أمن المعلومات

إعداد

د/زينب علي بكري علي

قسم المكتبات وتكنولوجيا المعلومات

كلية الآداب- قنا

العام الجامعي

٢٠٢٣/٢٠٢٤م

محاضرات في

أمن المعلومات

إعداد

د/ زينب على بكرى على

كلية الآداب بقنا- جامعة جنوب الوادي

٢٠٢٣/٢٠٢٤م

بيانات الكتاب

الكلية : الآداب

الفرقة : الرابعة

التخصص : المكتبات والمعلومات

تاريخ النشر : ٢٠٢٤/٢٠٢٣

عدد الصفحات : ١٤٦ صفحة

إعداد : د. زينب علي بكري علي

بسم الله الرحمن الرحيم

" ((يَا أَيُّهَا الَّذِينَ آمَنُوا اتَّقُوا اللَّهَ وَقُولُوا قَوْلاً سَدِيداً * يُصْلِحْ لَكُمْ أَعْمَالَكُمْ وَيَغْفِرْ لَكُمْ ذُنُوبَكُمْ وَمَنْ يُطِعِ اللَّهَ وَرَسُولَهُ فَقَدْ فَازَ فَوْزاً عَظِيماً)) "

صدق الله العظيم .

[الأحزاب: ٧٠-٧١] .

قائمة المحتويات

مقدمة:

تشكل المعلومات للمنظمات البنية التحتية التي تمكنها من أداء مهامها، إذ أن نوع المعلومات وكميتها وطريقة عرضها تُعد الأساس في نجاح عملية صنع القرارات داخل المنظمات المعاصرة وعليه يكون للمعلومات قيمة عالية تستوجب وضع الضوابط اللازمة لاستخدامها وتداولها ووضع السبل الكفيلة بحيازتها، لذا كانت المشكلة التي يجب أخذها بالحسبان هي توفير الحماية اللازمة للمعلومات وإبعادها عن الاستخدام غير المشروع لها.

ونظرا لأهمية المعلومات فإن الاهتمام بكيفية الحفاظ عليها وحمايتها تنامي، مما أدي إلي ظهور ما يسمي علم أمن المعلومات Information Security Science، إن قضية أمن المعلومات ليست عملية تقنية بحتة يقوم بها المتخصصون فقط، وإنما هي نتاج تعاون بين جميع موظفي المؤسسة الواحدة بحيث تتوزع الأدوار والمسئوليات بما يخدم مصالح المؤسسة، ومن ثم فإن أي خطة تضعها المؤسسة

بخصوص أمن المعلومات لابد من احتوائها علي عناصر وبنود شاملة لكل العمليات والسياسات المتعلقة بالنواحي التقنية والبشرية.

ويتناول مقررنا هذا أمن المعلومات، يعرف به وبعناصره، وبالمخاطر والتهديدات التي تواجه أمن المعلومات

ويتضمن الكتاب خمسة فصول على النحو التالي:

الفصل الأول: التعريف بأمن المعلومات وتطوره التاريخي ومبادئه والتحديات التي تواجه أمن المعلومات

الفصل الثاني: تهديدات أمن المعلومات وسبل الحماية.

الفصل الثالث: أمن شبكات المعلومات وتصنيف جرائم المعلومات.

الفصل الرابع: خطة سياسة امن وحماية المعلومات.

الفصل الخامس: الخصوصية وأمن المعلومات وتأثير التقنيات الحديثة على الخصوصية.

الفصل الأول

أمن المعلومات

المفهوم؛ المبادئ؛ التحديات

مقدمة:

تحدث تكنولوجيا المعلومات والاتصال ثورة تمس القطاع الاقتصادي، السياسي، الاجتماعي والثقافي، في نفس أهمية الثورات السابقة. تعتمد هذه الثورة على المعلومة التي ترتكز عليها المعرفة البشرية. تسمح التكنولوجيات الحديثة للمعلومات برصد هذه الأخيرة معالجتها وتوزيعها على اختلاف أوعيتها المكتوبة، المرئية والمسموعة، ذلك بالتغلب على عائق حجم المعلومات والتقليص من الوقت اللازم لتوزيعها.

أدت هذه التكنولوجيا إلى طريقة عمل جديدة سهلت ميلاد مفهوم جديد وهو مفهوم مجتمع المعلومات الذي يرمي إلى الاستغلال الكثيف والأمثل للمعلومات في شتى مجالات الحياة. يعتبر هذه المجتمع وليد التقارب التكنولوجي بين المعلوماتية وتكنولوجيات الاتصال. وقد فتح أبواب التفاعل بين عدة متعاملين على المستوى العالمي الذي يقومون بتبادل للمعلومات عبر الشبكة العنكبوتية الانترنت.

إلا أنها في الوقت نفسه لا تخلو من السلبيات، التي قد يكون لها الأثر العكسي، خصوصًا في ظل تكاثر الاختراقات المتوقعة وتنوعها بين سرقة وابتزاز وأعمال تجسس، بيد أن الجانب الأخطر يتمثل في محاولات الاختراق التي تستدعي بذل اهتمام خاص لقضية أمن

المعلومات، ولاسيما أن الثورة المعلوماتية أحدثت ثورة إدارية لدى الحكومات والهيئات والمؤسسات على مستوياتها كافة، من خلال الدخول في مرحلة تغيير جذرية لتطوير المفاهيم وأساليب العمل بين بعضها البعض، أو بينها وبين المواطنين، أو بينها وبين مؤسسات وأفراد خارج الحدود الدولية، بحيث بات من المؤكد أن تشهد الفترة المقبلة توسعًا كبيرًا وتطورًا هائلاً في نطاق الحكومة الإلكترونية، كما نتج عن ثورة المعلومات اقتصاد جديد يسمى "الاقتصاد الرقمي". وهو يرتكز على الاستخدام الفعّال لخدمات الاتصالات والمعلوماتية في جميع الأنشطة.

الأمر الذي يفرض ضرورة وجود منظومة أمنية متكاملة للتعامل الآمن عبر الحاسب الآلي، بحيث تضمن التحقق من هوية المستخدمين، وسرية البيانات وسلامتها، والقدرة على التحقق من صحة الإجراءات. وبالإضافة إلى خطورة الاختراقات على أعمال الإدارة والاقتصاد والمال، فقد لعبت أنشطة المخابرات وأعمال التجسس دورًا هامًا للحصول على المعلومات، حيث أصبحت تعتمد على اختراق نظم المعلومات لدى الآخرين، ففي عصر تقنية المعلومات تحولت أنشطة المخابرات والتجسس إلى عمليات تقنية تعتمد على اختراق الأنظمة والشبكات. ولما كانت معظم الدول تحتفظ بالوثائق السرية مخزنة بهيئة

رقمية في مواقع سرية بعد تشفيرها، فإنه من الأهمية بمكان التأكيد على عدم كشف هذه المعلومات وسلامة محتواها من أي عبث، وهو ما لا يتحقق إلا من خلال أمن المعلومات، خصوصًا وأن حرب المعلومات أصبحت سمة مميزة للحرب الحديثة. ولذلك وغيره من الأسباب، أصبح من الضرورة بمكان نشر الوعي بأهمية أمن المعلومات، والأمن الإلكتروني، من خلال توفير رؤية علمية وعملية ترصد التحديات والصعوبات وتجد الحلول المناسبة لها.

ومن خلال هذا الانفتاح الواسع في مجال الاتصالات ونقل المعلومات وجب علينا معرفة كيف نحافظ على هذه المعلومات المنقولة من جهة لأخرى ومن هنا نشأ مفهوم ومصطلح" أمن المعلومات".

١/أمن المعلومات عبر التاريخ "السرية والخصوصية:"

إن حفظ الأسرار كان ولا يزال هاجس البشر منذ القدم، فقد سخر طاقته وإمكاناته الذهنية من اجل ابتكار طرق لإخفاء أسراره الهامة، حتى انه لم يتورع عن إخفائها في أحشاء الحيوانات كما كان يفعل الصينيون القدماء، فكانوا يكتبون رسائلهم على حرير ناعم ثم يضعونه في كرات صغيرة مصنوعة من الشمع، فيبلعها حاملها أو يدخلها في أحشائه من الخلف حتى إذا وصل إلى هدفه قام بإخراجها وتسليمها.

أما المغول فقد ابتكروا وسائل مختلفة لإخفاء وتامين رسائلهم الهامة، فقد كانوا يعمدون إلى اختيار أحد الرجال كثيف الشعر فيحلقون شعره ويكتبون عليه بقلم ناري ثم يتم سجنه في زنزانة انفرادية حتى ينموا شعره جيدا ليغطي الكتابة ثم يرسلونه إلى الطرف الأخر الذي يقوم بدوره بحلق شعره لقراءة الرسالة، بل وتطورت هذه الطريقة بعد اكتشاف الإمبراطور جنكيز خان لها، ليتم تقسيم الرسالة إلى أكثر من قسم وكل قسم يكتب على رأس شخص، بحيث إن تم كشف أحد الأشخاص والقبض عليه يكون من الصعب فهم الرسالة كاملة.

أما الهنود القدماء فقد عملوا على إشاعة ثقافة أمن المعلومات حتى ادخلوها في مناهجهم التعليمية، ففرضوا على النساء تعلم فنون الكتابة السرية إضافة إلى الفنون الأخرى التي يجب عليهن تعلمها وعددها أربعة وستون.

كما دلت الدراسات على أن المصريين القدماء قد نبغوا في الكتابة السرية وقد استخدموا ثلاثة أنواع من الكتابة السرية منذ عهود بعيدة في التاريخ، وكذلك الإغريق منذ القرن التاسع قبل الميلاد عندما استخدموا الكتابة السرية في معاهداتهم ولإخفاء أسرارهم.

ومن إبداعات اليونان في حفظ معلوماتهم وضع أسس لشفره خاصة تقوم على مبدأ الأرقام بدلا من الحروف.

وفي العصور الأوروبية الوسطى خطى امن المعلومات خطوات واسعة على يد الكنيسة، فقد نبغ العديد من رجال الكنيسة في تطوير فن امن المعلومات بأساليب منطقية مبتكرة، مثل استبدال الأحرف الصوتية بالنقاط في الكتابة السرية، واستبدال المقاطع بالأحرف.

ولم يكن العرب قبل الإسلام بعيدين عن هذه الفنون فقد برع العرب باستخدام شفرة الأرقام بدلا من الحروف وهذه الطريقة تسمى "حساب الجمل". فيما أبدع المسلمون بإرسال المعلومات بطرق غاية في السرية والحذر، وهنالك الكثير من القصص نذكر منها قصة ذلك الشيخ الذي أرسل بيتا من الشعر مع قاتليه تكشف ما فعلاه من دون أن يفهما قصده يقول فيه:

من مبلغ عني بان مهلهلاً..... لله دركما ودر أبيكما

فقالت ابنته: والله ما كان أبي ردي الشعر، ولا سفساف الكلام، فعرضوا هذا البيت على شاعر لديهم فقال لهم أحسن العزاء في أبيكم وإنما أراد أن يخبركم أن هؤلاء هم من قتلوه فصعقوا وقالوا ما دليلك فأنشدهم البيت كامل قال فيه:

من مبلغ عني بان مهلهلاً..... أضحى قتيلاً بالفلا مجندلا

لله دركما ودر أبيكما..... لا يبرح العبدان حتى يقتلا

في عام ١٣٦١ تم في بريطانيا سن قانون تم بموجبه منع اختلاس النظر والسمع وعاقب عليه بالسجن. وفي عام١٧٧٦ اصدر البرلمان السويدي قانونا نظم الوصول إلى السجلات العامة ومنع الوصول إليها إلا لأهداف مشروعة.

٢/تعريف أمن المعلومات:

من زاوية أكاديمية، هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها، وذلك من خلال توفير الأدوات والوسائل اللازمة لحماية المعلومات من المخاطر الداخلية أو الخارجية، أو هو المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين بالاطلاع عليها وذلك لضمان أصالة وصحة هذه المعلومات"

ومن زاوية تقنية، يشمل الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية.

ومن زاوية قانونية، فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوافر المعلومات ومكافحة أنشطة

الاعتداء عليها أو استغلال نظمها في ارتكاب جريمة، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم الحاسوب والإنترنت).

إذا فأمن المعلومات هو ممارسة حماية المعلومات في جميع أشكالها، سواء كانت مكتوبة أو منطوقة أو إلكترونية أو رسومية أو باستخدام طرق اتصال أخرى.

واستخدام مصطلح أمن المعلومات، وإن كان استخدامًا قديمًا سابقًا لولادة وسائل تكنولوجيا المعلومات، إلا أنه وجد استخدامه الشائع بل والفعلي، في نطاق أنشطة معالجة ونقل البيانات بوساطة وسائل الحوسبة والاتصال، إذ مع شيوع الوسائل التقنية لمعالجة وتخزين البيانات وتداولها والتفاعل معها عبر شبكات المعلومات، وتحديدًا الإنترنت، احتلت أبحاث ودراسات أمن المعلومات مساحة رحبة آخذة في النماء من بين أبحاث تقنية المعلومات المختلفة، بل ربما أمست أحد أهم الهواجس التي تؤرق مختلف الجهات.

أن أغراض أبحاث واستراتيجيات ووسائل أمن المعلومات، سواء من الناحية التقنية أو الأدائية، وكذلك هدف التدابير التشريعية في هذا

الحقل، هو ضمان توافر العناصر التالية لأي معلومات يراد توفير الحماية الكافية لها:

- **السرية أو الموثوقية:** وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.
- **التكاملية وسلامة المحتوى:** وتعني التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث بع، وبشكل خاص لن يتم تدمير المحتوى أو تغييره أو العبث به في أي مرحلة من مراحل المعالجة أو التبادل، سواء في مرحلة التعامل الداخلي (معلومات) أو عن طريق تدخل غير مشروع.
- **استمرارية توافر المعلومات أو الخدمة:** وتعني التأكد من استمرار عمل النظام المعلوماتي، واستمرار القدرة على التفاعل مع المعلومات، وتقديم الخدمة لمواقع المعلوماتية وأن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها.

٣/التطور التاريخي لمفهوم أمن المعلومات:

لكي نتمكن من استيعاب أكثر لمفهوم أمن المعلومات لابد من استعراض السياق التاريخي لتطور هذا المفهوم.

لقد ظل هذا المجال من الأمن حتى أواخر السبعينيات معروفاً باسم أمن الاتصالات (Communication Security COMSEC) والذي حددته توصيات أمن أنظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة بما يلي:

"المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات".

تضمنت النشاطات المحددة لأمن الاتصالات COMSEC أربعة أجزاء هي: أمن التشفير Crypto security ، أمن النقل Transmission Security، أمن الإشعاع Emission Security والأمن الفيزيائي Physical Security. كما تضمّن تعريف أمن الاتصالات خاصيتين تتعلقان بموضوع هذه الوحدة: السرية والتحقق من الهوية.

١-١ **السرية** Confidentiality:

التأكيد بأن المعلومات لم تصل لأشخاص، عمليات أو أجهزة غير مخولة بالحصول على هذه المعلومات(الحماية من إفشاء المعلومات غير المرخص).

١-٢ التحقق من الهوية:

إجراء أمني للتأكد من صلاحية الاتصال، الرسالة أو المصدر أو وسيلة للتحقق من صلاحية شخص ما لاستقبال معلومات ذات تصنيف محدد(أو التحقق من مصدر هذه المعلومات).

وبدأت في الثمانينات مع النمو المضطرد للحاسبات الشخصية حقبة جديدة من الأمن: أمن الحواسيب (Computer Security COMPUSEC) والتي حددتها توصيات أمن أنظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة بما يلي:

"المعايير والإجراءات التي تضمن سرية، كمال وتوفر مكونات أنظمة المعلومات بما فيها التجهيزات، البرمجيات، البرمجيات المدمجة Firmware والمعلومات التي تتم معالجتها، تخزينها ونقلها". وتضمن أمن الحواسيب الشخصية خاصيتين إضافيتين تتعلقان بموضوع هذه الوحدة: الكمال والتوفر.

١-٣ الكمال Integrity:

تعكس جودة أي نظام للمعلومات مدى صحة وموثوقية نظام التشغيل، التكامل المنطقي للتجهيزات والبرمجيات التي توفر آليات الحماية ومدى تناغم بني المعلومات مع البيانات المخزنة.

١-٤ **التوفر** Availability:

الوصول الموثوق إلى البيانات وخدمات المعلومات عند الحاجة إليها من قبل الأشخاص المخولين بذلك.

لاحقاً وفي التسعينات من القرن الماضي تم دمج مفهومي الأمن(أمن الاتصالات وأمن الحواسيب) لتشكيل ما أصبح يعرف باسم(أمن أنظمة المعلومات Information Systems Security- INFOSEC).

يتضمن مفهوم أمن أنظمة المعلومات الخصائص الأربعة المعروفة مسبقاً ضمن مفاهيم أمن الاتصالات وأمن الحواسيب: السرية، التحقق من الهوية، الكمال والتوفر، كما أضيف إليها خاصية جديدة: مكافحة الإنكار.

١-٥ **مكافحة الإنكار (المسئولية)** Non-repudiation:

التأكيد بأن مرسل البيانات قد حصل على إثبات بوصول البيانات إلى المرسل إليه وبأن المستقبل قد حصل على إثبات لشخصية المرسل مما يمنع احتمال إنكار أي من الطرفين بأنه قد عالج هذه البيانات.

٤/ تحديات أمن المعلومات:

إن التحديات الستة الأهم التي تواجه أمن المعلومات في وقتنا الراهن كما وردت في كتاب "المرشد التنفيذي لأمن المعلومات، المخاطر والتحديات والحلول" تأليف "مارك إيفن"، تتمثل في:

١- التجارة الإلكترونية:

أضحت شبكة الإنترنت مصدرًا هامًا للقيام بأعمال التجارة الإلكترونية، حيث وفر هذا المصدر عديدًا من الأساليب للشركات لتسويق منتجاتها وخدماتها، بعد أن كان التواصل مع العملاء على مدار الساعة في الماضي القريب حكرًا على الشركات الكبيرة فقط، أما الآن وبما ينتجه الإنترنت فقد أصبح في مقدور الشركات الصغيرة المحدودة الموارد أيضًا التواصل مع عملائها ٢٤ ساعة في اليوم، وعلى مدار الأسبوع عبر مواقعها على الشبكة. وقد أصبح وجود مواقع للشركات على الإنترنت ضرورة حتمية لاستمرار الشركات في العمل، وليس من الكماليات، وذلك بسبب رغبات العملاء وتوسع استخدامهم للإنترنت لقضاء حاجاتهم. ومع الإمكانات العديدة المتطورة التي تتيحها التجارة الإلكترونية عبر الإنترنت، خلقت مصاعب جديدة للشركات، والتي يجب التغلب عليها للنجاح والاستمرار في تقديم خدماتها ومنتجاتها عبر الإنترنت، ومن أمثلة تلك المصاعب:

- هناك ضغوط كبيرة على الشركات للتحول سريعًا للتجارة الإلكترونية، لأخذ السبق وكسب أكبر شريحة من العملاء.
- إتاحة الاطلاع على المعلومات الدقيقة للمتصفحين والعملاء والشركات، أصبحت ضرورة.
- يجب أن تقدم الشركات خدماتها بطريقة سهلة وآمنة في الوقت نفسه.
- يفترض أن تكون الأنظمة متاحة على مدار الساعة وطوال العام.

هذه التحديات وضعت متطلبات كبيرة على إدارة تقنية المعلومات، حيث إن تقديم أنظمة التجارة الإلكترونية بطريقة آمنة وآنية أمر صعب للغاية، ومع زيادة متطلبات العملاء زادت المتطلبات من الأنظمة والتقنيات والتأكد من أمنها.

٢- الزيادة مضطردة التعقيد في الهجمات على أمن المعلومات:

زادت هجمات الفيروسات على مواقع الشركات، وتحولت من حالات مزعجة إلى ضارة بعمليات هذه الشركات، وكانت الفيروسات سابقًا تصيب أجهزة محدودة، أما اليوم فإن آثارها تنعكس على غالبية الأجهزة المرتبطة بالشبكة العنكبوتية، مما يلحق خسائر مادية كبيرة بالشركات. وهذه المشكلة لا يمكن التغاضي عنها، حيث إن هذه الهجمات تكلف

بلايين الدولارات كل عام، فعلى سبيل المثال كلف فيروس الحب (Love Bug)، مبلغ /٧٥،٨/ بليون دولار عام ٢٠٠٥م.

كما أن سرقة المعلومات الخاصة تعتبر أيضًا من مخاطر أمن المعلومات الهامة، فعندما تكون حقوق الملكية الفردية موجودة في صيغة إلكترونية ومخزنة على الحاسب الآلي، فمن السهل سرقتها، وهذه تسبب أرقًا كبيرًا ومعضلة عظيمة للمحافظة على أسرار الشركات التجارية والصناعية منها. وهناك ثلاثة أمور مهمة دعت للزيادة في حالات أمن المعلومات، هي:

- زيادة في أعداد إمكانية التعرض لمخاطر أمن المعلومات.
- العمل المعتمد بشكل كبير على العامل البشري في التعامل مع مخاطر أمن المعلومات.
- زيادة تعقيد الهجمات على أمن المعلومات.

٣- عدم نضج منتجات أمن المعلومات:

- لا تزال أنظمة ومنتجات أمن المعلومات في مراحلها الأولية، نظرًا إلى قلة وجود مواصفات قياسية لمنتجات وخدمات أمن المعلومات. وهناك العديد من الشركات المنتجة لأنظمة أمن المعلومات، تختص بجزء معين ومحدود من متطلبات أمن المعلومات، مما نتج عنه صعوبة

وتحدٍ للعملاء في جعل تلك الحلول الجزئية تعمل مع بعضها البعض بشكل متكامل.

- فنية تقنية المعلومات، والتي تحتاج إلى وقت وجهد لفهمها وتحليلها، حيث إن كل نظام من أنظمة حماية وأمن المعلومات ينتج العديد من الإنذارات والسجلات الخاصة به، ويجب على المتخصصين بأمن المعلومات مراجعتها والتأكد من عدم وجود خلل فيها.
- القليل جدًا من هذه المعلومات (الإنذارات) قد تؤثر في أمن الشبكة، وبالتالي يكون خطرًا على أمن المعلومات، مما يجعل مهمة المسؤولين عن أمن المعلومات صعبة والإحاطة الكاملة ببيئة الأمن ووضع الخطط لمعالجة الأمور الخطيرة عسيرة.

٤- النقص الكبير في موظفي أمن المعلومات:

إيجاد الأشخاص الأكفاء المتخصصين في أمن المعلومات مهمة صعبة في الوقت الراهن والمستقبل القريب، ومما زاد صعوبة توافر المختصين في أمن المعلومات هو عدم نضج أنظمة وبرامج حماية المعلومات في الوقت الراهن، إضافة إلى المهارات المتعددة المطلوبة لحماية المعلومات. وبسبب عدم نضج منتجات حماية المعلومات، وقلة المواصفات القياسية أو انعدامها، وتعدد المنتجات الفردية التي تخدم

جانبًا واحدًا من جوانب أمن المعلومات، أصبح تدريب الفنيين في أمن المعلومات أمرًا صعبًا ومكلفًا.

كما أن توافر القوى العاملة المدربة تدريبًا كاملاً على جوانب أمن المعلومات المختلفة لم يتواءم مع الخطى المتسارعة لصناعة أنظمة وبرامج أمن وحماية المعلومات. ومع ازدياد التحديات لأمن المعلومات وزيادة التقنيات المطبقة، زاد العبء على الأشخاص المسؤولين عن أمن المعلومات للتدريب والاستمرار في تعلم الطرق والممارسات الأفضل لحماية المعلومات، وهذا يترجم إلى زيادة الوقت والمبالغ اللازمة للاستمرار في تدريب أفراد أمن المعلومات على المنتجات المتاحة. قد لا يكون المبلغ اللازم لإيجاد أفراد أمن معلومات وتدريبهم هو المشكلة الرئيسة لبعض الشركات ، لكن الوقت اللازم لتدريبهم والاستمرار في تدريبهم هو المشكلة التي تواجه الشركات كافة، وخاصة في ظل النقص الحاد في أفراد أمن المعلومات.

