تحديات الأمن الالكتروني في المؤسسة

د.علوطي ليـــن
جامعة المدية

الملخص :

تكمن أهمية هده الدراسة في إظهار المفاهيم الأساسية المتعلقة بـــالأمن الالكترونـــي وكيفية تحقيقه في المؤسسة لاسيما في ظل الاستخدام المتزايـــد لتكنولوجيـــا المعلومـــات و الاتصال و تطبيقاتها المتعددة كما سنتطرق إلى تعريف المشكل الأمني وكيفية القضاء عليه واستخدام مختلف الطرق و الأدوات لحماية نظم المعلومات و نظم التشـــغيل الالكترونـــي للبيانات في المؤسسة،كما نسعى من خلال هدا البحث إلى إعطاء بعـــض الحلـــول التقنيـــة لمشكل الاختراق الأمني لنظم المعلومات الخاصة بالمؤسسات.

Résume

l'importance de cette étude consiste à éclairer les différents concepts de base de la sécurité électronique et son application dans l'entreprise surtout avec l'utilisation flagrante des nouvelles technologie de l'information et de la communication et ses différentes applications, aussi en va définir le problème sécuritaire et comment le combattre par l'utilisation des outils et des méthodes de la sécurité électronique ainsi donner les solutions techniques pour résoudre le problème des attaques sur les systèmes d'information des entreprises.

مقدمة :

يتعرَّض العديد من شبكات الحاسوب إلى عمليات هجومٍ واختراقاتٍ بسبب الســـطو على البيانات والمعلومات أو تخريب الأجهزة الالكترونية بما في ذلك شبكات المؤسســـات، وكلما كانت المعلومات هامة وحسَّاسة كلما زاد اهتمام المُخرِّبين والمُختـــرِقين بهـــا؛ ممـــا يستدعي وجوب أخذ التدابير اللازمة لحماية المعلومات والشبكات. وقد ازداد اهتمام التقنيين بهذا الجانب مع زيادة الهجمات على الشبكات والسطو على المعلومـــات، إلـــى أن أصـــبح الأمن الالكتروني تخصُّصاً منفرداً ضمن مجالات الحاسوب، كما أصبحت لـــه مؤسســـات خاصة تقوم بإنتاج نُظم وعتاد الحماية ووضع الحلول الشاملة له.وباعتبار أن نظم العمل عن

بعد باستخدام الحاسوب هي الأكثر تعرضا للهجمات الالكترونية فانه رأينا أنه من الضروري أن نشير إلى الآليات التي تمكن المؤسسة من حماية نظمها المبنية على تكنولوجيا المعلومات و الاتصال حتى لا تصبح عرضة للقرصنة وسوف نتطرق في هذا المقال إلى مفهوم الأمن الالكتروني ثم إلى آليات حماية نظم العمل عن بعد باستخدام الحاسوب .

إشكالية البحث:

في ظل الاستخدام المتواصل و المكثف لتكنولوجيا المعلومات و الاتصال في المؤسسات الاقتصادية يظل توفير الحماية الالكترونية للمعلومات و البيانات التي تتداولها المؤسسات بمختلف أنواعها فيما بينها ضروريا بل عاملا محددا لبقائها و استمرارها في بعض الأحيان، وعليه سنحاول الإجابة عن السؤال التالي ما أهمية تطبيق آليات الأمن الالكتروني في المؤسسة على فاعلية وأداء هده المؤسسات؟

وللإجابة على هده الإشكالية ارتأينا أن نطرح سؤالين جزئيين كما يلي:

- ماهي أهم المشاكل الالكترونية التي تعترض المؤسسة في ظل استخدامها الواسع تكنولوجيا المعلومات و الاتصال؟
- كيف يمكن تبني استراتيجيات خاصة بتحقيق الأمن الالكتروني في المؤسسة؟

فرضيات البحث :

من أجل الإجابة عن الإشكالية المطروحة قمنا باقتراح الفرضيات التالية:

-يعتبر توفير الأمن الالكتروني في المؤسسة تحديا هاما يستوجب توفير كامل الإمكانيات البشرية و المادية .

- تتعرض المؤسسة في ظل استخدامها لتكنولوجيا المعلومات و الاتصال إلى مشاكل الكترونية جمة مرتبطة باستخدامها للوسائط الالكترونية.

-على المؤسسة أن تتخذ عدة إجراءات احتياطية في ظل إستراتيجية معينة لمكافحة أشكال الاقتحام الالكتروني .

المنهج المتبع:

للإجابة عن هذا السؤال سنستخدم الأسلوب الوصفي التحليلي بعرض أهم المفاهيم المتعلقة بالأمن الالكتروني وأنواعه وأشكاله وطرق تحقيقه .

أولا: مفهوم الأمن الالكتروني

لكي نتمكَّن من استيعاب مفهوم الأمن الالكتروني لابد من استعراض السياق التاريخي لتطوُّر هذا المفهوم.

1-1 ظهور مصطلح الأمن الالكتروني

لقد ظلَّ هذا المجال من الأمن حتى أواخر السبعينيات معروفاً باسم أمن الاتصالات (COMSEC) ، والذي حدَّدته توصيات أمن أنظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة بما يلي[1]:

« المعايير والإجراءات المُتَّخذة لمنع وصول المعلومات إلى أيدي أشخاصٍ غير مُخوَّلين عبر الاتصالات، ولضمان أصالة وصحة هذه الاتصالات ».

وتتمثل الأهداف الرئيسية لنظام أمن الاتصالات في[2] :

-تصديق المستخدم والخادم لبعضها البعض : بروتوكول نظام أمن الاتصالات يؤيد استخدام تقنيات ترميز المفتاح القياسي (التشفير بالمفتاح العمومي) لتوثيق الاتصال إلى كل الأطراف الأخرى. وإن كان الأكثر شيوعا في التطبيق يتألف توثيقه من خدمة المستخدم على أساس الشهادة . نظام أمن الاتصالات يمكن أيضا أن يستخدم نفس الأساليب لتوثيق الخادم.

-**ضمان سلامة البيانات** : أثناء أي دورة ، البيانات لا يمكن أن يعبث بها سواء كان عن قصد أو عن غير قصد.

