المبحث الثاني

امن المعلومات المحاسبية :

يتزايد الاهتمام بتوفير الوسائل الكفيلة بحماية تظم المعلومات والرقابة علي عملياتها بهدف ضمان استمرارية عملها بالطريقة المطلوبة فهذه النظم ينمن ان تكون مصدرا لمشاكل خطيرة في حال تعطلها عن العمل لاي سبب من الاسباب، فالتصرفات غير الصحيحة سواء عن قصد او غير قصد وكذلك الكوارث الطبيعية يمكن ان تجعل نظم المعلومات تعمل بطريقة غير الطريقة التي صممت من اجلها وفي مثل هذه الحالات تصبح المعلومات ليس فقط عديمة الفائدة بل مصدرا لمشاكل عديدة قد تحلق ضررا كبيرا بعمليات المنظمة.

ومن هنا تظهر مهمة جديدة ومسئولية كبيرة امام ادارة نظم المعلومات في المنظمة وهو ضرورة توفير الوسائل والاساليب اللازمة لضمان استمرارية عمل هذه النظم بشكل صحيح والتخطيط الدقيق لمواجهة جميع الاخطار التي يمكن ان تؤدي الي تعطيلها او توقفها عن العمل وفي حال حدوث ذلك ، ولتمكن من اعادة تشغيلها باسرع وقت ممكن ، وتسمي هذه الوظيفة الهامة والضرورية جدا حماية وامن ونظم المعلومات.

وتهدف هذه الوظيفة الي حماية الموارد المحوسبة ومن الاخطار والتهديدات المقصودة وغير المقصودة ، التي يمكن ان تؤدي الي عمليات غير مسموح بها مثل تعديل او اكتشاف او تخريب البيانات او البرامج وتشمل اجراءات وطرق حماية البيانات قبل وخلال وبعد ادخالها علي الحاسبات ، وذلك عن طريق تدقيق المدخلات بوساط وطرق تضمن سرية ودقة الادخال من دون أي تلاعب او عطاء وحفظها في مكان امن ، وتسمية الاشخاص

المحولين للتعامل مع هذا النسخ وهنالك عدد من الاساليب للحافظ علي اسرية وامن البيانات والحسابات منها استخدام اسلوب كلمات السر ومفتاح السر .

مخاطر نظم المعلومات المحاسبية :

تضمن نظم المعلومات المحاسبية عدد من المكونات التي يمكن ان تتواجد في مواقع مختلفة ومتباعدة ، ومما يجعل هذه النظم غير محصنة ومعرضة لكثير من الاخطار ويكمن ان تكون غير مقصودة كالاخطاء البشرية او الكوارث الطبيعية ، او قد تكون اخطاء مقصودة كسرقة المعلومات وادخال الفيروسات وغيرها . وتعتبر الاخطاء المقصودة اشد ضررا علي نظم المعلومات المحاسبية لنظرا لتزايد اعداد الجرائم المحوسبة والتي يمكن ان يكون مصدرها داخل او خارج المنظمة والتي يصعب التنبؤ بها باالدوافع العديدة للاشخاص الذين يقومون بها ومن ومن اهم هذه الاخطر التي يمكن ان تحدث للنظم المحوسبة هي:

١. الوصول غير المرخص أي (غير المسموح به).الي قواعد البيانات التي تعمل علي تشغيل نظم المعلومات المحاسبية سواء من داخل او خارج الشركة.
٢. عدم كفاءة اجراءات حماية قواعد البيانات مثل استخدام نظام معلومات نظام محاسبي غير محمي بشكل كافي او يكون من السهل علي الغير اكتشاف الية الحماية المستخدمة فيها او القدرة علي تعطيلها
٣. تعطيل الاليات والتجهيزات وتوقفها عن العمل بسبب أي عطل ميكانيكي او سبب اعطال في برمجيات نظم المعلومات المستخدمة فيها
٤. التلف الذي يصاحب دخول الفيروسات اثناء انتقال المعلومات عبر قنوات او وسائل اتصال مختلفة.

٥. وجود بعض التجهيزات او المحطات الطرفية في اماكن غير آمنة ، مما يجعل سرقة المعلومات او البيانات امراً سهلاً.

٦. الكوارث الطبيعية .

٧. الاختراق المحتمل بقصد الاضرار والتحقيق .

ويمكن تصنيف الاخطار المحتملة التي يمكن ان تتعرض لها نظم المعلومات المحاسبية الي ثلاثة فئات هي :

- الاخطار البشرية وهذه الاخطار يمكن تعريفها بانها تلك الاخطار التي يمكن ان تحدث اثناء اعداد وتصميم التجهيزات وقنوات الاتصال واجهزة الحاسوب التي ستعمل علي تنفيذ نظم المعلومات المحاسبية ، وكذلك من خلال عمليات البرمجة او الاختبار او تجميع البيانات او ادخالها الي نظام ومعالجتها واسترجاعها واستخراج النتائج ، او في عمليات تحديد الصلاحيات وتشكل هذه الاخطاء البشرية الغالبية العظمي للمشاكل المتعلقة بامن وسلامة نظم المعلومات المحاسبية للمنظمات.
- الاخطار البيئية وهي الاخطار التي تسببها الزلازل والعواصف والفيضانات والاعاصير والمشاكل المتعلقة باعتبار التيار الكهربائي والحرائق ، والمشاكل الناتجة عن تعطيل نظم التكيف والتبريد وغيرها ، وتؤدي هذه الاخطار الي تعطيل عمل التجهيزات وتوقفها الي فترات طويلة نسبة لاجراء الاصلاحات اللازمة واسترداد البرمجيات وقواعد البيانات ، مما له الاثر الواضح علي امن وسلامة نظم المعلومات المحاسبية بالاضافة الي المشاكل الناجمة عن تاخير العمليات وما يصاحب ذلك من زيادة التكاليف.

- وهذه الاخطار تمثل تحديا كبيراً لادارة نظم المعلومات المحاسبية لما تسببه من خسارة كبيرة ، ويمكن ان تتم الجرائم المحوسبة سواء من خارج المنظمة من قبل اشخاص يقومون باختراق نظم المعلومات المحاسبية باستخدام الحاسوب ، وقد يتم ذلك في الغالب من خلال شبكات الاتصال ، او من قبل اشخاص ضمن المنظمة يملكون صلاحية الدخول الي النظام ولكنهم يقومون باساءة استخدام النظام بدوافع مختلفة[١٢] .

