البرمجيات الخبيثة والتهديدات السيبرانية:

يستعرض هذا الدليل أنواع البرمجيات الخبيثة الشائعة، من برامج التجسس إلى الفيروسات، ويسلط الضوء على مفهوم القرصنة والتخريب، بالإضافة إلى استعراض لأشهر برامج الفدية. كما يناقش الدليل التهديدات المستمرة وكيفية تأثيرها على المؤسسات، مقدماً رؤى حول الأمن السيبراني لمساعدة الأفراد والمؤسسات على فهم هذه المخاطر وحماية أنظمتهم وبياناتهم.

أنواع البرمجيات الخبيثة الشائعة

برامج التجسس (Spyware)

تتسلل هذه البرامج لجمع معلومات عن عادات تصفحك، وحتى بياناتك الشخصية دون علمك. بعضها قد يتضمن 'مسجلات النقرات' التي تسجل كل ما تكتبه، بما في ذلك كلمات المرور، مما يجعلها أداة خطيرة لسرقة الهوية.

البرامج الدعائية (Adware)

هدفها الأساسي عرض إعلانات منبثقة مزعجة بشكل مستمر. في كثير من الأحيان، تجمع هذه البرامج بيانات عن اهتماماتك لتوجيه إعلانات أكثر استهدافاً، مما ينتهك خصوصيتك وقد يبطئ أداء جهازك.

برامج الفدية (Ransomware)

تعمل على تشفير ملفاتك ومنعك من الوصول إليها، ثم تطلب فدية مالية، غالباً بالعملات الرقمية، مقابل استعادتها. تنتشر عادةً عبر مرفقات البريد الإلكتروني الخبيثة أو الروابط المشبوهة.

الفيروسات (Viruses)

تنتشر بسرعة عبر الشبكات والبريد الإلكتروني، وتتخذ أشكالاً متعددة: **الفيروسات المتنقلة** التي تنتشر بين الأجهزة، و**فيروس الجذر (Rootkit)** الذي يمنح المتسللين سيطرة تامة على جهازك عن بعد، و**حصان طروادة** الذي يتخفى كبرنامج شرعي ليخدعك وتنزله.

تجنب المواقع الإلكترونية غير الموثوقة التي تحاول دفعك لتنزيل برمجيات خبيثة أو سرقة بياناتك الحساسة. كن دائماً حذراً وتأكد من مصدر أي برنامج قبل تنزيله.

مفاهيم أساسية في الأمن السيبراني

القرصنة (Hacking) والتخريب (Sabotage)

- **القرصنة:** محاولة اختراق الأنظمة لعدة أسباب، منها التسلية، سرقة البيانات، أهداف تجارية، أو حتى التجسس السياسي.
- **التخريب:** لا يقتصر على سرقة البيانات، بل يشمل تعطيل الأنظمة لأغراض مثل الانتقام أو الابتزاز أو الإرهاب الإلكتروني، وقد تنفذه حكومات لاستهداف أنظمة استراتيجية.

أمثلة على برامج الفدية الشهيرة

- **CryptoLocker (2013-2014):** أصاب ربع مليون جهاز وطلب فدية بالبيتكوين.
- **WannaCry (2017):** استغل ثغرة في نظام Windows، وأصاب 70 ألف جهاز في هيئة الخدمات الصحية الوطنية البريطانية، ويُعتقد أن مصدره كوريا الشمالية.

تأثير التهديدات السيبرانية على المؤسسات

1

الخسارة التشغيلية

تتسبب الأعطال في الأنظمة بتوقف الخدمات أو تراجع الأداء بشكل كبير، مما يشلّ العمل تماماً في حال هجمات الفدية أو الفيروسات، وتزداد حدتها في حال الكوارث الطبيعية.

2

الخسارة المالية

تحدث عندما تعجز المؤسسة عن تنفيذ عملياتها التشغيلية، وتشمل تكاليف توظيف خبراء الأمن، استبدال الأجهزة، دفع تعويضات للعملاء، وحتى الغرامات القانونية نتيجة لتسرب البيانات الشخصية.

3

خسارة السمعة

المؤسسات التي تتعرض للاختراق تفقد ثقة عملائها، مما يؤثر على إيراداتها المستقبلية ويجعل العملاء يترددون في التعامل معها. كما يمكن أن يؤثر ذلك على جذب المواهب، حيث قد يتردد الموظفون المحتملون في العمل بها.

4

خسارة الملكية الفكرية

تشمل هذه الخسارة سرقة الأسرار التجارية، الأسعار، وتصاميم المنتجات. تحدث هذه السرقات في هجمات تهدف إلى كسب ميزة تنافسية غير مشروعة، مما يؤدي إلى تداعيات اقتصادية خطيرة على المؤسسات.

مستويات التأثير

1

مباشرة

مثل سرقة الأموال مباشرة من حساب الشركة.

2

غير مباشرة

مثل توقف الإنتاج أو الخدمة بسبب تعطل الأنظمة.

تطور تهديدات الأمن السيبراني

تتطور التهديدات السيبرانية باستمرار، مما يفرض على المؤسسات تحديث نظم الحماية بشكل دوري ومواكبة أحدث الاستراتيجيات لمواجهة التحديات الجديدة وضمان استمرارية الأعمال.

عمل الطالبة رحاب سعد ابوتايه

هذا العمل المتميز للطالبة رحاب سعد ابوتايه يتناول موضوع البرمجيات الخبيثة والتهديدات السيبرانية وتأثيرها على المؤسسات. يشرح العمل بالتفصيل كيفية انتشار هذه التهديدات وأساليب الحماية منها. كما يقدم حلول وتوصيات عملية لمواجهة هذه المخاطر السيبرانية.