أمن المعلومات:
كيفية وطرق حماية البيانات في العصر الرقمي

أ.محمد محمود البنا
أخصائي نظم ومعلومات
الإدارة العامة لنظم المعلومات والتحول الرقمي

مع تزايد الاعتماد على التكنولوجيا والإنترنت، أصبحت البيانات الرقمية هدفًا رئيسيًا للهجمات الإلكترونية. سواء كنت فردًا عاديًا، أو صاحب عمل، أو مؤسسة حكومية، فإن حماية البيانات الشخصية والحساسة تُعد ضرورة ملحّة، فقد يؤدي الإهمال أو الاختراق إلى خسائر مالية، وانتهاك الخصوصية، وحتى الابتزاز الإلكتروني.

في هذا المقال، سنتناول بالتفصيل أهم الطرق والاستراتيجيات لحماية البيانات من المخاطر الأمنية، بدءًا من تقنيات الأمان الأساسية، وصولًا إلى الحلول المتقدمة.

تتعدد أنواع التهديدات الإلكترونية، ولكل نوع طريقة معينة يؤثر بها على الأنظمة؛ ومن أبرز التهديدات:

- البرمجيات الخبيثة (Malware):

تشمل الفيروسات، وأحصنة طروادة، وبرامج التجسس، حيث تُزرَع هذه البرمجيات الخبيثة بهدف تعطيل الأنظمة أو سرقة البيانات.

- الهجمات الموجهة (Targeted Attacks):

يتم تصميمها خصيصًا لاختراق نظامٍ معيّن أو شركةٍ محددة، وغالبًا ما تُستخدم فيها تقنيات معقّدة وتخصيصٌ دقيق للرسائل (شخصنة)، بهدف خداع الضحية واستهداف نقاط الضعف بفعالية.

- برامج الفدية (Ransomware):

تقوم بتشفير بيانات الشركة وتطالب بفدية مقابل فك التشفير، وتُعتبر من أخطر التهديدات التي تواجهها الشركات

- التصيد الإلكتروني (Phishing):

يتم فيه خداع الأفراد للحصول على معلومات حساسة، مثل كلمات المرور وأرقام البطاقات الائتمانية، من خلال رسائل بريد إلكتروني مزيفة

- هجمات (الحرمان من الخدمة) DDoS:

تعتمد على إغراق النظام بكميةٍ ضخمةٍ من الطلبات، مما يؤدي إلى تعطيله وعدم استجابته للطلبات المشروعة.

كلمات المرور وإدارتها بذكاء:

تُعد كلمات المرور الضعيفة من أكثر الأسباب شيوعًا لاختراق الحسابات، لذا يُنصح باتباع القواعد التالية:

- إنشاء كلمات مرور معقدة :

- أن تحتوي على أحرف كبيرة وصغيرة، وأرقام، ورموز خاصة (@، #، !، $، ...)، وألا تقل عن ١٢ إلى ١٦ حرفًا.

- تجنُّب استخدام المعلومات الشخصية في كلمات المرور، مثل الاسم، وتاريخ الميلاد، أو رقم الهاتف.

- عدم تكرار كلمة المرور عبر الحسابات المختلفة :

إذا تم اختراق أحد الحسابات، فسيكون من السهل على القراصنة الوصول إلى باقي الحسابات في حال كانت كلمات المرور متشابه

- إستخدام برامج إدارة كلمات المرور :

بدلًا من حفظ كلمات المرور يدويًا، يمكن الاعتماد على برامج إدارة كلمات المرور مثل: Bitwarden وLastPass، حيث تتميز هذه البرامج بتشفير قوي للبيانات، وتوافق مع العديد من الأجهزة والمنصات، كما أنها تدعم المصادقة الثنائية، ويمكن استخدامها سواء عبر الإنترنت أو على الجهاز المحلي.

