٥ في المحاور تدابير تجنب والمخاطر الداخلية والخارجية و نقاط الضعف و تدابير إزالة نقاط الضعف وللتعرف على مصادر الفروق الدالة إحصائياً تم استخدام اختبار (LSD) البُعدي كما يلي:

الجدول رقم (٤/٢٦)

مصادر الفروق في تدابير تجنب المخاطر و نقاط الضعف و تدابير إزالة نقاط الضعف والتي ترجع إلى اختلاف الوظيفة

المحور	الخبرة	n	المتوسط	١	٢	٣
تدابير تجنب المخاطر	١-إدارية	١٠	٤.٢٤٢	–	–	–
	٢- فنية	٤٩	٤.١٩٨	–	–	**
	٣- إدارية وفنية	٤٤	٣.٩٠٠	–	**	–
نقاط الضعف	١-إدارية	١٠	٣.٧٠٠	–	**	–
	٢- فنية	٤٩	٤.٣٤٦	**	–	*
	٣- إدارية وفنية	٤٤	٤.٠٧٣	–	*	–
تدابير إزالة نقاط الضعف	١-إدارية	١٠	٣.٧٦١	–	**	–
	٢- فنية	٤٩	٤.٢٨١	**	–	**
	٣- إدارية وفنية	٤٤	٣.٩٠٦	–	–	–

(*) دال عندما تكون قيمة p أقل من ٠.٠٥

(**) دال عندما تكون قيمة p أقل من ٠.٠١

يظهر من بيانات الجدول رقم (٤/٢٦) أنه توجد فروق في تدابير تجنب المخاطر بين استجابات الوظائف الإدارية واستجابات الوظائف الفنية دالة عند مستوى أقل من ٠.٠٠١.

أ – توجد فروق في تدابير تجنب المخاطر بين استجابات الوظائف الفنية واستجابات الوظائف الإدارية دالة عند مستوى أقل من ٠.٠٠١.

ب – توجد فروق في تدابير تجنب المخاطر بين استجابات الوظائف الفنية واستجابات الوظائف الإدارية والفنية دالة عند مستوى أقل من ٠.٠٥.

ت – توجد فروق في نقاط الضعف بين استجابات الوظائف الإدارية واستجابات الوظائف الفنية دالة عند مستوى أقل من ٠.٠٠١.

ث – توجد فروق في نقاط الضعف بين استجابات الوظائف الفنية واستجابات الوظائف الإدارية دالة عند مستوى أقل من ٠.٠٠١.

ج – توجد فروق في نقاط الضعف بين استجابات الوظائف الفنية واستجابات الوظائف الإدارية والفنية دالة عند مستوى أقل من ٠.٠٥.

ح – توجد فروق في نقاط الضعف بين استجابات الوظائف الإدارية والفنية واستجابات الوظائف الفنية دالة عند مستوى أقل من ٠.٠٥.

خ – توجد فروق في تدابير إزالة نقاط الضعف بين استجابات الوظائف الإدارية واستجابات الوظائف الفنية دالة عند مستوى أقل من ٠.٠٠١.

د – توجد فروق في تدابير إزالة نقاط الضعف بين استجابات الوظائف الفنية واستجابات الوظائف الإدارية دالة عند مستوى أقل من ٠.٠٠١.

ذ – توجد فروق في تدابير إزالة نقاط الضعف بين استجابات الوظائف الفنية واستجابات الوظائف الإدارية والفنية دالة عند مستوى أقل من ٠.٠٠١.

الجدول رقم (٤/٢٧)

فروق المتوسطات في محاور الدراسة تبعا لاختلاف العمر

المحور	مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة ف	قيمة p (*)
الهياكل التنظيمية	بين المجموعات	٠.٠٤٠	٢	٠.٠٢٠	٠.١٨٣	٠.٨٣٣
	داخل المجموعات	١٠.٩٨٦	١٠٠	٠.١١٠		
	المجموع	١١.٠٢٧	١٠٢			
الإجراءات	بين المجموعات	٠.٣٥٢	٢	٠.١٧٦	١.١٠٧	٠.٣٣٤
	داخل المجموعات	١٥.٨٩٨	١٠٠	٠.١٥٩		
	المجموع	١٦.٢٥٠	١٠٢			
المخاطر الداخلية والخارجية	بين المجموعات	٠.٠٤٤٠	٢	٠.٢٢٠	٠.٧٠٠	٠.٤٩٩
	داخل المجموعات	٣١.٤٢١	١٠٠	٠.٣١٤		
	المجموع	٣١.٨٦١	١٠٢			
تدابير تجنب المخاطر	بين المجموعات	٠.٥٥٩	٢	٠.٢٧٩	٠.٩٢٢	٠.٤٠١
	داخل المجموعات	٣٠.٣٠٥	١٠٠	٠.٣٠٣		

	المجموع	٣٠.٨٦٤	١٠٢			
نقاط الضعف	بين المجموعات	٣.٨١٠	٢	١.٩٠٥	٤.٦٤٢	٠.٠١٢ *
	داخل المجموعات	٤١.٠٣١	١٠٠	٠.٤١٠		
	المجموع	٤٤.٨٤٠	١٠٢			
تدابير إزالة نقاط الضعف	بين المجموعات	٣.٨٢٤	٢	١.٩١٢	٧.٠٧٤	٠.٠٠١ *
	داخل المجموعات	٢٧.٠٣٠	١٠٠	٠.٢٧٠		
	المجموع	٣٠.٨٤٥	١٠٢			

(*) دال عندما تكون قيمة p أقل من ٠.٠٥

يتضح من الجدول رقم (٤/٢٧) بأنه لا توجد فروق ذات دلالة إحصائية تبعاً لاختلاف العمر في محاور الدراسة ما عدا نقاط الضعف وتدابير إزالتها حيث توجد فروق ذات دلالة إحصائية عند مستوى ٠.٠٥ وللتعرف على مصادر الفروق الدالة إحصائياً تم استخدام اختبار (LSD) البُعدي كما يلي:

الجدول رقم (٤/٢٨)

مصادر الفروق في نقاط الضعف و تدابير إزالة نقاط الضعف والتي ترجع إلى اختلاف العمر

المحور	الخبرة	n	المتوسط	١	٢	٣
نقاط الضعف	١-أقل من ٣٠ سنة	٤٤	٤.٢١٥	–	–	–
	٢- من ٣٠ إلى أقل من ٤٠ سنة	٤٠	٣.٩٦٠	–	–	**
	٣- من ٤٠ سنة فأكثر	١٩	٤.٤٩١	–	**	–
تدابير إزالة نقاط الضعف	١-أقل من ٣٠ سنة	٤٤	٤.٢٠٩	–	**	–
	٢- من ٣٠ إلى أقل من ٤٠ سنة	٤٠	٤.٨٢٩	–	–	**
	٣- من ٤٠ سنة فأكثر	١٩	٤.٢٥٥	–	**	–

(**) دال عندما تكون قيمة p أقل من ٠.٠١

يظهر من بيانات الجدول رقم (٤/٢٨) ما يلي:

أ – توجد فروق في نقاط الضعف بين استجابات الفئة العمرية من ٣٠ إلى أقل من ٤٠ سنة واستجابات الفئة من ٤٠ سنة فأكثر دالة عند مستوى أقل من ٠.٠٠١.

ب –توجد فروق في نقاط الضعف بين استجابات الفئة العمرية من ٤٠ سنة فأكثر واستجابات الفئة من ٣٠ إلى أقل من ٤٠ سنة دالة عند مستوى أقل من ٠.٠٠١.

ت -توجد فروق في تدابير إزالة نقاط الضعف بين استجابات الفئة العمرية أقل من ٣٠ سنة واستجابات الفئة من ٣٠ إلى أقل من ٤٠ سنة دالة عند مستوى أقل من ٠.٠٠١

ث -توجد فروق في تدابير إزالة نقاط الضعف بين استجابات الفئة العمرية من ٣٠ إلى أقل من ٤٠ سنة واستجابات الفئة من ٤٠ سنة فأكثر دالة عند مستوى أقل من ٠.٠٠١

ج -توجد فروق في تدابير إزالة نقاط الضعف بين استجابات الفئة العمرية من ٤٠ سنة فأكثر واستجابات الفئة من ٣٠ إلى أقل من ٤٠ سنة دالة عند مستوى أقل من ٠.٠٠١

الفصل الخامس

خلاصة الدراسة ونتائجها وتوصياتها

٥-١ خلاصة الدراسة

٥-٢ نتائج الدراسة

٥-٣ توصيات الدراسة

٥-٤ مقترحات الدراسة

الفصل الخامس

خلاصة الدراسة ونتائجها وتوصياتها

يتضمن هذا الفصل أربعة عناصر رئيسة وهي: خلاصة الدراسة، وعرض لأهم النتائج التي توصلت إليها الدراسة، والتوصيات والمقترحات التي تمخضت عنها نتائج وذلك في ضوء أهداف الدراسة المتمثلة بحصر الأجهزة والبرامج المستخدمة لحماية الشبكات وطرق إعدادها وتحديثها. و تحديد نقاط الضعف في الشبكات المدروسة وتدابير تقويمها. والتعرف على مشكلات الهياكل التنظيمية في إدارات تقنية المعلومات، وعلاقتها بالوظائف الفنية والإدارية المطبقة في مجال الحماية، للوصول إلى إجراءات عمل مناسبة لتنفيذ سياسات الحماية. وكذلك تحديد سياسات الحماية وإجراءات العمل اللازمة لتحقيق حماية عالية لشبكات المعلومات الرئيسة. بالإضافة إلى حصر المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات المعلومات وحصر التدابير الاحتياطية اللازمة لتجنب تلك المخاطر.

٥-١ خلاصة الدراسة:

اشتملت الدراسة على خمسة فصول بالإضافة إلى المراجع والملاحق. وتضمن الفصل الأول مشكلة الدراسة وتساؤلاتها وفرضياتها وأهدافها وأهميتها وتناول أهم المصطلحات الواردة فيها.

وقد انطلقت فكرة الدراسة من أهمية المعلومات المخزنة في موارد شبكات الحاسب والحاجة الماسة لحماية تلك المعلومات في ضوء الأخطار المتعددة التي تهدد أمن وسلامة الشبكات وما تحويه من معلومات بالإضافة لضرورة تجنب أي توقف مهما كان قصيراً لما له من آثار سلبية اقتصادية ومعنوية على المؤسسات التي تعتمد في تسيير أعمالها على تقنية المعلومات. وذلك بالتعرف على طرق ووسائل حماية الشبكات المستخدمة في المؤسسات التي تستخدم تقنية المعلومات والتعرف على إجراءات الأمان المستخدمة وأساليب إدارة أمن المعلومات ثم تحليلها وبناء على النتائج المستخلصة من التحليل يتم استنتاج توصيات تفيد في تطوير إجراءات الأمان، للوصول إلى أفضل حماية بظروف وصول مرنة لا تسبب تأخير في تعاملات المستفيدين وكذلك تحسين جودة حماية شبكات المعلومات بشكل عام وشبكات المؤسسات التعليمية بشكل خاص.

وطرحت الدراسة تساؤلاً رئيساً تمثل بالسؤال الرئيس التالي: ما هي طرق ووسائل حماية موارد شبكات الحاسب الآلي وانبثقت منه التساؤلات الفرعية التالية:

١. ما الأجهزة والبرامج المستخدمة لحماية الشبكات وما مدى إعدادها وتحديثها.
٢. ما نقاط الضعف التي تُستغل لاختراق شبكات المعلومات وما التدابير الوقائية المتخذة لمنع استغلالها.
٣. ما الهياكل التنظيمية المناسبة لإدارات تقنية المعلومات وما مدى توافق الوظائف المستخدمة في مجال أمن شبكات المعلومات معها.
٤. ما إجراءات العمل المعتمدة لحماية شبكات المعلومات وما مدى إتباعها والعمل بها.
٥. ما التدابير الاحتياطية اللازمة لتجنب المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات المعلومات، وما التدابير الفعلية المتخذة للتغلب على تلك المخاطر.

وبنت الدراسة فرضياتها على تساؤلاتها الفرعية حيث كانت الفرضيات

١. لا توجد فروق ذات دلالة إحصائية بين كمية الأجهزة والبرامج المستخدمة لحماية الشبكات بإعداد وتحديث تلك الأجهزة والبرامج.
٢. لا توجد فروق ذات دلالة إحصائية بين نقاط الضعف التي تُستغل لاختراق شبكات المعلومات وبين التدابير الوقائية المتخذة لمنع استغلال تلك النقاط.
٣. لا توجد علاقة ذات دلالة إحصائية بين الهياكل التنظيمية لإدارات تقنية المعلومات وبين توافق الوظائف المستخدمة في مجال حماية شبكات المعلومات.
٤. لا توجد علاقة ذات دلالة إحصائية بين إجراءات حماية شبكات المعلومات وبين اتباعها والعمل بها.
٥. لا توجد فروق ذات دلالة إحصائية بين التدابير الاحتياطية اللازمة لتجنب المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات المعلومات، وبين التدابير الفعلية المتخذة للتغلب على تلك المخاطر.

وتضمن الفصل الثاني الإطار النظري الذي استعرض المفاهيم العلمية والأسس النظرية لبناء الشبكات وتطرق إلى أهم لبناتها وتناول أجهزة الحماية وبرامجها وأهم الأخطار والهجمات التي تهدد أمن وسلامة محتويات الشبكات وكذلك استعرض أساليب تصميم الشبكات بالشكل الأمثل الذي ينسجم مع وسائل الحماية الحديثة بالإضافة إلى تطرقها لكيفية إعداد عتاد الشبكة وأجهزة حمايتها بهدف الوصول إلى الحل الأمثل للحماية.

وتناول الفصل الثاني أيضاً الدراسات السابقة ذات الصلة بموضوع الدراسة حيث عرض تسع دراسات سابقة منها ست دراسات عربية وأخرى ثلاث أجنبية. وقد صدرت هذه الدراسات في

الفترة (١٩٩٦-٢٠٠٧م) وبين الفصل أن الدراسة الحالية تختلف عن تلك الدراسات، بأنها تتناول موضوع حماية شبكات المعلومات من مفهوم الحماية الشامل في حين أن الدراسات السابقة تناولت موضوع الحماية من زوايا محددة، وقد كانت المؤسسات التعليمية في مدينة الرياض مكاناً لتطبيق أداة الدراسة على مجتمع العاملين في إدارة الشبكات وحمايتها وحل مشكلاها. وقد استفاد الباحث من الدراسات السابقة في تجميع الحلول والتوصيات المتوفرة وكذلك التوصل على حلول وتوصيات لم تلاحظ في الدراسات السابقة ووضع الجميع في إطار شامل يهدف للتوصل إلى حماية قصوى بإجراءات سهلة تؤمن للمستفيد وصول مرن إلى موارد شبكات المعلومات.

وتضمن الفصل الثالث منهج الدراسة وحدودها الزمنية والمكانية حيث حدد زمانها بالنصف الثاني من عام ٢٠٠٩م ومكانها مدينة الرياض بالمملكة العربية السعودية. وتناول مجتمع الدراسة المتمثل بالعاملين في إدارة وحماية شبكات الحاسب الآلي في المؤسسات التعليمية. وتناول أداة الدراسة ومراحل بنائها وصدقها حيث عرضها على عشرة محكمين من المتخصصين في موضوع الدراسة وبين إجراءات تطبيقها وتناول أيضاً الأساليب الإحصائية لمعالجة البيانات وتحليل نتائجها.

وتضمن الفصل الرابع عرض وتحليل الدراسة الميدانية حيث تناول البيانات الديموغرافية لمجتمع الدراسة و عرض النتائج المتعلقة بأسئلة الدراسة.
وتكونت أداة الدراسة من قسمين فالأول وضّح الخصائص الديموغرافية لأفراد مجتمع الدراسة والقسم الثاني عرض خمسة محاور تحاكي التساؤلات الفرعية الخمس، وقد تضمنت جميعاً (١٨٩) عبارة حيث كان نصيب المحور الأول (٤٨) عبارة وحصة المحور الثاني (٢٧) عبارة وحاز المحور الثالث على (٢٨) عبارة وتكون المحور الرابع من (٢٧) عبارة ونال المحور الخامس حصة الأسد حيث تضمن (٥٩) عبارة.
وطبقت أداة الدراسة على العينة التي تكونت من مجموعة من المؤسسات التعليمية التي تعتمد على تقنيات الحاسب الآلي في تسيير معظم أعمالها الأكاديمية والمالية وقد بلغ عدد تلك المؤسسات التي خضعت للدراسة (٧٥) مؤسسة تعليمية أخذت كعينة عشوائية من أصل (٤٢٩) مؤسسة تعليمية في مدينة الرياض،أي ما نسبته ١٧.٥% من مجتمع الدراسة وقد بلغ عدد أفراد العينة الذين خضعت استباناتهم للتحليل (١٠٥) فرداً وقد تم الاكتفاء بهذه العينة نظراً لكبر مجتمع الدراسة وصعوبة الوصول إلى جميع أفراده في الحدود الزمنية للدراسة.
واستخدم الباحث الحاسب الآلي في تحليل البيانات الخاصة بالدراسة برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS) الإصدار ١٥.

