حماية أمن المعلومات فى شبكة المكتبات بجامعة أم القرى

دراسة حالة

د. فاتن سعيد بامفلح
أستاذ مساعد قسم المكتبات والمعلومات
جامعة أم القرى – مكة المكرمة

مقدمة منهجية:

شغلت قضية أمن المعلومات فى الآونة الأخيرة اهتمام أفراد المجتمع والمتخصصين ، وأصبحت الصحف اليومية تطالعنا باستمرار بآخر المستجدات المتعلقة بتلك القضية وعقدت العديد من المؤتمرات التى تركزت حول مناقشة ذلك الجانب الذى شغل الشخص العادى كما شغل المتخصص . والواقع أن الحرص على حماية أمن المعلومات ليس بالموضوع الجديد على المكتبات ؛ فقد كانت المكتبات ولازالت تحمى مجموعاتها بأساليب متعددة تتمثل فى إجراءات الصيانة والتجليد والترميم وكذلك باستخدام النظم الأمنية التى تكفل حماية مجموعاتها من السرقة مثل access systems أو حراس الأمن على سبيل المثال .

وتراعى المكتبات باستمرار الموازنة بين أساليب الحماية المتبعة وبين إتاحتها لمصادر المعلومات وذلك على اعتبار أن تشديد الإجراءات الأمنية يؤدى إلى تقييد الاستخدام فى بعض الأحيان ؛ فبعض المكتبات تمنع إعارة بعض مصادر المعلومات القيمة المتوافرة بها خوفاً من ضياعها وتستعيض عن خدمة الإعارة بخدمات أخرى لإتاحة استخدام تلك المصادر .

وقد ظهرت فى المكتبات أساليب حديثة ومختلفة لحماية أمن المعلومات فى عصر شبكات المعلومات التى أصبحت أشكال التهديد فيها مختلفة عما كانت عليه فى السابق وبالتالى فإن أساليب الحماية اختلفت أيضاً .

وتبرز الحاجة للمحافظة على أمن المعلومات بدرجة أكبر فى شبكات المعلومات عنها عند التعامل مع أجهزة الحاسب الشخصية التى تعمل بصورة مستقلة ؛ حيث يمكن معها إلحاق الضرر بالمعلومات والأجهزة عن بعد دون الحاجة إلى التواجد فى نفس المكان . ويأخذ تهديد أمن المعلومات أكثر من شكل إلا أنه من الممكن إجمالها فى الآتى :

١- تعرض الشبكة ومواردها لعمليات الاختراق والتجسس والسرقة .

٢- تعرض المعلومات للإتلاف أو التحريف أو التخريب .

وفى هذه الدراسة تستعرض الباحثة أساليب حماية أمن المعلومات المتبعة فى المكتبات فى ظل استخدامها لشبكات المعلومات ، وتتناول تطبيق تلك الأساليب على شبكة المكتبات بجامعة أم القرى للتعرف على مدى كفاية تلك الأساليب المتبعة فيها لتحقيق أمن المعلومات .

وتهدف الدراسة إلى قياس كفاية الإجراءات الأمنية المطبقة على شبكة مكتبات جامعة أم القرى، والتعرف على مواطن القوة وجوانب القصو فيها وذلك فى سبيل تطوير تلك الإجراءات وزيادة إحكامها .

وتركز الدراسة من الناحية الموضوعية على الجوانب المتعلقة بحماية أمن المعلومات فى الشبكات ومدى تطبيقها على شبكة مكتبات جامعة أم القرى فى زمن إجراء هذه الدراسة والمتمثل فى عام ١٤٢١ / ١٤٢٢ هـ سواء كان ذلك فى المكتبة المركزية للطلاب أم فى المكتبة المركزية للطالبات .

وتنقسم الدراسة إلى قسمين أحدهما نظرى يعتمد على المنهج الوثائقى فى جمع المعلومات من الإنتاج الفكرى المكتوب حول الموضوع ، والقسم الثانى يمثل دراسة حالة لشبكة المعلومات بجامعة أم القرى حيث أجرت الباحثة دراسة وصفية على الشبكة القائمة فى عمادة شئون المكتبات تناولت فيها جوانب الحماية المطبقة وكيفية تطبيقها ، وقد استعانت الباحثة باستمارة لجمع المعلومات (ملحق ١) تم إرسالها إلى سعادة عميد شئون المكتبات ، كما اعتمدت الباحثة على بعض الوثائق الرسمية المكتوبة والمرتبطة بمجال الدراسة ، بالإضافة إلى إجراء بعض المقالات مع كل من مدير المكتبة المركزية ، ونائب رئيس قسم الحاسب الآلى بالمكتبة المركزية ، والمسئول عن الشبكات فى مركز المعلومات والحاسب الآلى والتطوير الجامعى بالجامعة .

وتجيب الدراسة على التساؤلات التالية :

١- ما الإجراءات الأمنية المتبعة فى شبكة المعلومات بعمادة شئون المكتبات بجامعة أم القرى ؟

٢- ما الإجراءات الأمنية التى تفتقدها شبكة المعلومات بالعمادة ؟

٣- هل تعد الإجراءات الأمنية التى تتبعها العمادة كافية ؟

٤- كيف يمكن تطوير الأساليب المتبعة لحماية أمن شبكة معلومات العمادة ؟

وقد ظهرت العديد من الدراسات السابقة التى تناولت موضوع أمن المعلومات ومن بينها دراسة Rawley - I [1] الصادرة عام ١٩٩٥م والتى تناولت الجوانب التى تهدد أمن المكتبات والمعلومات سواء فى شكلها التقليدى أم فى غيره بما فى ذلك نظم الحاسبات الآلية ، واستعرضت الدراسة السياسات الأمنية ومكوناتها ، كما تناولت تأثير التهديد وفقدان الأمن على المكتبات ، مشيرةً إلى أنواع المخاطر التى تتعرض لها .

وفى عام ١٩٩٧م صدرت دراسة

Lervane F[٢] التى تناولت الجوانب المتعلقة بأمن شبكة المعلومات فى نظام Illinais I L L Inet an-line بعد إدخال الفهرس الموحد المباشر online unian cataloging ، وقد أشارت الدراسة إلي المفاهيم العامة المتعلقة بأمن الشبكات ، كما تناولت بعض الاعتبارات الفنية التى تراعى على مستوى محطات العمل وأجهزة الخادم الخاصة بالشبكات المحلية LAN server وأجهزة الخادم الخاصة بالويب web server ، كما تعرضت الدراسة للجوانب المتعلقة بتفاعل الأفراد مع الحاسبات على اعتبار أنها تمثل جانباً من الجوانب الهامة التى ينبغى مراعاتها لتطبيق النظام الأمنى .

وفى عام ١٩٩٨م استعرضت دراسة أشرف الغنيمى[٣] الطرق المتعددة لانتهاك أمن المعلومات فى نظم الحاسب الآلى وأساليب الحماية منها ، وأوضحت المخاطر التى تهدد أجهزة الحاسب بما فى ذلك الفيروسات وكيفية تحقيق الحماية منها، وقد خصصت الدراسة فصلاً للجوانب المتعلقة بأمن شبكات المعلومات والمخاطر الأمنية التى تتعرض لها .

وفى عام ٢٠٠٠م صدرت دراسة لكل من Elawkins - S و Yen L - E و Thaw L - E[٤] تناولت الطرق المتعددة لتحقيق أمن البيانات للهيئات المرتبطة بشبكة الإنترنت ، سواء كان ذلك عند نقل تلك البيانات عبر الشبكة أو عند تخزينها ؛ بما فى ذلك التشفير ، والحوائط النارية ، والشبكات الخاصة .

وفى العام نفسه صدرت دراسة لحسن طاهر داود[٥] تناولت مفهوم أمن المعلومات وكيفية تحقيقه سواء على مستوى تطبيق الأمن المادى للمنشآت أو للأجهزة أو للأفراد ، أم من خلال تشفير البيانات ، أم ما سوى ذلك من أساليب ، كما تناولت جرائم الحاسب المختلفة وفيروسات الحاسب . وأوضحت الدراسة كيفية تحقيق أمن التطبيقات ، وأمن قواعد البيانات ، وأمن شبكات نقل المعلومات ، وأمن شبكات إنترانت المحلية ، وأمن شبكة الإنترنت .

المخاطر التى تتعرض لها الشبكات :

هناك أساليب عديدة تتبع لحماية الشبكات منها ما يخص التجهيزات المادية ومنها ما يخص البرامج والبيانات ، منها ما يتم محلياً فى موقع تجهيزات الشبكة ومنها ما يتم لحماية الشبكة خلال الاتصال عن بعد . وقبل الإشارة إلى أساليب الحماية ينبغى التعرف على أبرز المخاطر التى تتعرض لها الشبكات ، وتتمثل فى الآتى :

١- اقتحام الهاكرز Hackers (*) والكراكرز Krackers (**) للشبكة مما يؤدى إلى تفشى أسرار العمل والعاملين ، أو تخريب البيانات وإتلافها ، وذلك على اعتبار أن وصول أشخاص غير مصرح لهم إلى ملفات البيانات

(*) الهاكرز Hackars : (هو الشخص الذى حقق مهارة تقنية عالية ويجد متعة خاصة فى الدخول غير المشروع إلى أنظمة الحاسبات الكبيرة عبر الشبكات ، وذلك لمجرد سعادته بالتغلب على التحدى المتمثل فى التغلب على نظام الحماية والأمان الذى تستعمله الشركة)[٦] .

(**) الكراكر Kracker : شخص يخترق النظم الأمنية بغرض سرقة أو إفساد البيانات ، أي أن هدفه تخريبى أو إجرامى[٧] .

قد يعرض البيانات للتغيير أو التعديل أو المسح وبالتالى يؤدى إلى تخريب البيانات أحياناً وإلى سرقتها فى أحيان أخرى .

٢- تعليق شخص لمعدات معينة على الكابلات بغرض التنصت عليها .

٣- مراقبة خطوط الهاتف والتجسس على مستخدمى الشبكة .

٤- إقحام الفيروسات للشبكة سواء كانت فيروسات مزعجة فقط أم مدمرة تعرض أجهزة الشبكة وبياناتها للتلف أو الفقد .

٥- إطلاع الأشخاص المصرح لهم باستخدام الشبكة عن معلومات غير مصرح لهم بالإطلاع عليها .

٦- التشويش على الإشارات المنقولة عبر الكابلات .

٧- تعطيل أحد الأشخاص لنظام الأمن الخاص بالشبكة أو كشفه لإجراءات الحماية المتبعة .

وإن كان من الممكن تعرض الشبكة للمخاطر السابقة وغيرها سواء تم استخدامها من نفس الموقع أم عن بعد ، إلا أن هناك مخاطر أخري تتعرض لها الشبكة فى الموقع نفسه فقط ، فى حين تؤثر على استخدامها سواء عن قرب أم عن بعد ، وتتمثل فى الآتى :

١- سرقة الأقراص المحملة عليها البيانات مما يؤدى إلى فقدان البيانات وتفشى أسرار عن الأشخاص وعن العمل .

٢- تخريب الأجهزة سواء بقصد أو بدون قصد مما يؤدى إلى انقطاع الخدمة .

٣- إغلاق أجهزة الخادم مما يؤدى إلى توقف الشبكة عن العمل .

٤- تعرض المكان للحريق مما يؤدى إلى فقدان البيانات وتلف الأجهزة .

٥- تعطل مولد الطاقة مما يؤدى إلى توقف الشبكة وانقطاع الخدمة .

٦- تعطل مكونات الشبكة مثل الأقراص الصلبة على سبيل المثال[٨] .

ويتضح مما سبق أن ما تتعرض له الشبكة من مخاطر فى الموقع نفسه يفوق ما يمكن أن تتعرض له عن بعد ، وعلى الرغم من ذلك إلا أن إلحاق الأذى بالشبكة عن بعد يعد أكثر سهولة وأكثر خطورة من إلحاق الأذى بها فى الموقع نفسه وذلك للإعتبارات التالية[٩] :

١- أن الشخص يمكنه الوصول إلى المعلومات عن بعد دون الحاجة لتجاوز الأسوار والأبواب المغلقة أو الحراسة التى قد تخصص فى موقع تواجد أجهزة الشبكة .

٢- يمكن رؤية المستخدم فى الموقع وكشف ما يفعله بالأجهزة وما يفعله بالبيانات بسهولة ، أما فى الاتصال عن بعد فلا يمكن معرفة الشخص المتصل بالشبكة حيث أن كل ما يظهر هو الحساب account الذى يستخدمه ، وهو الأمر الذى لا يعبر عن المستخدم الفعلى للشبكة .

٣- استخدام كابلات غير محمية للاتصال بالشبكة لربط المتصل عن بعد يؤدى إلى صعوبة حماية الشبكة نظراً لصعوبة منع خط الهاتف

العمومي من تعرضه للمراقبة فى نقطة معينة خلال الاتصال بالشبكة .