- تفعيل المصادقة الثنائية (2FA) :

تفعيل المصادقة الثنائية (2FA) هو عملية تهدف إلى زيادة أمان الحسابات عبر الإنترنت من خلال إضافة طبقة أمان إضافية إلى عملية تسجيل الدخول، وذلك عبر إرسال رمز تحقق إلى الهاتف أو البريد الإلكتروني. تهدف هذه الطبقة الإضافية إلى تأكيد هوية المستخدم، وتحقيق مستوى أعلى من الأمان، مما يمنع المخترقين من الوصول إلى الحساب، حتى في حال امتلاكهم لكلمة المرور.

تشفير البيانات لحمايتها من الاختراق:

تُعَدّ كلمات المرور الضعيفة من أكثر الأسباب شيوعًا لاختراق الحسابات، لذا يجب اتباع القواعد التالية:

● كيف يعمل تشفير الملفات والمجلدات؟

تشفير الملفات والمجلدات يتم من خلال استخدام خوارزميات تشفير قوية لتحويل البيانات إلى شكل غير مقروء. تعتمد هذه الخوارزميات على مفاتيح تشفير تُستخدم لتحويل البيانات، ويجب امتلاك هذه المفاتيح لإعادة ترجمة البيانات إلى شكلها المقروء من جديد.

● أدوات تشفير الملفات والمجلدات :

- VeraCrypt: برنامج تشفير مجاني ومفتوح المصدر، يمكنه تشفير الملفات والمجلدات.
- BitLocker: برنامج تشفير مدمج في نظام التشغيل (Windows)، يُستخدم لتشفير الملفات والمجلدات.
- FileVault: برنامج تشفير مدمج في نظام التشغيل (macOS)، يُستخدم لتشفير الملفات والمجلدات.

● استخدام البريد الإلكتروني المشفر :

البريد الإلكتروني المشفَّر يعمل من خلال استخدام خوارزميات تشفير قوية لتحويل محتوى الرسالة إلى شكل غير مقروء. وتستخدم هذه الخوارزميات مفاتيح تشفير لتحويل البيانات، ولا يمكن قراءة الرسالة مرة أخرى إلا بامتلاك المفاتيح الصحيحة لفك التشفير وإعادتها إلى شكلها الأصلي.

إستخدام بروتوكولات إتصال آمنة :

التأكّد من أن المواقع التي يتم زيارتها تستخدم HTTPS بدلًا من HTTP يُعد خطوة مهمة لضمان أمان البيانات المُرسلة أو المُستلمة عبر الإنترنت.

● ما هو HTTPS؟

HTTPS (HyperText Transfer Protocol Secure) هو بروتوكول اتصال أمن يستخدم لتحميل صفحات الويب وتبادل البيانات عبر الإنترنت، يعتمد HTTPS على تشفير البيانات باستخدام تقنيات التشفير مثل SSL/TLS، مما يحمي البيانات من الوصول غير المصرح به أو التلاعب بها.

● لماذا يجب استخدام HTTPS بدلًا من HTTP؟

- أمان البيانات: يضمن HTTPS أن البيانات التي يتم إرسالها أو استلامها عبر الإنترنت تكون مُشفّرة، مما يحميها من الوصول غير المصرح به أو التلاعب أثناء انتقالها.

- الحماية من الهجمات: يُوفّر HTTPS حماية من الهجمات التي تستهدف بروتوكول HTTP، مثل هجمات "الرجل في الوسط" (Man-in-the-Middle - MitM)، والتي تهدف إلى اعتراض البيانات وسرقتها أثناء نقلها.

- زيادة الثقة: يُعزّز استخدام HTTPS من ثقة المستخدمين في الموقع، إذ يُعتبر علامة على أن الموقع يُولي أمان البيانات أهمية كبيرة، ويحرص على حماية معلومات الزوار.

استخدام VPN : (الشبكة الخاصة الافتراضية) عند تصفح الإنترنت عبر شبكات غير آمنة يُعد خطوة مهمة لحماية البيانات من التتبع والتجسّس.

النسخ الاحتياطي المنتظم للبيانات :

النسخ الاحتياطي هو خط الدفاع الأخير ضد فقدان البيانات بسبب هجمات الفدية أو الأعطال التقنية.

