وسائل الحماية من الهجمات الإلكترونية

عبدالله عمير آل عائض

رابط لتقييم الأثر

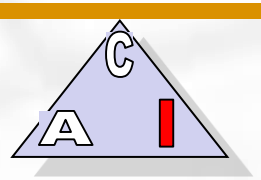
https://forms.gle/beBkGpeAfhxt6wNc6

أمن المعلومات

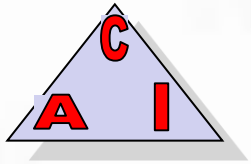
- **تعريف أمن المعلومات** :
  - توفير بيئة آمنة للمعلومات بغض النظر عن مكانها سواء في :
    - حالة التخزين
    - حالة المعالجة
    - حالة النقل
    - حالة التملك
    - أو عند الأفراد

أركان أمن المعلومات الأساسية

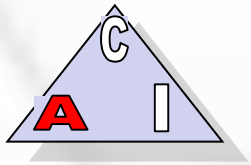
- أخطاء مدخلين



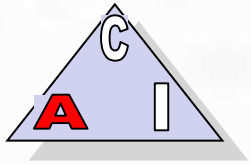
- هاكرز



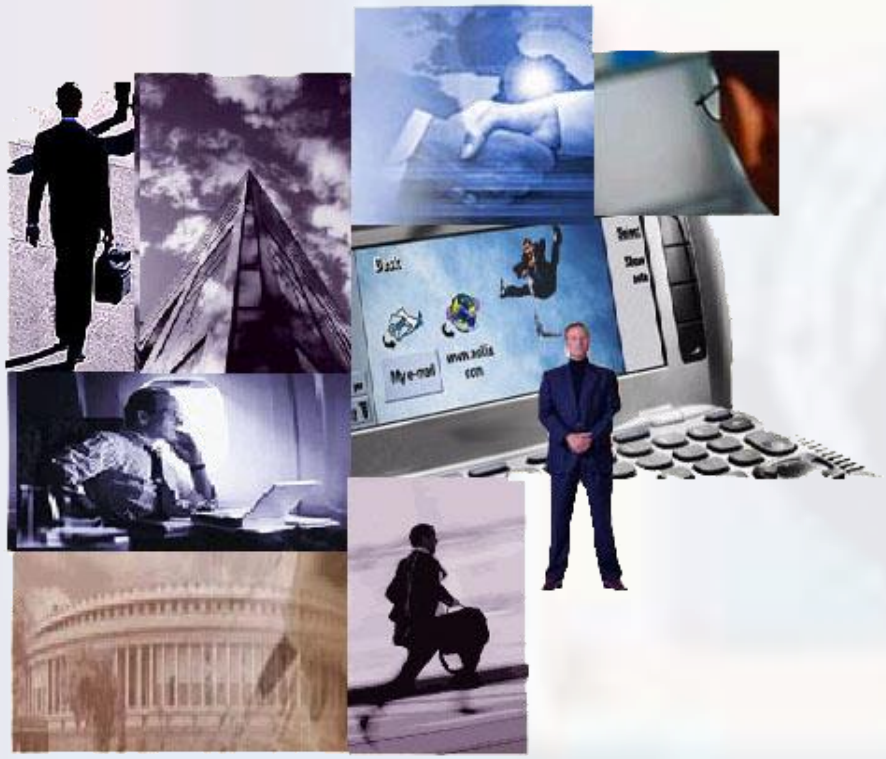
- حذف معلومات



- الحرمان من الخدمة



أهمية أمن المعلومات



- زيادة الاعتماد على أنظمة المعلومات في إنجاز العمل.
- التجارة الإلكترونية، والحكومة الإلكترونية.
- انتشار استخدام شبكات الحاسب واستخدام الانترنت لأداء الأعمال.
- سرعة تغير مجال التقنية المعلوماتية.
- تزايد عدد المخترقين ويقابلها زيادة عدد الثغرات الأمنية.

شمولية أمن المعلومات

- **يشمل أمن المعلومات**:
  - الأمن الفيزيائي (أمن المنشآت).
  - النسخ الاحتياطية.
  - عدم الانكار.
  - التشفير.
  - استمرارية الخدمة رغم كل الظروف.
  - مواجهة الكوارث والحوادث (الحرائق، ... إلخ).
  - مكافحة الفيروسات.
  - التحقيق في جرائم الحاسب.

وسائل الحماية من الهجمات الإلكترونية

- لا يوجد ما يسمى بالحماية المطلقة، وحماية المعلومات كغيرها من أنواع الحماية ، تستوعب نسبة خطر، كلما زادت تقنيات الحماية زادت التكاليف، فمدى عمق الحماية يعتمد على حساسية البيانات المطلوب حمايتها. وإذا حصلت الكارثة يجب أن يكون هناك خطة لاستعادة ما تم العبث به.

