2.7. أمن المعلومات: المفهوم، والعناصر[7].

Information Security: Concept, Elements, and Strategy.

1.2.7. أمن النظام Systems Security

يُشير مفهوم أمن النظام إلى حماية مصادر معلومات المنشأة من السّرقة أو الاستخدامات غير الصحيحة مثل: منع تغيير المعلومات، أو إلغاءها أو الاستفادة منها بطريقة غير شرعية، أو نشر معلومات غير صحيحة من قبل أطراف غير مُخوّل لهم باستخدام النظام. مع الأخذ بعين الاعتبار أن إدارة البرمجيات لا بد أن تعمل على الموائمة بين مخاطر البرمجيات وإدارة تلك المخاطر، وهذا يحتاج إلى تعاون كبير ومستوى عال من التكامل الداخلي، ومن الطُرق الملائمة لذلك استخدام معايير الأداء[8].

2.2.7. أمن المعلومات Information Security

هي حماية التجهيزات الحاسوبيّة وغير الحاسوبيّة والتسهيلات والبيانات والمعلومات من الأخطار فهي مجموعة الإجراءات والتدابير الوقائيّة التي تستخدمها المنظمة للمحافظة على المعلومات وسرّيتها سواء من الأخطار الداخلية أو الخارجية، كالحفاظ عليها من السرّقة والتلاعب والاختراق أو الإتلاف غير المشروع، سواء قبل أو خلال أو بعد إدخال المعلومات إلى الحاسب من خلال تدقيق المُدخلات وحفظها في مكان أمين وتسمية الأشخاص المُخولين لهم التعامل مع هذه البيانات[9]

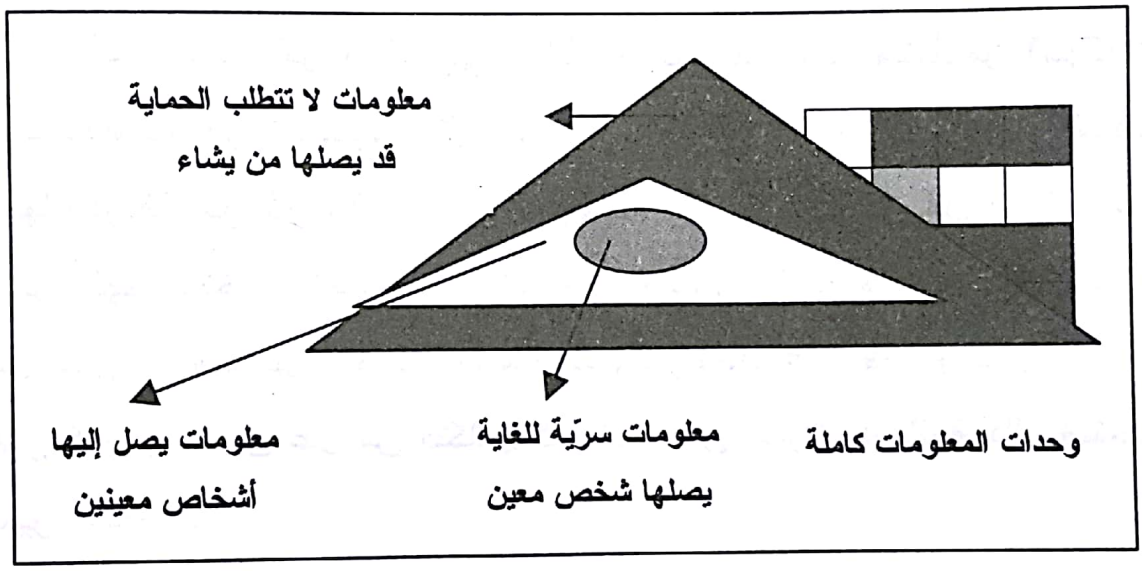
لـــذا فإن أمن النظم والمعلومات يشمل تحقّق الأمن عند إدخال المعلومات، وانتقالها داخل المنظمة، وتخزينها واستخدامها.

ويعتمد ضمان عناصر أمن المعلومات كُلّها أو بعضها على المعلومات محل الحماية واستخداماتها وعلى الخدمات المتصلة بها، فليس كُلّ المعلومات تتطلّب السرّية وضمان عدم الإفشاء، وليس كل المعلومات في منشأة واحدة بذات الأهمية من حيث الوصول لها أو ضمان عدم العبث بها.

ويبيّن الشكل (7/ 2) مدى الحماية المطلوبة لأنواع المعلومات.

الشكل (7/ 2)

مدى الحماية المطلوبة لأنواع المعلومات



Stalling, William (2004). ***Cryptography and Network Security: Principles and Practices*** (3rd ed.).

3.2.7. العناصر الأساسيّة لنظام أمن المعلومات[10].

