العنوان:	سياسات أمن المعلومات : البناء والتطوير
المصدر:	الأمن والحياة
الناشر:	جامعة نايف العربية للعلوم الأمنية
المؤلف الرئيسي:	العنزي، سليمان بن مهجع
المجلد/العدد:	مج 22, ع 255
محكمة:	لا
التاريخ الميلادي:	2003
الشهر:	شعبان / أكتوبر
الصفحات:	46 - 51
رقم MD:	322784
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	HumanIndex
مواضيع:	الإنترنت، أمن المعلومات، السياسة الأمنية، نظم المعلومات، تقنية المعلومات، المؤسسات التجارية، جرائم المعلومات، علم المعلومات
رابط:	http://search.mandumah.com/Record/322784

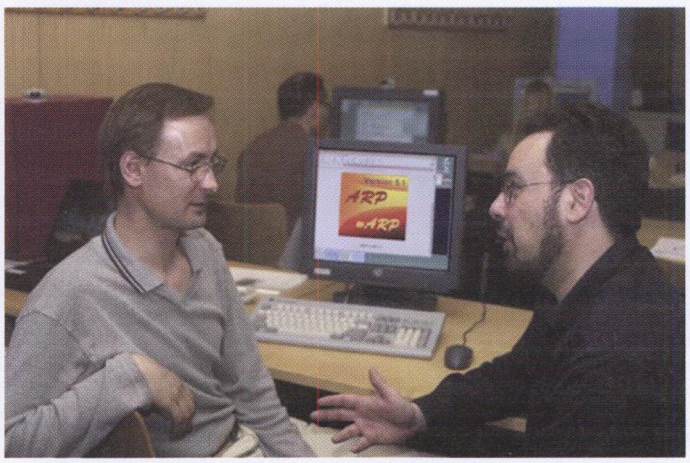
سياسات أمن المعلومات: البناء والتطوير

سليمان بن مهجع العنزي*

يتم استهداف المعلومات ونظمها للاستحواذ عليها أو تقليلها أو وتخريبها أو تعطيل أجهزتها لأهداف تجارية بين المؤسسات أو استراتيجية أو عسكرية بين الدول. ونتج عن ازدهار صناعة تقنية المعلومات وانتشارها في السنوات القليلة الماضية، تسهيلاً لمهام التجسس المعلوماتي بين الدول، التي تعتمد على عناصر يعملون داخل الجهة الأخرى للحصول على معلومات حساسة، بقيامهم بسرقة معلومات سرية وإرسالها إلى الجهة المستفيدة بوسائط الإنترنت. أو قد يتم الحصول على المعلومات بالتجسس من بعد بأدوات خاصة، ويمكن للشخص قليل الخبرة الحصول على عدة أدوات تجسسية من مواقع كثيرة على شبكة الإنترنت، ويمكنه استخدامها للدخول على الأجهزة المرتبطة بالشبكة وإحداث أشكال مختلفة من التخريب، والسرقة، والتعطيل. ولذا أصبحت الحاجة ماسة لتنمية معارف ومهارات المتعاملين بالمعلومات، ووضع لوائح وقوانين تتبع لتطبيق الإجراءات الفنية لأمن برامجها، وأمن الاتصالات في شبكاتها، والإجراءات الإدارية لأمن استخدامها وذلك بصياغة سياسة أمنية واضحة لجميع منسوبيها.

وقدرت خسائر المؤسسات التجارية حول العالم نتيجة للهجمات المدروسة التي تصيب نظم المعلومات بمبلغ مائة مليار دولار، وهذا الرقم في ازدياد مستمر، وفي إحدى الدراسات التي نشرها معهد أمن الحاسب الآلي بالتعاون مع مكتب التحقيقات الفيدرالية، وشارك فيها أكثر من خمسمائة من مسؤولي أمن المعلومات أفادت الدراسة أن مؤسسات الأعمال الأميركية تتكبد خسائر مالية متزايدة نتيجة لمخالفات وجنايات أمن المعلومات، وأفادت أن نسبة (٩٠٪) من المجيبين (وغالبيتهم من المؤسسات الكبرى والهيئات الحكومية) اكتشفوا مخالفات أمنية لحسابتهم الآلية، وأن نسبة (٨٠ ٪) اعترفوا بخسائر مالية، كما أن نسبة (٤٤ ٪) أفادوا عن خسائر بقيمة (٠٠٠، ٤٥٥,٨٤٨) دولار مقارنة بـ: (٣٧٨) مليون دولار تقريباً بلغ عنها (١٦٨) فرداً عام ٢٠٠١م ومقارنة بـ: (٢٦٥) مليون دولار بلغ عنها (٢٥٠) شخصاً استطلعت آراؤهم في عام ٢٠٠٠م، كما أن متوسط الخسارة السنوية على مدى ثلاث سنوات قبل عام ٢٠٠٠م كان في حدود (١٣٠) مليون دولار. كما أفادت الدراسة أن. (٩١٪) اكتشفوا إساءة استخدام موظفين لديهم لشبكة الإنترنت مثل الإتصال بمواقع إباحية ولبرمجيات قرصنة وطباعة محتوياتها أو استخدام غير لائق لنظم البريد الإلتكتروني، وأن (١٣٪) أبلغوا عن سرقة معلومات أو بيانات تتعلق بمعاملات تجارية، وأن (٤٠٪) اكتشفوا أن النظام المعلوماتي لديهم قد تم إختراقه من الخارج، وأن (٩٨٪) منهم يملكون موقعاً على الشبكة العنكبوتية، كما أفادت الدراسة أن هناك زيادة في جرائم نظم المعلومات في عام ٢٠٠١م أكثر من عام ٢٠٠٠م، حيث أن (٩٤٪) اكتشفوا فيروسات حاسب آلي مقارنة بـ: (٨٥٪) في عام ٢٠٠٠م، ونسبة (٩٠٪) منهم ابلغوا عن عمليات تخريب مقابل (٦٤٪) في ٢٠٠٠م، ونسبة (٨٪) ابلغوا عن حالات إحتيال أو تزوير مالي مقابل (٣٪) في عام ٢٠٠٠م.