-**خصوصية البيانات المؤمنة** : البيانات المتناقلة بين المستخدم والخادم يجب أن تكون محمية من الاعتراض كما يمكن قراءة هذه البيانات فقط من قبل المرسل إليه(مستقبل الرسالة.

وقد تضمَّنت الأنشطة المُحدِّدة لأمن الاتصالات أربعة أجزاء هي: أمن التشفير، أمن النقل، أمن الإشعاع والأمن المادي. كما تضمّن تعريف أمن الاتصالات خاصيتين تتعلَّقان بموضوع هذه الوحدة: السرِّية والتحقُّق من الهوية.

1- السرِّية: التأكيد بأن المعلومات لم تصل لأشخاص، عمليات أو أجهزة غير مُخوَّلة بالحصول على هذه المعلومات (الحماية من إفشاء المعلومات غير المُرخَّص).

2- التحقُّق من الهوية: إجراءٌ أمني للتأكُّد من صلاحية الاتصال، الرسالة أو المصدر أو وسيلة للتحقُّق من صلاحية شخصٍ ما لاستقبال معلوماتٍ ذات تصنيفٍ مُحدَّد (أو التحقُّق من مصدر هذه المعلومات).

ولهذا المصطلح كذلك استخدام عسكري بحيث يعرف بأنه مجموعة الإجراءات التي تكفل منع العدو من الحصول على معلومات عن طريق الاتصالات وتقوم أيضاً بمنعه من التدخل الفني أو التكتيكي على شبكة الاتصالات[3].

ويستخدم كذلك مصطلح أمن المعلومات[4] وإن كان استخداماً قديماً سابقاً لولادة وسائل تكنولوجيا المعلومات والاتصال، إلا أنه وجد استخدامه الشائع بل والفعلي، في نطاق أنشطة معالجة ونقل البيانات بواسطة وسائل الحوسبة والاتصال. إذ مع شيوع الوسائل التقنية لمعالجة وخزن البيانات وتداوُلها والتفاعُل معها عبر شبكات المعلومات – وتحديداً الإنترنت – احتلَّت أبحاث ودراسات أمن المعلومات مساحةً رحبة، آخذةً في النماء من بين أبحاث تقنيات المعلومات المختلفة، ولقد تطور هذا المصطلح ليصبح حاليا الأمن الالكتروني وهو مصطلح يطلق على أمن مختلف الأجهزة الالكترونية.

وقد أصبحت النظم المعلوماتية وقواعد البيانات وشبكات الاتصال عصب العالم المعرفي والصناعي والمالي والصحي وغيرها من القطاعات. حيث أصبح من المهم الحفاظ على أمن المعلومات بعناصره الرئيسية : السرية،الأمن،التكامل والتزامن أو الاستمرارية. وعلى المستوى العالمي يبرز نظام الأيزو للاعتماد والتقييم والتقييس 27001 لضمان أمن المعلومات. كما يوجد نظام HIPAA في الولايات المتحدة الأمريكية لضمان أمن المعلومات الصحية ونظام COBIT من ISACA لأمن المعلومات[5].

2-1 تعريف الأمن الالكتروني.

نتيجة للاستخدام المكثف لتكنولوجيا المعلومات و الاتصال في المؤسسة وفي الحياة العامة بحيث أصبحت عدة أجهزة مرتبطة بالحاسوب ولواحقه تطور مفهوم امن المعلومات إلى الأمن المعلوماتي فالأمن الالكتروني وهو ذلك الفرع من علم الالكترونية و التكنولوجيا الدقيقة الذي يهدف إلى توفير السرية و الأمان لكافة الأجهزة الالكترونية المرتبطة بالوحدات الحاسوبية.

ويشمل الأمن الالكتروني بالإضافة إلى أمن المعلومات كلا من:الرقابة عن بعد (Télésurveillance)،أجهزة الإنذار (Alarme)،الرقابة عن طريق الفيديو(Vidéo surveillance)،الخ...

إن تعزيز إطار الطمأنينة الذي يشمل أمن الاتصالات ،المعلومات والشبكات وحماية البيانات والخصوصية شرطٌ أساسي لا غنى عنه لتنمية المؤسسة في إطار مجتمع المعلومات والمعرفة، وبناء الثقة بين مُستخدمي أدوات وتطبيقات تكنولوجيا الاتصالات والمعلومات. وفيما يلي الخطوط الرئيسية لتنفيذ المحور[6]:

- تأمين وإدارة حقوق النشر الرقمية على الإنترنت، وصياغة السياسات المُلزِمة لمكافحة التعدِّي على حقوق الملكية الفكرية.
- التعاوُن مع العالم الخارجي لمكافحة جرائم الفضاء الإلكتروني وإساءة استخدام تكنولوجيا الاتصالات والمعلومات؛
- تشريعات حماية البيانات وحماية الخصوصية؛
- أمن المعلومات والشبكات لضمان خصوصية المُستخدِم، وإصدار قوانين وتشريعات تُجرِّم اختراق الشبكات وتنفيذها بدقة.

إن المعلومات المهمة والإستراتيجية للمؤسسة ينبغي أن يتمَّ الحفاظ عليها، والتعامُل معها بشكلٍ سرِّي ووفق ضوابط تُحدَّد من قبل الإدارة العليا. ومن المُتطلَّبات المطلوبة لتحقيق هذا الغرض ما يلي[7]:

- **الأمن:** وهي حماية قاعدة البيانات من التخريب أو الخرق؛
- **التكامُل:** وهي حماية أجهزة الحواسيب والنُظم المُتَّصلة بها من الأخطار الخارجية؛

- السرِّية: وتعني عدم إفشاء المعلومات من قبل المستفيدين من النظـــام، وتُطبَّـــق عليهـــا النواحي القانونية في حالة مخالفة ذلك؛
- التزامُن: وهي ضمان استمرار تدفُّق المعلومات.

ويُعبِّر عن الأمن الالكتروني بأنه:« مجموعة الإجراءات الوقائية المُتَّخـــذة لحمايـــة المعلومات من السرقة أو الضياع أو التلف، ووضعها في شكل أمنٍ لحمايتها من أي اعتداءٍ عليها »[8].