Major Elements of Information Security System

تُمثّل استراتيجيات ووسائل أمن المعلومات أغراض حماية البيانات الرئيسة وتعمل على ضمان توفر العناصر التالية لأية معلومات يُراد توفير الحماية الكافية لها:

1.3.2.7. الخصوصيّة Privacy

ادّعاء بأن يترك الأفراد لوحدهم بدون مراقبة أو تشويش من قبل أفراد أو منظمات أو حكومـــات أخـــرى. والتأكّد من أن المعلومات التي يستخدمونها سرّية ولا يَطّلع عليها أحد دون إذن أو تخويل، كما تشمل حماية البيانات المُستخدمة من الأقسام.

2.3.2.7. السّلامة Integrity

هي التأكد من أن سلامة مُحتوى المعلومات بحيث لم يتم تعديله أو العبث به، ولن يـــتم تدمير المحتوى أو تغيره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل، سواء في مرحلة التعامل الداخلي مع المعلومات، أو عن طريق تدخل غير مشـــروع. والـــتأكّد مـــن أن المعلومات التي أرسلت هي نفسها التي يتم تلقيها من الطرف الآخر.

3.3.2.7. الإثبات Authentication

القدرة على إثبات شخصيّة الطرف الآخر على الشّبكة، وإثبات شخصيّة الموقع.

4.1.2.7. الوَفرة/ توفر المعلومة Availability

الـــتأكد من توفّر المعلومة واستمرار عمل نظام المعلومات، وتقديم الخدمة لمواقع المعلوماتـــية، وضـــمان اســـتمرار وحماية النظام من أنشطة التعطيل، وعدم منع المُستخدم من استخدام المعلومات أو الدخول إليها.

5.3.2.7. عدم الإنكار Non-Repudiation

ضمان عدم إنكار الشخص الذي قام بتصرّف ما مُتّصل بالمعلومات أو مواقعها بأنه هـــو الذي قام بهذا التصرف، بحيث تتوفّر قُدرة إثبات أن تصرفاً ما قد تَمّ من قبل شخص ما في وقت مُحدّد.

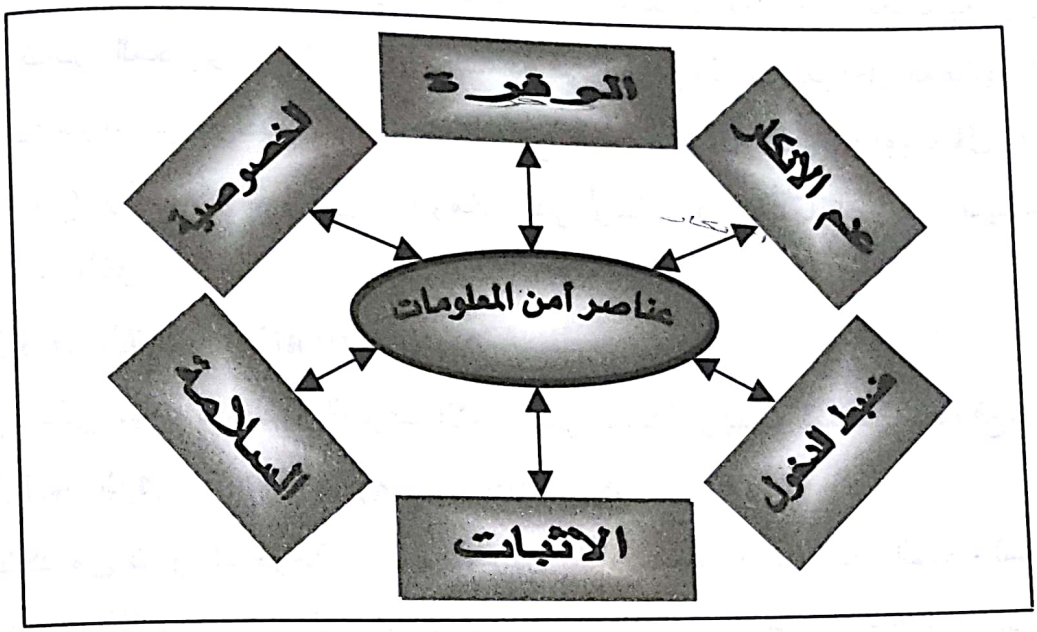
6.3.2.7. ضبط الدخول Access Control

هـــي تحديـــد السياســـات والإجـــراءات والصـــلاحيات، وتحديد مناطق الاستخدام المســـموحة لكـــل مُســـتخدم وأوقاته لمنع دخول من لا يملك حق شرعي إلى نظام المعلومات سواء من الداخل أو الخارج.

ويمثّل الشكل (7/ 3) العناصر الرئيسة لنظام أمن المعلومات.

الشكل (7/ 3)

العناصر الرئيسة لنظام أمن المعلومات



4.2.7. المخاطر الرئيسة في بيئة المعلومات.