وهناك أساليب عديدة تتبع لحماية الشبكة والمحافظة على أمن المعلومات فيها ، ولابد من مراعاة تطبيق بعض تلك الأساليب عند التخطيط للشبكة وإنشائها ، فى حين يراعى البعض الآخر عند اختيار البرامج ، هذا إلى جانب الأساليب المرتبطة بالقائمين على الشبكة ومستخدميها . وفيما يلى إيضاح لأبرز الأساليب المتبعة لحماية الشبكات :

اولاً : اساليب الحماية الفيزيائية :

Physical security

تتمثل فى اختيار المكان الملائم والتجهيزات الأكثر حفاظا على الأمن . ولتحقيق هذا المستوى من الحماية لابد من مراعاة الآتى[٤٠] :

١- تخصيص غرف مغلقة لحفظ أجهزة خادم الشبكة servers فى حالة وضعها فى غرف مركزية ، أما إذا لم يكن ذلك متاح فلابد من حفظ أجهزة الخادم ضمن غرض الإداريين .

٢- اختيار الكابلات الأكثر حماية للمعلومات كلما كان أمن المعلومات ضرورياً للهيئة ، وتتمثل فى كابلات الألياف الضوئية Filer Optics وذلك على اعتبار أنها تلغى الإشعاع الثانوى للكابلات وبالتالى تمنع التنصت على البيانات خلال نقلها عبر الكابلات .

٣- تركيب تمديدات وكابلات الشبكة فى أماكن محمية غير معرضة لوصول غير المختصين لها، بحيث لا تكون ظاهرة للعيان ، فيمكن على سبيل المثال تمريرها عبر الجدران وفوق السقف وتحت الأرض حتى تتم حمايتها قدر الإمكان من أجهزة التنصت وكذلك حمايتها من التعرض للقطع أو الثنى فى حالة وضعها تحت قطع المفروشات الثقيلة .

٤- استخدام الكابلات المغلفة وذلك لتقليل الإشعاع الثانوى المنبثق من خلالها ، ويمكن إضافة أكثر من غلاف عليها لمنع الإشعاع نهائياً .

٥- تأمين النوافذ والفتحات الأخري الموجودة فى غرفة الخادم خصوصاً إذا كانت قريبة من الأرض .

٦- تأمين الأبواب والمنافذ كالنوافذ باستخدام أجهزة إنذار آلية تقوم بتشغيل أجراس للتنبيه فى حالة دخول أشخاص للموقع فى غير أوقات العمل .

٧- توفير وسائل مراقبة للموقع مثل الدوائر التلفزيونية المغلقة ، وذلك لإتاحة المراقبة بعد ساعات الدوام .

ثانياً : ضبط الوصول إلى الشبكة وإتاحة مواردها :

Access control system

من الضرورى ضبط الوصول إلى الشبكة لحمايتها من التعرض لعمليات الاقتحام ، ولا يقتصر الأمر هنا على حماية الشبكة من الاقتحام من قبل أشخاص غير مصرح لهم نهائياً بالدخول إليها واستخدام مواردها ، ولكن يتجاوزه إلى حمايتها أيضاً من محاولة دخول أشخاص مصرح لهم إلى ملفات ومصادر غير مصرح لهم باستخدامها . ولتحقيق ذلك لابد من تخصيص اسم

أو رقم تعريف لكل مستخدم للشبكة User ID وكلمة مرور Password حيث تعد هذه هى الخطوة الأولى المتبعة لمنع اقتحام الشبكات يتبعها الحقق من أن المستخدم لديه حقوق ممارسة ما يريد ممارسته على موارد الشبكة مثل حق الإنشاء للملفات والفهارس ، أو حق المسح والاستعراض أو التغيير أو الفتح والقراءة أو الكتابة ... إلخ ويمكن أن يمنح المستخدم حقاً أو أكثر من تلك الحقوق حسب تصنيفه ، كما يمكن تخصيص صفات للملفات نفسها مثال : ملف للقراءة فقط ، ملف للقراءة والكتابة ، ملف غير قابل للإلغاء ، ملف غير قابل للنسخ .. وهكذا ...[١١] . وبذلك يتضح أن هناك شكلين متاحين لضبط إتاحة الوصول إلى الشبكة وهما على النحو التالى :

أ – إتاحة على مستوى مشاركة :

يتم وفقاً لهذا الشكل تحديد اسم تعريف وكلمة مرور لكل مصدر متاح للمشاركة على الشبكة ، ويتم استخدام نفس الاسم وكلمة المرور من قبل كل مستقبل يريد الوصول إلى هذا المصدر .

ويحدد لكل مصدر مستوى الإتاحة الخاص به مثال : قراءة فقط ، أو كتابة فقط ، أو مشاركة كاملة ... إلخ .

ويعيب هذا الشكل انه يتطلب من المستخدم تذكر كلمات مرور متعددة كل منها خاصة بمصدر من مصادر المشاركة ، وبذلك فإنه يصعب استخدامه كلما زاد عدد موارد الشبكة لأن ذلك يعنى زيادة عدد كلمات المرور ، وهو بذلك أكثر ملاءمة للشبكات الصغيرة ، ويفيد فى الاستخدام مع شبكات النظير للنظير peer ta peer . ومن عيوبه أيضاً أنه من السهل تفريط الشخص بكلمة المرور الخاصة بالمورد وتعريف آخرين بها حيث أنها ليست كلمة المرور الخاصة به شخصياً .

ب– إتاحة على مستوى مستخدم :

يتم وفقاً لهذا الشكل تحديد اسم تعريف وكلمة مرور لكل مستخدم ، ويتم تحديد لائحة المستخدمين إلى الموارد أو الموارد المصرح لهم باستخدامها ، وتتم إضافة أى مستخدم جديد لتلك اللائحة أو حذف مستخدم منها عند الحاجة لذلك ، ويمكن تحديد مستوى الإتاحة الممنوح لكل مستخدم أو مجموعة متسخدمين بحيث يحدد ما إذا كان مصرح له بالقراءة فقط أم التعديل أم الإلغاء أم غير ذلك .

ويتميز هذا الشكل بأنه لا يتطلب من المستخدم أن يتذكر سوى كلمة مرورة واحدة لتسجيل الدخول إلى موارد الشبكة ، وكذلك من الصعب على أى شخص أن يمنح كلمة مرور خاصة به لشخص آخر لاستخدامها كما هو الحال بالنسبة لمستوى المشاركة[١٢] .

ولابد على المستخدم من مراعاة القواعد المتبعة لحماية كلمة المرور وذلك لضمان عدم كشفها من قبل الآخرين ، ومن تلك القواعد مايلى :

أ – تغيير كلمة المرور بانتظام ، على أن يراعى عدم الإبقاء عليه أكثر من ٣٠ يوماً دون تغيير .

ب– عدم استخدام كلمات من السهل على الآخرين تخمينها مثل الكلمات القصيرة

والمألوفة والمرتبطة بأمور شخصية مثل اسم الشخص أو أسماء أبنائه أو المقربين إليه أو تاريخ ميلاده أو الفريق المفضل لديه ، أو الكلمات المرتبطة بمجال عمله ... وما شابه ذلك .

جـ- عدم استخدام كلمات مرور قصيرة ، حيث ينصح بأن يصل عدد حروفها إلى ١١ حرف[١٣] .

وقد ظهرت أساليب متعددة للتحقق من هوية المستخدم ومن ذلك حفظ كلمات المرور فى غير شكلها المطبوع ، ومن الأساليب المتبعة لذلك ما يلى :

- **استخدام البطاقات الذكية Smart Cards :**

هى بطاقات تختزن فيها المعلومات مثل اسم الشخص وبياناته وكلمة المرور الخاصة به على شريط مغناطيسى وعند رغبة الشخص فى الدخول للشبكة أو استخدام موادها فعلية تمرير البطاقة خلال ماسح رقمى يعمل على قراءة البيانات المختزنة عليها ومضاهاتها بالمختزنة فى النظام فإذا تطابقت يسمح له بالدخول والاستخدام .

- **تقنية البيولوجيا الإحصائية**

Biometric devices

هى تقنيات تعرف بهوية المستخدم بشكل منفرد عن طريق بصمة إصبعه أو بصمة يده أو بصمة صوته أو غير ذلك من معرفات لا يمكن أن تتشابه بين الأشخاص ، وتحول تلك التقنيات تلك المعرفات إلى إشارات رقمية تحفظ فى ملف لكلمات المرور ، وعند محاولة الشخص الدخول إلى الشبكة واستخدام مواردها يقوم بإظهار بصمة يده أو إصبعه أو عينه أو صوته للماسح scanner فيتم التعرف على البصمة وتحويلها إلى إشارات رقمية ومقارنتها بالنسخة المختزنة فى النظام فإذا تطابقت معها بدرجة كافية يسمح النظام للشخص بالدخول إلى الشبكة أو المورد المطلوب[١٤] .

وتسمح نظم تشغيل الشبكات الحديثة بمراقبة النظام monitoring ومتابعة نشاطات المستخدم على الشبكة ومواردها من خلال اتباع سياسة التدقيق lagging security التى تتيح معرفة من يفعل ماذا على الشبكة ؟ وذلك بمتابعة عناصر متعددة على النحو التالى :

أ - تتبع نجاح أو فشل كل محاولة من محاولات دخول كل مستخدم للشبكة .

ب- تتبع نجاح أو فشل كل محاولة من محاولات المستخدم للوصول للملفات والموارد الأخرى على الشبكة .

جـ- تتبع نجاح أو فشل كل ممارسة من كل مستخدم للحقوق الممنوحة له .

د - تتبع نجاح أو فشل كل محاولة من محاولات التعديل فى سجلات المستخدمين والمجموعات .

هـ - تتبع نجاح أو فشل كل محاولة لتعديل سياسة الحماية بما فى ذلك تعديل حقوق المستخدمين أو سياسة التدقيق أو ما سوى ذلك .

و - تتبع نجاح أو فشل كل محاولة لإعادة تشغيل النظام أو إقفاله .

ز - تتبع نجاح أو فشل كل محاولة معالجة للنظام مثل استخدام التطبيقات وما سوى ذلك[١٥]

ويتضح مما سبق أن نظام التدقيق يعطى مؤشرات لمحاولات اقتحام الشبكة واختراق أمنها ، ولابد من ضبط هذا النظام بحيث تتم مراجعته كل فترة زمنية (يوم أو أسبوع) وإلغاء المعلومات القديمة بعد تخزينها فى ملفات للرجوع إليها عند الحاجة[١٦] .

ثالثاً : تشفير البيانات Encryption :

يعرف التشفير بأنه عملية تشكيل البيانات باستخدام خوارزمية algarithm معينة تسمى المفتاح key تصبح بها غير قابلة للقراءة إلا بعد استخدام الخوارزمية لفكها . ويتم عادة تشفير البيانات قبل إرسالها عبر الشبكة وذلك لضمان سلامة وصولها دون التعرض لأي عملية تجسس أو تحريف لمضمونها ، على أن يتم فك الشفرة لدى مستقبل الرسالة باستخدام مفتاح فك الشفرة[١٧] .

وينبغى الحرص على تشفير البيانات عند الرغبة فى إرسالها عبر الشبكة ، سواء كانت تلك البيانات كلمات مرور أم أرقام بطاقات الائتمان أم رسائل بريد إلكترونى أم ملف أم غير ذلك . وكلما كانت سرقة البيانات تمثل خطورة كلما هناك ضرورة أكبر لتشفيرها .

ويمكن قراءة البيانات المشفرة واضحة من قبل أى شخص يعرف مفتاح الشفرة . ويتم فى بعض الأحيان كسر الشفرة من قبل آخرون والتعرف على مفتاحها ، وكلما كان مفتاح الشفرة طويل كلما كان من الصعب كسرة ، فعلى سبيل المثال يسهل كسر مفتاح طوله ٨ بت فى حين أنه من الصعب كسر شفرة بطول ١٢٨ بت . وهناك شفرات بطول ٤٠ بت وهى شائعة الاستخدام فى العالم ، وكذلك شفرة بطول ٥٦ بت كالمستخدمة من قبل الحكومة الأمريكية والمعتمدة على نظام (DES) Data Encryption Standards وتمنع الحكومة الأمريكية الشركات من انتاج برامج تشفير تستخدم شفرة أكثر من طول ٤٠ بت إلا فى نطاق محدود وذلك لاحتياطيات أمنية[١٨] .

انواع التشفير :

للتشفير نوعان هما :

١ . التشفير المتماثل Symmetric Encryption :

يستخدم فيه المفتاح نفسه للتشفير وفك الشفرة ، وبذلك فإن المفتاح يكون معروفاً من قبل كل من مرسل الرسالة ومستقبلها ، ولا يتم إرسال المفتاح من الرسالة ولكنه يرسل بوسيلة أخرى .

وحرصاً على حماية سرية المفتاح وعدم اطلاع الغير عليه عند إرساله إلى مستقبل الرسالة ، فقد استخدمت كتب للأكواد secure code book ، وتتضمن قائمة بمفاتيح التشفير التى يجب أن تستخدم بطرق محددة ، فعلى سبيل المثال فإن أى رسالة ترسل يوم الأربعاء يتم استخدام مفتاح A لفك شفرتها . وتفقد كتب الأكواد قيمتها إذا ما سرقت لأن ذلك يعنى كشف المفتاح من قبل الغير .

