

الحلول الحديثة لأمن المعلومات لمواجهة المخاطر الالكترونية

Modern solutions for information security to deal with electronic risks

Les solutions modernes pour la sécurité de l'information
face aux risques électroniques

الطالبة/ منصور أحلام *

تاريخ قبول النشر: 2018/06/20

تاريخ الاستلام: 2017/12/19

Abstract:

With the great developments taking place in the modern business environment and the increasing competition among the various economic institutions due to the huge and accelerating technological developments, it is necessary for the economic institution to control these modern technologies, especially the internet. The Internet has provided many advantages to the institution, but it carries a number of risks related primarily to information security, hence the study to identify the main electronic risks faced by the institution and how to address them.

Key words: Internet Security, Information Security, Electronic Risk, Security Solutions.

* طالبة دكتوراه علوم – جامعة الجزائر 3

ملخص:

مع التطورات الكبيرة التي تشهدها بيئة الأعمال المعاصرة واشتداد المنافسة بين مختلف المؤسسات الاقتصادية بسبب التطورات التكنولوجية الضخمة والمتسارعة، أصبح من الضروري بالسبب للمؤسسة الاقتصادية التحكم في هذه التكنولوجيات الحديثة وخاصة الإنترنت. إن الإنترنت قد وفرت مزايا عديدة للمؤسسة إلا أنها تحمل عددا من المخاطر المتعلقة أساسا بأمن المعلومات، ومن هنا جاءت هذه الدراسة للتعرف على أهم مخاطر الإعتداءات الإلكترونية التي تعترض المؤسسة وكيفية مواجهتها.

الكلمات المفتاحية: الإنترنت، أمن المعلومات، مخاطر الإعتداءات الإلكترونية، الحلول الأمنية.

Abstract:

Avec les grands développements dans l'environnement des affaires modernes et la concurrence croissante entre les différentes institutions économiques en raison de l'évolution technologique énorme et en accélération, il est nécessaire pour l'institution économique de contrôler ces technologies modernes, en particulier l'Internet. L'Internet a apporté de nombreux avantages à l'institution, mais il comporte un certain nombre de risques liés principalement à la sécurité de l'information, d'où l'étude visant à identifier les principaux risques cyber-attaques électroniques auxquels l'établissement est confronté et à y remédier.

Mots clés: Sécurité Internet, Sécurité de l'information, Risque cyber-attaques électronique, Solutions de sécurité.

مخطط المقال:

مقدمة

1) مدخل لأمن ومخاطر المعلومات والإعتداءات الإلكترونية

1-1) أمن المعلومات والمخاطر التي تواجهه

2-1) الإعتداءات الإلكترونية

2) الأشكال المختلفة للإعتداءات الإلكترونية

1-2) أساليب الحماية الفيزيائية

2-2) أساليب الحماية المنطقية

خاتمة

مقدمة:

أدخل الحاسوب والانترنت خدمات وتسهيلات ومعارف، بل ومصطلحات جديدة فقد أعطيا عالم الجريمة أبعادا جديدة، فصار من الممكن ارتكاب جريمة اختلاس أو سرقة، أو تزوير عن بعد، وأصبحت وسائل الأمن والحماية المحسوسة من حراسة وصناديق حفظ وأماكن تخزين لا تكفي وحدها لحماية المعلومات من اللصوص. وظهر مصطلح Cybercrime الذي يعنى الجرائم التي ترتكب باستخدام الحاسوب وشبكة الانترنت. فالتقدم التكنولوجي الكبير، وتطور وسائل التواصل والاتصال المتنوعة، وانفتاح العالم على بعضه، واعتماده على إرسال شتى أنواع البيانات خلال الشبكات، كل ذلك أدى إلى إحداث مخطر على تسرب هذه البيانات، ووصولها للأشخاص الخاطئين، أو المنافسين، وبالتالي أصبحت الحاجة الملحة للحفاظ على أمن المعلومات. وهذا ما يبين الأهمية الكبيرة التي أصبح يحظى بها موضوع أمن المعلومات الالكترونية.

انطلاقا مما سبق يمكننا صياغة الإشكالية التالي: ما المقصود بأمن المعلومات الالكترونية، وماهي أهم المخاطر الالكترونية التي تهدد أمن معلومات المؤسسة؟ وكيف يمكن مواجهتها؟ ومحاولة للإجابة على الإشكالية السابقة، يمكن لنا صياغة الفرضيات التالية:

- أمن المعلومات الالكترونية هو مجموعة من الإجراءات المتخذة لحماية المعلومات؛
- تعتبر البرامج الخبيثة والقرصنة من أهم المخاطر الالكترونية التي تهدد أمن المعلومات؛
- ويمكن للمؤسسة مواجهة المخاطر الالكترونية عن طريق توفير مجموعة من الأنظمة وبرامج الحماية.

1) مدخل لأمن ومخاطر المعلومات والإعتداءات الإلكترونية:

مع تعميم الرقمية، وحركة انتقال المعلومات، واعتماد الأفراد والمؤسسات والحكومات على تكنولوجيا المعلومات والاتصالات، وانخراط جميع القطاعات، العلمية، والاجتماعية، والأكاديمية، والاقتصادية والحكومية في مجتمع المعلومات، والاتصال الشبكي بين الأنظمة، وبروز الوسائط المتعددة واستعمالها بشكل مكثف، نجد أنفسنا أمام حاجة ملحة إلى الأمن في الفضاء الرقمي. ذلك أن الأمن هو شرط أساسي من شروط تحقق الثقة. وتعتبر هذه الأخيرة، الهدف الأول الذي تسعى إليه الحكومات، التي تسعى إلى الإفادة من إمكانيات تكنولوجيا المعلومات والاتصالات في دعم التنمية والتطور والتجارة والاقتصاد. وتكفي مراجعة النصوص القانونية التي أقرت، سواء في دول الاتحاد الأوروبي، أو الولايات المتحدة الأمريكية، وغيرها، لملاحظة تشديدها على دعم الثقة في تكنولوجيا المعلومات والاتصالات، تحقيقاً لازدهار التجارة الإلكترونية، والمبادلات الاقتصادية¹.

1-1) أمن المعلومات والمخاطر التي تواجهه:

مع تطور العلم والتكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة، أو ما يسمى نقل البيانات عبر الشبكة من موقع لآخر، أصبح النظر إلى أمن تلك البيانات والمعلومات مهماً للغاية عبر أمن المعلومات الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها بالسرقة أو التعديل، وذلك من خلال توفير الأدوات والوسائل اللازمة لحماية المعلومات من المخاطر الداخلية أو الخارجية، واتباع المعايير وإجراءات الاتصالات المناسبة؛ لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين، ولضمان أصالة وصحة تلك الاتصالات².