انواع المخاطر :

المخاطر هي : الاضرار المحتملة من بعض العمليات الجارية في المؤسسة والتي قد تحدث نتيجة تمكن مصادرات التهديدات من استغلال احدي نقاط الضعف في الموجودة . والمخاطر موجودة في كل مجالات الحياة ، ويتم مواجهتها لما ينبغي من ادوات واجراءات تختلف من مجال الي اخر وترتبط المخاطر بالقضاء السيراني لطبيعة الانترنت من جهة ويشمل ذلك المكونات التقنية من جهة ذاتها وكذلك فيما يتعلق بها من امور قانونية وطبيعة النشاط الانساني من جهة اخري ويشمل الاعمال والتصرفات الانسانية التي يمكنها ان تعرض سلامة الاموال والاشخاص والدول في القضاء السيراني للخطر سواء كانت هذه الاعمال مقصودة كالاعمال الاجرامية او غير المقصودة كالاخطاء والاهمال وقلة الادراك. وهذا التلازم التقني والقانوني وكذلك بين المقصود وغير المقصود هو امرا مؤكد لا سيما وان التقنية هي التي تنتج ارتكاب بعض الجرائم كما يمكن ان تكون في نفسها هدفا وموضوعاً للاعتداء.

---

[١٢] حماية انظمة المعلومات ، مصدر سبق ذكره ، ص ٣٤٠-٣٤٧.

المخاطر التقنية :

مع كل تطور تكنولوجي يزداد الاعتماد علي الاتصالات والشبكات الحاسوبية وكلما ازدادة امكانية جمع المعلومات زادت معها القدرة الي الوصول المعلومات الشخصية في الافراد ازدات امكانية الاعتداء علي الحياة الخاصة. ومع الانتشار الواسع للبرمجيات زادت المصادر المفتوحة والبرمجيات المشتركة ذات الاسس البرمجية المتشابهة ومع ارتفاع نسبة توزيع البرامج والتطبيقات المقرصنة من قبل مواقع الهارت وانتشار المعلومات الخاصة باقتحام المواقع بانخفاض تكلفتها فان كل ذلك يخلق امكانية هائلة لاستغلال نقاط الضعف في البرامج والانظمة من قبل ذو الميول الاجرامية كما يؤدي الي زيادة القدرة علي ارسال الفيروسات الحاسوبية التي يتم توزيعها عبر البريد غير المرغوب وعبر الاعلانات التي تحول قسم كبير منها الي وسيلة لزرع البرامج الخبيثة ويؤدي كل ما سبق الي كثير من الجرائم منها

علي سبيل المثال :

١. اختراق الانظمة الحاسوبية والتعرض لسرية الاتصالات.
٢. تلاعب بالمعلومات وسرقتها واستثمارها بصورة غير مشروعة.
٣. التعرض لسلامة المواقع من خلال اعاقة الخدمات او تحويل مستخدميها الي مواقع مشابهة.
٤. اساءة الاستعامل او الاهمال او التخريب من قبل القائمين علي الانظمة الحاسوبية او من قبل مستخدمين الشرعين.
٥. الجرائم السريانية المنظمة.
٦. المنافسة التجارية غير المشروعة.
٧. الاعتداء علي الملكية الفكرية[١٣] .

---

[١٣] امن المعلومات أ د. جبريل بن حسن العريسي ، استاذ ، علم المعلومات ، بجامعة الملك سعود ، وعضو في المجلس الشوري السعودي ، ود. محمد حسن الشلعوب ، ادارة المعرفة ، قسم علم المعلومات ، جامعة الملك عبد العزيز ، ص ١٤.

المبحث الثالث

امن المعلومات :

ويمكن استعراض بعض تعاريف امن المعلومات والتي وردت في مصادر الدراسة ومنها :

١. المحافظة علي اتاحة المعلومات وسلامتها وسيرتها وملكيتها والاستفادة منها
٢. الطرق والوسائل المعتمدة للسيطرة علي كافة انواع ومصادر المعلومات وحمايتها من السرقة والتشويه والابتزاز والتلف والضياع والتزوير والاستخدام غير المرخص وغير القانوني .
٣. الحماية الدقيقة والتي غالبا ما تنجز من خلال صياغة ضوابط واضحة ومحددة بشكل سليم للمراقبة والامنية وتطبيقها في فاعلية في اطار استخدام مجموعة من القواعد الرقابية.
٤. حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات حيث يتم تامين المنظمة نفسها والافراد العاملين فيها والاجهزة والحاسبات ووسائط المعلومات التي تحتوي علي بيانات المنظمة وذلك باتباع اجراءات ووسائل حماية عديدة تضمن في النهاية سلامة المعلومات.

طرق اختراق امنية المعلومات :

١. التجسس التنافسي (الصناعي) وهو عملية الدخول غير المشروع الي المعلومات والسبب في ظهور عملية التجسس التنافسي هو:

- زيادة حدة التنافس بين المنظمات.
- قصر دورة حياة المنتج.
- انخفاض هامش الربح.
- انخفاض ولاء العاملين.

وتتم عملية التجسس التنافسي بعدة طرق منها :

- الالتفاظ الذهني وهو عملية التقاط المعلومات التي تظهر علي شاشة الحاسب من قبل الاشخاص غير المحولين وذلك بوضعية الجهاز غير السليمة.
- التصنت وهي عملية التقاط المعلومات عبر خطوط الهاتف والتي تتم مباشرة عند التصنت عن المتكلم وضع مركز تصنت او مكبرات صوت صغيرة.
- التفتيش الدقيق لنفايات الشركة بحثا عن المعلومات .
- اعتماد زرائع وهمية في عملية الدخول الي نظم الحاسب المنظم مثل الادعاء بانه باحث اكاديمي او محلل شركات او مشتري يرغب بكسب ثقة الافراد العاملين.