ب- التشفير غير المتماثل :

Asymmetric Encryption

يستخدم فيه مفتاحان لكل مستخدم ؛ أحدهما مفتاح عام public key معروف من قبل

الآخرين حيث يسجله الشخص عادة مع توقيعه على البريد الإلكترونى e-mail signature وفى حالة الرغبة فى إرسال رسالة مشفرة إلى ذلك الشخص يتم استخدام ذلك المفتاح العام لكتابة الشفر ، أما لفكها فيستخدم مفتاح خاص private key لا يعرفه سوى المستقبل نفسه ، ويستخدمه لفك الشفرة المكتوبة باستخدام مفتاحه العام .

وعلى الرغم من ارتباط كل من المفتاح العام والخاص ببعضهما إلا أن أى منهما لا يدل على الآخر مطلقاً ، فلا يمكن الاستدلال على المفتاح الخاص من خلال العام أو العكس[١٩] .

وهناك طرق متعددة للتشفير تتراوح فى درجة تعقيدها ؛ فقد تكون سهلة للغاية ولا تتعدى فكرة الاستبدال كما هو الحال فى «شفرة قيصر» التى تمثل فى أبسط صورها استبدال كل حرف فى الأبجدية بحرف آخر وفقاً لمفتاح الشفرة المحدد والذى قد يكون رقم (٣) على سبيل المثال وبالتالى يتم استبدال كل حرف من حروف النص الأصلى بثالث حرف يليه فى الأبجدية ، ويقوم مستقبل الرسالة بفك الشفرة باستخدام نفس المفتاح الذى يمثل رقم (٣) فى هذا المثال فيعيد الحروف الأصلية للرسالة .

وقد تم تطوير طريقة الاستبدال حتى تصبح أكثر تعقيداً وبالتالى يصبح كسرها أمراً أكثر صعوبة فاستخدمت طريقة استبدال الحرف الأول فى الأبجدية بالحرف الذى يليه واستبدال الحرف الثانى بالحرف الذى يليه بحرفين واستبدال الثالث بثالث حرف يليه فى الأبجدية ثم نعود لنستبدل رابع حرف بأول حرف يليه وهكذا ... ووفقاً لهذا المثال فإن حرف الألف يستبدل بحرف الباء ، وحرف الباء يستبدل بالثاء ، أما التاء فيستبدل بالحاء ، فى حين يستبدل حرف الثاء بالحرف الذى يليه وهو الجيم وهكذا ....

وقد تكون الشفرة أكثر قوة وتعقيداً من فكرة الاستبدال كما هو الحال بالنسبة لأسلوب تشفير البيانات القياسى Data Encryption Standards (DES) وهو أيضا أسلوب من أساليب استخدام المفتاح السرى كما هو الحال بالنسبة للطريقتين السابقتين ، وهذا الأسلوب هو المتبع من قبل الحكومة الأمريكية منذ عام ١٩٧٧م حيث اعتمدته بعد أن أجرت عليه تعديلات كثيرة بعد أن طورته فى منتصف السبعينات شركة IBM .

وهناك أساليب أخرى للشفرة تعتمد على استخدام المفتاح العام public key منها نظام خوارزمية (RSA) Rivest, Shamir, Adleman للتشفير الذى ظهر عام ١٩٧٨م بواسطة ثلاث علماء هم رايفست وشامير وأدلمان . ويمكن الحصول على هذا النظام فى شكل رقيقة chip يتم تركيبها فى الحاسب الآلى ، وتعمل على التشفير وفك الشفرة ، ولكن هذه الرقائق غير متاحة فى كل دول العالم لاعتبارات أمنية[٢٠] .

رابعاً: استخدام الحوائط النارية :

الحائط النارى هو عبارة عن برنامج Soft-ware أو عتاد Hardware لحماية موارد الشبكة من مستخدمى الشبكات الأخرى . وتستخدم فى حالة ارتباط بشبكات واسعة WAN ، وتعمل على منع المستخدمين الخارجيين من الوصول إلى موارد الشبكة وبياناتها الخاصة[٢١] .

وتمثل الحوائط النارية نظاماً أمنياً قد يقتصر على برنامج فقط يحمل على جهاز الخادم server، وقد يتجاوز ذلك أحيانا ليشمل حلولاً متكاملة تضم برنامج وأجهزة مخصصة يعمل عليها ومزودة بمودمات وبطاقات شبكات[٢٢] .

وتعمل هذه الحوائط كفلتر أو مصفاة لاختبار كل محاولات الدخول للشبكة بحيث لا تسمح بالمرور إلا للاتصالات المسموح بها وتحجز كل ما عدا ذلك ، وبذلك فإن دورها يشمل الآتى :

١- فحص كل الأنشطة الداخلة إلى الشبكة من مصادر خارجية مثل الإنترنت أو الشبكات الواسعة WAN الأخرى .

٢- ضبط المنافذ ports المستخدمة بحيث يسمح باستخدام منافذ معينة لأغراض معينة ؛ فعلى سبيل المثال إذا أتيح منفذ 21 لنشاط FTP فإنه لن يسمح بدخول FTP من منفذ آخر .

٣- رفض وصول أنشطة معينة من عناوين محددة[٢٣] .

ويراعى فى الحوائط النارية ألا تؤدى إلى إعاقة عمل مستخدمى الشبكة الفعليين حتى تؤدى الغرض منها على النحو المطلوب . وتعمل حوائط النار عادةً وفقاً لقواعد أمنية محددة يضعها مدير الشبكة الداخلية ؛ كأن تسمح سياستها بالمرور من داخل الشبكة إلى البيئة الخارجية (الشبكة الخارجية) بحرية فى حين لا تسمح فى المقابل بالمرور من الخارج إلى الداخل نهائياً أو تسمح به فى حدود معينة كالسماح بالمرور لمستفيدين دون غيرهم ، أو لمواقع دون غيرها أو ما شابه ذلك .

وهناك اتجاهان متبعان لضبط الفعل التلقائى default للحوائط النارية وهما على النحو التالى :

١) أن يكون الفعل التلقائى default هو الإباحة : ويقصد به أن كل ما لم ينص على منعه فهو مباح .

٢) أن يكون الفعل التلقائى default هو المنع : ويقصد به أن كل ما لم ينص على إباحته فهو ممنوع .

ويعد الاتجاه الثانى هو الأكثر إحكاماً للأمن ، أما الأول فهو الأفضل بالنسبة للمستفيدين[٢٤] .

وقد تتم الإباحة أو المنع بناءً على اسم المستخدم وكلمة المرور ، أو عنوان TP ، أو رقم هاتف المتصل فى حالة السماح بالدخول عبر اتصال dial in . وتجدر الإشارة إلى أنه على الرغم من أن الحوائط النارية تحمى الشبكة من هم خارج حدودها ، كما يمكن أن تحمى جزءاً من الشبكة بعزلة عن باقى أجزائها ، إلا أنها على الرغم من ذلك لا تحمى من خطر العاملين داخل الحوائط[٢٥] .

وتصدر تقارير عن الحوائط النارية تبين نشاطها خلال فترة معينة مما يتيح متابعة محاولات اختراق الشبكة ، وللتأكد من استمرار فعالية الحوائط النارية فإنه يجب تحديثها بصورة منتظمة .

ويصم بعض العتاد hardware خصيصاً ليكون حائطاً نارياً فقط بحيث لا يؤدى وظائف أخرى على الشبكة ؛ ومن ذلك bloch box system ، وقد تكون أجهزة تقوم بوظائف أخرى إلى جانب عملها كحوائط نارية لتحميل برامج حوائط النار عليها ؛ ومن ذلك :

١) الراوتر rauter : وتؤدى أبسط ما يمكن أن تقدمه أنواع الحوائط النارية حيث تعمل كحاجز مصفى filtering firewalls يقوم بفحص عناوين المعلوماتTP addresses وتحديد ما يسمح بمروره وما يمنع مروره منها .

٢) البروكسى أو الوكيل proxy : ويطلق عليها حوائط نار البروكسى proxy firewalls وتعمل على فحص المعلومة قبل مرورها من الشبكة الخارجية إلى الشبكة الداخلية[٢٦] .

خامساً: برامج الحماية ضد الفيروسات :

Virus protection software

الفيروس virus هو برنامج مصم لتحقيق الهدفين التاليين :

أ . الانتشار من خلال إنشاء نسخ من نفسه وكل نسخة تنسخ نفسها تلقائياً وتنشر فى المزيد من أجهزة الحاسب الآلى .

ب- إلحاق الأذى بالبرامج أو الأجهزة .

وقد لا يتجاوز تأثير الفيروس بعد انتشاره أداء عمل غير ضار كعرض رسالة ساخرة على سبيل المثال ، فى حين يلحق فى أحيان أخرى ضرراً بالغاً بالحاسبات مثل مسح المعلومات من قرص التخزين ، أو تشتيت البرامج ، أو حذف التطبيقات ، أو خلق غير مفهومة ، أو تخريب القرص الصلب[٢٧] .

انواع الفيروسات :

يمكن تقسيم الفيروسات إلى نوعين رئيسيين هما فيروس الماكرو macro virus ، وفيروس قطاع التشغيل Baat sectar virus وكل من النوعين يختلف فى طريقة إصابته لأجهزة الحاسب ، كما يختلف فى طريقة تأثيره عليها .

أ . فيروس الماكرو macro virus :

هو عبارة عن برنامج صغير مكتوب باستخدام لغة برمجة داخلية للتطبيقات مثل فيجوال بيسيك للتطبيقات Visuall Basic Application (VBA) ، ويقوم فيروس الماكرو على عمل نسخ من نفسه بداخل الملفات المنشأة باستخدام البرامج التطبيقية مثل برامج Win Word ، Excel . ويعمل الماكرو عند فتح أو إغلاق الملف أو عند حفظ ملف أو أثناء تشغيل البرنامج .

ب- فيروس قطاع التشغيل :

Boot sector virus

تتركز هذه الفيروسات فى قطاع التشغيل لأقراص الحاسب الآلى ، ولا تحتاج كالنوع السابق إلى ملفات للدخول إلى الجهاز حيث يصاب الجهاز بالفيروس عند محاولة تشغيله من خلال قرص مصاب بالفيروس . وبتشغيل جهاز الحاسب ينتقل الفيروس إلى الذاكرة ويحدث عدوى لكل قرص يتم تشغيله على الجهاز ، ويقوم الفيروس بكتابة نسخة من نفسه على كل قرص سليم ليصيبه بالعدوى[٢٨] . ويسبب هذا النوع من الفيروسات ظهور رسالة خطأ عند تشغيل الحاسب الآلى تتضمن الآتى : missing operating system أو system or hard disk not found

وعلى الرغم من أن الانتشار بالنسخ التلقائى يعد أحد السمات المميزة للفيروسات ، إلا أن

مصطلح فيروس يطلق أيضاً على برامج أخرى مصممة لإلحاق الأذى بالحاسبات على الرغم من أن أنها لا تستطيع نسخ نفسها ، ومنها ما يلى[٢٩] :

١- أحصنة طروادة Trojan Harses :

هى برامج تتضمن تعليمات خفية تهدف للتخريب وإلحاق الأذى بالنظام على الرغم من أنه فى ظاهرة يبدو كأنما يؤدى أعمالاً عادية ، فهى توحى للمستخدم بأنها تقوم بعمل معين فى حين أنها فى واقع الأمر تؤدى عملاً آخر تخريبى فى الغالب ، فتقوم أحياناً بالتجسس ومتابعة كل ما يتم عمله من إجراءات أو تسجيله من بيانات على الجهاز المصاب بها ، وتقوم أحياناً أخرى بإحداث أنواع أخرى من الأذى على الأجهزة المصابة مثل تشفير البيانات أو مسحها أو ما سوى ذلك . ولا تتمكن أحصنة طروادة من نسخ نفسها والالتصاق بالبرامج الأخرى ولكنها تؤدى عملاً معيناً تم تصميمها من أجله .

٢- القنابل المنطقية Logic Bombs والقنابل الموقوتة : Time Bombs

هى من أنواع أحصنة طروادة ، وتعمل القنابل المنطقية عند حدوث شرط منطقى محدد مثل بلوغ الموظفين عدداً معيناً أو رفع اسم أحد الموظفين من كشف الرواتب ، أو كتابة كلمة معينة ، أو عند تشغيل برنامج معين لعدد محدد من المرات . أما القنابل الموقوتة فتعمل وفقاً لتوقيت معين مثل ساعة محددة أو يوم محدد .

٣- الديدان worms:

لا تحتاج الدودة إلى برنامج آخر تلتصق به للقيام بدورها كما هو الحال بالنسبة للفيروس الذى يلزمه حاضن hast لتنفيذ مهمته ، ولكنها تعمل بمفردها حيث لديها القدرة على إعادة توليد نفسها والانتقال من ملف إلى آخر ومن جهاز إلى آخر متصل بالشبكة لتحقيق الانتشار .

ولا تعمل الديدان على تخريب الملفات وإتلافها كما هو الحال بالنسبة للفيروسات ولكنها تسبب زيادة عبء على تحميل الشبكة حيث تقوم باستهلاك الذاكرة أو المعالج أو الأقراص أو سائر موارد الحاسب ، وقد تؤدى بالتالى إلى توقف النظام .

٤- باب الفخ او المصيدة Trapdoor:

يطلق عليها أيضاً الأبواب الخلفية backdoors، وتمثل كود يوضع عمداً عند البرمجة لتجاوز نظم الحماية فى البرنامج . وهو يسهل على المبرمج والتعديل فيه دون الحاجة إلى اتباع الخطوات التقليدية لذلك .