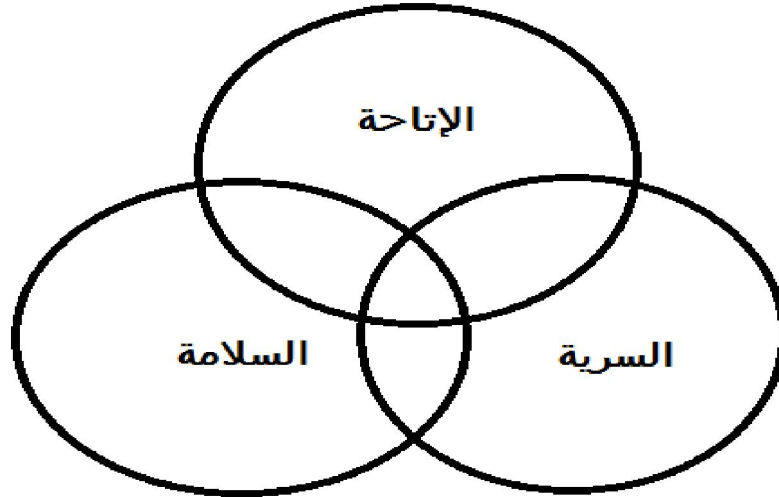
- مفهوم أمن المعلومات:

تتعدد تعاريف أمن المعلومات من مؤلف لآخر ووفق التطور التي وصلت إليه المعلوماتية، ومنها نلخص على أنها:

- مجموعة من التدابير والإجراءات التي تتخذها المؤسسة بهدف حماية أصولها الإلكترونية المتمثلة في المعلومات من كل استخدام غير مرخص كالتخريب والتغيير والسرقة والتلف

- والضياح والاستخدام غير المرخص وغير القانوني وذلك بالاعتماد على وسائل تقنية وأدوات تضمن لها الوصول إلى الحماية³؛
- القدرة على التفاعل وحماية المعلومات وقواعد البيانات من العبث والتدمير والكشف عن أي مخاطر تتعرض لها ومحاولة معالجتها بالسرعة والدقة الممكنتين ويعد من السياسات الأمنية التي يجب على المؤسسة أن تتبناها من خلال أفضل الممارسات الأمنية وأحدث التقنيات للحفاظ عليها من الاختراق غير المباشر من قبل غير المخولين ومهاجمة البيانات والمعلومات المخزنة في الحاسوب لإلحاق الضرر بالمؤسسة⁴؛
 - ومن زوايا أكاديمية، تقنية، وقانونية⁵ :
 - ✓ العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها-من زاوية أكاديمية-؛
 - ✓ الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من المخاطر الداخلية والخارجية-من زاوية تقنية-؛
 - ✓ ومحل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم الكمبيوتر والإنترنت) -من زاوية قانونية-.
- ويمكننا القول أن أمن المعلومات هو مجموعة من الاحتياطات التي تتخذها المؤسسة لحماية أنظمة معلوماتها عبر مجموعة من الوسائل الفيزيائية كتأمين أجهزة المؤسسة المادية من التلف أو المنطقية والمتمثلة في مجموعة من برامج الحماية التي تجنب المؤسسة تعرض معلوماتها للسرقة أو القرصنة أو تغيير المحتوى".
- ولكي يكون أمن المعلومات فعالا يجب أن تتوفر فيه ثلاثة عناصر أساسية، تتمثل في⁶ :
1. **الإتاحة**: هو ضمان إمكانية الوصول إلى البيانات (يمكن قراءتها والبحث فيها)؛
 2. **السلامة**: تضمن أن المعلومات لا تغير جوهرها أو شكلها أثناء النقل أو المعالجة أو التخزين، وبشكل عام، هو ضمان أن المعلومات "صحيحة" (بمعنى "غير مشوهة" من قبل طرف ثالث)، لذلك نسعى إلى التأكد من أن المعلومات واضحة في دقتها وكذلك في مجملها؛
 3. **السرية**: هي حقيقة أن المعلومات يتم قراءتها والوصول إليها فقط من قبل أولئك الذين لديهم حق الوصول.
- والشكل التالي يوضح هذه العناصر :

الشكل 01 - عناصر أمن المعلومات

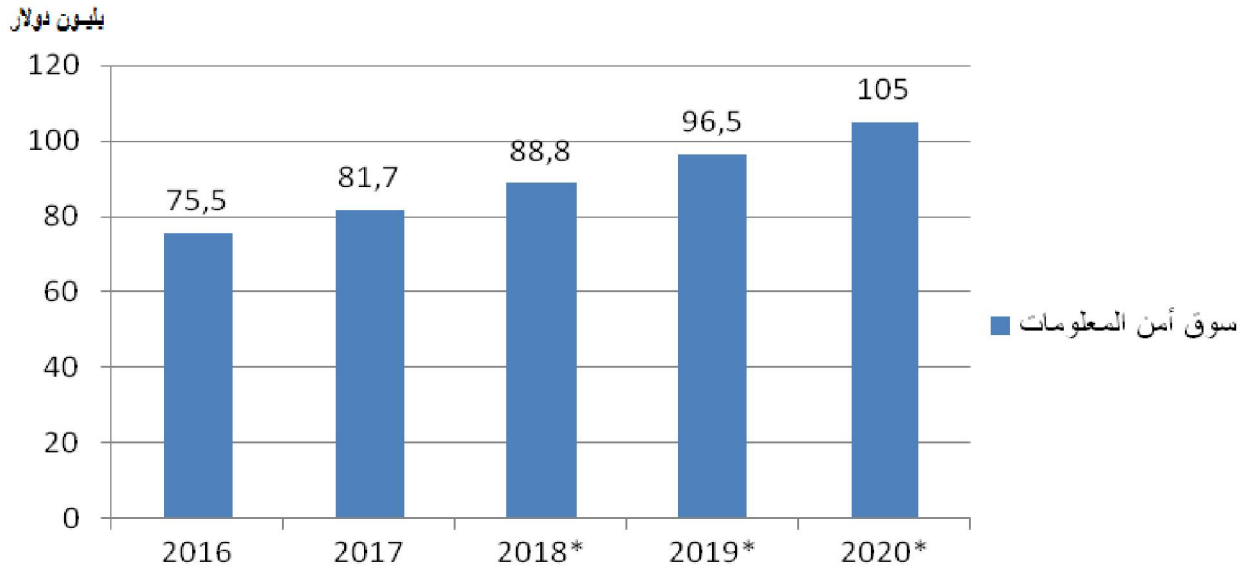


المصدر: DORIGNY Mickael, Qu'est ce que la sécurité de l'information, 21/10/2016, <https://www.information-security.fr/quest-ce-que-la-securite-de-linformation/>

- بالإضافة إلى معايير الإتاحة والسلامة والسرية، تم إضافة عنصرين جديدين، لتصبح خمسة⁷:
4. **موثوقية البيانات:** وتعني التحقق من هوية المستخدم، أي أن الشخص أو الجهة المتعامل معها هي ذاتها دون لبس أو غموض؛
 5. **وعدم الإنكار:** ويعني القدرة على ضمان عدم إنكار الطرف المتعامل معه لوقوع المعاملة والنتائج المترتبة عنها، فهي تتعلق بمسؤولية الشخص اتجاه الفعل الذي قد يكون ارسال رسالة أو أي فعل آخر.