٢. سوء استخدام المعلومات : وهي الحالة التي يتم فيها استخدام المعلومات من قبل اشخاص مسموح لهم بالاطلاع عليها ولكنها تختص اهداف غير مشروعة ويتم اساءة استخدام المعلومات بهدف تحقيق :

- اهداف شخصية مثل الانتقام في حالة طرد العامل من الشركة وبالتالي قيامه باكتشاف اسرار الشركة.
- تحقيق اهداف المنافسين مقابل الحصول علي المال.
- نسخ المعلومات المحذوفة في دائرة الحاسب او في وسائط التخريب

- تعديل في برامج الحاسب اثناء تصميمه او تحديثه وذلك لتحقيق اهداف معينة غير مشروعة.
- اجراء تحويلات وهمية للنقود من خلال مستحقات مصطنعه.
- دفع مستحقات لشركة وهمية بتغذية الحاسب بقوائم دفع وهمية.
- طبع قوائم حسابات غير حقيقية واستغلال ثقة الزبائن بالحاسوب.

الإهمال:

من الأسباب الرئيسية لعملية الأفراد العاملين هو تعاونهم وضعف إدراكهم لأهمية الاحتفاظ بسرية المعلومات أوعدم معرفتهم بالمعلومات التي تحتاج الى حماية ومن يمتلك الدافع الى سرقتها سواء من داخل المنظمة أو خارجها.

تدمير المعلومات :

وتتم عملية تدمير المعلومات من خلال استخدام الفيروسات والتي تعمل على إتلاف البرامج والمعلومات وحذفها وتشوييهها وتحريفها وحذف الملفات وإعاده تسميتها وتغير تواريخ الملفات المخزونة .

مجالات اختراق أمنيه المعلومات:

تعتبر مجالات اختراق أمنية المعلومات الأساس فى توفير الفرص المناسبة للاختراق وذلك من خلال :

١. الملفات الورقية : ما زالت تحتل الملفات الورقية النسبة الأكبرمن الملفات المستخدمة فى المنظمة على الرغم من استخدم الملفات المحوسبة ،ولذلك تعتبر مجالا مناسبة

لاختراق أمنيه المعلومات من خلال:

- استعمال أجهزة النسخ :حيث يتم استعمال أجهزة النسخ فى نسخ ملفات أكثر لأنفسهم،أونسيان النسخة الأصلية او بعض النسخ المصورة فى الجهاز ،ولذلك يجب عدم نسخ أكثر من النسخ المقررة مع الحزر الشديد فى استرداد النسخ الأصلية بعد الأنتهاء من عملية النسخ.
- رمي النسخ رديئة الطبع والتي تحتوي على معلومات مهمة دون القيام بعملية إتلافها بصورة مناسبة.
- فشل اداره المنظمة فى التعامل مع بحوثها الداخلية من خلال نشرها لمعلومات هامة مثل اعلان طرح منتج جديد وغيرها.

٢. الهاتف النقال: إن استخدام الهاتف النقال قد كون مجالاً مناسباً لاختراق أمنية المعلومات وذلك من قبل المهتمين بالمعلومات المتدفقة من خلال استراق السمع من قبل الأفراد المهتمين اومن خلال التقاط المعلومات بواسطه(SCANNERS) الخاصة بالراديو وذلك عندما يتم ضبطها مع التردد المناسب ،ولذلك أفضل إجراء يجب اتخاذه فى هذه الحالة هو تجنب مناقشه الأمور الهامه عبر التلفون،والامتناع عن التحدث بالمعلومات الهامة التي تضر بالمنظمة عند تسربها.

٣. الثرثرة: تعتبر الثرثرة مجالاً هاماً فى اختراق أمنية المعلومات ،وهي تتم من خلال:

- المناقشات التي تجري خلال الاجتماعات الرسمية والمؤتمرات والتي يجب ان يتواخى المتحدث باسم المنظمة الحذر الشديد فى طرح ومناقشة بعض الامور التي تخص المنظمة وذلك لاسباب المنافسة.

- المناقشات والحديث الذي يجري خلال فتره استراحة الموظفين والتي قد يقضوها معاً فى تناول الاكل والمشروبات ،وذلك من خلال التطرق لموضوعات ومعلومات سرية تخص العمل قد يستفيد منها بعض الجالسين مع الموظفين وغير المسموح لهم بالأطلاع على هذه المعلومات ، وقد ينصت بعض الأفراد الجالسين بالقرب منهم وقد يكونوا مع علاقة مع المنافسين.

٤. التجسس وانتحال الصفة :وهذا المجال قد يضم عده فرص مختلفة فى اشكالها تفرط الثقة في نفوس العاملين فى المنظمة وبالتالي الحصول على المعلومات منها:

- الجولات السياحية التي تهتم يهدف مشاهدة المعدات وعمليات الإنتاج .
- طلب وظيفة: وقد يدعي هذا الشخص بانه طالب وظيفة ومن ثم معرفة الكثير عن المنظمة ، علما بانه يكون موظف في شركة اخري منافسة .
- باحث اكاديمي : قد يدعي البعض بانهم باحثون اكادميون وذلك لتسهيل عملية الحصول علي معلومات هامة تخص المنظمة وبذلك يجب علي اخذ الاحتياطات اللازمة للحد من تأثير هذا المجال وذلك من خلال :

١. السماح باجراء الجولات السياسية في حالات متعددة.
٢. تجنب اعطاء الكثير من المعلومات عن المنظمة لطالبي الوظيفة او الباحثين الاكاديمي
٥. الملفات الالكترونية قد يتيح هذا المجال فرصا كثيرة في عملية اخترق امنية المعلومات

منها :

- اساءة استخدام كلمة السر وذلك من خلال

- معرفة الافراد الاخرين لكلمة السر وذلك من خلال اشتراكهم بها وبالتالي ايصالها للجهات المهمة.
- وقد تكون كلمة السر ذات دلالات خاصة في حياتهم اليومية مثل اسم العائلة ، ورقم الهاتف ، ورقم السيارة ، وتاريخ الميلاد .
- الاستمرار مدة طويلة دون تغيير كلمة السر.
- كتابة كلمة السر علي المكاتب او بالقرب من اجهزة الحاسب خوفا من نسيانها.
- ترك اجهزة الحاسب المحمولة لابتوب مفتوحا اثناء السفر او في غرفة الفندق او الطيارة او القطار ، مما يعطي مجالات لاختراق امنية المعلومات من خلال الاطلاع علي ما يظهر علي الشاشة، او من خلال نسخ المعلومات بواسطة وسائط التخزين.