أما في دراسة منظمة طوارئ الحاسب الآلي (CERT،٢٠٠١) والتي كانت عن «نمو المخالفات والإنترنت» فقد أظهرت أنه كلما زادت الحاجة لاستخدام نظم المعلومات زادت معدلات عدد المستخدمين للإنترنت، وبالتالي يكون هناك ازدياد طردي مرافق في معدلات ارتكاب الجرائم عن طريقها. فمنذ إنشاء تلك المنظمة عام ١٩٨٨م لاحظت أن الجرائم تزداد بازدياد عدد المشتركين في الإنترنت فكانت



أقل من مائة حادثة عام ١٩٨٨م وأكثر من (٢٤٠٠) جريمة عام ١٩٩٥م. ويتضح من هذا أن مهددات أمن المعلومات تتزايد سنة عن ا لأخرى. وقد يحمل المستقبل أنواعاً جديدة غير متوقعة من مخالفات أمن المعلومات، وقد تكون الحرب القادمة معلوماتية يحاول كل طرف إلحاق الضرر بالآخر عن طريق تدمير البنية المعلوماتية للخصم وإفساد قواعد البيانات ونظم المعلومات لما فيها من قيمة إستراتيجية عظيمة.

ونحن بصدد الحديث عن سياسات أن المعلومات ينبغي الإشارة إلى أن السياسة الأمنية تعني مجموعة من اللوائح والقوانين والإجراءات التي تنطلق من معايير وإستراتيجيات تتخذ لمواجهة المخاطر والتهديدات الإجرمية المحتملة، وتحدد سبل مواجهتها وفي مجال أمن المعلومات تعرف منظمة طوارئ الحاسب الآلي. السياسة الأمنية بأنها «توثيق خطة عالية المستوى في مؤسسة تعتمد الحاسب الآلي في نشاطها، لتوفر هيكلاً لاتخاذ قرارات محددة، لحماية تلك الأجهزة التقنية أثناء استخدامها، ودليل تطوير أمن البرامج، وإجراءات المستفيدين، ومدراء النظام، لتكفل أمن المعلومات في تلك المؤسسة». وتعتبر السياسة الأمنية مجموعة من القوانين والقواعد والممارسات التي تضبط كيفية أداء المؤسسة لأعمالها، وتقديم خدماتهم لتحقيق أهدافها بصورة آمنة، وأحد الأغراض الرئيسية للسياسة الأمنية الوقوف على حجم التهديدات التي تواجه المؤسسة لمحاولة تجنبها أو معالجتها بعد وقوعها، ومعاقبة المخالفين والمتجاوزين للحدود المقررة.

ومن خصائص السياسة الأمنية أنها توفر للمؤسسات هيكلاً لاتخاذ قرارات محددة، في كيفية شكل الخدمات المقدمة، وإجراءات المستفيدين ومديري النظام لتحقيق أمن المعلومات في تلك المؤسسة. وتخاطب السياسة الأمنية كافة المستويات كل بما يخصه (الإدارة العليا، والمشرفين والمختصصين والمستخدمين. كما تكون السياسة الأمنية مرجعاً قوياً في حالة حدوث الكوارث التي تهدد النظام المعلوماتي والتي بإتباعها تقلل من تكلفة الأضرار الناتجة عن حدوث تلك المهددات بعد وقوعها وتحديد الإجراءات لتلافي تكرارها وتحدد السياسة الأمنية ما هو المسموح به والغير مسموح به من الأعمال والتي بناءً عليه يتم معاقبة المخالف وتعتبر المرشد لمديري النظام المعلوماتي في كيفية إدارة ذلك النظام، وتحدد الاستخدام المقبول للمستخدمين كما تحدد طبيعة الأعمال بالمؤسسة من واجبات وإجراءات. كما ترشد في ردود الأفعال تجاه التعامل مع الأعلام بعد وقوع الجرائم. وتمد القانون بالقوة بتوضيحها وتسهيلها الكشف عن الجرائم وتحديد شخصية مرتكبيها لتقديمهم للعدالة، وبما توفره من وسائل تتبع للمخترقين، أو الذين يقومون في تعطيل وعمل تغيرات على النظام المعلوماتي.

