الهجوم الإلكتروني

ما المقصود به

على عكس التهديدات الجسدية التي تتطلب اتخاذ إجراء فوري، غالبًا ما يكون من الصعب تحديد التهديدات والهجمات السيبرانية أو فهمها. يشمل الأمن الإلكتروني منع الحوادث السيبرانية واكتشافها والاستجابة لها. تعتمد كل المؤسسات الحديثة تقريبًا - بما في ذلك الحكومات والمستشفيات والشركات والبنوك والمرافق - على أنظمة الكمبيوتر من أجل إدارة عملياتها وبياناتها، ومن ثمَّ فهي عرضة للهجمات السيبرانية.

قد يشمل ما يسمى بـ "الأجزاء المعرضة للهجوم" والتي قد تكون عرضة لعناصر سيئة أجهزة الكمبيوتر والأجهزة اللوحية والهواتف والعديد من الأجهزة والأدوات الأخرى المدعومة بخدمات الويب فيما يسمى بـ "إنترنت الأشياء". تتضمن مخاطر الهجمات السيبرانية قيام المتسللون بمسح أنظمة كاملة أو الاحتفاظ ببيانات أو أنظمة تشغيل للحصول على فدية أو سرقة معلومات سرية أو شخصية أو اختراق أنظمة وتبديل الملفات أو استخدام جهاز كمبيوتر أو جهاز آخر للوصول إلى قوائم جهات الاتصال ومهاجمة الآخرين أو نقل البرامج الضارة إلى أجهزتهم.

ما يجب القيام به

قبل حالة الطوارئ (الاستعداد/التخفيف)

- ❑ احرص على تشغيل جدار الحماية وتحديثه باستمرار.
- ❑ قم بتثبيت برنامج حماية من الفيروسات/برنامج حماية من برامج التجسس أو تحديثهما.
- ❑ استخدم كلمات مرور قوية وفريدة وغيِّرها بانتظام.
- ❑ ابحث عن جميع تحديثات نظام التشغيل والبرامج الثابتة والبرامج وبرنامج الحماية من الفيروسات وثبتها على الفور.
- ❑ انتبه إلى ما تقوم بتنزيله. لا تنقر مطلقًا فوق مرفق أو رابط أو ماكرو في بريد إلكتروني أو نص غير مطلوب.
- ❑ قم بإيقاف تشغيل جهاز الكمبيوتر الخاص بك عندما لا تكون تستخدمه.
- ❑ تحقق دائمًا من مصدر رسائل البريد الإلكتروني، وإذا ساورتك شكوك بشأنها، فاحذفها.
- ❑ انتبه إلى رسائل البريد الإلكتروني التي تتلقاها من جهات اتصال معروفة ولكن يبدو أنها "مريبة" - الأخطاء الإملائية والصياغة الغريبة للجمل أو الاستخدام الغريب للكلمات والعبارات العامة وعناوين URL لرابط غريب - حيث ستقوم العديد من حملات الاختراق بتقليد رسائل البريد الإلكتروني المعروفة.
- ❑ التقط لقطة شاشة للمحتوى المريب قبل حذفه، وذلك لأغراض التحليلات.
- ❑ انسخ جميع بياناتك احتياطيًا على محرك أقراص ثابتة خارجي أو على Cloud بانتظام، وقم بتمكين ميزة "Time Machine" (آلة الزمن) إذا كنت تستخدم جهاز Mac.

أثناء حالة الطوارئ (الاستجابة)

- ❑ افصل الجهاز المصاب عن شبكتك.
- ❑ إذا كنت في مكان العمل، فأبلغ موظفي تكنولوجيا المعلومات لديك عن أي هجمات مشتبه فيها أو مؤكدة على أجهزتك، وقدِّم لقطة شاشة.
- ❑ إذا تسبب الحادث في فقدان معلومات مالية أو شخصية أو طبية، فاملأ تقريرًا وقدِّمه للشرطة.

بعد حالة الطوارئ (التعافي)

- ❑ أعلِم أي شخص قد يتأثر سلبيًا، بما في ذلك الحسابات الائتمانية والحسابات البنكية والعملاء ورب العمل والعائلة والأصدقاء. غيِّر حساباتك وجميع كلمات المرور الخاصة بك.
- ❑ أجرِ الفحوصات الملائمة وشغِّل الأدوات المساعدة المناسبة لإزالة أي إصابات.
- ❑ راقب التقرير الائتماني والبيانات البنكية والاستثمارات وبيانات بطاقة الائتمان.
- ❑ تأكد من أن جهازك غير مصاب، وامسح محرك الأقراص الثابتة وأعد تثبيت جميع البرامج إذا ساورتك أي شكوك.

المصطلحات الأساسية

- **الهجوم الإلكتروني** قد يقوم به الأفراد أو مجموعات الربط الشبكي أو الجماعات الإرهابية أو الدول، وقد يسبب مشكلات بالغة (وخطيرة) للحكومات والمؤسسات التجارية والمرافق والجمهور العام.
- **الاختراق** يشير إلى هجوم مباشر ضد أحد الأنظمة "عبر الشبكة"، حيث يتمكن فيه المهاجم (سواء كان شخصًا أم "روبوت" آلي) من الوصول مباشرةً إلى بيانات أو عمليات مُؤمَّنة/مقيدة. يتم غالبًا فتح المسارات التي تسمح بمثل عمليات الاختراق هذه عبر " التصيد الاحتيالي" أو تنزيل الرسائل الخادعة.
- **إنترنت الأشياء (IoT)** يشمل الأجهزة المدعومة بخدمات الويب بما في ذلك الثلاجات وأنظمة الصوت والساعات ومنظمات الحرارة وأنظمة الأمان وماكينات تحضير القهوة وما إلى ذلك.
- **التصيد الاحتيالي** يتضمن نشر رسائل البريد الإلكتروني أو الرسائل النصية على نطاق واسع أملاً في أن ينقر بعض المتلقين فوق أي مكان في الرسالة (على سبيل المثال مرفق أو رابط أو زر "تمكين وحدات ماكرو") مما يُنشط الفيروس أو البرامج الضارة. تسمى حملة التصيد الاحتيالي التي تستهدف - على سبيل المثال - حكومة أو مرفق معين باسم التصيد الاحتيالي الموجّه.
- **الهندسة الاجتماعية** تتضمن استغلال مَواطن الضعف لدى المستخدم، بدلاً من نظامه، للتحايل على إجراءات الأمان الخاصة بتكنولوجيا المعلومات. تشمل الأمثلة التصيد الاحتيالي والرسائل الخادعة عبر البريد الإلكتروني وغيرها من الانتهاكات. وغالبًا ما يكون المستخدمون هم أكثر العناصر التي يسهُل التعدي عليها في بنية أمان تكنولوجيا المعلومات.