• حافظات الاقراص هي ايضا تعتبر مجالا لاختراق امنية المعلومات عندما تترك مفتوحة وذلك من خلال

- سرقتها
- نسخها
- تعرضها للتلف بسبب اللعب من قبل الافراد الاخرين لمحاولتهما لاستخدامها
- بيع الاجهزة القديمة من الحواسيب وتريد المنظمة استخدامها وقد تضم معلومات سرية يجب عدم الاطلاع عليها
- القيام بالاكل والشرب حول الاجهزة مما يعرضها للتلف وبالتالي فقدان المعلومات[١٤].

[١٤] نظم المعلومات المحاسبية ، مصدر سابق ، ص ٣٤-٣٨.

استراتيجية امن المعلومات :

تشمل السياسة الواضحة بشأن الاقتناء وشراء الاجهزة التنقية وادواتها والبرمجيات والحلول المتعلقة بالنظام كما تشمل استراتجية وخصوصية المعلوماتية كما تضم استراتيجية الاشتراك التي تحدد سياسة المنشاة بشان اشتراكات الغير بالمنظمة وكذلك استراتجيات تعامل مع المخاطر والاختراق حيث تعدد ما هي المخاطر والاجراءات المتبعة والتعامل معها في الجهات المسئولة.

سياسة امن المعلومات:

هي مجموعة القواعد التي يطبقها الاشخاص لدي التعامل مع التقنية ومع المعلومات داخل المنظمة وتتمثل بشئون الدخول للمعلومات والعمل علي نظمها وادارتها واخيرا لابد من التأكد من ان استراتيجية المعلومات لا تحقق نجاحا الا اذا كانت واضحة ودقيقة في محتواها ومفهومها الي كافة المعنيين.

اهداف إستراتيجية امن المعلومات :

١. تعريف المستخدمين والاداريين بالتنظيم وواجباتهم المطلوبة لحماية نظم المحاسبة والشبكات وكذلك حماية المعلومات من كافة اشكالها سواء في مراحل ادخالها او معالجتها ونقلها واعادة استرجاعها.
٢. تحديد الاليات التي يتم من خلالها تحقيق الواجبات علي من له علاقة في المعلومات ونظمها وتحديد المسئوليات عند حدوث الخطر.

٣. بيان الاجراءات المتبعة لتجاوز التهديدات والمخاطر والتعامل معها في الجهات المحاطة بها للقيام بذلك[١٥].

---

[١٥] A DIMN@WABRBAYLON.EDUIQ مصدر سابق ، جامعة بابل

المبحث الرابع

عناصر امن المعلومات

السرية :

وتعني عدم السماح للاشخاص الذين لا يحق لهم الاطلاع علي المعلومات .

الاستمرارعلي عمل الخدمة :

فمن عناصر امن المعلومات هو المحافظة علي صلاحية امن المعلومات والمحافظة استمرار الخدمة المتوفرة من خالها واستمرارية القدرة للوصول اليها لمن يسمح لهم بذلك.المحافظة علي صحة المعلومات الموجودة والتاكد من عدم العبث بها او تعديلها او تغيرها في أي مرحلة من مراحل المعالجة واستخدامها.

حسن المراقبة :

حيث تتوفر القدرة معرفة كل شخص الي المعلومات وما اجري عليها وبالتالي السيطرة علي الامور حتي لو امكن الشخص ذلك.

كيفية تحقق امن المعلومات :

اتجهت المؤسسات الي البحث عن من يستطيع تطبيق سياسة امنية لما تمتلكه من معلومات نظرا لاهميتها ومدي خطورة امتلاك بعض الاشخاص لها لذلك اتجه الكثير من الاشخاص بالتخصص في مجال امن المعلومات ، ويمكن تلخيص مقياس امن المعلومات بـ

١. التحكم بالوصول : وتعبر هذه النقطة هي المقياس الاول لتحقيق الامن فمن خلال التحكم بما يصل الي المعلومات موجودة داخل خزائن او غرف خاصة او علي اجهزة حواسيب او علي شبكة الانترنت من خلال وضع كلمات السر التي تستخدم في هذه المرحلة وتضمن عدم الاقتراب .

٢. اسباب الصلاحية : بعد ان يستطيع الشخص تجاوز المرحلة الاولي لابد من الخضوع لمرحلة اثبات الصلاحية من خلال معلومات تعطي كل شخص صلاحية تختلف عن الاخرين وهذا يضمن عملية المحافظة علي كامل المعلومات من الاقتراب ، ولو اعطينا جميع الداخلين نفس الصلاحيات علي كافة المعلومات فان عملية الاقتراع ستكون اسهل وتكون عملية ضياع المعلومات محتملة بشكل اكبر.

٣. التدقيق وحتي بعد اتمام مرحلة اثبات الصلاحية لابد من ان يخفي الشخص لمرحلة التدفيق[١٦] .

طرق واساليب امن المعلومات :

مع تزايد الحاجة الى الاتصالات وتبادل المعلومات والبيانات تزداد الحاجة الى توثيق تلك الاتصالات والتأكد من الأساليب التي تضمن شرعيتها وتأمينها من المخاطر المحتملة .ويمكن تلخيص هذه الأساليب كالأتي:

---

[١٦] موضوع اكبر موقع عرب بالعلم ، كتابة سناء الدويكات اخر تحديث ، ٢٨/ يونيو /٢٠١٦م

١. الأساليب الإداريه:

عند تجهيز نظام الأمن وإجراءاته يجب أولاً وضع موظفين الشركة فى الحسبان باعتبارهم أكبر مهدد لأمن معلوماتها والذين فى مقدرتهم العبث بنظام الحماية المعد من قبل الشركة وبذلك تمكنهم من الدخول من خارج المنشأة والسماح لغيرهم بالقيام بالمهمة.

٢. الأساليب المادية:

ويقصد بها التأكد من حماية الأجهزة ماديا وذلك عن طريق تغيير الدخول الي المكاتب والأقسام التي تحتوي على موارد حاسوبية هامه والتأكد من الاستعداد للطؤاري كالحرائق والكوارث الطبيعية بالاضافة الى ذلك حماية بيئة الحاسب الألي من التيارات الكهربائية غير المنتظمة والحقول الممغنطة والتأكد من مناسبة درجات الحرارة والرطوبة وغيرها من الأحوال المناخية التي تؤثر على اداء الحاسي الالي على الأجل الطويل.