واستعرض هذا الفصل نتائج الدراسة وتحليلها وتفسيرها من خلال خمسة تساؤلات غطتها (١٨٩) عبارة وتمحورت التساؤلات حول توفر أجهزة وبرامج الحماية ومدى إعدادها وتحديثها، ونقاط الضعف وتدابير التغلب عليها، وإجراءات الحماية ومدى تطبيقها، والهياكل التنظيمية ومدى توافقها مع متطلبات الحماية، والمخاطر التي يمكن أن تضر بالشبكات ومدى اتخاذ التدابير للوقاية منها.

أما الفصل الخامس فقد تناول خلاصة الدراسة وأهم النتائج التي توصلت إليها. وأهم التوصيات التي اقترحتها للوصول إلى حماية متكاملة لشبكات المعلومات وتمكين المستفيدين من الوصول إلى موارد الشبكات بشكل مرن وسهل دون التأثير على أداء الشبكات من سرعة المعلومات وانسيابها.

٥-٢ نتائج الدراسة :

توصلت الدراسة إلى مجموعة من النتائج أهمها مرتبة تبعاً لتسلسل محاور الدراسة ما يلي:

٥-٢-١الأجهزة والبرامج المستخدمة لحماية الشبكات و مدى استخدام تلك الأجهزة والبرامج ومدى إعدادها وتحديثها.

١ - توفر المؤسسات التي تعتمد في تسيير أعمالها على تقنية المعلومات أجهزة لحماية شبكاتها، ومن أهم تلك الأجهزة وسيط (proxy) لتوزيع خدمة الإنترنت على المستفيدين، وجدران حماية تتوفر فيها إمكانيات التحديث الآلي والاتصال الافتراضي VPN ومكافحة البريد الدعائي وتقسيم الشبكة إلى أجزاء تفوق الثلاثة أجزاء وكشف ومنع الاختراق و تصفية المواقع غير المرغوبة، ويقوم المسؤولون عن إدارة أجهزة الحماية بإعداد وتحديث تلك الأجهزة بشكل جيد ولكن لا يرتقي إلى الحد المطلوب.

٢ - توفر المؤسسات أجهزة شبكات أهمها موزعات مركزية ونقاط شبكة لاسلكية وموجهات ويقوم المسؤولون عن إدارتها بإعدادها وتحديثها بشكل جيد ولكن لا يرتقي إلى الحد المطلوب.

٣ - توفر المؤسسات نظم مكافحة الفيروسات والبريد الدعائي و مراقبة استخدام الإنترنت.

٤ - تستخدم المؤسسات نظم احترافية للنسخ الاحتياطي مع وجود تقصير من قبل المسؤولين عن تشغيلها في وضع سياسات النسخ الاحتياطي ومراجعتها.

٥ – توفر المؤسسات عقوداً للدعم الفني لنظم الحماية من الفيروسات وجدران الحماية.

٦ – يوجد لدى نصف المؤسسات مخططات واضحة لجدران الحماية والخوادم والموجهات، ويقوم المسؤولون عنها بتحديثها دورياً.

٧ – لا توفر المؤسسات نظام متكامل مخصص لإدارة قضايا أمن المعلومات من جميع الجوانب.

٨ – يتم في ثلث المؤسسات إعداد الموزعات لعزل حاسبات المتدربين عن موارد الشبكة.

٩ – يتم في نصف المؤسسات تحديد صلاحيات الوصول للمبرمين وخمسها يحددون صلاحيات وصول مدراء أنظمة التشغيل إلى جميع موارد الشبكة.

١٠ –تستخدم ثلث المؤسسات بيئة تجربة لتثبيت التحديثات قبل اعتمادها في بيئة الإنتاج وبيئة تطوير لبناء وتجربة التطبيقات الجديدة قبل نقلها إلى بيئة الإنتاج.

١١ –تُعِدّ ثلث المؤسسات شبكاتها بحيث لا يتمكن المستخدمون من تثبيت وإزالة أي برنامج في حاسباتهم المكتبية.

١٢ –تقوم ثلث المؤسسات بإعداد لوائح التحكم بالوصول (access control list) في الموجهات.

١٣ –تقوم خمس المؤسسات بإعداد مفاتيح النقاط اللاسلكية.

٥–٢–٢ خطورة نقاط الضعف التي يمكن أن تُستغل لاختراق شبكة الحاسب و اللازمة للتخلص منها وأولويات تدابير إزالة تلك النقاط:

أ. حسب استجابات أفراد عينة الدراسة كانت نقاط الضعف الخطرة جداً كما يلي:

١. عدم تحديث أنظمة تشغيل جدران الحماية بانتظام.

٢. عدم وجود سياسة للحماية.

٣. عدم تحديث خاصية الحماية من الفيروسات في جدران الحماية بانتظام.

٤. عدم تثبيت تحديثات أنظمة تشغيل أجهزة الخادم والحاسبات المكتبية بانتظام.

٥. قلة الخبرة لدى العاملين بالحماية.

ب. حسب استجابات أفراد عينة الدراسة كانت نقاط الضعف الخطرة كما يلي:

١. عدم وجود خاصية كشف ومنع التلصص IPS في جدران الحماية المستخدمة.

٢. أداء بعض الأجهزة ضعيف ولا تستطيع تشغيل مكافح الفيروسات.
٣. وجود كلمات مرور افتراضية في بعض الأجهزة والبرمجيات العاملة بالشبكة.
٤. قلة الكفاءة المهنية عند المستفيدين من موارد الشبكة.
٥. عدم تحديث خاصية الحماية من البريد الدعائي Spam في جدران الحماية.
٦. وجود نظم تشغيل غير مرخصة تعمل في أجهزة الشبكة.
٧. عدم تحديث خاصية تصفية المواقع غير المرغوبة في جدران الحماية.
٨. عدم تحديث مكونات أجهزة الوسيط (Proxy) بانتظام.
ولا يوجد عبارات موضوعها عديم الخطورة أو قليل الخطورة أو متوسط الخطورة.

ت. تدابير إزالة نقاط الضعف ذات الأولوية العالية حسب استجابات أفراد عينة الدراسة هي:
١. تنفيذ اختبار دوري لكشف نقاط الضعف من داخل الشبكة.
٢. استخدام أدوات قياس أداء أجهزة الشبكة.
٣. تزويد وتفعيل خاصية الحماية من البريد الدعائي (Spam) في جدار الحماية.
٤. تزويد وتفعيل خاصية تصفية المواقع غير المرغوب فيها في جدران الحماية.
٥. استخدام قائمة تتضمن المهام اليومية لأعمال الحماية بمتوسط.
ث. لا يوجد تدابير لإزالة نقاط الضعف ذات أولوية متوسطة أو ذات أولوية قليلة ، أو ذات أولوية قليلة جداً وذلك حسب استجابات أفراد عينة الدراسة.

٥-٢-٣ الهياكل التنظيمية المناسبة لمراكز تقنية المعلومات ومدى توافق الوظائف المستخدمة في مجال أمن شبكات المعلومات معها.

أ. الهياكل التنظيمية والوظائف غير المناسبة لمراكز تقنية المعلومات تبعاً استجابات عينة الدراسة:
١ - التدريب كاف لتأدية أعمال الموظفين بالحماية.
٢ - يوجد قسم/إدارة/وحدة تحت مسمى أمن المعلومات أو أمن الشبكة أو ما شابه ذلك.
٣ - تثمن المؤسسات أعمال الحماية بتقديم المكافآت أو العلاوات أو شهادات التقدير
٤ - يوجد موظف واحد على الأقل بمسمى ضابط أمن المعلومات .(Security Officer)
٥ - يتم تبديل الموظفين العاملين بالحماية باستمرار بمبادرة من الإدارة.

٦ – يوجد مدقق (Security Auditor) واحد على الأقل يراجع تنفيذ السياسات الأمنية.

ب. الهياكل التنظيمية والوظائف المناسبة إلى حد ما، لمراكز تقنية المعلومات تبعاً استجابات عينة الدراسة:

١ – يوجد مسؤول (Network Admin) واحد على الأقل لأعمال الكابلات والموزعات.

٢ – يوجد موظف واحد على الأقل يقوم بإدارة أجهزة الحماية.

٣ – الدخل الذي يتقاضاه العاملون بالحماية غير مناسب.

٤ – الدعم الفني لبرامج الحماية من الفيروسات جيد.

٥ – يتم مراعاة التسلسل الإداري في المعاملات الفنية.

٦ – الهيكل التنظيمي لإدارة/مركز تقنية المعلومات مناسب و مواكِب للتطور السريع في تقنية المعلومات.

٧ – توفر المؤسسات عقوداً لتأمين الدعم الفني لأجهزة الحماية يشمل تبديل الجهاز عند اللزوم.

٨ – توفر المؤسسات عقوداً لتأمين الدعم الفني لبرامج الحماية يشمل الحضور لموقع المؤسسة.

٩ – مدير إدارة تقنية المعلومات متخصص في إحدى مجالات تقنية المعلومات.

١٠ –المدير المباشر متخصص في إحدى مجالات تقنية المعلومات.

١١ –تقوم إدارة المؤسسات بتخصيص ميزانية جيدة لتحسين الحماية.

١٢ –المؤهل العلمي للعاملين في مجال الحماية يناسب لمسميات وظائفهم.

١٣ –الدعم الفني الخاص بجدار الحماية.

١٤ –يوجد لجنة لإدارة التعديلات (شبكات وقواعد بيانات وموقع الانترنت).

١٥ –المؤهل العلمي للعاملين في مجال الحماية يناسب لمسميات وظائفهم.

١٦ –تقوم المؤسسات بابتعاث العاملين بالحماية لحضور ندوات/مؤتمرات تتعلق بالحماية وأمن المعلومات.

١٧ –يوجد مسميات وظيفية للوظائف المتعلقة بالحماية في إدارة تقنية المعلومات مرفق بالمهام والواجبات والمسؤوليات والصلاحيات لكل وظيفة.

ت. الهياكل التنظيمية والوظائف المناسبة لمراكز تقنية المعلومات تبعاً استجابات عينة الدراسة:

١ – يوجد هيكل تنظيمي معتمد ومعمم، يتضمن الإدارة/القسم.

٢ – يعاني العاملون بالحماية من ضغط في العمل ويحتاجون لوقت إضافي لإنجاز جميع واجباتهم.

٣ – عدد الموظفين الذين يعملون في مجال الحماية غير كاف.

٤ – يوجد موظف واحد على الأقل يقوم بإدارة برامج الحماية (برامج مكافحة الفيروسات والبريد الدعائي ومراجعة سجلات الأحداث (Events) لأجهزة الشبكة.

٥ – يتم مراعاة التسلسل الإداري في المعاملات الإدارية والمالية.

٥–٢–٤ إجراءات العمل في حماية شبكات المعلومات و مدى تطبيقها والعمل بها.

أ. إجراءات العمل المتوفرة والمطبقة في مؤسسات عينة الدراسة:

١ – يتوفر إجراء تحديث أنظمة التشغيل.

ب. إجراءات العمل المتوفرة والمطبقة إلى حد ما في مؤسسات عينة الدراسة:

٢ – يوجد إجراءات عمل خاصة بإدارة عمليات تحديث التطبيقات والبرمجيات.

٣ – يوجد موظف واحد على الأقل يقوم بإدارة الإجراءات (إنشاءها ، تحديثها، توثيقها).

٤ – يوجد صعوبات تدريبية تعترض تنفيذ إجراءات إدارة نظم أمن المعلومات.

٥ – يوجد صعوبات إدارية تعترض تنفيذ إجراءات حماية شبكة الحاسب.

٦ – تتوفر في المؤسسات سياسة (policy) للنسخ الاحتياطي والاسترجاع.

٧ – يوجد وثيقة توضح طريقة تحديث نظام الحماية من الفيروسات والبرامج الضارة.

٨ – يوجد صعوبات مالية تعترض تنفيذ إجراءات حماية شبكة.

٩ – يوجد وثيقة توضح أمكنة توضع أجهزة وبرامج الحماية.

١٠ –تتوفر سياسة التوريد وتأمين الخدمات من خارج المنظمة.

١١ –يوجد وثيقة توضح خطوات إعداد وتشغيل عمليات النسخ الاحتياطي والاسترجاع.

١٢ –تتوفر في المؤسسات سياسة توظيف الأفراد المناسبين في إدارة تقنية المعلومات.

١٣ –يتم أخذ موافقة لجنة التعديل قبل إجراء أي تعديل في أجهزة وبرامج الحماية.

١٤ -تتوفر سياسة أرشفة وسائط حفظ البيانات.

١٥ -تتوفر سياسة أرشفة وسائط حفظ.

١٦ -توجد خطة تم تدريب المعنيين على تطبيقها لاسترداد النظام في الحالات الطارئة.

١٧ -يوجد في خطة الطوارئ بيان واضح للأنظمة الحرجة.

١٨ -يوجد وثيقة توضح طريقة تحديث جدران الحماية.

١٩ -تتوفر سياسة لتقييم درجة سرية.

٢٠ -تتوفر سياسة للتدريب في تخصصات تقنية المعلومات.

ت. إجراءات العمل غير المتوفرة أو غير المطبقة:

١ - إجراء تسمية الأصول المعلوماتية (Information Assets) وتسجيله على الوسائط المعلوماتية.

٢ - وثيقة مكتوبة تتضمن خطة طوارئ خاصة بتقنية المعلومات.

٣ - نظام لإدارة وثائق الإجراءات يتم تحديثه باستمرار.

٤ - إجراء إتلاف الأصول المعلوماتية (Information Assets) المنتهية الصلاحية.

٥ - خطة طوارئ تتضمن مدة زمنية تبين الحد الزمني الأدنى لإعادة تشغيل النظام.

٦ - ميزانيات خطط الطوارئ.

٥-٢-٥ المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات الحاسب و التدابير الاحتياطية اللازمة لتجنبها.

أ. المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات الحاسب والتي تعد خطر جداً وفقاً لاستجابات عينة الدراسة:

١ - اختراق لتعديل البيانات وتغيرها أو إتلافها.

٢ - اندلاع الحريق.

٣ - التعدي على الكابلات.

٤ - تعديل إعدادات أجهزة الشبكة بطريقة يصعب تعقبها لإطالة فترة الانقطاع.

٥ – حصول إغراق بالمياه بسبب الفيضانات.

٦ – اختراق أجهزة الخادم من داخل المؤسسة (عبث،إساءة استخدام...).

٧ – التعرض لهجوم إرهابي.

٨ – استخدام برامج بغرض التجسس من قبل المستفيدين من داخل المؤسسة.

٩ – الدخول غير المصرح به إلى مركز البيانات وتعطيل عمل أجهزته.

ب. المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات الحاسب والتي تعد خطرة وفقاً لاستجابات عينة الدراسة:

١ – الإصابة بفيروسات مصدرها وسائط التخزين وذواكر الفلاش.

٢ – الإصابة بفيروسات مصدرها الانترنت.

٣ – زيارة مواقع إنترنت غير موثوقة تسمح بتنزيل البرمجيات الضارة.

٤ – سرقة الأجهزة ووسائط التخزين.

٥ – تنزيل برامج غير مصرح بها.

ت. لا توجد في مؤسسات عينة الدراسة وفقاً لاستجابات العينة مخاطر عديم الخطورة، ولا مخاطر قليلة الخطورة ولا متوسطة الخطورة.

٥-٢-٥-٣ تدابير الحماية من المخاطر الداخلية والخارجية

أ. توجد تدابير حماية من المخاطر الداخلية والخارجية تعد ذات أولوية عالية جداً وفقاً لاستجابات عينة الدراسة:

١ – قفل مركز البيانات (غرفة أجهزة الخادم وأجهزة الشبكة) بحيث لا يدخلها إلا المتخصصون ممن لديهم ترخيص بالدخول.

٢ – توفير سياسة خاصة بكلمات المرور وتطبيقها.

٣ – تأمين جهاز احتياطي لجدار الحماية والموجه والوسيط و أجهزة الخادم.

٤ – مركز البيانات بحساسات الحرارة والحركة ونظام الإطفاء والإنذار.

٥ – توفير نظام لحماية البريد الالكتروني من الفيروسات والبريد الدعائي.

٦ – تنفيذ اختبارات دورية لنقاط الضعف انطلاقا من داخل الشبكة.

٧ – إبعاد وسائط النسخ لاحتياطي ووسائط التخزين عن أماكن تسرب المياه.

٨ – عمل النسخ الاحتياطي والاسترجاع الآلي يومياً.

٩ – وضع وسائط النسخ الاحتياطي في خزائن مضادة للصدمات والحريق.

١٠ –تحديث نظام تشغيل أجهزة الشبكة بشكل دوري.

١١ –استخدام خاصية اتصال الشبكة الافتراضية (VPN).