ونظرا للأهمية التي أصبح يحظى بها موضوع أمن المعلومات، قامت عدة مؤسسات بالاستثمار في سوق أمن المعلومات من خلال مختلف المعدات والأجهزة والبرمجيات المضادة للاعتداءات الإلكترونية، وهذا ما يوضحه الشكل التالي:

الشكل 02 - حجم سوق أمن المعلومات من 2016 إلى 2020*



Statistics, 08/04/2018,

المصدر:

<https://www.statista.com/statistics/640141/worldwide-information-security-market-size/>

من الملاحظ من خلال الشكل أعلاه، الازدهار الكبير الذي يعرفه سوق أمن المعلومات حيث انتقل حجمه من 75.5 بليون دولار سنة 2016 إلى 81.7 بليون دولار سنة 2017، ويتوقع أن يصل حجمه إلى 88.8 بليون دولار سنة 2018 وإلى 96.5 بليون دولار سنة 2019 ليصل إلى 105 بليون دولار سنة 2020، وهذا راجع إلى تزايد استعمال الانترنت من طرف المؤسسات والحكومات والأفراد وارتفاع مستوى المخاطر والتهديدات الرقمية وبالتالي أصبحت الحاجة لتأمين المعلومات أمرا ضروريا.

- المخاطر التي تواجه أمن أنظمة المعلومات:

تكون الأنواع الكبيرة من البيانات عند تخزينها بشكل الكتروني عرضة لأنواع جديدة من التهديدات أكثر مما لو كانت موجودة بشكل يدوي، فالاتصالات المتقدمة وبرمجيات الحاسوب قد وسعت

* الأرقام المتوقعة.

من هذا التعرض للمخطر. إذ يمكن ربط نظم المعلومات في مواقع مختلفة من خلال شبكات الاتصالات، والإمكانية لوصول غير المخول أو سوء الاستخدام أو الاحتيال إذ أنها غير محدودة بموقع واحد ولكن يمكن أن تحدث في أي نقطة وصول في الشبكة. ووفقا لذلك، يمكن تصنيف المخاطر المحتملة التي يمكن أن تتعرض لها نظم المعلومات بالآتي⁸:

- **المخاطر البشرية:**
وهي التي يمكن أن تحدث خلال تصميم التجهيزات أو نظم المعلومات أو أثناء عمليات البرمجة أو الاختبار أو التجميع للبيانات وأثناء إدخالها إلى النظام، أو في عمليات تحديد الصلاحيات للمستخدمين.
- **المخاطر البيئية:**
تشمل الزلازل والعواصف والفيضانات والأعاصير والمشاكل المتعلقة بأعطال التيار الكهربائي والحرائق فضلا عن المشاكل القائمة عن تعطل أنظمة التكييف والتبريد وغيرها ودرجات الحرارة والرطوبة كلها تؤدي إلى توقف هذه التجهيزات لفترات طويلة نسبياً لإجراء الإصلاحات اللازمة واسترداد البرمجيات وقواعد البيانات.
- **ومخاطر الجرائم المحوسبة:**
تمثل تحدياً كبيراً لإدارة نظم المعلومات لما تسببه من خسارة كبيرة من خلال الاستخدام والوصول، التعديل، التدمير غير المفوض للماديات والبرمجيات أو البيانات والموارد الشبكية، فضلا عن النشر والنسخ غير المفوض للمعلومات وحرمان المستفيد النهائي من الوصول إلى ماديته وبرمجياته أو بياناته، وقد تكون جريمة الحاسوب بريئة نسبياً مثل الاستخدام غير المفوض للحاسبات لأغراض شخصية، أو تكون خطرة كاستخدام الحاسبات لإرسال موجودات المؤسسة الحالية لحساب مؤسسات أخرى، ومنها فيروسات الحاسوب*، القرصنة**، وجرائم الفضاء الرقمي.
- وتتزايد مخاطر التقنيات الحديثة على حماية الخصوصية، كتقنيات رقابة (كاميرات الفيديو) وبطاقات الهوية الإلكترونية، قواعد البيانات الشخصية، وسائل رقابة واعتراض البريد والاتصالات

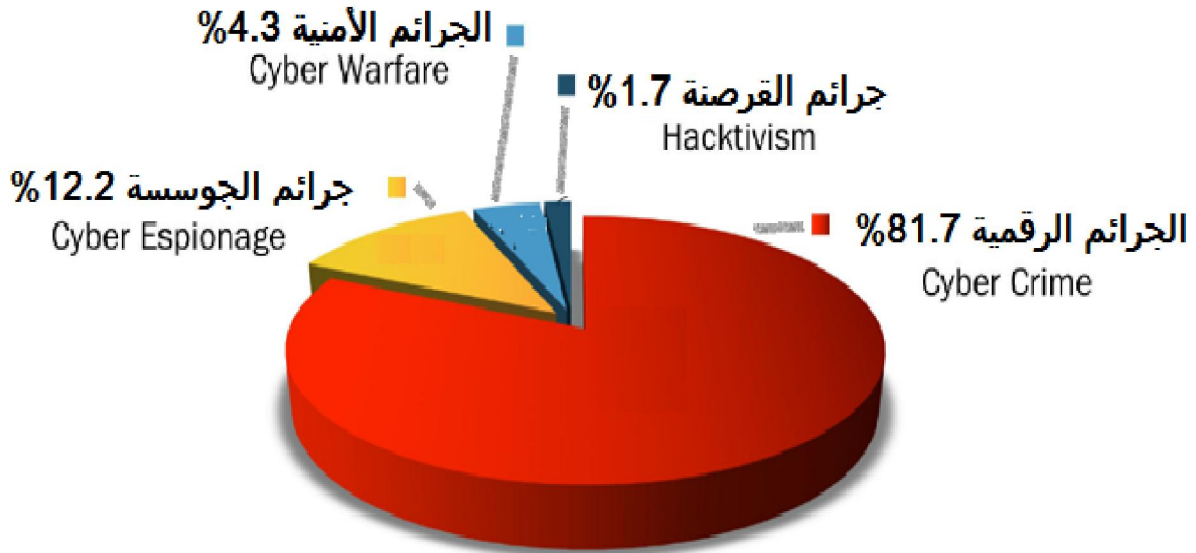
* فيروسات الحاسوب هي عبارة عن برمجيات مستقلة تقوم بتحميل نفسها ضمن برمجيات الحاسوب ونسخ نفسها بشكل متكرر وبدون معرفة المستفيد، والعديد من هذه الفيروسات يمكن أن تنتشر من نظام إلى آخر أو تستقر في ذاكرة نظام ما وتقوم بتدمير برامج وبيانات معينة.

** القرصنة هي اختراق الأجهزة بدون عناء وبمجرد إنزال إحدى برامج القرصنة إذ المقصود بالقرصنة هو سرقة المعلومات من برامج وبيانات بصورة غير شرعية وهي مخزونة في دائرة الحاسوب أو نسخ برامج معلوماتية بصورة غير قانونية ويتم ذلك بالحصول على كلمة السر أو بواسطة التقاط موجات الكهرومغناطيسية بحاسبة خاصة والهدف من ذلك هو سرقة الأسرار والمعلومات التجارية أو التسويقية أو التعرف على حسابات المؤسسات والتلاعب بقيود المصارف والمؤسسات المالية أو الكشف عن أسرار صناعية لتصميم المنتجات وإعادة تصنيفها دون إجازة قانونية.