٣. الأساليب الألكترونية:

أي أن يكون الجهاز على اتصال بالشبكة العالمية مالم يقم المستخدم فعليا بطلب هذا الاتصال وبمجرد الانتهاء فان الجهاز يقوم بقطع ذلك الاتصال.واليوم مع تقدم الاتصالات فان الغالبية العظمى من المنظمات والأفراد تعتمد على أسلوب (broadband)فى الاتصالات والتي تعني أن خط الاتصال مفتوح دائماً.وبمجرد تشغيل الجهاز،مع العلم بأن المنشات الادارية والتجارية لا تقوم بايق وتشغيل أجهزتها الى بما ندر.فانه يفتح خط الاتصال بالشبكة

العالمية ،لذلك فان اجراءات الوقاية يجب أن تكون صارمة ومكتملة ومستمرة باستمرار الاتصالات واستمرار العمل[١٧].

بعض المشاكل التي تواجه أمن أنظمة المعلومات:

تواجه أنظمه أمن المعلومات بعض المشاكل الشائعة التي بدأت تغزو أنظمه المعلومات وتساهم في تدميرها أو تخريبها أو سرقة الخزين المعلوماتي المحفوظ في أجهزه الحاسوب ومن أهم هذه المشاكل هي:

١. **الفيروسات :** تعتبر من أهم جرائم الحاسوب وأكثرها انتشاراً فى الوقت الحاضر ولم يعد يخفى على أحد ما المقصود بفيروس الحاسوب،حتى من العامة ممن لا يستخدموا الحاسوب وذلك بسبب تناقل الصحف لأخبار خسائر الشركات والحكومات والأفراد بسبب تخريب أحداثه فيروس معين ولم يعد أحد يخلط بين معنى فيروس الحاسوب والفيروس البيلوجي الذي يصيب الإنسان كما كان يحدث سابقاً بسبب عدم انتشار ثقافة الحاسوب ويمكن تعريفه على أنه برنامج حاسوب له أهداف تدميرية تهدف الى إحداث أضرار جسمية بنظام الحاسوب سواء البرامج أو الأجهزة ويستطيع ان يعدل تركيب البرامج الأخرى حيث يرتبط بها ويعمل على تخزينها ، وهو برنامج مكتوب بإحدي لغات البرمجة من قبل المبرمجين وهو قادر على التوالد والتناسخ ويستطيع الدخول الى البرامج وعلى الأفضلية أكبر من نظم التشغيل تساعده فى فحص المكونات المادية مثل الذاكره الرئيسية أو القرص المرن أو اليزري ،وقد ظهرت الفيروسات فى نهاية الأربعينات وكان أول من فكر فيها هو اختصاصي الكمبيوتر (جون قون تيونات)

---

[١٧] موقع HTTP://KENAN ON LIN.COM/USERSالتنمية التكنولوجيا ، تنمية امن المعلومات

حيث نشر مقاله حولها وظهرت بعد ذلك اثار الفيروسات فى عام ١٩٥٠م الإ أنها بقت محدودة الانتشار حتى عام ١٩٨٣م عندما تفشت الفيروسات فى برامج(UNIX) وأثارذلك ضجة على الساحة العلمية والعملية ثم ظهرت بعض الحوادثالفردية لصغار المبرمجين الذين قاموا بزرع الفيروسات فى شبكات الحاسوب،فقد قام موريس الذي كان طالباً فى جامعة كورنيل بإعداد برنامج مدمر ساهم فى تعطيل الآلف من الحواسيب مما كلف الشركات الأمريكية مائة مليون دولار ،أما كيفية اكتشاف الفيروس ،فكان عن طريق المبرمج هندي ،حيث قام بعمل برنامج خفي من أجل المحافظة على برنامجه الذي أحدث برنامج للطباعة ،حيث قام بحمايته من النسخ من خلال دخوله فى الملفات التشغيلية وهي في حالة عدم النسخ ثم يقوم بتكبير حجم الملفات ومن تخريبها واستمرت مع التطورات الحاصلة في مجال تكنولوجيا الحاسوب والبرمجيات وتطور كل من برامج الحماية مقابل ازدياد حالات ابتكار واعداد برامج فيروسية.

الاجراءات الوقائية للحماية من الفيروسات :

ان التطورات الحاصلة في مجال اعداد برامج الفيروسات جعلت من الصعوبة ايجاد طريقة مضمونة بدرجة كبيرة للوقائية من الفيروسات . ولكن هنالك بعض الاساليب الفعالة التي يمكن اتباعها للحماية وهي:

- تركيز برنامج مضاد للفيروسات ملائم لنظام التشغيل للمستخدم في جهاز الحاسوب ويفضل ان يكون نسخة اصلية للاستفادة من الدعم الفني للشركات التي يتم شراء البرامج المضادة منها.

- عدم وضع أي برنامج جديد علي جهاز الحاسوب الا بعد اختباره والتاكد من خلوه من الفيروسات بواسطة برنامج مضاد للفيروسات.
- عدم استقبال أي ملفات من افراد مجهولي الهوية علي الانترنت.
- عمل نسخ احتياطية من الملفات الهامة وحفظها في مكان امن.
- التأكد من نظافة اقراص الليزر التي يحمل منها نظام التشغيل الخاص لجهاز الحاسوب

وهذه الاساليب اضافة الي العديد من الخطوات التي يمكن اتباعها من شان ان تساهم في ضمان حماية اجهزة الحاسوب ولكن يجب ان يضع في الاعتبار ان وجود برنامج مضاد للفيروسات محدث دائما في اجهزة الحاسوب كما ان أي مشكلة لا تعني دائما ان هنالك فيروس وسبب المشكلة ومحاولة ايجاد العلاج لها.