- بنائية أمن المعلومات أساسها هو مدى كفاءتها في كل مستوى من مستويات المنشأة، ومدى تفاعل أقسام هذه المؤسسة وموظفيها مع القوانين والأحكام التي وضعت لحماية أمن المنشأة. وعلى المنشأة التأكد من أن جميع عامليها أو حتى عملائها الانصياع لمبادئها وقوانينها وأحكامها، لهذا فإن بنائية المنشأة يجب أن تبنى بالشكل الصحيح لضمان التواصل بين موظفيها.

وسائل الحماية من الهجمات الإلكترونية

- **مسؤوليات التنفيذ والخطة الزمنية**
  - إدارة أمن المعلومات (Information Security Management): هي الجهة التي توفر التوجيهات الأزمة لكل المنشأة وتنشأ القوانين والأحكام لتغطي معظم المخاطر التي تهدد أمن المنشأة,
  - مدقق داخلي **(Internal Audit):** الجهة التي ترفع تقارير دورية في كفاءة إدارة أمن المعلومات إلى المسؤولين عن إدارة المنشأة.

وسائل الحماية من الهجمات الإلكترونية

- **مسؤوليات التنفيذ والخطة الزمنية**
  - منسق أمني **(Security Coordinator):** المسؤول عن التنسيق بين إدارة أمن المعلومات والأقسام.
  - مشرف الأمن(Security Administrator): الجهة التي تقوم على ضمان تطبيق القوانين والأحكام التي تصدر من إدارة أمن المعلومات باستخدام الوسائل المتوافرة لديهم لكل قسم.
  - فريق العمل الأمني **(Security Working Team).**

وسائل الحماية من الهجمات الإلكترونية

- **الخطط الأمنية (Security Plans):**
  - خطة أمن المعلومات هي خطة مكتوبة ومعتمدة من قبل المسؤولين في الإدارة ومعدة للتنفيذ، وعلى أن يتم اختبارها والتأكد من سلامة الإجراءات المتبعة باستمرار، هذه الخطة هدفها هو وضع إجراءات واجب اتباعها للرفع من فاعلية أمن المعلومات ومقاومة أي تدخل خارجي ، مع الأخذ في عين الاعتبار تقليل الخسائر التي قد تنتج إذا ما نجح المتطفلون في الدخول إليها وتمكين الإدارة من استعادة نشاطها في أقل وقت وبأقل تكلفة.

وسائل الحماية من الهجمات الإلكترونية

- **ولضمان نجاح هذه الخطة يجب أن تتوافر لديها العوامل التالية:**
  - دعم الإدارة العليا لهذه الخطة بعد عرضها عليهم وتبيان جميع الأخطار التي قد تحدث ويكون لها آثار سلبية على سير العمل.
  - توعية جميع الموظفين بالإدارة بأهمية المعلومات بالنسبة إلى نشاطات وأعمال الإدارة في خلال عقد الاجتماعات الدورية وأيضاً المقالات والنشرات والندوات.
  - تحديد الموارد المالية اللازمة للحفاظ على استمرارية الخطة وتشغيل التطبيقات بالشكل الصحيح.
  - تدريب المختصين وذوي العلاقة بالمعلومات على تنفيذ هذه الخطة وأيضاً اختبارها باستمرار.
  - المرونة في إعداد الخطة والواقعية في تقدير الأخطار.

وسائل الحماية من الهجمات الإلكترونية

- يجب تصميم خطط أمن المعلومات لكل مجموعة من الأنظمة المتشابهة ، مثال على ذلك (الأجهزة الخاصة بمشرفي الشبكات يجب أن تغطى من قبل خطة أمنية) ، حيث تعرف بنائية النظام وهرمية المعلومات ومستخدمي النظام ، مبينا التهديدات الممكنة على كل نظام ، ثم ذكر كيفية حمايته ووضع خطط بديلة (Contingency Plans) في حالة حدوث الكارثة ، وتفاصيل عملية الحفاظ على الأمن .

وسائل الحماية من الهجمات الإلكترونية

- **الأحكام والقوانين (Security Policy):**
  - أهم عناصر بنائية أمن المعلومات هي الأحكام والقوانين (Policies) ، كل منشأة بحاجة إلى قوانين وأحكام لتعريف الحدود المقبولة للسلوك في العمل وكيفية الرد على أي مخالفة تحدث. وبالطبع تختلف القوانين والأحكام من منشأة إلى أخرى ، حسب احتياجات كل منشأة ، ومن الأمثلة على بعض هذه القوانين والأحكام:
    - منع استخدام ألعاب الكمبيوتر على أجهزة الحاسب في المنشأة.
    - منع إرسال رسائل إلكترونية بحجم أكبر من 2 ميجابايت.
    - عدم استخدام أي برامج مقرصنة.