٥- التشريعات الحكومية والنظم الصناعية:

زيادة الاعتماد على الإنترنت، وحوادث أمن المعلومات التي ازدادت في السنوات الأخيرة، حدت بالحكومات إلى عمل تشريعات إضافية لتنظيم بيئة الأنظمة، وشملت تلك التشريعات محاور عدة، مثل:

معلومات العملاء الخاصة، وتشريعات خاصة بمهن معينة مثل الصحة، والخدمات المالية. ويمكن الدخول إلى الإنترنت والتعامل عن طريقها في أنحاء الكرة الأرضية كافة، وعليه، فليس من المهم تطبيق القوانين والتشريعات ذات العلاقة بأمن المعلومات في البلد الموجودة الشركات فيه، بل يجب أن تطبق التشريعات والقوانين الملزمة كافة في البلدان التي يوجد بها عملاء لتلك الشركات. وباختصار صار لزامًا على الشركات أن تطبق تشريعات بلدها وتشريعات بلدان العالم الأخرى الموجود فيها عملاء لها.

٦- <u>القوى العاملة المتحركة والحوسبة اللاسلكية:</u>

أثرت أجهزة الحاسب المتنقلة على نمط الحياة اليومية، فالاتصال اللاسلكي مكَّن الموظفين والعملاء من تقليل الاعتماد على الهاتف العادي للاتصال، فالبحث عن أقرب كابينة هاتف أو الذهاب للمكتب للاطلاع على البريد الإلكتروني صارت في اضمحلال، وخاصة بعد ظهور الهاتف الجوال وتصفح الإنترنت والبريد الإلكتروني عبر الأجهزة المحمولة المتصلة لاسلكيًا.

في الماضي كان هناك جهاز حاسب آلي في المكتب لأغراض العمل، وحاسب شخصي آخر في البيت للأعمال الشخصية، ويوجد

خط فاصل واضح بين الاثنين، لكن مع تطور وتوافر الأجهزة المحمولة صار الفصل بينهما في حكم المستحيل. وأصبحت حماية أجهزة المكتب تتم مركزيًا عن طريق الشركة، لكن من الصعب حماية ومراقبة والتحكم بالأجهزة المحمولة والتي قد تحوي معلومات حساسة ومهمة للشركة، مما قد نتج عنه أساليب وممارسات جديدة لضمان أمن المعلومات على هذه الأجهزة المحمولة، والتي تعد بطبيعتها أكثر تعقيدًا وصعوبة لحمايتها مقارنة بالأجهزة المكتبية الثابتة.

والبعد الآخر، هو ظهور بروتوكولات جديدة ذات مواصفات قياسية تسهل تخاطب الأجهزة المحمولة مع بعضها البعض، مما سهل الاتصال بين أجهزة الأفراد المحمولة مثل: أجهزة الجوال، وأجهزة الحاسب المحمولة. وهذه البروتوكولات مثل: (بلوتوث، وآي فاي... إلخ)، فيها العديد من الثغرات الأمنية التي تسمح باختراق تلك الأجهزة بعلم أو من دون علم صاحبها، وهذه كارثة بالنسبة لمسؤولي أمن المعلومات، وخاصة إذا كانت تلك الأجهزة تحوي معلومات حساسة للشركة يتوجب معها حماية تلك الأجهزة النقالة على غرار حماية الأجهزة المكتبية في الشركة.

٥/اتجاه المخاطر والاعتداءات في البيئة المعلوماتية:

تطال المخاطر والاعتداءات في بيئة المعلومات أربعة مواطن أساسية هي مكونات تقنية المعلومات في أحداث تجلياتها:

- **الأجهزة:** وهي المعدات والأدوات المادية كافة التي تتكون منها النظم، كالشاشات، والطابعات ومكوناتها الداخلية، ووسائط التخزين المادية.
- **البرامج:** وهي الأوامر المرتبة في نسق معين لإنجاز الأعمال، وهي إمّا مستقلة عن النظام أو مخزنة فيه.
- **المعطيات:** وهي الدم الحي للأنظمة وما سيكون محلاً لجرائم الحاسب، وتشمل كل البيانات المدخلة، والمعلومات المستخرجة عقب معالجتها، وتمتد بمعناها الواسع للبرمجيات المخزنة داخل النظام، وقد تكون المعطيات في طور الإدخال أو الإخراج أو التخزين أو التبادل بين النظم عبر الشبكات، وقد تختزن داخل النظم على وسائط التخزين وخارجه.
- **الاتصالات:** وتشمل شبكات الاتصال التي تربط الأجهزة التقنية بعضها مع بعض محليًا ونطاقيًا ودوليًا، وتتيح فرصة اختراق النظم عبرها، كما أنها بذاتها محل للاعتداء، وموطن من مواطن الخطر الحقيقي.

٦/عمليات المعلومات الرئيسة المتصلة بأمن المعلومات:

تتعدد عمليات التعامل مع المعلومات في بيئة النظم وتقنيات المعالجة والاتصال وتبادل البيانات، ولكن يمكن بوجه عام تحديد العمليات الرئيسة التالية:

٦-١ تصنيف المعلومات Information Classification:

وهي عملية أساسية لدى بناء أي نظام أو في بيئة أي نشاط يتعلق بالمعلومات وتختلف التصنيفات حسب المنشأة مدار البحث، فمثلاً قد تصنف المعلومات إلى معلومات متاحة، وموثوقة، وسرية، وسرية للغاية أو قد تكون معلومات متاح الوصول إليها وأخرى محظور التوصل إليها وهكذا.

٦-٢ التوثيق Documentation:

وتتطلب عمليات المعلومات أساساً إتباع نظام توثيق خطي لتوثيق بناء النظام وكافة وسائل المعالجة والتبادل ومكوناتها. وبشكل رئيس فإن التوثيق لازم وضروري لنظام التعريف والتخويل، وتصنيف المعلومات، والأنظمة التطبيقية. وفي أطار الأمن، فإن التوثيق يتطلب أن تكون استراتيجية أو سياسية الأمن موثقة ومكتوبة وأن تكون إجراءاتها ومكوناتها كاملة محل توثيق، إضافة إلى خطط التعامل مع المخاطر

والحوادث، والجهات المسئولية ومسئولياتها وخطط التعافي وإدارة الأزمات وخطط الطوارئ المرتبطة بالنظام عند حدوث الخطر.

٦-٣ المهام والواجبات الإدارية والشخصية:

Administration and Personnel Responsibilities

إن مهام المتصلين بنظام أمن المعلومات تبدأ في الأساس من حسن اختيار الأفراد المؤهلين وعمق معارفهم النظرية والعملية، على أن يكون مدركاً أن التأهيل العملي يتطلب تدريباً متواصلاً ولا يقف عند حدود معرفة وخبرة هؤلاء لدي تعيينهم، وبشكل رئيس فأن المهام الإدارية أو التنظيمية تتكون من خمسة عناصر أو مجموعات رئيسة: تحليل المخاطر، وضع السياسة أو الاستراتيجية، وضع خطة الأمن، وضع البناء التقني الأمني- توظيف الأجهزة والمعدات والوسائل، وأخيرا تنفيذ الخطط والسياسات.

٦-٤ وسائل التعريف والتأكد من المستخدمين وحدود صلاحيات الاستخدام:

:Identification and Authorization

إن الدخول إلى أنظمة الكمبيوتر وقواعد البيانات ومواقع المعلوماتية عموما، يمكن تقيده بالعديد من وسائل التعرف على شخصية المستخدم

وتحديد نطاق الاستخدام، وهو ما يعرف بأنظمة التعريف والتخويل Identification and Authorization systems. والتعريف أو الهوية مسألة تتكون من خطوتين، الأولى وسيلة التعريف على شخص المستخدم، والثانية قبول وسيلة التعريف أو ما يسمى التوثق من صحة الهوية المقدمة.

ووسائل التعريف تختلف تبعاً للتقنية المستخدمة، وهي نفسها وسائل أمن الوصول إلى المعلومات أو الخدمات في قطاعات استخدام النظم أو الشبكات أو قطاعات الأعمال الإلكترونية، وبشكل عام، فإن هذه الوسائل تتوزع إلى ثلاث أنواع:

- شيء ما يملكه الشخص مثل البطاقة البلاستيكية أو غير ذلك.
- شئ ما يعرفه الشخص مثل كلمات السر أو الرمز أو الرقم الشخصي غير ذلك.
- شيء ما يرتبط بذات الشخص أو موجود فيه مثل بصمة الأصبع أو بصمة العين والصوت وغيرها.

وتعد وسائل التعريف والتوثق الأقوى، تلك الوسائل التي تجمع بين هذه الوسائل جميعاً على نحو لا يؤثر على سهولة التعريف وفعاليته في ذات الوقت.

٦-٥ سجل الأداء Logging:

تحتوي مختلف أنواع الكمبيوترات نوعا ما من السجلات التي تكشف استخدامات الجهاز وبرمجياته والنفاذ إليه، وهي ما يعرف بسجلات الأداء أو سجلات النفاذ إلى النظام، تتخذ سجلات الأداء أهمية استثنائية في حال تعدد المستخدمين وتحديداً في حالة شبكات الكمبيوتر التي يستخدم مكوناتها أكثر من شخص، وفي هذه الحالة تحديداً، أي شبكات المستخدمين، فإن هناك أكثر من نوع من أنواع سجلات الأداء وتوثيق الاستخدامات، كما أن سجلات الأداء تتباين من حيث نوعها وطبيعتها وغرضها، فهناك سجلات الأداء التاريخية والسجلات المؤقتة، وسجلات التبادل وسجلات النظام وسجلات الأمن وسجلات قواعد البيانات والتطبيقات وسجلات الصيانة أو ما يعرف بسجلات الأمور التقنية وغيرها.

٦-٦ **عمليات الحفظ** Back-up:

وعمليات الحفظ تتعلق بعمل نسخة إضافية من المواد المخزنة على إحدى وسائط التخزين سواء داخل النظام أو خارجه، وتخضع عمليات الحفظ لقواعد يتعين أن تكون محددة سلفاً وموثقة ومكتوبة ويجري الالتزام بها لضمان توحيد معايير الحفظ وحماية النسخ الاحتياطية.

ويمثل وقت الحفظ، وحماية النسخة الاحتياط، ونظام الترقيم والتبويب، وآلية الاسترجاع والاستخدام، ومكان الحفظ وآمنة، وتشفير النسخ التي تحتوي معطيات خاصة وسرية، مسائل رئيسة يتعين اتخاذ معايير واضحة ومحددة بشأنها.

٦-٧ وسائل الأمن الفنية ونظام منع الاختراق:

تتعدد وسائل الأمن التقنية المتعين استخدامها في بيئة الكمبيوتر والانترنت، كما تتعدد أغراضها ونطاقات الاستخدام وتتخذ الجدران النارية Firewalls، إضافة للتشفير Cryptography، وكذلك نظم التحكم في الدخول ونظام تحري الاختراق Intrusion Detection Systems (IDS)، وأنظمة وبرمجيات مقاومة الفيروسات أهمية متزايدة، لكنها لا تمثل جميعها وسائل الأمن المستخدمة، بل هي إضافة لوسائل التعريف والتوثيق المتقدم الإشارة إليها تمثل أهم وسائل الأمن التقنية في الوقت.

٦-٨ نظام التعامل مع الحوادث Incident Handling system:

بغض النظر عن حجم وسائل الأمن التقنية المستخدمة، ومعايير الأمن وإجراءاته المتبعة، فإنه لابد من توفر نظام متكامل للتعامل مع

المخاطر والحوادث والاعتداءات، ويعدو متطلباً رئيساً بالنسبة لمؤسسات الأعمال كما في حالة البنوك والمؤسسات المالية.

وأول ما يتعين إدراكه في هذا الصدد أن التعامل مع الحوادث عملية وليست مجرد مشروع أو خطوة واحدة، بمعنى أنها عملية متكاملة تتصل بأداء متواصل متدرج خاضع لقواعد محددة سلفاً ومتبعة بدقة وانضباط، ومتى ما تم التعامل مع الحوادث على أنها مجرد حالة تنشأ عند الحادث كنا أمام حالة قصور تمثل بذاتها أحد عناصر الضعف في نظام الأمن.

وتختلف مكونات ومراحل وخطوات نظام التعامل مع الحوادث من مؤسسة إلى أخرى تبعاً لعوامل عديدة تتعلق بطبيعة الأخطار التي أظهرتها عملية تحليل المخاطر وما أظهرته استراتيجية الأمن الموضوعة في المؤسسة، وتبعا للنظام محل الحماية، إذ تتباين خطوات ومحتوى وعناصر خطط التعامل مع الحوادث لدى بنوك الانترنت مثلا عنها لدى المواقع المعلوماتية، ومع ذلك، وبوجه عام، فإن نظام التعامل مع الحوادث يتكون عادة من ستة مراحل(خطوة فخطوة) هي: الإعداد المسبق والتحري والملاحظة الاحتواء والاستئصال، والتعافي والعودة للوضع الطبيعي، والمتابعة.

الفصل الثاني

أمن المعلومات

التهديدات وسبل الحماية

مقدمة:

استطاع الإنسان على مرِّ العصور أن يسخر الطاقات المحيطة به في سبيل حياة أفضل، ومع ما حققه من تقدم في مجالات متعددة، ظل تسهيل أمور حياته هدفًا رئيسًا يحرص على تحقيقه بشتى الوسائل، فبعد أن حقق الترابط بين تقنية الحواسيب المتطورة وتقنية الاتصالات المتقدمة تمكن من بلوغ عصر المعرفة، وأدخلها في صميم أنشطته الحياتية كافة، فأصبحت لديه القدرة على الاتصال والتواصل مع الآخرين أينما كانوا، وتيسرت له إمكانية الحصول على المعلومات التي يريد في وقت قصير.

وإذا كانت إنجازات العصور السابقة قد أسهمت في انتقال البشرية من وضع اجتماعي ومادي إلى وضع آخر أكثر تقدمًا ورقيًا، فإن تقنية المعلومات باعتبارها إحدى أهم منجزات هذا العصر تشكل إحدى أهم القوى التي تدفع المجتمعات الإنسانية إلى التطور القائم على المعرفة والمعلوماتية، حيث فتحت الأبواب أمام إمكانية تناقل كميات هائلة من البيانات والمعلومات عبر مسافات جغرافية متباعدة بسرعة فائقة، وهو ما جعلها إحدى البنى الأساسية لاقتصاديات الدول جميعًا، المتقدمة منها والنامية، وإحدى المحركات الأساسية لنمو ودفع عجلة الاقتصاد

فيها، ورفع كفاءتها وفاعليتها وإنتاجيتها. وبقدر ما تحفل به تقنية المعلومات من أهمية كبرى في تطوير المجتمعات في مجالات شتى.

إلا أنها في الوقت نفسه لا تخلو من السلبيات، التي قد يكون لها الأثر العكسي، خصوصًا في ظل تكاثر الاختراقات المتوقعة وتنوعها بين سرقة وابتزاز وأعمال تجسس، بيد أن الجانب الأخطر يتمثل في محاولات الاختراق التي تستدعي بذل اهتمام خاص لقضية أمن المعلومات، ولاسيما أن الثورة المعلوماتية أحدثت ثورة إدارية لدى الحكومات والهيئات والمؤسسات على مستوياتها كافة، من خلال الدخول في مرحلة تغيير جذرية لتطوير المفاهيم وأساليب العمل بين بعضها البعض، أو بينها وبين المواطنين، أو بينها وبين مؤسسات وأفراد خارج الحدود الدولية، بحيث بات من المؤكد أن تشهد الفترة المقبلة توسعًا كبيرًا وتطورًا هائلاً في نطاق الحكومة الإلكترونية، كما نتج عن ثورة المعلومات اقتصاد جديد يسمى "الاقتصاد الرقمي". وهو يرتكز على الاستخدام الفعّال لخدمات الاتصالات والمعلوماتية في جميع الأنشطة.

الأمر الذي يفرض ضرورة وجود منظومة أمنية متكاملة للتعامل الآمن عبر الحاسب الآلي، بحيث تضمن التحقق من هوية المستخدمين، وسرية البيانات وسلامتها، والقدرة على التحقق من صحة

الإجراءات. وبالإضافة إلى خطورة الاختراقات على أعمال الإدارة والاقتصاد والمال، فقد لعبت أنشطة المخابرات وأعمال التجسس دورًا هامًا للحصول على المعلومات، حيث أصبحت تعتمد على اختراق نظم المعلومات لدى الآخرين، ففي عصر تقنية المعلومات تحولت أنشطة المخابرات والتجسس إلى عمليات تقنية تعتمد على اختراق الأنظمة والشبكات. ولما كانت معظم الدول تحتفظ بالوثائق السرية مخزنة بهيئة رقمية في مواقع سرية بعد تشفيرها، فإنه من الأهمية بمكان التأكيد على عدم كشف هذه المعلومات وسلامة محتواها من أي عبث، وهو ما لا يتحقق إلا من خلال أمن المعلومات، خصوصًا وأن حرب المعلومات أصبحت سمة مميزة للحرب الحديثة.

ولذلك وغيره من الأسباب، أصبح من الضرورة بمكان نشر الوعي بأهمية أمن المعلومات، والأمن الإلكتروني، من خلال توفير رؤية علمية وعملية ترصد التحديات والصعوبات وتجد الحلول المناسبة لها.

١/ شبكة الانترنت وتأثيرها على أمن المعلومات:

يعرف أحد الباحثين شبكة الانترنت على أنها أكبر آلة عرفتها البشرية لجمع ومعالجة ونقل البيانات، لذلك فهي تعد أكبر ساحة لحرب المعلومات، فمنها يمكن الحصول على المعلومات والبيانات الشخصية

للأفراد، وأحيانا بعض البيانات المالية المهمة التي قد تستخدم لاحقا لأغراض معينة.

فمن خلالها يمكن للشركات وبعض المؤسسات البحثية أن تتبع عمليات الشراء التي يقوم بها الأفراد، أو التحويلات المالية، وكذلك تتبع المواقع التي يزورها الأفراد والمواقع التي قاموا بالاشتراك أو التسجيل بها، وهي بالنسبة لغالبية مستخدمي الانترنت تعتبر معلومات عادية. ولكن المفاجئة الكبرى تأتي بعد أن تقوم تلك الجهات بإدخال هذه البيانات إلى قاعدة بيانات بعض البرامج الذكية التي تقوم بدورها بتجميع وتصنيف وتحليل هذه البيانات واستخلاص نتائج وحقائق عن تفاصيل حياة الفرد اليومية الدقيقة التي لا يرغب بنشرها ومعرفتها من قبل الآخرين.

إن أهم ما يميز شبكة الانترنت أنها لا تعترف بحدود وبالتالي فان المعلومات المتداولة عليها تتدفق عابرة لكل الحدود الشخصية المجتمعية والوطنية، وبالتالي فمن الممكن جدا أن يتم اختراق معلوماتك الخاصة من خلال هذه الشبكة.

وبما أن شبكة الانترنت تقوم بنقل وإتاحة معلومات عن جميع الأنشطة والمستويات الاجتماعية والتجارية والسياسية والثقافية

والاقتصادية عبر العالم الافتراضي، فقد رافقها توجه واسع لحماية خصوصية الأفراد والجماعات وبالتالي تأمين المعلومات في عالم الشبكات الدولية.

فكان لشبكة الانترنت الفضل الأكبر في اهتمام العالم بحماية وتأمين المعلومات، وعلى النقيض كان لها السبب الأكبر في انتهاكها.

٢/تصنيف الاعتداءات على البيئة المعلوماتية:

تنوعت وتعددت الجرائم المرتبطة والمرتكبة بوساطة المعلومات، وكل ما له علاقة بنظمها واستخداماتها، وقد تنوعت أساليب عرضها ومسمياتها من قبل الباحثين والكتَّاب والمعنيين بالمحافظة عليها وصيانتها من المتخصصين بعلم الحاسب الآلي والبرمجيات المختلفة، وعمومًا تصنف الاعتداءات في الحقل التقني على النحو التالي:

أولاً : خرق الحماية المادية:

- التفتيش في مخلفات التقنية Dumpster diving ويقصد به قيام المهاجم بالبحث في مخلفات المؤسسة من القمامة والمواد المتروكة بحثا عن أي شيء يساعده على اختراق النظام، كالأوراق المدون عليها كلمات السر، أو مخرجات الكمبيوتر التي قد تتضمن معلومات مفيدة، أو الأقراص الصلبة المرمية بعد استبدالها، أو غير

ذلك من المواد المكتوبة أو الأقراص أو الملاحظات أو أي أمر يستدل منه على أية معلومة تساهم في الاختراق.

- الالتقاط السلكي Wiretapping: والمقصود هنا ببساطة التوصل السلكي المادي مع الشبكة أو توصيلات النظام لجهة استراق السمع أو سرقة والاستيلاء على المعطيات المتبادلة عبر الأسلاك، وهي أنشطة تتم بطرق سهلة أو معقدة تبعا لنوع الشبكة وطرق التوصل المادي.
- استراق الأمواج Eavesdropping on Emanations: ويتم ذلك باستخدام لواقط تقنية لتجميع الموجات المنبعثة من النظم باختلاف أنواعها كالتقاط موجات شاشات الكمبيوتر الضوئية أو التقاط الموجات الصوتية من أجهزة الاتصال.
- انكسار أو إلغاء الخدمة Denial or Degradation of Service: والمقصود هنا الأضرار المادي بالنظام لمنع تقديم الخدمة، أما أن كنا نتحدث عن إنكار الخدمة مثلا على مواقع الإنترنت فإن ذلك يتم عبر تقنيات مختلفة، كضخ الرسائل البريدية الإلكترونية دفعة واحدة لتعطيل النظام.

ثانيًا: خرق الحماية المتعلقة بالأشخاص وشؤون الموظفين:

تعد المخاطر المتصلة بالأشخاص والموظفين وتحديدًا المخاطر الداخلية منها واحدة من مناطق الاهتمام العالمي لدى جهات أمن المعلومات، إذ ثمة فرصة لأن يحقق أشخاص من الداخل ما لا يمكن نظريًا أن يحققه أحد من الخارج، وتظل أيضًا مشكلة صعوبة كشف مثل هؤلاء قائمة، إن لم يكن ثمة نظام أداء وصلاحيات يتيح ذلك، وعمومًا ثمة مسميات وطوائف عديدة لهذه المخاطر، أبرزها:

- التخفي بانتحال صلاحيات شخص مفوض Masquerading: والمقصود هنا الدخول إلى النظام عبر استخدام وسائل التعريف العائدة لمستخدم مخول بهذا الاستخدام، كالاستغلال كلامة سر أحد المستخدمين واسم هذا المستخدم، أو عبر استغلال نطاق صلاحيات المستخدم
- الهندسة الاجتماعية Social Engineering ويصنف هذا الأسلوب ضمن الحماية المادية أحيانا ويرجع إلى أنشطة الحصول على معلومات تهيئ الاقتحام من خلال علاقات اجتماعية وذلك باستغلال الشخص أحد عناصر النظام–أشخاصه– بإيهامه بأي أمر يؤدي إلى حصول هذا الشخص على كلمة مرور أو على أية معلومة تساعد في تحقيق.