٢. **قرصنة المعلومات :** قد يسمح الكثير عما يسمي بالهاتف او مخترقي الاجهزة والسؤال كيف يتم ذلك ؟ وهل الامر بسيط الي هذا الحد ؟ ام يحتاج لدراسة وجهد وفي الحقيقة انه ومع انتشار برامج القرصنة ووجودها في الكثير من المواقع اصبح من الممكن اختراق أي جهاز حاسوب وبدون عناء فور انزال احدي برامج القرصنة والمقصود بالقرصنة هو سرقة المعلومات وبرامج المعلومات من برامج بصورة غير شرعية وهي مخزونة في دائرة الحاسوب او نسخ برامج معلوماتية بصورة غير قانونية وتتم هذه العملية ام بالحصول علي كلمة السر او بواسطة التقاط موجات الكهرمغناطيسية بحاسوب خاص ويمكن اجراء عملية القرصنة بواسطة رشوة العاملين في المنظمات المنافسة . اما عن الهدف من عمليات القرصنة وهو سرقة الاسرار او المعلومات التجارية او التسوقية او التعرف علي حسابات المنظمات او احيانا بهدف التلاعب بقيود

المصارف او المؤسسات بهدف سرقة الاموال او يكون الهدف الكشف عن اسرار صناعية بهدف اعادة تصنيعها بدون اجازة قانونية ،أو لأهداف سياسية وعسكرية من أجل الحصول على الملفات والخطط السرية العسكرية أو الحكومية والأمثلة على حالات القرصنة عديدة ،فقد قامت الشركات الصينية بنقل أسرار تكنولوجيا صناعية من الولايات المتحدة وكندا مستخدمة الحاسوب ،ومن ثم القيام بإنتاج سلع على ضوء ذلك وتصديرها لهاتين الدولتين لتباع في أسواقها بثلث الأسعار الأصلية ،ونفس الشيء قامت به شركة متسوبيشي لبناء السفن والصناعات التقليدية حيث استخدمت سماسرة للقيام بعملية التجسس الصناعي[١٨] .

[١٨] مراجعة انظمة المحاسبة الالكترونية في بيئة الاعمال المعاصرة ، د. عبد الوهاب نصر علي ، أ. المحاسبة والمراجعة ، ص ١٩٤-١٩٧.

الفصـــــل الرابع

الجهاز المصرفي

دراسة حالة بنك الادخار والتنمية فرع بربر

الفصل الرابع

الجهاز المصرفي لمحلية بربر

دراسة حالة بنك الادخار بربر

اهداف النظام المحاسبي المصرفي :

الاهداف العامة :

وهي معرفة التهديدات الامنية الموجودة وطرق مواجهتها.

الاهداف التطبيقية: وهي:

١. معرفة مدي الحاجة للمعلومة.

٢. التعرف علي الحوادث الامنية المحتملة بعد دراسة البيئة المحيطة وسبل الرد في حال حدوث أي اختراق.

٣. تحديد الوقت المناسب لتطبيق الطرق المناسبة لمواجهة الخطر المتوقع.

٤. معرفة المفاهيم الامنية الاساسية والممارسات التي لها علاقة باجهزة الحاسوب والشبكات والانترنت.

٥. تحديد سبل تبادل ونقل الملفات والنسخ الاحتياطية للبيانات وتشفير وفك تشفير الملفات.

٦. حجب محاولات التجسس.

٧. الاستجابة للحوادث.

٨. تفعيل نظام امن الرسائل الالكترونية (مضاد الفيروسات).

٩. تطبيق امن شبكات الحاسوب FIREWALL

١٠. استخدام شبكات تشعيبية لتقوية مسارات النقاط علي الشبكة من الاختراقات الخارجية.

١١. تعزيز الامن بسطح المكتب (كلمة المرور) وعدم اعلانها للغير.

١٢. حماية اجهزة المكتب من هجمات الفيروسات.

١٣. التخلص من المعلومات منتهية الصلاحية.

١٤. عدم الدخول الي المواقع المشبوهة والتحفظ عند الاستجابة لرسائلها.

انظمة الصيرفة الالكترونية بالمصرف:

شهد مصرف الادخار بمحلية بربر في العشرة اعوام الماضية تطورا تقنيا ملموسا مستصحبا المسيرة التراكمية لبداية التقنية في العام ١٩٩٤م وتطور المصرف في مجال الانظمة واجهزة الحاسوب وملحقاته والشبكات المحلية والواسعة وتامينها.

تطبيق انظمة المشاريع القومية المربوطة ببنك السودان والتمثل في (المقاصة الالكترونية) نظام التسويات الانية الاجمالية (RTGS)، من خدمات محول القيود القومي (N- S- S) الترميز الائتماني (CODE) ، نظام سوفت العالمية بالاضافة الي خدمات المصرف عبر النظام المصرفي الشامل وربطها بانظمة الالكترونية (التحاويل الفورية ، المرتبات المركزية ، ارسال الشيكات و البطاقات الالكترونية) وواجهت ربط مع الجهات الاعتبارية للتحقيق الشمولي المالي من خلال تقديم الخدمات الالكترونية للمجموعات المتجانسة[١٩].

---

[١٩] زيارة ميدانة ومقابلات شخصية ببك الادخار فرع بربر قسم انظمة الحاسوب.

الاجانب بالاضافة الي ربط الخدمة بنظام الموبايل المصرفي وخدمة سودابان عبر الرسائل القصيرة المربوطة بالصرفات الالية.

ث. سداد اورنيك (١٥) الالكتروني وتم ربط النظام المصرفي مع اورنيك (١٥) عبر شركة الخدمات المصرفية الالكترونية واكتمال الاختبارات باتاحة خدمة السداد عبر جميع فروع المصرف المنتشرة بولايات السودان المختلفة (٥٢) فرع وتوكيل وفي انتظار انطلاق وزارة المالية للخدمة بالاضافة الي ربط الخدمة بنظام الموبايل المصرفي ونظام الدفع عبر الموبايل (ادخارك).

انظمة الصيرفة الالكترونية بالمصرف :

١. نظام الدفع عبر الهاتف النقال : هي عملية الدفع الالكتروني التي تتم بواسطة الهاتف النقال باستخدام نقود الالكترونية، ادخارك هو تطبيق مقدم من المصرف كبعد جديد ومبتكر للخدمات المصرفية الالكترونية ، من حيث نوع خدماته ، وسهولة استخدامه ليلائم شريحة عملاء المصرف اضافة الي شموله لجميع خدمات الدفع عبر الموبايل ليعطي تجربة افضل لمستخدمي البنك.

٢. ما هو البنك الالكتروني : البنك الالكتروني يشير الي النظام الذي يتيح للزبون الوصول الي حساباته او أي معلومات يردها والحصول علي مختلف الخدمات والمنتجات المصرفية من خلال الانترانت عبر جهاز الحاسوب الخاص به او عن طريق متصفح هاتفه النقال.

٣. ما هو نظام الرسائل القصيرة : هو نظام يمكن من خلاله معرفة كل ما يحدث في الحسابات الخاصة بالعمل في المصرف في أي زمان واي مكان وذلك عن طريق

ارسال الرسائل القصيرة والتي تحوي تفاصيل أي عملية تتم علي حساب العميل المصرفي.