ب. تدابير الحماية من المخاطر الداخلية والخارجية والتي تعد ذات أولوية عالية وفقاً لاستجابات عينة الدراسة:

١ – تنفيذ اختبارات دورية لنقاط الضعف انطلاقاً من خارج الشبكة.

٢ – تصميم أو توفير برنامج إدارة الحماية من جميع جوانبها.

٣ – تدريب المستفيدين من موارد شبكة المعلومات.

٤ – إتاحة استخدام خاصية التحقق من الصحة في جدار الحماية.

٥ – تدريب كل الموظفين على أمن المعلومات كل حسب واجباته الوظيفية.

٦ – توفير إجراءات مكتوبة ومعتمدة توضح ما يلزم لتنفيذ أعمال الحماية.

٧ – توفير خدمة الاتصال البعيد فقط للأفراد المعتمدين من الإدارة.

٨ – تركيب برامج مخصصة لمراقبة استخدام المستفيدين.

٩ – استخدام نظام لإدارة الأحداث (Logs) في جميع خوادم وأجهزة الشبكة.

١٠ –تأمين بديل واحد على الأقل لكل موظف يعمل في مجال الحماية.

١١ –توفير موظف واحد على الأقل يقوم بإدارة أجهزة الحماية وتحديثها.

١٢ –بتجهيز الوسيط (Proxy) بخدمة توليد التقارير وتحليلها.

١٣ –استخدام توفير مركز بيانات (Data Center) بديل لاستخدامه عند الطوارئ.

١٤ –عقد دورات تدريب للتوعية في أمن المعلومات والحماية.

١٥ –تجهيز مركز البيانات بآلية تسجيل للداخلين بالاسم والوقت وسبب الدخول.

١٦ -توفير خطة طوارئ واضحة ومعتمدة.

١٧ -جعل إدارة أمن المعلومات تابعة مباشرة لرئيس أو مدير المؤسسة.

١٨ -توفير مراقبة داخلية باستخدام كاميرات تلفزيونية مع التسجيل.

١٩ -توفير موظف واحد على الأقل يقوم بإدارة برامج الحماية وتحديثها.

٢٠ -اشتراط توفر المهارات المناسبة لمستخدمي الحاسب الآلي.

٢١ -السعي للتوصل إلى اتفاقيات تعاون مع المتخصصين في الحماية.

٢٢ -توفير برنامج للتحكم بمنافذ الحاسبات ومشغلات الوسائط القابلة للإزالة.

٢٣ -اختبار خطة الطوارئ.

٢٤ -توظيف أشخاص مناسبين من حيث المؤهل والخبرة بنسبة ٩٠% على الأقل.

٢٥ -توفير إدارة خاصة بأمن المعلومات.

٢٦ -اعتماد ميزانية خاصة بخطة الطوارئ.

٢٧ -السعي لمطابقة إجراءات العمل لتتوافق مع معايير دولية (آيزو) تتعلق بالحماية.

٢٨ -تنفيذ اختبارات دورية لنقاط الضعف انطلاقا من خارج الشبكة.

٢٩ -إتلاف وسائط التخزين والنسخ الاحتياطي المنتهية الصلاحية.

٣٠ -تطبيق التشفير على وسائط النسخ الاحتياطي.

٣١ -إعداد خطة للتراجع (Rollback) تطبق في حالة عدم نجاح خطة الطوارئ.

٣٢ -توفير حراسة عند بوابات مركز البيانات على مدار الساعة.

٣٣ -زيادة الاعتماد على أنظمة تشغيل أقل تأثرا بالفيروسات (يونكس، لينوكس..).

٣٤ -تقليل الاعتماد على نظام تشغيل مايكروسوفت كونه الأكثر تأثرا بالفيروسات.

٥-٢-٦ نتائج تتعلق بالفروق والدلالات الإحصائية

١ -توجد فروق ذات دلالة إحصائية بين توفر الأجهزة والبرامج التي تستخدم في حماية الشبكات وبين تطبيق الإعدادات وتثبيت التحديثات لتلك الأجهزة والبرامج، وذلك لصالح توفر

الأجهزة والبرامج ويدل ذلك على عدم اكتمال الإعداد والتحديث للأجهزة والبرامج التي توفرها المؤسسات.

٢ – توجد فروق ذات دلالة إحصائية بين درجة خطورة نقاط الضعف التي يمكن أن تُستغل لاختراق شبكات الحاسب وبين التدابير الوقائية المتخذة لتلافي نقاط الضعف، وذلك لصالح درجة خطورة نقاط الضعف ويدل ذلك على عدم اكتمال التدابير الوقائية التي تتخذها المؤسسات التعليمية لتلافي نقاط الضعف.

٣ – توجد فروق ذات دلالة إحصائية بين المخاطر الداخلية والخارجية وبين التدابير المتخذة لتجنب تلك المخاطر، وذلك لصالح المخاطر الداخلية والخارجية ويدل ذلك على عدم اكتمال التدابير الوقائية التي تتخذها المؤسسات التعليمية لتجنب المخاطر الداخلية والمخاطر الخارجية

٤ – توجد فروق جوهرية في الهياكل التنظيمية لصالح الذكور.

٥ – توجد فروق جوهرية في الإجراءات لصالح الذكور.

٦ – لا توجد فروق ذات دلالة إحصائية تبعاً للخبرة في محاور الهياكل التنظيمية و الإجراءات والمخاطر الداخلية والخارجية ونقاط الضعف وتدابير إزالة نقاط الضعف ما عدا محور تدابير تجنب المخاطر الداخلية والخارجية.

٧ – توجد فروق جوهرية في التدابير لصالح ذوي الخبرة من ٥ سنوات إلى أقل من ١٠ سنوات.

٨ – توجد فروق جوهرية في التدابير لصالح ذوي الخبرة من ١٠ سنوات فأكثر.

٩ – لا توجد فروق ذات دلالة إحصائية في محاور الهياكل التنظيمية والإجراءات والمخاطر الداخلية والخارجية،

١٠ –توجد فروق في المحاور تدابير تجنب والمخاطر الداخلية والخارجية و نقاط الضعف و تدابير إزالة نقاط الضعف.

١١ –توجد فروق في تدابير تجنب المخاطر بين استجابات الوظائف الإدارية واستجابات الوظائف الفنية.

١٢ –توجد فروق في تدابير تجنب المخاطر بين استجابات الوظائف الفنية واستجابات الوظائف الإدارية.

١٣ –توجد فروق في تدابير تجنب المخاطر بين استجابات الوظائف الفنية واستجابات الوظائف الإدارية والفنية.

١٤ -توجد فروق في نقاط الضعف بين استجابات الوظائف الإدارية واستجابات الوظائف الفنية.

١٥ -توجد فروق في نقاط الضعف بين استجابات الوظائف الفنية واستجابات الوظائف الإدارية.

١٦ -توجد فروق في نقاط الضعف بين استجابات الوظائف الفنية واستجابات الوظائف الإدارية والفنية.

١٧ -توجد فروق في نقاط الضعف بين استجابات الوظائف الإدارية والفنية واستجابات الوظائف الفنية.

١٨ -توجد فروق في تدابير إزالة نقاط الضعف بين استجابات الوظائف الإدارية واستجابات الوظائف الفنية.

١٩ -توجد فروق في تدابير إزالة نقاط الضعف بين استجابات الوظائف الفنية واستجابات الوظائف الإدارية.

٢٠ -توجد فروق في تدابير إزالة نقاط الضعف بين استجابات الوظائف الفنية واستجابات الوظائف الإدارية والفنية.

٥-٣ توصيات الدراسة :

في ضوء نتائج الدراسة يقترح الباحث مجموعة من التوصيات التي تركز على أن الجهود التي ينبغي إكمالها لتحقيق حمية قصوى لا تكمن في المعدات أو البرمجيات وإنما تكمن في الجانب الإداري والموارد البشرية وأهم تلك التوصيات ما يلي:

١. توفير أخصائيين في أمن المعلومات لإنشاء السياسات الأمنية ومراجعة تنفيذها.
٢. تقدير أعمال الحماية بتقديم المكافآت أو العلاوات أو شهادات التقدير.
٣. تدريب العاملين في الحماية وفق مسارات تدريبية تخصصية بشكل يكفي لتأدية أعمالهم على الوجه الأكمل.
٤. زيادة دخل موظفي الحماية للتقليل من مغادرة ذوي الخبرة بحماية الشبكات لوظائفهم رغبة بفرص أفضل.
٥. السعي لمطابقة إجراءات العمل بالشبكات مع معايير (الآيزو).
٦. تعديل الهياكل التنظيمية لإدارات/مراكز تقنية المعلومات لتتناسب مع إجراءات الحماية.

٧. توفير عدد كاف من موظفي الحماية ممن يحملون مؤهلات علمية تتناسب مع متطلبات أعمال الحماية. وتوفير وصف وظيفي للوظائف المتعلقة بالحماية والأمان. وتشكيل اللجان والمجالس المطلوبة لتسيير إجراءات العمل في مجال أمن المعلومات.
٨. توفير إجراءات العمل الخاصة بأعمال تقنية المعلومات عامة والحماية خاصة. وتوثيقها.ً
٩. توفير سياسة توظيف الأفراد المناسبين في إدارة تقنية المعلومات، تتضمن تعيين مدراء متخصصون. بحيث تتوفر فيهم الصدق والأمانة والأخلاق العالية وينبغي التأكد من الالتزام الأخلاقي دورياً لجميع مستخدمي الحاسبات الآلية وخصوصاً للعاملين في حماية موارد شبكات الحاسب الآلي

٥-٤ مقترحات الدراسة

تقترح الدراسة على إدارات المؤسسات التي تعتمد في تسيير أعمالها على تقنية المعلومات أن يعتنوا عناية خاصة بالموارد البشرية العاملة في مجال أمن وحماية الشبكات فهي القادرة على التغلب على صعوبات الحماية ومما يقلل من تلك الصعوبات ما يلي:

١. العناية بالهياكل التنظيمية للمؤسسات وتضمينها أقسام خاصة بأمن المعلومات. وتعيين مدراء متخصصين بالحماية على رأس تلك الهياكل. وتدريب المدراء والعاملين في مجال الشبكات وأمن المعلومات وفق مسارات تدريبية.
٢. توفير السياسات الأمنية والإجراءات اللازمة لتنفيذ أعمال الحماية، والعناية بخطط الطوارئ وتدريب المعنيين على تنفيذها وإنشاء مراكز بيانات احتياطية.
٣. السعي لمطابقة مواصفات الشبكات وإجراءات العمل فيها مع المعايير العالمية ذات الصلة بأمن المعلومات.
٤. توظيف الكوادر المؤهلة من ذوي الخبرة في مجال الحماية وتحفيزهم بالمكافآت المالية والمعنوية. وإعطاء السلوك النزيه والتمتع بالأخلاق العالية والصدق أولوية عالية عند التوظيف، والتأكد من محافظة الموظفين على مستويات تلك الأخلاقيات.

الملاحق

الملحق رقم (١) مسودة أداة الدراسة

الملحق رقم (٢) نموذج تحكيم أداة الدراسة

الملحق رقم (٣) أداة الدراسة في صورتها بعد التحكيم

الملحق رقم (٤) قائمة أسماء المحكمين

الملحق رقم (١)

مسودة أداة الدراسة

جمهورية السودان

وزارة التعليم العالي والبحث العلمي

جامعة النيلين

كلية الدراسات العليا – كلية الحاسوب

الاستبانة الأولية
(المسودة)

أداة دراسة بعنوان

حماية الشبكات الرئيسة من الفيروسات والبرامج الضارة

إعـــداد

زكريا أحمد عمار

إشراف

الأستاذ الدكتور السماني عبد المطلب

١٤٣٠هـ - ٢٠٠٩م

بسم الله الرحمن الرحيم

أخي الكريم:

السلام عليكم ورحمة الله وبركاته وبعد :

الاستبانه التي بين يديك هي جزء من دراسة عن " حماية الشبكة الرئيسة من الاختراق والبرامج الضارة" : دراسة مسحية تحليلية على حماية الشبكات في المؤسسات التعليمية بمدينة الرياض" استكمالا للحصول على درجة الماجستير في أمن المعلومات .

لذا يود الباحث معرفة رأيك الشخصي وذلك بالإجابة على أسئلة الاستبانه التي بين يدك.

علما بأن البيانات التي ستدلي بها من خلال إجاباتك ستستخدم لأغراض البحث العلمي فقط.

مع الشكر والتقدير على حسن تعاونكم

الباحث

مهندس/ زكريا أحمد عمار

هـ العمل: ١٥٠٨ ت ٣٤٤٤-٢٤٦

جوال : ٠٥٠٣٤٤٢٥٧٢

القسم الاول: البيانات الأولية

الرجاء الإجابة على الأسئلة التالية وذلك بكتابة العبارة المناسبة بالفراغات أو وضع علامة (✓) داخل المربع:

أ. معلومات شخصية:

١. ☐ ذكر		٢. ☐ أنثى	
٣. العمـــر : ..... سنة		٤. الجنسية:	
وظيفتي:	٥. ☐ إدارية فقط	٦. ☐ فنية فقط	٧. ☐ فنية إدارية معاً

ب. المؤهل العلمي

١. ☐ شهادة الثانوية العامة فأقـل	٢. ☐ دبلوم (سنتين بعد الثانوية)
٣. ☐ بكالوريوس (كلية جامعيـة)	٤. ☐ ماجستير
٥. ☐ دكتوراه	

ت. التخصص:

١. ☐ شبكات	٢. ☐ برمجة
٣. ☐ نظم معلومات إدارية	٤. ☐ أُخرى (تُذكر) .....

ث. عدد سنوات الخبرة: .....

ج. الشهادات المعتمدة دولياً:

١. ☐ CISSP	٢. ☐ CEH
٣. ☐ Security +	٤. ☐ سيسكو
٥. ☐ مكافي	٦. ☐ جنبر
٧. ☐ نورتون	٨. ☐ أُخرى (تُذكر) .....

ح. إن المؤسسة التي أعمل بها تعد من القطاع:

١. ☐ الحكومي	٢. ☐ الأهلي (خاص)	٣. ☐ المشترك (حكومي&خاص)

خ. المؤسسة التي أعمل بها تعنى بتعليم المراحل التالية:

١. ☐ ثانوية وما دون	٢. ☐ **معهد**
٣. ☐ **جامعة**	٤. ☐ مراحل مختلفة (مركز تدريب)

القسم الثاني: أسئلة محاور الدراسة

المحور الأول: الأجهزة والبرامج المستخدمة لحماية الشبكات والطرق المتبعة في إعدادها وتحديثها

العبارة	مدى وضوح العبارة		مدى أهمية العبارة		مدى مناسبة العبارة للمحور		ملاحظات
	واضحة	غير واضحة	مهمة	غير مهمة	مناسبة	غير مناسبة	
أ. الأجهزة والبرامج المستخدمة لحماية الشبكات في مؤسستي							
١.تستخدم مؤسستي جدار حماية (FireWall) واحد أو أكثر عند بوابة الشبكة المحلية.							
٢.قُسمت الشبكة إلى ثلاثة شبكات فرعية أو أكثر (داخلية و DMZ وخارجية).							
٣.جدران الحماية المستخدمة في مؤسستي تقبل التحديث الآلي							
٤.توجد خاصية تصفية البريد الدعائي Spam في جدار الحماية المستخدم .							
٥.جدران الحماية المستخدمة في مؤسستي مزودة بخاصية كشف التلصص IDS							
٦.جدران الحماية المستخدمة في مؤسستي مزودة بخاصية كشف ومنع التلصص IPS							
٧.جدران الحماية المستخدمة في مؤسستي مزودة بخاصية تصفية المواقع غير المرغوب فيها.							
٨.تستخدم مؤسستي موجه (Router) واحد على الأقل.							
٩.تستخدم مؤسستي اتصال الشبكة الافتراضية VPN							
١٠.توفر إدارة مؤسستي عقد دعم فني لجدران الحماية يجدد سنويا من الشركة الصانعة							
١١.يوجد برنامج أو جهاز مخصص لحماية خادم البريد من الفيروسات والبريد الدعائي Spams							
١٢.يوجد في مؤسستي وسيط (proxy) لتوزيع خدمة الإنترنت على المستفيدين.							
١٣.في شبكة مؤسستي يوجد مبدل مركزي Core Switch واحد على الأقل.							
١٤.توجد نقاط شبكة لاسلكية (Access Points) مثبتة داخل الشبكة المحلية.							
١٥.تستخدم مؤسستي نظام نسخ احتياطي احترافي.							
١٦.يوجد في مؤسستي مخطط واضح لشبكة المعلومات تظهر فيه جدران الحماية والموجهات والخوادم الهامة مع عناوينها.							