- الازعاج والتحرش Harassment: وهي تهديدات يندرج تحتها أشكال عديدة من الاعتداءات والأساليب، ويجمعها توجيه رسائل الإزعاج والتحرش وربما التهديد والابتزاز أو في أحيان كثيرة رسائل المزاح على نحو يحدث مضايقة وإزعاجاً بالغين، وليست حكراً على البريد الإلكتروني بل تستغل مجموعات الحوار والأخبار والنشرات الالكترونية في بيئة الانترنت والويب.
- قرصنة البرمجيات Software Piracy وقرصنة البرامج تتحقق عن طريق نسخها دون تصريح أو استغلالها على نحو مادي دون تخويل بهذا الاستغلال، أو تقليدها ومحاكاتها والانتفاع المادي بها على نحو يخل بحقوق المؤلف، وهو نشاط يندرج في حقيقته ضمن طائفة الاعتداءات والمخاطر التي تستهدف البرمجيات عموما، وهو قطاع استقل بذاته من بين قطاعات جرائم الكمبيوتر.

ثالثًا: خرق الحماية المتصلة بالاتصالات والمعلومات بأنواعها المختلفة:

والمقصود بذلك الأنشطة التي تستهدف المعلومات والبرمجيات وتشمل طائفتين:

أ- **هجمات المعلومات:**

١) النسخ غير المصرح به للمعطيات Unauthorized Copying of Data: وهي العملية الشائعة التي تستتبع الدخول غير المصرح به للنظام، حيث يمكن الاستيلاء عن طريق النسخ على كافة أنواع المعطيات، وهنا تشمل البيانات والمعلومات والأوامر والبرمجيات وغيرها.

٢) **تحليل الاتصالات** Traffic Analysis: الفكرة هنا ببساطة أن الهجوم ينصب على دراسة أداء النظام في مرحلة التعامل ومتابعة ما يتم فيه من اتصالات وارتباطات بحيث يستفاد منها في تحديد مسلكيات المستخدمين وتحديد نقاط الضعف ووقت الهجوم المناسب وغير ذلك من مسائل يجمعها فكرة الرقابة على حركة النظام بغرض تيسير الهجوم عليه.

٣) القنوات المخفية Covert Channels: وهي عمليا صورة من صور اعتداءات التخزين، حيث يخفي المقتحم معطيات أو برمجيات أو معلومات مستولي عليها كأرقام بطاقات ائتمان في موضع معين من النظام، وتتعدد أغراض الإخفاء، فقد تكون تمهيداً لهجوم لاحق أو تغطية اقتحام سابق أو مجرد تخزين لمعطيات غير مشروعة.

ب- <u>هجمات البرمجيات: وتشمل:</u>

١) المصائد أو الأبواب الخلفية Trap Doors: الأبواب الخلفية ثغرة أو منفذ في برنامج يتيح للمخترق الوصول من خلاله إلى النظام، أنه ببساطة مدخل مفتوح تماماً كالباب الخلفي للمنزل الذي ينفذ منه السارق.

٢) الهجمات عبر التلاعب بنقل المعطيات عبر إنفاق النقل Tunneling: إنفاق النقل في الأصل طريقة تقنية مشروعة لنقل المعطيات عبر الشبكات غير المتوافقة، لكنها تصبح طريقة اعتداء عندما تستخدم حزم المعطيات المشروعة لنقل معطيات غير مشروعة.

٣) الهجمات الوقتية Timing attacks وهي هجمات تتم بطرق تقنية معقدة للوصول غير المصرح به إلى البرامج أو المعطيات، وتقوم جميعها على فكرة استغلال وقت تنفيذ الهجمة متزامنا مع فواصل الوقت التي تفصل العمليات المرتبة في النظام، وتضم في نطاقها العديد من الأساليب التقنية لتنفيذ الهجوم، منها إساءة استغلال الأوضاع أو الأنماط العادية للأداء والكيفية في النظام Race conditions والهجمات غير المتزامنة أو غير المتوافقة المتصلة باستغلال ترتيب تنفيذ العمليات الاعتيادية Asynchronous attacks.

٤) البرمجيات الخبيثة Malicious Code كالفيروسات Viruses وحصان طروادة Trojan Horses والدودة الإلكترونية Warms والسلامي salamis والقنابل المنطقية Logic Bombs: الجامع المشترك بين هذه البرمجيات أنها برمجيات ضارة تستغل للتدمير سواء تدمير النظام أو البرمجيات أو المعطيات أو الملفات أو الوظائف أو تستثمر للقيام بمهام غير مشروعة كإنجاز احتيال أو غش في النظام، والحقيقة أنها ليست تسميات مترادفة للفيروسات الشائعة.

رابعًا: الهجمات والمخاطر المتصلة بعملية الحماية:

وإذا ما أردنا أن نوصف المخاطر المتصلة بعمليات الحماية ذاتها ربما نكون في الحقيقة أمام كافة أنواع المخاطر والهجمات والاعتداءات، لكن من زاوية تقنية ضيقة، يشار إلى خمسة أنواع من الأساليب ضمن هذه الطائفة، بعضها يتصل بالهجمات التي تستهدف نظام أو استراتيجية الدخول، بعضها يستهدف نظام إدخال ومعالجة والبيانات، وبعضها يصنف كفعل أولى لتحقيق عمليات الدخول غير المصرح به إلى مختلف أنواع الشبكات، وسنشير بإيجاز إلى هذه الأساليب والاعتداءات:

١) العبث(الغش) بالبيانات Data Diddling: ويستهدف هذا الهجوم أو الاعتداء تغيير البيانات أو إنشاء بيانات وهمية في مراحل الإدخال أو الاستخراج، ويتم في الحقيقة بعشرات الأنماط والأساليب التقنية، جامعها المساح بأمن وحماية مرحلة إدخال البيانات أو استخراجها.

٢) خداع بروتوكول الإنترنت IP Spoofing(التخفي باستغلال بروتوكولات النقل): الحقيقة أن اصطلاح Spoofing لا يعني التخفي، فهو اصطلاح يتعلق بالغش والخداع والإيهام والتقليد والمحاكاة والسخرية، لكن استخدامه الشائع الآن يتعلق بهجمات فيروسات الانترنت، والفكرة هنا قريبة من فكرة التخفي التي عرضنا لها أعلاه عندما يتخذ شخص أو ينتحل صفة مستخدم آخر مخول بالاستخدام، لكن الفرق هنا، أننا نتحدث عن وسيلة تقنية بحتة، بحيث يقوم المهاجم عبر هذه الوسيلة بتزوير العنوان المرفق مع حزمة البيانات المرسلة بحيث يظهر للنظام–طبعا المعتمد في تبادل المعطيات على بروتوكولات النقل وأهمها هنا بروتوكولات الانترنت الأساسي– على أنه عنوان صحيح مرسل من داخل الشبكة، بحيث يسمح النظام لحزمة البيانات بالمرور باعتبارها حزمة مشروعة(إن جاز التعبير).

٣) تشمم كلمة السر(جمعها والتقاطها) Password Sniffing: وإذا كانت أنشطة الاعتداء التي تتم باستعمال كلمات السر كانت تتم غالبا فيما سبق عن طريق تخمين كلمات السر مستفيدة من ضعف الكلمات عموما وشيوع اختيار الأفراد لكلمات سهلة تتصل بمحيطهم الأسري أو محيط العمل أو حياتهم الشخصية، فإن الجديد استخدام برمجيات يمكنها تشمم أو التقاط كلمات السر خلال تجوالها في جزء من الشبكة أو أحد عناصرها ومراقبتها ومتابعتها لحركة الاتصال على الشبكة، بحيث يقوم هذا البرنامج من حيث الأصل بجمع أول ١٢٨ بايت أو أكثر –مثلا– من كل اتصال بالشبكة التي تجري مراقبتها وتتبع حركة الاتصال عليها، وعندما يطبع المستخدم كلمة السر أو اسم المستخدم، فإن البرنامج(الشمام) يجمع هذه المعلومات وينسخها إضافة إلى أن أنواع من هذه البرامج تجمع المعلومات الجزئية وتعيد تحليلها وربطها معا كما تقوم بعضها بإخفاء أنشطة الالتقاط بعد قيامها بمهمتها.

٤) المسح والنسخ Scanning: وهو أسلوب يستخدم فيه برنامج(الماسح– Ware Dialer أو Demon Dialer Processes) الذي هو برنامج احتمالات يقوم على فكرة تغيير التركيب أو تبديل احتمالات المعلومة، ويستخدم تحديداً بشأن احتمالات كلمة السر أو

رقم هاتف الموديم أو نحو ذلك، وأبسط نمط فيه عندما تستخدم قائمة الاحتمالات لتغيير رقم الهاتف بمسح قائمة أرقام كبيرة للوصل إلى احدها الذي يستخدم موديم للاتصالات بالإنترنت، أو إجراء مسح لاحتمالات عديدة لكلمة سر للوصل إلى الكلمة الصحيحة التي تمكن المخترق من الدخول لنظام، ومن جديد فإن هذا أسلوب تقني يعتمد واسطة تقنية هي برنامج(الماسح) بدلا من الاعتماد على التخمين البشري.

٥) هجومات استغلال المزايا الإضافية Excess Privileges:
الفكرة هنا تتصل بواحد من أهم استراتيجيات الحماية، فالأصل أن مستخدم النظام–تحديداً داخل المؤسسة– محدد له نطاق الاستخدام ونطاق الصلاحيات بالنسبة للنظام، لكن ما يحدث في الواقع العملي أن مزايا الاستخدام يجري زيادتها دون تقدير لمخاطر ذلك أو دون علم من الشخص نفسه أنه يحظى بمزايا تتجاوز اختصاصه ورغباته، في هذه الحالة فإن أي مخترق للنظام لن يكون فقط قادرا على تدمير أو التلاعب ببيانات المستخدم الذي دخل على النظام من خلال اشتراكه أو عبر نقطة الدخول الخاصة به، أنه ببساطة سيتمكن من تدمير مختلف ملفات النظام حتى غير المتصلة

بالمدخل الذي دخل منه لأنه استثمر المزايا الإضافية التي يتمتع بها المستخدم الذي تم الدخول عبر مدخله.

٣/ المخاطر، التهديدات والاعتداءات وأساليبها:

إن الحدود بين الجريمة والفعل غير الأخلاقي تبدو غير واضحة المعالم في بيئة الكمبيوتر والانترنت، وتمييز وضبط هذه الحدود هو المسألة الجوهرية لتحديد متى يمكن أن يعد فعل ما جريمة من بين جرائم الكمبيوتر والانترنت أو أنه مجرد إساءة استخدام لا ينطوي على قصد جرمي وهي المسألة التي أحدثت جدلاً واسعاً في مطلع الستينات وحتى منتصف السبعينات وهي ذات الفترة التي شهدت ميلاد ظاهرة جرائم الكمبيوتر، ومن جديد يعود هذا الجدل بسبب شيوع استخدام الانترنت وما حملته من أنشطة جديدة لا يزال الخلاف قائماً حول ما إذا كانت جريمة أم أنها مجرد ممارسة غير مقبولة كسلوك أخلاقي لكنها لا ترقي إلى حد الجريمة.

إن غرض هذا التقديم محاولة تقديم تحديد منضبط للاصطلاحات المستخدمة في عالم جرائم الكمبيوتر والانترنت لجهة التمييز بين العديد من الاصطلاحات التي يجري الخلط بينها، فثمة فرق بين الجريمة الإلكترونية، الإرهاب الإلكتروني، حرب المعلومات، المخاطر،

الحوادث، نقاط الضعف، والأخطاء، الاختراقات، حرب المعلومات....وغيرها.

وفيما يلي عرض لبعض المصطلحات.

٣/١التهديد Threats:

ويعني الخطر المحتمل الذي يمكن أن يتعرض له نظام المعلومات وقد يكون شخصاً، كالمتجسس أو المجرم المحترف أو الهاكرز المخترق، أو شيئاً يهدد الأجهزة أو البرامج أو المعطيات، أو حدثاً كالحريق وانقطاع التيار الكهربائي والكوارث الطبيعية.

٣/٢نقاط الضعف أو الثغرات Vulnerabilities:

وتعني عنصر أو نقطة أو موقع في النظام يحتمل أن ينفذ من خلاله المعتدي أو يتحقق بسببه الاختراق فمثلاً يعد الأشخاص الذين يستخدمون النظام نقطة ضعف إذا لم يكن تدريبهم كافياً لاستخدام النظام وحمايته، وقد يكون الاتصال بالإنترنت نقطة ضعف مثلاً إذا لم يكن مشفراً. وقد يكون الموقع المكاني للنظام نقطة ضعف كأن يكون غير مجهز بوسائل الوقاية والحماية، وبالعموم فإن نقاط الضعف هي الأسباب المحركة لتحقيق التهديدات أو المخاطر. ويرتبط بهذا الاصطلاح اصطلاح وسائل الوقاية Countermeasures: وتعني

التكنيك المتبع لحماية النظام ككلمات السر والأقفال ووسائل الرقابة والجدران النارية وغيرها.

٣/٣المخاطر Risks:

فإنها تستخدم بشكل مترادف مع تعبير التهديد، مع أنها حقيقة تتصل بأثر التهديدات عند حصولها، وتقوم استراتيجية أمن المعلومات الناجحة على تحليل المخاطرة Risk analysis، وتحليل المخاطر هي عملية Process وليست مجرد خطة محصورة، وهي تبدأ من التساؤل حول التهديدات ثم نقاط الضعف وأخيرا وسائل الوقاية المناسبة للتعامل مع التهديدات ووسائل منع نقاط الضعف.

٣/٤الحوادث Incident:

فهو اصطلاح متسع يشمل المخاطر ويشمل الأخطاء، وهو بالمعني المستخدم في دراسات أمن المعلومات التقنية يشير إلى الأفعال المقصودة أو غير المقصودة، ويغطي الاعتداءات والأخطاء الفنية ويتعين أن يحمله على الحوادث غير المقصودة والتي قد تكون مخاطر بفعل الطبيعة ودون عامل قصدي أو تكون أخطاء فنية غير مقصودة.

٣/٥الهجمات Attacks:

فهو اصطلاح لوصف الاعتداءات بنتائجها أو بموضع الاستهداف، فنقول هجمات إنكار الخدمة، أو هجمات إرهابية، أو هجمات البرمجيات، أو هجمات الموظفين الحاقدة أو الهجمات المزاحية. ويستخدم كاصطلاح رديف للهجمات اصطلاح الاختراقات أو الإخلالات Breaches، وهو اصطلاح توصف به مختلف أنماط الاعتداءات التقنية، وبالتالي يكون مرادفاً أيضاً للاعتداءات.

٣/٦اختراق الشبكات Hacking:

هو الوصول إلي البرامج والملفات والبيانات وغيرها بهدف التخريب أو السرقة أو التلاعب في محتويات نظام معين، ويكون ذلك من خلال ثغرات في نظام الحماية الخاص بالهدف.

٣/٧الهندسة الاجتماعيةSocial Engineering :

ويقصد بها مختلف الوسائل المستخدمة للحصول علي المعلومات الحساسة وتجاوز الأنظمة الأمنية من خلال استغلال نقاط ضعف العنصر البشري. حيث يستخدم المخترق مجموعة من الخدع النفسية من شأنها خداع المستخدم وتحفيزه علي الإفصاح عن بيانات سرية من خلال طرح أسئلة بهدف جمع معلومات دون إثارة أي شبهه ويطلق عليها أيضا(فن اختراق العقول).

٣/٨التصيد Phishing:

هو عبارة عن عملية احتيالية يتم فيها الحصول علي معلومات شخصية أو معلومات سرية كمعلومات بطاقات الائتمان أو اسم المستخدم أو كلمة المرور عن طريق الإيهام بأنه كيان يمكن الوثوق فيه في البيئة الرقمية.

٣/٩البرمجيات الضارة Malware:

وهي كل برنامج يدخل في النظام ويكون عمله ضاراً. وبالنسبة لأنواع البرامج الضارة فقد قسمها أستاذ أمن المعلومات مارتينيز توريس Martinez إلي ثلاث فئات رئيسة من حيث الاعتماد علي كيفية انتشارها عبر شبكات الإنترنت وهي الفيروسات واحصنة طروادة والديدان.

٣/١٠برامج التجسسSpyware:

وهي نوع من البرمجيات الخبيثة التي تتوافر فيها الأغراض غير الشرعية فهي تعمل علي مراقبة كل ما يكتبه الضحية حتي أنها تسجل النقرات علي لوحة المفاتيح وترسلها إلي المخترق.

٤/مستوى الحماية المطلوبة لأمن المعلومات:

٤/١مستوى الحماية المطلوبة:

لم تعد الشركات مهددة فقط بالمنافسين وسرعة التغيرات، وإنَّما أيضًا بمحترفي الجرائم المعلوماتية، والهواة من المخترقين الذين تتزايد مظاهرهم، وأشكال الأضرار التي يلحقونها بالأعمال الإلكترونية، وهو ما يستوجب عملية الحماية، إلا أنه ليست كل المعلومات تتطلب السرية وضمان عدم الإفشاء، وليست كل المعلومات في منشأة واحدة بالأهمية ذاتها من حيث الوصول لها أو ضمان عدم العبث بها، لهذا تنطلق خطط أمن المعلومات من تحديد المعلومات من حيث أهمية الحماية. وبعد تحديد درجة أهمية الحماية تجد كل منشأة وكل هيئة طريقتها الخاصة في توفير الأمن من المخاطر محل التهديد، بحيث لا تكون إجراءات الأمن رخوة ضعيفة لا تكفل الحماية، وبالمقابل لا تكون مبالغًا فيها إلى حد يؤثر على عنصر الأداء في النظام محل الحماية.

٢/٤أهم أدوات ووسائل حماية أمن المعلومات:

وسائل أمن المعلومات هي مجموعة من الآليات والإجراءات والأدوات والمنتجات التي تستخدم للوقاية من أو تقليل المخاطر والتهديدات التي تتعرض لها الكمبيوترات والشبكات وبالعموم نظم المعلومات وقواعدها.

وكما أوضحنا، فإن وسائل الأمن متعددة من حيث الطبيعة والغرض، لكن يمكننا بشكل أساسي تصنيف هذه الوسائل في ضوء غرض الحماية إلى الطوائف التالية:

١) مجموعة وسائل الأمن المتعلقة بالتعريف بشخص المستخدم وموثوقية الاستخدام ومشروعيته Identification and authentication، وهي الوسائل التي تهدف إلى ضمان استخدام النظام أو الشبكة من قبل الشخص المخول بهذا الاستخدام، وتضم هذه الطائفة كلمات السر بأنواعها، والبطاقات الذكية المستخدمة للتعريف، ووسائل التعريف البيولوجية التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي، ومختلف أنواع المنتجات التي تزود كلمات سر آنية أو وقتية متغيرة الكترونياً، والمفاتيح المشفرة، بل تضم هذه الطائفة ما يعرف بالأقفال الإلكترونية التي تحدد مناطق النفاذ.

٢) مجموعة الوسائل المتعلقة بالتحكم بالدخول والنفاذ إلى الشبكة Access Control وهي التي تساعد في التأكد من أن الشبكة ومصادرها قد استخدمت بطريقة مشروعة، وتشمل من بين ما تشمل الوسائل التي تعتمد على تحديد حقوق المستخدمين، أو قوائم أشخاص المستخدمين أنفسهم، أو تحديد المزايا الاستخدامية أو غير

ذلك من الإجراءات والأدوات التي تتيح التحكم بمشروعية استخدام الشبكة ابتداءً.

٣) مجموعة الوسائل الهادفة لحماية التكاملية(سلامة المحتوى) Data and Massage Integrity وهي الوسائل المناط بها ضمان عدم تعديل محتوى المعطيات من قبل جهة غير مخولة بذلك، وتشمل من بين ما تشمل تقنيات الترميز والتوقيع الإلكترونية وبرمجيات تحري الفيروسات وغيرها.

٤) مجموعة الوسائل المتعلقة بمنع الإنكار(إنكار التصرفات الصادرة عن الشخص) Non-repudiation، وتهدف هذه الوسائل إلى ضمان عدم قدرة شخص المستخدم من إنكار أنه هو الذي قام بالتصرف، وهي وسائل ذات أهمية بالغة في بيئة الأعمال الإلكترونية والتعاقدات على الخط، وترتكز هذه الوسائل حالياً على تقنيات التوقيع الإلكتروني وشهادات التوثيق الصادرة عن طرف ثالث.

٥) وسائل مراقبة الاستخدام وتتبع سجلات النفاذ أو الأداء(الاستخدام) Logging and Monitoring، وهي التقنيات التي تستخدم لمراقبة العاملين على النظام لتحديد الشخص الذي قام

بالعمل المعين في وقت معين، وتشمل كافة أنواع البرمجيات والسجلات الإلكترونية التي تحدد الاستخدام.

وفيما يلي أهم وسائل الحماية، والأخطاء الواجب تلافيها:

- **<u>برمجيات كشف ومقاومة الفيروسات:</u>**

بالرغم من أن تقنيات مضادات الفيروسات تعد الأكثر انتشاراً وتعد من بين وسائل الأمن المعروفة للعموم، إلا أنها حجم تطبيق هذه التقنيات واستراتيجيات وخطة التعامل معها تكشف عن ثغرات كبيرة وعن أخطاء في فهم دور هذه المضادات، وبالعموم ثمة خمسة آليات أساسية لكيفية تحري هذه المضادات للفيروسات التي تصيب النظام، كما ثمة قواعد أساسية تحقق فعالية هذه الوسائل والتي تعتمد في حقيقتها على الموازنة ما بين ضرورات هذه التقنيات لحماية النظام وما قد يحدثه الاستخدام الخاطئ لها من تأثير على الأداء وفعالية النظام.

- **<u>حواجز العبور (جدار النار):</u>**

هذا الجدار في الواقع هو عبارة عن أسلوب لحماية ومراقبة البيانات والملفات والنظم الداخلية للمؤسسة أو الدائرة وشبكة الإنترنت، أو بين الشبكتين، وهذه الجدران تستخدم للحد من دخول

المتطفلين والعابثين، أو بالأحرى منعهم من تسريب معلومات غير مرغوب فيها أو برمجيات سيئة. وفي الوقت نفسه تحمي المعلومات المهمة والأساسية المتعلقة بأهداف وعمل وإجراءات وخدمات وأنشطة المؤسسة، وذلك من خلال منع خروجها، فهي جدار سميك ومنظم للحماية.

- **التشفير:**

يعرف بأنه عملية تغيير مظهر وشكل المعلومات لإخفاء معناها الحقيقي عن طريق تحويل شكل البيانات لكي تكون غير مفهومة لمن يحاول التلصص عليها، أو هي عملية تحويل النص المكتوب أو المفهوم والواضح للناس إلى رموز، وهو وسيلة لاستبدال أي مستند أو وثيقة مقروءة ومفهومة إلى شكل وضعية لا يمكن معرفة وفهم محتواها، لكونها تحولت من شكل حر ومقروء إلى شكل مرمز يمكن قراءته ولا يمكن فهمه. ويهدف التشفير للتغلب على معدات أمن المعلومات، مثل: الاطلاع على المعلومات المحظورة، وتأخير إيصال بعض الرسائل، وتغيير وتسوية محتويات الرسائل المتبادلة، وانتحال شخصية المستخدم الحقيقي، وإدخال رسائل زائفة ضمن الرسائل الحقيقية، وتغيير كلمة السر الخاصة بالمستفيدين وغير ذلك من المخاطر.

- **تلافي الأخطاء:**

يرتكب الموظفون أخطاء فاحشة وساذجة، وتؤدي في الوقت نفسه إلى كوارث معلوماتية، ومن ذلك الأخطاء:

١. **تعليق كلمات المرور:** فكثيرًا ما يقوم المستخدمون بتدمير كل إجراءات أمن المعلومات بلصق كلمات المرور على مقدمة شاشة الحاسب، أو على سطح المكتب، بحيث يمكنهم رؤيتها بسهولة، هم وكل من حولهم، ثقة منهم فيهم أو لأي سبب آخر، وقد أثبتت دراسة حديثة أن (٢٠%) من موظفي تكنولوجيا أمن المعلومات يفعلون ذلك.