وعادةً يتم حذف أبواب الفخ بعد الانتهاء من جميع الاختبارات الخاصة بالبرنامج ، ولكن فى بعض الأحيان تترك تلك الأبواب سواء بقصد أو بدون قصد . وقد يكشف البعض تلك الأبواب ويستغلها لأغراض تخريبية للتجسس وانتهاك سرية البيانات أو لزرع الفيروسات .

٥- برامج الطوفان flooders :

تتمثل فى مجموعة كبيرة جداً (مئات أو

ألوف) من الرسائل التى تصل من جهات غير معروفة إلى الشبكة عن طريق البريد الإلكترونى أو عن طريق برامج TPQ ، وهى بدون شك تسبب إزعاجاً كبيراً حتى وإن كانت لا تسبب ضرراً .

٦- برامج الخداع spoofing :

تؤدى إلى تضليل مستقبل المعلومات حيث يبدو أنها مرسلة من جهة معينة فى حين أنها فى الواقع مرسلة من جهة أخرى ؛ الأمر الذى يسمح بدخول المعلومة إلى الشبكة ويجعل مستقبلها يتعامل معها دون معرفة هوية مرسلها الحقيقى .

استخدام البرامج المضادة للفيروسات :

هناك شركات عديدة تنتج برامج مضادة للفيروسات من بينها : Symantec, Command, Mcafee وغيرها ... وتعمل تلك البرامج الآتى :

١) فحص ذاكرة الحاسب عند بدء تشغيله بحثاً عن أى فيروسات .

٢) فحص أقراص التخزين بحثاً عن أى فيروسات ، وفى حالة وجودها يتيح إزالتها أو إلغاء الملفات المصابة بها .

٣) فحص الملفات المراد تحميلها على جهاز الحاسب سواء كانت تلك الملفات متاحة من خلال الشبكة أو على أقراص مرنة وذلك للتأكد من سلامتها من الفيروسات .

٤) فحص الملفات سواء المتاحة للمشاركة أم المنقولة عبر الإنترنت أم المرسلة عبر البريد الإلكترونى للتأكد من خلوها من الفيروسات والتنبيه بوجودها إن وجدت وتوفير الحماية ضدها .

٥) الفحص المستمر للنظام للتأكد من خلوه من الفيروسات ، والتنبيه عنها فى حالة وجودها[٣٠] .

سادساً : النسخ الاحتياطي Backup :

على الرغم من الاحتياطات الأمنية المتعددة التى قد تتبع لحماية البيانات إلا أنه من المحتمل وقوع أى نوع من التلف أو التحريف أو الفقدان للبيانات ، لذا كان لابد من تأمين طريقة يمكن من خلالها استعادة البيانات التالفة أو المفقودة أو المحرفة لضمان مستوى أعلى من الحماية للنظام . ويحقق النسخ الاحتياطى للبيانات هذا المستوى من الحماية ، حيث يتم من خلاله إنشاء نسخ احتياطية يتم حفظها سواء فى نفس مقر العمل أو خارجه ، ويتم تحديثها بصورة منتظمة لضمان أقل قدر من الخسائر فى حالة فقدان البيانات الأصلية .

ولابد من تحديد ما ينبغى نسخه احتياطياً ومتى ينبغى نسخه ، ويعتمد ذلك على درجة أهمية البيانات المختزنة على خادم الملفات .

★ البيانات اللازم نسخها :

لابد من تحديد ما ينبغى احتياطياً من المعلومات . ويشمل النسخ عادةً كل المعلومات الأساسية والحيوية الخاصة بالنظام والمختزنة على الخادم ، وقواعد البيانات ، والملف بالمستخدمين ، والبريد الإلكترونى .

★ **فترات النسخ :**

يتم النسخ على فترات يومية أو أسبوعية أو شهرية وذلك وفقاً لما يلائم العمل ؛ فعلى سبيل المثال إذا كانت الشبكة معتمدة كلياً على البيانات المختزنة على خادم الملفات ولا يمكن إنجاز العمل بدونها ، ففى هذه الحالة لابد من إجراء عملية النسخ يومياً ، وهذا يعنى نسخ جميع الملفات الموجوة على خادم الملفات ، أما فى حالة احتفاظ مستخدمى الشبكة بالبيانات الخاصة بهم على حاسباتهم الشخصية ففى هذه الحالة يمكن عمل نسخة احتياطية كاملة أسبوعية بدلاً من النسخ اليومى[٣١] .

وينبغى أن يجرى النسخ الاحتياطى دورياً على فترات منتظمة محددة مسبقاً وليس بشكل عشوائى ؛ فلابد من تحديد يوم معين فى كل أسبوع أو ساعة معينة فى اليوم وذلك حتى يسهل معرفة الفترة التى ينبغى الرجوع إليها لتصحيح أى خطأ فى حالة حدوثه .

وهناك حالات قليلة لا يتم فيها النسخ الدورى بصورة منتظمة وذلك فى حالات الملفات شبه الثابتة التى لا يحدث فيها تغيير بصورة مستقلة ، الأمر الذى تنتفى معه الحاجة للتحديث المتكرر ، ويكفى أن يتم النسخ على فترات متقاربة فى الفترات النشطة التى يحدث فيها تغيير على الملف ، فى حين تتباعد فترات النسخ فى الفترات الميتة التى يقل فيها التغيير[٣٢] .

ولابد من متابعة نظام النسخ بصورة دورية للتأكد من فعاليته وسلامته ويتم ذلك عن طريق إجراء عملية استرجاع للمعلومات من النسخ الاحتياطية ومقارنتها بالأصلية ، كما ينبغى حفظ سجل مفصل لعمليات النسخ يوفر معلومات مثل تاريخ النسخ ونوعه والشخص الذى قام بإجرائه ، وعلى أى وسيط تم النسخ[٣٣] .

وهناك أكثر من طريقة تتبع للنسخ الاحتياطى تتمثل فى الآتى :

★ **النسخ الاحتياطي الكامل Full Backup :**

يتم وفقاً له نسخ جميع الملفات المحملة على الخادم بغض النظر عما إذا كان قد أجرى تعديل عل تلك الملفات من عدمه .

★ **النسخ الاحتياطي التراكمى أو التزايدى :**

Incremental Backup

يتم وفقاً له إجراء نسخ احتياطى للملفات التى تم تعديلها بعد آخر نسخ احتياطى ، ويتم فى هذه الحالة تعديل سمات الملفات بحيث يظهر أنه أجرى لها نسخاً احتياطياً .

★ **النسخ الاحتياطي التباينى أو التفاضلى :**

Differential Backup

يتم وفقاً له إجراء نسخ احتياطى للملفات التى تم تعديلها بعد آخر نسخ احتياطى ، ولا تعدل سمات الملفات فى هذه الحالة[٣٤] .

ويجرى النسخ التباينى فى كل مرة على البيانات ابتداءً من آخر نسخ احتياطى كامل لها ، فى حين يجرى النسخ التراكمى على البيانات ابتداءً من آخر نسخ احتياطى لها .

وتدعم برامج تشغيل الشبكات عمليات إنشاء

النسخ الاحتياطية ، وإلى جانب ذلك فإن هناك برامج أخرى تؤدى ذلك الدور ومنها على سبيل المثال :

Norton Utilities, Fast Back Plus, Central Bachup

سابعاً: دعم أجهزة عدم انقطار التيار :

Uninterruptable Power Supply (UPS)

يمثل UPS مولد للطاقة يعمل كمصدر احتياطى فى لحظة انقطاع المصدر الاعتيادى للطاقة بحيث يتم بواسطته تشغيل خادم الشبكة ومكوناتها الأخرى لفترة وجيزة تكون كافية لاغلاق النظام بشكل طبيعى حتى لا يتم فقد البيانات أو تلفها أو تحريفها عند انقطاع التيار الكهربائى . وبذلك فإن عمل UPS يتمثل فى الاتى :

* الإبقاء على الأجهزة عاملة لفترة وجيزة من الوقت .
* تنفيذ عملية ليتم توقف الأجهزة عن العمل بصورة آمنة دون إحداث تلف أو فقدان للمعلومات[٣٥] .

ويتوافر نوعان من أجهزة UPS وهى على النحو التالى :

أ- مصدر الطاقة الدائمة المباشرة :

Online Power Supplies

يمثل هذا النوع أجهزة UPS الحقيقية ويتم وفقاً له تزويد الحاسب بالطاقة بشكل مستمر ، حيث يتوافر جهاز UPS بين مصدر الطاقة الاعتيادية وبين جهاز الحاسب ، ويعمل على تزويد الحاسب بالطاقة بصورة مستمرة بغض النظر عما إذا كان هناك انقطاع للطاقة الاعتيادية من عدمه ؛ وذلك على اعتبار أن مولد طاقة UPS يستقبل الطاقة الكهربائية من مصدرها الاعتيادى ويحفظها بداخله ويعمل على تزويد جهاز الحاسب بالطاقة من داخله وليس من مصدرها الرئيسى وبذلك فإن توصيل الطاقة إلى الحاسب لن ينقطع فى حالة انقطاع المصدر الاعتيادى للطاقة ؛ حيث يظل مولد الطاقة UPS يزود الحاسب بالطاقة الكامنة بداخله لفترة وجيزة جداً تسمح بإغلاقه بطريقة طبيعية .

ب- مصدر الطاقة الدائمة البديل :

Suitched Power Supplies

يطلق عليه أيضاً Standby Power Supplies ويعد هذا النوع أقل تكلفة من النوع الأول حيث يتم وفقاً له تفعيل عمل الطاقة الاحتياطية فى حالة انقطاع الطاقة الاعتيادية فقط . ويعمل مصدر الطاقة البديل المتصل بالحاسب على مراقبة تقلبات مستوى الطاقة ، وفى حالة توقف الطاقة الاعتيادى يقوم بالتحويل إلى مصدر الطاقة البديل ، ويقوم مولد الطاقة فى هذه الحالة بتوصيل الطاقة من مصدرها الاعتيادى مباشرة إلى الحاسب، وفى حالة انقطاع الطاقة الاعتيادية تكون هناك فترة توقف بسيطة جداً إلى حين بدأ تزويد الحاسب بالطاقة المحفوظة بداخل المولد الاحتياطى[٣٦] .

ثامناً: الحماية من خلال الاشخاص :

يقصد بها الأساليب المتبعة لتحقيق الحماية من خلال مستخدمى النظام سواء كانوا موظفين أم مستفيدين :

أ - الموظفون :

يعد الموظفون من العناصر الأساسية التى قد تؤدى إلى إلحاق الضرر بالمعلومات وتهديد أمنها سواء بشكل مقصود فى حالة رغبتهم الإساءة للهيئة التى يتبعونها لأى دافع من الدوافع (كراهية ، أو ملل ، أو طمع ، أو إثبات الذات) ، أم كانت بشكل غير مقصود بسبب ضعف مستوى إعدادهم فنياً للتعامل مع النظام ، لذا ينبغى اتباع ما يلى[٣٧] :

١) تحديد كلمات مرور للموظفين وفقاً لما تم إيضاحه سابقاً ، على أن يراعى تحديد صلاحيات كل موظف بما يتناسب مع طبيعة عمله ، فمن غير الملائم منح جميع الموظفين صلاحية الدخول إلى جميع مناطق العمل على النظام وإجراء التعديلات على البيانات والبرامج لأن ذلك قد يعرض النظام للخطر ، ومن ناحية أخرى فإن منح الصلاحيات بدون حدود أمر لا ضرورة له حيث أن هناك مناطق عمل لا تعنى جميع الموظفين ولا تخص عملهم .

٢) اختيار الموظفين بعناية تامة خصوصاً أولئك الذين يتعاملون مع بيانات حساسة والذين يمنحون صلاحيات عالية ، حيث ينبغى التأكد من أمانتهم وإخلاصهم وذلك بإجراء تحريات عنهم وملاحظة سلوكياتهم بعد عملهم .

٣) تدريب الموظفين بشكل جيد وذلك تجنباً للعديد من المشكلات التى قد تواجهها الشبكة ومواردها نتيجة لضعف المستوى الفنى للعاملين عليها ؛ ومنها على سبيل المثال حذف شىء من البيانات بطريقة الخطأ أو تحديث البرامج أو إزالتها بطريقة خاطئة مما يؤثر على النظام والعمل القائم ، فلابد من تدريب الموظفين على استخدام الأجهزة بكفاءة من ناحية ، وكذلك تدريبهم على سبيل التعامل مع المشكلات البسيطة التى قد تواجههم وكيفية التغلب عليها من ناحية أخرى .

٤) التأكد من إزالة بيانات الموظفين المنتهية مدة خدمتهم فى المؤسسة من قائمة مستخدمى النظام ، وقد يتطلب الأمر تغيير كلمة المرور الخاصة بمجموعة من الموظفين عند انتهاء خدمة أحدهم ، وذلك فى حالة معرفة الموظف بكلمات المرور الخاصة بالمجموعة .

ويرى البعض ضرورة اتباع إجراءات أخرى حرصاً على الأمن من جانب الموظفين كأن لا تمنح صلاحيات عالية للموظفين حديثى التعيين ، وكذلك ضرورة تضمين عقود عمل المتعاقدين لشرط يمنع إفشاء المعلومات الحساسة أو الإجراءات الأمنية للنظام .