١٧.يوجد خادم أو جهاز مخصص لمكافحة الفيروسات داخل الشبكة							
١٨.توفر مؤسستي عقد دعم فني لنظام الحماية من الفيروسات يجدد سنويا							
١٩.موقع مؤسستي على الإنترنت محتضن في شبكة المؤسسة.							
٢٠.يوجد نظام مخصص لمراقبة استخدام الإنترنت داخل مؤسستي.							
٢١.توفر مؤسستي نظام Event Manager لإدارة تسجيلات الأحداث Events /logs							
٢٢.توفر مؤسستي نظام متكامل مخصص لإدارة قضايا أمن المعلومات من جميع الجوانب.							
١.العلامة التجارية للجهاز المستخدم في مؤسستي هي سيسكو ، سونك وول ، ...							
٢.العلامة التجارية لبرنامج الحماية المستخدم في مؤسستي هي سوفس ، ترند مايكرو، ...							
٢٣.أجهزة وبرامج أخرى ترى أنها لم تُذكر	....						
ب. الطرق المتبعة في إعداد وتحديث أجهزة وبرامج الحماية في مؤسستي							
٢٤.تم تفعيل نظام حماية من البريد الدعائي Spam في جدار الحماية							
٢٥.يتم تحديث خاصية الحماية من الفيروسات في جدار الحماية بشكل آلي							
٢٦.يتم استخدام تشفير لحماية اتصالات VPN							
٢٧.يتم تفعيل خاصية تصفية المواقع غير المرغوبة في جدران الحماية المستخدمة في مؤسستي.							
٢٨.يتم تحديث نظام تشغيل جدار الحماية (Firewall Image) بشكل دوري							
٢٩.يتم تحديث نظام تشغيل الموجهات (Router Image) بشكل دوري							
٣٠.تم إعداد لوائح التحكم بالوصول access control list في الموجهات Routers							
٣١.يتم تحديث نظام تشغيل الوسيط (Proxy) بشكل دوري							
٣٢.يتم تثبيت التحديثات الأمنية patches للوسيط proxy بشكل دوري							
٣٣.يتم مراجعة تقارير استخدام الانترنت يومياً.							
٣٤.يتخذ إجراء تقويمي لمن يسيء استخدام الانترنت.							

٣٥.يتم إعداد نظام النسخ الاحتياطي لأخذ النُّسخ الاحتياطية بشكل يومي							
٣٦.يتم تحديث مخطط الشبكة بشكل دوري							
٣٧.يتم تحديث أنظمة تشغيل المبدلات المركزية ومبدلات التوزيع(Switch Image) دورياً							
٣٨.يتم تحديث نظام تشغيل أجهزة نقاط شبكة لاسلكية (Access Points) دورياً							
٣٩.يتم تثبيت تحديثات جهزة نقاط شبكة لاسلكية (Access Points) دورياً							
٤٠.يتم إعداد مفاتيح النقاط اللاسلكية بطول ٦٤ بت							
٤١.يتم إعداد مفاتيح النقاط اللاسلكية بطول ١٢٨ بت							
٤٢.في مؤسستي يتم إعداد المبدلات Switches لعزل حاسبات المتدربين عن موارد الشبكة.							
٤٣.تستخدم مؤسستي بيئة تجربة لتثبيت التحديثات قبل اعتمادها في بيئة الإنتاج.							
٤٤.تستخدم مؤسستي بيئة تطوير لبناء وتجربة تطبيقات جديدة قبل نقلها إلى بيئة الإنتاج.							
٤٥.يستطيع مستخدمو الحاسبات المكتبية بمؤسستي لتثبيت وإزالة أي برنامج يرغبونه في حاسباتهم.							
٤٦.يستطيع مستخدمو حاسبات المعامل الوصول إلى موارد شبكة المؤسسة.							
٤٧.يستطيع المبرمجون الدخول إلى جميع التطبيقات بصلاحيات كاملة							
٤٨.يستطيع مدير نظام تشغيل الشبكة الدخول إلى جميع موارد الشبكة بصلاحيات كاملة							

المحور الثاني: نقاط الضعف التي يمكن أن تُستغل لاختراق شبكة المعلومات والتدابير الوقائية التي ينبغي اتخاذها

العبارة	مدى وضوح العبارة		مدى أهمية العبارة		مدى مناسبة العبارة للمحور		ملاحظات
	واضحة	غير واضحة	مهمة	غير مهمة	مناسبة	غير مناسبة	
أ. **نقاط الضعف التي يمكن أن تُستغل لاختراق شبكات المعلومات**							
١.عدم تثبيت تحديثات أنظمة تشغيل أجهزة الخادم والحاسبات المكتبية							
٢.عدم تحديث أنظمة تشغيل جدران الحماية							
٣.عدم تحديث خاصية تصفية المواقع غير المرغوبة في جدار الحماية.							

٤.عدم تحديث خاصية الحماية من الفيروسات في جدار الحماية.							
٥.عدم تحديث خاصية الحماية من البريد الدعائي Spam في جدار الحماية.							
٦.عدم وجود خاصية كشف ومنع التلصص IPS تُحدث يومياً في جدار الحماية.							
٧.عدم تحديث مكونات البروكسي.							
٨.وجود نظم تشغيل غير مرخصة بالشبكة							
٩.قلة الكفاءة المهنية للمستخدمين							
١٠.قلة خبرة العاملين بالحماية							
١١.وجود كلمات مرور افتراضية في بعض الأجهزة العاملة بالشبكة.							
١٢.وجود كلمات مرور افتراضية في بعض البرمجيات العاملة بالشبكة.							
١٣.عدم وجود سياسة للحماية							
١٤.أداء بعض الأجهزة ضعيف ولا تستطيع تشغيل مكافح الفيروسات.							
١٥.نقاط ضعف أخرى ترى أنها لم تُذكر:							

ب. التدابير الوقائية

العبارة	وضوح العبارة		أهمية العبارة		مناسبتها للمحور		ملاحظات
	واضحة	غير واضحة	مهمة	غير مهمة	مناسبة	غير مناسبة	
١٦.تخصيص خادم لتحديث نظم تشغيل الحاسبات المكتبية وأجهزة الخادم.							
١٧.تفعيل التحديث الآلي لجدران الحماية							
١٨.تفعيل التحديث الآلي لبرامج الحماية							
١٩.استخدام برمجيات لقياس أداء مكونات الشبكة لاتخاذ ما يلزم لمنع توقفها في المستقبل القريب.							
٢٠.تزويد وتفعيل خاصية كشف ومنع التلصص IPS							

في جدار الحماية							
٢١.تزويد وتفعيل خاصية الحماية من الفيروسات في جدار الحماية							
٢٢.تزويد وتفعيل خاصية تصفية المواقع غير المرغوب فيها في جدار الحماية							
٢٣.تزويد وتفعيل خاصية الحماية من البريد الدعائي Spam في جدار الحماية							
٢٤.استخدام قائمة مهام الحماية اليومية Check list							
٢٥.تنفيذ اختبار دوري لكشف نقاط الضعف من داخل الشبكة.							
٢٦.تنفيذ اختبار دوري لكشف نقاط الضعف بدءا من خارج الشبكة.							
٢٧.مراجعة محاولات الدخول إلى النظام وخصوصا من داخل الشبكة.							
٢٨.تدابير وقائية أخرى ترى أنها لم تُذكر:	....						

المحور الثالث: الهياكل التنظيمية المناسبة لمراكز تقنية المعلومات ومدى توافق الوظائف المستخدمة في مجال أمن شبكات المعلومات معها.

العبارة	مدى وضوح العبارة		مدى أهمية العبارة		مدى مناسبة العبارة للمحور		ملاحظات
	واضحة	غير واضحة	مهمة	غير مهمة	مناسبة	غير مناسبة	
١.يوجد في مؤسستي هيكل تنظيمي معتمد ومعمم، يتضمن الإدارة/القسم الذي أعمل فيه.							
٢.أرى أن الهيكل التنظيمي لإدارة/مركز تقنية المعلومات الذي أعمل فيه مناسب و مواكِب للتطور السريع في تقنية المعلومات.							
٣.في مؤسستي يتم مراعاة التسلسل الإداري في							

المعاملات الفنية والإدارية والمالية.							
٤.في مؤسستي يوجد مجلس/لجنة لإدارة التعديلات (شبكات وقواعد بيانات وموقع الانترنت..).							
٥.يوجد قسم/إدارة/وحدة تحت مسمى أمن المعلومات أو أمن الشبكة أو ما شابه ذلك							
٦.يوجد في مؤسستي مسمى وظيفة مرفقة بالمهام والواجبات والمسؤوليات والصلاحيات لكل وظيفة من الوظائف المتعلقة بالحماية في إدارة تقنية المعلومات.							
٧.في مؤسستي يتم تبديل الموظفين العاملين بالحماية باستمرار بمبادرة من الإدارة.							
٨.في مؤسستي تتكرر مغادرة موظفي حماية الشبكات لوظائفهم رغبة بفرص عمل افصل.							
٩.المؤهل العلمي للعاملين في مجال الحماية في مؤسستي يتناسب مع مسميات وظائفهم.							
١٠.في مؤسستي يوجد مدقق يقوم بمراجعة تنفيذ السياسات Security Editor							
١١.ويوجد مسؤول شبكات Network Admin يقوم بإدارة توصيلات الكابلات والمبدلات							
١٢.ويوجد موظف بمسمى ضابط أمن المعلومات Security Officer							
١٣.ويوجد موظف يقوم بإدارة أجهزة الحماية (جدران الحماية والموجهات والنقاط الوصول اللاسلكية)							
١٤.ويوجد موظف يقوم بإدارة برامج الحماية (برامج مكافحة الفيروسات والبريد الدعائي ...)							
١٥.حسب رأيي، الموظفون الذين يعملون في مجال الحماية في مؤسستي غير كافين من حيث العدد.							
١٦.أعاني من ضغط في العمل وأحتاج لوقت إضافي							

لإنجاز جميع واجباتي							
١٧.يوجد تقدير لأعمال الحماية من قبل إدارة مؤسستي يظهر بتقديم المكافآت أو العلاوات أو الشكر.							
١٨.مديري المباشر متخصص في إحدى مجالات تقنية المعلومات.							
١٩.مدير إدارة تقنية المعلومات متخصص في إحدى مجالات تقنية المعلومات.							
٢٠.أرى أن الدخل الذي أتقاضاه غير مناسب.							
٢١.تولي إدارة المؤسسة التي أعمل فيها اهتمام في أمن المعلومات يظهر من خلال تخصيص ميزانية جيدة لتحسين الحماية.							
٢٢.أرى أن التدريب الذي أحصل عليه من مؤسستي كاف لتأدية عملي في مجال الحماية.							
٢٣.توفر مؤسستي عقد مع شركة خارجية لتأمين الدعم الفني لأجهزة الحماية يشمل تبديل الجهاز							
٢٤.أرى أن الدعم الفني الخاص بجدار الحماية الذي تستخدمه مؤسستي جديد.							
٢٥.توفر مؤسستي عقد مع شركة خارجية لتأمين الدعم الفني لبرامج الحماية يشمل الحضور لموقع المؤسسة لإصلاح المشكلات عند طلب ذلك.							
٢٦.أرى أن الدعم الفني الخاص ببرنامج الحماية من الفيروسات الذي تستخدمه مؤسستي جيد.							
٢٧.هل سبق وأن اشتركت في ندوات أو محاضرات أو مؤتمرات حول إدارة مراكز المعلومات							
٢٨.أو حول الأخطار والتهديدات المحتملة وخطط الطوارئ							
٢٩.أو حول التوعية في مجال في أمن المعلومات							
٣٠.أو حول أنظمة الحماية (مكافحات الفيروسات و							

جدران الحماية)							
٣١. هل سبق وأن اشتركت في ندوات أو محاضرات أو مؤتمرات أو دورات أُخرى ترى أهمية لذكرها:							

المحور الرابع: توفُّر إجراءات العمل في حماية شبكات المعلومات و مدى تطبيقها والعمل بها.

العبارة	مدى وضوح العبارة		مدى أهمية العبارة		مدى مناسبة العبارة للمحور		ملاحظات
	واضحة	غير واضحة	مهمة	غير مهمة	مناسبة	غير مناسبة	
١.في مؤسستي يوجد وثيقة توضح طريقة تحديث جدران الحماية							
٢.ويوجد وثيقة توضح طريقة تحديث برامج الحماية							
٣.ويوجد وثيقة توضح خطوات إعداد وتشغيل عمليات النسخ الاحتياطي والاسترجاع							
٤.يوجد وثيقة توضح تركيب برامج حماية داخل الشبكات							
٥.يوجد وثيقة توضح تركيب أجهزة حماية على حدود الشبكات							
٦.في مؤسستي يتم أخذ موافقة مجلس/لجنة التعديل عند تعديل مكونات جدار الحماية.							
٧.ويوجد موظف واحد على الأقل يقوم بإدارة الإجراءات (إنشاءها ، تحديثها، توثيقها، تطويرها)							
٨.ويوجد إجراءات عمل خاصة بإدارة عمليات تحديث التطبيقات والبرمجيات							
٩.وتتوفر خطة مكتوبة وتم التدرب على تطبيقها لاسترداد النظام في الحالات الطارئة.							
١٠.ويوجد نظام لإدارة وثائق الإجراءات يتم تحديثه باستمرار.							

١١.يوجد صعوبات إدارية تعترض تنفيذ إجراءات إدارة نظم أمن المعلومات							
١٢.يوجد صعوبات مالية تعترض تنفيذ إجراءات إدارة نظم أمن المعلومات							
١٣.يوجد صعوبات تدريبية تعترض تنفيذ إجراءات إدارة نظم أمن المعلومات							
١٤.يتوفر في مؤسستي سياسة النسخ الاحتياطي والاسترجاع							
١٥.يتوفر في مؤسستي سياسة الاستخدام المقبول							
١٦.يتوفر في مؤسستي سياسة التدريب (لموظفي تقنية المعلومات)							
١٧.يتوفر في مؤسستي سياسية ضمان المعلومات							
١٨.يتوفر في مؤسستي سياسة توظيف منسوبي إدارة تقنية المعلومات.							
١٩.يتوفر في مؤسستي سياسة توريد وتأمين الخدمات من خارج المنظمة Outsourcing							
٢٠.يتوفر في مؤسستي سياسة تقييم المعلومات من حيث درجة السرية							
٢١.يتوفر في مؤسستي سياسة واضحة تتعلق بعمليات حفظ وتخزين المعلومات							
٢٢.يتوفر في مؤسستي إجراء إتلاف الأصول المعلوماتية المنتهية الصلاحية							
٢٣.يتوفر في مؤسستي إجراء تسمية الأصول المعلوماتية وتسجيله على الوسائط المعلوماتية							
٢٤.يتوفر في مؤسستي إجراء تحديث أنظمة التشغيل							
٢٥.أرى أن نظام تشغيل ويندوز هو الأكثر تأثرا بالفيروسات							
٢٦.أرى أن نظام تشغيل يونكس هو الأكثر تأثرا							

بالفيروسات							
٢٧.أرى أن نظام تشغيل لينكس هو الأكثر تأثرا بالفيروسات							
٢٨.أرى أن نظام تشغيل ماكنتوش هو الأكثر تأثرا بالفيروسات							
٢٩.إجراءات أخرى أرى أنه من المفيد ذكرها	.....						

المحور الخامس: درجة المعرفة بالمخاطر التي يمكن أن تؤثر سلباً على أمن شبكات المعلومات، و درجة تطبيقها فعلا بحالات الحدوث.