إذ يمكن استرجاع كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل المؤسسات والدوائر والوكالات الخاصة والحكومية، ونقل المعلومات المؤتمتة في قاعدة البيانات عبر البلد في ثوان وبتكاليف منخفضة نسبيا إذ أن ذلك يكشف إلى أي مدى يمكن أن يكون التهديد للقضاء الرقمي. فضلا عن الكوارث والفيروسات والخروقات الأمنية لأنظمة المعلومات هناك أيضا تخلف البرمجيات والبيانات الناقصة والتي تسبب تهديدا دائما لنظم المعلومات مسببة خسائر لا مثيل لها في الإنتاجية والخطأ غير المكتشف في برمجيات إئتمان المؤسسة أو البيانات المالية الخاطئة يمكن أن ينتج عنه خسائر بملايين الدولارات فضلا عن الأعطال والأخطاء في البرمجيات وضعف البيانات كمدخلات.

والشكل التالي يوضح أنواع الجرائم المحوسبة التي تمت على مستوى العالم شهر جانفي 2018:

الشكل 03- أنواع الجرائم المحوسبة (جانفي 2018)



February 2018 Cyber Attacks Statistics, 08/04/2018,

<https://www.hackmageddon.com/2018/04/06/february-2018-cyber-attacks-statistics/>

المصدر:

نلاحظ من خلال الشكل السابق، أن أكثر نوع من الجرائم المحوسبة الذي تم في شهر جانفي 2018 هو الجرائم الرقمية بنسبة 81.7% تليها الجرائم المتعلقة بالجوسسة بنسبة 12.2% ثم الجرائم الأمنية بنسبة 4.3% وأخيرا جرائم القرصنة بنسبة 1.7%.

1-2) الاعتداءات الإلكترونية:

الاعتداءات الإلكترونية Cyber-attaques هي كل الاعتداءات التي تهدف إلى إلحاق الضرر بأنظمة المعلومات، ومصدر توافر المعلومات وسريتها في هذه الأنظمة، هذه الاعتداءات تختلف درجة خطورتها باختلاف الدافع من الاعتداء، فمنها ما يكون بدافع سياسي، اقتصادي أو بدافع تجاري أو فردي ومنها من يقوم بالاعتداء من أجل الفضول والافتخار وغيرها من الدوافع.

- الأشكال المختلفة للاعتداءات الإلكترونية:

تأخذ الاعتداءات الإلكترونية التي يمكن أن تصيب أجهزة، برامج وشبكات المؤسسة، أشكالاً مختلفة وأساليب متعددة وهي في تطور مستمر وتستغل أي ثغرة موجودة في الأنظمة من أجل اختراقها أو إلحاق الضرر بها، وتعد شبكة الإنترنت الوسيلة المفضلة للمخترقين لارتكاب هذه الجرائم، ومن هذه الاعتداءات نذكر ما يلي¹⁰:

- الاعتداء باستعمال البرمجيات الخبيثة

البرمجيات الخبيثة هي عبارة عن برامج أو أجزاء برامج خبيثة، تعمل بعيداً دون مساعدة مستعمل الحاسب، موجهة إلى عرقلة، تغيير أو تخريب أي جزء من مكونات الحاسب. وهي تنقسم إلى البرمجيات غير المتكاثرة كحصان طروادة والبرمجيات المتكاثرة ذاتياً (كالفيرسات والديدان).

- الاعتداء باستعمال برامج الجوسسة:

هي برامج تعمل خفية عن مستعمل الجهاز، وتقوم بجمع المعلومات عن النظام وإرسالها إلى الخارج من خلال شبكة الإنترنت، وهي لا تهدد تكامل البيانات، التطبيقات أو النظام. كما يمكنها أن تستعمل برنامج Keylogger الذي يسمح بتسجيل النقرات على لوحة المفاتيح بما في ذلك كلمات السر.

- الاعتداء باستعمال أسلوب اعتراض البيانات:

تسمح التقنية باستراق السمع للبيانات التي تنتقل في شبكة المؤسسة من خلال اعتراض وتحليل البيانات المتنقلة بداخل الشبكة بغرض الاستفادة منها بطريقة غير شرعية. بمعنى آخر اعتراض البيانات بعد إرسالها من قبل المرسل وقبل استقبالها من طرف المستقبل*.

- **الاعتداء باستعمال أسلوب منع تقديم الخدمة:**
أي الإضرار المادي بالخادم لمنع تقديم الخدمة. وعادة ما يعتمد على برامج خاصة لتحقيق هذا الهدف تسمى ببرامج **Flooders** حيث تعمل على إغراق خوادم الويب بسيل من الإيعازات دفعة واحدة لتعطيلها، وإرسال مئات الآلاف من الرسائل الإلكترونية لخوادم البريد الإلكتروني دفعة واحدة لإيقافها عن العمل، وذلك انطلاقاً من حاسب واحد فقط.
- **الاعتداء باستعمال البريد غير المرغوب فيه:**
تعرف رسائل البريد الإلكتروني غير المرغوبة بأنها إساءة استخدام نظام الرسائل الإلكترونية بإرسال كم هائل من الرسائل العشوائية وغير المطلوبة أو المتوقعة أو المرغوبة من قبل المستقبلين لهذه الرسائل وغالباً ما يكون الغرض من هذه الرسائل هو الإعلان التجاري أو الاحتيال على صاحب البريد الإلكتروني.
- **الاعتداء باستعمال أسلوب انتحال عنوان IP:**
تعني هذه التقنية تعويض عنوان IP للمرسل بعنوان حاسب آخر، مما يسمح للمعتدي بالقيام بالاعتداء والتخفي وراء عناوين أخرى وبالتالي إخفاء كل أثر يؤدي إلى التعرف عليه. كما تمكن هذه التقنية المعتدي، من اقتحام شبكة مؤسسة ما عند تزوير عنوان IP الخاص به واستعمال عنوان شخص عامل بالمؤسسة، وهكذا لن يتمكن جدار النار المستعمل من معرفة المعتدي.
- **الاعتداء باستعمال أسلوب انتحال نظام أسماء النطاقات DNS:**
المقصود بهذا الأسلوب توجيه مستخدمي الإنترنت أوتوماتيكياً إلى المواقع المحتوية على "برامج الجوسسة" أو المواقع التي تحاكي في تصميمها المواقع التجارية والبنكية الحقيقية والتي تنجز من قبل المعتدين بغرض الإيقاع بهم. ويتم هذا التوجيه من خلال الرسائل الإلكترونية غير المرغوب فيها.
- **والاعتداء باستعمال أسلوب الاضطهاد الإلكتروني:**
ويقصد به سرقة البيانات الشخصية السرية والحساسة عن طريق رسائل البريد الإلكتروني لغرض انتحال الشخصية، وذلك عن طريق انتحال شخصية إحدى البنوك، أو مؤسسة معينة وإيهام الضحية بجدية الطلب وأهميته. سمي هذا النوع من الرسائل رسائل الاضطهاد

* كمثال على هذا النوع من البرمجيات نذكر كل من Mpsnif و Sniffer Ettercap.

الالكتروني لأن مرسلها يستخدمون رسالة البريد الإلكتروني كطعم لاصطياد الأرقام السرية وغيرها من البيانات الشخصية السرية.

وتجدر الإشارة أن عدد الأشخاص والمؤسسات الذين تعرضوا للاعتداءات الالكترونية بلغ أرقاما هائلة ومبالغ مالية جد مرتفعة تمثل ميزانيات بعض الدول؛ فحسب بعض المختصين في أمن المعلومات وصل عدد الاعتداءات الالكترونية في سنة 2013 حوالي 1.700.870.654 اعتداء، في حين وصل حجم الخسائر المالية سنة 2011 فقط حوالي 388 مليار دولار، أما موقع Kaspersky Lab يشير إلى أن معظم الاعتداءات الالكترونية يكون مصدرها الولايات المتحدة الامريكية ب 25.54% وروسيا ب 19.44%، وبدرجة أقل هولندا وألمانيا على التوالي ب 12.80 و 12.51%¹¹.