كما تحدد السياسة الأمنية مدى إنفتاح المعلومات لوسائل النشر وللأشخاص الذين لا ينتمون للمؤسسة أو من أقسام أخرى داخل المؤسسة. وتحدد طرق تنظيم البيانات والمعلومات، كتحديد نوع

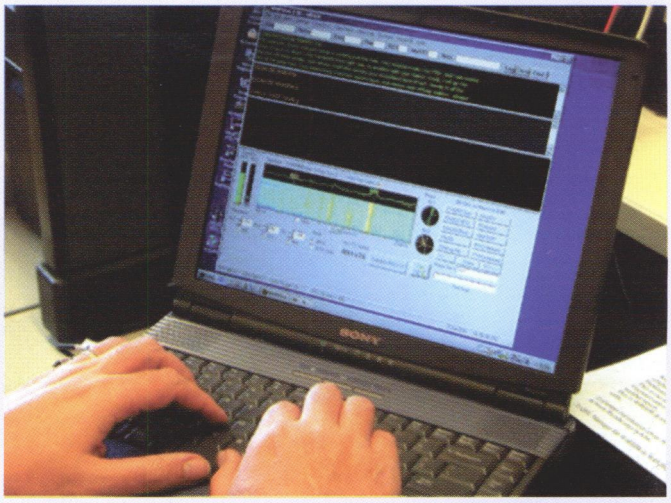
السجلات المستخدمة، ونوعية المعلومات التي تحتويها وهناك متطلبات لبناء وتطوير السياسة الأمنية من بينها:

١ ـ إيجاد لوائح جوهرية لأمن المعلومات تكون متطابقة مع المواصفات الأمنية القياسية لمساعدة تلك المؤسسات في حماية معلوماتها على أن يتم تصميمها لتناسب الإحتياجات المختلفة للمؤسسة إستناداً على القياسات العالمية للأيزو التي توفر إرشادات عامة لإدارة أمن المعلومات، وبعد تنقيحها وتضمينها للإجراءات الموجودة في المؤسسة، فإنها تصبح بمثابة التعليمات المستديمة للتعامل مع المعلومات الحساسة بشكل آمن.

٢ ـ الأخذ بالحسبان تحديات أمن المعلومات والتي تنحصر في أربعة محاور هي، خصوصية المعلومات وسلامة المعلومات وتوفر المعلومات، والتحقق من هوية ا لأطراف الأخرى.

٣ ـ تحديد مستوى الأخطار الواجب التغلب عليها وتحليلها ومن ثم تحديد الإجراءات التطبيقية الضرورية الواجب تغييرها لصياغة السياسة الأمنية بحيث تتسم بالوضوح والسهولة مما يمكن من فهمها لجميع العاملين وخصوصاً غير المختصين وعند تطبيقها يجب العمل على تقييمها بعد التنفيذ لمعرفة ما مدى القصور فيها لتلافيه.

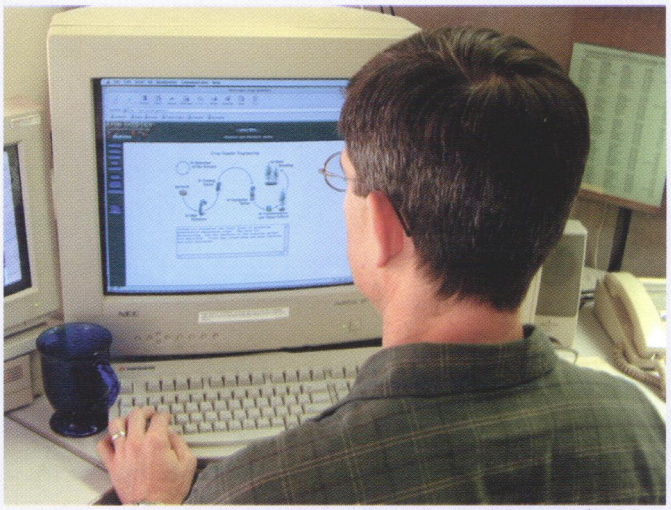
٤ ـ تحديد الغرض المراد كالأجهزة والبرامج والبيانات. وتعتمد السياسة الأمنية على نوع التقنية المستخدمة، فالمؤسسات التي لا تستخدم الحاسب الآلي فإن سياستها الأمنية في مجال أمن المعلومات تتركز حول عدم خروج الأوراق من المؤسسة مثلاً، والمؤسسة التي لا تستخدم الإنترنت لا تسمح بخروج وسائط الحفظ، وإغلاق غرف الحاسب الآلي، وأما المؤسسات التي تستخدم الإنترنت فإن الفائدة من منع الخروج بوسائط الحفظ غير عملي إذا لجاء المستخدمون إلى استعمال وسائل نقل البيانات إلكترونياً كوسيلة البريد الإلكتروني. ولهذا فإن السياسة الأمنية تبنى على معرفة مكونات النظام المعلوماتي. وتستخدم كل مؤسسة احتياجها من التقنية مع مراعاة أمنها. ولا يغيب عن صانعي تلك السياسات الأمنية بأنه لا توجد حماية كاملة، فارتباط الحاسب الآلي بالطاقة الكهربائية أكثر خطورة



من كونه مفصولاً، وارتباط الحاسب الآلي بالشبكة الداخلية أكثر خطورة من كونه غير مرتبط، وارتباطه بالأنترنت أكثر خطورة مما سبق.

٥ ـ تحديد مجال السياسة الأمنية وذلك بتحديد الأفراد المعنيين بتطبيقها، وعلى من يطبقونها، وما نوع الأجهزة المستخدمة التي تشملها (حاسبات صغيرة، متوسطة، كبيرة) ووسائط الإتصالات (مودم، مكررات، جسور) ونظم التشغيل في الأجهزة والشبكات، ومحطات العمل، ومنطقة امتدادها، وما تشمله من إجراءات، وعلاقات مع كافة المتعاملين في مجال النظام المعلوماتي، والعاملين والمواقع الوظيفية لهم وامتداد أعمالهم، وبشكل عام تحديد امتداد بيئة النظام.