العبارة	مدى وضوح العبارة		مدى أهمية العبارة		مدى مناسبة العبارة للمحور		ملاحظات
	واضحة	غير واضحة	مهمة	غير مهمة	مناسبة	غير مناسبة	
من وُجهة نظرك ما درجة معرفتك المخاطر التالية : (مخاطر خارجية)							
١.التعدي على الكابلات وتخريبها							
٢.التعدي على الكابلات وتخريبها							
٣.اندلاع الحريق							
٤.حصول إغراق بسبب فيضان							
٥.اختراق لتعديل البيانات وتغيرها أو إتلافها							
٦.التعرض لهجوم إرهابي							
من وُجهة نظرك ما درجة معرفتك المخاطر التالية : (مخاطر داخلية)							
٧.اختراق أجهزة الخادم من داخل المنظمة (عبث،إساءة استخدام...)							
٨.استخدام برامج بغرض التجسس من قبل المستفيدين من داخل المؤسسة							
٩.اختراق أجهزة الخادم من داخل المنظمة (عبث،إساءة استخدام...)							
١٠.استخدام برامج بغرض التجسس من قبل المستفيدين من داخل المؤسسة							

١١.زيارة مواقع غير موثوقة تسمح بتنزيل البرمجيات الضارة							
١٢.الإصابة بفيروسات مصدرها الانترنت							
١٣.الإصابة بفيروسات مصدرها وسائط التخزين وذواكر الفلاش							
١٤.تنزيل برامج غير مصرح بها.							
١٥.سرقة الأجهزة ووسائط التخزين							
من وُجهة نظرك ما درجة أهمية التدابير الوقائية التالية:							
١٦.توفير حراسة عند بوابات مركز البيانات على مدار الساعة							
١٧.تجهيز مركز البيانات بنظام إطفاء الحريق والإنذار.							
١٨.قفل مركز البيانات (غرفة أجهزة الخادم وأجهزة الشبكة) بحيث لا يدخلها إلا المتخصصون ممن لديهم ترخيص بالدخول.							
١٩.تجهيز مركز البيانات بنظام تسجيل لجميع الداخلين بالاسم والوقت وسبب الدخول							
٢٠.توفير مراقبة داخلية باستخدام كاميرات تلفزيونية مع التسجيل							
٢١.عمل النسخ الاحتياطي والاسترجاع الآلي يومياً							
٢٢.وضع وسائط النسخ الاحتياطي في خزائن مضادة للصدمات والحريق.							
٢٣.تطبيق التشفير على وسائط النسخ الاحتياطي							
٢٤.إبعاد وسائط النسخ لاحتياطي ووسائط التخزين عن أماكن تسرب المياه							
٢٥.إتلاف وسائط التخزين والنسخ الاحتياطي المنتهية الصلاحية.							
٢٦.تركيب برامج مخصصة لمراقبة استخدام							

المستفيدين							
٢٧.وضع وسائط النسخ الاحتياطي في خزائن مضادة للصدمات والحريق.							
٢٨.تطبيق التشفير على وسائط النسخ الاحتياطي							
٢٩.إبعاد وسائط النسخ لاحتياطي ووسائط التخزين عن أماكن تسرب المياه							
٣٠.إتلاف وسائط التخزين والنسخ الاحتياطي المنتهية الصلاحية.							
٣١.تركيب برامج مخصصة لمراقبة استخدام المستفيدين							
٣٢.توفير خطة طوارئ واضحة ومعتمدة.							
٣٣.إعداد خطة واضحة للتراجع (Rollback) تطبق في حالة عدم نجاح خطط الطوارئ.							
٣٤.تدريب كل الموظفين على أمن المعلومات كل حسب واجباته الوظيفية.							
٣٥.السعي لمطابقة إجراءات العمل لتتوافق مع إحدى المعايير الدولية المعتمدة (آيزو) في مجال أمن المعلومات.							
٣٦.السعي للتوصل إلى اتفاقيات تعاون مع المتخصصين في أمن المعلومات							
٣٧.تنفيذ اختبارات دورية لنقاط الضعف انطلاقا من داخل الشبكة.							
٣٨.تنفيذ اختبارات دورية لنقاط الضعف انطلاقا من خارج الشبكة.							
٣٩.استخدام تشفير لقواعد البيانات							
٤٠.استخدام التشفير لاتصالات VPN							
٤١.توفير مركز بيانات Data Center بديل لاستخدامه عند الطوارئ							

٤٢.تجهيز الوسيط Proxy بخدمة توليد التقارير وتحليلها.							
٤٣.توفير إجراءات مكتوبة ومعتمدة توضح ما يلزم لتنفيذ أعمال الحماية							
٤٤.توفير موظف واحد على الأقل يقوم بإدارة أجهزة الحماية وتحديثها.							
٤٥.توفير موظف واحد على الأقل يقوم بإدارة برامج الحماية وتحديثها.							
٤٦.تأمين بديل واحد على الأقل لكل موظف يعمل في مجال الحماية.							
٤٧.توظيف الأشخاص المناسبين من حيث المؤهل والخبرات الفنية.							
٤٨.تصميم أو توفير برنامج إدارة الحماية من جميع جوانبها.							
٤٩.تأمين جهاز إضافي لكل جهاز بالشبكة كجدار الحماية والموجه والوسيط							
٥٠.تأمين خادم server احتياطي لكل خادم يعمل بالشبكة مثل: DHCP،DNS، قواعد البيانات ، الويب.							
٥١.تخصيص إدارة خاصة بأمن المعلومات							
٥٢.اشتراط امتلاك المهارات المناسبة لمستخدمي الحاسب الآلي.							
٥٣.عقد دورات تدريب للتوعية في أمن المعلومات والحماية.							
٥٤.توفير خدمة الاتصال البعيد فقط للأفراد المعتمدين من الإدارة.							
٥٥.توفير نظام مخصص لحماية البريد الالكتروني من الفيروسات والبريد الدعائي Spam.							

٥٦.تحديث نظام تشغيل أجهزة الشبكة بشكل دوري							
٥٧.إتاحة استخدام خاصية التحقق من الصحة في جدار الحماية							
٥٨.تفعيل خاصية التشفير في جدار الحماية عند استخدام VPN							
٥٩.توفير سياسة خاصة بكلمات المرور وتطبيقها.							
٦٠.تدريب أعضاء الهيئة التدريسية على ما يحتاجون من أمن المعلومات.							
٦١.تدريب الطلاب والباحثين على ما يحتاجون من أمن المعلومات.							
٦٢.توفير برنامج لتحكم بمنافذ الحاسبات ومشغلات الوسائط القابلة للإزالة من حيث التعطيل أو الإتاحة أو الفتح التلقائي أو الفحص قبل الفتح...							
٦٣. تدابير وقائية أخرى ترى أهمية لذكرها	....						

الملحق رقم (٢)

نموذج تحكيم أداة الدراسة

جمهورية السودان
وزارة التعليم العالي والبحث العلمي

جامعة النيلين
كلية الدراسات العليا – كلية الحاسوب

استبانة

دراسة بعنوان

حماية الشبكات الرئيسة من الفيروسات والبرامج الضارة

إعـــداد

زكريا أحمد عمار

إشراف

الأستاذ الدكتور السماني عبد المطلب

١٤٣٠هـ - ٢٠١٠م

بسم الله الرحمن الرحيم

سعادة الأستاذ الدكتور .... المحترم

السلام عليكم ورحمة الله وبركاته

تعد حماية شبكات المعلومات من أكثر قضايا العصر أهمية فأي اختراق أو تسريب للمعلومات السرية يؤدي إلى الإضرار بالمنشأة المعنية بل بالدولة إذا كانت المنشاة عسكرية أوأمنية وبذلك تكون الحماية قضية وطنية. وانطلاقاً من أهمية حماية شبكات المعلومات يقوم الباحث بإعداد دراسة ميدانية على بعض المؤسسات التعليمة في مدينة الرياض التي تعتمد على تجهيزات تقنية المعلومات وتتوفر فيها حواسيب وبرامج ضمن شبكة متصلة بالإنترنت.

وقد أعدّ الباحث هذه الاستبانة كأداة لقياس المتغيرات التي جاءت في خمسة محاور هي الأجهزة والبرامج المستخدمة لحماية الشبكات، ونقاط الضعف التي تُستغل لاختراق شبكات المعلومات، والهياكل التنظيمية المناسبة لإدارات تقنية المعلومات، وإجراءات العمل المعتمدة لحماية الشبكات، والتدابير الاحتياطية اللازمة لتجنب المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات المعلومات.

ولكونكم من ذوي الخبرة في مجال الدراسة نرجو تعاونكم من خلال إبداء الرأي حول مدى وضوح صياغة عبارات الاستبانة، ومدى مناسبتها للقياس، ومدى مناسبة العبارات للمبحوثين (مهندسون وفنيون يعملون بمجال الشبكات وأمن المعلومات والدعم الفني ومدراء ورؤساء الأقسام بمراكز تقنية المعلومات)

وللتوضيح نورد نموذجا يبين كيفية طرح العبارات التي تتضمنها محاور الدراسة وكيفية الإجابة عليها من قبل المبحوثين.

علماً أن نماذج المحاور الأول والثالث والرابع كالتالي:

- **الهياكل التنظيمية المناسبة لمراكز تقنية المعلومات ومدى توافق الوظائف المستخدمة معها:**

م	العبارة	نعم (١)	إلى حد ما (٢)	لا (٣)
١	يوجد في مؤسستي هيكل تنظيمي معتمد ومعمم، يتضمن الإدارة/القسم الذي أعمل فيه.			

ونموذج المحاور الثاني والخامس كالتالي:

- **درجة خطورة نقاط الضعف التي يمكن أن تُستغل لاختراق شبكة المعلومات والتدابير الوقائية التي ينبغي اتخاذها:**

م	العبارة	درجة الخطورة (١) أقل خطورة (٥) أعلى خطورة				
		(١)	(٢)	(٣)	(٤)	(٥)
١	عدم تثبيت تحديثات أنظمة التشغيل الحاسبات المكتبية					

شاكرين ومقدرين تعاونكم

الباحث مهندس/ زكريا أحمد عمار

القسم الاول: البيانات الأولية

الرجاء الإجابة على الأسئلة التالية وذلك بكتابة العباة المناسبة بالفراغات أو وضع علامة (✓) داخل المربع:

د. معلومات شخصية:

٨. ☐ ذكر		٩. ☐ أنثى	
١٠. العمـــر : ..... سنة		١١. الجنسية:	
وظيفتي:	١٢. ☐ إدارية فقط	١٣. ☐ فنية فقط	١٤. ☐ فنية إدارية معاً

ذ. المؤهل العلمي

٦. ☐ شهادة الثانوية العامة فأقـل	٧. ☐ دبلوم (سنتين بعد الثانوية)
٨. ☐ بكالوريوس (كلية جامعيــة)	٩. ☐ ماجستير
١٠. ☐ دكتوراه	

ر. التخصص:

٥. ☐ شبكات	٦. ☐ برمجة
٧. ☐ نظم معلومات إدارية	٨. ☐ أخرى (تُذكر) .....

ز. عدد سنوات الخبرة: .....

س. الشهادات المعتمدة دولياً:

٩. ☐ CISSP	١٠. ☐ CEH
١١. ☐ Security +	١٢. ☐ سيسكو
١٣. ☐ مكافي	١٤. ☐ جنبر
١٥. ☐ نورتون	١٦. ☐ أُخرى (تُذكر) .....

ش. إن المؤسسة التي أعمل بها تعد من القطاع:

٤. ☐ الحكومي	٥. ☐ الأهلي (خاص)	٦. ☐ المشترك (حكومي&خاص)

ص. المؤسسة التي أعمل بها تعنى بتعليم المراحل التالية:

٥. ☐ ثانوية وما دون	٦. ☐ **معهد**
٧. ☐ **جامعة**	٨. ☐ مراحل مختلفة (مركز تدريب)

القسم الثاني: أسئلة محاور الدراسة

المحور الأول: الأجهزة والبرامج المستخدمة لحماية الشبكات والطرق المتبعة في إعدادها وتحديثها

العبارة	مدى وضوح العبارة		مدى أهمية العبارة		مدى مناسبة العبارة للمحور		ملاحظات
	واضحة	غير واضحة	مهمة	غير مهمة	مناسبة	غير مناسبة	
ب. الأجهزة والبرامج المستخدمة لحماية الشبكات في مؤسستي							
٤٩.تستخدم مؤسستي جدار حماية (FireWall) واحد أو أكثر عند بوابة الشبكة المحلية.							
٥٠.قُسمت الشبكة إلى ثلاثة شبكات فرعية أو أكثر (داخلية و DMZ وخارجية).							
٥١.جدران الحماية المستخدمة في مؤسستي تقبل التحديث الآلي							
٥٢.توجد خاصية تصفية البريد الدعائي Spam في جدار الحماية المستخدم .							
٥٣.جدران الحماية المستخدمة في مؤسستي مزودة بخاصية كشف التلصص IDS							
٥٤.جدران الحماية المستخدمة في مؤسستي مزودة بخاصية كشف ومنع التلصص IPS							
٥٥.جدران الحماية المستخدمة في مؤسستي مزودة بخاصية تصفية المواقع غير المرغوب فيها.							
٥٦.تستخدم مؤسستي موجه (Router) واحد على الأقل.							
٥٧.تستخدم مؤسستي اتصال الشبكة الافتراضية VPN							
٥٨.توفر إدارة مؤسستي عقد دعم فني لجدران الحماية يجدد سنويا من الشركة الصانعة							
٥٩.يوجد برنامج أو جهاز مخصص لحماية خادم البريد من الفيروسات والبريد الدعائي Spams							
٦٠.يوجد في مؤسستي وسيط (proxy) لتوزيع خدمة الإنترنت على المستفيدين.							
٦١.في شبكة مؤسستي يوجد مبدل مركزي Core Switch واحد على الأقل.							
٦٢.توجد نقاط شبكة لاسلكية (Access Points) مثبتة داخل الشبكة المحلية.							
٦٣.تستخدم مؤسستي نظام نسخ احتياطي احترافي.							

٦٤.يوجد في مؤسستي مخطط واضح لشبكة المعلومات تظهر فيه جدران الحماية والموجهات والخوادم الهامة مع عناوينها.							
٦٥.يوجد خادم أو جهاز مخصص لمكافحة الفيروسات داخل الشبكة							
٦٦.توفر مؤسستي عقد دعم فني لنظام الحماية من الفيروسات يجدد سنويا							
٦٧.موقع مؤسستي على الإنترنت محتضن في شبكة المؤسسة.							
٦٨.يوجد نظام مخصص لمراقبة استخدام الإنترنت داخل مؤسستي.							
٦٩.توفر مؤسستي نظام Event Manager لإدارة تسجيلات الأحداث Events /logs							
٧٠.توفر مؤسستي نظام متكامل مخصص لإدارة قضايا أمن المعلومات من جميع الجوانب.							
٣.العلامة التجارية للجهاز المستخدم في مؤسستي هي سيسكو ، سونك وول ، ...							
٤.العلامة التجارية لبرنامج الحماية المستخدم في مؤسستي هي سوفس ، ترند مايكرو، ...							
٧١.أجهزة وبرامج أخرى ترى أنها لم تُذكر	....						
ت. الطرق المتبعة في إعداد وتحديث أجهزة وبرامج الحماية في مؤسستي							
٧٢.تم تفعيل نظام حماية من البريد الدعائي Spam في جدار الحماية							
٧٣.يتم تحديث خاصية الحماية من الفيروسات في جدار الحماية بشكل آلي							
٧٤.يتم استخدام تشفير لحماية اتصالات VPN							
٧٥.يتم تفعيل خاصية تصفية المواقع غير المرغوبة في جدران الحماية المستخدمة في مؤسستي.							
٧٦.يتم تحديث نظام تشغيل جدار الحماية (Firewall Image) بشكل دوري							
٧٧.يتم تحديث نظام تشغيل الموجهات (Router Image) بشكل دوري							
٧٨.تم إعداد لوائح التحكم بالوصول access control list في الموجهات Routers							
٧٩.يتم تحديث نظام تشغيل الوسيط (Proxy) بشكل دوري							
٨٠.يتم تثبيت التحديثات الأمنية patches للوسيط proxy بشكل دوري							

٨١.يتم مراجعة تقارير استخدام الانترنت يومياً.							
٨٢.يتخذ إجراء تقويمي لمن يسيء استخدام الانترنت.							
٨٣.يتم إعداد نظام النسخ الاحتياطي لأخذ النُّسخ الاحتياطية بشكل يومي							
٨٤.يتم تحديث مخطط الشبكة بشكل دوري							
٨٥.يتم تحديث أنظمة تشغيل المبدلات المركزية ومبدلات التوزيع(Switch Image) دورياً							
٨٦.يتم تحديث نظام تشغيل أجهزة نقاط شبكة لاسلكية (Access Points) دورياً							
٨٧.يتم تثبيت تحديثات جهزة نقاط شبكة لاسلكية (Access Points) دورياً							
٨٨.يتم إعداد مفاتيح النقاط اللاسلكية بطول ٦٤ بت							
٨٩.يتم إعداد مفاتيح النقاط اللاسلكية بطول ١٢٨ بت							
٩٠.في مؤسستي يتم إعداد المبدلات Switches لعزل حاسبات المتدربين عن موارد الشبكة.							
٩١.تستخدم مؤسستي بيئة تجربة لتثبيت التحديثات قبل اعتمادها في بيئة الإنتاج.							
٩٢.تستخدم مؤسستي بيئة تطوير لبناء وتجربة تطبيقات جديدة قبل نقلها إلى بيئة الإنتاج.							
٩٣.يستطيع مستخدمو الحاسبات المكتبية بمؤسستي لتثبيت وإزالة أي برنامج يرغبونه في حاسباتهم.							
٩٤.يستطيع مستخدمو حاسبات المعامل الوصول إلى موارد شبكة المؤسسة.							
٩٥.يستطيع المبرمجون الدخول إلى جميع التطبيقات بصلاحيات كاملة							
٩٦.يستطيع مدير نظام تشغيل الشبكة الدخول إلى جميع موارد الشبكة بصلاحيات كاملة							

المحور الثاني: نقاط الضعف التي يمكن أن تُستغل لاختراق شبكة المعلومات والتدابير الوقائية التي ينبغي اتخاذها

العبارة	مدى وضوح العبارة		مدى أهمية العبارة		مدى مناسبة العبارة للمحور		ملاحظات
	واضحة	غير واضحة	مهمة	غير مهمة	مناسبة	غير مناسبة	
ت. **نقاط الضعف التي يمكن أن تُستغل لاختراق شبكات المعلومات**							
٢٩.عدم تثبيت تحديثات أنظمة تشغيل أجهزة الخادم والحاسبات المكتبية							
٣٠.عدم تحديث أنظمة تشغيل جدران الحماية							