إذن من خلال ما سبق، يمكن أن نلاحظ تعدد واختلاف وسائل الاعتداء الالكتروني نظرا لاختلاف الدافع والهدف وراء كل اعتداء، فبعض الاعتداءات يكون الهدف منها سرقة البيانات أو التجسس عليها والبعض الآخر تخريبها أو منع الوصول إليها أو حتى تغيير محتواها، وهذا ما يوجب على المؤسسة اتخاذ كافة اجراءات الحماية التي تناسب كل نوع أو وسيلة من وسائل الاعتداء الالكتروني لضمان حماية معلوماتها من أي تهديد.

- مخاطر وتهديدات الإعتداءات الإلكترونية:

فيما يخص أهم المخاطر والتهديدات التي تتعرض لها مواقع معلومات المؤسسة على شبكة الانترنت فتمثل فيما يلي¹²:

- تغيير المحتوى:

يقوم بعض المحترفين بالهجوم على موقع المؤسسة على شبكة الانترنت واختراقه وتغيير محتوياته أو بعضها، كما تقوم بذلك أيضا بعض المؤسسات المنافسة لهذه المؤسسة، وذلك بهدف الإساءة إليها أو إساءة العلاقة بينها وبين زبائنها. كما يتم تغيير محتويات موقع المؤسسة على شبكة الانترنت أيضا من خلال هجمات بعض الهواة استخفايا وسخرية بالمؤسسة، وذلك كما حدث عند تغيير محتويات موقع البيت الأبيض الأمريكي، حيث تم تغيير صور بعض الشخصيات الهامة بصورة فاضحة مما اضطر المسؤولين إلى غلقه لعدة أيام.

- استخدام موقع المؤسسة على شبكة الانترنت لتنفيذ بعض الأعمال غير المشروعة:

يمكن لموقع المؤسسة الغير محمي على شبكة الانترنت بعض الهواة أو المحترفين من الهجوم على هذا الموقع واستخدامه في تنفيذ بعض الأعمال غير المشروعة كتتفيذ بعض الجرائم، إخفاء بعض المسروقات أو بعض الملفات كما في حالة التجسس الاقتصادي. كما يمكن لبعض المجرمين الاختراق التصنتي لهذا الموقع بحيث يمكن سرقة المعلومات

الخاصة بالمشاركين مثل سرقة أرقام حسابات الزبائن أو أرقام الإئتمان، فضلا عن سرقة معلومات الفواتير.

- التعرف على النظم والسياسات الداخلية للمؤسسة:

يمكن للهواة وكذلك المؤسسات المنافسة أن يدخلوا إلى موقع المؤسسة ويعبثوا بالنظم الداخلية لها؛ حيث يمكنهم إلغاء بعض المعلومات الداخلية ذات الأهمية للمؤسسة، كما يمكنهم أيضا الحصول على بعض المعلومات عن السياسات الداخلية لها واستغلالها استغلالا سيئا، مما يترتب عنه نتائج سلبية للمؤسسة.

- توقف موقع المؤسسة عن العمل:

ويتم ذلك من خلال قيام المهاجمين بشغل الموقع الرئيسي للمؤسسة بكثير من المعاملات والاستفسارات والرسائل، مما يترتب عليه فقدان هذا المقر لقدرته على التعامل مع المستخدمين له، ويمثل ذلك خطرا جسيما بالنسبة للمؤسسات التي تعتمد بصفة رئيسية على هذا الموقع لتوفير خدماتها الأساسية لزبائنهم.

- وتخريب موقع المؤسسة:

ويتم هذا التخريب من خلال دخول المهاجمين على البرامج الخاصة بإدارة موقع المؤسسة وتغيير بعض المؤشرات الخاصة به، مما يترتب عليه حدوث أخطاء في التشغيل أو حتى توقف الموقع كليا عن العمل.

نلاحظ من خلال ما سبق أن المخاطر والتخريب التي تتعرض لها نظم وتكنولوجيا المعلومات كثيرة ومتنوعة منها ما يكون عن قصد وعمدا كالقرصنة، ومنها ما يكون غير مقصود كإهمال العاملين أو وجود خلل في المنظومة الأمنية. وإن أي منظومة للمعلومات في المؤسسة تكون عرضة للهجوم من جبهتين مختلفتين ألا وهي الجبهة الداخلية والجبهة الخارجية¹³. ويمكننا القول أن المخاطر الالكترونية التي تتعرض لها المؤسسة تكون ناتجة عن الاعتداءات الالكترونية المختلفة التي تواجهها، ويمكن أن يكون مصدرها داخلي (العاملين داخل المؤسسة) أو خارجي (محيط المؤسسة).

(2) الأشكال المختلفة للاعتداءات الإلكترونية:

قبل الشروع في تأمين وحماية المعلومات على المؤسسة أولا القيام بتقدير لمخاطر، ثم تحديد المخاطر المحتملة من حيث الاحتمالية والشدة وتحديد كميا وتأهيلها، يحين الوقت لاختيار حلول الوقاية بمقارنة تكلفة الاستخدام والمخاطر التي يتم تغطيتها مع تحديد شامل لوسائل الكشف عن الهجمات والتدخلات في أسرع وقت ممكن. وأخيرا تحديد خطط أمان الكمبيوتر الاحتياطية وكيفية العودة بأسرع ما يمكن إلى الوضع قبل الهجوم¹⁴.

(1-2) أساليب الحماية الفيزيائية:

إن أي مؤسسة لا تمتلك مقومات الحماية الفيزيائية، يصبح الوصول إليها وإلى أجهزتها ومعلوماتها أمرا سهلا. تستخدم المؤسسات اليوم العديد من طبقات الحماية، مثل حساسات الحركة وأجهزة الإنذار، وبطاقة تعريف الموظفين الذكية لحفظ الأجهزة ومنع وصول أشخاص غير مرغوب بهم إلى مبنى المؤسسة، حيث أن وصول أي شخص غريب إلى محيط المؤسسة قد يؤدي به إلى تخريب ما يمكنه تخريبه، أو ساقط أجهزة، أو حتى وضع أجهزة تنصت على الشبكة في أي مكان من أماكن تمديدات الشبكة¹⁵.