٢. **ترك الجهاز مفتوحًا:** والحركة بعيدًا عنه للحظات أو لمدة من الوقت، وهو ما يسهل مهمة السارق في حصوله على كلمة المرور، وخاصة إذا كان خبيرًا بما يفعل أو عليمًا بما يريد.

٣. **فتح مرفقات البريد الإلكتروني:** فالبعض لا يكلف نفسه عناء التفكير فيما ورد إليه من رسائل، فإذا كان البعض قد فوجئ، أو لم تكن لديه خبرة سابقة في كيفية انتشار الفيروس، فلماذا وقعوا في الخطأ نفسه بالنقر على مرفق رسالة البريد الإلكتروني.

٤. **اختيار كلمة مرور سيئة:** وهذا ما يخيف خبراء أمن المعلومات، حيث يمكن للمقربين التكهن بهذه الكلمة التي ترتبط باسم الابن، أو فريق الكرة، وكلما طالت الكلمة وتعقدت كلما كان التكهن بها

أصعب أو مستحيلاً، ولاختيار كلمة المرور قواعد يحسن أن تقوم المؤسسات باتباعها.

٥. **ترك الحاسب المحمول:** فمن الواجب عدم تركه من دون مراقبة، خصوصًا في الأماكن العامة، ولقد قالوا في ذلك: الحاسب المحمول شأنه شأن الهاتف المحمول، وكل شيء (منتج إلكترونيًا) محمول خائن، يبغض صاحبه، ويحب سارقه.

٦. **تجاهل سياسة أمن المعلومات:** فمهما كانت هذه السياسة جيدة، فإن إهمالها يتساوى مع عدم وجودها، فهناك من العاملين من لا يقتنع بهذه القواعد، ويرى أن لديه الأسباب الوجيهة لإهمالها، فمثلاً قد يعطل بعضهم برامج الكشف عن الفيروسات، لأنها تبطئ من سرعة الجهاز.

٧. **الفشل في مراقبة الموظفين:** لأنهم أعلم بأوجه الضرر أكثر من غيرهم.

٨. **البطء في المواكبة:** فالجريمة بشكل عام، وجرائم المعلوماتية بشكل خاص في تطور مستمر، وهي في أغلب الأحيان تسبق وسائل الأمن والحماية، لذلك ينبغي تحديث وسائل وسياسات أمن المعلوماتية بشكل دائم.

٥/ المعايير الدولية لأمن المعلومات:

تشمل المعايير الدولية لأمن المعلومات في المعايير التالية :

اولا : معيار ISO/IEC ٢٧٠٠٢:

هذا المعيار هو أحد معايير المنظمة العالمية للمعايير ISO International Organization for Standardization ,)وهي معنية بإعداد معايير لمختلف المجالات ومن ضمنها مجال تقنية المعلومات. وقد طور هذا المعيار بالتعاون مع منظمة الكهروتقنية الدولية International Electro technical Commission واختصارا IEC. وهذا المعيار جزء من مجموعة من المعايير تسمى عائلة ISO/IEC ٢٧٠٠٠ أو يطلق عليها معايير تقنية المعلومات – تقنيات الأمن

كود الممارسة الأفضل لإدارة أمن المعلومات.

ويهدف هذا المعيار إلى إيجاد خطط ومبادئ أساسية لإنشاء وتنفيذ وصيانة وتطوير نظم إدارة أمن المعلومات في المنظمة. وينقسم هذا المعيار إلى مجموعة من الأجزاء الفرعية يجب على المنظمة الراغبة في الحصول على هذا المعيار تطبيقها ، وهي :

- تقييم المخاطر.
- أنواع السياسات الأمنية المطبقة.
- الهيكل التنظيمي لأمن المعلومات.
- إدارة الأصول.
- إدارة أمن الموارد البشرية.
- أمن المرافق والبيئة المحيطة.
- إدارة العمليات والاتصالات.
- التحكم في الوصول.
- إدارة الحوادث العرضية لتقنية المعلومات.
- إدارة استمرارية الخدمة.
- إدارة التوافقية مع الأنظمة والتشريعات.

ثانيا : معيار COBIT

تم تطوير وتصميم معيار COBIT عام ١٩٩٥ م من قبل معهد حوكمة تقنية المعلومات IT Governance Institute وهو الآن في نسخته الرابعة] ٥[. وكلمة COBIT اختصار ل ضوابط المعلومات والتقنيات المتعلقة بها Control Objectives for Information and related Technology . عبارة عن

هيكلية تهدف إلى ربط تقنية المعلومات بأهداف ومتطلبات أعمال المنظمة عن طريق إيجاد نموذج عام لأنشطة تقنية المعلومات في المنظمة مما يؤدي إلى التعرف على موارد تقنية المعلومات المهمة وتعزيزها و ربط ذلك كله بضوابط تحكم هذه العمليات والأنشطة والموارد. ويركز هذا المعيار على أربع أجزاء رئيسية هي:

- التخطيط والتنظيم لتقنية المعلومات.
- الاستحواذ وتطبيق تقنية المعلومات.
- توصيل ودعم تقنية المعلومات.
- المراقبة والمتابعة.

ثالثا : معيار ITIL

معيار ITIL اختصار ل Information Technology Infrastructure Library أو مكتبة البنية الأساسية لتقنية المعلومات ويصدر عن مكتب التجارية الحكومية البريطاني Office of Government Commerce (OGC (.وهذا المعيار عبارة عن مجموعة من

المفاهيم والسياسات لإدارة وتطوير خدمات تقنية المعلومات والعمليات المتعلقة بها. وفي هذا المعيار هناك وصف تفصيلي للمهام والعمليات المتعلقة بتقنية المعلومات مع قوائم مرجعية متكاملة بحيث تستطيع أي منظمة تستخدم تقنية المعلومات موائمته حسب احتياجاتها.وفي هذا المعيار يجب أن تتوافق إدارة أمن المعلومات في المنظمة مع ما يلي:

- السياسات الحالية و المستقبلية لأمن إدارة الأعمال.
- متطلبات الأمن.
- المتطلبات التشريعية والقانونية.
- إدارة تقييم مخاطر الأعمال وتقنية المعلومات.

رابعا: المعيار العالمي لأمن المعلومات(ISO17799)

يحتوي على أفضل الممارسات في المراقبة وفي السياسات والضوابط التي تتبع في إدارة أمن المعلومات في المجالات التالية:

١- تقييم المخاطر: تحديد المخاطر التي تتعرض لها المنظمة، مثل المخاطر التي قد تؤثر على معلومات المنظمة المهمة أو على موظفيها أو ممتلكاتها، ويكون هذا التقييم بناءً على شيئين رئيسيين وهما :

أ/ تحديد مدى تأثير هذه المخاطر على المنظمة: حيث أن هذه المخاطر من المؤكد أن يكون لها تأثير سلبي على المنظمة لكن هذا التأثير يختلف من خطر لآخر بناءً على تكلفة الخسائر التي يسببها للمنظمة.

ب/ احتمالية حدوث هذه المخاطر من خلال تحديد احتمال حدوث هذا الخطر في المنظمة فإذا كانت نسبة حدوث هذا الخطر قليل جداً يتم تجاهل هذا الخطر.

٢- السياسات الأمنية: هي مجموعة من المعايير والأنظمة التي تقوم بتطبيقها المنظمة لحماية معلوماتها ومرافقها من خلال فرض قوانين وقواعد تلزم المنظمة موظفيها على إتباعها، مثل أن تفرض المنظمة على موظفيها أن يكون الرقم السري لحسابه على شبكة المنظمة لا يقل عن ٨ أحرف أو أن قاعدة بيانات المنظمة لا يسمح الوصول لها إلا عن طريق موظفين معينين. فالهدف منها هو توفير الدعم والتوجيه في إدارة أمن المعلومات.

الفصل الثالث

أمن شبكات المعلومات الالكترونية

مقدمة:

لقد أضحت الشبكات الإلكترونية من الضروريات الحاصلة في عصرنا الحديث، بحيث أصبح لا غنى عنها في المؤسسات والشركات والحكومات بل وحتى في البيوت، فحيثما أنت تجد من حولك أنواع عديدة من شبكات الحواسيب التي تنقل كماً هائلاً من المعلومات والبيانات بين الأشخاص والمؤسسات على مستوى العالم، وتتنوع هذه المعلومات والبيانات في أهميتها ودرجة سريتها من المعلومات العامة والعلمية العادية إلى المعلومات والإحصائيات الحكومية وميزانيات الدول والمعلومات الاستخباراتية بالغة الخطورة والسرية، وكل هذه الأنواع من المعلومات والبيانات إنما يتم تناقلها وحفظها في غالب الأحيان عبر شبكات الحاسوب على اختلاف أنواعها وأماكنها.

ومن هنا تأتي أهمية هذه الشبكات في العالم المعاصر والتعاملات اليومية بين البشر بشكل عام، ومن هذه الأهمية تنبع خطورة ما يمثله أمن هذه الشبكات وأمن المعلومات التي يتم تداولها عبر خطوطها.

١/تعريف الشبكات:

يقصد بالشبكات Networks نظام معين لربط جهازين حاسوب أو أكثر باستخدام إحدى تقنيات الاتصالات، وذلك بهدف تبادل المعلومات

والبيانات المتاحة بين أكثر من طرف، وكذلك بهدف تشارك الموارد المتاحة مثل الطابعات Printers والبرامج التطبيقية Software، كما أن هذه الشبكات تسمح أيضًا بالتواصل المباشر بين أفراد مجتمع الشبكة.

كما يمكن القول أن شبكات المعلومات هي عبارة عن نوع من تقنية الاتصالات التي تستخدم في عمليات الربط بين مجموعة من مراكز المعلومات بهدف مشاركة وتبادل المعلومات فيما بينهم عن طريق أجهزة الحواسيب.

٢/الحاجة إلى الشبكات:

ما هي الحاجة التي أدت إلى ظهور الشبكات في عالمنا المعاصر؟

هناك العديد من العوامل التي أدت إلى ظهور شبكات المعلومات وفي أن تصبح عاملاً مهمًا من عوامل تقدم ورقي الأمم في العصر الحديث، ذلك أن كل شيء تقريباً في عصرنا الحديث والحضارة الحديثة يعتمد بشكل أو بآخر على ما تقدمه هذه الشبكات من خدمات في عمليات توفير المعلومات والبيانات على مدار الساعة، وليس هناك دليل أوضح من "شبكة الإنترنتInternet" للتدليل على ذلك، فمن

الصعب الآن أن تجد من يسأل ما هي جدوى وجود الشبكة العالمية "الإنترنت" في حياتنا؟

وسوف نبرز فيما يلي أهم العوامل التي يمكن أن يعزى إليها السبب في ظهور الحاجة إلى الشبكات:

- **تبادل المعلومات:** الهدف الرئيسي من شبكات المعلومات هو عمليات تبادل المعلومات والبيانات بين أطراف مجتمع الشبكة في سهولة ويسر وفي أسرع وقت ممكن، وهذا ما تعمل عليه الشبكات القائمة مثلاً بين أجزاء المؤسسات فهي تعمل على تحقيق السيولة والسهولة في الحصول على المعلومات وتبادلها بين العاملين في هذه الشركة.
- **المشاركة في البرامج التطبيقية Sharing Software:** حيث تعمل الشبكات على تحقيق إمكانية المشاركة في البرامج المتاحة في مجتمع شبكة المعلومات بين جميع أفراد الشبكة، وذلك يعمل على توفير النفقات المالية في شراء نسخ متعددة من تلك البرامج.
- **المشاركة في موارد الشبكات Sharing Hardware:** من مميزات الشبكات أنها تعمل على التوفير أيضاً في الأجهزة والمعدات المستخدمة وذلك من خلال استغلال خاصية مشاركة

موارد الشبكات مثل الطابعات وأجهزة التصوير وأجهزة الفاكس وغيرها كثير.

- **البريد الإلكتروني E-Mail:** إحدى ميزات شبكات المعلومات هي توفير إمكانية استخدام البريد الإلكتروني للعاملين وأفراد مجتمع الشبكة، مما يتيح إرسال واستقبال الرسائل والوثائق وأوامر العمل فيما بينهم.
- **إنشاء مجموعات العملWork Groups:** تتيح الشبكات فرصة تكوين مجموعات العمل لتنفيذ مهمة معينة، وتكون بتخصيص جزء من مساحة التخزين على الشبكة لأفراد هذه المجموعة فقط بعيدًا عن باقي أفراد الشبكة.
- الإدارة المركزية Central Management: يحقق وجود معظم الموارد على الشبكة في عمليات الإدارة المركزية لهذه الموارد والاستفادة منها بالشكل الأمثل، كما تحقق سهولة تنفيذ عمليات النسخ الاحتياطي Backup.
- **التأمين Security:** حيث يمكن لمدير النظام Administrator التحكم في عمليات الولوج Enter والإتاحة Access.

- **القدرة على ربط أنظمة التشغيل المختلفة** Access to other Operating Systems: يمكن عن طريق تكنولوجيا شبكات المعلومات ربط أنظمة تشغيل مختلفة والعمل عليها.
- **تحسين الإنتاجية** Improve Productivity: حيث تعمل شبكات المعلومات على تحسين التعاون بين أفراد مجتمعها مما يؤدي إلى تحسين الإنتاجية بين الأفراد

٣/أمن شبكات المعلومات Information Networks Security:

لقد أوضحنا فيما سبق الأهمية الكبيرة لشبكات المعلومات وما تقدمه من خدمات كبيرة على كافة المستويات، ومن تلك الأهمية تنبع أهمية أن يكون هناك مستوى معين من الأمان في هذه الشبكات حماية للمستخدمين والمعلومات التي تحتويها، فقد انتشرت في السنوات الأخيرة العديد من المشاكل والجرائم التي تتعلق بأمن المعلومات واختراق العديد من شبكات المعلومات على مستوى العالم، بل وصل الأمر إلى اختراق أعلى الشبكات سرية في العالم مثل شبكة المخابرات الأمريكية CIA وغيرها من الشبكات، ولنا أن نتصور ما يمكن أن يمثله ذلك من تهديد

للدول في عصر أصبحت فيها الحرب هي حرب المعلومات وليس حرب الأسلحة كما كان سابقًا.

ويمكننا تعريف "**أمن شبكات المعلومات**" على أنه مجموعة من الإجراءات التي يمكن خلالها توفير الحماية القصوى للمعلومات والبيانات في الشبكات من كافة المخاطر التي تتهددها، وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية.

أو هي مجموعة من المعايير التي تحول دون وصول المعلومات المخزنة في الشبكات إلى الأشخاص غير المخول لهم الحصول عليها.

٤/ لماذا أمن شبكات المعلومات؟

يشكل أمن المعلومات في العصر الحديث حجر الزاوية في علميات نهضة تكنولوجيا المعلومات والاتصالات، حيث أن المساهمة المتاحة للخصوصية تتناسب عكسيًا مع التقدم التكنولوجي المعلوماتية والاتصالات، لقد أنهينا في الفقرات السابقة إيضاح أهمية شبكات المعلومات للجميع، وبالتالي فإنه من البديهي أن يكون لهذه الأهمية درجة من الحماية تتدرج في الأهمية بتدرج أهمية المعلومات المخزنة في هذه الشبكات، للإجابة على هذا السؤال لا بد لنا أن نعرض بعض

النماذج التي تم فيها اختراق بعض الشبكات لنبين أهمية أمن الشبكات والمخاطر التي يمكن أن تحدث في حالة عدم توفره.

- **الحالة الأولى:** في عام ٢٠٠٢ اكتشفت شركة Daewoo Securities أن ما قيمته ٢١,٧ مليون دولارًا من الأسهم التي تديرها قد بيعت بشكل غير قانوني، وذلك نتيجة مباشرة لاختراق شبكة الحاسوب الخاصة بها.
- **الحالة الثانية:** في عام ٢٠٠٣ قام موظف بإحدى الشركات الروسية باختراق شبكة المعلومات الخاصة بالشركة، وقام بتعديل راتبه الشهري ومجموعة من زملائه بزيادة الرواتب بنسبة معينة مما أدى بخسائر مالية للشركة لعدة شهور لعدم اكتشاف هذا الاختراق.

وهناك العديد من الحالات الأخرى مثل اختراق شبكة معلومات وزارة الدفاع الأمريكي الذي حدث مرات عديدة في السنوات الأخيرة، ويمكن أن نرى مدى الخسائر التي تمثلها مثل هذه الاختراقات الأمنية لشبكات المعلومات، سواء كانت هذه الخسائر مالية كما في حالة الشركات أو خسائر معلوماتية واستخباراتية لا تقدر بمال ويمكن أن تمس باستقرار بلدان كبيرة مثل أمريكا، ومن هنا يتضح الأهمية القصوى لعمليات تأمين شبكات المعلومات.

ويمكن أن نجمل بعض الأسباب التي أدت إلى الاهتمام بموضوع "أمن شبكات المعلومات" مؤخرًا في النقاط التالية:

١. **التقدم التكنولوجي:** فكما أدت التطورات الهائلة في مجال تكنولوجيا المعلومات والاتصالات إلى طفرة كبيرة في وسائل الاتصال وتكنولوجيا شبكات المعلومات وتخزينها، فإنه في نفس الوقت أدى إلى وجود عقول تعمل على إيجاد الثغرات الأمنية في هذه الشبكات واستغلالها الاستغلال السيئ فيما يسمى بـ"الوجه القبيح للتكنولوجيا".

٢. **الطفولية والاندفاع.** حيث يتملك بعض الشخصيات دوافع طفولية واندفاعية للحصول على المعلومات بطرق غير مشروعة لمجرد الإحساس بنشوة الانتصار وكسر حواجز السرية والأمان المفروضة على شبكات المعلومات.

٣. **انتشار جرائم المعلومات.** فقد سادت في الفترة الأخيرة هوس الجرائم الإلكترونية وجرائم المعلومات والتي تبدأ من الأشخاص والمنظمات والشركات المتنافسة وتنتهي بالدول، وذلك فيما يعرف بـ"حرب المعلومات".

وهنا يمكن أن نقول أن أنظمة أمن شبكات المعلومات تتطلب حماية أصول وموارد نظم المعلومات بطرق مشروعة، وكذلك تنظيم العلاقات

والاتصالات داخل شبكات المعلومات من دون تأثير على كفاءة النظام ولا على قدرة المستخدمين في الأداء.

ولكن .. هل كل شبكات المعلومات تحتاج إلى تأمين؟ بالتأكيد يعتمد ذلك على ما تحتويه هذه الشبكات من معلومات وبيانات وطبيعة المستخدمين فيها، وكذلك رغبة الجهة المسئولة عن هذه الشبكات في حماية موارد وممتلكات هذه الشبكات من عدمه، ولكن بصفة عامة يجب أن يكون هناك نوع من الحماية ولو على الأقل الحماية البسيطة لهذه الشبكات على سبيل الاحتياط ومنع دخول غير المرغوب فيهم من الأوساط الخارجية، وعلى الجانب الآخر فإن هناك أنواع من شبكات المعلومات لابد من وجود نظام أمان وحماية لها ولا يمكن أن تترك بلا أمان، وذلك نظرًا لما تمثله من أهمية كبيرة سواء على مستوى ما تحمله من بيانات ومعلومات أو على مستوى المستخدمين لهذه الشبكات، ومن أمثلة هذه الشبكات ما يلي:

- **الشبكات الداخلية** LAN: مثل شبكات الشركات الصغيرة أو المدارس أو المستشفيات.
- **الشبكات الواسعة** WAN: مثل الشبكات الدولية التي تربط بين أجزاء من الدول
- **الشبكات الخاصة**Internet .

٥/جرائم المعلومات:

"**للحقيقة وجوه أخرى**" يمكن أن تكون هذه العبارة معبرة بشكل كبير عما يمكن الحديث عنه في موضوع جرائم المعلومات وعلاقتها بتطور تكنولوجيا المعلومات والاتصالات والطفرة الهائلة في صناعة المعلومات ومعالجتها على المستوى العالمي، فكما جلبت هذه التكنولوجيا لنا العديد من المنافع والخدمات والتسهيلات التي لا يمكن لعاقل أن يشكك في مدى جدواها للأفراد والأمم على السواء، فقد جلبت لنا نفس التكنولوجيا أيضًا العديد من الأبعاد الجديدة للجرائم والمسميات التي لم يكن يألفها من عاشوا قبلنا، بل لم يكن يتخيل أحد أن تصل الحرفية والقدرة على ارتكاب الجرائم إلى هذا الحد من استخدام التكنولوجيا التي يتغنى بها العالم على أنها أهم منجزاته وأنها ما جعلت إلا لراحته وتحقيق أعلى معدلات الأمن والأمان له ولاستثماراته ورفاهيته.

فقد أصبح من الممكن، ارتكاب جرائم مثل الاختلاس والسرقة أو جرائم التزوير عن بعد باستخدام التكنولوجيا، وأصحبت وسائل الأمان والحماية المحسوسة وصناديق الحفظ وأماكن التخزين لا تكفي وحدها لتحقيق الأمان المنشود لحماية المعلومات من لصوصها، وقد ظهر

حديثًا مصطلحات مثل (Cybercrime) والذي يعني النوع الجديد من الجرائم التي يتم ارتكابها بواسطة الحواسيب وشبكات المعلومات، بل لقد وصل الأمر إلى إطلاق الحكومة الأمريكية في فبراير ٢٠٠٣ مبادرة خاصة تهتم بحماية المجال المعلوماتي والتي أطلقت عليها (Cyberspace)، وقد بدأت العديد من الدول المتقدمة في السير في نفس الاتجاه في سبيل إيجاد الحلول التي تعمل على الحد من ظاهرة الجرائم الالكترونية Cybercrimes.

ومن هنا يمكن القول أن جرائم المعلومات هي "تعبير شامل يشير إلى جريمة تتعلق باستخدام إحدى وسائل تكنولوجيا المعلومات والاتصالات بغرض خداع الآخرين أو تضليلهم، أو من أجل تحقيق هدف معين أو تربح".

٦/تصنيف جرائم المعلومات:

يمكننا تصنيف الجرائم التي تتم عن طريق استخدام تكنولوجيا المعلومات إلى عدة أقسام وكل قسم يختص بنوع معين من الجرائم التي يمكن ارتكابها وهي كالتالي:

١. **جرائم تهدف لنشر معلومات:**

في مثل هذا النوع يتم نشر معلومات سرية تم الحصول عليها بطرق غير مشروعة عن طريق الاختراقات لشبكات المعلومات ونشر هذه المعلومات على الملأ، ومن أمثلة ذلك نشر معلومات بطاقات الائتمان البنكية، وأرقام الحسابات المصرفية، وأيضًا نشر المعلومات الاستخباراتية المتعلقة بدول أو أشخاص كما حدث في اختراق وكالة المخابرات الأمريكية CIA.

٢. **جرائم تهدف لترويج الإشاعات:**

وهنا يتم نشر معلومات مغلوطة وغير صحيحة تتعلق بالأشخاص أو المعتقدات أو الدول بهدف تكدير السلم العام في البلدان، وكذلك نشر الإشاعات عن بعض الأشياء وإحداث البلبلة في المجتمعات.

٣. **جرائم التزوير الإلكترونية:**

وهنا يتم استخدام وسائل التكنولوجيا في عمليات التزوير بغرض تحقيق هدف معين، مثل تزوير البطاقات الائتمانية وجوازات السفر وغيرها من الأوراق الرسمية والثبوتية التي يمكن تزويرها باستخدام وسائل تكنولوجية متقدمة، وكذلك يندرج تحتها عمليات التحويل المصرفي الوهمية من حسابات إلى أخرى عن طريق اختراق شبكات المصارف.

٤. **جرائم تقنية المعلومات:**

وأهم مثال لها هو عمليات القرصنة التي تحدث للبرامج الحاسوبية الأصلية والتي يتم عمل نسخ منها لتباع في الأسواق بدلاً من النسخ الأصلية، مثل برامج التشغيل أو البرامج التطبيقية غالية الثمن، والتي يتم تقليدها عن طريق قراصنة محترفين في هذا المجال.