٣١.عدم تحديث خاصية تصفية المواقع غير المرغوبة في جدار الحماية.							
٣٢.عدم تحديث خاصية الحماية من الفيروسات في جدار الحماية.							
٣٣.عدم تحديث خاصية الحماية من البريد الدعائي Spam في جدار الحماية.							
٣٤.عدم وجود خاصية كشف ومنع التلصص IPS تُحدث يومياً في جدار الحماية.							
٣٥.عدم تحديث مكونات البروكسي.							
٣٦.وجود نظم تشغيل غير مرخصة بالشبكة							
٣٧.قلة الكفاءة المهنية للمستخدمين							
٣٨.قلة خبرة العاملين بالحماية							
٣٩.وجود كلمات مرور افتراضية في بعض الأجهزة العاملة بالشبكة.							
٤٠.وجود كلمات مرور افتراضية في بعض البرمجيات العاملة بالشبكة.							
٤١.عدم وجود سياسة للحماية							
٤٢.أداء بعض الأجهزة ضعيف ولا تستطيع تشغيل مكافح الفيروسات.							
٤٣.نقاط ضعف أخرى ترى أنها لم تُذكر:							

ث. التدابير الوقائية

العبارة	وضوح العبارة		أهمية العبارة		مناسبتها للمحور		ملاحظات
	واضحة	غير واضحة	مهمة	غير مهمة	مناسبة	غير مناسبة	
٤٤.تخصيص خادم لتحديث نظم تشغيل الحاسبات المكتبية وأجهزة الخادم.							
٤٥.تفعيل التحديث الآلي لجدران الحماية							
٤٦.تفعيل التحديث الآلي لبرامج الحماية							
٤٧.استخدام برمجيات لقياس أداء مكونات الشبكة							

لاتخاذ ما يلزم لمنع توقفها في المستقبل القريب.							
٤٨.تزويد وتفعيل خاصية كشف ومنع التلصص IPS في جدار الحماية							
٤٩.تزويد وتفعيل خاصية الحماية من الفيروسات في جدار الحماية							
٥٠.تزويد وتفعيل خاصية تصفية المواقع غير المرغوب فيها في جدار الحماية							
٥١.تزويد وتفعيل خاصية الحماية من البريد الدعائي Spam في جدار الحماية							
٥٢.استخدام قائمة مهام الحماية اليومية Check list							
٥٣.تنفيذ اختبار دوري لكشف نقاط الضعف من داخل الشبكة.							
٥٤.تنفيذ اختبار دوري لكشف نقاط الضعف بدءا من خارج الشبكة.							
٥٥.مراجعة محاولات الدخول إلى النظام وخصوصا من داخل الشبكة.							
٥٦.تدابير وقائية أخرى ترى أنها لم تُذكر:	....						

المحور الثالث: الهياكل التنظيمية المناسبة لمراكز تقنية المعلومات ومدى توافق الوظائف المستخدمة في مجال أمن شبكات المعلومات معها.

العبارة	مدى وضوح العبارة		مدى أهمية العبارة		مدى مناسبة العبارة للمحور		ملاحظات
	واضحة	غير واضحة	مهمة	غير مهمة	مناسبة	غير مناسبة	
٣٢.يوجد في مؤسستي هيكل تنظيمي معتمد ومعمم، يتضمن الإدارة/القسم الذي أعمل فيه.							
٣٣.أرى أن الهيكل التنظيمي لإدارة/مركز تقنية المعلومات الذي أعمل فيه مناسب و مواكِب							

للتطور السريع في تقنية المعلومات.							
٣٤.في مؤسستي يتم مراعاة التسلسل الإداري في المعاملات الفنية والإدارية والمالية.							
٣٥.في مؤسستي يوجد مجلس/لجنة لإدارة التعديلات (شبكات وقواعد بيانات وموقع الانترنت..).							
٣٦.يوجد قسم/إدارة/وحدة تحت مسمى أمن المعلومات أو أمن الشبكة أو ما شابه ذلك							
٣٧.يوجد في مؤسستي مسمى وظيفة مرفقة بالمهام والواجبات والمسؤوليات والصلاحيات لكل وظيفة من الوظائف المتعلقة بالحماية في إدارة تقنية المعلومات.							
٣٨.في مؤسستي يتم تبديل الموظفين العاملين بالحماية باستمرار بمبادرة من الإدارة.							
٣٩.في مؤسستي تتكرر مغادرة موظفي حماية الشبكات لوظائفهم رغبة بفرص عمل افصل.							
٤٠.المؤهل العلمي للعاملين في مجال الحماية في مؤسستي يتناسب مع مسميات وظائفهم.							
٤١.في مؤسستي يوجد مدقق يقوم بمراجعة تنفيذ السياسات Security Editor							
٤٢.ويوجد مسؤول شبكات Network Admin يقوم بإدارة توصيلات الكابلات والمبدلات							
٤٣.ويوجد موظف بمسمى ضابط أمن المعلومات Security Officer							
٤٤.ويوجد موظف يقوم بإدارة أجهزة الحماية (جدران الحماية والموجهات والنقاط الوصول اللاسلكية)							
٤٥.ويوجد موظف يقوم بإدارة برامج الحماية (برامج مكافحة الفيروسات والبريد الدعائي ...)							
٤٦.حسب رأيي، الموظفون الذين يعملون في مجال							

الحماية في مؤسستي غير كافين من حيث العدد.							
٤٧.أعاني من ضغط في العمل وأحتاج لوقت إضافي لإنجاز جميع واجباتي							
٤٨.يوجد تقدير لأعمال الحماية من قبل إدارة مؤسستي يظهر بتقديم المكافآت أو العلاوات أو الشكر.							
٤٩.مديري المباشر متخصص في إحدى مجالات تقنية المعلومات.							
٥٠.مدير إدارة تقنية المعلومات متخصص في إحدى مجالات تقنية المعلومات.							
٥١.أرى أن الدخل الذي أتقاضاه غير مناسب.							
٥٢.تولي إدارة المؤسسة التي أعمل فيها اهتمام في أمن المعلومات يظهر من خلال تخصيص ميزانية جيدة لتحسين الحماية.							
٥٣.أرى أن التدريب الذي أحصل عليه من مؤسستي كاف لتأدية عملي في مجال الحماية.							
٥٤.توفر مؤسستي عقد مع شركة خارجية لتأمين الدعم الفني لأجهزة الحماية يشمل تبديل الجهاز							
٥٥.أرى أن الدعم الفني الخاص بجدار الحماية الذي تستخدمه مؤسستي جديد.							
٥٦.توفر مؤسستي عقد مع شركة خارجية لتأمين الدعم الفني لبرامج الحماية يشمل الحضور لموقع المؤسسة لإصلاح المشكلات عند طلب ذلك.							
٥٧.أرى أن الدعم الفني الخاص ببرنامج الحماية من الفيروسات الذي تستخدمه مؤسستي جيد.							
٥٨.هل سبق وأن اشتركت في ندوات أو محاضرات أو مؤتمرات حول إدارة مراكز المعلومات							
٥٩.أو حول الأخطار والتهديدات المحتملة وخطط الطوارئ							

٦٠.أو حول التوعية في مجال في أمن المعلومات							
٦١.أو حول أنظمة الحماية (مكافحات الفيروسات و جدران الحماية)							
٦٢. هل سبق وأن اشتركت في ندوات أو محاضرات أو مؤتمرات أو دورات أُخرى ترى أهمية لذكرها:							

المحور الرابع: توفُّر إجراءات العمل في حماية شبكات المعلومات و مدى تطبيقها والعمل بها.

العبارة	مدى وضوح العبارة		مدى أهمية العبارة		مدى مناسبة العبارة للمحور		ملاحظات
	واضحة	غير واضحة	مهمة	غير مهمة	مناسبة	غير مناسبة	
٣٠.في مؤسستي يوجد وثيقة توضح طريقة تحديث جدران الحماية							
٣١.ويوجد وثيقة توضح طريقة تحديث برامج الحماية							
٣٢.ويوجد وثيقة توضح خطوات إعداد وتشغيل عمليات النسخ الاحتياطي والاسترجاع							
٣٣.يوجد وثيقة توضح تركيب برامج حماية داخل الشبكات							
٣٤.يوجد وثيقة توضح تركيب أجهزة حماية على حدود الشبكات							
٣٥.في مؤسستي يتم أخذ موافقة مجلس/لجنة التعديل عند تعديل مكونات جدار الحماية.							
٣٦.ويوجد موظف واحد على الأقل يقوم بإدارة الإجراءات (إنشاءها ، تحديثها، توثيقها، تطويرها)							
٣٧.ويوجد إجراءات عمل خاصة بإدارة عمليات تحديث التطبيقات والبرمجيات							
٣٨.وتتوفر خطة مكتوبة وتم التدرب على تطبيقها لاسترداد النظام في الحالات الطارئة.							

٣٩.ويوجد نظام لإدارة وثائق الإجراءات يتم تحديثه باستمرار.							
٤٠.يوجد صعوبات إدارية تعترض تنفيذ إجراءات إدارة نظم أمن المعلومات							
٤١.يوجد صعوبات مالية تعترض تنفيذ إجراءات إدارة نظم أمن المعلومات							
٤٢.يوجد صعوبات تدريبية تعترض تنفيذ إجراءات إدارة نظم أمن المعلومات							
٤٣.يتوفر في مؤسستي سياسة النسخ الاحتياطي والاسترجاع							
٤٤.يتوفر في مؤسستي سياسة الاستخدام المقبول							
٤٥.يتوفر في مؤسستي سياسة التدريب (لموظفي تقنية المعلومات)							
٤٦.يتوفر في مؤسستي سياسية ضمان المعلومات							
٤٧.يتوفر في مؤسستي سياسة توظيف منسوبي إدارة تقنية المعلومات.							
٤٨.يتوفر في مؤسستي سياسة توريد وتأمين الخدمات من خارج المنظمة Outsourcing							
٤٩.يتوفر في مؤسستي سياسة تقييم المعلومات من حيث درجة السرية							
٥٠.يتوفر في مؤسستي سياسة واضحة تتعلق بعمليات حفظ وتخزين المعلومات							
٥١.يتوفر في مؤسستي إجراء إتلاف الأصول المعلوماتية المنتهية الصلاحية							
٥٢.يتوفر في مؤسستي إجراء تسمية الأصول المعلوماتية وتسجيله على الوسائط المعلوماتية							
٥٣.يتوفر في مؤسستي إجراء تحديث أنظمة التشغيل							
٥٤.أرى أن نظام تشغيل ويندوز هو الأكثر تأثرا							

بالفيروسات							
٥٥.أرى أن نظام تشغيل يونكس هو الأكثر تأثرا بالفيروسات							
٥٦.أرى أن نظام تشغيل لينكس هو الأكثر تأثرا بالفيروسات							
٥٧.أرى أن نظام تشغيل ماكنتوش هو الأكثر تأثرا بالفيروسات							
٥٨.إجراءات أخرى أرى أنه من المفيد ذكرها	.....						

المحور الخامس:درجة المعرفة بالمخاطر التي يمكن أن تؤثر سلباً على أمن شبكات المعلومات، و درجة تطبيقها فعلا بحالات الحدوث.

العبارة	مدى وضوح العبارة		مدى أهمية العبارة		مدى مناسبة العبارة للمحور		ملاحظات
	واضحة	غير واضحة	مهمة	غير مهمة	مناسبة	غير مناسبة	
من وُجهة نظرك ما درجة معرفتك المخاطر التالية : (مخاطر خارجية)							
٦٤.التعدي على الكابلات وتخريبها							
٦٥.التعدي على الكابلات وتخريبها							
٦٦.اندلاع الحريق							
٦٧.حصول إغراق بسبب فيضان							
٦٨.اختراق لتعديل البيانات وتغيرها أو إتلافها							
٦٩.التعرض لهجوم إرهابي							
من وُجهة نظرك ما درجة معرفتك المخاطر التالية : (مخاطر داخلية)							
٧٠.اختراق أجهزة الخادم من داخل المنظمة (عبث،إساءة استخدام...)							
٧١.استخدام برامج بغرض التجسس من قبل المستفيدين من داخل المؤسسة							
٧٢.اختراق أجهزة الخادم من داخل المنظمة (عبث،إساءة استخدام...)							

٧٣.استخدام برامج بغرض التجسس من قبل المستفيدين من داخل المؤسسة							
٧٤.زيارة مواقع غير موثوقة تسمح بتنزيل البرمجيات الضارة							
٧٥.الإصابة بفيروسات مصدرها الانترنت							
٧٦.الإصابة بفيروسات مصدرها وسائط التخزين وذواكر الفلاش							
٧٧.تنزيل برامج غير مصرح بها.							
٧٨.سرقة الأجهزة ووسائط التخزين							
من وُجهة نظرك ما درجة أهمية التدابير الوقائية التالية:							
٧٩.توفير حراسة عند بوابات مركز البيانات على مدار الساعة							
٨٠.تجهيز مركز البيانات بنظام إطفاء الحريق والإنذار.							
٨١.قفل مركز البيانات (غرفة أجهزة الخادم وأجهزة الشبكة) بحيث لا يدخلها إلا المتخصصون ممن لديهم ترخيص بالدخول.							
٨٢.تجهيز مركز البيانات بنظام تسجيل لجميع الداخلين بالاسم والوقت وسبب الدخول							
٨٣.توفير مراقبة داخلية باستخدام كاميرات تلفزيونية مع التسجيل							
٨٤.عمل النسخ الاحتياطي والاسترجاع الآلي يومياً							
٨٥.وضع وسائط النسخ الاحتياطي في خزائن مضادة للصدمات والحريق.							
٨٦.تطبيق التشفير على وسائط النسخ الاحتياطي							
٨٧.إبعاد وسائط النسخ لاحتياطي ووسائط التخزين عن أماكن تسرب المياه							
٨٨.إتلاف وسائط التخزين والنسخ الاحتياطي							

المنتهية الصلاحية.							
٨٩.تركيب برامج مخصصة لمراقبة استخدام المستفيدين							
٩٠.وضع وسائط النسخ الاحتياطي في خزائن مضادة للصدمات والحريق.							
٩١.تطبيق التشفير على وسائط النسخ الاحتياطي							
٩٢.إبعاد وسائط النسخ لاحتياطي ووسائط التخزين عن أماكن تسرب المياه							
٩٣.إتلاف وسائط التخزين والنسخ الاحتياطي المنتهية الصلاحية.							
٩٤.تركيب برامج مخصصة لمراقبة استخدام المستفيدين							
٩٥.توفير خطة طوارئ واضحة ومعتمدة.							
٩٦.إعداد خطة واضحة للتراجع (Rollback) تطبق في حالة عدم نجاح خطط الطوارئ.							
٩٧.تدريب كل الموظفين على أمن المعلومات كل حسب واجباته الوظيفية.							
٩٨.السعي لمطابقة إجراءات العمل لتتوافق مع إحدى المعايير الدولية المعتمدة (آيزو) في مجال أمن المعلومات.							
٩٩.السعي للتوصل إلى اتفاقيات تعاون مع المتخصصين في أمن المعلومات							
١٠٠.تنفيذ اختبارات دورية لنقاط الضعف انطلاقا من داخل الشبكة.							
١٠١.تنفيذ اختبارات دورية لنقاط الضعف انطلاقا من خارج الشبكة.							
١٠٢.استخدام تشفير لقواعد البيانات							
١٠٣.استخدام التشفير لاتصالات VPN							

١٠٤.توفير مركز بيانات Data Center بديل لاستخدامه عند الطوارئ							
١٠٥.تجهيز الوسيط Proxy بخدمة توليد التقارير وتحليلها.							
١٠٦.توفير إجراءات مكتوبة ومعتمدة توضح ما يلزم لتنفيذ أعمال الحماية							
١٠٧.توفير موظف واحد على الأقل يقوم بإدارة أجهزة الحماية وتحديثها.							
١٠٨.توفير موظف واحد على الأقل يقوم بإدارة برامج الحماية وتحديثها.							
١٠٩.تأمين بديل واحد على الأقل لكل موظف يعمل في مجال الحماية.							
١١٠.توظيف الأشخاص المناسبين من حيث المؤهل والخبرات الفنية.							
١١١.تصميم أو توفير برنامج إدارة الحماية من جميع جوانبها.							
١١٢.تأمين جهاز إضافي لكل جهاز بالشبكة كجدار الحماية والموجه والوسيط							
١١٣.تأمين خادم server احتياطي لكل خادم يعمل بالشبكة مثل: DHCP،DNS، قواعد البيانات ، الويب.							
١١٤.تخصيص إدارة خاصة بأمن المعلومات							
١١٥.اشتراط امتلاك المهارات المناسبة لمستخدمي الحاسب الآلي.							
١١٦.عقد دورات تدريب للتوعية في أمن المعلومات والحماية.							
١١٧.توفير خدمة الاتصال البعيد فقط للأفراد المعتمدين من الإدارة.							