٦ ـ توفير قسم متخصص بأمن المعلومات يكون من المتخصصين في مجال أمن المعلومات ومن ذوي الخبرة الفنية والأمنية ليشرف على بناء وتطوير السياسة الأمنية بالمؤسسة، كما يشرف على تنفيذها، وينسق مع فريق تطوير النظم، ومديري الشبكات، وفريق الصيانة، والإشراف على عقود توريد الأجهزة والبرامج حتى يتأكد من مطابقتها للنواحي الأمنية، كما يكون على إطلاع على كل ما هو جديد في مجال



جرائم نظم المعلومات.

وفي ما يخص تحديد مكونات السياسة الأمنية فإنه يصعب تحديد هذه المكونات في ظل المتغيرات السريعة بشكل التقنية، ورغم هذا فحاجة المؤسسات لأمن نظم المعلومات أمر ضروري. فبعد تحديد عناصر السياسة الأمنية التي تحتاجها المؤسسة يجب أن تشمل تلك العناصر توجيهات وأوامر إلى الأفراد العاملين بالمؤسسة في كل عنصر من عناصر السياسة الأمنية ويكون مفادها (إفعل أو لا تفعل) ومن العناصر التي يجب أن تتركز على العناصر الأساسية لأمن المعلومات هي: أمن الأجهزة والبيانات (المحفوظة ـ المنقولة) والعاملين، وبشكل عام سوف يتم التطرق إلى بعض العناصر المهمة التي تحتاجها غالبية المؤسسات، على النحو التالي:

١ ـ مراعاة الجانب البشري كإخضاع الموظفين الذين سوف يعملون في مناطق حساسة للتحريات الأمنية للتأكد من سجلهم الجنائي قبل قبولهم في تلك الوظائف الحساسة. وإطلاع الأفراد على السياسة الأمنية وتوقيعهم عليها، ومعاقبة المخالفين لتعليماتها بالعقوبات المناسبة. ومنع التوظيف المؤقت نهائياً، ومراعاة إجراءات إنهاء خدمة الموظف بطلب تسليم كل ما كان بحوزته كالمفاتيح والبطاقات الممغنطة، وتغيير كلمة المرور قبل مغادرته. ومتابعة العاملين ونقلهم إجبارياً بين الأقسام المختلفة في الإدارة، وملاحظة الذين لا يطلبون إجازة بإجبارهم على الإجازة ومراقبة النظام بعد ذلك للتأكد من عدم وجود خلل كانوا يتفادونه بوجودهم. وعقد ندوات ومؤتمرات ومحاضرات بشكل دوري في مجال أمن المعلومات، والاشتراك في المجلات المتخصصة بأمن المعلومات، وعرض النشرات الداخلية وتعليمات الإدارة التي تتضمن إطلاع الأفراد على المعلومات المهمة في مجال الأمن، لإلزام العاملين بالنظم الإدارية المحددة. وندب العاملين لحضور المعارض العالمية للأجهزة والبرامج، والابتعاث إلى الدورات المتخصصة بأمن المعلومات، ليكون لديهم الخلفية القوية بما يكفل تحقيق أمن المعلومات بالمؤسسة. واعتماد تجزئة الأعمال والمهام الحساسة وعدم احتكارها من البداية إلى النهاية لدى شخص معين. ومنح الحوافز وربط الترقية والدورات (والحوافز الأخرى) بمدى التقيد بأمن المعلومات.

٢ ـ القيام بالتدقيق الأمني للبنية التحتية لتقنية المعلومات من منظور (داخلي ـ خارجي) حيث يعطي صورة جيدة للوضع الأمني القائم بالمؤسسة، ومعرفة مدى صحة اتباع الإجراءات والقوانين والنظم الداخلية، وكذلك الخطوات الفنية الخاصة بحماية المعلومات في المؤسسة بصورة سليمة. ويشمل التدقيق الأمني خطة استمرارية العمل، وطريقة التحكم بالنفاذ إلى نظم إدارة أجهزة الحاسب الآلي والشبكات، وإجراءات صيانة النظم، وأمن البيئة وأعمال الحراسة الأمنية، وتحديد الموارد والتحكم بها، وأسلوب تحقيق الأمن الشخصي.

٣ ـ توفير برامج الحماية المناسبة لأمن المعلومات المخزنة بالحاسب الآلي، وعمل الإعدادات الخاصة بالحاسب الآلي والأجهزة الملحقة به

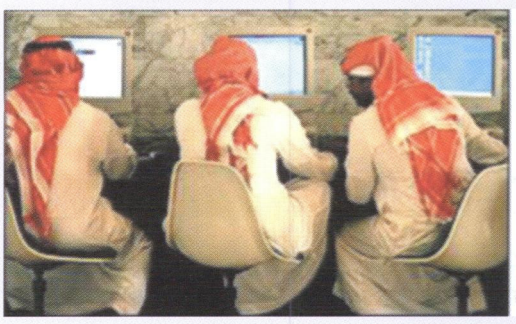
والتي تكفل أمن المعلومات الداخلية، كحذف الملفات غير المهمة ولو كانت المعلومات التي تحويها ضئيلة وعديمة الفائدة. لأنها في المقابل قد تكون ثمينة بالنسبة للآخرين، وقد تكون الخيط الرفيع الذي سيقودهم إلى معلومات أكثر أهمية، ولإزالة تلك البيانات القديمة يتم استخدام أدوات تقوم بحذف الملفات من المساحات حذفاً لا يمكن استعادته بعد ذلك، والكشف على الحاسب الآلي بعد الغياب عن طريق المستكشف، ومسح الآثار من قائمة المستندات، لأنها تبقى ركيزة أساسية للاختراق، ونسخ البيانات الحساسة على قرص مرن خارجي، وحذف الملفات الأصلية والمهمة عن القرص الصلب، وعدم ترك الملفات المهمة بالقرص الصلب وخصوصاً عند الارتباط بالشبكات. وأخذ الاحتياطات الأمنية المتعلقة بتغيير الإعدادات للتطبيقات ولنظام التشغيل كإخفاء شريط المهام، حتى لا يتمكن قليل الخبرة من معرفة مكانه، بجعله على وضع الإخفاء التلقائي لشريط المهام، ليخفي قائمة «إبدأ» وأسماء البرامج، ومنع تعديل الملف من قبل الآخرين عن طريق الخطأ أو العمد وجعله للقراءة فقط.