ب- المستفيدون :

يسرى عليهم بعض ما يسرى على الموظفين حيث أنه لم يتم تدريب مستخدمى النظام بشكل كافى فإنه قد يلحق الضرر بالنظام وذلك بنقل الفيروسات أو إلحاق الضرر بالأجهزة .

وقد يتعمد بعض المستفيدين إلحاق الضرر بالنظام فى حالة تصورهم أن هناك إجراءات أمنية متشددة تتبع ضدهم بشكل يؤدى إلى إزعاجهم

بدون مبرر مقنع بالنسبة لهم ، مما يضطرهم إلى التحايل على النظام ومحاولة إلحاق الضرر به ، ومن هنا يرى البعض ضرورة توعية المستفيدين بالأسباب التى تدعو إلى استخدام كلمات المرور ، والخروج من النظام log aff بطريقة سليمة ، وتعريفهم بالأسباب التى تدعو إلى ضرورة عمل مسح للأقراص المرنة فى حالة جلبها معهم للتأكد من خلوها من الفيروسات[٣٨] .

شبكة المكتبات بجامعة أم القرى :

تم إنشاء شبكة المعلومات فى عمادة شئون المكتبات فى أواخر عام ١٤١٧هـ ، ويعد إنشاؤها جزء من تنفيذ المرحلة الثانية من مشروع توسعة الشبكة المحلية للجامعة والتى شملت إلى جانب عمادة شئون المكتبات كل من معهد خادم الحرمين الشريفين ، ومعهد البحوث العلمية وإحياء التراث الإسلامى ، ومركز الوسائل وتقنيات التعليم ، وعمادة الدراسات الجامعية .

وبدأت شبكة المكتبات فى المرحلة الأولى لإنشائها لتربط بين الحاسبات بداخل مقر المكتبة المركزية للطلاب بمنطقة العزيزية بمكة المكرمة ، ثم توسعت فى عام ١٤٢١هـ لتضم المكتبة المركزية للطالبات بمكة المكرمة ، وسيتم بإذن الله تعالى لاحقاً التوسع فى الشبكة لتربط كل من مقر الجامعة بمنطقة العابدية وكذلك المكتبة المركزية للطلاب فى فرع الجامعة بمدينة الطائف .

وتوفر الشبكة للمكتبات المشاركة فى الآتى :

* برنامج الأفق الذى يمثل النظام المتكامل الذى تعمل به المكتبات التابعة للعمادة .
* قواعد البيانات التى تشترك فيها العمادة على أقراص مدمجة .

هذا إلى جانب ما نتيجة شبكة الجامعة من الاتصال بشبكة الإنترنت حيث تم توصيل مركز المعلومات والحاسب الآلى فى الجامعة بشبكة الإنترنت عن طريق مدينة الملك عبد العزيز للعلوم والتقنية وعن طريق شركة الاتصالات السعودية .

وتخصص عمادة شئون المكتبات خادم رئيسى واحد للشبكة بداخلها حيث يتم تشغيل البرنامج الآلى المتكامل للمكتبات عليه وهو نظام الأفق Horizon ، وكذلك يتم تحميل الأقراص المدمجة التى تشترك فيها العمادة وتطبيقاتها بحيث تعمل على الخادم نفسه ، كما تخصص العمادة خادم احتياطى للشبكة كأحد أنظمة احتمال الخطأ fault tolerance التى توفرها لضمان استمرار عمل الشبكة فى حالة توقف الخادم الرئيسى . ويتواجد الخادم الاحتياطى فى مقر مركز المعلومات والحاسب الآلى ، أى خارج مقر عمادة شئون المكتبات .

وقد أجرت الباحثة دراسة حالة على شبكة جامعة أم القرى ، ووجدت أن الحفاظ على أمن المعلومات فى الشبكة يعد مسئولية موزعة ما بين عمادة شئون المكتبات وبين مركز المعلومات والحاسب الآلى والتطوير الجامعى ، وقد وضع مركزا المعلومات قواعد تنظيمية لضبط العمل على الحاسبات واستخدام الشبكات بشكل يراعى فيه العديد من الجوانب ومن بينها حماية أمن المعلومات على الشبكات وتم اعتماد تلك القواعد من قبل إدارة الجامعة حتى يتم العمل بموجبها فى مختلف الإدارات والأقسام والعمادات ومن بينها عمادة شئون

المكتبات (وسيشارك إلى تلك القواعد فى الدراسة لاحقاً بالقواعد الصادرة عن إدارة الجامعة) . وفيما يلى توضح الباحث الأساليب المتبعة لحماية أمن المعلومات فى شبكة مكتبات الجامعة :

اولاً : الحماية الفيزيائية (المادية) :

تتبع العمادة عدداً من العناصر التى تكفل بعض جوانب الحماية الفيزيائية للشبكات ومواردها ومن ذلك ما يلى :

١) تخصص مكاناً مستقلاً لحفظ أجهزة الخادم بداخل مبنى المكتبة المركزية للطلاب .

٢) استخدام كابلات الألياف الضوئية fiber optics للتمديدات الداخلية ، ويضمن هذا النوع من الكابلات درجة كبيرة من الحفاظ على أمن المعلومات أثناء نقلها عبرها .

٣) الحرص على تركيب الكابلات بشكل يضمن حمايتها ؛ فلا توضع فوقها قطع الأثاث أو ما شابه ذلك .

٤) توفر عوازل بلاستيكية لتغطية كابلات الشبكة بهدف تحقيق أكبر قدر من الحماية لها .

ويلاحظ أن هناك جوانب عديدة للحماية المادية لم تحرص عليها العمادة ومن ذلك توفير المراقبة للمكان سواء عن طريق أشخاص أم كاميرات مراقبة ، وكذلك استخدام أجهزة إنذار للتنبيه فى حالة دخول شخص غير مصرح له إلى موقع الخادم. وتعتقد الباحث أنه من غير الضرورى فى المكتبات توفير هذه الدرجة من الحماية وذلك على اعتبار أن مستوى الحماية المطلوب يختلف وفقاً لاختلاف درجة حساسية المعلومات وسريتها ومن غير المتوقع أن يتسلل أحد الأشخاص إلى موقع الخادم لسرقة قواعد بيانات المكتبة أو ليتعمد إلحاق تلفيات بها على سبيل المثال ، وإن كان تصرف كهذا وارد فى جهات أخرى مثل أجهزة المخابرات فى الدولة أو الجهات التى تحتفظ بمعلومات سرية عن منتجات معينة ، أو ما شابه ذلك .

وقد تضمنت القواعد التنظيمية الصادرة عن إدارة الجامعة بعض القواعد التى من شأنها أن تكفل بعض الجوانب الأخرى المتعلقة بحماية أمن الشبكة ومواردها من الناحية الفيزيائية ؛ فعلى سبيل المثال نصت تلك القواعد على الآتى :

١- منع تغيير إعدادات وتوصيلات الشبكات من قبل المستخدمين سواء كان ذلك فعلياً أم منطقياً .

٢- منع تركيب عتاد أو برامج دون التنسيق مع مدير النظام (مثل تركيب جهاز مود على الحاسب الشخصى أو وسيط إنترنت proxy) .

٣- منع التنصت أو مراقبة الاتصالات الإلكترونية الخاصة بمستخدمين آخرين .

ثانياً : ضبط الوصول للشبكة وموارها :

تحدد العمادة حسابات لمستخدمى الشبكة account تتضمن أسماء تعريف وكلمات مرور ، وتحدد ذلك حسب الموقع فى بعض الحالات وحسب المستخدمين فى حالات أخرى .

إتاحة الوصول حسب الموقع :

تتيح العمادة الوصول للفهرس العام للجمهور PAL باستخدام اسم تعريف وكلمة مرور للموقع

نفسه وتحدد صلاحيات المستخدم بحيث يتاح له البحث والقراءة من قاعدة البيانات فقط ولا يتاح له الدخول إلى قاعدة بيانات الفهرسة أو غيرها أو التعديل فى البيانات ، وتتيح العمادة الوصول حسب الموقع أيضاً لقواعد البيانات الإلكترونية التى تشترك فيها العمادة على أقراص مدمجة ، وكذلك قواعد البيانات الإلكترونية التى تشترك فيها من خلال شبكة الإنترنت حيث تتيح الوصول إليها باستخدام اسم تعريف وكلمة مرور لكل قاعدة من تلك القواعد على أساس الموقع .

وتجدر الإشارة إلى أن المكتبة لا تحدد استخدام قواعد البيانات الخاصة بها من عنوان معين IP address وهو العنوان الخاص بجامعة أم القرى ، ولكن يمكن الدخول إلى قواعد البيانات (حتى وقت إجراء هذه الدراسة) من أى عنوان عبر شبكة الإنترنت . ومن ناحية أخرى تخصص العمادة أيضاً أسماء تعريف وكلمات مرور حسب الموقع للعمل فى قسم الإعارة بالمكتبة . وقد أوضح سعادة مدير المكتبة أن تحديد الإتاحة بقسم الإعارة كان يتم فى السابق وفقاً للأشخاص وقد تم تغيير ذلك النظام لظروف وقتية معينة ؛ وبذلك فإن هذا الوضع يعتبر مؤقت حيث سيجرى قريباً تعديل النظام لتصبح الإتاحة حسب الأشخاص .

إتاحة الوصول حسب الأشخاص :

يتم ذلك فى قسم الإجراءات الفنية بمكتبة الطلاب وكذلك مكتبة الطالبات ؛ حيث يتاح الدخول إلى الموقع الخاص بالفهرس والإضافة إلى قواعد البيانات والحذف منها والتعديل فيها باستخدام اسم تعريف وكلمة مرور خاصة بكل موظف وموظفة من الموظفين والموظفات على حده .

وقد تبين للباحثة عدم اختلاف الصلاحيات الممنوحة لكل موظف أو موظف بقسم الإجراءات الفنية ؛ بل إن لرئيس القسم نفس الصلاحيات دون أى اختلاف عن موظفى القسم .

ولعل اعتماد العمادة على تحديد أسماء التعريف وكلمات المرور للمواقع نفسها يحقق السهولة فى الاستخدام للمستفيدين ، كما أنه يحقق أكبر فائدة من قواعد البيانات المستخدمة . وقد لا يكون لدى العمادة الدافع الذى يجعلها تخصص كلمات مرور للأشخاص فيها يتعلق بقواعد البيانات التى تشترك فيها سواء على أقراص مدمجة أم من خلال شبكة الإنترنت ؛ خصوصاً إذا لم يكن هناك تعارض بين هذا الإجراء وبين شروط تراخيص استخدام تلك القواعد التى تحفظ حقوق الملكية الفكرية للناشرين . فمن جانب العمادة ليس هناك معلومات سرية فى تلك القواعد ترغب فى حفظها بعيداً عن المستخدمين ، بل أنها تسعى إلى تحقيق أكبر قدر من الاستفادة من تلك القواعد سواء من داخل المكتبة أم من خارجها لمنسوبى المكتبة أم غيرهم لأن فى ذلك ما يحقق الجدوى من اشتراك العمادة فى تلك القواعد ، يضاف إلى ذلك أن الصلاحيات التى يمنحها موردو تلك القواعد للمستخدمين تقتصر على الاستخدام ولا تتيح التعديل أو التغيير فى البيانات المختزنة فى تلك القواعد .

أما فيما يتعلق بمواقع العمل المكتبى كالإعارة فإن استخدام كلمة مرور للموقع تعد طريقة غير

آمنة بالدرجة الكافية ؛ وذلك على اعتبار أن حرص الشخص على حفظ كلمة المرور الخاصة بالموقع لا ترقى فى درجتها إلى حرصه على حفظ كلمة المرور الخاصة به ؛ وبالتالى فإن الأمر يتطلب تخصيص كلمات مرور لكل مستخدم على حده ؛ بل إنه يتطلب تحديد صلاحيات كل موظف بما يتلاءم مع حجم عمله ؛ فهناك نشاطات فى قسم الإعارة وكذلك فى قسم الفهرسة ينبغى ألا] تترك حرية ممارستها لجميع الموظفين ؛ ومن ذلك على سبيل المثال النشاطات المتعلقة بضبط غرامات الإعارة وصلاحيات رفعها عن المستفدين وكذلك التعديل والتغيير فى قواعد بيانات الفهرسة التى تحفظها ، وينبغى لتحقيق مستوى أعلى من أمن المعلومات أن يتم تحديد ممارسة تلك الصلاحيات وما شابهها بحيث تكون متاحة لرئيس القسم فقط .

وينبغى الإشارة إلى لرئيس قسم الحاسب الآلى فى العمادة ونائبه الحق فى تعديل صلاحيات مستخدمى شبكة معلومات المكتبة المحفوظة فى ملفات المستخدمين الخاصة بنظام الأفق ، ويتم التعديل عادة وفقاً لمقتضيات العمل والحاجة لإجراء التعديل .