Major Risks in Information Environment.

تطال المخاطر والاعتداءات في بيئة المعلومات مواطن أساسيّة هي مُكوّنات تقنية المعلومات وتتمثّل في:

1.4.2.7. الأجهـــزة Hardware هي كافّة المعدّات والأدوات المادّية التي تتكون منها النظم، كالشاشات والطابعات ومُكوّناتها الداخليّة ووسائط التخزين المادّية وغيرها. لذلك لا بد من إعطاء الأهمية الكبيرة لحماية مواقع منظومة الأجهزة الإلكترونية ومُلحقاتها والتي تحوي الأجهزة المختلفة في نظم المعلومات واتخاذ كافة الإجراءات الاحترازية لحماية الموقع، سواء من السرّقة أو الأخطار البيئية المختلفة وإدامة الطاقة الكهربائية وانتظامها، وتحديد الإجراءات المختلفة للتفتيش والتحقّق من هوية الداخلين إلى الموقع[11].

2.4.2.7. البرامـــج Programs تُمثّل البرمجيات المُستخدمة في تشغيل النظام عُنصر أساسي في نجاح النظام، لذلك لا بد من اختيار البرمجيات الحديثة صعبة الاختراق، ووضع علامات السّر المختلفة لإدارة وتشغيل النظام، وتكون إما مُستقلة عن النظام أو مُخزّنة فيه.

3.4.2.7. المُعطيـــات/ البيانات والمعلومات تشمل كافّة البيانات المُدخلة والمعلومات المُستخرجة عقب معالجتها، وتمتد بمعناها الواسع للبرمجيات المُخزّنة داخل النظم. والمُعطيات قد تكون في طور الإدخال أو الإخراج أو التخزين أو التبادل بين النظم عبر الشّبكات.

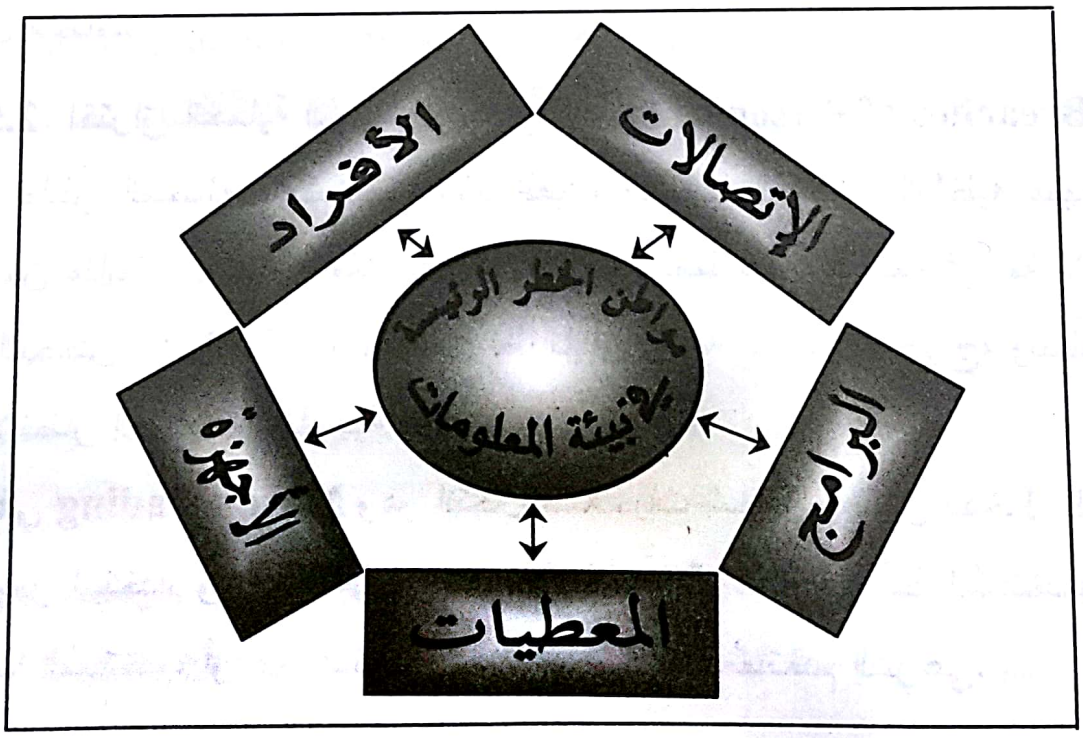
4.4.2.7. الاتصـــالات Communications تشمل شبكات الاتصال التي تربط أجهزة التقنية بعضها ببعض محلياً ودولياً، وتُتيح فرصة اختراق النظم عبرها كما أنها بذاتها محل للاعتداء وموطن من مواطن الخطر الحقيقي. لذلك لا بد أن تتمتّع الشبكة بكفاءة عالية في الكشف عن التسلّل إلى الشبكة.