● أنواع النسخ الاحتياطي :

- نسخ إحتياطي محلي: حفظ نسخة من البيانات على أقراص خارجية أو أجهزة NAS.
- نسخ إحتياطي سحابي: استخدام خدمات مثل، Google Drive، OneDrive Dropbox لتخزين البيانات المشفرة.

● تطبيق قاعدة النسخ الاحتياطي ٣ - ٢ - ١

هو نهج شائع لحماية البيانات من الفقدان أو التلف وهي قاعدة بسيطة تنص على أن يتم إنشاء ثلاث نسخ من البيانات، على وسائط مختلفة، في مواقع مختلفة، هذه القاعدة تهدف إلى حماية البيانات من الفقدان أو التلف الناجم عن الأعطال الفنية أو الكوارث الطبيعية أو الهجمات الإلكترونية.

● ما هي المكونات الثلاثة لقاعدة النسخ الاحتياطي ٣ - ٢ - ١ ؟

١- ثلاث نسخ : يجب إنشاء ثلاث نسخ من البيانات، بما في ذلك النسخة الأصلية والنسختين الإحتياطيتين

٢- وسائط مختلفة : يجب تخزين النسخ الثلاثة على وسائط مختلفة، مثل الأقراص الصلبة والوسائط البصرية والخدمات السحابية.

٣- مواقع مختلفة : يجب تخزين النسخ الثلاثة في مواقع مختلفة، مثل المكتب والمنزل ومراكز البيانات وذلك تحسبًا للكوارث.

الحذر من التصيد الاحتيالي والهجمات الإلكترونية:

● كيف تتعرف على محاولات التصيد؟

- رسائل البريد الإلكتروني أو الرسائل النصية التي تطلب معلومات حساسة مثل كلمات المرور.
- رسائل تحتوي على روابط مشبوهة أو عناوين بريدية غير متطابقة مع الموقع الرسمي.
- رسائل تطلب إجراءات عاجلة مثل "حسابك سيتم إغلاقه خلال ٢٤ ساعة".

● كيفية تتجنب التصيد الاحتيالي؟

- لا تنقر على الروابط غير المعروفة.
- تحقق من هوية المرسل قبل مشاركة أي معلومات.
- إستخدم إضافات المتصفح مثل (Netcraft وuBlock Origin) لحظر المواقع الاحتيالية.
- فعّل ميزة الحماية المتقدمة في (Gmail أو Outlook) لإكتشاف الرسائل الضارة.

تأمين الشبكات والاتصالات:

● ما هي المكونات الثلاثة لقاعدة النسخ الاحتياطي ٣ - ٢ - ١ ؟

النسخ الاحتياطي هو خط الدفاع الأخير ضد فقدان البيانات بسبب هجمات الفدية أو الأعطال التقنية.

- استخدم تشفير WPA3 أو WPA2-PSK بدلاً من WEP): WEP (Wired Equivalent Privac هو تشفير قديم وغير آمن، ويجب استبداله بتشفير WPA3 أو WPA2-PSK WPA3 وهو تشفير أحدث وأكثر أمانًا، بينما WPA2-PSK هو تشفير شائع الاستخدام ويتمتع بمستوى جيد من الأمان.

- غيّر أسم وكلمة مرور الراوتر الافتراضية:اسم وكلمة مرور الراوتر الافتراضية تكون عادة معروفة للجميع، وبالتالي يجب تغييرها لمنع الوصول غير المصرح به إلى الشبكة، أختر أسم وكلمة مرور قوية ومميزة.

- قم بإيقاف WPS لأنها نقطة ضعف أمنية شائعة في الشبكات: WPS (Wi-Fi Protected Setup) هي ميزة تتيح لك توصيل الأجهزة بسهولة إلى الشبكة، ولكنها يمكن أن تكون نقطة ضعف أمنية إذا لم يتم إيقافها. قم بإيقاف WPS لمنع الوصول غير المصرح به إلى الشبكة.