الأمن الالكتروني، من زاويةٍ أكاديمية، هو كذلك العلم الذي يبحث فـــي نظريـــات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تُهدِّدها ومن أنشـــطة الاعتـــداء عليها. ومن زاويةٍ تكنولوجية، هو الوسائل والأدوات والإجراءات اللازم توفيرها لضـــمان حماية المعلومات من الأخطار الداخلية والخارجية. ومن زاويـــةٍ قانونيـــة، فـــإن الأمـــن الالكتروني هو محلُّ دراسات وتدابير حماية سرِّية وسلامة محتـــوى وتـــوفُّر المعلومـــات ومكافحة أنشطة الاعتداء عليها أو استغلال نُظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونيـــة التـــي تســـتهدف المعلومات ونُظمها (جرائم الحاسوب والإنترنت) [9].
الأمن الالكتروني هو كذلك:« مجموعة الإجراءات والتدابير الوقائية التي تُستخدم للمحافظة على المعلومات وسرِّيتها »[10].

لقد أصبحت مشكلة حماية البيانات أو المعلومات والحفاظ عليهـــا مـــن الســـرقة أو التلاعُب أو الاختراق غير المشروع موضع اهتمام العـــاملين والبـــاحثين. وهـــذا يتطلَّـــب ضرورة دراسة جميع المجالات الفنية والمادية والبشرية والقانونية التي تحمل في طياتهـــا إجراءات حماية المعلومات والحدِّ من محاولات الانتهاك أو الإتلاف.

1-3 المشكلة الأمنية

تحدث المشكلة الأمنية عندما يتم اختراق نظام العمل عن بعد من خلال أحد المهاجمين أو المتسللين (الهاكر) أو الفيروسات أو نوع آخر من أنواع البرامج الخبيثة. حيث يتسبب الاختراق في مشاكل مزعجة مثل تبطئ حركة التصفح وانقطاعه على فترات

منتظمة. ويمكن أن يتعذر الدخول إلى البيانات وفي أسوأ الأحوال يمكن اختراق المعلومات الشخصية للمستخدم[11].

وقد يتم الهجوم على الأنظمة الالكترونية للمؤسسة بواسطة[12]:

1-هجوم التنصت على الرسائل:بحيث يقوم المهاجم بمراقبة الاتصال بين المرسل و المستقبل للحصول على المعلومات السرية وهو ما يسمى بالتنصت على الاتصال؛

2-هجوم الإيقاف:هدا النوع يعتمد على قطع قناة الاتصال لإيقاف الرسالة أو البيانات من الوصول إلى المستقبل وهو ما يسمى أيضا برفض الخدمة؛

3-هجوم يعدل في محتوى الرسالة:وهنا يتدخل المهاجم بين المرسل والمستقبل وعندما تصل إليه الرسالة يقوم بتغيير محتواها ومن ثم إرسالها إلى المستقبل الذي لا يكون على علم بتغيير الرسالة؛

4-الهجوم المزور أو المفبرك:وهنا يرسل المهاجم رسالة مفادها انه صديقه ويطلب منه معلومات او كلمات سرية خاصة بالمؤسسة مثلا.

ومن أشهر أنواع الهجمات الالكترونية هجوم **السيد-العبيد** ويقوم هدا النوع من الهجوم الالكتروني على مبدأ توزيع الأدوار بين البرنامج قائد الهجوم والبرامج المنفذة للهجوم .ويقوم الشخص الآمر بالهجوم بإعداد برنامج رئيسي يرسل إشارة الهجوم لبرامج فرعية موجودة على العديد من الأنظمة المربوطة بالانترنيت[13].

وفي حالة وجود أخطاء برمجة أو إعدادات خاطئة في خادم الويب، فمن الجائز أن تسمح بدخول المستخدمين عن بعد غير المصرح لهم إلى الوثائق السرية المحتوية على معلومات شخصية أو الحصول على معلومات حول الجهاز المضيف للخادم مما يسمح بحدوث اختراق للنظام. كما يمكن لهؤلاء الأشخاص تنفيذ أوامر على جهاز الخادم المضيف مما يمكنهم تعديل النظام وإطلاق هجمات إغراقية مما يؤدي إلى تعطل الجهاز مؤقتاً، كما أن الهجمات الإغراقية تستهدف إبطاء أو شل حركة مرور البيانات عبر الشبكة. كما أنه من

خلال الهجمات الإغراقية الموزعة فإن المعتدي يقوم باستخدام عدد من الحواسيب التي سيطر عليها للهجوم على حواسيب أخرى. ويتم تركيب البرنامج الرئيسي للهجمات الإغراقية الموزعة في أحد أجهزة الحاسوب مستخدماً حساباً مسروقاً.
إن التجسس على بيانات الشبكة واعتراض المعلومات التي تنتقل بين الخادم والمستعرض يمكن أن يصبح أمراً ممكناً إذا تركت الشبكة أو الخوادم مفتوحة ونقاط ضعفها مكشوفة.

وهناك عددٌ من الأساليب للحفاظ على سرِّية وأمنية البيانات والحاسبات، منها استخدام أسلوب كلمات السر، ولكن مفاتيح السر غير كافية في الكثير من الأحيان، وهناك بعض النُظم تعتمد أسلوب التحضير وتُستخدم لتحضير قواعد البيانات.

إذن، يُعتبر موضوع حماية البيانات والحواسيب من الأمور الواجب الاهتمام بها في كافة مراحل إعداد نُظم المعلومات باتِّخاذ إجراءاتٍ عديدة، منها تخصصُّ قواعد البيانات والبرامج، ومنها مادي يخصُّ مواقع الحواسيب نفسها، كذلك تخصُّ إجراءاتٍ أمنية تخصُّ الأفراد العاملين وتحديد المُخوَّلين للولوج وكلمات السر والقيود الفنية التي تمنع غير المُخوَّلين من دخول قواعد البيانات.