5.4.2.7. الأفراد People يُمثّل الإنسان محور الخطر، سواء المُستخدم أو الشخص المناط به مهام تقنية مُعينة تتصل بالنظام، فإدراك هذا الشخص حدود صلاحياته، وسلامة الرقابة على أنشطته في حدود احترام حقوقه القانونية، مسائل رئيسة يعنى بها نظام الأمن الشامل، خاصة في بيئة العمل المُرتكزة على نظم الكمبيوتر وقواعد البيانات.

ويُبيّن الشكل (7/ 4) المخاطر الرئيسة في بيئة المعلومات.

الشكل (7/ 4)

المخاطر الرئيسة في بيئة المعلومات



5.2.7. تصنيف المخاطر Risks Classifications

تُصنّف المخاطر والاعتداءات في ضوء مناطق ومحل الحماية إلى الآتي:

1.5.2.7. اختراق الحماية المادّية Breaches of Physical Security

أ. **التّفتيش في المُخلفّات Dumpster Diving** ويقصد به قيام المهاجم بالبحث في مُخلفّات تقنية المؤسسة بحثاً عن أي شيء يُساعده على اختراق النظام، كالأوراق المُدوّن عليها كلمات السّر، أو مخرجات الكمبيوتر التي قد تتضمّن معلومات مفيدة ، أو أي أمر يُستدّل منه على أية معلومة تُساهم في الاختراق.

ب. **الالتقاط السّلكي Wiretapping** ويُمثّل التوصل السّلكي المادّي مع الشّبكة أو توصيلات النظام لجهة استراق السمع أو الاستيلاء على المُعطيات المتبادلة عبر الأسلاك، وهي أنشطة تتم بطرق سهلة أو مُعقّدة تبعاً لنوع الشبكة وطرق التوصل المادّي.

ج. **استراق الأمواج Waves Dropping on Emanations** ويتم باستخدام لواقط تقنية لتجميع الموجات المُنبعثة من النظم باختلاف أنواعها كالتقاط موجات شاشات الكمبيوتر الضوئية أو التقاط الموجات الصوتية من أجهزة الاتصال.

د. **إنكار أو إلغاء الخدمة Denial or Degradation of Service** هو الإضرار المادّي بالنظام لمنع تقديم الخدمة، أو ضخ الرسائل البريدية الإلكترونية دفعة واحدة لتعطيل النظام.

2.5.2.7. اختراق الحماية الشخصيّة Breaches of Personnel Security

تعد المخاطر المتصلة بالأشخاص والموظفين، وتحديداً المخاطر الداخلية منها، واحدة من مناطق الاهتمام العالي لدى جهات أمن المعلومات، إذ ثمة فرصة لأن يُحقّق أشخاص من الداخل ما لا يُمكن نظرياً أن يُحقّقه أحد من الخارج، وتتعلّق هذه بالأخطار الداخليّة والخارجيّة معاً.

أ. **التّخفي Masquerading** وهو انتحال صلاحيات شخص مُفوّض للدخول إلى النظام عبر استخدام وسائل التعريف العائدة له كاستغلال كلمة سرّ أحد المُستخدمين واسم هذا المُستخدم، أو عبر استغلال نطاق صلاحيات المُستخدم الشرعي.

ب. الهندسة الاجتماعية Social Engineering هي خداع الأفراد ومعرفة أرقامهم السّريّة بواسطة ادّعاء شخص بأنّه مستخدم شرعي أو عضو في الشركة أو أحد عناصر النظام يحتاج إلى معلومات وذلك من خلال استغلال علاقات اجتماعية. وأبسط مثال على ذلك أن يتصل شخص بأحد العاملين ويطلب منه كلمة سرّ النظام تحت زعم أنه من قسم الصيانة أو قسم التطوير أو أي قسم آخر، ونظراً لطبيعة الأسلوب الشخصي في الحصول على معلومة الاختراق أو الاعتداء سُميت بالهندسة الاجتماعيّة.

ج. الإزعاج Harassment هي تهديدات يندرج تحتها أشكال عديدة من الاعتداءات والأساليب، ويجمعها توجيه رسائل الإزعاج والتحرّش وربما التهديد والابتزاز، وهي ليست حكراً على البريد الإلكتروني بل تستغلها مجموعات الحوار والأخبار والنشرات الإلكترونية في بيئة الإنترنت والويب، وهي نمط مُتواجد في مختلف التفاعلات عبر الشّبكة وعبر البريد الإلكتروني.

د. قرصنة البرمجيات Software Piracy تتحقق قرصنة البرمجيات عن طريق نسخ الأقراص دون تصريح، أو استغلالها على نحو مادّي دون تخويل بهذا الاستغلال، أو تقليدها والانتفاع المادّي بها على نحو يخلّ بحقوق المُؤلف.