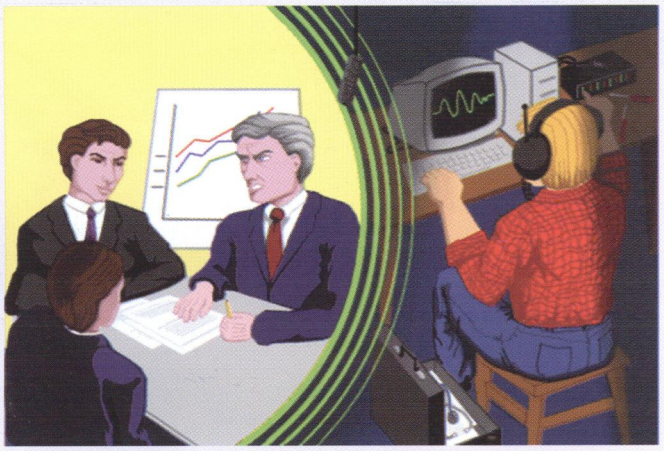
٤ ـ توزيع الصلاحيات والمسؤوليات حسب الهيكل التنظيمي، ووضع آلية يتم تنفيذها للقيام بالنسخ الإحتياطي ووسائط الحفظ الخارجية بما يكفل أمنها وتحديثها، وصياغة الضوابط المنظمة لعمليات التشغيل، ولمبرمجي قواعد البيانات ومديريها، ولإدارة الشبكات وخطوط الاتصال، ولعمليات الإدخال والإخراج، والضوابط الأمنية لبناء وتشغيل البرامج التطبيقية، ورصد الثغرات التي يمكن أن تستغل لارتكاب الجرائم. واستخدام وسائل حماية تساعد في تتبع المجرمين، والتأكد من مزامنة ساعات الأجهزة باستمرار. واتخاذ الإجراء اللازم في حالة وقوع الجريمة.

٥ ـ حماية البيانات المنقولة وتأمين جميع مكونات الشبكة، حيث يلزم استخدام برامج حماية تعمل كجدار ناري تمنع المخترقين وتعطي معلومات عن جهة الإتصال.

٦ ـ تحديد إجراءات الدخول للموقع المكاني لخدمات تقنية المعلوماتية، وتحديد المعدات المادية والتقنية والتي يجب استخدامها لتأمين الدخول إلى الموقع، بالإضافة إلى تحديد واجبات الحراسات البشرية.

٧ ـ وضع خطط للطوارئ تتبع في حالة حدوث كوارث طبيعية، أو صناعية وتتطلب الخطة توضيح الإجراءات التي يتطلبها النظام المعلوماتي حين وقوع الكوارث وبالتفصيل كشرح أهداف الخطة، وطرق مواجهة الكوارث، ونقل البيانات، ووسيلة الإنذارات، كما يجب أن تتضمن مواصفات المباني الخاصة بالأجهزة، وسلامتها من حدوث المخاطر، وسياسات بناء المرافق الجديدة أو مركز الاتصالات وأيضاً طريقة الدخول للمبنى، والعمل على تفريغ الكهرباء الساكنة، ومراعاة التكييف والخدمات التي يجب تأمينها والتي قد يسبب توقفها تلفاً للأجهزة واختيار المكان المناسب للأجهزة.





٨ ـ تحديد طريقة توليف كلمات المرور لتسجيل الدخول إلى شبكة أو الحاسب الآلي بنمط يلائم الوظيفة وتحديدها بمواصفات تمنع من كسرها.

٩ ـ توضيح أسلوب حفظ النسخ الإحتياطية ووسائط الحفظ وإتلاف البيانات وتكمن هذه الحماية للمحافظة على المعلومات من التلف ولحفظ المعلومات للأوقات الحرجة وتعالج الحفظ الداخلي للبيانات، وطريقة إعداد النسخ والفترة الزمنية للحفظ وإجراءات المراجعة والتدقيق، وتحديد الطرق والأدوات المستعملة في إتلاف البيانات.

١٠ ـ وضع تعليمات لكافة المستويات الإدارية، وجميع التخصصات، توضح الواجبات المتعلقة بالوظيفة التي لا تتغير إلا بتغير الأداة المستخدمة أو الهيكل التنظيمي، والإجرات التي يمكن تطويرها باستمرار لتكفل سرعة الأداء وتبسيطه.

١١ ـ اختبار البرامج الجاهزة ومدى ملاءمتها للقيام بالأعمال المنوطة بها مع مراعاة الجانب الأمني للأداء، والعمل على تحديث تلك البرامج من بيئة الإنتاج.