ومن الأمثلة على ذلك قانون " التجسُّس الصناعي "في الولايات المتحدة الأمريكية، وتطوير مظلة من الإجراءات الأمنية تُغطِّي المؤسسات الوطنية الأمريكية على اختلاف أنواعها وأنشطتها، وتنطبق مثل هذه الإجراءات وغيرها على البعض الآخر من الدول المُتقدِّمة.

1-4 عناصر الأمن الالكتروني.

إن أغراض أبحاث واستراتيجيات ووسائل أمن المعلومات – سواءً من الناحية التقنية أو الأدائية – وكذا هدف التدابير التشريعية في هذا الحقل، ضمان توفُّر العناصر التالية لأية معلومات يُراد توفير الحماية الكافية لها[14]:

1- **السرِّية أو الموثوقية:** وتعني التأكُّد من أن المعلومات لا تُكشف ولا يُطَّلع عليها من قبل أشخاصٍ غير مُخوَّلين بذلك.
2- **التكاملية وسلامة المحتوى:** التأكُّد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به، وبشكلٍ خاص لن يتم تدمير المحتوى أو تغيره أو العبث به في أية مرحلةٍ

من مراحل المعالجة أو التبادُل، سواءً في مرحلة التعامُل الداخلي مع المعلومـــات، أو عن طريق تدخُّلٍ غير مشروع.

3- **استمرارية توفُّر المعلومات أو الخدمة:** – التأكُّد من استمرار عمل النظام المعلوماتي، واستمرار القُدرة على التفاعُل مع المعلومات، وتقديم الخدمة لمواقع المعلوماتيـــة، وأن مُستخدِم المعلومات لن يتعرَّض إلى منع استخدامه لها أو دخوله إليها.

4- **عدم إنكار التصرُّف المرتبط بالمعلومات ممن قام به:** ويُقصد به ضمان عـــدم إنكـــار الشخص الذي قام بتصرُّفٍ ما مُتَّصل بالمعلومات أو مواقعها إنكار أنه هو الـــذي قـــام بهذا التصرُّف، بحيث تتوفَّر قُدرة إثبات أن تصرفاً ما قد تمَّ من شخصٍ ما فـــي وقـــتٍ معين.

تطال المخاطر والاعتداءات في بيئة المعلومات أربعة مواطن أساسية هي مكوناتٌ تكنولوجيا المعلومات و الاتصال في أحدث تجلِّياتها:

✓ **الأجهزة:** وهي كافة المعدات والأدوات المادية التي تتكوَّن منها النُظم، كالشاشات والطابعات ومُكوناتها الداخلية ووسائط التخزين المادية وغيرها؛

✓ **البرامـــــج:** وهي الأوامر المُرتَّبة في نسقٍ معين لإنجاز الأعمال، وهي إما مُستقلَّة عن النظام أو مُخزَّنة فيه؛

✓ **البيانات:** إنها الدم الحي للنُظم، وما سيكون محلاً لجرائم الحاسوب كما سنرى، وتشمل كافة البيانات المُدخَلة والمعلومات المُستخرَجة عقب معالجتها، وتمتدُّ بمعناها الواسع للبرمجيات المُخزَّنة داخل النُظم. والبيانات قد تكون في طور الإدخال أو الإخراج أو التخزين أو التبادُل بين النُظم عبر الشبكات، وقد تُخزَّن داخل النُظم أو على وسائط التخزين خارجه؛

✓ **الاتصـــالات:** – وتشمل شبكات الاتصال التي تربط الأجهزة التقنية بعضها بعض، محلِّياً ونطاقياً ودولياً، وتُتيح فُرصة اختراق النُظم عبرها. كما أنها بذاتها محلٌّ للاعتداء وموطنٌ من مواطن الخطر الحقيقي. ومحور الخطر، الإنسان، سواءً المُستخدِم أو الشخص المناط به مهامٌ تقنية معينة تتَّصل بالنظام. فإدراك هذا الشخص حدود صلاحياته، وإدراكه آليات التعامُل مع الخطر، وسلامة الرقابة على أنشطته في حدود احترام حقوقه القانونية، مسائل رئيسة يعنى بها نظام الأمن الشامل.

4-1 الرقابة الإدارية على أمن النظام المعلوماتي.

يمكن التغلُّب على معظم مخالفات الحواسيب من خلال التخطيط الإداري الجيِّد لأمن النظام، والذي يعمل على تحقيق أقصى منافع ممكنة. وينبغي أن يتضمَّن التخطيط والرقابة الإدارية على أمن النظام ما يلي[15]:

1- تحديد الأهداف والتي تُعتبر بمثابة معايير لتقييم أمن النظام فيما بعد، وتتمثَّل هذه الأهداف في حماية التجهيزات والبرامج البيئية ومخالفات الحواسيب؛

2- تقدير الاحتمالات والتكاليف المُرتبِطة بمخاطر أمن تشغيل البيانات؛ حيث تُسهم هذه التقديرات في اختيار الإجراءات الملائمة لأمن النظام؛

3- إعداد خطة تضمن مستوى مقبولاً من الأمن وبتكلفةٍ معقولة، وتصفُ هذه الخطة كافة الإجراءات الرقابية التي سيتمُّ تطبيقها وأهداف هذه الإجراءات. هذا وينبغي أن يتمَّ فحص الخطة والتصديق عليها قبل وضعها موضع التنفيذ؛

4- تحديد المسؤوليات عن أمن النظام؛

5- اختبار إجراءات الرقابة على أمن النظام، وذلك للتحقُّق من مدى فعاليتها في تحقيق أهدافها المرجوَّة؛ حيث أن هذا الاختبار يُؤكِّد على تحديد المسؤوليات بفهم الإجراءات وتنفيذها توظيف الأساليب الرقابية بصورةٍ ملائمة.

6- الاستنجاد بالوسائل التقنية، مثل حوائط النار، ...إلخ.

ثانيا:آليات توفير الأمن الالكتروني.

من الضروري أن تسير أي إستراتيجية موضوعة وفقا لرؤية شاملة للأهداف بعيدة المدى للجهة أو الهيئة.تمثل هده الرؤية الدافع للإستراتيجية والتي يجب أن تمد المؤسسة بهيكل عمل مرن و شامل يساعدها في تحقيق أهدافها الأكثر أهمية ومتطلبات العمل و الفوائد العائدة،بالإضافة إلى أي قرارات تكنولوجية مهمة يمكن أن تؤثر على العمل داخل المؤسسة[16].