وعلى الرغم من ضبط العمادة لعمليات الوصول إلى الشبكة ومواردها باستخدام أسماء تعريف وكلمات مرور لمستخدميها إلا أنها لا تراعى اختيار كلمات صعبة الكشف من قبل الآخرين ؛ فلا تحرص على سبيل المثال أن تجعل كلمات المرور طويلة ، أو أن تخلط فيها بين الحروف والأرقام أو الرموز ، ولكنها على العكس من ذلك تحرص على اختيار كلمات مرور قصيرة وسهلة التذكر ، كما أنها لا تحرص على تغيير كلمات المرور على فترات منتظمة ، ولكن يتم تغيير كلمات المرور وفقاً لتغيير المهام المطلوبة للمستخدم .

ولا تقوم العمادة بمراقبة monitoring لمستخدمى الشبكة الخاصة بها ؛ وبالتالى فإنها لا تعمل على متابعة مرات دخول المستخدمين وخروجهم ، ولا تتابع كذلك ما يقومون بعمله على الشبكة وما يدخلون عليه من مواقع أو ما سوى ذلك .

وإذا كان ما سبق يوضح الضوابط والإجراءات التى تتبعها العمادة لضبط إتاحة الوصول إلى شبكة المعلومات الخاصة بها ، فإن هناك ضوابط محددة فى القواعد التنظيمية الصادرة عن إدارة الجامعة حيث تؤكد تلك القواعد على ضرورة الالتزام باستخدام الأجهزة والخدمات والشبكات المصرح بها فقط من قبل إدارة الجامعة ، وتشير إلى أن الحصول على تصريح لاستخدام جزء من الشبكة لا يعنى السماح باستخدام كلها . كما تنص على ضرورة المحافظة على كلمة المرور الخاصة بكل شخص وضمان عدم إطلاع الآخرين عليها واتباع التعليمات الخاصة بها .

وقد حددت تلك القواعد صلاحيات مستخدمى شبكة الجامعة والأوقات المصرح بالاستخدام فيها من أى موقع بالجامعة بما فى ذلك المكتبات وذلك بتقسيمهم إلى ثلاث فئات وفقاً لصلاحياتهم، وتأتى الفئات على النحو التالى :

١- الفئة الأولى : تشمل جميع أعضاء الهيئة الأكاديمية وطلاب الدراسات العليا وموظفى الجامعة من يتطلب عملهم استخدام شبكة

الإنترنت ، ويصرح لهم باستخدام البريد الإلكترونى ، والشبكة الداخلية للجامعة intranet ، والشبكة العنكبوتية العالمية world wide web طوال اليوم .

٢- الفئة الثانية: وتشمل جميع موظفى الجامعة ، ويصرح لهم باستخدام البريد الإلكترونى والشبكة الداخلية للجامعة intranet طوال اليوم ؛ فى حين تحدد ساعات استخدامهم للويب فى الفترات ما بين ٧ - ٩ صباحاً و ٢ - ٤ مساءً .

٣- الفئة الثالثة : وتشمل طلاب وطالبات الجامعة ، ويصرح لهم باستخدام الشبكة من خلال معامل الحاسب الآلى فى الجامعة ، وحسب الأوقات المحددة لذلك .

وترى الباحثة أن هذا التقسيم ملائم جداً ؛ حيث يتم من خلاله تلافى بعض السلبيات التى قد تحدث عند فتح المجال لاستخدام شبكة الإنترنت للجميع طوال فترة الدوام الرسمى ؛ الأمر الذى قد يؤثر على أداء الموظفين لأعمالهم ، ومن ناحية أخرى فإن هذا النظام يتعامل مع الموظفين الذين يتطلب عملهم استخدام الشبكة بشكل يحفظ لهم حقهم فى أداء عملهم ، وبذلك يتم توزيع الصلاحيات حسب حاجة العمل والقائمين عليه .

ثالثاً: برامج الحماية ضد الفيروسات :

تستخدم عمادة شئون المكتبات برنامج وقاية ضد الفيروسات على أجهزة الخادم الخاصة بها وكذلك على محطات العمل الموجودة فى كل من المكتبة المركزية للطلاب والمكتبة المركزية للطالبات . وتستخدم العمادة برنامج Norton Anti Virus (NAV) الذى تصدره شركة Symantec corporation ويتميز البرنامج بالآتى[٣٩] :

١- يقدم برنامج NAV حماية من الفيروسات المعروفة التى تم تحليلها من قبل باحثى الفيروسات ، وكذلك الفيروسات الجديدة وغير المعروفة .

٢- يوفر البرنامج نظام إنذار مركزى يعمل فى حالة اكتشاف فيروس على النظام .

٣- يوفر البرنامج تحديثاً مجانياً له عبر الإنترنت باستخدام تقنية Live updates المزود بها البرنامج .

٤- يوفر مركز أبحاث Symantec دعماً فنياً لمقتنى البرنامج .

٥- يعد البرنامج سهل الاستخدام والتحديث .

وفى دراسة أجريت حول البرامج المضادة للفيروسات ونشرت فى مجلة PL Magazine تم اختبار ست حزم برمجية مضادة للفيروسات تعمل فى بيئة ويندوز ، وقد توصلت الدراسة إلى أن NAV من أفضل تلك البرامج بل إنه تم اختياره كبديل أمثل من قبل المحررين حيث وجد أن أدائه مطابق لما تعلن عنه الشركة ، ففى العينة التى تم تطبيق الدراسة عليها تبين أن NAV قد تمكن من اكتشاف جميع الفيروسات الموجودة على لائحة الفيروسات الفعلية wild list المحددة من قبل جمعية NPSA كما أن أدائه كان حسن فى التغلب على الفيروسات الماكروية ، إضافة إلى اكتشافه نسبة كبيرة جداً ٩٩,٣٪ من الفيروسات

النظرية Zoo التى اكتشفت فى المختبرات ولم تسجل أى إصابة بها فى الواقع . ويعاب على البرنامج بطىء أدائه مقارنة بغيره من البرامج المضادة للفيروسات[٤٠] .

وعلى الرغم من المميزات العديدة لبرنامج NAV وإمكانياته العالية إلاّ أن العمادة لا تستفيد من معظم المميزات بل إنها لا تعمل على تحديث البرنامج على جهاز الخادم أو على محطات العمل ؛ الأمر الذى عرض بعض محطات العمل فى المكتبة المركزية للطلاب ، وكذلك بعض محطات العمل فى المكتبة المركزية للطالبات إلى الإصابة بالفيروسات أكثر من مرة ، وقد تمت معالجة الأمر دون أن يلحق الضرر بالشبكة ومواردها وذلك بإحالة الأجهزة المصابة إلى مركز المعلومات والحاسب الآلى والتطوير الجامعى لحل المشكلة وإجراء الصيانة اللازمة للأجهزة . ولا شك أن عدم تحديث برنامج الحماية ضد الفيروسات يجعل البرنامج لا قيمة له وذلك على اعتبار أنه لن يستطيع مقاومة عشرات الفيروسات التى تظهر يومياً فى العالم .

وتراعى إدارة الجامعة توجيه العديد من الإرشادات لمستخدمى الشبكات للتقليل من مخاطر التعرض للفيروسات ، وقد تم تحديد تلك الإرشادات فى شكل نصائح أمنية اشتملت عليها قواعد التعامل مع الأنظمة الحاسوبية والشبكات والصادرة عن إدارة الجامعة ؛ حيث تضمنت تلك النصائح الإرشادات التى تكفل الحماية من الفيروسات ومن بينها مايلى :

١- المحافظة على الجهاز من الفيروسات بتركيب برامج مكافحة الفيروسات وتحديثها بشكل دورى .

٢- الحذر من الملفات المرفقة مع الرسائل الإلكترونية والتأكد من خلوها من الفيروسات أو البرامج التى تمكن الآخرين من اختراق النظام .

٣- عدم تحميل برامج من مواقع غير معروفة أو غير موثوق بها من خلال شبكة الإنترنت .

رابعا: النسخ الاحتياطى :

تقوم العمادة بعمل نسخ احتياطية لقواعد بياناتها وذلك تحسباً لوقوع أى طارىء يحدث تلف لتلك البيانات .. ولا تحرص العمادة على عمل نسخ احتياطية من الملف الخاص بالمستخدمين والمتضمن كلمات المرور الخاصة بهم وحقوقهم ، كما لا تحرص على عمل نسخ احتياطية من مراسلاتها البريدية . وبذلك تكون عمادة شئون المكتبات قد خصصت عمليات النسخ الاحتياطى لقواعد البيانات الببليوجرافية التى تمثل مقتنيات المكتبة من مصادر المعلومات ، وكذلك سجلات الإعارة .

ويتم النسخ بصورة منتظمة بحيث يتم إجراء نسخاً احتياطياً تراكمياً incremental backup مرة كل أسبوع على القرص الصلب فى حين يتم إجراء نسخاً احتياطياً كاملاً full backup مرة كل شهر على أقراص مدمجة . وبذلك فإنه فى حالة تعرض البيانات للتلف أو الفقدان لا قدر الله فإن العمادة ستستعين بآخر نسخة احتياطية كاملة بالإضافة إلى جميع النسخ الاحتياطية التراكمية التى تمت منذ آخر نسخ احتياطى كامل ؛ وذلك

على اعتبار أن النسخ الاحتياطى التراكمى يجرى على البيانات منذ آخر نسخ احتياطى لها وليس كحال النسخ التباينى differential backup الذى يجرى فيه النسخ الاحتياطى على المعلومات منذ آخر نسخ احتياطى كامل لها ؛ وبالتالى ففى حالة فقدان البيانات يكتفى بالرجوع لآخر نسخة للنسخ الاحتياطى التباينى إلى جانب آخر نسخة احتياطية كاملة .

وتعد الفترة التى تخصصها العمادة للنسخ الاحتياطى متباعدة إلى حد ما ، وقد يكون من الملائم أن يتم إعداد النسخ التراكمى على فترات أكثر تقارباً ؛ وذلك على اعتبار أن إضافة المعلومات إلى قاعدة البيانات يتم بصورة يومية من كل من مكتبة الطلاب ومكتبة الطالبات حيث تجرى الفهرسة تعاونياً فى العمادة . ويتم يومياً إدخال بيانات فهرسة تصل فى المتوسط إلى (٧٩) تسجيلة فهرسة - وذلك وفقاً لما أشار إليه نائب رئيس قسم الحاسب الآلى فى العمادة من خلال البيانات الموضحة فى التقارير اليومية للأسبوع الثانى من شهر مايو لعام ٢٠٠١م - وبالتالى فإن الإبقاء على قاعدة البيانات دون إجراء نسخاً احتياطياً لها لمدة أسبوع يجعل بيانات حوالى (٣٩٥) تسجيلة فهرسة فى المتوسط معرضة للفقدان خلال تلك الفترة - والمتمثلة فى خمسة أيام بعد استبعاد يومى الإجازة الأسبوعية - هذا إلى جانب سجلات الإعارة المعرضة للفقدان خلال الفترة نفسها .

وقد تتحاشى العمادة السلبيات التى قد تقع بسبب تباعد الفترة وطولها ما بين كل نسخ احتياطى والتالى له عن طريق توجيه الموظفين إلى ضرورة عمل نسخ احتياطية للبيانات التى تخصهم بصفة يومية وذلك تمشياً مع ما نصت عليه قواعد التعامل مع الأنظمة الحاسوبية والشبكات الصادرةعن إدارة الجامعة والتى نصت على أن مستخدم النظام مسئول عن حفظ نسخة احتياطية من البيانات التى تخصه ، وضرورة متابعة ذلك بشكل دورى . وبتتبع الباحثة لمدى تطبيق ذلك فعلياً فى مكتبات الجامعة وجدت أن موظفات قسم الإجراءات الفنية بالمكتبة للطالبات لا يقومون بعمل نسخاً احتياطية للبيانات المدخلة يومياً من قبلهم وكذلك الحال بالنسبة للموظفين فى المكتبة المركزية للطلاب سواء العاملين منهم بقسم الإجراءات الفنية أم فى قسم الإعارة .

وتقوم العمادة بعمل نسخة احتياطية واحدة ، يتم حفظها على قرص مدمج CD وذلك لسعة هذا الوسيط التخزينية العالية التى تتناسب مع ضخامة حجم البيانات ، ويتم تسجيل تاريخ النسخ على القرص ، وتحفظ النسخة فى مركز المعلومات والحاسب الآلى والتطوير الجامعى حيث يتم إعدادها عن طريق نفس المركز وذلك من خلال جهاز الخادم الاحتياطى المتوافر لديهم ؛ وبذلك فإن العمادة تحرص على تأمين النسخة الاحتياطية خارج مقر العمادة بعيداً عن النسخة الأصلية ، ولاشك أن فى ذلك الإجراء تأمين للنسخة الاحتياطية من أن يلحقها التلف فى حالة تعرض الموقع نفسه لأى طارئ .

خامسا: الحماية من خلال الاشخاص:

لم يتم تدريب الموظفين بعمادة شئون المكتبات على مواجهة المشكلات التى قد تعترضهم أثناء استخدامهم للحاسبات ونظم الشبكات ؛ وذلك على اعتبار أن هناك متخصصين يقومون بمهمة صيانة الحاسبات فى الجامعة نفسها ؛ وبذلك فإن العمادة تعمل على إرسال الأجهزة إلى جهة الاختصاص فى الجامعة عند تعرضها لأى نوع من المشكلات ، أو يتم استدعاء أحد المتخصصين إلى المكتبة لحل المشكلة .