٧/دوافع الهجوم على شبكات المعلومات:

يمكن أن يتبادر إلى الذهن سؤال وهو لماذا يقوم المخربون أو المخترقون بعمليات مثل اختراق شبكات المعلومات وتهديد أمن المعلومات؟ وما هي الدوافع التي يمكن أن تكون لديهم لكي يقوموا بمثل هذه الأعمال؟ فلابد لكل شخص من دوافع للقيام بعمل ما، وهنا سنتعرف على بعض الدوافع التي رصدها المختصون بمراقبة عمليات الاختراق وجرائم المعلومات لدى القائمون بهذه الهجمات.

أولًا: وجود الدافع:

إن القاتل حين يقتل القتيل يكون لديه دافع معين سواء كان الانتقام أو السرقة أو حتى دافع مرضي، وبالتالي فالقائمون بعمل الهجمات والاختراقات لشبكات المعلومات لابد لهم من دافع حتى يقوموا بهذه العمليات، وخاصة أنها تكلفهم جهدًا ذهنيًا وفكريًا وحتى ماليًا كبيرًا في

بعض الأحيان، وقد يكون هذا الدافع الحصول على الأموال أو التخريب المتعمد أو حتى مجرد إثبات قدرات المخترق وأن يثبت قدرته على اختراق موقع معين كنوع من التحدي التقني.

وفي بعض الحالات يكون الوضع له دوافع سياسية، ومن هنا يتضح التباين في دوافع من يقوم بمثل هذه الهجمات على شبكات المعلومات، حيث تتعدد ما بين الشخصية والمالية والنفسية وحتى السياسية بين الدول وبعضها البعض والانتماءات الفكرية والعقائدية والسياسية للأفراد والدول.

ثانيًا: وجود الخطة Plan:

ونعني هنا بالخطة أي وجود خطة لتنفيذ علمية الهجوم واختراق الموقع المراد تدميره، فالمهاجم لن يتمكن من تنفيذ أهدافه بدون وجود خطة محكمة تتيح له شن هجماته على الموقع واختراقه وتنفيذ ما يريد.

ثالثًا: وجود الثغرات Vulnerabilities:

ونقصد هنا بالثغرات أي نقاط الضعف الموجودة في نظام المعلومات ككل أو في شبكة المعلومات أو الأجهزة التي تعمل ضمن الشبكة أو حتى البرمجيات التي يتم إتاحتها على شبكة المعلومات، ويمكن أن تكون هذه الثغرات في تصميم شبكة المعلومات Network Design

أو تهيئة الشبكة Network Configuration أو البرمجيات Software أو قواعد البيانات Data Bases التي تحتويها الشبكة، ومن خلال هذه الثغرات أو نقاط الضعف يمكن للمهاجمين أن يخترقوا شبكات المعلومات ويحدثوا فيها الأضرار أو حتى الاستيلاء على ما يريدوا منها، وعلى مدير النظام ومديرو الشبكة أن يقوموا بعمليات فحص باستمرار لشبكة المعلومات لكي يقفوا على أي نقاط ضعف أو ثغرات يمكن أن تحدث ويعملوا على الفور على معالجها وسد هذه الثغرات تجنبًا لاكتشافها من قبل بعض العابثين.

٨/مصادر الخطر على شبكات المعلومات:

بعد كل ما سبق الحديث عنه من الأخطار التي تواجه شبكات المعلومات وأنظمة الحماية بها، نود هنا أن نورد المصادر التي يمكن من خلالها تشكيل تهديد أو اختراقات لشبكات المعلومات.

أولًا: الخطر الداخلي Internal:

يقصد بالخطر الداخلي المهاجمون من داخل نطاق عمل شبكة المعلومات، وهم الأفراد أو العاملون الذين ينتمون لنفس الجهة المستهدفة، ولعل هذا النوع من الخطر هو أشد فتكًا وخطورة من خطر

الأعداء الخارجيون، ويمثل ذلك التهديد الأكبر للمؤسسات سواء كانت شركات أو هيئات حكومية أو حتى الحكومات نفسها، فخطر انتهاك الخصوصية من الداخل سهل الحدوث وصعب الكشف عنه في حالات كثيرة، وخصوصاً إذا الشخص المهاجم يمتلك صلاحية الولوج إلى نظام شبكات المعلومات فلا يواجه أي صعوبة في عمليات الأمان والسرية الموجودة على الشبكة بل ويمكنه طمس معالم الهجوم ويمحو آثار أي دخول بسهولة، ويمكن إيجاز أهم جوانب الأخطار الداخلية فيما يلي:

أ. اختراق الشبكات الداخلية للمؤسسات.

ب. اختراق نظم المعلومات بالسرقة أو التبديل أو التغيير أو الحذف.

ت. إيجاد وتهيئة ثغرات في النظام الأمني للشبكات.

ث. تغيير تهيئة نظام شبكات المعلومات.

فقد جاء في التقرير التقني المعنون "دراسة استقصائية عن انتهاكات أمن المعلومات" الذي اجرته شركة برايس ووتر هاوس كوبرز في بريطانية أن" الخطأ البشري وليس التكنولوجيا هو السبب الجذري لمعظم الاختراقات الأمنية" وهم أشد خطرًا على أنظمة المعلومات المتاحة داخل هذه المؤسسات من الخطر الخارجي.

وهنا يمكننا طرح تساؤل مشروع حول الدوافع التي يمكن أن تدفع أحد العاملين في مؤسسة أو حكومة ما إلى انتهاك سرية المعلومات المتاحة وشن هجوم يمكن أن يضر بهذه الجهة التي يعمل بها؟ ونجد الإجابة على ذلك في النقاط التالية:

١. **حالات عدم الرضا:**

فكثيرًا ما توضح تحقيقات حالات الاختراق الأمني الداخلي لشبكات المعلومات عن أن السبب كان هو وجود حالة من عدم الرضا عند من قام بالعمل تجاه الجهة التي يعمل بها، سواء كانت هذه الحالة عدم الرضا المادي أو الوظيفي أو الانتقام من مدير أو ما إلى ذلك من أسباب شخصية.

٢. **إثبات الذات:**

أحياناً ما ينتاب العاملون في حقول المعلومات بعض لحظات الأنانية التي يشعر فيها الفرد بحاجته لإثبات قدرته على اختراق الحواجز وانتهاك خصوصية الشبكة، أو الوصول إلى قواعد بيانات محمية بجدران سرية، وما إلى ذلك لمجرد أن يرضي غروره أنه قادر على التحدي، أو الشهرة كما يحدث في حالات كثيرة من اختراق الهاكرز

للمواقع الحكومية في كافة أنحاء العالم، وقد ساعد انتشار برامج كسر الحماية والاختراق الكثير على محاولة تنفيذ هجمات لخرق الشبكات.

٣. **الاستفادة المادية:**

قد يكون الاختراق في حالات مدفوع الأجر من جهات منافسة بغرض الضرر أو إلحاق الهزيمة أو سرقة معلومات أو ما إلى ذلك، فتقوم بعض الشركات والمؤسسات برشوة بعض الأشخاص بغرض تسريب المعلومات واختراق شبكات المعلومات نظير مبالغ مالية.

ثانيًا: الخطر الخارجي External:

يقصد بالخطر الخارجي بالطبع هم الأشخاص الذين يقومون بمحاولات الاختراق لأمن الشبكات من خارج المؤسسات، سواء كانوا على صلة بهذه المؤسسات أو لا، وبالطبع نسمع كل يوم عن اختراق العديد من شبكات المعلومات من قبل بعض قراصنة الإنترنت، بل وفي بعض الأحيان تصل الأمور إلى حد اختراق المواقع الحكومية والمالية كالبنوك وغيرها من المؤسسات التي بها شبكات معلومات على درجة عالية من السرية والأمان.

ولكن في الخطر القادم من الخارج تكون درجة خطورته أقل وذلك لعدة أسباب منها أنه من المتوقع أصلاً أن تكون هناك هجمات خارجية وبالتالي فإن أي شبكة لابد وأن تكون مزودة بنظم وبروتوكولات الحماية

التي تعمل على صد المهاجمين ومحاولات الاختراق الأمني لها من قبل العابثين، كما أن بناء الشبكات الآن أصبح على درجة عالية من الحرفية والدقة بحيث أصبح القائمون على بناء وتركيب الشبكات على دراية بكافة أنواع الهجمات والاختراقات التي يتبعها المخترقون بل ويقومون بدراستها بدقة لعمل الحلول السريعة لها والحيلولة دون وقوعها.

ثالثًا: خطر التشويش:

ويقصد بذلك العوامل التي تؤثر على إرسال واستقبال البيانات والمعلومات عن طريق شبكات المعلومات، فقد تتعرض المعلومات إلى نوع من التشويش في الإرسال والاستقبال عن طريق بعض المعدات أو البرامج التي تعمل على ذلك، وفي بعض الأحوال يكون هذا التشويش غير مقصود أي أنه يكون ناتجًا عن بعض العوامل والظروف الطبيعية كظروف الطقس والمناخ التي تؤثر على أبراج الإرسال والاستقبال وخاصة في الشبكات التي تعتمد على الألياف الضوئية ونظم الاتصالات اللاسلكية، وفي أحيانٍ أخرى يكون "التشويش" ناتج عن عمل متعمد ومقصود من جهات معينة، فقد يكون هناك من يترصد المعلومات عبر الشبكات ومن يقوم بعمليات التشويش عليها بواسطة إشارات تماثل نفس نطاقات التردد المستخدمة في عمليات الإرسال عن طريق الشبكة الأم.

رابعًا: خطر سوء التصميم:

في بعض الأحيان يكون هناك بعض الأخطاء الفنية في تصميم الشبكات أو الأنظمة التي تعمل عليها هذه الشبكات، ومع أن مثل هذه الأخطاء قليلة وأيضًا غير مقصودة إلا أنها تعد خطرًا يهدد أمن وسلامة شبكة المعلومات لأنها لا تؤثر على بنيتها وأدائها الوظيفي فحسب، ولكنها أيضًا يمكن أن تكون منفذًا سهلًا لعمليات الاختراق الأمني من قبل مخربي الشبكات، وتكون هذه الأخطاء غير المقصودة هي نقطة الضعف في شبكة المعلومات والتي يمكن من خلالها تهديد أمن وسلامة المعلومات.

خامسًا: خطر سوء الاستخدام:

العامل البشري هام جدًا حتى في الشبكات، وكلما كان العنصر البشري مدربًا ومؤهلًا بالشكل العلمي والقدر الكافي كان ذلك أحد أسباب حماية شبكات المعلومات، فهناك بعض الأخطاء التي تنتج عن سوء استخدام الأفراد لشبكات المعلومات تلحق بالضرر البالغ على أمن وسلامة البيانات داخل الشبكة، وسواء كان هذا الإهمال وسوء الاستخدام متعمدًا أو غير متعمد فإنه في النهاية يؤدي إلى النتيجة

نفسها، بحيث يمكن أن يكون نافذة إلى إحداث ثقوب في جدر الحماية الخاصة بالشبكات.

سادساً: خطر الكوارث الطبيعية:

شبكات المعلومات هي جزء العالم الذي نعيش فيه تتأثر بما تتأثر به الأشياء الأخرى ومن ضمن ما يمكن أن يكون خطراً على الشبكات وبنيتها هي الكوارث الطبيعية التي يمكن أن تقع دون سابق إنذار ودون أي تدخل بشري، مثل الزلازل والبراكين والانفجارات والحرائق وغيرها، ولذا يجب الاحتياط وعمل النسخ الاحتياطية Backup بشكل منتظم لمحتويات الشبكة وتكون هذه النسخ الاحتياطية في أماكن بعيدة عن المكان الرئيسي للشبكة الأم حتى يمكن حماية المعلومات واسترجاعها في حالة حدوث أي نوع من هذه الكوارث للشبكة نفسها.

سابعاً: الدخلاءHackers:

الهاكر هو الشخص الذي يقوم بإنشاء وتعديل البرمجيات والعتاد الحاسوبي، وقد أصبح هذا المصطلح ذا مغزى سلبي حيث صار يطلق على الشخص الذي يقوم باستغلال النظام من خلال الحصول على دخول غير مصرح به للأنظمة والقيام بعمليات غير مرغوب فيها وغير مشروعة، غير أن هذا المصطلح (هاكر) يمكن أن يطلق على الشخص

الذي يستخدم مهاراته لتطوير برمجيات الكمبيوتر وإدارة أنظمة الحاسوب وما يتعلق بأمن نظم المعلومات، وأطلقت كلمة هاكر أساساً على مجموعة من المبرمجين الأذكياء الذين كانوا يتحدوا الأنظمة المختلفة ويحاولوا اقتحامها، وليس بالضرورة أن تكون في نيتهم ارتكاب جريمة أو حتى جنحة، ولكن نجاحهم في الاختراق يعتبر نجاحًا لقدراتهم ومهارتهم. إلا أن القانون اعتبرهم دخلاء تمكنوا من دخول مكان افتراضي لا يجب أن يكونوا فيه.

ثامنًا: الفيروسات Viruses:

فيروس الحاسوب هو برنامج خارجي صُنع عمدًا بغرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب وما شابهها من عمليات. أي أن فيروسات الكومبيوتر هي برامج تتم كتابتها بواسطة مبرمجين محترفين بغرض إلحاق الضرر بكومبيوتر آخر، أو السيطرة عليه أو سرقة بيانات مهمة، وتتم كتابتها بطريقة معينة.

وتعد فيروسات الحاسوب من المشاكل الأكثر شيوعًا في أمن المعلومات والشبكات، والفيروس هو أحد البرامج الخبيثة أو المتطفلة، والبرامج المتطفلة الأخرى تسمى الديدان أو أحصنة طروادة أو برامج الدعاية أو برامج التجسس، يمكن للبرامج الخبيثة أن تكون فقط للإزعاج

من خلال التأثير على استخدامات الكمبيوتر وتبطئيه وتتسبب في حدوث انقطاعات وأعطال في أوقات منتظمة وتؤثر على البرامج والوثائق المختلفة التي قد يرغب المستخدم في الدخول إليها، أما البرامج الخبيثة الأكثر خطورة فيمكن أن تصبح مشكلة أمنية من خلال الحصول على معلوماتك الشخصية من رسائلك الإلكترونية والبيانات الأخرى المخزنة في جهازك عبر شبكة المعلومات.

٩/حماية شبكات المعلوماتNetwork Protection:

تم فيما سبق استعراض أهم المخاطر التي تواجه شبكات المعلومات وتحول دون حماية المعلومات في داخلها، ورأينا أنها تنقسم إلى عدة أقسام منها ما يمكن التحكم فيه ومنها ما يحدث دون تدخل من الإنسان، والسؤال الآن الذي يمكن طرحه هو هل يمكن تفادي هذه المخاطر والأضرار؟ وما هي الوسائل التي يمكن عن طريقها تجنب حدوث مثل هذه المشاكل والاختراقات في شبكات المعلومات التي تخصنا؟ وهذا ما سنناقشه في الفقرات التالية.

أولًا: كلمات المرورPasswords:

بدونها لا يمكن لأي شخص غير مخول بالدخول على شبكة المعلومات، وهي جواز مرور المستخدم إلى الشبكة، فكلمة المرور تثبت للشبكة بأنك أنت الشخص المخول للدخول إليها، وهي أبسط أنواع حماية المعلومات على شبكة المعلومات فهي تعمل على حماية معلوماتك الشخصية ومعلومات العمل الخاصة بك وسجلاتك الشخصية، وغيرها من البيانات، كما أنها في بعض الأحيان تكون حماية للأفعال مثل كلمة السر في المشتريات والحسابات البنكية وغيرها. ومن أهمية كلمة المرور يجب علينا أن نحرص عليها وعند اختيارها يجب مراعاة ثلاثة أمور هي:

- اختيار كلمة مرور صعبة ولا يسهل تخمينها.
- عدم إطلاع الغير عليها.
- تغييرها بشكل دوري.
- لا تجعل كلمة المرور كلمة واحدة مثل ragab.
- لا تضمن كلمة المرور بيانات شخصية عنك مثل تاريخ الميلاد.
- لا ينبغي أن تقل كلمة المرور عن عشرة خانات.
- اجعل كلمة المرور خليط بين الحروف والأرقام.

ثانيًا: جدران الحماية Firewalls:

يكون جدار الحماية الناري إما برنامجًا أو جهازًا يستخدم لحماية الشبكة والخادم من المتسللين، وتختلف جدران الحماية حسب احتياجات المستخدم، فإذا استدعت الحاجة إلى وضع جدار الحماية على عقدة منفردة عاملة على شبكة واحدة فإن جدار الحماية الشخصي هو الخيار المناسب، وفي حالة وجود حركة مرور داخلة وخارجة من عدد من الشبكات، فيتم استخدام مصافي لجدار الحماية في الشبكة لتصفية جميع الحركة المرورية.

وفي بعض الأحيان تقوم بعض شبكات المعلومات بوضع جدران حماية لعزل شبكتها الداخلية عن شبكة الإنترنت، ولا يكون هذا العزل كليًا بالطبع حتى يمكن للمستخدمين الاستفادة من بعض خدمات الإنترنت وفي نفس الوقت منع المخربين من الدخول إلى الشبكة الداخلية أو اختراق أمن وسرية المعلومات على الشبكة.

وبالطبع فإن هناك العديد من أنواع جدران الحماية التي تلائم كافة أنواع شبكات المعلومات وفقًا لحجم الشبكة والمؤسسة التي تعمل عليها، فهناك جدران الحماية التي تكون للمؤسسات الحكومية والشركات الكبيرة ذات سرعات وقدرات عالية جدًا، مثل ما توفره شركة Sisco كما أن هناك جدران حماية للمنشآت الصغيرة والشركات المحدودة، وهناك أيضًا

برامج جدران الحماية التي يتم تحميلها على الحواسيب الشخصية لحماية الجهاز فقط.

ثالثًا: تحويل العناوين الرقمية Network Address Translation:

تقنية NAT تعتمد على إعطاء كل حاسوب متصل بالشبكة رقم مميز يختلف عن باقي الأجهزة، وتقوم منظمة Internet Assigned Numbers Authority IANA بإعطاء هذه الأرقام ولا يكون معترفًا بها إلا عن طريقها، ونظرًا لقلة هذه الأرقام فإنه يعطى رقم واحد للشبكة ثم تقوم هذه الشبكة بإعطاء أرقام داخلية للحواسيب المرتبطة بها بحيث لا يتكرر أي رقم، وعندما يرغب جهاز حاسوب من الشبكة الداخلية في الاتصال بشبكة خارجية يأتي هنا دور تقنية NAT حيث نقوم بتنصيب جهاز حاسوب يلعب دور الوسيط بين الشبكة الداخلية والشبكة الخارجية ويحمل الرقم المعترف به المعطى من قبل IANA للشبكة الأم، ويكون مهمته تحويل العنوان الرقمي الداخلي إلى عنوان رقمي خارجي معترف به من قبل LANA ومن ثم يقوم بإرسال المعلومات من الشبكة الداخلية إلى الشبكة الخارجية، وكذلك في استقبال المعلومات من الخارج يقوم بعكس الوظيفة وإرسال المعلومات إلى رقم الجهاز في الشبكة الداخلية، وغالبًا ما يكون هذا الجهاز الوسيط الذي يقوم بتطبيق تقنية NAT إما جدار حماية ناري Firewall أو موزع Router.

رابعًا: التحديث التلقائيAutomatic Update:

يعد التحديث الدائم والتلقائي للبرامج وأنظمة التشغيل من أهم نقاط حماية أمن شبكات المعلومات، ذلك أن عملية بناء هذه النظم هي غاية في التعقيد ولا تخلو من بعض الأخطاء التي تحدث في فترات البناء وتعمل الشركات عادة على إيجاد التحسينات المستمرة لسد نقاط الضعف في هذه البرامج والأنظمة، وهذه التحسينات تتاح دائمًا فيما يعرف بالتحديثات، ومن ثم تأتي أهمية أن يقوم الشخص بعمليات التحديث الدائم للبرامج والأنظمة التي يتبناها في جهازه الشخصي على المستوى الفردي وعلى مستوى البرامج والأجهزة المستخدمة في شبكات المعلومات، ونظرًا لصعوبة مطالبة الشركات لمستخدمي هذه البرامج بتحديث البرامج بأنفسهم فإن معظم الشركات المصنعة لهذه البرامج قامت بإضافة خاصية التحديث الآلي والتلقائي لهذه البرامج، ولكي تعمل هذه الخاصية يقوم البرنامج المثبت في الشبكة بالاتصال تلقائيًا وعلى فترات معينة بالشركة المنتجة له والقيام بالبحث عن آية تحديثات جديدة وتنزيلها تلقائيًا.

خامسًا: التشفير Encryption:

التشفير هو 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 التشفير المعلومات في جهازك غير قابلة للقراءة من قبل أي شخص يستطيع أن يتسلل خلسة إلى جهازك دون إذن.

عبارة عن إدخال تعديلات على المعلومات عند إرسالها إلى جهة معينة، أو تحويلها إلى رموز غير ذات معنى؛ حيث عندما تصل إلى أشخاص آخرين لا يستطيعون فهمها أو الاستفادة منها، لذا فهي عبارة عن تشفير وتحويل للنصوص العادية الواضحة إلى نصوص مشفرة وغير مفهومة، وتبنى على أساس أن كل معلومة تحتاج لفكها وإعادتها إلى الوضع الأصلي شفرة.

ويستخدم مفاتيح تشفير Encryption النصوص المرسلة وفك الشفرة من قبل صاحبها والمسموح له بتسلمها، وتستند هذه المفاتيح إلى صيغ رياضية معقدة في شكل خوارزميات وتعتمد قوة وفعالية التشفير على نوعية الخوارزميات، ومازالت تلك العملية تتم بواسطة مفتاح سري يعتمد لتشفير النصوص وفي نفس الوقت لفك تشفيرها وترجمتها إلى وضعها الأصلي باستخدام نفس المفتاح السري، وهو ما يعرف بالتشفير المتناظر Symmetric، ثم جاء ما يعرف بالتشفير اللامتناظر

Asymmetric حلا لمشكلة التوزيع الغير أمن للمفاتيح في عملية التشفير المتناظر معوضًا عن استخدام مفتاح واحد باستخدام مفتاحين اثنين مرتبطين بعلاقة رياضية عند بنائهما، وهما مفتاحان الأول: المفتاح العام؛ والثاني: المفتاح الخاص.

سادسًا: التخزين الاحتياطي Backup:

النسخ الاحتياطي Backup هو عمل نسخ احتياطية من محتويات الحواسيب أو شبكات المعلومات وحفظ هذه النسخ الاحتياطية في مكان آمن بعيد، بحيث يمكن الرجوع إليها في حالة حدوث أعطال أو حوادث وكوراث للشبكة وتدميرها لأي سبب كان، وعادةً ما يتم أخذ هذه النسخ بشكل دوري وفق النظام المتبع على الشبكة أسبوعيًا أو شهريًا أو حتى يوميًا، كما أنه في أغلب الأحوال يتم أخذ هذه النسخ بطريقة آلية من النظام نفسه في وقت محدد.