2-1 المشكلات الخاصة بنُظم التشغيل الالكتروني للبيانات:

فيما يلي نستعرض المشكلات الخاصة بنُظم التشغيل الالكتروني:

1- إن التوسُّع في استخدام شبكات الحواسيب التي يمكن الاتصال بها عن بُعد، قد جعل من السهل إمكانية الولوج إلى البيانات والتعامُل معها؛ مما أدَّى إلى زيادة رُقعة جرائم الحواسيب؛ حيث يمكن لأي شخصٍ خارجي بمعرفته لكلمة السر الوصول للنظام، وارتكاب جرائمه؛ بحيث شكَّل هذا النوع من الجرائم عبئاً ثقيلاً على العديد من المؤسسات البريطانية والأمريكية، وتُرتكب معظم هذه الجرائم من خلال نظام المودم للشبكات؛

2- يصعُب إلى حدٍّ كبير نقل نظام وأساليب الأمن المُطبَّقة في بيئة الحواسيب الكبيرة إلى الحواسيب الصغيرة التي تُشكِّل شبكات الحواسيب؛ لذا فإن نظام وأساليب أمن شبكة الحواسيب في الوقت الحالي لا تُعدُّ كافية؛

3- قد أدَّى استخدام البريد الإلكتروني في تبادُل الرسائل بين الحواسيب في ظل استخدام نُظم الشبكات أو استخدام الصراف الآلي، أو نظام البنك التليفوني في شبكات البنوك، إلى زيادة فُرصة ارتكاب جرائم الحواسيب؛

4- قد ترتبط شبكة الحواسيب بعددٍ كبير من محطات العمل، والتي يتكوَّن كل منها من شاشة ولوحة مفاتيح ووسيلة للاتصال بالمُشغِّل المركزي[17]. وتُؤدِّي هذه المحطات إلى زيادة خطر الوصول غير المُصرَّح به لملفات البيانات والبرامج، مما يزيد من فُرص ارتكاب جرائم الحاسوب، ويرجع ذلك إلى صعوبة الرقابة السليمة على هذه المحطات؛

5- لقد أدَّى استخدام شبكات الحواسيب إلى خلق نُظم معلوماتٍ مُتكامِلة تُحقِّق مركزية البيانات؛ مما أتاح لمُرتكبي جرائم الحواسيب فُرصة الوصول إلى كافة ملفات بيانات وبرامج المؤسسة؛

6- إن تعقيد تدفُّق البيانات في ظل النُظم المُتكامِلة التي تَستخدِم شبكات الحواسيب، ومركزية البيانات، قد تجعل من الصعب على المدراء فهم تدفُّق البيانات، وهذا القصور في الفهم له عواقبه الوخيمة على الرقابة وتقييم الأداء؛

7- نُقص العاملين ذوي الخبرة في مجال التعامُل مع البرامج التي تُساعد على منع واكتشاف حالات التلاعُب وفيروسات الحواسيب، فضلاً عن عدم انتشار استخدام مثل

هذه البرامج في نُظم الشبكات؛

8- بالإضافة إلى أن الحاسوب الذي يعمل كخادمٍ للشبكة عرضةٌ للمخاطر نفسها التي تتعرَّض لها محطات العمل، فإن به مناطق إضافية يمكن اقتحامه من خلالها، حيث يمكن الوصول إليه من خلال الأسطوانات الثابتة أو المرنة؛

9- إن معظم الشبكات ليس لها أماكن مُستقلَّة مُغلَقة؛ مما يُسهِّل من الاتصال غير المُصرَّح به وارتكاب حالات التلاعب؛

10- من أهم المشكلات كذلك هو التنافُس بين الحواسيب بغرض الوصول للشبكة؛ لذا ينبغي أن تكون هناك خطةٌ لإدارة هذا التنافُس؛

11- غالباً ما تفتقر نُظم شبكات الحواسيب إلى التخصُّص وفصل المهام؛ وذلك لصغر مراكز التشغيل المحلِّية، كما يتولَّى الرقابة عليها المستفيدون، بما يفي عدم توفُّر مُقوِّمات النظام الجيِّد للرقابة الداخلية في ظل بيئة نُظم الشبكات؛

12- تعمل نُظم شبكات الحواسيب في ظل بيئةٍ غير رسمية؛ مما يُصعِّب الرقابة عليها؛ وبالتالي تتزايد فُرص ارتكاب جرائم الحاسوب.

إن مشاكل الفيروسات وعمليات القرصنة حفَّزت المؤسسات لأنْ تجد الأساليب التي تُمكِّنها من التعامُل مع هذه التحدِّيات بمنتهى الكفاءة، ومن بين هذه الأساليب نجد اختبار القرصنة الحميدة؛ حيث يقوم فريقٌ من الخبراء بإجراء اختبارٍ لحالة اعتداءٍ افتراضي على نظام المعلومات المُتعلِّق بالمؤسسة، ويعمل هذا الاختبار على كشف الثغرات الموجودة في الشفرات من جانب، ويُشخِّص نقاط الضعف في النُظم؛ التي يمكن أن تطرح الكثير من المشكلات الأمنية في الجانب الآخر. وبالتالي يُتيح للمؤسسة تحقيق تفهُّمٍ كامل بأداء عمليات الحماية من منظور القراصنة، ومنه تعزيز آليات التحكُّم والحماية[18].

إذن، هناك جانبٌ سلبي لاستخدام تكنولوجيا المعلومات والاتصالات، على المؤسسة أن تتجنَّبه بتطوير نُظم الحماية، وتحسيس كافة المُوظَّفين والعمال بهذه الجوانب، وقد يصل الأمر إلى وضع بعض الأشخاص المشكوك في ولائهم تحت المراقبة.

2-2 طبيعة التهديدات الحاسوبية.