وتعتقد الباحثة أنه من الملائم تدريب الموظفين أو بعضهم على بعض الأساسيات التى تؤهلهم للتعامل مع المشكلات البسيطة لتلافى تعطل العمل فى حالة وجود مشكلات بسيطة لا تتطلب فنيين متخصصين فى صيانة الشبكات أو الحاسبات .

ومن إيجابيات الوضع الحالى أن العمادة تتجنب المخاطرة بقيام البعض بمحاولات للإصلاح قد تؤدى إلى إحداث مشكلات أكبر مثل تلف المعلومات أو موارد الشبكة وتجهيزاتها ، وذلك نظراً لعدم تدريب الموظفين على معالجة المشكلات ، وبذلك فإنها تحيل الأمر إلى جهة الاختصاص .

ولتجنب سواء استخدام المستفيدين من خدمات المكتبات للشبكة فإن استرجاع المعلومات من خلال شبكة الإنترنت أو الانترانت يتم فى المكتبة المركزية للطلاب عن طريق الموظف المختص بعد تعبئة المستفيد لنموذج مخصص لذلك .

أما فى المكتبة المركزية للطالبات فيتاح استخدام النظام للمستفيدات سواء عن طريق الموظفة المختصة أم عن طريق المستفيدة نفسها ؛ إلا أن المكتبة تتبع بعض الخطوات لحماية أمن الشبكة ومواردها ومن ذلك :

أ - مراقبة المكان من قبل الموظفة المختصة لملاحظة سواء استخدام الأجهزة وموارد الشبكة من قبل بعض المستفيدات .

ب- تقديم خدمات تدريب على استخدام النظام للمستفيدات وذلك لتجنب الاستخدام الخاطىء من قبل البعض .

جـ- منع استخدام المستفيدات للأقراص المرنة إلا بعد عرضها على الموظفة المختصة للتأكد من خلوها من الفيروسات .

د- توعية المستفيدات وإرشادهن حول استخدام الخدمات الإلكترونية ، وتحرص المكتبة على سبيل المثال على أن توضح للمستفيدات السبب الذى يدعو إلى ضرورة عرض الأقراص المرنة على الموظفة ، وتعلن المكتبة ضوابط استخدام الخدمات الإلكترونية فى لوحة إرشادية فى موقع تقديم الخدمة .

وتجدر الإشارة إلى أن العناصر السابقة قد وردت فى القواعد التنظيمية الخاصة بتقديم الخدمات الإلكترونية فى المكتبة المركزية للطالبات والتى وضعتها كاتبة هذه الدراسة فى تاريخ ١٤٢١/٧/٢٤ هـ ، وتمت الموافقة على تطبيقها من قبل سعادة عميد شئون المكتبات . وقد تضمنت تلك القواعد فى كل من الجوانب الخاصة بالاستخدامات المشروعة للنظام ، ومدة الاستخدام المتاحة لكل مستفيدة ، وضوابط خدمات التدريب والإرشاد المرتبطة بالخدمات

الإلكترونية ، وكذلك ضوابط خدمات الطباعة والنسخ على أقراص مرنة ، وقد تمت مراعاة بعض الجوانب التى تضمن حماية أمن الشبكة ومواردها من الناحية المتعلقة بالمستخدمين .

ولم تغفل القواعد التنظيمية الصادرة عن إدارة الجامعة الاهتمام بالجانب الخاص بالمستخدمين ، وقد تناولت العديد من الجوانب الهامة ومن بينها على سبيل المثال :

١- توجيه النصح للمستفيدين بما يكفل توعيتهم ببعض الجوانب الأساسية التى من شأنها الحد من المخاطر التى قد تهدد أمن المعلومات وسلامتها ؛ بما فى ذلك الفيروسات أو الاختراق ، وكذلك تضمن تقليص حجم الخسائر حدوثها من خلال توجيه المستخدمين إلى ضرورة الاهتمام بالنسخ الاحتياطى للبيانات . وقد سبقت الإشارة إلى أبرز تلك النصائح المتعلقة بالحماية ضد الفيروسات فى موقع آخر من هذه الدراسة .

٢- تحديد المسئوليات التى تقع على عاتق مستخدمى النظام والتى من شأنها حماية أمن المعلومات والشبكات ومن ذلك :

أ - ضرورة تقيد المستخدم بالتعليمات الصادرة بشأن حفظ الأمن الإلكترونى .

ب- ضرورة التزامه بأنظمة الاستخدام الخاصة بالشبكات .

جـ- مسئولية المستخدم عن استخدامه ، وعدم جواز إساءة الاستخدام حتى فى حالة وجود ثغرات أمنية فى النظام .

د - ضرورة إبلاغ مسئولى النظام والشبكات فى الجامعة عن أى إخلال بالأمن الإلكترونى .

هـ - مسئولية المستخدم عن حماية البيانات السرية والحساسة المسئول عنها .

٣- تحديد الاستخدامات الممنوعة التى من شأنها إلحاق الضرر بالشبكة وأمن المعلومات ومن ذلك :

أ- استخدام النظام للدخول على حسابات الآخرين سواء تم ذلك بمعرفة صاحب الحساب أم دون معرفته .

ب- تعمد استخدام الخدمة واستغلالها بطريقة تعرض الشبكة الداخلية للخطر أو تؤدى إلى فتح ثغرات أمنية فى الشبكة .

جـ- الاستخدام الذى يمكن أن يؤدى إلى تهديد أو تخريب أو إزعاج أو مضايقة لأى شخص أو جهة أو أمنها الإلكترونى : مثل إرسال بريد إلكترونى بشكل متكرر وغير مرغوب فيه ، أو لغرض الغش ، أو لخداع الآخرين .

د - محاولة فك تشفير بيانات الآخرين فى الأنظمة الحاسوبية .

هـ - العبث أو الاطلاع على معلومات خاصة بمستخدمين آخرين .

و - نشر الفيروسات .

ز - استخدام الأنظمة الحاسوبية للجامعة للدخول غير المشروع لأنظمة حاسبات أو شبكات أو مصادر معلومات دون الحصول على إذن .

ح – انتحال شخصية شخص أو جهاز آخر .

ط – إشراك الآخرين فى الحسابات الشخصية أو التنازل لهم عن الحسابات .

ويلاحظ أن إدارة الجامعة اهتمت بالجوانب المتعلقة بالمستخدمين إدراكاً منها لدورهم الكبير فى الحفاظ على أمن المعلومات ، كما يلاحظ أن الجامعة لم تكتف بوضع قواعد لكفالة أمن الشبكة الخاصة بها فقط ، وإنما وضعت قواعد أخرى تمنع أى تعدى على أمن الشبكة الأخرى ؛ الأمر الذى يحتسب لتلك القواعد من وجهة نظر الباحثة وذلك من جانبين :

أ – أن فى ذلك مراعاة لما تقتضيه أخلاقيات تبادل المعلومات والاستفادة من مصادرها .

ب– أن فى ذلك حماية لشبكة الجامعة نفسها حيث أن تعرض الآخرين للأذى من خلال شبكة الجامعة قد يؤدى فى المقابل إلى رد فعل من الآخرين قد تلحق الأذى بشبكة الجامعة ومواردها .

أساليب الحماية غير المستخدمة فى الشبكة:

على الرغم من استخدام العمادة لأساليب متعددة للحماية إلا أن هناك أساليب أمنية أخرى لم تستخدمها العمادة ومن ذلك ما يلى :

١) الحوائط النارية Firewalls :

لا تدعم العمادة شبكة المعلومات الخاصة بها بأى من أنواع الحوائط النارية ، وقد أوضح المسئول عن الشبكات فى مركز المعلومات والحاسب الآلى بأن شبكة الجامعة مزودة بحائط نارى يتمثل فى برنامج محمل على خادم شبكة الجامعة ، كما أوضح بأن الوصول إلى الشبكة الداخلية للمكتبة وقواعد بياناتها لا يمكن أن يتم إلا من خلال موقع الجامعة وبالتالى فإن ذلك الحائط من وجهة نظره كافٍ لتأمين الشبكة المحلية للعمادة . وترى الباحثة أن توفير حائط نارى للشبكة الداخلية للمكتبات من شأنه أن يوفر لقواعد بياناتها الحماية من أى اقتحام من خارج حدود العمادة – بما – فى ذلك الجهات الأخرى بالجامعة وهو ما لا يمكن تحقيقه من خلال الحائط النارى لشبكة الجامعة الى من شأنه أن يوفر الحماية من الجهات الخارجية .

٢- دعم أجهزة عدم انقطاع التيار الكهربائى UPS :

تعرضت شبكة العمادة لبعض المشكلات بسبب الانقطاع المفاجىء للتيار الكهربائى منذ شهور مضت ، وعلى الرغم من ذلك فإن العمادة لم توفر أجهزة UPS حتى تاريخ إعداد هذه الدراسة ؛ الأمر الذى يجعل موارد الشبكة عرضة للتلف أو الفقدان نتيجة لعدم إغلاق الملفات بصورة صحيحة عند التعرض للانقطاع المفاجئ فى التيار الكهربائى .

٣) التشفير Encryption :

تتبادل العمادة الرسائل مع جهات متعددة عبر الإنترنت باستخدام البريد الإلكترونى ولا تستخدم فى ذلك أساليب تشفير البيانات عند نقلها عبر الشبكة . وقد يرجع السبب فى ذلك إلى عدم نقل بيانات سرية عبرها .

النتائج والتوصيات :

توصلت الدراسة إلى النتائج التالية :

١- تهتم عمادة شئون المكتبات بجامعة أم القرى بتطبيق أساليب متعددة لحماية أمن المعلومات على الشبكة الخاص بها ، وتتمثل تلك الأساليب فى الآتى :

أ - تأمين الشبكة من الناحية المادية باتباع إجراءات عديدة خاصة بالمكان والتمديدات .

ب- ضبط إتاحة الوصول إلى شبكة المكتبات وذلك بتخصيص حسابات accounts للموقع أحياناً وللأشخاص فى أحيان أخرى .

جـ- عمل نسخة احتياطية واحدة كاملة على قرص مدمج مرة كل شهر ، إضافة إلى عمل نسخ احتياطى تراكمى على القرص الصلب مرة كل أسبوع .

د - استخدام برنامج Nartan Anti Virus للحماية من الفيروسات على كل من خادم الشبكة ومحطات العمل .

هـ . تحقيق الحماية من الاستخدام السيئ للمستفيدين من خدمات المكتبة من خلال بعض الإجراءات المتمثلة فى تقييد الاستخدام بحيث يكون عن طريق الموظف المختص بالمكتبة المركزية للطلاب ، وعن طريق بعض الإجراءات التنظيمية لاستخدام الشبكة ومواردها فى المكتبة المركزية للطالبات .

و - اعتماد إدارة الجامعة لبعض القواعد التنظيمية لاستخدام الشبكات فى الجامعة والتى قام بوضعها مركز المعلومات والحاسب الآلى والتطوير الجامعى ، وتضمن تلك القواعد تحقيق جانب كبير من الحماية الأمنية لشبكات الجامعة ككل والتى تعد شبكة المكتبات واحدة منها .

٢- تفتقد العمادة تطبيق بعض الأساليب الأمنية الضرورية مثل الحوائط النارية ، ودعم أجهزة عدم انقطاع التيار الكهربائى ، ونظام التشفير وذلك على الرغم من أهميتها .

٣- يوجد بعض الجوانب السلبية فى تطبيق بعض أساليب الحماية المتبعة من قبل العمادة ومن ذلك ما يلى :

أ - عدم تحديث برنامج الحماية ضد الفيروسات بشكل منتظم لخادم الشبكة وجميع محطات العمل مما أدى إلى تعرض بعض محطات العمل للإصابة بالفيروسات أكثر من مرة .

ب- تباعد الفترة الفاصلة بين كل نسخ احتياطى والنسخ التالى له مما يعرض بيانات (٣٩٥) تسجيلة فهرسة فى المتوسط للفقدان خلال تلك الفترة إلى جانب تسجيلات الإعارة المعرضة للفقدان فى الفترة نفسها .

جـ- عد تحديد صلاحيات المستخدمين من الموظفين وفقاً لما يتطلب عملهم الفعلى بالمكتبة .

د – ضبط إتاحة الوصول للشبكة وفقاً للموقع فى قسم الإعارة بدلاً من ضبط وفقاً للأشخاص .

هـ – عدم تدريب موظفى المكتبة على التعامل مع المشكلات التى قد تواجههم والمتعلقة أمن المعلومات .

و– عدم مراعاة القواعد المتبعة لحماية كلمات المرور والتى تضمن عدم كشفها من قبل الآخرين .

ز – عدم الإلتزام فعلياً بتطبيق بعض ما جاء فى القواعد التنظيمية الصادرة عن مركز المعلومات والحاسب الآلى والتطوير الجامعى والمعتمدة من إدارة الجامعة .

ولتطوير الأساليب المتبعة لحماية أمن شبكة المعلومات بالعمادة توصى الباحثة بالآتى :

١– اتباع بعض الإجراءات الأمنية اللازمة لإحكام أمن المعلومات خصوصاً فى ظل ارتباط الشبكة المحلية بشبكة الإنترنت ؛ ومن تلك الإجراءات تقنية الحوائط النارية والتشفير ودعم أجهزة عدم انقطاع التيار الكهربائى .