وسائل الحماية من الهجمات الإلكترونية

- القواعد والأحكام في المنشأة يجب أن تهدف إلى كيفية عمل الأنشطة ، ثم تتبع بكتيبات وتدريبات واجتماعات لشرح هذه القواعد، ومعرفة كيفية تطبيقها. كل قسم في المنشأة يجب أن يحوي قواعد وأحكاماً خاصة به تعرف أنشطة القسم ، حيث ترتبط هذه القواعد والأحكام (Departmental Policy) بالقواعد والأحكام بأمن المعلومات في الحاسب الآلي (Departmental Information Security)، التي بدورها يجب أن تنشأ من قبل الفنيين والإدارة العليا.

وسائل الحماية من الهجمات الإلكترونية

- القوانين والأحكام يجب أن تكون مباشرة ولا تتجاوز العشر صفحات، ويجب أن تكون سهلة الفهم ويتم مراجعتها من قبل القانونيين ومعرفة كل الثغرات القانونية، ويجب أن يبين دور كل موظف وكل قسم، وهدف القوانين والأحكام أيضاً يجب أن تبين الوثيقة أهمية حماية المعلومات في هذه المنشأة.

وسائل الحماية من الهجمات الإلكترونية

- **أمن المعلومات هو مسؤولية كل الأفراد في المنشأة لأن قوة أمن المعلومات تقاس بأضعف نقطه به، ولضمان قبول الأفراد في المنشأة لهذه القوانين والأحكام ينصح القيام بالتالي:**
  - لا يتم نشر القوانين مرة واحدة على الأفراد، وإنما يجب تقديمها لهم نقطة نقطة.
  - تقديم أمثله حية لمتطلبات الأمن والاختراقات الممكنة.
  - نبذ جرائم الكمبيوتر بجميع أشكالها.
  - تشجيع العاملين بدلاً من تخويفهم (مثلاً تقديم حوافز مالية للموظف المثالي).
  - القيام بالتدريب اللازم للأفراد للمحافظة على أمن المعلومات.
  - المعرفه الشخصية للأفراد من قبل مشرفي الأمن.
  - عمل اجتماعات دوريه تثقيفية للأفراد لتقديم أحدث المخاطر الأمنية.

وسائل الحماية من الهجمات الإلكترونية

- **هناك وظيفتان رئيسيتان للقواعد والأحكام (Policies) :**

1. داخلية **(Internal Policies):** حيث يذكر فيها ما هو المطلوب من الموظفين وكيفية جزائهم على الأعمال التي يقومن بها.
2. خارجية **(External Policies):** حيث يتم تذكير العالم خارج المنشأة عن كيفية عملها ، وأن هناك أحكاماً وقواعد لحمايتها.

وسائل الحماية من الهجمات الإلكترونية

الخطط البديلة :

- هدف أمن الحاسب الآلي هو حماية المعلومات في المنشأة ، المعلومات يجب أن لا تضيع ولا تلغى ولا تعدل ، وتكون دائما متوافرة للمستخدمين ، أما هدف الخطط البديلة فهو التقليل بقدر الإمكان من آثار أي حادث أو اختراق يتم في المنشأة ، الخطط البديلة يجب أن تركز على استمرارية العمل في المنشأة، حيث يجب أن تشمل الخطة كل النواحي الحساسة في المنشأة.
- الخطط البديلة قد تطبق وقد لا تطبق ، ويجب أن يكون في داخلها إجراءات لكل كارثة ممكنة ، ويجب أخذ الأسئلة التالية بعين الاعتبار عند إنشاء الخطط البديلة:

1) كيف يمكن للكارثة أن تؤثر في عمل المنشأة؟ وما مدة هذا التأثير؟
2) ما مستوى عمل المنشأة بعد هذا التأثير؟.

وسائل الحماية من الهجمات الإلكترونية

- **النسخ الاحتياطي وحماية الملفات (Backup & File Protection):**
  - من أهم وسائل حماية المعلومات وجود إستراتيجية للنسخ الاحتياطي للعتاد والبرمجيات والمعلومات والتوثيقات ، ويجب تحديد هذه الإستراتيجية في القواعد والأحكام الخاصة في النسخ الاحتياطي (Backup Policy) ، حيث يتم ذكر الإجراءات والخطوات اللازمة لعمل النسخ الاحتياطية وذكر الجدول الزمني لكل منها.