من أهم الهجمات على شبكة الحواسيب أثناء تأدية العمل عن بُعد هي[19]:

1- المُقاطَعة: يتمُّ في تدمير موجودات النظام أو جعلها غير مُتوافِرة أو غير قابلة للاستخدام. مثالٌ على ذلك تدمير القرص الصلب، وقطع الاتصال، أو تعطيل نظام إدارة الملف.

2- الإيقاف أو التدفُّق[20]: طرفٌ غير صالح يتمكَّن من الولوج إلى موجودات النظام، ويمكن لهذا الطرف أن يكون شخصاً أو برنامجاً أو جهاز حاسوب. مثل: سرقة الأسلاك لالتقاط البيانات في الشبكة، والنسخ غير المُصرَّح به للملفات أو البرامج.

3- التعديل: فريقٌ لا يملك الصلاحية ولا يحصُل فقط على الولوج، وإنما يتلاعب بالموجودات، وهذا هجومٌ على النزاهة. مثل: تغيير القيم في ملف بيانات وتعديل برنامج؛ بحيث يُؤدِّي عمله بشكلٍ مختلف ويُغيِّر فحوى الرسائل المُرسَلة في الشبكة.

4- الفَبرَكة: يقوم فريقٌ لا يملك تصريحاً بإدخال موادٍ مُزوَّرة في النظام. هذا يُعدُّ هجوماً على الموثوقية، ومثال ذلك إدخال رسائل زائفة إلى شبكة، أو إضافة سجلاتٍ إلى ملفٍ ما.كذلك من أهم التهديدات هي المراقبة والتنصت و كذا اعتراض البيانات.

2-3 أدوات الحماية لنظم التشغيل الالكتروني .

تشتمل نظم الحماية على ما يلي :

1- حماية المعلومات:

تتم حماية المعلومات من خلال :

- كلمات السر الآمنة، إذ ينبغي اختيار كلمات السر بشكلٍ دقيق: ينبغي أن تكون طويلة، صعبة لا يمكن للغير معرفتها أو تكهُّنها، تحتوي على مزيجٍ من الأرقام والأحرف، ومن أهم الأمور أن لا تكون مستخدمةً كثيراً، إذ يمكن القراصنة تشغيل برنامجٍ قادر على معرفتها في هذه الحالة.
- عدم الثقة بأجهزة حاسوبٍ غير معروفة؛ إذ أن الكثير منها يتضمَّن مثل هذه البرامج؛
- استخدام برنامجٍ خاص، وهو الجدران النارية، فرغم أن فعاليته هي من خلال جهاز الـ Hardware، إلا أن الـ Windows يُقدِّم الجدران النارية كبرنامج (Software) يُقدِّم

بعض الحماية، وخصوصاً الـ (Shared files)؛ إذ لا يمكن اقتحام الجهاز ما لم يسمح المُستخدِم بذلك، كما يوجد عددٌ من البرامج التي تُؤمِّن حماية Firewall.

2- خدمة التحقُّق من هوية المُستخدِم المُتَّصل عن بُعد (RADIUS):

تُدعّم أغلب أجهزة معدات الاستخدام عن بُعد خادم RADIUS في أجهزة الخادم للاتصال عن بُعد للتحقُّق من هوية المُستخدِم والذي يُتيح كذلك تبسيط إدارة الهوية من خلال قاعدة بياناتٍ مركزية لحقوق الاستخدام. هذا الخادم له القُدرة على التحقُّق من هوية المُستخدِمين الذين يتَّصلون بالمؤسسة، من خلال خادمات الاستخدام عن بُعد المُتعدِّدة والمُتفرِّقة، من خلال قاعدة بياناتٍ مُشترَكة تحوي مستويات صلاحية مختلفة؛ وبناءً على البيانات الموجودة في قاعدة البيانات هذه يتمُّ التأكُّد من هوية وبيانات المُستخدِمين.

3- البرمجيات المضادة للاعتداءات الالكترونية:

تعدُ البرمجيات المضادة للاعتداءات الالكترونية أمراً أساسياً، وتلعب الدور الرئيسي في حماية الحواسيب و الشبكات؛ فعلى كل جهاز حاسوب أن يحتوي على أحد هذه البرامج. ومن هذه البرامج الفعالة: Norton antivirus, PcCiline, Macafee, Kasperki...etc. [21] وقد أصبح يطلق عليها البرامج المضادة للاعتداءات الالكترونية لمحاربة ما أصبح يصطلح على تسميته بالبرامج الخبيثة وكذلك نظرا لتطور أشكال المخاطر الالكترونية؛بحيث يعتبر حاليا الفيروس أبسط أنواعها.

إن البرنامج المضاد للاعتداءات الالكترونية قادرٌ أن يمنع أي برنامج خطر أو برنامج خبيث من اقتحام الأجهزة وتدميرها، وينبغي على المُستخدِمين تحديثها دائماً (updated) لحماية الحاسوب من أحدث هده البرامج التي يتمَّ إطلاقها باستمرار؛ لذا من المُحبَّذ وضع البرنامج ليُحدِّث نفسه يومياً عبر الإنترنت.

4-التوقيع الإلكتروني:

هو عبارة عن ملف رقمي صغير مكون من بعض الحروف والأرقام والرموز الإلكترونية تصدر عن إحدى الجهات المتخصصة والمعترف بها حكوميا ودوليا ويطلق عليها الشهادة الرقمية Digital Certificate وتخزن فيها جميع معلومات الشخص وتاريخ ورقم الشهادة ومصدرها، وعادة يسلم مع هذه الشهادة مفتاحان أحدهما عام والآخر خاص،

أما المفتاح العام فهو الذي ينشر في الدليل لكل الناس والمفتاح الخاص هو توقيع الشخص الإلكتروني[22]،

- هي ليست كما يعتقد البعض بأنها ما هي إلا توقيعٌ باليد ولكنها مُصوَّرةٌ رقمياً، ولو كانت كذلك لأصبح بإمكان أي شخصٍ أن يُصوِّر أي توقيعٍ ويَدَّعي بأنه صاحب التوقيع؛
- هي شهادةٌ رقمية تصدُر عن أحد الهيئات المُستقلَّة تُميِّز كل مُستخدِم؛
- يمكن استخدامها في إرسال أي وثيقةٍ أو عقدٍ تجاري أو تعهُّدٍ أو إقرارٍ، وتُعتبر قانونية في القانون الأمريكي الآن وقريباً في عدة دولٍ أخرى؛
- الوثائق والعقود التجارية المُذيَّلة بالتوقيع الإلكتروني لا تحتاج إلى مصادقةٍ من كاتب عدل أو أي جهةٍ أخرى؛ لأنها صادرة أساساً من جهةٍ مُعترَف بها.