٢– تحديد صلاحية المستخدمين بحيث لا يتاح لكل موظف ممارسة أى نشاط على قاعدة البيانات حتى لو كانت تلك النشاطات مرتبطة بالقسم الذى يعمل فيه الموظف سواء كان قسم الإجراءات الفنية أم قسم الإعارة أم غيرهما .

٣– التوثيق للمشكلات التى تعترض الشبكة والأساليب التى تم اتباعها لحلها وذلك حتى يمكن التغلب على تلك المشكلات بشكل سريع فى حالة تكرار الوقوع فيها .

٤– الحرص على تحديث برنامج الحماية ضد الفيروسات بصورة منتظمة ومتقاربة لكل من خادم الشبكة ومحطات العمل .

٥– إلحاق بعض موظفى المكتبة بدورات تدريبية حول حماية أمن المعلومات على الشبكات .

٦– العمل فعلياً بما جاء فى القواعد التنظيمية الصادرة عن مركز المعلومات والحاسب الآلى والتطوير الجامعى والمعتمدة من إدارة الجامعة .

قائمة المراجع

1- Rawley I. Is your computer system secure? .- managing Information .- 2 (7/8) Iul / Aug 1995 .- p. 38 - 39 .

2- Cervan F. Security and the new ILLINEF online system .- Illinois - Libraries .- 79 (3) summer 1997 . - p. 117 - 122 .

٣– أشرف الغنيمى . نظم الحماية من قراصنة الكمبيوتر – القاهرة : دار الفاروق للنشر والتوزيع ، ١٩٩٨م – ١٦٤ ص .

4- Hawkins S . & Yen D. L & Thau D. L. Awareess and challenge of Internet security .- Information Management and Computer Security .- 8 (2/3) 2000 .- p. 131 - 143.

٥- حسن طاهر داود. الحاسب وأمن المعلومات . - الرياض : معهد الإدارة العامة ، ١٤٢١ هـ / ٢٠٠٠م . - ٤٣١ ص .

٦- دليل مصطلحات الحاسب : دليل المستخدم / ترجمة عماد مصطفى . - حلب : شعاع للنشر والعلوم ، ١٩٩٤ ، ص ٢٤٤ .

7- Christa Anderson & Mark Minasi. Mastering Local Area Netwarks .- San Francisco: SYKEH Network Press, 1999 .- p. 560 .

٨ - حسن طاهر داود . مرجع سابق . - ص ٣٠٥ - ٣٠٩ .

9- Christa Anderson & Mark Minasi. op. cit., p 574.

١٠- مارك سبورتاك ، والتر غلين . علم نفسك MCSE أساسيات شبكات الاتصال . - بيروت : الدار العربية للعلوم ، ١٩٩٨م .- ص ٢٤٢ - ٢٤٤ ، وحسن طاهر داود . مرجع سابق .- ص ٣٨ ، ٤٥ - ٤٦ ، ٣٣٢ .

١١- سيد مصطفى أبو سعود . كيف تصبح مديراً لشبكة الكمبيوتر . - القاهرة : دار الكتب العلمية ، ٢٠٠٠م . - ص ٣٦٧ - ٣٧١ .

12- Lyn Robinson. Installing a Local Area Network .- London : Aslib, 1995 . - p 36 .

ومارك سبورتاك ، والتر غلين . مرجع سابق . - ص ٢٤٤ - ٢٤٥ .

Christa Anderson & Mark Minasi. op. cit., p 562 - 563 .

14. Ibid .- p 565 , 6565 - 666 .

١٥- مارك سبورتاك ، والتر غلين . مرجع سابق . ٢٤٥ - ٢٤٦ .

16. Christa Anderson & Mark Minasi. op. cit., p 578.

17. Patrik Grate. Netwok + Cheat Sheet . - Indianapolis : Que carparation, 2000 .- p 175 .

١٨- تركي بن أحمد العصيمي . إحم جهازك المخاطر الأمنية وطرق الحماية منها . - الرياض : دار المعارج ، ١٤٢ هـ . - ص ١٨٨ - ١٨٩ .

19- Christa Anderson & Mark Minasi op. cit., 571 - 574.

٢٠- حسن طاهر داود . مرجع سابق . - ص ١٧٩ - ١٩٠ ، ٢٠٢ - ٢٠٣ .

21- Glossary of messaging and network security Terms .- http :// www. ssimail. com / Glossary . htm. [1/3/01] .

٢٢- تركي بن أحمد العصيمي . مرجع سابق . - ص ٢٣٦ .

٢٣- حسن طاهر داود . مرجع سابق . - ص ٣٦٨ .

24- Patrik Gvate. op. cit.- p 176 .

٢٥- أشرف الغنيمي . مرجع سابق . - ص ١٥٠ .

٢٦- تركى بن أحمد العصيمى . مرجع سابق . - ص ٢٠٢ - ٢٠٦ .

٢٧- دودج لوى . الشبكات للمبتدئين . - الرياض : مكتبة جرير ، ١٩٩٨م . - ص ٢٤٠ .

٢٨- أشرف الغنيمى . مرجع سابق . - ص ٢٩ - ٣٢ و Glossary of messaging and network security Ferms.- op . cit .

٢٩- دليل مصطلحات الحاسب : دليل المستخدم . مرجع سابق . - ص ٤٤٦ ، وتركى بن أحمد العصيمى . مرجع سابق . - ص ٨٣ ، ٢١٦ - ٢١٧، والحاسب وأمن المعلومات .- ص ٧٧ و تركى بن أحمد العصيمى . مرجع سابق . - ص ٢١٥ - ٢١٦ ، وأشرف الغنيمى . مرجع سابق . - ص ٥٣ .

٣٠- ماترك سبورتاك ، والتر غلين . مرجع سابق . - ص ٢٤٩ .

31. Patrik Grate. op . cit.- p 202 .

٣٢- حسن طاهر داود . مرجع سابق . - ص ٢٤٢ - ٢٤٤ .

٣٣- مارك سورتاك ، والتر غلين . مرجع سابق . - ص ٣٢٠ - ٣٢٢ ، ٢٥٠ - ٢٥١ .

٣٤- دودج لوى . مرجع سابق . - ص ٢٣٠ - ٢٣١ ، وسيد مصطفى أبو السعود . - مرجع سابق . - ص ٣٧٥ ، ومارك سبورتاك ، والتر غلين . مرجع سابق . - ص ٢٥١ .

٣٥- جايمس سيميك . Microsoft MLSE الاستعداد الأقصى للامتحان ٠٥٨ - ١٠ أساسيات شبكات الاتصال . - بيروت : الدار العربية للعلوم ، ١٩٩٩م . - ص ٢٤٣ ، ومارك سورتاك ، والتر غلين . مرجع سابق . - ص ٢٥٠ .

٣٦- مارك سبورتاك ، والتر غلين . مرجع سابق . - ص ٢٥٠ .

٣٧ - أشرف الغنيمى . مرجع سابق . - ص ١٣١ - ١٣٦، ١٣٩ - ١٤٠، وحسن طاهر داود . مرجع سابق . - ص ٥٠ - ٥١ .

38. Christa Anderson & Mark Minasi op. cit.- p 559 .

٣٩- البرامج الخدمية المضادة للفيروسات . - PL Magazine . -٠ الطبعة العربية . - ص ٣ ، ع ٧ (يوليو / أغسطس ١٩٩٧) . - ص ٥٦ - ٦٢ .

٤٠- حلول جديدة للفيروسات . - PC Maga-zine . - الطبعة العربية . - س ٤ ، ع ٢ (فبراير ١٩٩٨) . - ص ٢١ وبرنامج كشف إزالة الفيروسات نورتن أنتى فيروس ديلوكس 4.0 . - PC Magazine - . - الطبعة العربية . - س٤ ، ع ٣ (مارس ١٩٩٨) . - ص ٤٦ .

ملحق (١)

١- هل تخصص غرفة مستقلة لحفظ أجهزة الخادم .

( ) نعم ( ) لا

- فى حالة الإجابة بلا .. فأين يتم وضعها :

( ) مع مكاتب الموظفين .

( ) فى مكان استخدام المستفيدين .

( ) فى موقع آخر .. الرجاء تحديده ...

٢- هل تستخدم تقنية الحوائط النارية firewalls لحماية الشبكة :

( ) نعم ( ) لا

- فى حالة الإجابة بلا .. فالرجاء الانتقال إلى سؤال رقم ٥ .

٣- هل تستخدم تقنية الحوائط النارية لديكم :

( ) برنامج فقط .

( ) برنامج مع أجهزة .

٤- ما التقنية المستخدمة لديكم :

( ) Mc Aff Firewalls

( ) Guardian NT firewall

( ) أخرى .. الرجاء تحديدها ...

٥- هل تستخدم برنامج حماية ضد الفيروسات :

( ) نعم ( ) لا

- فى حالة الإجابة بنعم .. فما البرنامج المستخدم لديكم :

( ) Mc Affee

( ) Norton Anti Virus

( ) أخرى .. الرجاء تحديده ...

٦- هل تعمل المكتبة نسخاً احتياطية للملفات :

( ) نعم ( ) لا

- فى حالة الإجابة بلا .. فالرجاء الانتقال إلى سؤال رقم ١٣ .

٧- هل يتم النسخ الاحتياطى على فترات منتظمة :

( ) نعم ( ) لا

- فى حالة الإجابة بنعم .. الرجاء تحديد الفترة ... .

٨- ما نوع النسخ الذى تقوم به المكتبة :

( ) نسخ كامل لكافة الملفات والبرامج full backup

( ) نسخ تراكمى incermental backup

( ) نسخ تفاضلى differential backup

( ) طريقة أخرى .. الرجاء تحديدها .

٩- ما البيانات التى يتم نسخها احتياطياً

( ) الملف الخاص بالمستخدمين وحقوقهم وكلمات المرور الخاصة بهم .

( ) البريد الإلكترونى .

( ) قواعد البيانات .

( ) أخرى .. الرجاء تحديدها ..

١٠- على أى وسيط يتم النسخ الاحتياطى :

( ) أقراص مرنة

( ) أقراص صلبة .

( ) وسيط آخر .. الرجاء تحديده ...

١١- كم عدد النسخ الاحتياطية التى تحتفظ بها المكتبة :

( ) نسخة واحدة .

( ) نسختان .

( ) عدد آخر .. الرجاء تحديده .

١٢- أين يتم حفظ النسخ الاحتياطية :

( ) داخل المكتبة .

( ) خارج المكتبة . الرجاء التحديد ...

( ) بعضها داخل المكتبة والبعض خارجها .

١٣- هل تحدد المكتبة كلمات عبور password لمستخدمى الشبكة :

( ) نعم ( ) لا

- فى حالة الإجابة بلا .. فالرجاء الانتقال إلى سؤال رقم ١٧ .

١٤- على أى أساس تحدد كلمات العبور :

( ) على أساس المستخدم .

( ) على أساس الموقع .

١٥- هل يتم تغيير كلمات المرور كل فترة :

( ) نعم ( ) لا

- فى حالة الإجابة بنعم .. الرجاء تحديد مدة استخدام كلمة المرور ...

١٦- ما الذى يميز كلمات المرور التى يتم اختيارها عادة :

( ) طويلة ولا تقل عن ٨ محارف .

( ) قصيرة وسهلة التذكر .

( ) تتكون من حروف فقط .

( ) تتكون من حروف وأرقام ورموز .

( ) مرتبطة بعبارات مستخدمة فى المكتبة .

( ) غير ذلك .. الرجاء التحديد ...

١٧- ما المشكلات الأمنية التى تعرضت لها الشبكة من قبل :

( ) اقتحام بعض المستخدمين غير المصرح لهم بالاستخدام .

( ) تعرض البيانات للتلف أو الفقدان نتيجة لعوامل طبيعية

( ) تعرض البيانات للتلف أو الفقدان نتيجة سوء استخدام الموظفين .

( ) تعرض البيانات للتلف أو الفقدان نتيجة لتعرض الشبكة للفيروسات .

( ) مشكلات أخرى .. الرجاء تحديدها ..

١٨- كيف تمت معالجة تلك المشكلات :

( ) تمت إحالة الجهاز إلى جهة الاختصاص بالجامعة لحل المشكلة .

( ) تم استدعاء الشخص المختص من خارج العمادة لحل المشكلة .

( ) تم استدعاء الشخص المختص من داخل العمادة لحل المشكلة .

( ) طريقة أخرى .. الرجاء تحديدها ...

١٩- هـل تم تدريـب موظفى المكتبة علـى كيفيـة التعامل مـع المشكلات التـى تواجههم :

( ) نعم ( ) لا

- فى حالة الإجابة بلا .. فهل يرجع السبب إلى .

( ) وجود متخصصين فى صيانة الشبكات فى المكتبة .

( ) وجود متخصصين فى صيانة الشبكات فى الجامعة .

( ) أسباب أخرى .. الرجاء تحديدها ..

٢٠- هل توثق المكتبة المشكلات التى تعترض الشبكة وطرق حلها :

( ) نعم ( ) لا

٢١- الرجاء ذكر أى معلومات أخرى مرتبطة بأمن شبكة المكتبة فـى المساحة المتبقية من الصفحة ....