١٢ ـ تحديد الموارد المتاحة للتشارك، وإعطاء الصلاحيات للعاملين حسب الهيكل التنظيمي للمهام والاستفادة من الموارد، وتضمين السياسة استخدام تطبيقات تقوم بمراقبة منافذ التشارك في الموارد.

١٣ ـ عدم إدخال أو إخراج أي جهاز حاسب الآلي أو جهاز أخر أو وسائط حفظ من غير إذن المؤسسة، كما يجب لفت انتباه الموظفين بعدم إحضار أي أجهزة شخصية لهم داخل المؤسسة، أو وسائط حفظ، كما يجب تضمينها إلزام الموظفين بحفظ النسخ الإحتياطية بطريقة آمنة، والمحافظة على وسائط الحفظ، وتأمين الأجهزة بما يضمن عدم اختراقها من أي مصدر.

١٤ ـ إبرام الإتفاقيات والشروط بين المؤسسات وبين المنتجين والموردين للتقنية، والجهات التي تقوم بتجهيز وتركيب العتاد داخل المؤسسات، ولهذا عليهم فهم واحترام السياسات الأمنية للمؤسسات.

ويجب أن تكون هناك اتفاقيات تنظم الأعمال المشتركة بين الشركات، وما تفعله الشركة باتجاه المنافسين كأن تمنع موظفيها حتى ولو خارج العمل بالذهاب أو العمل أو الدعاية لمنتجات المنافسين، أو استعمالها.

١٥ ـ وضع القواعد الأساسية لتطوير برامج آمنة تتوافق مع آليات نظم التشغيل وقاعدة البيانات أوالبرامج المساعدة، وعدم تركيب البرامج التي تخل بأمنه.

١٦ ـ وضع سياسة أمنية لاستخدام الإنترنت. وتتطلب السياسة، استخدام الإنترنت وفق احتياجات المؤسسة ومنع منتسبيها من الاستخدام غير الضروري، وشرح إجراءات تحميل البرامج، والإلزام بتزويد المواقع بوسائل الحماية وخصوصاً عندما يكون الموقع مرتبطاً بالشبكة الداخلية للمؤسسة. ولاستمرارية عمل الموقع لا بد من تضمين السياسات الأمنية صيانة برامج ودعم المواقع، كما يجب أن تحكم السياسات محتوى المعلومات على موقع الإنترنت، وتحديد المعلومات المناسبة وكيفية التعامل بالمعلومات التي يتم جمعها من خدمات المواقع وإلزام الموظفين عند استخدام الإنترنت بعدم حفظ كلمة المرور الخاصة بالمستخدم وقت الدخول للإنترنت، وغلق المتصفح حال الابتعاد عن الجهاز لتعطيل خاصية الرجوع للخلف في المتصفح، وعدم استخدام خاصية تذكر اسم المستخدم وكلمة المرور. وعدم استخدام خاصية الإكمال الآلي للإسم وفراغات النماذج في المتصفح. وعدم استخدام خاصية تذكر الصفحات التي تتم زيارتها لفترات طويلة.

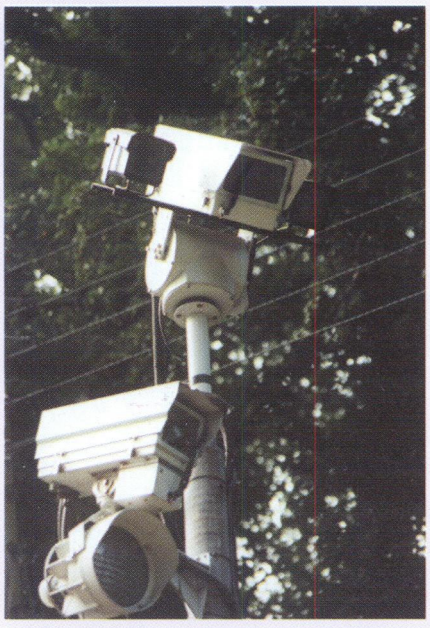
١٧ ـ وضع سياسة أمنية لاستخدام البريد الإلكتروني. وتتطلب سياسة البريد الإلكتروني وصف الأعمال التي تتبع في إدارة نظام البريد الإلكتروني، وتحديد من لهم الحق بمسح الرسائل، وتحديد حجم الرسائل لمنع ازدحام الشبكة وتخفيف المشاكل الأخرى، وتعيين المفوضين باستخدام البريد الإلكتروني، ورصد الوسائل المساعدة في إرسال الرسائل، وتوضيح طرق حفظ الرسائل، واستخدام الاتصال الآمن بتشفير البيانات قبل الإرسال وإلزام الموظفين عند استخدام البريد الإلكتروني بعدم فتح الملفات المرفقة إلا بعد التأكد منها، وعدم تحويل الرسائل المشبوهة.

١٨ ـ وضع تعليمات الحماية من الفيروسات وكل ما يؤدي لعدم الإصابة بها كتركيب البرامج المضادة للفيروسات على الجهاز وتشغيلها طوال فترة استخدام الجهاز حيث أن هذا يتيح لهذه البرامج البحث عن الفيروسات وتدميرها سواء كان أسبوعياً أو يومياً أو عند التشغيل، ومن الضروري أيضاً تحديث برامج كشف الفيروسات بصورة دورية، من خلال الحصول عليها من الشركة المنتجة، أو من مواقع الإنترنت المختلفة لضمان الحصول على آخر المعلومات والأعراض الخاصة بالفيروسات الجديدة، وطريقة الوقاية منها وإلزام الموظفين بتشغيل برامج كشف الفيروسات، وتفحص أية ملفات أو برامج جديدة تصل عبر البريد الإلكتروني، والإنترنت، والأقراص المرنة وعدم السماح بإدخال وتشغيل أية ملفات أو برامج مجهولة المصدر وبدون الفحص مسبقاً، والإنتباه إلى عدم تشغيل أو إعادة تشغيل الحاسب الآلي بوجود القرص المرن في موقعه.