2-6 إستراتيجية الأمن الالكتروني وكيفية بنائها.

إن إستراتيجية الأمن الالكتروني، أو سياسة الأمن الالكتروني هي مجموعة القواعد التي يُطبِّقها الأشخاص لدى التعامُل مع التقنية ومع المعلومات والوسائط الالكترونية داخل المؤسسة، وتتَّصل بشؤون الولوج إلى قواعد البيانات والمعلومات والعمل على نُظمها وإدارتها.

تهدف إستراتيجية الأمن الالكتروني إلى ما يلي:

- تعريف المُستخدِمين والإداريين بالتزاماتهم وواجباتهم المطلوبة لحماية نُظم الحاسوب والشبكات، وكذلك حماية المعلومات بكافة أشكالها، وفي مراحل إدخالها ومعالجتها وخزنها ونقلها وإعادة استرجاعها؛
- كما تهدف الإستراتيجية إلى تحديد المسؤولية الإلكترونية التي يتمُّ من خلالها تحقيق وتنفيذ الواجبات المُحدَّدة على كل من له علاقةٌ بالمعلومات ونُظمها وتحديد المسؤوليات عند حصول الخطر وحصر الأخطاء ومن ثم إيجاد الحلول لها ؛
- بيان الإجراءات المُتَّبعة لتجاوُز التهديدات والمخاطر والتعامُل معها والجهات المُناط بها القيام بذلك. لدى إعداد أية إستراتيجية بشأن الأمن الالكتروني، ولكي تكون هذه الإستراتيجية فاعلة ومنتجة وهادفة لا بد أن يُساهِم في إعدادها وتفهُّمها وتقبُّلها وتنفيذها مختلف مستويات الوظيفة في المؤسسة الواحدة، إضافةً إلى حاجتها إلى التعاوُن والدعم الكامل من الكافة. من هنا فإن المعنيين بإعداد سياسة الأمن الالكتروني يتوزَّعون إلى

مراتب وجهاتٍ عديدة داخل المؤسسة. لكن بوجهٍ عام، تشمل مسئولي أمن الموقع ومديري الشبكات، ومُوظِّفي وحدة الحاسوب، ومديري الوحدات المختلفة في المؤسسة، كوحدة الأعمال والتسويق والبحث وغيرها. وتشمل أيضاً فريق الاستجابة للحوادث والأعطال، ومُمثِّلي مجموعات المُستخدِمين ومستويات الإدارة العليا، إلى جانب الإدارة القانونية.

وتضمُّ إستراتيجية الأمن الالكتروني أيضاً إستراتيجية الاشتراكات التي تُحدِّد سياسة المؤسسة بشأن اشتراكات الغير في شبكتها أو نُظمها مثلا استراتيجيات العلم ضمن نظم الشبكات الخارجية(Extranet)، وكذلك استراتيجيات التعامُل مع المخاطر والأخطاء بحيث تُحدِّد ماهية المخاطر وإجراءات إبلاغ عنها، والتعامُل معها، والجهات المسئولة عن التعامُل مع هذه المخاطر.

زيادة على ما تم إدراجه سابقا يمكن إدراج بعض التدابير التي نراها ضرورية لتوفير الأمن الالكتروني في المؤسسة وخاصة أثناء تأدية مهمات الاتصالات عن بعد باستخدام الحاسوب

1- التحديثات:بحيث يتم المحافظة على تحديث جميع البرامج بما في ذلك أحدث نسخة من برنامج التشغيل الذي تستخدمه نظم العمل عن بعد. ومن الأحسن استخدام التحديث التلقائي الذي يقوم بالبحث يومياً عن التحديثات عند بدء تشغيل الجهاز.

2- فحص مواطن الضعف في نظام العمل عن بعد والكشف عنها ومحاولة إصلاحها؛

3- طريقة فعالة لمراقبة الحركة المرورية عبر الشبكة باستخدام أحد برامج مراقبة بيانات الشبكة، حيث يتم من خلاله تجميع البيانات الداخلة والخارجة، وهي طريقة ممكن أن تكون مفيدة في الكشف عن محاولات التسلل عبر الشبكة، وكذلك يمكن استخدامها لتحليل مشاكل الشبكة وتصفية وحجب المحتوى المشكوك فيه من الدخول إلى الشبكة.

4- التشفير وهو ترميز البيانات كي يتعذر قراءتها من أي شخص ليس لديه كلمة مرور لفك شفرة تلك البيانات. ويقوم التشفير بمعالجة البيانات باستخدام عمليات رياضية غير قابلة

للعكس. ويجعل تشفير المعلومات في نظم العمل عن بعد غير قابلة للقراءة من قبل أي شخص يستطيع أن يتسلل خلسة إلى النظام دون إذن.

5- التعريف:بحيث يكون للأجهزة ومديرو الشبكات أسماء تعريف افتراضية في النظام، ومن السهل كثيراً على الهاكر إيجاد هذه الأسماء، ومن ثم عمل كلمات مرور واسم مستخدم شخصي لك من خلال تعديل أسماء التعريف الافتراضية في النظام. لذا ننصح بإعطاء الأجهزة التي تربط أسماء لا تكشف عن هوية صاحبها أو أماكنها، ومثال ذلك بدلاً من استخدام العنوان الفعلي للمستخدم مثل اسم المبنى أو اسم الشركة كأسماء للأجهزة، يمكن استخدام أسماء مختلفة مثل "الجبل "Mountain أو "جهازي My Device".