وتعد هذه الطريقة من أهم وأسهل الطرق التي يمكن من خلالها الحفاظ على سلامة المعلومات الخاصة بشبكات المعلومات وخاصة في حالة التدمير الكامل للشبكة أو اختراقها بهدف محو وتدمير البيانات والمعلومات المتاحة عليها، وتكون في هذه الحالة النسخ الاحتياطية هي الملاذ الآمن لمحتويات الشبكات، وأخذ النسخ الاحتياطية من محتويات

شبكات المعلومات تعد من أبجديات الأمن والسلامة للمعلومات والشبكات. ويقدم المختصون بشبكات المعلومات والنظم عدة نصائح يجب على الفرد اتباعها عند القيام بعمل نسخ احتياطية من محتوى شبكات المعلومات وهي:-

١. حفظ النسخ الاحتياطية Backup في مكان بعيد وآمن وسري، ويفضل أن يكون المكان بعيد عن مقر الشبكة الأم أو المؤسسة المالكة للشبكة تفاديًا لضياع هذه النسخ في حالة قيام الكوارث الطبيعية في نفس المكان، فيكون قد ضاعت المعلومات الأصلية والنسخ الاحتياطية أيضًا معها.
٢. اختيار وسائط تخزين ذات جودة عالية تقاوم عوامل الزمن ولا تتقادم تكنولوجيًا بسرعة.
٣. القيام بعمليات النسخ الاحتياطي بشكل دوري وفقًا للسياسة المتبعة والإجراءات الخاصة بالمؤسسة المالكة لشبكة المعلومات، وفي كل الأحوال ينبغي ألا تزيد المدة عن شهر.

١٠/متطلبات أمن شبكات المعلومات:

تحدثنا عن المخاطر التي تحيط بشبكات المعلومات والوسائل والإجراءات التي يمكن من خلالها مكافحة ومواجهة هذه المخاطر،

وفيما يلي بعض النصائح العامة التي يمكن وضعها في الاعتبار كوسائل احترازية يمكن تطبيقها والتي يمكن التعبير عنها بأنها من متطلبات أمن الشبكة بصفة عامة وهي كالتالي:

١. **تحديد سياسات العمل في شبكات المعلومات:** بأن تكون واضحة تمام الوضوح ما هو المسموح به والممنوع فيما يتعلق بأمن المعلومات على الشبكة.
٢. **توفير آليات تنفيذ سياسات العمل:** بأن يكون معروفًا كيفية تنفيذ هذه السياسات وما هي العقوبات التي ستوقع في حالة المخالفة.
٣. **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.
٤. **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.
٥. **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 وتفادي تفاقم الأوضاع.

٦. **حسن اختيار مواقع نقاط الشبكة:** فيجب أن يتم التدقيق جيدًا عند اختيار نقاط الاتصال بشبكات المعلومات، وأن تكون هذه النقاط في مواقع جيدة ومؤمنة ومحمية.

٧. **بروتوكولات 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.

الفصل الرابع

خطة وسياسة أمن وحماية المعلومات

١/ خطة أمن وحماية المعلومات:

إن ضمان عناصر أمن المعلومات كلها او بعضها يعتمد على المعلومات محل الحماية واستخداماتها وعلى الخدمات المتصلة بها، فليس كل المعلومات تتطلب السرية وضمان عدم الافشاء، وليس كل المعلومات بذات الاهمية من حيث الوصول لها او ضمان عدم العبث بها، ولهذا تنطلق خطط امن المعلومات من الاجابة على سلسلة تساؤلات متتالية وهي:

- **هل كل المعلومات تحتاج لعناصر الحماية ذاتها وبذات القدر؟**

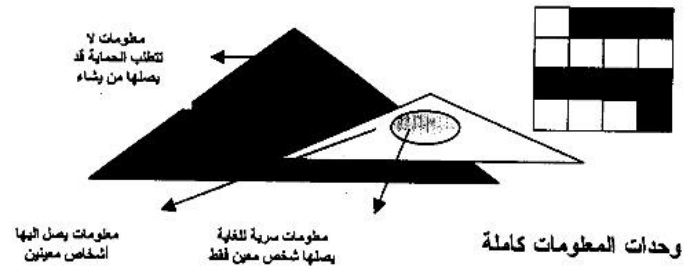
إن ضمان عناصر أمن المعلومات كلها أو بعضها يعتمد على المعلومات محل الحماية واستخداماتها وعلى الخدمات المتصلة بها، فليس كل المعلومات تتطلب السرية وضمان عدم الإفشاء، وليس كل المعلومات في منشأة واحدة بذات الأهمية من حيث الوصول لها أو ضمان عدم العبث بها، لهذا تنطلق خطط أمن المعلومات من الإجابة عن سلسلة تساؤلات متتالية:

- **التساؤل الأول: ما الذي نريد أن نحميه؟**

وإجابة هذا التساؤل تحدد تصنيف البيانات والمعلومات من حيث أهمية الحماية، إذ تصنف المعلومات تبعا لكل حالة على حدة، من

معلومات لا تتطلب الحماية، إلى معلومات تتطلب حماية قصوى (انظر الشكل ١).

شكل رقم (1)



- **التساؤل الثاني: ما المخاطر التي ينبغي حماية المعلومات من التعرض لها؟**

وتبدأ عملية تحديد المخاطر بتصور كل خطر قد يمس المعلومات محل الحماية أو يهدد أمنها، ابتداء من قطع مصدر الكهرباء عن الكمبيوتر وحتى مخاطر اختراق النظام من الخارج بواحد أو أكثر من وسائل الاختراق عبر نقاط الضعف، مروراً بإساءة الموظفين استخدام كلمات السر المعدة لهم، وتصنف هذه المخاطر ضمن قوائم تبعا لأساس التصنيف، فتصنف كمخاطر من حيث مصدرها ومن حيث وسائل تنفيذها، ومن حيث غرض المتسببين بهذه المخاطر، ومن حيث أثرها على نظام الحماية وعلى المعلومات محل الحماية. وهو ما

استعرضناه سابقا بشكل تفصيلي. ومتى ما تم الانتهاء من هذا التحديد يجري الانتقال إلى التساؤل التالي.

- **التساؤل الثالث: كيف يتم توفير الحماية لما نرغب بحمايته من المخاطر التي تم تحديدها(وسائل الحماية)؟**

وهنا تجد كل منشأة وكل هيئة طريقتها الخاصة في توفير الأمن من المخاطر محل التحديد وبحدود متطلبات حماية المعلومات المخصوصة التي تم تحديدها وبحدود امكاناتها المادية والميزانية المخصصة للحماية، فلا تكون إجراءات الأمن رخوة ضعيفة لا تكفل الحماية وبالمقابل لا تكون مبالغاً بها إلى حد يؤثر على عنصر الأداء في النظام محل الحماية.

وفي بيئة المعلومات فمن الطبيعي مثلا أن نضع على جهاز الكمبيوتر الشخصي كلمة سر للولوج إلى الملفات الهامة أو حتى للنظام كله وأن لا نعطي الكلمة لأحد، وأن نضع برنامجاً أو أكثر لمقاومة الفيروسات الإلكترونية الضارة، ونراعي إجراءات مقبولة في حماية الدخول إلى شبكة الانترنت والتأكد من مصدر البريد الإلكتروني مثلا. فإذا كان الكمبيوتر خاص بشركة أو مؤسسة ويضم بيانات هامة ومصنف أنها سرية، كان لزاما زيادة إجراءات الأمن، فمثلا يضاف

للنظام جدران نارية تحد من دخول أشخاص من الخارج وتمنع اعتداءات منظمة قد يتعرض لها النظام أو الموقع المعلوماتي، وإذا كان النظام يتبادل رسائل إلكترونية يخشي على بياناتها من الإفشاء، تكون تقنيات التشفير مطلوبة بالقدر المناسب.

بمعني أن إجراءات الحماية تنطلق من احتياجات الحماية اللازمة، فإن زادت عن حدها أمست ذات أثر سلبي على الأداء، فأصبح الموقع أو النظام بطيئا وغير فاعل في أداء مهامه الطبيعية، وإن نقصت عن الحد المطلوب، ازدادت نقاط الضعف وأصبح أكثر عرضه للاختراق الداخلي والخارجي. فإذا فرغنا من اختيار وسائل الحماية التقنية واستراتيجياتها الإدارية والأدائية الملائمة، انتقلنا بعدئذ إلى التساؤل الأخير.

- **التساؤل الرابع: ما الذي يجب فعله إذا ما تحقق أي من المخاطر رغم وسائل الحماية؟**

وإجابة هذا التساؤل هو ما يعرف بخطط مواجهة الأخطار عند حصولها، وتتضمن مراحل متتالية، تبدأ من مرحلة الإجراءات التقنية والإدارية والإعلامية والقانونية اللازمة عند حصول ذلك، ومرحلة إجراءات التحليل لطبيعية المخاطر التي حصلت وسبب حصولها

وكيفية منع حصولها لاحقاً. وأخيرا إجراءات التعافي والعودة إلى الوضع الطبيعي قبل حصول الخطر مع مراعاة تنفيذ ما أظهره التحليل عن كيفية حصول المخاطر وضمان عدم حصولها.

إذن، وفي الوقت التي تتطلب بعض المعلومات كالمتصلة بالأمن القومي والأسرار العسكرية مثلا إيلاء عنصري السرية والتكاملية أقصى درجات الاهتمام، نجد بالنسبة للبنوك أنه إضافة للعنصرين المتقدمين يتعين بالنسبة للنظام نفسه ايلاء عنصر الاستمرارية ذات القدر من الأهمية، فأن عملت المصارف في حقل البنوك الإلكترونية أو الخدمات المصرفية الإلكترونية عند بعد، كان عنصر عدم الإنكار بنفس أهمية بقية العناصر.

ونجد أن مواقع الإنترنت مثلا تتطلب ايلاء عنصر الاستمرارية الاهتمام الأكبر، في حين أن مواقع التجارة الإلكترونية من بين مواقع الانترنت تتطلب الحرص على توفير عناصر الحماية الأربعة بنفس القدر والأهمية إذ تحتاج ضمان السرية، وتحديداً بالنسبة للبيانات الخاصة بالزبائن كأرقام بطاقات الائتمان، وتتطلب التكاملية والسلامة بالنسبة للبيانات المتبادلة عبر الرسائل الإلكترونية بين الزبون والموقع، فلا يصل أمر الشراء مثلا وقد لحقه تغيير أو تحريف ما، وتتطلب استمرارية الموقع في تقديم خدماته وقدرة الزبون على الولوج إليه طوال

وقت سريان عملية التصفح والشراء بل وفي أي وقت يريد للدخول إلى الموقع، وتتطلب ضمان عدم إنكار الزبون إن التصرف الذي أجراه على الموقع (كطلب الشراء) قد صدر عنه أو إنكار الموقع نفسه أنه تعاقد مع الزبون في شأن ما.

٢/ سياسة أمن المعلومات Definition of Security Policy:

سياسة أمن المعلومات هي توثيق خطة عالية المستوى في مؤسسة تعتمد الحاسب الآلي في نشاطها، لتوفر هيكلا لاتخاذ قرارات محددة، لحماية تلك الأجهزة التقنية أثناء استخدامها، ودليل تطوير أمن البرامج، وإجراءات المستفيدين، ومدراء النظام، لتكفل أمن المعلومات في تلك المؤسسة"

وهي عبارة عن تعبير رسمي يقصد به مجموعة القواعد والقوانين التي يتم تطبيقها عند التعامل مع المعلومات والتقنيات المرتبطة بها داخل المنشأة فهي توضح ما هو مسموح به وما لا يسمح به. ترتبط سياسة أمن المعلومات بطرق الوصول للمعلومات وإدارتها والعمليات عليها. وهي تُعنى بتعريف المعاملات والحلول الأمنية تجاه كل معاملة ولكنها لا تهتم بكيفية صياغة وهندسة هذه الحلول. يتم تعزيز سياسة

أمن المعلومات، في مرحلة التطبيق نظام أمن المعلومات، بواسطة مجموعة الإجراءات والادوات والطرق التي يصطلح على تسميتها بـ "Security Mechanisms" والتي تمثل الآليات لتطبيق سياسات أمن المعلومات.

١/٢ أهداف سياسة أمن المعلومات Security Policy Goals:

- ترجمة وتوضيح الأمن كما تم تعريفه في القواعد والمبادئ والأهداف العليا للمنظمة
- تعريف المستخدمين بمسؤولياتهم وواجباتهم تجاه أمن نظم المعلومات والذي يتضمن الأفراد الأجهزة، البرامج، المعلومات...الخ
- بيان الإجراءات التي يجب إتباعها لتفادي المخاطر والمهددات والتعامل معها إذا ما وقعت
- تحديد الآليات التي يتم من خلالها تنفيذ وتحقيق المسؤوليات والواجبات لكل مستخدم

٢/٢خصائص ومميزات سياسة الأمن Security Policy Characteristics of

- يجب أن تكون مناسبة اقتصاديا (ذات جدوى اقتصادية)
- يجب أن تكون مفهومة للمستخدمين

- يجب أن تكون واقعية تتناسب مع واقع المنظمة
- يجب أن تكون متناغمة مع أهداف المنظمة
- يجب أن تكون مرنة وقابلة للمعالجة
- يجب أن توفر حماية معقولة لأهداف الإدارة المعلنة
- يجب أن تكون مستقلة أي (لا تعتمد على أجهزة Hardware ولا برامج Software محددة)

أما خصائص سياسة الأمن الجيدة Characteristic of Good Security Policy

- يجب أن تكون قابلة للتطبيق Implementable من خلال الإجراءات والتوجيهات الإدارية
- يجب تدعيمها بالأدوات الأمنية والقوانين والمراسيم الإدارية
- يجب تحديد المسؤوليات على كل مستويات الهيكل التنظيمي
- يجب أن تكون موزعة Distributed على كل وحدات المنظمة
- يجب أن تكون موثقة Documented (للمرجعية)
- يجب أن تكون مرنة وفعالة لأطول فترة ممكنة وحتى تتحقق هذه الخاصية فلابد من أن تكون مستقلة Independent عن أي Hardware أو Software لان هذين العنصرين يتغيران بشكل سريع.

٣/٢ مكونات سياسة الأمن Security Policy Composition:

تتكون استراتيجية أمن المعلومات من ثلاث مكونات هي:

١. **الاستراتيجية** نفسها والتي توثق لدوافع حماية المؤسسة لبياناتها وما هي هذه البيانات والتي يمكن بناءها في الخطوات التالية:

- تحديد المادة Subject (الموضوع) محل الاهتمام والمراد عمل الاستراتيجية لها.
- ما هي العمليات والنشاطات المسموح بها وما هي المرفوضة(غير المسموح بها) ولمن من المستخدمين
- تحديد الأشخاص (المستخدمين) المتأثرين بهذه الاستراتيجية
- تحديد كيفية تطبيق الاستراتيجية في بيئة المنظمة
- تحديد المخاطر المتوقعة في البيئة المحددة
- تحديد وتصنيف البيانات وموارد النظام
- تحديد خدمات الأمن الأساسية في بيئة المنظمة
- تحديد قائمة بالسياسات التي تم إنشاءها
- إنشاء تحليل لانسياب البيانات المصنفة منذ مرحلة الإنشاء وحتى الحذف من النظام
- توثيق الاستراتيجية

٢. **المعايير Standard** وهي توثق لماهية المقاصد المنشودة لتطبيق وإدارة أمن المعلومات في المنظمة.

٣. **الإجراءات Procedures** وهي توثق للكيفية التي تنجز بها المنظمة المتطلبات المفروضة بالمعايير والاستراتيجيات. وهي الأدوات التي بها يتم تحويل السياسات إلى أحداث وعمليات.

بعد إنشاء السياسات يجب توزيعها على كل مستويات الهيكل التنظيمي (مستخدمين ، موظفين ،الإدارة ، الزبائن ،الاستشاريين ...الخ.

لضمان صلاحية السياسات يجب تعهدها بالمراجعة المستمرة وذلك بتحديث آلياتها وأدواتها ويجب عكس التغييرات في بيئة عمل المنظمة على سياسات التأمين أول بأول.

٤/٢ أنواع سياسات أمن المعلومات:

تتمثل أنواع سياسات أمن المعلومات فى التالي:

١/ سياسات الحماية الإدارية : ويقصد بها سيطرة إدارة تقنية المعلومات على ادارة نظم المعلومات وقواعدها مثل التحكم بالبرمجيات الخارجية او الاجنبية عن المنشأة ، ومسائل التحقيق باخلالات الأمن، ومسائل الاشراف والمتابعة لأنشطة الرقابة اضافة الى القيام بانشطة

الرقابة ضمن المستويات العليا ومن ضمنها مسائل مراقبة توقيع الموظفين على الالتزام بكافة السياسات والإجراءات والمعايير والإرشادات الخاصة بأمن المعلومات، التأكد من حصول الموظفين بصورة منتظمة بالتحديثات التي تتمثل بالسياسات والإجراءات ويكون لها صلة بمسئولياتهم الوظيفية تجاه أمن المعلومات، سحب حقوق وصلاحيات استخدام الموظف لموارد وأجهزة تقنية المعلومات عند إنهاء خدمته وإقامة الدورات التدريبية للموظفين الجدد حول سياسات وإجراءات امن المعلومات في المؤسسة

٢/ سياسات تحديد الهوية الآلية لأمن المعلومات : وتشمل كافة الوسائل التي تمنع الوصول الى نظم المعلومات وقواعدها ، مثل المقاييس الحيوية ، أدوات تكنولوجيا متقدمة وأنظمة الحماية البيئية التي تمنع الوصول الى الاجهزة الحساسة .

٣/ سياسات الحماية الفنية: وهى تتعلق بالوسائل الخاصة بحماية الأجهزة وبرامج نظم التشغيل وبرامج التطبيقات وشبكات الاتصال، مثل سياسات كلمات المرور، سياسات برامج الحماية والجدران النارية، سياسات التحكم بالوصول، سياسات إدارة أصول المعلومات، تشفير البيانات، سياسات النسخ الاحتياطي، سياسات إدارة وصول المستخدمين، وسياسات التعامل مع البريد الالكتروني.

٤/ سياسات تقدير المخاطر: وتشمل تقدير المخاطر والتهديدات التى يتعرض لها نظام معلومات المؤسسة نتيجة قلة الخبرة و الوعي والتدريب لمستخدمى نظام المعلومات بالمؤسسة، وتقدير المخاطر والتهديدات التي يتعرض لها نظام معلومات المؤسسة نتيجة لعدم توافر أو ضعف الأدوات والأجهزة والبرامج الرقابية المستخدمة.

الفصل الخامس

الخصوصية وأمن المعلومات
ومخاطر التقنيات الحديثة عليها

مقدمة:

ترتبط البيانات الخاصة بالأفراد بالخصوصية وأحياناً بالسرية، وهو ما ينسحب غالبا على الوثائق بجميع أشكالها وصورها سواء أكانت في شكل تقليدي مثل السجلات والدفاتر الورقية والوثائق المفردة أم كانت في شكل غير تقليدي مثل الميكروفيلم والوثائق الرقمية والمحولة رقمياً. ومنذ المحاولات الأولى لوضع قواعد لإتاحة البيانات وحرية تداول المعلومات وهناك إشكالية يتم تداولها بشكل دائم ألا وهي مشكلة حدود العلاقة بين حرية إتاحة المعلومات وتداولها وبين الخصوصية وسرية البيانات الشخصية. وقد كانت الوثائق ودور الأرشيف دائما محط أنظار المتسللين والسارقين ومحبي الاطلاع على بيانات أو أسرار الغير سواء أكان أحد الجانبين أو كلاهما أفراداً أو هيئات وكيانات اعتبارية.

ومع التطور التكنولوجي ودخول التقنيات الحديثة مجال إدارة الوثائق زاد الجدل حول هذه النقاط وأصبحت بيانات الأفراد والمؤسسات في مهب ريح التكنولوجيا الحديثة التي أصبحت تمثل شبحا مرعبا لكل الكيانات والهيئات العاملة بالأرشيف والحاضنة له، ولكل الأفراد الذين لهم وثائق تحوي بيانات سرية أو شخصية عنهم. وأصبحت مؤسسات إدارة الوثائق وحفظها هدفاً للجريمة المعلوماتية مثلها مثل بقية

المؤسسات والهيئات، كما أصبحت البيانات الشخصية للأفراد هدفاً آخر لهذه الجريمة.

حيث بات من السهل للغاية التسلل إلى البيانات الشخصية للأفراد من خلال البرمجيات الحديثة وتطبيقات الهواتف المحمولة التي تطلب أحياناً من الأشخاص أنفسهم أذون للسماح لها للولوج إلى هواتفهم وحساباتهم الشخصية وبياناتهم الخاصة بل والولوج إلى حياتهم الخاصة نفسها من خلال كاميرات وميكروفونات الحواسب المكتبية والمحمولة والهواتف الذكية، وأصبح الكثيرون يعطون أذوناً بذلك للبرامج الحديثة وتطبيقات الحاسب الآلي والهواتف المحمولة دون دراية بالخطر المحدق بهم من خلال هذه التقنيات الحديثة الذي لا يقتصر على التسلل إلى معلوماتهم وبياناتهم الخاصة فقط بل تستطيع هذه التطبيقات في كثير من الأحيان السيطرة على حساباتهم الالكترونية المختلفة وأحيانا على مكونات هواتفهم المحمولة وحاسباتهم الخاصة نفسها.

١/تعريف الخصوصية:

ما الخصوصية؟ وماذا يقصد بها تحديداً بالنسبة للأفراد وبالنسبة للهيئات؟

هذا السؤال يطرح نفسه عند الحديث عن حماية بيانات الأشخاص والهيئات داخل الوثائق. ويستمر المدافعون عن حرية تداول المعلومات في الدفاع عن موقفهم ضد الخصوصية ويعتبرونها قيداً على تداول المعلومات وحاجباً للشفافية ومجرد ذريعة لحجب معلومات معينة عن فئة أو أكثر أو لاستحواذ فرد أو هيئة على هذه المعلومات بشكل حصري.

بينما يدافع أصحاب الرأي الآخر عن موقفهم بوجوب حجب معلومات أو بيانات معينة وضمان سريتها بأن لكل فرد الحق في خصوصيته وعدم إفشاء معلومات أو بيانات خاصة به إلا بإذنه ورغبته، والأمر نفسه بالنسبة للكيانات الاعتبارية التي يحق لها الاحتفاظ ببيانات و/ أو معلومات خاصة عنها أو عن العاملين بها وعدم أحقية أي شخص في الاطلاع عليها بدون إذن أو ترخيص.

والحقيقة أنه لا يوجد تعريف علمي محدد وجامع للخصوصية، ويرجع السبب في عدم تحديد تعريف واضح للخصوصية أو الحياة الخاصة إلى تنوع العادات والتقاليد واختلافها بين المجتمعات وإلى تطور تلك المفاهيم الاجتماعية والسياسية والاقتصادية والدينية والثقافية، وتبدل مفهوم الحياة الخاصة نفسه وتطوره باستمرار، وبين التطور

التكنولوجي والقدرة على الوصول إلى المعلومات والبيانات بطرق غير مشروعة من ناحية أخرى.

ويعرف البروفيسور الأمريكي وأستاذ القانون الدولي آلان ويستن Alan Westin مؤلف كتاب "الحرية والخصوصية Privacy and Freedom " 1967 خصوصية المعلومات أو الحق في الحياة الخاصة أو الحرمة الشخصية بأنها "حق الأفراد أو الجماعات أو المؤسسات في أن يقرروا بأنفسهم زمن وكيفية ومدى نقل المعلومات عن أنفسهم الى الآخرين.

في حين عرفها ميلر Miller مؤلف كتاب "الاعتداء على الحرية The Assault on Privacy " بأنها " قدرة الأفراد في التحكم بدورة المعلومات التي تتعلق بهم".

ويعرف محمد الطاهر الخصوصية بأنها "قدرة الأشخاص في التحكم في سرية بياناتهم ومعلوماتهم الشخصية والتحكم في من يمكنه الوصول لهذه المعلومات سواء أكانوا أفراداً آخرين أو حكومات أو حواسيب

ومع تطور وسائل الاتصال تطور مفهوم الخصوصية على الانترنت ليعني كل عمليات جمع المعلومات الشخصية على الخط المباشر On Line واستخدامها مثل اسم الشخص أو عنوانه أو رقم هاتفه أو حالته

العائلية أو ضمانه الاجتماعي أو غير ذلك من المعلومات الشخصية الأكثر عمقا مثل رقم الهوية والإحصاءات المالية والصحية.