وتتمثل أساليب الحماية الفيزيائية في اختيار المكان الملائم والتجهيزات الأكثر حفاظا على الأمن. ولتحقيق هذا المستوى من الحماية لابد من مراعاة الآتي¹⁶:

- في حالة وضع الخوادم في غرف تخصيص غرف مغلقة لحفظ أجهزة خادم الشبكة مركزية، أما إذا لم يكن ذلك متاح فلا بد من حفظ أجهزة الخادم ضمن غرف الإداريين؛

- اختيار الكابلات الأكثر حماية للمعلومات كلما كان أمن المعلومات ضرورياً للهيئة، وذلك على اعتبار أن تلغي الإشعاع وتتمثل في كابلات الألياف الضوئية الثانوي للكابلات وبالتالي تمنع التنصت على البيانات خلال نقلها عبر الكابلات؛
 - تركيب تمديدات وكابلات الشبكة في 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 الثني في حالة وضعها تحت قطع المفروشات الثقيلة؛
 - استخدام الكابلات المغلفة وذلك لتقليل الإشعاع الثانوي المنبثق من خلالها، ويمكن إضافة أكثر من غلاف عليها لمنع الإشعاع نهائياً؛
 - تأمين النوافذ والفتحات الأخرى الموجودة في غرفة الخادم خصوصاً إذا كانت قريبة من الأرض؛
 - تأمين الأبواب والمنافذ الأخرى كالنوافذ باستخدام أجهزة إنذار آلية تقوم بتشغيل أجراس للتنبيه في حالة دخول أشخاص للموقع في غير أوقات العمل؛
 - وتوفير وسائل مراقبة للموقع مثل الدوائر التلفزيونية المغلقة، وذلك لإتاحة المراقبة بعد ساعات الدوام.
- يمكننا القول من خلال ما سبق، أن أساليب الحماية الفيزيائية تعتمد بشكل أساسي على حماية الأجهزة والمعدات المادية كالحاسوب والكابلات والخوادم ووضعها في أماكن ملائمة لمنع تخريبها أو إلحاق الضرر بها بالإضافة إلى تأمين مقر المؤسسة ككل من خلال وضع كاميرات المراقبة وتأمين الأبواب والمنافذ المختلفة.

2-2) أساليب الحماية المنطقية:

أدى ظهور الجرائم الالكترونية إلى جعل المجتمعات والمؤسسات الاقتصادية والأفراد في العالم أكثر عرضة للمخاطر الالكترونية، مما أدى إلى ظهور وسائل حديثة في الحماية تدعى بوسائل الأمن الالكتروني. ويعتبر مفهوم الأمن الالكتروني من المفاهيم الحديثة، حيث ظهر في بداية الألفية الجارية تماشياً مع انتشار مفهوم التجارة الالكترونية والأعمال الالكترونية والمراقبة الالكترونية وغيرها من المفاهيم¹⁷.

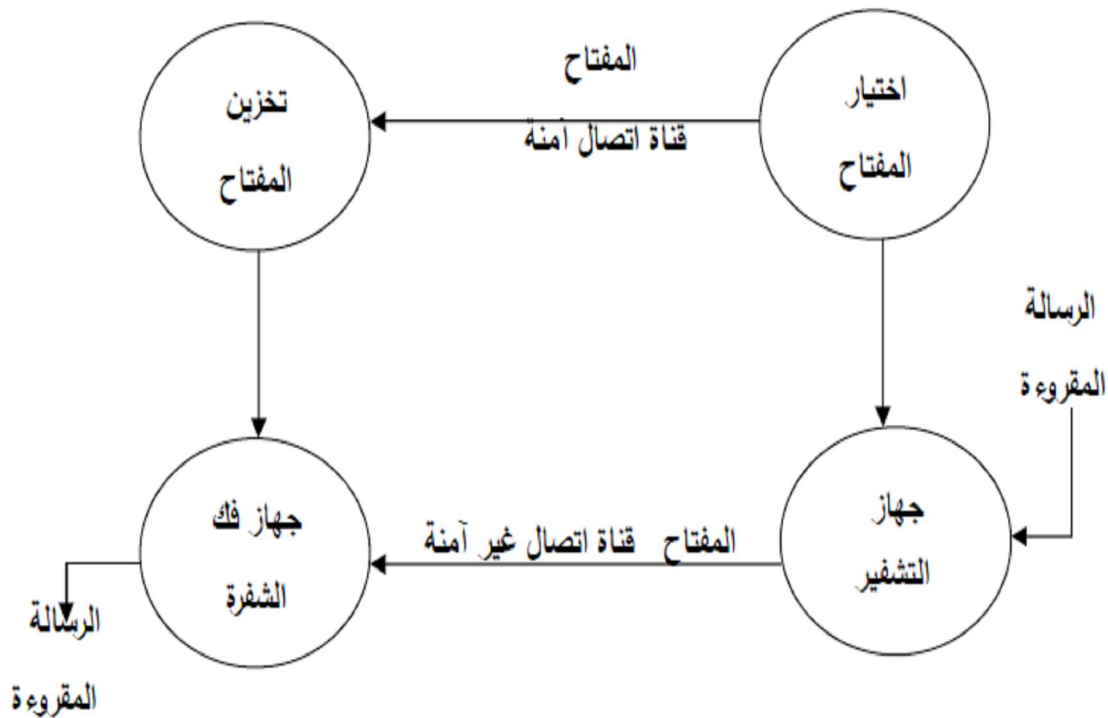
تتمثل أساليب الحماية المنطقية في مختلف الوسائل والبرمجيات التي تهدف إلى حماية النظام والمحافظة على المعلومات التي يحتويها، ويمكن ذكرها كما يلي:

- التشفير الإلكتروني:

يعرف التشفير بأنه عملية تشكيل البيانات باستخدام خوارزمية معينة تسمى المفتاح 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 عمليات تجسس أو تحريف لمضمونها، على أن يتم فك الشفرة لدى مستقبل الرسالة باستخدام مفتاح فك الشفرة¹⁸.

والشكل التالي يوضح نظام التشفير الإلكتروني بشكل عام:

الشكل 04 - التشفير الإلكتروني



المصدر: أحمد محمد غنيم، «التسويق والتجارة الإلكترونية»، المكتبة العصرية، القاهرة، 2009، ص 275.

لضمان سرية المعلومات في المؤسسة وسلامة محتواها وتوافرها عند الحاجة إليها، يستعمل أسلوبين هما¹⁹:

1. أسلوب الشبكة الخاصة الافتراضية: المعتمد على بروتوكول IPsec الذي يسمح بإنشاء ممر آمن بين المرسل والمستقبل الذي من خلاله يتم تشفير كل البيانات والرسائل قبل تبادلها. يستخدم هذا الأسلوب للربط بين مقر المؤسسة وفروعها أو بينها وبين المتعاملين معها؛
2. الأمن من خلال البروتوكول *SSL: الذي يسمح بتشفير كل بيانات المعاملات التجارية بين المؤسسة وزبائنها وبدعم الشهادات الالكترونية التي يمكن أن يحصل عليها الموقع التجاري ليصبح جديراً بالثقة والتأكد بأن الصفقات التي تجرى هي مع موقع المؤسسة الأصلي وليس مع موقع قرصنة يسيره محتال أو مخادع.
- التوقيع الإلكتروني:
يقصد بالتوقيع الإلكتروني استخدام طريقة أو وسيلة معينة للتحقق من أن صاحب المعاملة هو نفس الشخص الذي قام بإرسالها أو تنفيذها، ويطلق على هذا التوقيع أيضاً البصمة الإلكترونية. ويتم إصدار التوقيعات الإلكترونية في عدة أشكال أساسية يتمثل أهمها في شكل التوقيع الرقمي التقليدي أو يتم إدخاله وقراءته رقمياً من خط اليد، أو يتم في شكل مفتاح تشفير شخصي.²⁰
- ضبط الوصول إلى الشبكة وإتاحة مواردها:
من الضروري ضبط الوصول إلى الشبكة لحمايتها من التعرض لعمليات الاقتحام ولتحقيق ذلك لابد من تخصيص اسم أو رقم تعريف لكل مستخدم للشبكة وكلمة مرور حيث تعد هذه هي الخطوة الأولى المتبعة لمنع اقتحام الشبكات يتبعها التحقق 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.²¹
- جدران المنع:
هي مجموعة من البرمجيات والأجهزة التي يتم إعدادها لتشكيل حدود فاصلة بين شبكة المؤسسة الخاصة إنترنت وشبكة الإنترنت، والهدف منه هو التغلب على أكبر قدر ممكن من الثغرات الأمنية، من خلال بناء قناة اتصالات توجه إليها المعلومات المرسل والمتبادلة مع شبكة الإنترنت لمراقبتها والسيطرة على خروجها ودخولها من وإلى شبكة المؤسسة الخاصة، وذلك وفق أسس وقواعد يتم تحديدها وبنائها في جدار النار وبالتالي يقوم جدار النار بدور المرشح حيث يراقب تدفقات البيانات التي تمر عبره دخولا وخروجاً، ويقوم بتحليلها ومن ثم السماح بمرورها إذا كانت تحقق الشروط، أو منعها في حالة العكس.²²
- الشهادات الإلكترونية:
أسفرت ممارسات وتطبيقات معاملات التسويق والتجارة الإلكترونية عن ضرورة وجود شهادة من جهة مختصة موثوق فيها تعرف بهيئة الاعتماد، تؤكد وتثبت أن الشخص صاحب