الفصـــــل الخامس

تحليل الاستبيان واختبار الفرضية

الفصل الخامس

تحليل الاستبيان واختبار الفرضية

وفي هذا الفصل سيتم التطرق الي التأكد من صدق الاستبانة بالاضافة الي التحليل الوصفي لعينة الدراسة واختبار الفرضية.

اولا : صدق وثبات الاستبانة للدراسة :

ولقد قام الباحثون لتوزيع(١٤)استبانه على موظفين بنك الادخار وتتكون استبانه الدراسة من جزئين كما يلي:

الجزء الأول:وهو مكون من عده اسئلة تتعلق بمعلومات عامه عن أفراد العينة مثل المؤهل العلمي وسنوات الخبرة والمسمى الوظيفي ومعلومات أخرى.

الجزء الثاني:ويتكون من المخاطر التي تهدد أمن المعلومات .

صدق الاتساق الداخلي :ويقصد به مدى اتساق فقرات الإستبانه مع المجال الذي تنتمي إلية هذه الفقرة[٢٠].

[٢٠] زيارة ميدانية ومقابلات شخصية للعاملين ببنك الادخار فرع بربر

ثانياً. وصف العينة:

المؤهل العلمي	أفراد الدراسة
ثانوية عامه	٠
بكالريوس	٩
دبلوم	٥
ماجستير	٠
دكتوراه	٠
المجموع	١٤

جدول رقم(١) يوضح المؤهل العلمي

ويتضح من خلال الجدول رقم (١)أن أغلبية المشاركين في الاستقصاء كانوا بكالريوس ويمثلون (٩)من عينة أفراد الدراسة وبعض منهم دبلوم ويمثلون(٥)من أفراد عينة الدراسة ولايوجد أفراد من عينه الدراسة يمثلون ثانوية عامه ولاحتى ماجستيرأو دكتوراه، وهذا يعني أن الموظفين الذين يعملون بالبنك لهم كفاءة عالية للعمل بوظائفهم.

جدول رقم(٢) يوضح المسمي الوظيفي

المسمي الوظيفي	افراد الدراسة
محاسب مالي	٧
مراجع لنظم المعلومات الالكترونية	٠
مراجع داخلي	٠
رئيس قسم	٢
مراقب مالي	١
مدير	-
غير ذلك	٤
المجموع	١٤

من خلال الجدول رقم (٢) يمكن القول بان المحاسبون الماليون هم اكثر فئة وهم يمثلون الهيكل الوظيفي لعينة الدراسة.

جدول رقم (٣) يوضح عدد سنوات الخبرة

عدد سنوات الخبرة	افراد الدراسة
اقل من ٣ سنوات	٠
من ٣ سنوات الي ٦ سنوات	١٠
من ٧ سنوات الي ١٠ سنوات	١
من ١١ سنة الي ١٥ سنة	٢
اكثر من ١٥ سنة	١
المجموع	١٤

من خلال الجدول رقم (٣) يتضح ان عدد كبير من المشاركين في الاستقصاء تزيد خبرتهم من ٣ سنوات الي ٦ سنوات ويمثلون ١٠ من عينة الدراسة والذين تزيد خبرتهم من ٧

سنوات الي ١٠ سنوات يمثلون ١ من عينة الدراسة وان الذين تزيد خبرتهم من ١١ سنة الي ١٥ سنة يمثلون ٢ من عينة الدراسة والذين تزيد خبرتهم يمثلون ١ من اجمالي الدراسة حيث ان مع زيادة الخبرة تزداد قدرة المصرف علي مواجهة المخاطر التي يتعرض لها.

جدول رقم(٤) يوضح النظام المحاسبي بالبنك

النظام المحاسبي بالبنك	افراد الدراسة
يدوي لا يستخدم الحاسبات الالية	٠
يعتمد بدرجة كبيرة علي الكمبيوتر(شديد الالية)	١٠
خليط من العمل اليدوي والتشغيل الالكتروني	٤
المجموع	١٤

يتضح من الجدول اعلاه بان المصرف يعتمد بنسبة كبيرة علي العمل الالي وهذا يتطلب توفير حماية اكبر لنظام المعلومات لمواجهة المخاطر التي قد تتعرض لها انظمة المعلومات في المصرف.

جدول رقم (٥) يوضح مخاطر امن نظم المعلومات المحاسبية الالكترونية:

مخاطر امن نظم المعلومات المحاسبية الالكترونية	اقل من مرة واحدة سنوية	اقل من مرة سنويا الي مرة شهريا	اكثر من مرة شهريا الي مرة اسبوعيا	اكثر من مرة اسبوعيا الي مرة يوميا	اكثر من مرة يوميا او بصفة متكررة
الادخال غير المعتمد لبيانات غير سليمة بواسطة الموظفين	٨	١	١	٤	٠
الادخال المعتمد لبيانات غير سليمة بواسطة الموظفين	١٣	٠	٠	١	٠
التدمير غير المعتمد بواسطة الموظفين	١٠	١	٠	٠	٣
التدمير المعتمد للبيانات بواسطة الموظفين	١٢	٢	٠	٠	٠
الوصول غير الشرعي للبيانات النظام بواسطة الموظفين	٩	٥	٠	٠	٠
الوصول غير الشرعي لبيانات النظام بواسطة اشخاص اخرين	١٢	١	٠	١	٠
اشتراك الموظفين في كلمة السر	١١	١	١	١	٠
ادخال فيروس الكمبيوتر للنظام المحاسبي	١٢	١	٠	٠	١
المجموع	٧٥	١٢	٢	٥	٣

من خلال الجدول رقم (٥) يتضح الاتي : ندرة حدوث المخاطر في بنك الادخار أي انها تحدث مرة سنويا وذلك نسبة لاجابات افراد العينة عن التساؤلات التي طرحت لهم من خلال الاستبانة التي تمثل مخطار نظم المعلومات المحاسبية الالكترونية التي يمكن ان تحدث.

ثبات الاستبانة :

يقصد بثبات الاستبانة انها تعطي نفس النتيجة لو تم اعادة توزيعها اكثر من مرة ، وان ثبات الاستبانة يعني الاستقرار في نتائج الاستبانة وعدم تغيرها بشكل كبير فيها ولو تم اعادة توزيعها الي افراد العينة عدت مرات خلال فترات زمنية مختلفة وقد تحقق الباحثون من ثبات الاستبانة.