3.5.2.7. اختراق حماية الاتصالات.

Breaches of Communications and Security.

هي الأنشطة التي تستهدف المُعطيات والبرمجيات وتشمل طائفتين:

أ. هجمات البيانات Data Attacks

- **النّسخ غير المُصرّح به Unauthorized Copying** وهي العملية الشائعة التي تستتبع الدخول غير المُصرّح به للنظام، حيث يُمكن الاستيلاء عن طريق النّسخ على كافة أنواع المُعطيات وتشمل البيانات والمعلومات والأوامر والبرمجيات وغيرها.
- **تحليل الازدحام Traffic Analysis** هي دراسة أثر الازدحام على أداء النظام في مرحلة التعامل، ومتابعة ما يتم فيه من اتصالات وارتباطات بحيث

يُستفاد منها في تحديد مَسلكيات المُستخدمين وتحديد نقاط الضّعف ووقت الهجوم المناسب بغرض تسهيل الهجوم على النظام.

- **القنوات الخفيّة Covert Channels** صورة من صور اعتداءات التّخزين، وقد تكون تمهيداً لهجوم لاحق أو تغطية اقتحام سابق أو مجرّد تخزين لمُعطيات غير مشروعة.

ب. هجمات البرمجيات Software Attacks

- **أبواب المصائد Trap Doors** برنامج يُتيح للمُخترق الوصول إلى النظام، إنه ببساطة مدخل مفتوح تماماً كالباب الخلفي للمنزل الذي يَنفذ منه السّارق.
- **اختلاس المعلومة Session Hijacking** وهي أن يستغل الشخص استخداماً مشروعاً من قبل غيره لنظام ما، فيسترق النظر أو يستخدم النظام عندما تُتاح له الفرصة لانشغال المُستخدم دون علمه، أو أن يجلس ببساطة مكان مُستخدم النظام فيطّلع على المعلومات، أو يُجري أية عملية في النظام بقصد الاستيلاء على بيانات أو معلومات تُستخدم في اختراق أو اعتداء لاحق.
- **التلاعب بنقل المُعطيات عبر أنفاق النقل Tunneling** هي استخدام حُزَم المُعطيات المشروعة لنقل معطيات غير مشروعة.
- **الهجمات الوقتية Timing Attacks** هي هجمات تتم بطرق تقنية مُعقّدة للوصول غير المُصرّح به إلى البرامج أو المُعطيات، وتقوم جميعها على فكرة استغلال وقت تنفيذ الهجمة مُتزامناً مع فواصل الوقت التي تفصل العمليات المُرتّبة في النظام.
- **الشيفرات الخبيثة Malicious Code** برامج كاملة أو قسم من شيفرة يمكن أن تكتسح وتغزو النظام وتُعدّ وظائف ليست مقصودة من مالكي النظام تُستثمر للقيام بمهام غير مشروعة كإنجاز احتيال أو غش في النظام.

4.5.2.7. اختراق حماية العمليات Breaches of Operations Security

هي المخاطر المتصلة بعمليات الحماية والتي تستهدف إستراتيجية الدخول، ونظام إدخال ومعالجة والبيانات.

أ. **العبث بالبيانات Data Diddling** هي تغيير البيانات أو إنشاء بيانات وهميّة في مراحل الإدخال أو الإخراج.

ب. **خداع بروتوكول الإنترنت Internet Protocol Spoofing/ IP Spoofing** وسيلة تقنيّة بحتة، بحيث يقوم المُهاجم عبر هذه الوسيلة بتزوير العنوان المُرفق مع حُزمة البيانات المُرسلة بحيث يظهر للنظام على أنه عنوان صحيح مُرسل من داخل الشبكة، بحيث يسمح النظام لحُزمة البيانات بالمرور باعتبارها حُزمة مشروعة.

ج. **تخمين كلمة السرّ Password Sniffing** وتتم عن طريق تخمين كلمات السّر مُستفيدا من ضعف الكلمات عموماً، إذ يجمع البرنامج هذه المعلومات وينسخها إضافة إلى أن أنواع أخرى من هذه البرامج تجمع المعلومات الجزئية وتُعيد تحليلها وربطها معاً، كما يقوم البرنامج بإخفاء أنشطة الالتقاط بعد قيامها بمهمتها.

د. **المسح Scanning** هو برنامج احتمالات يقوم على فكرة تغيير التركيب أو تبديل احتمالات المعلومة، فهو أسلوب تقني يعتمد واسطة تقنيّة هي برنامج (الماسح) بدلاً من الاعتماد على التخمين البشري.