١١٨.توفير نظام مخصص لحماية البريد الالكتروني من الفيروسات والبريد الدعائي Spam.							
١١٩.تحديث نظام تشغيل أجهزة الشبكة بشكل دوري							
١٢٠.إتاحة استخدام خاصية التحقق من الصحة في جدار الحماية							
١٢١.تفعيل خاصية التشفير في جدار الحماية عند استخدام VPN							
١٢٢.توفير سياسة خاصة بكلمات المرور وتطبيقها.							
١٢٣.تدريب أعضاء الهيئة التدريسية على ما يحتاجون من أمن المعلومات.							
١٢٤.تدريب الطلاب والباحثين على ما يحتاجون من أمن المعلومات.							
١٢٥.توفير برنامج لتحكم بمنافذ الحاسبات ومشغلات الوسائط القابلة للإزالة من حيث التعطيل أو الإتاحة أو الفتح التلقائي أو الفحص قبل الفتح...							
١٢٦. تدابير وقائية أخرى ترى أهمية لذكرها	....						

الملحق رقم (٣)

أداة الدراسة في صورتها بعد التحكيم

بسم الله الرحمن الرحيم

أخي الكريم:

السلام عليكم ورحمة الله وبركاته وبعد :

الاستبانه التي بين يديك هي جزء من دراسة عن " حماية الشبكة الرئيسة من الاختراق والبرامج الضارة" : دراسة مسحية تحليلية على حماية الشبكات في المؤسسات التعليمية بمدينة الرياض" استكمالا للحصول على درجة الماجستير في أمن المعلومات .

لذا يود الباحث معرفة رأيك الشخصي وذلك بالإجابة على أسئلة الاستبانه التي بين يدك.

علما بأن البيانات التي ستدلي بها من خلال إجاباتك ستستخدم لأغراض البحث العلمي فقط.

مع الشكر والتقدير على حسن تعاونكم

الباحث

مهندس/ زكريا أحمد عمار

هـ العمل: ١٥٠٨ ت ٣٤٤٤-٢٤٦

جوال : ٠٥٠٣٤٤٢٥٧٢

الجزء الأول

البيانات الأولية

الرجاء الإجابة على الأسئلة التالية وذلك بكتابة العبارة المناسبة بالفراغات أو وضع علامة (✓) داخل المربع:

١. بيانات شخصية:

١. ☐ ذكر	٢. ☐ أنثى	٣. العمر : .....سنة
٤. ☐ وظيفتي إدارية	٥. ☐ وظيفتي فنية	٦. ☐ وظيفتي إدارية وفنية

٢. المؤهل العلمي

١. ☐ شهادة الثانوية العامة فأقـل	٢. ☐ دبلوم (سنتين بعد الثانوية)
٣. ☐ بكالوريوس (كلية جامعيــة)	٤. ☐ ماجستير
٥. ☐ دكتوراه	

٣. التخصص:

١. ☐ شبكات	٢. ☐ برمجة
٣. ☐ نظم معلومات إدارية	٤. ☐ أخرى (تُذكر) .....

٤. عدد سنوات الخبرة ....

٥. الشهادات التي حصلت عليها والمعروفة دولياً هي:

....

٦. إن المؤسسة التي أعمل بها تعد من القطاع:

٧. ☐ الحكومي	٨. ☐ الأهلي (خاص)	٩. ☐ المشترك (حكومي&خاص)

٧. المؤسسة التي أعمل بها تختص بتعليم المراحل التالية:

٩. ☐ ثانوية وما دون	١٠. ☐ معهد
١١. ☐ جامعة	١٢. ☐ مراحل مختلفة (مركز تدريب)

٨. الدورات أو الندوات أو المؤتمرات التي حضرتها تختص في مجال:

١. ☐ إدارة مراكز المعلومات	٢. ☐ الأخطار المحتملة وخطط الطوارئ
٣. ☐ التوعية في أمن المعلومات	٤. ☐ أجهزة جدران الحماية
٥. ☐ برامج الحماية من الفيروسات	

٩. نالت المؤسسة التي أعمل بها شهادة آيزو

١. ☐ لا	٢. ☐ **نعم وهي.....**

الجزء الثاني: أسئلة محاور الدراسة

المحور الأول: فيما يلي عبارات الأجهزة والبرامج المستخدمة لحماية الشبكات ونرجو منك تحديد مدى استخدام مؤسستك لتلك الأجهزة والبرامج ومدى إعدادها وتحديثها بوضع علامة (✓) بالمكان المناسب.

العبارة	نعم (١)	إلى حد ما (٢)	لا (٣)
١. الأجهزة والبرامج المستخدمة لحماية الشبكات في مؤسستي			
١.تستخدم مؤسستي واحد أو أكثر من جدران الحماية (FireWalls) عند بوابات الشبكة المحلية.			
٢.تتوفر في جدران الحماية التي تستخدمها مؤسستي منافذ كافية لتقسيم الشبكة إلى ثلاثة شبكات فرعية أو أكثر (داخلية و DMZ وخارجية).			
٣.جدران الحماية المستخدمة في مؤسستي تقبل التحديث الآلي.			
٤.تتوفر خاصية تصفية البريد الدعائي (Spam) في جداران الحماية المستخدمة.			
٥.جدران الحماية المستخدمة في مؤسستي مزودة بخاصية كشف محاولات الاختراق (IDS) فقط.			
٦.جدران الحماية المستخدمة في مؤسستي مزودة بخاصية كشف ومنع الاختراق (IPS) معاً.			
٧.جدران الحماية المستخدمة في مؤسستي مزودة بخاصية تصفية المواقع غير المرغوبة.			
٨.تتوفر خاصية اتصال الشبكة الافتراضية VPN في معظم جدران الحماية المستخدمة.			
٩.توفر إدارة مؤسستي عقد دعم فني لجدران الحماية يجدد سنويا من الشركة الصانعة.			
١٠.يوجد في مؤسستي وسيط (proxy) لتوزيع خدمة الإنترنت على المستفيدين.			
١١.يوجد نظام مخصص لمراقبة استخدام الإنترنت داخل مؤسستي.			
١٢.في شبكة مؤسستي يوجد مبدل مركزي Core Switch واحد على الأقل.			
١٣.توجد نقاط شبكة لاسلكية (Access Points) مثبتة داخل الشبكة المحلية.			
١٤.تستخدم مؤسستي نظام احترافي للنسخ الاحتياطي.			
١٥.يوجد في مؤسستي مخطط واضح لجدران الحماية والخوادم والموجهات.			
١٦.يوجد نظام مخصص لمكافحة الفيروسات داخل الشبكة.			
١٧.يوجد نظام مخصص لحماية البريد من الفيروسات والبريد الدعائي (Spams).			
١٨.توفر مؤسستي عقد دعم فني لنظام الحماية من الفيروسات يجدد سنويا.			
١٩.تستخدم مؤسستي موجه (Router) واحد على الأقل.			
٢٠.موقع مؤسستي على الإنترنت محتضن في شبكة المؤسسة.			
٢١.توفر مؤسستي نظام لإدارة تسجيلات الأحداث (Events /logs).			
٢٢.توفر مؤسستي نظام متكامل مخصص لإدارة قضايا أمن المعلومات من جميع الجوانب.			

٢.مدى تطبيق الإعدادات والتحديثات اللازمة لأجهزة وبرامج الحماية في مؤسستي	نعم (١)	إلى حد ما (٢)	لا (٣)
٢٣.يتم تحديث مخطط الشبكة دورياً.			
٢٤.يتم تفعيل خاصية الحماية من البريد الدعائي Spam في جدار الحماية.			
٢٥.يتم تحديث خاصية الحماية من الفيروسات في جدار الحماية بشكل آلي.			
٢٦.يتم استخدام كلمة مرور بطول ٨ محارف على الأقل لحماية اتصالات (VPN).			
٢٧.يتم تفعيل خاصية تصفية المواقع غير المرغوبة في جدران الحماية في مؤسستي.			
٢٨.يتم تحديث نظام تشغيل جدار الحماية (Firewall Image) بشكل أسبوعي على الأقل.			
٢٩.يتم تحديث نظام تشغيل الموجهات (Router Image) بشكل شهري على الأقل.			
٣٠.يتم إعداد لوائح التحكم بالوصول (access control list) في الموجهات (Routers).			
٣١.يتم تحديث نظام تشغيل الوسيط (Proxy) بشكل أسبوعي على الأقل.			
٣٢.يتم تثبيت التحديثات الأمنية (patches) للوسيط (proxy) بشكل أسبوعي على الأقل.			
٣٣.يتم مراجعة تقارير استخدام الانترنت يومياً.			
٣٤.يتخذ إجراء تأديبي لمن يسيء استخدام الانترنت.			
٣٥.يتم إعداد نظام النسخ الاحتياطي لأخذ النُّسخ الاحتياطية بشكل يومي.			
٣٦.يتم تحديث أنظمة تشغيل المبدلات المركزية ومبدلات التوزيع(Switch Image) دورياً.			
٣٧.يتم تثبيت تحديثات أجهزة نقاط شبكة لاسلكية (Access Points) دورياً.			
٣٨.يتم إعداد مفاتيح النقاط اللاسلكية بطول ٦٤ بت على الأقل.			
٣٩.يتم إعداد مفاتيح النقاط اللاسلكية بطول ١٢٨ بت على الأقل.			
٤٠.يتم في مؤسستي إعداد المبدلات (Switches) لعزل حاسبات المتدربين عن موارد الشبكة.			
٤١.تستخدم مؤسستي بيئة تجربة لتثبيت التحديثات قبل اعتمادها في بيئة الإنتاج.			
٤٢.تستخدم مؤسستي بيئة تطوير لبناء وتجربة التطبيقات الجديدة قبل نقلها إلى بيئة الإنتاج.			
٤٣.لا يستطيع المستخدمون بمؤسستي تثبيت وإزالة أي برنامج في حاسباتهم المكتبية.			
٤٤.لا يستطيع مستخدمو حاسبات المعامل الوصول إلى موارد شبكة المؤسسة.			
٤٥.لا يستطيع المبرمجون الدخول إلى جميع التطبيقات بصلاحيات كاملة.			
٤٦.لا يستطيع مدير نظام تشغيل الشبكة الدخول إلى جميع موارد الشبكة بصلاحيات كاملة.			

المحور الثاني: فضلاً عبر عن وجهة نظرك بوضع علامة (✓) مقابل درجة خطورة نقطة الضعف التي يمكن أن تُستغل لاختراق شبكة الحاسب وكذلك أمام درجة الأولوية للتدابير الوقائية.

العبارة	درجة الخطورة (١) أقل خطورة (٥) أعلى خطورة				
	(١)	(٢)	(٣)	(٤)	(٥)
١ - نقاط الضعف التي يمكن أن تُستغل لاختراق شبكة المعلومات					
١.عدم تثبيت تحديثات أنظمة تشغيل أجهزة الخادم والحاسبات المكتبية بانتظام.					
٢.عدم تحديث أنظمة تشغيل جدران الحماية بانتظام.					
٣.عدم تحديث خاصية تصفية المواقع غير المرغوبة في جدران الحماية بانتظام.					
٤.عدم تحديث خاصية الحماية من الفيروسات في جدران الحماية بانتظام.					
٥.عدم تحديث خاصية الحماية من البريد الدعائي Spam في جدران الحماية.					
٦.عدم وجود خاصية كشف ومنع التلصص IPS في جدران الحماية المستخدمة.					
٧.عدم تحديث مكونات أجهزة الوسيط (Proxy) بانتظام.					
٨.وجود نظم تشغيل غير مرخصة تعمل في أجهزة الشبكة.					
٩.قلة الكفاءة المهنية عند المستفيدين من موارد الشبكة.					
١٠.قلة الخبرة لدى العاملين بالحماية.					
١١.وجود كلمات مرور افتراضية في بعض الأجهزة والبرمجيات العاملة بالشبكة.					
١٢.عدم وجود سياسة للحماية.					
١٣.أداء بعض الأجهزة ضعيف ولا تستطيع تشغيل مكافح الفيروسات.					
٢- التدابير الوقائية المتخذة لتلافي نقاط الضعف	(١)	(٢)	(٣)	(٤)	(٥)
	(١) أقل أولوية، (٥) أعلى أولوية				
١٤.تخصيص خادم لتحديث نظم تشغيل الحاسبات المكتبية وأجهزة الخادم.					
١٥.تفعيل التحديث الآلي لجدران الحماية.					
١٦.تفعيل التحديث الآلي لبرامج الحماية.					
١٧.استخدام أدوات قياس أداء أجهزة الشبكة.					
١٨.تزويد وتفعيل خاصية كشف ومنع الاختراق (IPS) في جدران الحماية.					
١٩.تزويد وتفعيل خاصية الحماية من الفيروسات في جدران الحماية.					
٢٠.تزويد وتفعيل خاصية تصفية المواقع غير المرغوب فيها في جدران الحماية.					

٢١.تزويد وتفعيل خاصية الحماية من البريد الدعائي (Spam) في جدار الحماية.					
٢٢.استخدام قائمة تتضمن المهام اليومية لأعمال الحماية (Check list) .					
٢٣.تنفيذ اختبار دوري لكشف نقاط الضعف من داخل الشبكة.					
٢٤.تنفيذ اختبار دوري لكشف نقاط الضعف بدءا من خارج الشبكة.					
٢٥.مراجعة محاولات الدخول إلى النظام وخصوصا من داخل الشبكة.					
٢٦.تدابير أخرى ترى أنها لم تُذكر:					

المحور الثالث: فضلاً ضع علامة (✓) في الخانة التي تعبر عن وجهة نظرك إزاء الهيكل التنظيمي لمركز/إدارة تقنية المعلومات في مؤسستك ومدى توافقه مع الوظائف المتعلقة بأمن شبكة الحاسب معه.

العبارة	نعم (١)	إلى حد ما (٢)	لا (٣)
١.يوجد في مؤسستي هيكل تنظيمي معتمد ومعمم، يتضمن الإدارة/القسم الذي أعمل فيه.			
٢.أرى أن الهيكل التنظيمي لإدارة/مركز تقنية المعلومات الذي أعمل فيه مناسب و مواكِب للتطور السريع في تقنية المعلومات.			
٣.يتم مراعاة التسلسل الإداري في المعاملات الفنية.			
٤.يتم مراعاة التسلسل الإداري في المعاملات الإدارية والمالية.			
٥.يوجد لجنة لإدارة التعديلات (شبكات وقواعد بيانات وموقع الانترنت..).			
٦.يوجد قسم/إدارة/وحدة تحت مسمى أمن المعلومات أو أمن الشبكة أو ما شابه ذلك			
٧.يوجد في مؤسستي مسميات وظيفية للوظائف المتعلقة بالحماية في إدارة تقنية المعلومات مرفق بالمهام والواجبات والمسؤوليات والصلاحيات لكل وظيفة.			
٨.يتم تبديل الموظفين العاملين بالحماية باستمرار بمبادرة من الإدارة			
٩.تتكرر مغادرة الموظفين في مجال الحماية والشبكات لوظائفهم رغبة بفرص عمل أفضل.			
١٠.المؤهل العلمي للعاملين في مجال الحماية في مؤسستي يناسب لمسميات وظائفهم.			
١١.يوجد مدقق (Security Auditor) واحد على الأقل يراجع تنفيذ السياسات الأمنية.			
١٢.يوجد مسؤول (Network Admin) واحد على الأقل لأعمال الكابلات والمبدلات.			
١٣.يوجد موظف واحد على الأقل بمسمى ضابط أمن المعلومات (Security Officer).			
١٤.يوجد موظف واحد على الأقل يقوم إدارة أجهزة الحماية.			
١٥.يوجد موظف واحد على الأقل يقوم بإدارة برامج الحماية (برامج مكافحة الفيروسات والبريد الدعائي ومراجعة سجلات الأحداث (Events) لأجهزة الشبكة...).			
١٦.عدد الموظفين الذين يعملون في مجال الحماية في مؤسستي غير كاف.			
١٧.أعاني من ضغط في العمل وأحتاج لوقت إضافي لإنجاز جميع واجباتي.			
١٨.تثمن مؤسستي أعمال الحماية بتقديم المكافآت أو العلاوات أو شهادات التقدير.			

١٩.مديري المباشر متخصص في إحدى مجالات تقنية المعلومات.			
٢٠.مدير إدارة تقنية المعلومات متخصص في إحدى مجالات تقنية المعلومات.			
٢١.أرى أن الدخل الذي أتقاضاه غير مناسب كموظف في مجال الحماية.			
٢٢.تقوم إدارة المؤسسة التي أعمل فيها بتخصيص ميزانية جيدة لتحسين الحماية.			
٢٣.أرى أن التدريب الذي أحصل عليه من مؤسستي كاف لتأدية عملي.			
٢٤.توفر مؤسستي عقداً لتأمين الدعم الفني لأجهزة الحماية يشمل تبديل الجهاز.			
٢٥.أرى أن الدعم الفني الخاص بجدار الحماية الذي تستخدمه مؤسستي جيد.			
٢٦.توفر مؤسستي عقداً لتأمين الدعم الفني لبرامج الحماية يشمل الحضور لموقع المؤسسة لإصلاح المشكلات عند طلب ذلك.			
٢٧.أرى أن الدعم الفني لبرامج الحماية من الفيروسات التي تستخدمها مؤسستي جيدة.			
٢٨.تقوم مؤسستي بابتعاثي لحضور ندوات/مؤتمرات تتعلق بالحماية وأمن المعلومات.			