6- ترشيح العناوينMAC filtering :يعرف عنوان (MAC) كذلك بأنه العنوان المادي، وهو معرف فريد لكل جهاز في الشبكة .ويعني مصطلح ترشيح العناوين أن نقوم يدوياً بإدخال قائمة بالعناوين الموجودة في الشبكة المحلية وتقوم بإعداد الموجه لديك (router) ليسمح فقط بتوصيل هذه العنوانين المحددة عبر الشبكة اللاسلكية.

خاتمة:

تعنى المؤسسة في ظل استخدامها الموسع لتكنولوجيا المعلومات والاتصال بجملة من المخاطر الالكترونية ،وعليه تلتزم هذه الأخيرة بوضع استراتيجيات محينة ومتغيرة على الدوام لضمان عدم اختراق قواعدها المعلوماتية و الالكترونية،وهذا لن يتأتى في نظرنا إلا بوضع نظم حديثة للإنذار عن وجود أي اختراق الكتروني ووضع نظم حديثة للتنبؤ بالتغيرات الحاصلة في مجال الاختراقات الالكترونية و الفيروسات وغيرها وضمان تحديث البرمجيات المساعدة على محاربتها بصفة مستمرة .

كما يمكن للمؤسسة أن تستفيد من الخبرات والاستشارات التي توفرها نظيراتها من المؤسسات و المكاتب المتخصصة في محاربة أشكال ما أصبح يطلق عليه بالجريمة الالكترونية ،وعليها بتوفير كامل الشروط الضرورية لتأهيل كوادرها البشرية لاسيما المتخصصة في مجال المعلوماتية من أجل أن تقف كحجر عثرة أمام أي محاولة لتهديد أمن مؤسستهم وأن تأخذ بعين الاعتبار التجارب السابقة .

إثبات صحة الفرضيات:

إن هذا المقال المتواضع قد أثبت لنا من خلال اطلاعنا على المراجع و المواقع المستخدمة فيه صحة الفرضيات التي تم تناولها في مقدمة البحث.

قائمة المراجع:

الكتب:

1-إيمان السامرائي، هيثم الزعبي، نظم المعلومات الإدارية، دار الصفاء للنشر والتوزيع، عمان، الأردن، ط1، 2004،

2-علاء عبد الرزاق محمد السالمي، شبكات الإدارة الإلكترونية، دار وائل للنشر، عمـــان، الأردن، ط1، 2005.

3-سمير كامل محمد، أساسيات المراجعة في ظل بيئة التشغيل الإلكتروني للبيانات، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 1999.

4-جلوريا ايقانز، الحكومة الالكترونية، ترجمةدار الفاروق للنشـــر والتوزيـــع، القـــاهرة، مصر،2005 .

5- زياد محمد الشرمان، مقدمة في نظم المعلومات الإدارية، دار الصفاء للنشر والتوزيع، عمان، الأردن، 2004.

6- وليد أبو سعد،،امن المعلومات،الموسوعة العربية للكمبيوتر،سلسلة الدورات التعليمية الالكترونية،2005.

المقالات:

غادة سعيد سمير، « مبادئ أمن الشبكات »، www.arabcin.net.

المواقع الالكترونية:

3rgob.org/af/uploads/
www.aticm.org.eg
publications.ksu.edu.sa
www.internet.gov.sa
www. ITEP.CO.AE
news.maktoob.com
http://ar.wikipedia.org/wiki
http://www.arabic-military.com/
http://www.egovconcepts.com

(1) 3rgob.org/af/uploads/11-07/d8c963fe24.doc، تاريخ التحميل: 9 سبتمبر 2007.

(2) http://ar.wikipedia.org/wiki تاريخ التحميل 2009/10/11

(3) http://www.arabic-military.com/montada-f35/topic-t8513.htm تاريخ التحميل 2009/10/11

(4) Information Security.

(5) http://ar.wikipedia.org/wiki تاريخ التحميل 2009/10/11

(6) « الاستراتيجية العربية العامة لتكنولوجيا الاتصالات والمعلومات بناء مجتمع المعلومات 2007-2012 »، http:/www.aticm.org.eg/admin/Farek_pal/Arab%20ICT%20Strategy-11-2-2007.doc، تاريخ التحميل: 9 سبتمبر 2007.

(7) زياد محمد الشرمان، مقدمة في نظم المعلومات الإدارية، دار الصفاء للنشر والتوزيع، عمان، الأردن، 2004، ص ص 19- 20.

(8) إيمان السامرائي، هيثم الزعبي، نظم المعلومات الإدارية، دار الصفاء للنشر والتوزيع، عمان، الأردن، ط1، 2004، ص 28.

(9) publications.ksu.edu.sa/IT%20Papers/Information%20Security/IT%20Sec.doc، تاريخ التحميل: 5 مارس 2008.بتصرف.

(10) زياد محمد الشرمان، مرجع سبق ذكره، ص 20.

(11) http://www.internet.gov.sa/learn-the-web-ar/guides-ar/information-security-and-the-internet-ar.

(12) وليد أبو سعد،،امن المعلومات،الموسوعة العربية للكمبيوتر،سلسلة الدورات التعليمية الالكترونية،2005،ص6.

13 http://www.egovconcepts.com/channels/security.html تاريخ التحميل :2009/07/08.

(14) publications.ksu.edu.sa/IT%20Papers/Information%20Security/IT%20Sec.doc، تاريخ التحميل: 5 مارس 2008..

(15) سمير كامل محمد، أساسيات المراجعة في ظل بيئة التشغيل الإلكتروني للبيانات، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 1999، ص 95.

(16) جلوريا ايقانز،الحكومة الالكترونية،ترجمة،دار الفاروق للنشر والتوزيع،القاهرة،مصر،2005،ص 204.

(17) Central Processor.

(18) www. ITEP.CO.AE/it portal/Arabic /content / news full. Asp.، تاريخ التحميل: 12 فيفري 2008.

(19) غادة سعيد سمير، « مبادئ أمن الشبكات »، www.arabcin.net، تاريخ التحميل:11 أكتوبر 2007.

(20) Interception.

(21) علاء عبد الرزاق محمد السالمي، شبكات الإدارة الإلكترونية، دار وائل للنشـــر، عمـــان، الأردن، ط1، 2005.ص 289.بتصرف

(22) http://news.maktoob.com/article/620364/