١٩ ـ استخدام التشفير لمنع التصنت على المعلومات، وذلك باستخدام الشهادات الرقمية من الجهات المانحة لها، أو استخدام البصمة الإلكترونية، أو استخدام التوقيع الرقمي.

النتائج والتوصيات

١ ـ تتكون عينة العاملين بمجال نظم المعلومات من (٦٨) فرداً، يمثلون كلاً من قطاع الشركات المتخصصة في مجال تقنية المعلومات (٥٠,٠٪)، والقطاع الحكومي (١٦,٢٪)، وقطاع الشركات غير المتخصصة في مجال تقنية المعلومات (١٧,٦٪). ويعمل ما نسبته (٩٨,٥٪) منهم في مؤسسات تتوفر فيها الإنترنت، وما نسبته (٨٦,٨٪) منهم يعملون في مؤسسات تربط الانترنت بالشبكة المحلية المربوطة بمزود الخدمة، وما نسبته (٧٩,٤٪) منهم يعملون بمؤسسات تتوفر فيها سياسات أمنية، وما نسبته (٥١,٥٪) منهم يعملون في مؤسسات تصرف أكثر من (٣٠٪) على تقنية المعلومات إلى إجمالي الميزانية، كما أن الشركات المتخصصة في مجال تقنية المعلومات تنفق على التقنية أكثر من بقية القطاعات، وما نسبته (٤٥,٦٪) منهم يعملون في مؤسسات تمتلك أكثر من (١٠٠٠) جهاز حاسب آلي، وما نسبته (٧٣,٥٪) منهم يعملون بمؤسسات يتوفر بها قسم متخصص في أمن المعلومات.



الإجراء الأمني	المتوسط الحسابي	الانحراف المعياري
١ ـ اختيار نوعية مناسبة من وسائل الحماية تلائم نوع التطبيق.	٤,١٦١٨	٠,٧٨٤٤
٢ ـ توزيع الصلاحيات والمسؤوليات حسب الهيكل التنظيمي بما يضمن رفع المستوى الأمني وتقليص الجرائم .	٤,٠٤٤١	٠,٢٠٦٩
٣ ـ الضوابط الأمنية لبناء وتشغيل البرامج التطبيقية.	٣,٩٥٥٩	٠,٦٠٩٢
٤ ـ عدم السماح لغير المصرح لهم بالدخول إلى غرفة الحاسب الآلي، ومخزن وسائط التخزين.	٣,٩٢٦٥	٠,٣٥٨٩
٥ ـ اللزام العاملين بالنظم الإدارية المحددة.	٣,٧٣٥٣	٠,٦٣٧٦
٦ ـ الطلب ممن يلتحق حديثاً بالخدمة تزكية كشرط للتوظيف.	٣,٧٣٥٣	٠,٦٣٧٦
٧ ـ الإجراءات التي تكفل أمن النسخ الاحتياطي ووسائط الحفظ الخارجية.	٠,٧٠٥٩	٠,٩٣١٤
٨ ـ الإجراءات الأمنية لصيانة الأجهزة.	٣,٦٦١٨	٠,٨٩١٣
٩ ـ ضوابط عمليات الإدخال والإخراج.	٣,٦١٧٦	٠,٦٩١٧
١٠ ـ رصد الثغرات التي يمكن أن تستغل لارتكاب الجرائم.	٣,٥٠٠٠	١,١٥٢٥
١١ ـ الضوابط المنظمة لعمليات التشغيل.	٣,٣٨٢٤	٥٧٣٨
١٢ ـ تحديث برامج الحماية باستمرار.	٣,٤٧٠٦	١,٤٠٨٦
١٣ ـ استخدام وسائل حماية تساعد في تتبع المجرمين.	٣,٣٦٧٦	١,١٥٧٨
١٤ ـ ضوابط إدارة الشبكات وخطوط الاتصال.	٣,٣٠٨٨	٧٣٨٢٠
١٥ ـ استخدام التقنية للدخول على النظم (بصمة الإصبع، بصمة العين، البطاقة المغنطة).	٣,٣٢٣٥	١,٥٨٧٦
١٦ ـ ضوابط مبرمجي قواعد البيانات ومدرائها.	٣,٣٠٨٨	١,٠١١٢
١٧ ـ إجراءات تحديث النسخ الاحتياطي المركزي.	٣,١٩١٢	١,٣٨٥٠
١٨ ـ تشكيل فريق طوارئ للتعامل مع الجريمة.	٣,٠٧٣٥	١,١٧٥٨
١٩ ـ التقدم بشكوى حول جرائم نظم المعلومات.	٢,٩٥٥٩	٠,٧٦١٧
٢٠ ـ تحديد مدة صلاحية كلمات المرور وتغييرها.	٢,٧٥٠٠	٠,٩٨٣١
٢١ ـ ربط الترقية والدورات (الحوافز الأخرى) بمدى التقيد بأمن المعلومات.	٢,٦٦١٨	١,٢٨٨٤
٢٢ ـ التأكد من مزامنة ساعات الأجهزة باستمرار.	٢,٤٤١٢	١,٣٠٨٨
٢٣ ـ منح ا لحوافز للالتزام بالإجراءات الأمنية.	٢,٢٥٠٠	١,١٧٦٦
٢٤ ـ توفير أجهزة بدون محركات أقراص مرنة لعدم إتاحة استخدامها.	٢,٢٠٥٩	١,٠٧٢٩
المتوسط الإجمالي.	٣,٣٢٢٤	٠,٩٣٨٨