* Secure Sockets Layer .

المعاملة الإلكترونية المعينة هو نفس الشخص المحدد لهذه المعاملة والذي قام بتنفيذها وأن صورته هي نفس الصورة الواردة في وثيقة إثبات الشخصية، وبناء على ذلك فإنه عند إجراء أية معاملات إلكترونية، فإن هيئة الاعتماد تقوم بإصدار شهادة إلكترونية لتحقيق الشخصية وذلك بالنسبة لكل معاملة من هذه المعاملات تشتمل على بيانات عن المرسل ونسخة من المفتاح العام له وتاريخ انتهاء صلاحية هذه الشهادة²³.

- البرمجيات المضادة للاعتداءات الإلكترونية:

هي تلك البرمجيات التي تسمح بحماية الحاسب والنظم المعلوماتية ضد الاعتداءات الإلكترونية وتختص بمراقبة وتحليل الملفات وتحطيم البرمجيات الخبيثة. تعمل البرمجيات المضادة للاعتداءات الإلكترونية بالاعتماد على قاعدة تحتوي مختلف التوقيعات والبصمات المعروفة بالبرنامج الخبيث أو على أنظمة الذكاء الاصطناعي لاكتشاف هذه البرامج. ولهذا ومن أجل فعالية مثلى للبرنامج يجب تحديثه وتحسينه باستمرار (تحسين البرنامج والقاعدة في نفس الوقت)²⁴.

- أنظمة كشف الاختراق:

إن أنظمة كشف الاختراق فعالة إلى أبعد حد عندما تنصب بشكل صحيح وتراقب بانتظام. ولكن يجب الحفاظ على طريقة عمل هذه الأنظمة بسرية بالغة، ومن الواجب حمايتها بثقة شديدة. تسجل أغلب أنظمة الكشف جميع التعاملات التي تجري داخل موقع الحماية وجميع الطلبات التي تأتي من خارجه. ويؤدي تحليل المعلومات في سجلات الأحداث إلى تحديد المتناقضات أو النشاطات والإجراءات غير النظامية. إن أنظمة كشف الاختراق فعالة في منع سرقة البيانات من قبل التهديدات الداخلية والخارجية²⁵.

- والنسخ الاحتياطي:

على الرغم من الاحتياطات الأمنية المتعددة التي قد تتبع لحماية البيانات إلا أنه من المحتمل وقوع أي 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 الاحتياطي للبيانات هذا المستوى من الحماية، حيث يتم من خلاله إنشاء نسخ احتياطية يتم حفظها سواء في نفس مقر العمل أو خارجه، ويتم تحديثها بصورة منتظمة لضمان أقل قدر من الخسائر في حالة فقدان البيانات الأصلية²⁶.

وهناك أكثر من طريقة تتبع للنسخ الاحتياطي تتمثل في الآتي²⁷:

- **النسخ الاحتياطي الكامل:** يتم وفقاً له نسخ جميع الملفات المحملة على الخادم بغض النظر عما إذا كان قد أجري تعديل على تلك الملفات من عدمه؛
- **النسخ الاحتياطي التراكمي أو التزايد:** يتم وفقاً له إجراء نسخ احتياطي للملفات التي تم تعديلها بعد آخر نسخ احتياطي، ويتم في هذه الحالة تعديل سمات الملفات بحيث يظهر أنه أجري لها نسخاً احتياطياً؛

■ **والنسخ الاحتياطي التبايني أو التفاضلي:** يتم وفقًا له إجراء نسخ احتياطي للملفات التي تم تعديلها بعد آخر نسخ احتياطي، ولا تعدل سمات الملفات في هذه الحالة ويجري النسخ التبايني في كل مرة على البيانات ابتداءً من آخر نسخ احتياطي كامل لها، في حين يجري النسخ التراكمي على البيانات ابتداءً من آخر نسخ احتياطي لها.

يمكننا أن نلخص متطلبات أمن شبكة المعلومات بالنقاط التالية²⁸:

- **تحديد سياسات العمل في شبكات المعلومات:** بأن يكون واضحاً ما هو المسموح به والممنوع فيما يتعلق بأمن المعلومات على الشبكة؛
- **توفير آليات تنفيذ سياسات العمل:** بأن يكون معروفاً كيفية تنفيذ هذه السياسات وما هي العقوبات التي ستوقع في حالة المخالفة؛
- **العنصر البشري.** بأن يتولى إدارة وتشغيل شبكات المعلومات عناصر بشرية مدربة ومؤهلة للتعامل مع هذه التكنولوجيا وألا يترك المجال للهواة للعبث بمثل هذه المقدرات الثمينة وخاصة في الأماكن الحكومية والحيوية على مستوى الدول؛
- **تغيير الأوضاع الأصلية لمعدات الشبكات:** وذلك بأن يتم كل فترة تغيير الأوضاع الأصلية للمعدات Hardware والبرامج Software الخاصة بشبكات المعلومات كإجراء احترازي كل فترة لمنع الاختراقات الخارجية؛
- **المراقبة:** يجب أن يكون هناك نوع من المراقبة والمتابعة لأنشطة المعلومات على الشبكة بشكل دقيق ودائم وذلك بهدف اكتشاف أي أنشطة مشبوهة أو حركات غير طبيعية ضمن نطاق الشبكة وتقادي تقاوم الأوضاع؛
- **حسن اختيار مواقع نقاط الشبكة:** فيجب أن يتم التدقيق جيداً عند اختيار نقاط الاتصال بشبكات المعلومات، وأن تكون هذه النقاط في مواقع جيدة ومؤمنة ومحمية؛
- **وبروتوكولات التحقق والتشفير:** يجب أن يتم تشغيل بروتوكولات التحقق من الهوية وأنظمة تشفير البيانات لتأمين المعلومات على الشبكة، وأن يتم اختيار البرامج ذات السمعة العالمية في هذا الإطار.