● استخدام VPN عند الاتصال بشبكات Wi-Fi عامة:

الشبكات العامة مثل مقاهي الإنترنت والمطارات غالبًا ما تكون غير آمنة، لذا أستخدم VPN لإخفاء نشاطك وتشفير إتصالك.

● تفعيل الجدران النارية : (Firewalls) :

تساعد الجدران النارية على منع الاتصالات المشبوهة وحماية الأجهزة من الهجمات الإلكترونية.

تأمين الشبكات والاتصالات:

في المؤسسات والشركات، يجب تطبيق مبدأ " الأقل امتيازًا " (Least Privilege) : مبدأ "الأقل امتيازًا" هو مفهوم في الأمن السيبراني يهدف إلى تقليل المخاطر من خلال منح المستخدمين أو البرامج أو الأنظمة الحد الأدنى من الصلاحيات اللازمة لأداء مهامهم. هذا يعني أن كل مستخدم أو نظام يجب أن يتمتع فقط بالصلاحيات اللازمة لعمله، ولا يزيد عن ذلك.

الغرض من هذا المبدأ هو تقليل خطر الاختراقات الأمنية ويشمل : تحديد الصلاحيات: تحديد الصلاحيات اللازمة لكل مستخدم أو مجموعة مستخدمين بناءً على مهامهم وواجباتهم، منح الصلاحيات: منح الصلاحيات اللازمة فقط لكل مستخدم أو مجموعة مستخدمين، مراقبة الصلاحيات: مراقبة الصلاحيات الممنوحة وتحديثها عند الضرورة، تقييد الوصول: تقييد الوصول إلى المعلومات أو الموارد الحساسة فقط للمستخدمين الذين يحتاجونها، استخدام أدوات الإدارة: استخدام أدوات الإدارة مثل Active Directory أو LDAP لتنظيم الصلاحيات وتحديثها، تفعيل تسجيل الدخول الثنائي للحسابات الحساسة.

التوعية والتدريب على حماية البيانات:

إن أقوى الأنظمة الأمنية يمكن أن تفشل إذا وقع المستخدمون ضحية لهجمات الهندسة الاجتماعية لذا يجب : عقد دورات تدريبية للموظفين حول كيفية اكتشاف رسائل التصيد، نشر ثقافة الأمن السيبراني بين المستخدمين سواء الأفراد أوالشركات، متابعة آخر المستجدات الأمنية من مصادر موثوقة مثل CISA وKaspersky.

التقنيات المستقبلية في حماية البيانات :

مع تطور التهديدات، تستمر تقنيات الأمان في التطور أيضًا، ومنها: الذكاء الاصطناعي والتعلم الآلي : يساعد الذكاء الاصطناعي في التنبؤ بالهجمات والتعرف على الأنماط المشبوهة في البيانات، كما يُستخدم في تحسين استجابة الأنظمة الأمنية للحوادث، تقنية البلوكتشين : تعد البلوكتشين من التقنيات التي تعزز من حماية البيانات والاتصالات، حيث تقوم بتأمين البيانات عبر سلسلة لا مركزية، مما يجعل من الصعب اختراقها أو التلاعب بها.

النصائح الختامية:

مع تزايد التهديدات، أصبح من الضروري تطبيق استراتيجيات قوية لحماية البيانات، من خلال الجمع بين كلمات مرور قوية، والتشفير، والتحديثات الأمنية، وتجنب التصيد الاحتيالي، وبالتالي يمكن تقليل المخاطر بشكل كبير، إن أمن المعلومات وحماية البيانات مسؤولية مشتركة، وكل شخص لديه دور في الحفاظ على سلامة بياناته وبياناته من حوله.

قائمة المراجع :

1 - kaspersky (me.kaspersky.com)
https://me.kaspersky.com/resource-center/preemptive-safety/how-to-protect-personal-online-privacy

2 - microsoft (www.microsoft.com)
https://www.microsoft.com/ar/security/business/security-101/what-is-data-protection

3 - fortinet (www.fortinet.com)
https://www.fortinet.com/resources/cyberglossary/data-security

4 - fproofpoint (www.proofpoint.com)
https://www.proofpoint.com/us/threat-reference/data-protection