المحور الرابع: فيما يلي إجراءات العمل لحماية شبكات الحاسب ونرجو منك تحديد مدى توفرها في مؤسستك ومدى تطبيقها وذلك بوضع علامة (✓) بالخانة المناسبة.

العبارة	نعم (١)	إلى حد ما (٢)	لا (٣)
١.يوجد وثيقة توضح طريقة تحديث جدران الحماية.			
٢.يوجد وثيقة توضح طريقة تحديث نظام الحماية من الفيروسات والبرامج الضارة.			
٣.يوجد وثيقة توضح خطوات إعداد وتشغيل عمليات النسخ الاحتياطي والاسترجاع.			
٤.يتم أخذ موافقة لجنة التعديل قبل إجراء أي تعديل في أجهزة وبرامج الحماية.			
٥.يوجد وثيقة توضح أمكنة توضع أجهزة وبرامج الحماية.			
٦.يوجد موظف واحد على الأقل يقوم بإدارة الإجراءات (إنشاءها ، تحديثها، توثيقها، ...).			
٧.يوجد إجراءات عمل خاصة بإدارة عمليات تحديث التطبيقات والبرمجيات.			
٨.توجد خطة تم تدريب المعنيين على تطبيقها لاسترداد النظام في الحالات الطارئة.			
٩.يوجد نظام لإدارة وثائق الإجراءات يتم تحديثه باستمرار.			
١٠.يوجد صعوبات إدارية تعترض تنفيذ إجراءات حماية شبكة الحاسب.			
١١.يوجد صعوبات مالية تعترض تنفيذ إجراءات حماية شبكة الحاسب.			
١٢.يوجد صعوبات تدريبية تعترض تنفيذ إجراءات إدارة نظم أمن المعلومات.			
١٣.تتوفر في مؤسستي سياسة (policy) للنسخ الاحتياطي والاسترجاع.			

١٤.تتوفر وثيقة مكتوبة تتضمن خطة طوارئ خاصة بتقنية المعلومات.			
١٥.تخصص مؤسستي ميزانية لخطة الطوارئ.			
١٦.يوجد مدة زمنية تبين الحد الزمني الأدنى لإعادة تشغيل النظام.			
١٧.يوجد في خطة الطوارئ بيان واضح للأنظمة الحرجة.			
١٨.تتوفر في مؤسستي سياسة للاستخدام المقبول لتجهيزات تقنية المعلومات.			
١٩.تتوفر في مؤسستي سياسة للتدريب في تخصصات تقنية المعلومات.			
٢٠.تتوفر في مؤسستي سياسة توظيف الأفراد المناسبين في إدارة تقنية المعلومات.			
٢١.تتوفر في مؤسستي سياسة التوريد وتأمين الخدمات من خارج المنظمة (Outsourcing)			
٢٢.تتوفر في مؤسستي سياسة لتقييم درجة سرية المعلومات.			
٢٣.تتوفر في مؤسستي سياسة أرشفة وسائط حفظ البيانات.			
٢٤.تتوفر في مؤسستي إجراء إتلاف الأصول المعلوماتية (Information Assets) المنتهية الصلاحية.			
٢٥.يتوفر في مؤسستي إجراء تسمية الأصول المعلوماتية (Information Assets) وتسجيله على الوسائط المعلوماتية.			
٢٦.يتوفر في مؤسستي إجراء تحديث أنظمة التشغيل.			

المحور الخامس: فضلاً ضع علامة (✓) في الخانة التي تعبر عن وجهة نظرك إزاء العبارات التي تضمنها محور المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات الحاسب والتدابير الاحتياطية اللازمة لتجنبها، ونريد منك بيان درجة خطورة عبارات المخاطر وبيان درجة الأولوية لاتخاذ التدابير الوقائية لتجنب تلك المخاطر.

العبارة	درجة الخطورة (١) أخفض خطورة (٥) أعلى خطورة				
	(١)	(٢)	(٣)	(٤)	(٥)
١. **المخاطر الخارجية**					
١.التعدي على الكابلات وتخريبها.					
٢.اندلاع الحريق.					
٣.حصول إغراق بالمياه بسبب الفيضانات.					
٤.اختراق لتعديل البيانات وتغيرها أو إتلافها.					
٥.التعرض لهجوم إرهابي.					

٢. **المخاطر الداخلية**					
٦.اختراق أجهزة الخادم من داخل المؤسسة (عبث،إساءة استخدام...).					
٧.استخدام برامج بغرض التجسس من قبل المستفيدين من داخل المؤسسة.					
٨.زيارة مواقع إنترنت غير موثوقة تسمح بتنزيل البرمجيات الضارة.					
٩.الإصابة بفيروسات مصدرها الانترنت.					
١٠.الإصابة بفيروسات مصدرها وسائط التخزين وذواكر الفلاش.					
١١.تنزيل برامج غير مصرح بها.					
١٢.سرقة الأجهزة ووسائط التخزين.					
١٣.الدخول غير المصرح إلى مركز البيانات وتعطيل عمل أجهزته.					
١٤.تعديل إعدادات أجهزة الشبكة بطريقة يصعب تعقبها لإطالة فترة الانقطاع.					
٣. التدابير الوقائية من المخاطر الداخلية والخارجية	**درجة الأولوية** (١) أقل أولوية، (٥) أعلى أولوية				
	(١)	**(٢)**	**(٣)**	**(٤)**	**(٥)**
١٥.توفير حراسة عند بوابات مركز البيانات على مدار الساعة.					
١٦.تجهيز مركز البيانات بحساسات الحرارة والحركة ونظام الإطفاء والإنذار.					
١٧.قفل مركز البيانات (غرفة أجهزة الخادم وأجهزة الشبكة) بحيث لا يدخلها إلا المتخصصون ممن لديهم ترخيص بالدخول.					
١٨.تجهيز مركز البيانات بآلية تسجيل للداخلين بالاسم والوقت وسبب الدخول.					
١٩.توفير مراقبة داخلية باستخدام كاميرات تلفزيونية مع التسجيل.					
٢٠.عمل النسخ الاحتياطي والاسترجاع الآلي يومياً.					
٢١.وضع وسائط النسخ الاحتياطي في خزائن مضادة للصدمات والحريق.					
٢٢.تطبيق التشفير على وسائط النسخ الاحتياطي.					
٢٣.إبعاد وسائط النسخ لاحتياطي ووسائط التخزين عن أماكن تسرب المياه .					
٢٤.إتلاف وسائط التخزين والنسخ الاحتياطي المنتهية الصلاحية.					
٢٥.تركيب برامج مخصصة لمراقبة استخدام المستفيدين.					
٢٦.توفير خطة طوارئ واضحة ومعتمدة.					
٢٧.إعداد خطة للتراجع (Rollback) تطبق في حالة عدم نجاح خطة الطوارئ.					
٢٨.تدريب كل الموظفين على أمن المعلومات كل حسب واجباته الوظيفية.					
٢٩.اختبار خطة الطوارئ.					
٣٠.اعتماد ميزانية خاصة بخطة الطوارئ.					
٣١.السعي لمطابقة إجراءات العمل لتتوافق مع معايير دولية (آيزو) تتعلق بالحماية.					
٣٢.السعي للتوصل إلى اتفاقيات تعاون مع المتخصصين في الحماية.					
٣٣.تنفيذ اختبارات دورية لنقاط الضعف انطلاقا من داخل الشبكة.					

٣٤.تنفيذ اختبارات دورية لنقاط الضعف انطلاقا من خارج الشبكة.					
٣٥.استخدام تشفير لقواعد البيانات.					
٣٦.استخدام خاصية اتصال الشبكة الافتراضية (VPN).					
٣٧.استخدام نظام لإدارة الأحداث (Logs) في جميع خوادم وأجهزة الشبكة.					
٣٨.توفير مركز بيانات (Data Center) بديل لاستخدامه عند الطوارئ.					
٣٩.تجهيز الوسيط (Proxy) بخدمة توليد التقارير وتحليلها.					
٤٠.توفير إجراءات مكتوبة ومعتمدة توضح ما يلزم لتنفيذ أعمال الحماية.					
٤١.توفير موظف واحد على الأقل يقوم بإدارة أجهزة الحماية وتحديثها.					
٤٢.توفير موظف واحد على الأقل يقوم بإدارة برامج الحماية وتحديثها.					
٤٣.تأمين بديل واحد على الأقل لكل موظف يعمل في مجال الحماية.					
٤٤.توظيف أشخاص مناسبين من حيث المؤهل والخبرة بنسبة ٩٠% على الأقل.					
٤٥.تصميم أو توفير برنامج إدارة الحماية من جميع جوانبها.					
٤٦.تأمين جهاز احتياطي لجدار الحماية والموجه والوسيط و أجهزة الخادم.					
٤٧.توفير إدارة خاصة بأمن المعلومات.					
٤٨.جعل إدارة أمن المعلومات تابعة مباشرة لرئيس أو مدير المؤسسة.					
٤٩.اشتراط توفر المهارات المناسبة لمستخدمي الحاسب الآلي.					
٥٠.عقد دورات تدريب للتوعية في أمن المعلومات والحماية.					
٥١.توفير خدمة الاتصال البعيد فقط للأفراد المعتمدين من الإدارة.					
٥٢.توفير نظام لحماية البريد الالكتروني من الفيروسات والبريد الدعائي (Spam).					
٥٣.تحديث نظام تشغيل أجهزة الشبكة بشكل دوري.					
٥٤.إتاحة استخدام خاصية التحقق من الصحة في جدار الحماية.					
٥٥.توفير سياسة خاصة بكلمات المرور وتطبيقها.					
٥٦.تدريب المستفيدين من موارد شبكة المعلومات.					
٥٧.توفير برنامج للتحكم بمنافذ الحاسبات ومشغلات الوسائط القابلة للإزالة .					
٥٨.زيادة الاعتماد على أنظمة تشغيل أقل تأثرا بالفيروسات (يونكس، لينوكس..)					
٥٩.تقليل الاعتماد على نظام تشغيل مايكروسوفت كونه الأكثر تأثرا بالفيروسات.					

ملحق رقم (٤)

قائمة بأسماء المحكمين

١. أ. د. عبدالحفيظ مقدم رئيس قسم العلوم الاجتماعية بكلية الدراسات العليا بجامعة نايف العربية للعلوم الأمنية.

٢. د. وليد النمي رئيس قسم الشبكات بمركز الحاسب بجامعة الملك سعود.

٣. المهندس حسن طاهر داوود مدير برامج الحاسب بجامعة الأمير سلطان.

٤. أ. د. محمد الأفندي رئيس قسم علوم الحاسب ومدير مركز الأمير سلطان للبحوث والترجمة في جامعة الأمير سلطان.

٥. فريق دكتور عباس أبو شامة رئيس قسم العلوم الشرطية بجامعة نايف العربية للعلوم الأمنية.

٦. أ. د. أحمد عودة رئيس قسم التوثيق والإحصاء بمركز المعلومات بجامعة نايف العربية للعلوم الأمنية.

٧. د. محمد أسعد عالم عميد مركز المعلومات بجامعة نايف العربية للعلم الأمنية.

٨. أ. د. عبد العاطي الصياد عميد مركز الدراسات والبحوث بجامعة نايف العربية للعلوم الأمنية.

٩. لواء دكتور جمال مظلوم عضو هيئة التدريس في كلية العلوم الإستراتيجية بجامعة نايف العربية للعلوم الأمنية.

١٠. مهندس أسامة يحيى مدير شركة القصيبي لأنظمة المعلومات بالمملكة العربية السعودية.

المراجع العلمية

أ – المراجع العربية:

١. القرآن الكريم.

٢. الفيروز آبادي ، القاموس المحيط ، مؤسسة الرسالة دار الريان للتراث ، (بيروت، ١٩٨٧ ط٢) ص١٢١٩

٣. توماس طوم : الخطوة الأولى نحو أمان الشبكات ، ترجمة مركز التعريب والترجمة ،(بيروت: الدار العربية للعلوم، ٢٠٠٤)

٤. جايمس سيميك ،أساسيات شبكات الاتصال ترجمة: مركز التعريب والترجمة (بيروت: الدار العربية للعلوم ١٩٩٩).

٥. حسن طاهر داود، الحاسب وأمن المعلومات، (الرياض: معهد الإدارة العامة، ٢٠٠٠).

٦. حاج علي، عوض ،أمير حسين خلف – طرق التخويل والتعريف والتواقيع الرقمية ،أمن المعلومات ٣ ، منشورات مركز الدراسات الإستراتيجية.

٧. حاج عوض، علي ، د. أمير حسين خلف – أمنية نظم التشغيل والشبكات الموزعة ،أمن المعلومات ٤ منشورات مركز الدراسات الإستراتيجية.

٨. حاج علي، عوض ، د. أمير حسين خلف طرق التشفير ،أمن المعلومات ٢ ، منشورات مركز الدراسات الإستراتيجية.

٩. حاج علي، عوض ، د. أمير حسين خلف مقدمة في نظم التشفير وأمنية المعلومات ، منشورات مركز الدراسات الإستراتيجية(١).

١٠. سكامبراي، جويل ، ستيوارت ماك كلور ، جورج كيرتز – "الهاكرز" القرصنة تحت الأضواء ، أسرار وحلول لحماية الشبكات، الطبعة الثانية ، ١٤٢١هـ/٢٠٠١م ، ترجمة مركز التعريب والترجمة الدار العربية للعلوم – بيروت.

١١. نعيم، مأمون – قراصنة البرامج بلا أقنعة "الأسس النظرية والعملية لكسر حماية البرامج وطرق الوقاية المضادة" ـــ دار شعاع للنشر والعلوم الطبعة الأولى ٢٠٠٤ – حلب – سوريا.

١٢. نور، قاسم عثمان، كيف تكتب دراسةً أو رسالة جامعية، مركز قاسم للمعلومات وخدمات المعلومات، الخرطوم. ٢٠٠٤م.

١٣. مدحت أبو النصر قواعد ومراحل البحث العلمي ط١ (القاهرة: مجموعة النيل العربية،٢٠٠٤م

١٤. فايز بن عبد الله الشهري ، استخدامات شبكة الانترنت في مجال الإعلام الأمني العربي ، مجلة البحوث الأمنية ، تصدر عن مركز الدراسات بكلية الملك فهد الأمنية ، الرياض، المجلد ١٠ العدد ١٩ نوفمبر ٢٠٠١

١٥. فادي حجار تشريح الفيروسات (حلب: شعاع للنشر والعلوم، ٢٠٠٣)

١٦. محمد أمين البشري ، التحقيق في الجرائم المستحدثة، (الرياض: مركز الدراسات والبحوث ، جامعة نايف العربية للعلوم الأمنية، ٢٠٠٤ ، طبعة ١)

١٧. عفاف شمدين، الأبعاد القانونية لاستخدامات تكنولوجيا المعلومات، (دمشق: بدون ، ٢٠٠٣)

١٨. عبد الحميد بسيوني الحروب الإلكترونية وقرصنة المعلومات (القاهرة: دار الكتب العلمية للنشر والتوزيع، ٢٠٠٤).

١٩. شركة الاتصالات السعودية ، دليل الصفحات الصفراء ، الوحدة اكسبريس السعودية ش ذ.م.م الرياض٢٠٠٧-٢٠٠٨

ب -المراجع الأجنبية:

1- Anti-Hacker Toolkit, KEITH J.JONES, C.JOHNSON by Mc Graw-Hill companies (US, 2002)
2- Brenton Chress and Others: (Mariana Village Parkway, Alameda: Syb ex inc, Mastering Network Security, 2nd ed., 2003).
3- Cisco systems inc. Fundamentals of network security (Indiana: Cisco press,2004)
4- Cisco System, Inc. Cisco Networking Academy Program: First – Year Companion Guide , Cico Press, Indianapolice, (USA, 2001)
5- Chris Brenton, Cameron Hunt, Network Security (Marian Village, Alameda: Sybex,2003)
6- Chris Brenton, Cameron Hunt, Network Security (Marian Village, Alameda: Sybex,2003) p42
7- Mastering – Network security, second edition , Chris Brenton, Cameron Hunt. By SYBEX Inc. US, 2003
8- Hacking exposed Windows Server 2003 , windows security secrets & solutions, Joel Scambry , Stuart McClure. by McGraw Hill Compny United States 2003.

ت -المواقع الإلكترونية:

1. http://www.thesecuritystandard.net
2. http://en.wikipedia.org/wiki/Cyber_security_standards
3. http://www.sans.org/
4. http://coeia.edu.sa/
5. http://www.internetworldstats.com/blog.htm
6. http://www.pewinternet.org/trends.asp
7. http:www.email-marketing-reports.com
8. http:www.email-marketing-reports.com
9. http://en.wikipedia.org/wiki/Host_computer
10. http://www.answers.com
11. http://ar.wikipedia.org/wiki/
12. http://www.reference.com/browse/availability
13. http://search.ebscohost.com