أمن المعلومات:
حماية البيانات في العصر الرقمي

أ.محمد محمود البنا

أخصائي نظم ومعلومات
الإدارة العامة لنظم المعلومات والتحول الرقمي

أمن المعلومات "Information Security" هو مجال متخصص ضمن علوم التقنية الحديثة يشير إلى مجموعة من الأدوات، العمليات، والإجراءات التي يتم إستخدامها لحماية البيانات الرقمية من الوصول أو التعديل غير المصرح به، وكذلك من التدمير أو السرقة سواءً كان الحديث عن تخزين البيانات أو نقلها من موقع إلى آخر، يهدف أمن المعلومات إلى حماية الخصوصية وضمان عدم تعرض البيانات للحوادث الأمنية.

أهمية أمن المعلومات :

في العصر الرقمي، أصبح أمن المعلومات أساسياً لكل مؤسسة، خاصة تلك التي تتعامل مع بيانات حساسة مثل البنوك أو المؤسسات الحكومية الأمان هنا ليس مجرد خيار، بل هو ضرورة للحفاظ على الثقة والمصداقية.

المبادئ الأساسية لأمن المعلومات :

تتمحور حماية المعلومات حول ثلاثة مبادئ أساسية تُعرف باسم "مثلث CIA"

١- السرية (Confidentiality) :

الحفاظ على سرية المعلومات هو الهدف الأول لأمن المعلومات، يعني هذا التأكد من أن البيانات لا يمكن الوصول إليها أو تعديلها إلا من قبل الأشخاص المخوّلين بذلك، تعتمد السرية على وسائل مثل التشفير وتحديد صلاحيات المستخدمين، لحماية المعلومات من الإختراقات أو التسريب.

٢- التكامل وسلامة المحتوى (Integrity):

يعنى هذا المبدأ بالحفاظ على سلامة البيانات من التعديل غير المصرح به أو الفقدان، يتطلب ذلك وسائل حماية تمنع التخريب أو الفساد المتعمد وغير المتعمد للمعلومات، يتم تحقيق ذلك من خلال نسخ إحتياطية مستمرة وإجراءات صارمة تضمن أن البيانات تظل صحيحة ودقيقة.

٣- استمرارية توفر المعلومات (Availability):

توافر المعلومات يعني ضمان أن تكون البيانات متاحة للإستخدام في أي وقت من قبل الأشخاص المخوّلين بذلك، يتم تحقيق هذا من خلال إستخدام الحوسبة السحابية والتقنيات الأخرى التي تضمن الوصول الآمن والسهل إلى البيانات في أي وقت ومن أي مكان.

العناصر الأساسية لأمن المعلومات :

لضمان الحماية الشاملة للمعلومات، يعتمد أمن المعلومات على عدة عناصر رئيسية، هي:

١- أمن الشبكات Network security:

يهدف هذا العنصر إلى حماية الشبكات التي تُنقل عبرها المعلومات من أي اختراقات أو تهديدات محتملة التي قد تؤثر على سرية وسلامة وتوافر البيانات التي يتم تبادلها عبر الشبكة، تستخدم الشركات والهيئات أنظمة متقدمة مثل الجدران النارية وأنظمة كشف التسلل وتقنيات التشفير و السياسات الأمنية لضمان أن البيانات والمعلومات تظل محمية من الهجمات والمخاطر.

٢- أمن البرمجيات Software security :

يتعلق هذا الجزء بحماية البرمجيات من الثغرات والتهديدات الأمنية التي قد تُستخدم لإستغلال البيانات، يعتمد على تطوير برامج آمنة تعمل على تشفير البيانات، وتقليل الأخطاء البرمجية التي يمكن أن تؤدي إلى اختراقات، تتضمن الإجراءات الرئيسية إختبارات الأمان الدورية وتحديثات البرامج لسد الثغرات المكتشفة.

مثال عملي :

تعتمد الأنظمة المصرفية بشكل أساسي على أمن البرمجيات لضمان حماية بيانات العملاء ومعاملاتهم اليومية، يتم إستخدام تقنيات التشفير المتقدمة لحماية كل عملية تتم عبر الإنترنت.

٣- أمن المعدات Hardware security :

يشمل أمن الأجهزة حماية المعدات المادية مثل (أجهزة الخوادم، الحواسيب، والمراكز البيانية) التي تُستخدم لتخزين ونقل المعلومات، يعتمد ذلك على تأمين المعدات من التلف ،السرقة، أو أي محاولات إختراق فيزيائية.

إجراءات الأمان :

تتضمن حماية المعدات إستخدام كاميرات المراقبة، أنظمة الدخول المعتمدة على بصمات الأصابع، ومراقبة الحرارة والرطوبة في مراكز البيانات لضمان حماية مثالية.

مكونات نظام أمن المعلومات :

يُقسم أمن المعلومات إلى عدة مستويات وأنظمة تهدف جميعها إلى حماية البيانات من التهديدات المختلفة. تشمل هذه الأنظمة:

١- الأمن المادي Physical security:

يهتم هذا الجانب بحماية الأصول المادية للمؤسسة، مثل المكاتب والمعدات، يتضمن إتخاذ تدابير تمنع الوصول غير المصرح به إلى أماكن تخزين المعلومات بإستخدام كاميرات المراقبة وأنظمة الدخول المحمية.

٢- الأمن الشخصي Personal security :

يُعنى بتثقيف الأفراد الذين لديهم صلاحية الوصول إلى البيانات والأنظمة المستخدمة، يتضمن تدريبهم على أفضل ممارسات الأمن السيبراني لضمان عدم تعرضهم لعمليات الإحتيال السيبراني أو إختراقات البيانات نتيجة لسوء الإستخدام، وبشكل عام، فإن هذه الوسائل تتوزع إلى ثلاثة أنواع:

شئ تعرفة: هو معلومة يمتلكها الشخص مثل كلمة المرور أو الرمز السري أو الرقم الشخصي.

شيء تملكه: هو شئ مادي يخص الشخص مثل بطاقة بلاستيكية (Credit Card) وما شابه ذلك.

شيء يرتبط بك: هو شئ مرتبط بخصائص الشخص البيلوجية أو الجسدية, مثل بصمة الأصبع أو بصمة العين أو الصوت.

مثال واقعي :

في الشركات والمؤسسات الكبرى، غالبًا ما يتم تنظيم دورات تدريبية دورية حول كيفية التعامل مع البريد الإلكتروني المشبوه والتأكد من عدم تسريب كلمات المرور.

٣- أمن المنظمات Security organizational :

يُركز على إتخاذ التدابير الوقائية داخل المنظمات لضمان حماية البيانات من التهديدات الداخلية والخارجية، يشمل إستخدام أنظمة الحماية للمعلومات مثل نظم إدارة الوصول وأنظمة حماية قواعد البيانات.

قائمة المراجع :

1 - https://academy.hsoub.com - https://tinyurl.com/4rjums79

2 - https://engineering.futureuniversity.com - https://tinyurl.com/4ae34cz8

3 - https://www.microsoft.com/en-us/security/business/security-101/what-is-information-security-infosec

تابعونا في الجزء الثاني من المقالة ....