الفصـــــل السادس

النتائج والتوصيات

الفصل السادس

النتائج والتوصيات

اولاً: النتائج:

لقد توصلت هذه الدراسة الى مجموعه من النتائج والتي تعتبر في مجملها خلاصه التحليلات والمناقشات بالإضافة الى النتائج الخاصة باختبار الفرضيات.

١. أوضحت الدراسة كفاءة المحاسبون في المنظمة ومدى خبرتهم في المصرف وقلة المخاطر نسبة لأمن المعلومات في المصرف.

٢. اعتماد المصرف بشكل كبير على النظام الالي وبالتالي توفير الوقت والجهد في العمل.

٣. تعتبر مخاطر الإدخال الغير معتمد واشتراك الموظفين في كلمه السر قد تحدث مره سنوياً.

٤. تم قبول الفرضية وهي عدم حدوث مخاطر نظم المعلومات المحاسبية في بنك الإدخار حيث اوضحت الدراسة ان تلك المخاطر لا تحدث بشكل متكرر في بنك الادخار.

ثانياً: التوصيات:

وبعد إستعراض نتائج الدراسة يمكننا الخروج بالتوصيات الاتية:

١. وضع اجراءت تضمن استمرارية عمل وجاهزية نظم المعلومات للعمل في حالة الازمات من خلال استخدام تجهيزات مرتبة بحيث تستطيع اكتشاف المخاطر قبل حدوثها.

٢. العمل على تشفير المعلومات عند الحفظ والنقل والتخزين علي مختلف الوسائط حتي لا يتمكن احد من اختراقها.

٣. التوصية بأهمية امن نظم المعلوماتية وضرورة وضع سياسة امنية لمنظوماتهاه المعلوماتية.

٤. ضرورة وجود خطة لحماية امنية شاملة.

٥. الاشراف علي حسن تطبيق اجراءات امن نظم المعلوماتية.

المصادر والمراجع

١. نظم المعلومات المحاسبية ، د. احمد حلمي جمعة ، قسم المحاسبة ، د. عصام فهد العربيد ، د. زياد احمد الزغبي ، قسم نظم المعلومات الادارية ، كلية الاقتصاد والعلوم الادارية ، جامعة الزيتونة الاردنية.

٢. حماية انظمة المعلومات ، د. محمد دباس الحميد ، د. ماركو ابراهيم نيمة ، قسم نظم المعلومات الادارية ، جامعة الاسراء الخاصة.

٣. نظم المعلومات الادارية ، د. سونيا محمد البكري، د. ابراهيم سلطان ، كلية التجارية ، جامعة الاسنكدرية.

٤. نظم المعلومات المحاسبية ، المؤلف : كمال الدين الدهواري ، جامعة الشيخ عبد الله البدري ، مكتبة التكنولوجيا.

٥. نظم المعلومات المحاسبية المحوسبة ، د. فياض حمزة رملي.

٦. البسيط في تحليل وتصميم النظم ، مهندس ، عزب محمد عزب ، دار الكتب العلمية ، للنشر والتوزيع القاهرة .

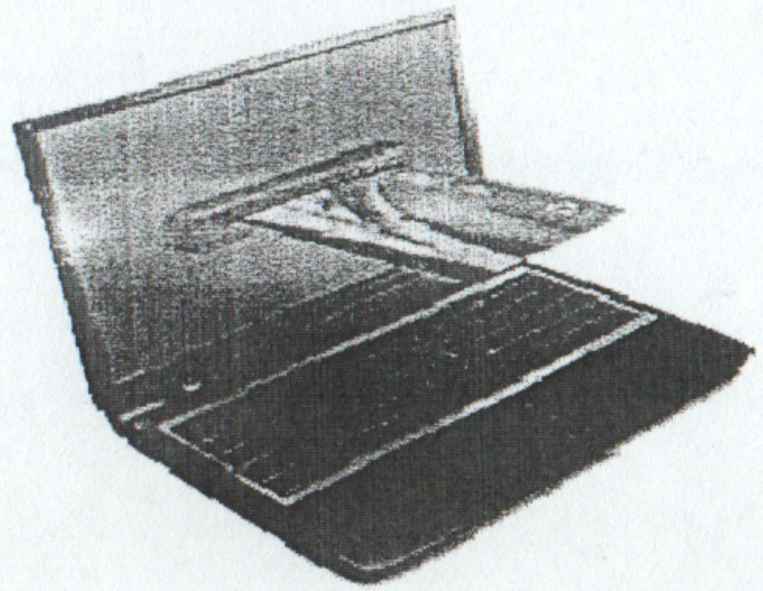
٧. CHANCELLEROFFIC٢٠١١-٢٠١٨ WEB DEVELOP DEPAR TENT

A DIMN@WABRBAYLON.EDUIQ

٨. نظم المعلومات المحاسبية ،د. سناء علي القباني ، استاذة ورئيس قسم المحاسبة ، كلية التجارة ، جامعة المنوفية.

٩. انظمة المعلومات المالية والمصرفية ، د. ثاير القدومي ، استاذ ، سامر بركات .

٣- نظام البنك الإلكتروني Electronic Bank



فهرس المحتويات

الموضوع	رقم الصفحة
الآية	أ
الإهداء	ب
الشكر والعرفان	ج
الفصل الأول	
خطة الدراسة	١
الفصل الثاني	
المبحث الأول : نظم المعلومات المحاسبية	٧
المبحث الثاني : تعريف نظام المعلومات	١٢
المبحث الثالث : أنواع نظم المعلومات	١٧
المبحث الرابع : تعريف نظم المعلومات المحاسبية	٢١
الفصل الثالث	
المبحث الأول : نظم المعلومات المحاسبية والالكترونية	٢٦
المبحث الثاني : امن المعلومات المحاسبة	٣٥
المبحث الثالث : أمن المعلومات	٤٠
المبحث الرابع : عناصر أمن المعلومات	٤٨
الفصل الرابع	
الجهاز المصرفي لمحلية بربر	٥٥
الفصل الخامس	
تحليل الاستبيان واختبار الفرضية	٦٠
الفصل السادس : النتائج والتوصيات	
أولاً : النتائج	٦٥
ثانياً : الفرضيات	٦٦
المصادر المراجع	٦٧