وسائل الحماية من الهجمات الإلكترونية

- **أنواع النسخ الاحتياطي**:

1) داخل المنشأة **(On Site):**

- وضع النسخ الاحتياطية في داخل المنشأة ، في مكان أمين ، مثل خزنة آمنة.

2) خارج المنشأة (Off Site):

- حيث توضع النسخ الاحتياطية في مكان آمن خارج المنشأة. مثل البنوك.

3) Remote Off Site :

- حيث توضع النسخ الاحتياطية في مكان آمن خارج المنشأة ولكن ممكن الوصول إليها عبر الإنترنت أو الشبكة باستخدام الاتصال عن بعد remote Connection.

وسائل الحماية من الهجمات الإلكترونية

- **وسائط التخزين (Storage Media) : فيما يلي أمثلة على وسائط التخزين:**

1. القرص المرن **(Floppy Disk)**
2. القرص الصلب **(Hard Disk)**
3. القرص الليزري **(CD-Rom)**
4. أشرطة ممغنطة **(Tapes)**
5. ذاكرة فلاش **(Flash memory)**

وسائل الحماية من الهجمات الإلكترونية

- **استرجاع المعلومات**:
  - عملية استرجاع التطبيقات هي عبارة عن وسيلة دفاعية لحماية التطبيقات من أي ظروف خارجية مثل الحريق أو الزلزال أو الفيضانات أو غيرها من الظروف. ويجب أن تكون الإدارة حريصة كل الحرص على تأمين هذه التطبيقات بشكل متكامل وبدون أي نقصان يكون له التأثير السلبي في عملها، ولضمان استرجاع التطبيقات نورد فيما يلي بعض الإجراءات التي يجب أن تتخذ وهي:
  - تخزين النسخ الاحتياطية في مكان آمن على أن يتم استرجاعها بواسطة برامج مساعدة وجاهزة.
  - يجب أن تكون معلومات استرجاع التطبيقات واضحة بالنسبة لجميع المشغلين المسؤولين عن عملية الاسترجاع.
  - التأكد من سلامة التطبيقات وطرق استرجاعها من وقت لآخر حتى نضمن سلامتها وعدم تعرضها لأي مشكلة تذكر.

وسائل الحماية من الهجمات الإلكترونية

- **الحماية حسب المادة المطلوب حمايتها (File Protection):**
  - يتكون الحاسب الآلي كنظام متكامل من عدة طبقات:

➢ الطبقة الخارجية المادية والتي تتمتع بدرجات مختلفة من الحماية تبدأ من وضع الجهاز في مكان آمن آخر بعيد عن الأشخاص المتطفلين أو أن تقوم بإزالة مزود الطاقة أو كابلات الاتصال أو لوحة المفاتيح، وطبعاً هذه الأمور ليست عملية، خاصة عند استخدام جهاز حاسب لشخص آخر.

وسائل الحماية من الهجمات الإلكترونية

- طبقة نظام التشغيل حيث تقدم غالبية أنظمة التشغيل برامج حماية وبرامج كلمة مرور فاعلة يصعب على المتطفلين اختراقها بسهولة.
- طبقة التطبيقات حيث يمكن حمايتها بالعديد من الطرق ابتداء بتسميتها بأسماء لا تعكس محتوياتها ولكنها معروفة لأشخاص معينين. أو إخفاء هذه التطبيقات في مجلدات لا يمكن الوصول إليها بسهولة.
- طبقة المجلدات ويمكن حمايتها من خلال تسميتها بأسماء لا تعكس محتواها أو إخفاؤها، أو إضافة برامج لحماية المجلدات بكلمة مرور.
- طبقة الملفات ويمكن حمايتها بوسائل مختلفة. إما بإخفائها بحيث يصعب الوصول إليها، وإما بتسميتها بأسماء لا تعكس محتواها أو وضع برامج حماية لها بكلمة مرور.

وسائل الحماية من الهجمات الإلكترونية

- **الحماية حسب صلاحيات المستخدم (User Privileges):**
  - حيث يجب تحديد الصلاحيات لكل مجموعة من مجموعات المستخدمين من قبل مشرفي الحاسب الآلي، الذين يمكن تصنيفهم على النحو التالي:
  - المستفيدون :
    - الإدارة العليا.
    - مديرو الإدارات.
    - الموظفون المسؤولون عن إدخال البيانات وتحديثها.
    - الموظفون الذين يستخدمون البيانات.
    - جمهور المتعاملين مع المؤسسة.