وقد عرف المجلس الدولي للأرشيف الخصوصية بأنها: الحق في ضمان عدم إفشاء المعلومات غير المصرح بها، الواردة في الوثائق الجارية/ الوثائق الأرشيفية والتي تتعلق بموضوعات شخصية أو خاصة.

كما عرف حماية البيانات بأنها: الحماية القانونية لحقوق الأفراد الخاصة بجمع البيانات الشخصية ومعالجتها وتخزينها في شكل مقروء آلياً وإتاحة مثل هذه البيانات.

بينما عرف رفع السرية بأنه: إزالة جميع القيود السرية المفروضة على المعلومات أو الوثائق".

وقد حددت المعايير القانونية الدولية التي صدرت في القرن العشرين الخصوصية كحق من حقوق الإنسان التي يجب احترامها وصيانتها حيث تضمن الإعلان العالمي لحقوق الإنسان الصادر ١٩٤٨، أول محاولة لحماية الخصوصية كحق إنساني متميز فنصت المادة ١٢ منه على ما يلي: "لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو المنزل أو المراسلات ، ولا الهجمات على

شرفه وسمعته فلكل فرد الحق في حماية القانون من مثل هذا التدخل أو الهجمات

ويمكن القول أن تطور التكنولوجيا الحديثة يزيد من الحاجة إلى تحديد وتطوير مفهوم الخصوصية بما يتلائم مع كل وضع جديد أو إمكانية تكنولوجية تستحدث في الكشف عن المعلومات أو اختراق خصوصية وحسابات الأفراد والهيئات أو حتى الحكومات نفسها، فلكل فرد الحق في الخصوصية علي الإنترنت بما في ذلك الحق في حماية البيانات الشخصية التي تتعلق به، والحق في اتصال مجهول الهوية على شبكة الانترنت واستخدام التكنولوجيا المناسبة لضمان اتصال آمن وخاص ومجهول.

٢/ الخصوصية وأمن المعلومات:

قد يبدو مصطلح الخصوصية متداخل مع أمن المعلومات أو أنه جزء منه أو أن كلا الأمرين يمثلان الشئ نفسه، لكن في الحقيقة هناك بعض الاختلافات الجوهرية بين الخصوصية وأمن المعلومات وإن كانا مرتبطين معاً في عدة أمور.

فالفارق بين أمن المعلومات وخصوصية البيانات الشخصية هو أن المعلومات معنى عام لكل ما تم حفظه لغرض الاطلاع المحدد وقد

يكون معلومات تخص أي شخص أو كيان أو جهة وتشمل جميع المعاملات والأنشطة البشرية، وأن مصطلح أمن المعلومات يشار به إلى الوسائل والاحتياطات والبرمجيات التي تعمل على ضمان سلامة نظم حفظ المعلومات نفسها وعدم اختراقها أو تعطيلها او تدميرها أو السيطرة عليها بأي شكل ومن خلال أي فرد أو كيان؛ بينما تتمحور الخصوصية حول البيانات المتعلقة بشخص أو كيان واللصيقة الصلة به في حد ذاته وليست المعلومات حوله أو حول أنشطته. وقد تكون خصوصية وسرية البيانات الشخصية للأفراد جزء أو مكون من مكونات أمن المعلومات في نظم المعلومات وأمن الشبكات.

والحقيقة أن كلاً من الخصوصية وأمن المعلومات تتهددهم العديد من الأخطار منها التطورات التكنولوجية المتسارعة، والمشكلات الفنية المتزايدة، والضعف البشري، وضعف قدرة الهيئات والكيانات الاعتبارية على مواجهة المتغيرات المتلاحقة، حيث تتبع التهديدات والمخاطر التي تواجه نظم المعلومات من الأفعال والتصرفات المقصودة وغير المقصودة علي السواء التي قد ترد من مصادر داخلية أو خارجية.

٣/بين خصوصية الأفراد وخصوصية الهيئات والكيانات:

أول ما يتبادر إلى الذهن عند الحديث عن مفهوم الخصوصية هو خصوصية الأفراد. ولكن يجب التنبيه على أن الهيئات والكيانات الاعتبارية سواء الاجتماعية أو حتى الحكومية تشارك الأفراد في الخصوصية وينبغي صياغة بروتوكول أو قواعد أو سياسة تحدد هذه الخصوصية بشكل واضح.

فبينما يمكن فهم خصوصية الأفراد أو ما يسمى الحياة الخاصة للأفراد على أنها البيانات اللصيقة الصلة بالشخص ذاته، يمكن فهم خصوصية الكيانات والهيئات من خلال مجموعة البيانات أو المعلومات التي يحجبها الكيان أو الهيئة عن الاطلاع العام ويحدد أدوار من يمكن لهم الاطلاع عليها وإلى أي مستوى يستطيع صاحب كل دور الوصول بدقة. ولا يمكن تأمين الأنظمة الحاسوبية وحمايتها بأدوات وبرمجيات فقط؛ فتطبيق أمن المعلومات بشكل كامل يتطلب بالإضافة إلى ذلك الاهتمام بالجانب البشري وكذلك سن السياسات والإجراءات الأمنية للتعامل مع المعلومات والمعدات والبرمجيات والمستخدمين بشكل منظم ومدروس.

٤/سياسة الخصوصية:

سياسة الخصوصية Privacy Policy عبارة عن وثيقة تتضمن مجموعة البنود والشروط التي توضح كيفية تعامل الجهة أو المنظمة أو الموقع الالكتروني مع البيانات والمعلومات التي يجمعها عن العملاء أو الزبائن أو أعضاء الجهة أو رواد وزوار الموقع الالكتروني، ومستوى الولوج المطلوب لبياناتهم، وطريقة تصرف الجهة في هذه المعلومات سواء بالنشر أو الإتاحة أو حتى البيع، حيث تعتبر سياسة الخصوصية تطبيقا لمبدأ الإشعار أو التوعية بإعطاء المستهلكين إشعارًا بممارسات المعلومات الخاصة بالهيئة أو الجهة قبل تجميع المعلومات الشخصية منهم.

وفي سياق تكنولوجيا المعلومات، يمكن تعريف سياسة الخصوصية بأنها وثيقة تطلع القراء على كيفية استخدام منتج أو مزود بالخدمة لمعلوماتهم الشخصية، ومن المفترض أن يعلن أي كيان أو جهة تقوم بجمع بيانات و/ أو معلومات عن الأفراد أو الهيئات أو تخول بالاطلاع عليها أو حتى تشارك في صنعها وانتاجها سواء بشكل تقليدي أو غير تقليدي عن سياسة الخصوصية لديها. وعادة ما يقترن استخدام مصطلح "سياسة الخصوصية" بتكنولوجيا المعلومات الرقمية لأن منتجات وتطبيقات ونظم تكنولوجيا المعلومات الرقمية تجمع المعلومات و/أو

البيانات الشخصية من/ عن المستخدمين وتستخدمها بطرق مختلفة وبشكل موسع ودوري.

وتختلف سياسة الخصوصية من موقع الكتروني أو تطبيق لآخر في مستوى الولوج لبيانات المستخدمين الشخصية ومعلوماتهم السرية وفي مستويات نشرها أو تخزينها أو تصديرها لمواقع أو تطبيقات أخرى تابعة لتلك المواقع أو التطبيقات أو مرتبطة بها. ومن المفترض أن تقوم المواقع المختلفة بشرح وإيضاح سياسة الخصوصية لديها لمستخدميها بكل وضوح وشفافية حتى يتسنى لهم الوقوف على مستويات الأمان لدى مستخدمي هذه المواقع، مثال الوثيقة التي تثبتها شركة جوجل على موقعها الشهير، وتحدثها بشكل دائم، وتوضح بها ثلاثة أمور مهمة وهي:

١. المعلومات التي يجمعها الموقع عن مستخدميه، ولماذا يجمعها؟
٢. كيف يستخدم الموقع هذه المعلومات.
٣. الخيارات التي يقدمها الموقع لمستخدميه عن استخدامه لمعلوماتهم وبياناتهم الشخصية، بما في ذلك تحديث هذه المعلومات والبيانات.

وقد تقتصر سياسة الخصوصية لدى بعض المواقع أو التطبيقات على شرح عام وقد تمتد لشرح مفصل عن الأنشطة التي تستخدم فيها معلوماتهم وبياناتهم المتاحة على الانترنت وما قد تفعله بهذه المعلومات

والبيانات خارج مستوى الموقع نفسه مثل تصديرها لمواقع ذات صلة أو أحقيتها في استخدام هذه المعلومات والبيانات في حالة ما تم إيقاف الموقع أو تعطيله أو تغيير نشاطه.

وإذا كانت كل المواقع والتطبيقات مجبرة على أخذ موافقة مستخدميها على ما تجمعه من معلومات عنهم وما تستخدمه من بياناتهم الشخصية قبل استخدامها فإن هذه المواقع والتطبيقات تجبر المستخدمين على عدم الولوج إليها إلا بعد الموافقة على سياسة الخصوصية الخاصة بها أولا وهو ما يفعله معظم المستخدمين دون قراءة وثيقة سياسة الخصوصية تلك ولا التدقيق بها ويقومون بالموافقة بشكل روتيني بدون الاكتراث لخطورة هذا الأمر على خصوصيتهم المعلوماتية بل وعلى حياتهم الخاصة نفسها.

٥/أنواع الخصوصية:

يمكن تقسيم الخصوصية إلى عدد من المفاهيم المنفصلة لكنها ترتبط معا في الوقت ذاته وهي:

١. **خصوصية المعلومات Information Privacy :**

وهي القواعد التي تحكم إدارة البيانات والمعلومات الخاصة كمعلومات بطاقات الهوية، والمعلومات المالية، والسجلات الطبية،

والسجلات الحكومية، وهي المجال الذي يتصل عادة بمفهوم حماية البيانات Data Protection .

٢. **الخصوصية الجسدية أو المادية Bodily Privacy :**

والتي تتعلق بالحماية الجسدية للأفراد ضد أية إجراءات ماسة بالنواحي المادية لأجسادهم كفحوص الجينات GENETIC TESTS ، وفحص المخدرات DRUG TESTING .

٣. **خصوصية الاتصالات** Telecommunication Privacy:

والتي تغطي سرية وخصوصية المكالمات الهاتفية، وبرمجيات الاتصال الصوتي والمرئي، والمراسلات البريدية الورقية، والبريد الالكتروني وغيرها من الاتصالات.

٤. **الخصوصية الاقليمية (نسبة إلى الاقليم المكاني):**

والتي تتعلق بالقواعد المنظمة للدخول إلى المنازل وبيئة العمل أو الأماكن العامة والتي تتضمن التفتيش والرقابة الالكترونية والتوثق من بطاقات الهوية.

٦/الجريمة المعلوماتية:

يعرف البعض الجريمة المعلوماتية بأنها "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي" في حين يعرفها آخرون بأنها

"الاعتداءات التي ترتكب باستخدام المعلومات بغرض تحقيق ربح" وتعرف كذلك بأنها "مجموعة الجرائم المتصلة بعلم المعالجة المنطقية للمعلومات" .

والجريمة المعلوماتية لصيقة الصلة بانتهاك الخصوصية على الإنترنت وعبر وسائل الاتصال الحديثة حيث أن كل جريمة معلوماتية هي بالضرورة تعدي على خصوصية فرد أو هيئة. وعلى الرغم من أن الجريمة المعلوماتية الالكترونية ظاهرة حديثة نسبيا إلا أنها احتلت مركز الاهتمام الدولي لأن العالم ببساطة يحيا عصر المعلومات.

وتتنوع أشكال الجرائم المعلوماتية باختلاف وسائلها ودوافعها؛ فمنها جرائم تحدث ضد أجهزة الكمبيوتر ونظم المعلومات ووسائل الاتصال ومنها جرائم الإضرار بالبيانات والمعلومات الخاصة أو العامة، وجرائم الاعتداء على الأشخاص سواء بالسب أو التشهير أو الابتزاز، وجرائم نشر الفيروسات والبرامج الضارة، وجرائم الاعتداء على الأموال.

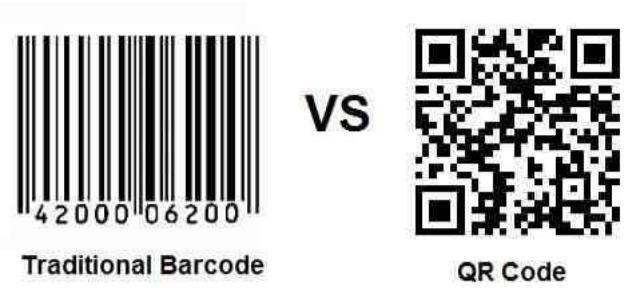
ومن ناحية الدوافع فيعتبر تحقيق ربح مالي دافعا أساسيا وراء ارتكاب الجرائم الالكترونية، بالإضافة لدوافع أخرى مثل الرضا أو المتعة عند بعض المتسللين نتيجة حصولهم على معلومات خاصة، أو الشعور بالانتصار عن طريق اختراق أنظمة معلوماتية محظورة أو

مؤمنة، ويضاف لكل ما سبق الدوافع السياسية والأمنية التي تحرك أجهزة رسمية لارتكاب مثل هذه الجرائم.

٧/مخاطر التقنيات الحديثة على الخصوصية:

١) مخاطر كود الاستجابة السريع: QR– Code

يمثل كود أو رمز الاستجابة السريع(Quick QR Code) Response code أحد أهم أنواع رموز تخزين المعلومات القابلة للاسترجاع حالياً، وهو واحد من أكثر أنواع رموز الباركود تطوراً وانتشاراً وحداثة **(شكل رقم ١)**



شكل ١ كود الاستجابة السريع مقارنة بالشكل التقليدي للباركود

ويتميز هذا الشكل من أشكال الرموز المشفرة أو رموز الباركود بأنه لا يحتاج لأجهزة أو معدات خاصة لقراءته والتعامل معه كما هو الحال في الشكل التقليدي للباركود (الشكل الشريطي) المعروف والمتداول الذي يحتاج إلى قارئ باركود خاص، حيث يمكن قراءة رمز

الاستجابة السريع بواسطة الحاسب الآلي عن طريق إدخال صورة الرمز لأي موقع ويب من المواقع المتخصصة في قراءة رموز الاستجابة فتتم قراءته وإظهار النتيجة فوراً عبر الانترنت، كما يمكن مسح هذا الكود ضوئيا باستخدام كاميرا الهاتف الذكي ومعالجته بأحد تطبيقات قراءة الباركود أو التقاط صورة له بالهاتف المحمول وادخال الصورة لأي موقع ويب أو أي تطبيق عبر الموبايل انترنت فتتم قراءتها وإظهار المعلومات المخزنة على الرمز مباشرة من خلال الهاتف مع إتاحة رابط لكل كود استجابة يُمَكَن من إظهار معلومات عنه بعد ذلك .

وقد تم تصميم رمز الاستجابة السريع في الأساس كتطوير للرمز الشريطي التقليدي (باركود) والذي لم يكن يسمح بتخزين أكثر من ٢٠ حرف فقط فقام فريق من قسم Denso Wave التابع لشركة دينسو اليابانية عام ١٩٩٤ بتطوير رمز ثنائي الأبعاد جديد هو كود الاستجابة السريع ليتم استخدامه في مصانع السيارات في تعقب قطع غيار المركبات أثناء عملية التصنيع مما جعل عمليات التصنيع أكثر كفاءة وفعالة ودقة، وهذا الأمر دفع بقية المصانع والشركات لاستخدام كود الاستجابة السريع ثم انتشر بعد ذلك على جميع المنتجات الغذائية والدوائية وغيرها.

ويتميز كود الاستجابة السريع بسهولة القراءة بشكل سريع ونسبة التخزين العالية حيث يحتوي معلومات مشفرة من أي نوع من البيانات (على سبيل المثال الأرقام، والحروف والأرقام، والبيانات الثنائية المتكونة من أرقام وحروف)، كما يتميز بفك محتوياته بسرعة عالية جداً إذ أنه يحمل بداخله بيانات مشفرة للمنتج أو السلعة التي يرفق حيث يمكن لأي شخص الاطلاع على بيانات الرمز فقط من خلال تصويره وادخاله إلى موقع أو برنامج لفك شفرة هذا الكود أو الرمز أو مسحه مباشرة من خلال أحد تطبيقات قراءة كود الاستجابة السريع المتوافرة حاليا على المتاجر الالكترونية للهواتف المحمولة حيث من الممكن أن تحمل الشفرة الموجودة داخل المربع بيانات عديدة مثل: رابط لموقع ما على الانترنت يحتوي أي نوع من البيانات مثل الفيديو أو الصوت أو النصوص المختلفة ... الخ، أو رقم هاتف، أو حتى بيانات شخصية مثل الاسم والبريد الالكتروني وحتى موقع الشركة وبيانات حول الشركة، أو تضمينه رسالة نصية تصل لأكثر من ١٦٠ حرف.

ويمكن الاستفادة من تكنولوجيا رمز الاستجابة السريع في مجال إدارة الوثائق لقدرته على تخزين المعلومات والبيانات وتخزين صور الوثائق بداخله. ولكن ظهرت بعض المخاطر التي نتجت عن إدارة الوثائق من خلال تكنولوجيا رمز الاستجابة السريعة، ومن هذه المخاطر

ظهور بعض رموز الاستجابة الضارة التي تحمل برمجيات خبيثة (فيروسات) والتي يمكن تصميمها بسهولة وتجعل محتويات كمبيوتر أو هاتف المستخدم في خطر بسبب انتهاكها لخصوصيته واستيلائها على معلوماته أو بياناته الخاصة مثل كلمات المرور وأسماء المستخدم التي يستخدمها للولوج للمواقع الالكترونية أو للبريد الالكتروني الخاص به أو خداعه والاستيلاء على معلوماته المالية عن طريق الاحتيال عليه باستخدام رموز استجابة سريعة تبدو شرعية لكنها محملة ببرمجيات ضارة ترسل معلومات المستخدم لمواقع المجرمين الالكترونيين. ويمكن إضافة البرمجيات الضارة والخبيثة إلى رموز الاستجابة السريعة الشرعية كجزء من محتوياتها ثم بثها عبر الانترنت أو في إعلانات ترويجية لاصطياد ضحايا يتم الاستيلاء على بياناتهم الخاصة واستعمالها في أنشطة غير مشروعة.

٢) **مخاطر التوسيم: Tagging**

والوسم بالإنجليزية: Tag هو كلمة مفتاحية أو عبارة تصنف بها معلومة معينة (صورة، خريطة، تدوينه، مقطع فيديو، إلى آخره) هذه الوسوم يتم إدراجها بغرض وصف المادة أو المعلومة ولتسهيل البحث والتصنيف. والتوسيم هو إحدى الآليات التكنولوجية البديلة للتكشيف

على شبكة الانترنت أو يمكن القول أن التوسيم هو أحد الأشكال غير التقليدية لتكشيف المعلومات والكلمات.

ويمكن تعريف التوسيم بأنه ربط المحتوى على موقع أو صفحة ويب بكلمات دلالية مميزة تدل على محتوى موضوعي أو أسماء مستخدمين محددين. أو هو وضع وصف بالكلمات لموقع معين أو محتوى معين على شبكة الانترنت.

وكان ظهور المواقع المتخصصة التي توفر خدمة التوسيم في عام ٢٠٠٣ عندما انطلقت بعض المواقع التي تقدم خدمة تخزين عناوين مواقع الإنترنت مع إضافة وسوم لوصف محتوى الموقع المخزن مما يجعلها متاحة لأي فرد من أي مكان وباستخدام أي جهاز.

وتقوم خدمة التوسيم على مشاركة مجتمع المستفيدين في المصادر المفضلة لدى كل منهم. وكان في مقدمة هذه المواقع موقع خدمة المفضلة الاجتماعية del.icio.us الذي ظهر في عام ٢٠٠٣ وهو أول موقع يقدم تطبيقات وصف المحتوى، ومن خلاله يمكن للمشتركين في الموقع حفظ أي موقع أو صفحة على الإنترنت ووضع الكلمات المفتاحية التي تصف الموقع، وبحفظ هذا الموقع في Delicious يصبِح لدى كل عضو في هذه الخدمات قائمة من الروابط لمواقع ولمحتويات مفضلة لديه، محفوظة ومفهرسة عن طريق

عملية التوسيم Tagging ويمكن للعضو أن يجعل قائمته مُشاعة بين كل الأعضاء المسجلين في نفس الخدمة، ويحق له أيضاً قصرها على نفسه فقط، دون أن يطلع عليها أحد. ثم استمرت هذه الخدمة في الانتشار بعد ذلك وظهرت مواقع كثيرة توفر نفس الخدمة وتتوسع فيها وظهرت نسخة نظام التشغيل ويندوز فيستا Vista لتكون أول نسخة ويندوز تعتمد نظام التوسيم لتخزين المواقع التي يزورها المستخدمون للرجوع لها أو لمحتوياتها بعد ذلك، ثم انتشرت الخدمة في الإصدارات التالية من الويندوز كما انتشرت بين متصفحات الانترنت المختلفة.

وتكمن أهمية التوسيم في إدارة الوثائق On Line في إنه يمثل طريقة للتكشيف المباشر بالكلمات الدلالية على المحتوى الالكتروني فيمكن من خلال البحث بالكلمات المستخدمة في التوسيم إظهار كل الكلمات المطابقة أو ذات الصلة على نطاق معين. وبتطبيق ذلك على إدارة الوثائق فيمكن من خلال توسيم الصور التي تعتبر وثائق أو توسيم صور الوثائق نفسها على شبكة الانترنت بكلمات مفتاحية معينة ليتم استرجاع هذه الصور أو استرجاع محتوى الوثائق مرة أخرى بالاستعانة بتلك الكلمات المفتاحية المستخدمة في توسيم هذه الوثائق. ويعتبر موقع فليكر flicker من أشهر المواقع التي تقدم خدمة التوسيم على الصور لاستخدامها في البحث عن الصور بعد ذلك.

وتتمثل الخطورة في استعمال التوسيم كأداة لتكشيف الوثائق بالكلمات الدلالية في أن التوسيم عبر الويب يجعل الوثائق/الصور نفسها متاحة بشكل واسع على شبكة الانترنت وحتى مع وجود احتياطات الأمن والخصوصية في بعض المواقع فإنه بإمكان قراصنة الويب الولوج للمواقع المختصة في تقديم هذه الخدمة واختراقها والاستيلاء على خزائن الصور بها وانتهاك خصوصية أصحاب الصور/ الوثائق.

كما ينطوي التوسيم على خطورة أخرى على خصوصية الأفراد والهيئات وتظهر بشكل أكبر في مواقع التواصل الاجتماعي ألا وهي التوسيم من الغير لموقع أو حساب شخص أو جهة على صورة ونشرها على مواقع التواصل الاجتماعي (خصوصا الفيس بوك وتويتر) مما يتيح نشر هذه الصور لدي جميع أصدقاء ومتابعي هذا الشخص أو الجهة وكأنه موافق عليها أو مشتركاً فيها مما يعد انتهاك واضح لخصوصيته ونشر أشياء مصحوبه باسمه قد لا يكون موافقا عليها أو متوافقا معها.

كما أن من مخاطر التوسيم في مواقع التواصل الاجتماعي استخدام القراصنة لبعض الحيل للاستيلاء على البيانات الشخصية وقوائم الأصدقاء لبعض مستخدمي مواقع التواصل الاجتماعي من

خلال وسمهم أو وسم أصدقاء لهم في لينكات وهمية لفيروسات أو برمجيات ضارة تحمل عناوين مشوقة وجذابة حسب رغبة المستخدم مثل أخبار فضائح المشهورين وبثها في لينكات موسومة بأسماء حساباتهم على مواقع التواصل الاجتماعي وما إن يضغط أي شخص على الرابط (اللينك) حتى يتم اختراق حسابه وسرقة بياناته الخاصة مثل بريده الالكتروني وكلمة مرور حسابه على موقع التواصل وقائمة الأصدقاء، وقد تكون بعض الفيروسات أكثر خطورة من ذلك إذ تقوم بعضها بإعادة إرسال نفسها تلقائياً بعد عمل وسم أو إشارة Tag بنفس اللينكات الوهمية لجميع قوائم أصدقاء الضحايا مما يدخل عدد كبير من مستخدمي مواقع التواصل الاجتماعي في هذه الحلقة من انتهاك الخصوصية أو الاستيلاء على البيانات الشخصية.