٢ ـ يتضح من الجدول أن أقل الإجراءات اتباعاً (على الترتيب) تكمن توفير أجهزة بدون محركات أقراص مرنة لعدم إتاحة استخدامها (٢,٢٠)، ومنح الحوافز للالتزام بالإجراءات الأمنية (٢,٢٥)، والتأكد من مزامنة ساعات الأجهزة باستمرار (٢,٤٤)، وربط الترقية والدورات (والحوافز الأخرى) بمدى التقيد بأمن المعلومات (٢,٦٦)، وتحديد مدة صلاحية كلمات المرور وتغييرها (٢,٧٥)، والتقدم بشكوى حول جرائم نظم المعلومات (٢,٩٥)، وتحديث النسخ الاحتياطي المركزي (٣,٠٧).

وهذا يدل على أن هناك قصوراً أمنياً باتباع تلك الإجراءات.. ولهذا توصي هذه الدراسات بضرورة الاهتمام باتباعها وبالتالي النهوض بمستوى أمن المعلومات.

٣ ـ يتضح أيضاً أن عدم تقارب وتركز إجابات العينة وتشتتها الإجراءات التالية (مرتبة تنازليا) استخدام التقنية للدخول على الأنظمة (بصمة الإصبع، بصمة العين، البطاقات المغنطة) (١,٥٩)، التدريب الدوري على أمن المعلومات (١,٤٥)، تحديث برامج الحماية باستمرار (١,٤٠)، تحديث النسخ الاحتياطي المركزي (١,٣٩)، التأكد من مزامنة ساعات الأجهزة باستمرار (١,٣٠)، ربط الترقية والدورات (والحوافز الأخرى) بمدى التقيد بأمن المعلومات (١,٢٩)، الضوابط المنظمة لعمليات التشغيل (١,٢٦)، منح الحوافز للالتزام بالإجراءات الأمنية (١,١٧)، تشكيل فريق طوارئ للتعامل مع الجريمة (١,١٧)، ضوابط مبرمجي قواعد البيانات ومديريها (١,٠١)، وهذا يدل على اختلاف الإجراءات الأمنية المتبعة بالمؤسسات، ويعزى إلى نوع المؤسسات المشمولة بهذه الدراسة إذ يعتمد مستوى الأمن لديها على درجة أهمية معلوماتها والنشاط الذي تمارسه تلك المؤسسات.

٤ ـ يدرك أفراد عينة الدراسة (العاملين بمجال نظم المعلومات) بدرجة قوية أهمية وجود إجراءات إدارية وفنية لأمن المعلومات(٤,٩٣).

٥ ـ أشارت النتائج إلى أن أقل إجراءات التوعية اتباعاً إقامة الندوات والمحاضرات (١٨,١٪). وأن الإشتراكات بالمجلات والدوريات بلغت نسبتها (٣٥,٣٪). ولهذا توصي هذه الدراسة بضرورة قيام المؤسسات بعقد الندوات والاشتراك بذلك النوع من المجالات، للتعرف على أحدث الطرق والإجراءات التي من شأنها أن تساعد على تحقيق أمن المعلومات.

٦ ـ أظهرت النتائج عدم وجود سياسة أمنية واضحة لأمن نظم المعلومات بالمؤسسات (٩٣,٣٪)، ولهذا توصي هذه الدراسة بضرورة إيجاد سياسة أمنية واضحة للنهوض بمستوى أمن المعلومات.

٧ ـ أظهرت النتائج أهم العناصر التي يجب توفرها بالسياسة الأمنية على الترتيب، عدم التزام الموظفين بالسياسة الأمنية ووضع عقوبات للمخالفين (٤,٩٣)، وعدم وجود سياسة معينة للتعامل مع من يرتكب الجرائم المعلوماتية (٤,٩١)، وعدم الإعلان عن السياسة الأمنية للموظفين بما يكفل تبليغها للعموم (٤,٨٠)، وعدم تقيد الرؤساء عند إعطاء التعليمات (٤,٤١). ولهذا توصي هذه الدراسة بضرورة الاهتمام بتوفر تلك العناصر بالسياسة الأمنية للنهوض بمستوى أمن المعلومات.

٨ ـ أظهرت النتائج أهم العناصر التي يجب توفرها بالسياسة الأمنية على الترتيب المشاركة في الخدمات (٢٢,٢٧٪)، والعلاقة بالمنافسين والشركاء (٢٤,١٪)، والوثائق ووسائط الحفظ (٢٧,٠٪)، والبرامج المطورة داخلياً (٢٩,١٪)، والجانب البشري (٤٣,٣٪).

ولهذا توصي هذه الدراسة بضرورة الاهتمام بتوضيح تلك العناصر بالسياسة الأمنية للنهوض بمستوى أمن نظم المعلومات.

---

*وزارة الدفاع والطيران ـ الرياض ـ المملكة العربية السعودية.