وسائل الحماية من الهجمات الإلكترونية

- متخصصون في الحاسب الآلي:
  - مدير النظام.
  - مدير قاعدة البيانات.
  - مدير أمن النظام.
  - المبرمجون.
  - المشغلون.

وسائل الحماية من الهجمات الإلكترونية

- **التحقق من الشخصية والصلاحيات**

(Authentication & Authorization):

- التحقق من الشخصية يعني ربط الشخص مع صلاحياته ، حيث إنه يجب تقديم بيانات تمكن النظام من التأكد من شخصية المستخدم ، هذه البيانات قد تأتي من إحدى الأمور التالية:

1. بيانات مقدمة من قبل المستخدم (كلمة السر).
2. ماذا بحوزة المستخدم؟ (كارت رقمي).
3. هوية المستخدم (بصمة الاصبع).
4. شكل المستخدم (Face or Eye Recognition).
5. صوت المستخدم (Voice Recognition).

وسائل الحماية من الهجمات الإلكترونية

- **استخدام كلمات المرور (Passwords):**
  - يعتبر هذا هو خط الدفاع الأول للتأكد من صلاحية المستخدم في بث البيانات. وهذا هو أسهل أسلوب وأرخص أسلوب كذلك ، ولكي يحقق هذا الأسلوب النجاح يجب توعية المستخدمين بعدم التخلي عن كلمة المرور لأي شخص، وأن يفرض عليهم تغييرها بصفة دورية. يجب كذلك تشفير كلمات المرور في الملفات المستخدمة لحفظها في الحاسب، وعند إدخال كلمة المرور لا يجب أن يعرض النظام حروفها حتى لا تنكشف أمام المتطفلين. كما تتبع بعض الجهات أسلوب تخصيص كلمات المرور بواسطة مختص الشبكة أو مسؤول أمن النظام، وذلك لتلافي المحاولات البسيطة لتخمين كلمة المرور التي قد تكون اسم أحد أبناء المستخدم أو تاريخ ميلاده مثلاً.
  - ومن عيوب هذا الأسلوب أنه يمكن كسره بسهولة بواسطة برامج تقوم بعمل عدد لا نهائي من المحاولات حتى تتوصل إلى الكلمة الصحيحة، ولذلك يجب تحديد عدد المحاولات الفاشلة التي يتم بعدها فصل الحاسب الشخصي عن الشبكة وإيقافه عن العمل تماماً.

وسائل الحماية من الهجمات الإلكترونية

- **وسائل أخرى للتحقق من الشخصية**

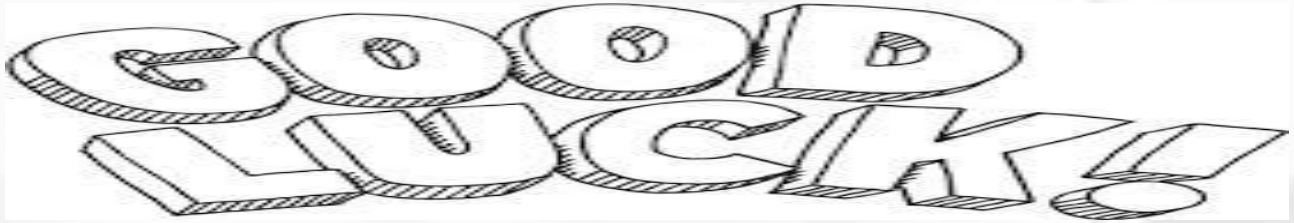
(Other Methods of Authentication):

- الملامح الفيزيائية للفرد (Biometric): حيث تستخدم هذه التقنية أدوات وأجهزة للتعرف على الشخص عن طريق ملامحه الفيزيائية التي تختلف من شخص لآخر ، وهناك عدة أنواع :

1) بصمة الصوت (Voice Print).
2) بصمة الأصبع (Finger Print).
3) التعرف على الوجه (Face Recognition).
4) التعرف على القزحية(Iris Recognition).

وسائل الحماية من الهجمات الإلكترونية

- **وسائل أخرى لحماية الأنظمة** :
  - جدران الحماية
  - IPS & IDS
  - البروتوكولات الآمنة
  - أنظمة الحماية
  - تقسيم الشبكة
  - تفعيل مبدئ الصلاحيات الأقل
  - عمل مسح للثغرات الموجودة بالأنظمة
  - Penetration test



عبدالله عمير آل عائض

ماجستير الأمن السيبراني

بكالوريوس هندسة حاسب آلي

Contact :

aom0885@gmail.com

LinkedIn :

http://linkedin.com/in/abdallah-o-alayed-276b66140

WITH BEST REGARDS.

To Reference : Google