ونظراً لسرعة التواصل عبر مواقع التواصل الاجتماعي وإقبال الجميع عليها فقد قامت معظم الهيئات والكيانات الاعتبارية بإنشاء حسابات خاصة بها على هذه المواقع، وبالطبع فإن مؤسسات حفظ الوثائق وإدارتها من ضمن هذه الكيانات التي تتعرض لخطورة الهجوم عليها من خلال فيروسات التوسيم على مواقع التواصل الاجتماعي وتهديد مستودعاتها الرقمية اذا كانت مرتبطة بالموقع أو تهديد مواقع ادارتها للوثائق عبر الانترنت.

٣) مخاطر إدارة الوثائق من خلال المستودعات الرقمية و/أو نظم إدارة البريد الالكتروني:

تمثل المستودعات الرقمية digital dipositories إحدى أهم الوسائل التكنولوجية الحديثة لإدارة الوثائق. وتنقسم إدارة الوثائق في البيئة الرقمية إلى عدة أقسام وأنواع حسب الأساس المستخدم في تقسيم إدارة الوثائق. فإذا ما اعتمد التقسيم على شكل أو طبيعة الوثائق نفسها فهناك إدارة الوثائق الورقية باستخدام أدوات ووسائل الكترونية، وإدارة الوثائق الرقمية ذات الأصل الورقي أو المحولة رقميا Digitalized، وإدارة الوثائق المنشأة في بيئة رقمية Non Paper material. ومن حيث طريقة الإدارة نفسها هناك إدارة الوثائق بالاعتماد على برامج أرشفة الكترونية في غير بيئة الويب، وإدارة الوثائق من خلال بيئة الويب سواء من خلال برامج أرشفة متصلة بالويب أو من خلال مواقع الويب مباشرة.

ولإنشاء مستودعات رقمية يجب الاعتماد على برامج إدارة الكترونية/ رقمية للوثائق أو ما يعرف ببرامج الأرشفة الالكترونية. وهذه البرامج تضم نوعين رئيسين؛ نوع تتم من خلاله إدارة الوثائق في معزل عن بيئة الويب ونوع آخر تتم من خلاله إدارة الوثائق بالاعتماد أو بالاستعانة بالإنترنت أو الويب.

وتعتبر برامج الأرشفة الالكترونية غير المعتمدة على بيئة الويب أكثر أمناً على خصوصية الأفراد والمؤسسات من تلك البرامج المعتمدة على الويب. ويرجع ذلك لأن البرامج التي لا تعتمد على الويب تعمل غالباً من خلال شبكات حاسب محلية Local Networks متصلة بجهاز خادم Server يعمل على إدارة البرنامج من خلال أسماء مستخدمين وكلمات مرور تحدد من لهم حق الولوج إلى النظام أو البرنامج ومن ثَم إلى مستودعات الحفظ الرقمي.

كما تعمل هذه البرامج عادة على تقسيم أدوار المستخدمين User's Rules وتحديد الصلاحيات بينهم سواء بشكل أفقي أو هرمي، وكل هذا يحدث في معزل عن بيئة الانترنت وتنحصر الخطورة في مثل هذه البرامج في عمليات اختراق النظام الكامل الذي يسمح باختراق برنامج الأرشفة الالكتروني والحصول على اسم/ أسماء المستخدمين، وكلمة/كلمات المرور وهو ما يؤدي إلى اختراق مستودعات الحفظ الرقمي بالسيرفر (الخادم) والحصول على أي بيانات خاصة بالأفراد داخل الهيئة أو الكيان الذي يخدمه البرنامج وبيانات الهيئات أو الكيانات ذات الصلة، وهي بلا شك خطورة كبيرة ولكنها تحتاج مجهود كبير من المخترقين سواء بالتسلل من الخارج أو التسريب من الداخل لأسماء المستخدمين وكلمات المرور.

وتمثل البرامج المتصلة بالإنترنت أو التي تعمل في بيئة الويب خطورة أكبر على خصوصية بيانات/ معلومات الأفراد والهيئات وذلك لأنها عرضة أكبر للاختراق مباشرة من خلال الانترنت أو بيئة الويب التي تحتوي على العديد من أساليب الاختراق أو السرقة أو انتهاك الخصوصية، ولأن تقييم مواقع الأرشيف على الانترنت يوضح أنها ذات مخاطر حقيقة وعالية لذا فهي تحتاج برامج ذات موثوقية عالية توفر الحفظ المستدام الآمن للوثائق والملفات بصيغها المختلفة، فقد يتم اختراق البرنامج من خلال الحصول على اسم المستخدم وكلمة المرور عبر برامج خاصة لسرقتهم، وهذه البرامج منتشرة على الانترنت، أو من خلال اختراق مواقع الشركات المنتجة لبرامج إدارة الوثائق والتي تكون أحياناً متصلة بها من خلال الانترنت لتحديث هذه البرامج وتقديم خدمات التحديث والصيانة عبر الخط المباشر On Line وهو ما يجعل كل البرامج المنتجة من هذه الشركات عرضة للاختراق وسرقة المعلومات و/أو البيانات الشخصية والسرية الخاصة بعملاء هذه الشركات سواء أكانوا شركات أو أفراد.

كما تتعرض نظم إدارة البريد الالكتروني للكثير من الأخطار التي تهدد خصوصية الأفراد والهيئات، ويعد الاختراق المباشر لحسابات البريد الالكتروني من أكبر المخاطر التي قد تمكن القراصنة من

الاختراق الكامل لمستودعات حفظ الوثائق المرتبطة بنظم الحفظ المعتمدة على البريد الالكتروني.

ومن أشهر حالات الاختراق التي حدثت في هذا الصدد التسريبات المعروفة باسم ويكيليكس WikiLeaks حيث تمكن مؤسسها الاسترالي "*جون أسانج*" من اختراق أنظمة وحسابات بريد الكتروني للعديد من الهيئات الدولية مثل وزارة الدفاع الأمريكية (البنتاجون) نفسها والولوج لمستودعاتها الرقمية وتسريب ملايين النسخ من الوثائق الأصلية أو صور الوثائق ونشرها على موقع ويكيلكس الذي يُحاكم *أسانج* حتى الآن بسبب تأسيسه له ومازال مطلوباً في دول عدة ويلوذ باللجوء السياسي للحماية من مصير السجن مدى الحياة عقابا على هذه التسريبات. وغير ذلك من أمثلة اختراق مستودعات حفظ الوثائق الخاصة والعامة التي لا يتوقع أن تنتهي أو يتم القضاء عليها قريبا أو بشكل نهائي.

٤) <u>مخاطر إدارة الوثائق في نظم الحياة الثانية: Second Life</u>

الحياة الثانية أو **Second Life** هي لعبة قامت بتصميمها شركة ليندن لاب Linden Lab ومقرها سان فرانسيسكو عام ٢٠٠٣ . وهذه اللعبة تقوم على تكوين عالم افتراضي متكامل من شخصيات وهيئات ومباني وأراضي وجامعات ومؤسسات صحفية وإعلامية .....الخ. وقد انتشرت الفكرة حتى خرجت من إطار اللعبة وانضمت إليها كيانات

حقيقة أنشأت لها كيانات افتراضية في عالم الحياة الثانية، وقد كان من بين هذه الكيانات وكالة رويترز، وبي بي سي، والكثير من الشركات الكبرى، وبعض الأندية الرياضية الشهيرة؛ حتى أن دولة السويد افتتحت سفارة افتراضية بالحياة الثانية. وقد أنشئت جامعات دولية كبرى فروع لها في عالم الحياة الثانية ومنها جامعات عربية مثل جامعة الملك عبدالعزيز، كما قامت جامعة ستانفورد بإنشاء مقر افتراضي لها في الحياة الثانية، وأنشأت كذلك أرشيف خاص بها هناك.

ومع تحول الحياة الثانية من مجرد لعبة إلى عالم وواقع افتراضي متكامل بدأ الاتجاه نحو إدارة الوثائق والأرشيف من خلال هذا الواقع الافتراضي الذي أصبح يتطور يوماً بعد يوم ويوفر إمكانيات كبيرة لإدارة الوثائق من خلاله. ولكن تبقى المخاطر قائمة لإدارة الوثائق في الحياة الثانية مثلها تماماً مثل تلك المخاطر التي تهدد إدارة الوثائق والأرشيف في المستودعات الرقمية المتصلة بالإنترنت حيث أن الحياة الثانية تمثل نوع من هذه المستودعات التي تعمل على إدارة الوثائق مباشرة من خلال بيئة الويب، وما قيل عن مخاطر تتهدد المستودعات الرقمية للوثائق ينطبق تماماً على إدارة الوثائق من خلال الحياة الثانية أو العالم الافتراضي حيث أنه عرضه للقرصنة والاختراق بشكل كامل.

٥) <u>المخاطر المبنية على إنشاء الوثائق في البيئة الرقمية:</u>

يعتبر إنشاء الوثائق في البيئة الرقمية إحدى تجليات عصر الانترنت والحكومة الالكترونية الذي أصبح منتشراً في العالم الآن. ويقصد بالوثائق المنشأة في البيئة الرقمية Born-digital archival material تلك الوثائق التي ليس لها أصل ورقي وإنما أنشئت واستعملت مباشرة عبر الحاسب الآلي وشبكة الانترنت، ومن أمثلة هذا النوع من الوثائق و/أو المواد الأرشيفية؛ المراسلات البريدية عبر البريد الالكتروني ومواقع الهيئات والكيانات ذات الصفة القانونية، والرسائل النصية الهاتفية....وغيرها.

وقد خصصت بعض الهيئات والجهات المتخصصة والبحثية برامج لدراسة الأخطار التي تهدد هذا النوع من الوثائق والمواد الأرشيفية واقتراح الخطط والبرامج لحمايتها من هذا الأخطار. وقد عمدت جامعة ستانفورد لإطلاق مشروع أطلق عليه برنامج الوثائق المولودة رقمياً The Born-Digital Program يتبع مكتبة جامعة استانفورد SUL حيث يهدف لحماية الوثائق المنشأة في البيئة الرقمية والعمل على الولوج إليها بشكل دائم وآمن ويمكن حصر الأخطار التي تواجه الوثائق المنشأة رقمياً في الآتي:

١. التقادم الذي يصيب البرامج التي توفر إمكانية قراءة هذه الوثائق أو المواد الأرشيفية والولوج إليها.

٢. إمكانية تدمير هذه الوثائق أو المستودعات الرقمية المتضمنة لها ومحوها من الوجود بشكل كامل، في حالة عدم وجود نظير مادي لها.
٣. الولوج غير المصرح لهذه الوثائق من قبل القراصنة.
٤. التلاعب في شكل وطبيعة هذه الوثائق من خلال البرامج الحديثة مما يغير من بياناتها أو يشكك في صحتها.
٥. عدم اكتسابها الحجية القانونية الكاملة في بعض الدول نتيجة تخلف البنية التشريعية عن البنية التكنولوجية.

٦) المخاطر المبنية على استعمال البطاقات الائتمانية/ الفيزا كارت ATM

تعتبر البطاقات الائتمانية/ الفيزا كارت أحدث شكل من أشكال التعامل المالي وأكثرها انتشاراً في العالم الآن فهي تحل محل النقود الورقية ويمكن الشراء والدفع عن طريقها في الأسواق والمحلات وعبر الانترنت. وبطاقات الائتمان هي نوع من أنواع الوثائق المالية المعترف بها عالمياً وتحمل بيانات مهمة لحاملها وعن حاملها.

وهناك العديد من المخاطر التي تواجه استعمال بطاقات الائتمان بسبب طمع اللصوص في الاستيلاء على بياناتها الخاصة مما يعني

الاستيلاء عملياً عليها واستعمالها في دفع ثمن سلع يتم شرائها عبر الانترنت، أو في تحويل مبالغ من حساب صاحبها لحساباتهم الخاصة.

وهناك أساليب متعددة للحصول على بيانات البطاقات الائتمانية بشكل غير مشروع، يمكن تلخيصها في الآتي:

- **أسلوب الخداع:** وتستخدم في هذا الأسلوب أشكال مختلفة من الخدع التي تستخدم للحصول على البيانات الخاصة ببطاقة الائتمان. ويعد أشهر هذه الأشكال إنشاء مواقع الكترونية وهمية للشركات والمؤسسات التجارية الكبرى عن طريق سرقة بيانات مواقع هذه الشركات من على الانترنت، ومن ثم اصطياد زبائن هذه الشركات وسرقة بيانات بطاقاتهم الائتمانية.
- **تخليق أرقام البطاقات:** ويسمى هذا الأسلوب Card cash وتستخدم فيه برامج متطورة تستعمل معادلات رياضية معقدة لتخليق أرقام بطاقات ائتمانية تبع بنك معين وسرقة حسابات هذه البطاقات.
- **الاختراق غير المشروع Illegal access لمنظومة خطوط الاتصالات العالمية:** وفي هذا الأسلوب يقوم القراصنة باختراق الحسابات الحقيقية الخاصة بالمتاجر والشركات على شبكة الانترنت وسرقة بيانات البطاقات الائتمانية لزبائن هذه المتاجر والشركات.

- **أسلوب تفجير الموقع المستهدف:** ويستهدف مستخدمو هذا الأسلوب في السرقة الحواسب المركزية للبنوك والمؤسسات المالية وذلك من خلال بث آلاف أو عشرات الآلاف من الرسائل الالكترونية للموقع المستهدف في نفس الوقت مما يشكل حملاً ثقيلاً على الموقع ومع تزايد الضغط قد ينفجر الموقع نتيجة تحميله سعة تخزينية أكبر من قدرته مما يتسبب في انفجار الموقع وتشتت المعلومات به، فيستطيع المخترقون الحصول على خزائن بيانات البطاقات الائتمانية بالموقع.
- **السرقة المباشرة لبيانات بطاقات الائتمان:** يعمد بعض اللصوص في المتاجر والمطاعم، وغيرها إلى استخدام ماكينات دفع اليكتروني تحتفظ ببيانات البطاقة الائتمانية والرقم السري الذي أدخله العميل ومن خلال هذه البيانات يتم استخدام البطاقة للدفع أو تحويل الأموال عبر الانترنت، أو يقومون بتخليق بطاقات مادية واستخدامها في صرف الأموال من حساب العميل.

٨/وسائل مكافحة السطو الرقمي على البيانات الشخصية:

يهيمن حاليًا اتجاهين رئيسين على النقاش حول كيفية حماية الخصوصية الشخصية على الإنترنت، المعسكر الأول يدعو إلى حماية

الخصوصية على شبكة الإنترنت عن طريق التدخل الحكومي باللوائح والقوانين ووضع تشريع يضع حدودًا صارمة على كيفية قيام الشركات بجمع البيانات عبر الإنترنت، وأنواع المعلومات الشخصية التي يمكنها جمعها، وكيفية استخدامها، ويؤكد أنصار هذا النهج على أن التنظيم الحكومي القوي ضروري لحماية مستخدمي الإنترنت غير المتشككين من سلوك الشركات على الإنترنت.

بينما ويقاوم أصحاب المعسكر الآخر تدخل الحكومة في اقتصاد الإنترنت الهش وسريع الحركة، ويرون أن التنظيم الذاتي للسوق والصناعة سيحقق نتائج أفضل من القواعد واللوائح الحكومية، ويؤكد أصحاب هذا الرأي أن شركات الإنترنت لديها بالفعل حافز في السوق لحماية خصوصية المستخدم لتجنب فقدان الزبائن، وبالتالي فإن التدخل الحكومي في هذه الحالة غير ضروري ويمكن أن يؤدي إلى نتائج عكسية.

تنقسم وسائل مكافحة السطو على البيانات الشخصية إلى عدة أقسام أو محاور قد تعمل منفردة كل على حدة أو تعمل معاً في تناغم وتكامل. وهذه المحاور أو الأقسام هي:

١. **الاحتياطات الشخصية للفرد أو المؤسسة للمحافظة على سرية البيانات الشخصية:**

استخدام اسم/أسماء مستخدمين، و كلمات مرور قوية يصعب التنبه بها ولا يمكن الوصول لها أو توقعها بسهولة، على أن يتم تغييرها كل فترة. كما تعمد بعض الجهات لتغيير كلمات المرور بشكل دائم وهو أمر مستحب يساعد في حماية النظام من التسلل. كما تستخدم بعض الهيئات أسلوب أدوار المستخدمين لتحديد صلاحيات كل فرد داخل الهيئة في الولوج للنظام بها.

٢. الإجراءات المتخذة لعدم الوقوع كفريسة للبرمجيات الخبيثة:

تتجه الهيئات الاعتبارية والأشخاص ذوي الأهمية لاستخدام برامج مكافحة الفيروسات، والجدران النارية، واستخدام برامج الكترونية أصلية وحديثة. ورغم التكلفة المالية التي تمثلها مثل هذه الاحتياطات لكنها توفر على مستخدميها الكثير في حماية خصوصيتهم، وبياناتهم الشخصية. كما تعمل البرمجيات الأصلية على منع تسلل الفيروسات والبرمجيات الضارة إلى النظام.

٣. الإجراءات الوقائية لمنع تسلل القراصنة إلى البيانات الشخصية.

لعدم تسلل القراصنة إلى البيانات الشخصية للأفراد والهيئات والكيانات الاعتبارية يعمد البعض لاتخاذ بعض الإجراءات الوقائية منها عدم الدخول على مواقع الكترونية غير موثوقة وعدم قبول أي دعوات

الكترونية غير معلومة المصدر ومؤمنة بشكل كامل. وكذلك عدم الدخول على مواقع الدعاية أو الألعاب، وعدم فتح رسائل البريد الالكتروني العشوائية/المؤذية Spam خصوصاً إذا كانت تحمل مرفقات Attachments، أو روابط لمواقع الكترونية.

قائمة المصادر والمراجع:

أولا: المصادر العربية:

١. الاتحاد الدولي للاتصالات (٢٠١٣). حماية البيانات والخصوصية في الحوسبة السحابية؛ جزء من تقرير "اتجاهات الإصلاح في الاتصالات لعام ٢٠١٣._ موقع مجلة الاتحاد الدولي للاتصالات.

٢. الأمم المتحدة – مجلس حقوق الإنسان (٢٠١٤). (الحق في الخصوصية الرقمية) تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان.

٣. أمنية عامر. التاريخ الشفهي (يونيو٢٠٠٥): تاريخ يغفله التاريخ._ cybrarian journal._ ع٥.

٤. أمينة حمشاشي (٢٠٠٩). ماهية الجريمة المعلوماتية._ دراسات وابحاث، مج١، ع١، ص ص ٤٥٠_٤٥٨.

٥. حسنين، رجب عبد الحميد. أمن شبكات المعلومات الإلكترونية: المخاطر والحلول Cybrarians Journal– ع ٣٠ (ديسمبر ٢٠١٢)

٦. رجب عبد الحميد حسنين (سبتمبر٢٠١٢). أمن شبكات المعلومات الالكترونية: المخاطر والحلول._ Cybrarians Journal._ ع٣٠.

٧. خالد بن سليمان الغثبر، أمل ناصر الصبيح (مايو ٢٠١٢). حال أمن المعلومات في المملكة العربية السعودية._ دراسات المعلومات، ع١٤.
٨. سوزان عدنان الأستاذ (٢٠١٣). انتهاك حرمة الحياة الخاصة عبر الانترنت: دراسة مقارنة._ مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مج٢٩، ع٣._ ص ص ٤٢١-٤٥٥.
٩. سليمان أحمد فضل. الجرائم المتعلقة باستخدام بطاقات الائتمان عبر شبكة الانترنت._ مركز الإعلام الأمني.
١٠. عايض المري. الخصوصية وحماية البيانات. متاح في: https://goo.gl/NjGqc6
١١. عبد الجبار الحنيص (٢٠١٠). الاستخدام غير المشروع لبطاقات الائتمان الممغنطة من وجهة نظر القانون الجزائي._ مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مج٢٦، ع١.
١٢. عزيزة عبدالرحمن العتيبي (٢٠١٠). أثر استخدام تكنولوجيا المعلومات على أداء الموارد البشرية: دراسة ميدانية على الأكاديمية الدولية الاسترالية._ الأكاديمية العربية البريطانية للتعليم العالي.
١٣. المجلس الدولي للأرشيف (٢٠١٢). مبادئ إتاحة الوثائق._ ترجمة: أماني محمد عبدالعزيز.
١٤. مجمع اللغة العربية (٢٠٠٤). المعجم الوسيط._ ط٤._ القاهرة: مكتبة الشروق الدولية.

١٥. محمد الطاهر(٢٠١٣). الحريات الرقمية: المفاهيم الأساسية._ ط١._ القاهرة: مؤسسة حرية الفكر والتعبير.
١٦. محمد على سالم، حسون عبيد هجيج (٢٠٠٧). الجريمة المعلوماتية._ مجلة جامعة بابل للعلوم الانسانية._ مج١٥، ع٢.
١٧. محمد محمد الهادي (يونيو ٢٠٠٦(. توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية._ _. Cybrarians journal ع ٩
١٨. منى تركي الموسوي (٢٠١٣). الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها._ منى تركي الموسوي، جان سيريل فضل الله._ جامعة بغداد: مجلة كلية بغداد للعلوم الاقتصادية الجامعة العدد الخاص بمؤتمر الكلية.
١٩. مؤسسة حرية الفكر والتعبير (٢٠١١). حرية تداول المعلومات: دراسة قانونية مقارنة._ ط١._ مؤسسة حرية الفكر والتعبير: القاهرة.
٢٠. ناهد حمدي أحمد. المصادر الشفوية والأرشيف. متاح في: https://goo.gl/DEXRva

ثانيا: المصادر الأجنبية:

1. Ajayi, E. F. G. (August 2016). Challenges to enforcement of cyber-crimes laws and policy.- Academic Journals; Journal of Internet and Information Systems. Vol. 6(1), PP. -12

2. Berman, Jerry & Mulligan, Deirdre (1998). Privacy in the Digital Age: Work in Progress. – Nova law review, vol.23. P549-582. January.
3. Hirsch, Dennis D. (2011). The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?.- Seattle University Law Review.- Vol.3. PP. 439-480.
4. Landesberg, Martha K. & Mazzarella, Laura. (July1999). Self-Regulation and Privacy Online: A Report to Congress.- U.S.A: Federal Trade Commission.
5. Lawrence, Gregory W. et al. (2000). Risk Management of Digital Information: A File Format Investigation.- Washington, D.C.: Council on Library and Information Resources
6. Mendel, Toby et al. (2012). Global survey on internet privacy and freedom of expression. – UNESCO: France. - UNESCO Series on Internet Freedom.
7. Micki, Krause. Handbook of Information Security Management.
8. Rhodes-Ousley, Mark (2013). Information Security: The Complete Reference.- Second Edition.- New york: McGraw-Hill.
9. Richard M., Marsh Jr. (2009). Legislation for Effective Self-Regulation: A New Approach to Protecting Personal Privacy on the Internet, Michigan Telecommunications and Technology Law Review, Volume15, Issue 2. PP. 542-563.

10. Strauss, Jared & Rogerson, Kenneth S. (2002). Policies for online privacy in the United States and the European Union.- Telematics and Informatics, vol. 19. PP. 173–192.
11. Westin, Alan F. (1967). Privacy and freedom. - New York: Atheneum.
12. Westin, Alan F. (2003). Social and Political Dimensions of Privacy.- Journal of Social Issues, Vol. 59, No. 2, pp. 431-453.