ونشير أخيراً إلى ظهور حلول معلوماتية حديثة تتضمن مجموعة خدمات متكاملة تعمل على إدارة أمن الأعمال الإلكترونية للمؤسسة، تجمع بين وظيفة كشف وإيقاف الاعتداءات الإلكترونية، وتسيير كل من الجدران المقاومة للنار والشبكات الخاصة الافتراضية، مع تشفير كل البيانات والملفات المتبادلة. ومن أهم هذه الحلول نذكر كل من eTrust PKI وOnlineGuardian والليزان يسمحان بضمان سرية ووثوقية وسلامة البيانات المتبادلة بالإضافة إلى عدم انكار التصرفات التي تمت عبر مختلف الشبكات²⁹.

خاتمة:

يعتبر أمن المعلومات من المواضيع الهامة التي يجب على المؤسسة الإعتناء بها، فأى مؤسسة متصلة بشبكة الإنترنت معرضة إلى مخاطر متعددة من قرصنة معلومات، وتخريب لموقع المؤسسة الالكتروني وتشويه سمعة المؤسسة بين زبائنهم من خلال تغيير المحتوى بالإضافة إلى خطر فقدان المؤسسة لمعلوماتها والتي تعد أهم مورد في عصرنا الحالي، وغيرها من المخاطر التي تستوجب على المؤسسة أخذ الحيطة والحذر من خلال تأمين معلوماتها بواسطة مختلف أشكال ووسائل الحماية الالكترونية.

من خلال دراستنا لموضوع أمن المعلومات، يمكن الخروج ببعض الاقتراحات التي نذكرها كما يلي:

- إن ضياع أو تلف أو تغيير معلومات المؤسسة ينجم عنه خسائر كبيرة مادية ومعنوية تصل إلى درجة تهديد وجود المؤسسة، لذا فعلى المؤسسة الاعتناء بشكل كبير بالحفاظ على أمن معلوماتها باعتباره موردا استراتيجيا لها؛
- من الضروري للمؤسسة في وقتنا الراهن أن تهتم بتوظيف أفراد مؤهلين في المجال المعلوماتي؛
- على المؤسسة الاهتمام بتوفير أساليب الحماية الفيزيائية والمنطقية معا للحفاظ على أمن معلوماتها؛
- ولا يجب على المؤسسة الاكتفاء فقط بتوفير برامج الحماية المناسبة بل عليها الاهتمام بتحديث هذه البرامج بصفة دورية ومحاولة الحصول على أحدث النسخ وأجودها.

الهوامش والمراجع:

- 1 منى الأشقر جبور & عزيز ملحم بربر، «أمن الشبكات والانترنت»، الحلقة العلمية حول «الانترنت والإرهاب»، جامعة نايف العربية للعلوم الامنية بالتعاون مع جامعة عين شمس، الجيزة، 15-19/11/2008 [كتاب الحلقة العلمية، ص 1].
- 2 موقع spectro، «أمن تكنولوجيا المعلومات (T_Security_Arabic_SampleLesson)»
http://www.specto.co/files/Books_Details/Samples/IT_Security_Arabic_SampleLesson.pdf
- 3 حديد نوفيل & كرييط حنان، «أمن المعلومات ودوره في مواجهة الاعتداءات الالكترونية على نظام معلومات المؤسسة»، مجلة "المؤسسة"، مخبر إدارة التغيير في المؤسسة الجزائرية، جامعة الجزائر 3، المجلد 03، العدد 03، 2014، ص ص 186-207.
- 4 ندى اسماعيل جبوري، «حماية أمن أنظمة المعلومات دراسة حالة في مصرف الرافدين / فرع شارع فلسطين»، مجلة "تكريت للعلوم الاقتصادية والإدارية"، جامعة تكريت (العراق)، المجلد 07، العدد 21، 2011، ص ص 72-94.
- 5 مقال، «أمن المعلومات: ماهيتها وعناصرها واستراتيجياتها»، 10/12/2017، ص 1،
http://www.m5zn.com/newuploads/2012/12/30/doc/m5zn_5056f7e72701105.doc
- 6 DORIGNY Mickael, «Qu'est ce que la sécurité de l'information», 21/10/2016,
<https://www.information-security.fr/quest-ce-que-la-securite-de-linformation/>
- 7 حديد نوفيل & مسوس كمال، «مقاربات حماية أنظمة معلومات المؤسسة من الإعتداءات الالكترونية»، مجلة "المؤسسة"، مخبر إدارة التغيير في المؤسسة الجزائرية، جامعة الجزائر 3، المجلد 05، العدد 05، 2016، ص ص 43-26.
- 8 ندى اسماعيل جبوري، مرجع سبق ذكره.

- 9 حديد نوفيل & مسوس كمال، مرجع سبق ذكره.
- 10 حديد نوفيل & كريبط حنان، مرجع سبق ذكره.
- 11 حديد نوفيل & مسوس كمال، مرجع سبق ذكره.
- 12 أحمد محمد غنيم، «التسويق والتجارة الالكترونية»، المكتبة العصرية، القاهرة، 2009، ص ص 270-273.
- 13 مدوكي يوسف، «إدارة مخاطر وأمن المعلومات في ظل ثورة ونظم وتكنولوجيا المعلومات»، مجلة "الافاق للدراسات الاقتصادية"، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة تبسة، المجلد 02، العدد 02، 2017، ص ص 119-132.
- 14 FERNANDEZ Allain, «La sécurité informatique», 28/06/2017,
<https://www.piloter.org/systeme-information/securite-informatique.htm>
- 15 مقال، «طريقة بناء تكنولوجيا أمنة»، 2016/12/27،
<https://nasainarabic.net/main/articles/view/using-defense-depth-model>
- 16 فاتن سعيد بامفلح، «حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى»، 2017/10/12،
http://www.kau.edu.sa/Files/0012433/Researches/56927_27244.pdf
- 17 حديد نوفيل، «تكنولوجيا الانترنت وتأهيل المؤسسة للاندماج في الاقتصاد العالمي»، أطروحة دكتوراه في علوم التسيير، كلية العلوم الاقتصادية وعلوم التسيير، جامعة الجزائر 03، 2007، ص 179.
- 18 حديد نوفيل & كريبط حنان، مرجع سبق ذكره.
- 19 حديد نوفيل & كريبط حنان، مرجع سبق ذكره.
- 20 أحمد محمد غنيم، مرجع سبق ذكره، ص 279.
- 21 فاتن سعيد بامفلح، مرجع سبق ذكره.
- 22 أحمد محمد غنيم، مرجع سبق ذكره، ص 282.
- 23 نفس المرجع، ص 282.
- 24 حديد نوفيل & كريبط حنان، مرجع سبق ذكره.
- 25 نفس المرجع السابق.
- 26 فاتن سعيد بامفلح، مرجع سبق ذكره.
- 27 نفس المرجع السابق.
- 28 رجب عبد الحميد حسنين، «أمن شبكة المعلومات الالكترونية: المخاطر والحلول»، مجلة "متصفح الانترنت"، دورية إلكترونية علمية تعنى بمجال المكتبات والمعلومات، العدد 30، 2012، ص 04،
http://journal.cybrarians.info/index.php?option=com_content&view=article&id=629:networks&catid=257:studies&Itemid=0
- 29 حديد نوفيل، «تكنولوجيا الانترنت وتأهيل المؤسسة للاندماج في الاقتصاد العالمي»، مرجع سبق ذكره، ص 188.