هـ. **استغلال المزايا الإضافيّة Excess Privileges** الأصل أن مُستخدم النظام وتحديداً داخل المؤسسة يكون مُحدّد له نطاق الاستخدام ونطاق الصلاحيات بالنسبة للنظام، لكن ما يحدث في الواقع العملي أن مزايا الاستخدام يجري زيادتها دون تقدير لمخاطر ذلك إذ يحظى المُستخدم بمزايا تتجاوز اختصاصه، وفي هذه الحالة فإن أيّ مخترق للنظام سيكون قادراً على تدمير أو التلاعب ببيانات المُستخدم الذي دخل على النظام من خلال اشتراكه أو عبر نقطة الدخول الخاصة به، إنه ببساطة سيتمكّن من تدمير مختلف ملفات النظام حتى غير المُتصلة بالمدخل الذي دخل منه لأنه استثمر المزايا الإضافية التي يتمتّع بها المُستخدم الذي تم الدخول عبر مَدخله.

3.7. استراتيجية أمن المعلومات[12] Strategy of Information Security

تشـــمل استراتيجية أمن المعلومات السياسة الواضحة بشأن اقتناء وشراء الأجهزة التقنية وأدواتها، والبرمجيات، والحلول المُتّصلة بالعمل، والحلول المُتعلقة بإدارة النظام، كما تشمل استراتيجية الخصوصيّة المعلوماتيّة. كما تضُم استراتيجية أمـــن المعلومـــات أيضـــاً استراتيجية الاشتراكات التي تُحدّد سياسة المنشأة بشأن اشـــتراكات الغير في شبكتها أو نظمها، وكذلك استراتيجيات التّعامل مع المخاطر والأخطـــاء بحيـــث تُحـــدّد ماهية المخاطر وإجراءات الإبلاغ عنها والتعامل معها والجهات المسؤولة عن التعامل مع هذه المخاطر.

أمـــا سياســـة أمـــن المعلومـــات Information Security Policy فهي مجموعـــة القواعـــد التي يُطبّقها الأشخاص لدى التعامل مع التقنية ومع المعلومات داخل المنشأة، وتتصل بشؤون الدخول إلى المعلومات والعمل على نظمها وإدارتها.

وأخـــيراً لا بـــد من التأكيد بأن الاستراتيجية لا تحقق نجاحاً إلا إذا كانت واضحة دقيقة في محتواها ومفهومة لدى كافة المعنيين.

1.3.7. أهداف استراتيجية أمن المعلومات.

1. تعـــريف المُســـتخدمين والإداريين بالتزاماتهم وواجباتهم المطلوبة لحماية نظم الحاســـب والشّـــبكات، وكذلـــك حماية المعلومات بكافة أشكالها سواء في مراحل إدخالها ومُعالجتها وخزنها ونقلها وإعادة استرجاعها.
2. تحديد الآليات التي يتم من خلالها تحقيق وتنفيذ الواجبات المُحدّدة على كل من له علاقة بالمعلومات ونُظمها وتحديد المسؤوليات عند حصول الخطر.
3. بيان الإجراءات المتبعة لتجاوز التهديدات والمخاطر والتعامل معها والجهات المُناط بها القيام بذلك.

2.3.7. منطلقات استراتيجية أمن المعلومات.

تنطلق استراتيجية أمن المعلومات من تحديد المخاطر، أغراض الحماية، ومواطن الحماية، وأنماط الحماية اللازمة، وإجراءات الوقاية من المخاطر.

وتـــتلخص المنطلقات والأسس التي تبنى عليها استراتيجية أمن المعلومات على الاحتياجات المُتباينة لكلّ منشأة من الإجابة عن تساؤلات ثلاث رئيسة هي:

ماذا أريد أن أحمي؟

ممن أحمي المعلومات؟

كيف أحمي المعلومات؟

ومن أكثر وسائل الأمن شيوعاً في بيئة نظم المعلومات:

- برمجيات كشف ومقاومة الفيروسات.
- الجدران النارية Firewall
- الشبكات الافتراضية الخاصة Virtual Private Networks وتتضمّن:
  - التحقّق من هويّة المُستخدمين.
  - الشّبكات الافتراضية الخاصة.
  - مراقبة المحتوى.
  - الجدران الناريّة الخاصّة.
- التشفير Cryptography

4.7. إستراتيجية أمن الإنترنت Strategy of Internet Security

تشمل إستراتيجية أمن الإنترنت على أمن المعلومات في ثلاث مواضع هامّة هي:

1.4.7. المواضع الرئيسة في استراتيجية أمن الإنترنت.

- أمن الشبكة.
- أمن التطبيقات.
- أمن النظم.

وينطوي كل من هذه المواضيع على قواعد ومُتطلبات تختلف عن الأخرى، ويتعيّن أن تكون أنظمة الأمن فيها مُتكاملة مع بعضها البعض حتى تُحقّق الوقاية المطلوبة لأنهـــا بالعموم تنطوي أيضاً على اتصال وارتباط بمستويات الأمن العامّة كالحماية المادّية والحماية الشخصيّة والحماية الإداريّة والحماية الإعلانيّة.

2.4.7. الأنواع الرئيسة المحتملة للهجوم على الشبكات[14].

1.2.4.7. الانقطـــاع Interruption وهي عندما تُرسل الرسالة من المُرسل ولا تصل المُستقبل وقد يكون السّبب في Router المسيّر أو الموجّه.

2.2.4.7. التّصـــدي Interception وهي عندما تُرسل الرّسالة من المُرسل إلى المُستقبل، ولكن وبطريقة غير شرعية يَتصدّى لها مُستمع آخر بالتّنصت واستراق السّمع على المُحادثة.

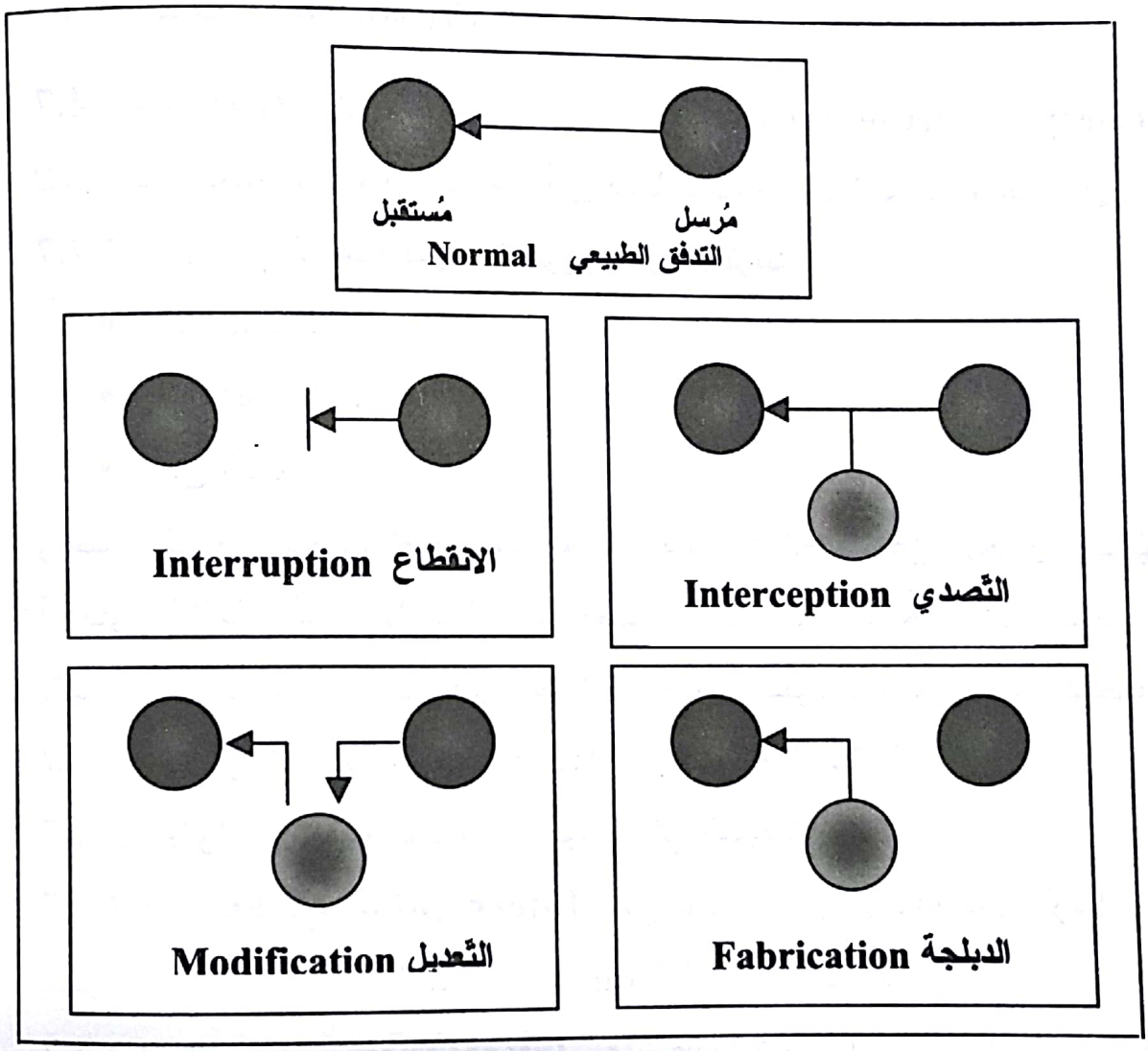
3.2.4.7. التعديل Modification وهي عندما تُرسل الرّسالة من المُرسل إلى المُستقبل ولكن تذهب أولاً إلى مُستمع ثالث يجري تعديل على الرّسالة ثم يُكمل إرسالها مُعدّلة.

4.2.4.7. الدبلجة Fabrication وهي عندما يقوم مُرسل ثالث بفبركة رسالة ثم يقوم بإرسالها بحيث ينظر إليها وكأنها من المصدر الشرعي.

ويبيّن الشكل (7/ 5) الأنواع الرئيسة المحتملة للهجوم على الشّبكات.

الشكل (7/ 5)

الأنواع الرئيسة المحتملة للهجوم على الشّبكات



Stalling, William (2004). ***Cryptography and Network Security: Principles and Practices*** (3rd ed.).

3.4.7. وسائل أمن الشبكات The Means of Networks Security

تتضمّن وسائل أمن الشّبكات عموماً على الآتي:

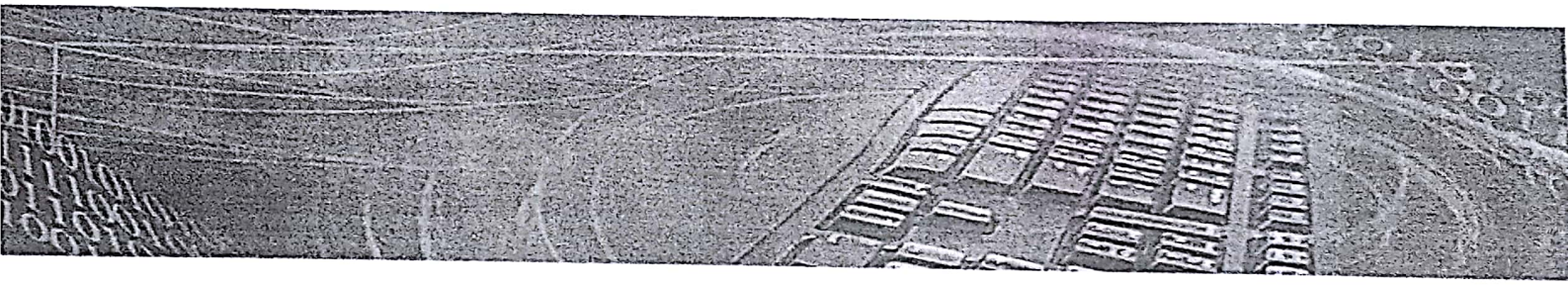
1.3.4.7. التّعريف والسّلامة: وتكون من خلال تزويد نظام المُستقبل بالثّقة في حماية حُزم المعلومات، والتّأكد من أن المعلومات التي وصلت لم يتم تعديلها.

2.3.4.7. السريّة: حماية محتوى المعلومات من الإفشاء إلاّ للجهات المُرسلة إليها.

3.3.4.7. التّحكم بالدخول: وهو تقييد الاتصالات بحصرها ما بين النظام المُرسل والنظام المُستقبل.

- التشفير Encryption : هو عملية تحويل المعلومات إلى شفرات غير مفهومة لمنع الأشخاص غير المرخص لهم من الإطلاع على المعلومات أو فهمها
- فك التشفير Decryption : هو عملية إعادة تحويل البيانات إلى صيغتها الأصلية
- تُستخدم المفاتيح في تشفير الرسالة وفك تشفيرها

- لتشفير عملية قديمة استخدمت لما تنقل الرسائل المهمة بحيث ان الجهة المطلوبة هي وحدها الي تقدر تعرف مضمونها .. ومع تطور الزمن صارت الناس تعتمد على التكنلوجيا في ارسال وإستقبال الرسائل فإنتقلت عملية التشفير لتصبح إلكترونية. ولأن الانترنت فكرته عبارة عن إرسال واستقبال رسائل بين اطراف فعملية الارسال والإستقبال لازم تكون آمنة بحيث محد يقدر يطلع على المعلومات.



- طرق التشفير:
  ١- تشفير متماثل.
- ٢- تشفير غير متماثل.

- عملية التشفير: هي عملية تحويل النص الواضح الى نص غير مفهومة، حالياً تتم بعمليات و معادلات رياضية.
- عملية فك التشفير: عكس عملية التفير أي تحول النص الغير مفهوم إلى نص مفهوم.
- النص الأصلي: هو النص المراد حمايته.
- النص المشفر: هو النص المحمي وفي حال إستلامه إلى اشخاص آخرين لن يحصلوا منه على اية معلومات لأن بيكون على شكل ارقام ورموز مخلوطة وعشوائية.
- مفتاح التشفير: مفتاح يدخل في عملية التشفير لتحويل النص ويدخل في عملية فك التشفير لإرجاع النص.
- ~~مفتاح عام: مفتاح يستخدم لعملية تشفير النصوص فقط.~~
- مفتاح خاص: مفتاح يستخدم لفك تشفير النصوص.