الهجمات السيبرانية

الهجوم السيبراني هو أي محاولة للحصول على وصول غير مصرح به إلى جهاز كمبيوتر أو شبكة كمبيوتر بقصد إحداث ضرر ويهدف إلى تعطيل أنظمة الكمبيوتر أو تعطيل الجهاز أو تدميره أو التحكم فيه أو تغيير أو حظر أو حذف أو تلاعب أو سرقة البيانات الموجودة ضمنها.

كل عمل تجاري ، بغض النظر عن حجمه ، هو هدف محتمل للهجوم السيبراني وذلك لأن كل عمل تجاري لديه أصول رئيسية قد يسعى المجرمون إلى استغلالها في بعض الأحيان يكون الهدف المال أو المعلومات المالية أو المعلومات الشخصية للموظفين والعملاء أو حتى البنية التحتية للمشركة.

من خلال التعرف على الدوافع وراء الهجمات الإلكترونية، يمكننا بناء فهم أفضل للمخاطر ومعرفة أفضل السبل لمواجهتها.

في أغلب الأحيان، تحدث الهجمات الإلكترونية لأن المجرمين يريدون:

. التفاصيل المالية للعمل

التفاصيل المالية للعملاء

. البيانات الشخصية الحساسة

. عناوين البريد الإلكتروني للعملاء أو الموظفين وبيانات تسجيل الدخول

. قواعد بيانات العملاء

قوائم العملاء

. البنية التحتية لتكنولوجيا المعلومات

. خدمات تكنولوجيا المعلومات

. الملكية الفكرية (مثل الأسرار التجارية أو تصميمات المنتجات)

غالبا ما تكون الهجمات الإلكترونية ضد الشركات متعمدة ودوافعها تكون لتحقيق مكاسب مالية ومع ذلك قد تشمل الدوافع الأخرى:

فرض وجهة نظر اجتماعية أو سياسية

التجسس

التحدي

أنواع الهجمات السيبرانية

البرامج الضارة Malware

يستخدم مصطلح malware لوصف البرامج الضارة بما في ذلك برامج التجسس وبرامج الفدية والفيروسات والديدان حيث تخترق البرامج الضارة الشبكة من خلال ثغرة أمنية وعادة يحدث ذلك عندما ينقر المستخدم فوق رابط خطير أو مرفق في البريد

الإلكتروني يقوم بعد ذلك بتثبيت برامج محفوفة بالمخاطر و بمجرد دخول البرنامج الضار إلى النظام ، يمكن أن يقوم بما يلي:

يمنع الوصول إلى المكونات الرئيسية (برامج الفدية)

تثبيت البرامج الضارة أو البرامج الضارة الإضافية

يحصل سراً على المعلومات عن طريق نقل البيانات من القرص الصلب (برامج التجسس)

يعطل مكونات معينة ويجعل النظام غير صالح للعمل

التصيد Phishing

التصيد الاحتيالي هو ممارسة اتصالات احتيالية يبدو أنها واردة من مصدر حسن السمعة عبر البريد الإلكتروني عادة و الهدف هو سرقة البيانات الحساسة مثل بطاقة الائتمان ومعلومات تسجيل الدخول أو تثبيت برامج ضارة على جهاز الضحية بعد التصيد الاحتيالي تهديداً إلكترونياً شائعاً بشكل متزايد نظراً لضعف وعي المستخدمين.

الرجل في الوسط Man in the Middle

هجمات الرجل في الوسط (MitM) ، والمعروفة أيضًا باسم هجمات التنصت عندما يدخل المهاجمون أنفسهم في صفقة بين طرفين بمجرد مقاطعة المهاجمين الحركة مرور البيانات يمكنهم تصفية البيانات وسرقتها أو تغييرها.

نقطتان مشتركتان لدخول هجمات MitM

1. في شبكة Wi-Fi الغير الآمنة يمكن للمهاجمين إدخال أنفسهم بين جهاز الزائر والشبكة حيث يقوم الزائر بتمرير جميع المعلومات

من خلال المهاجم دون علمه

. بمجرد اختراق أحد البرامج الضارة للجهاز يمكن للمهاجم تثبيت برنامج المعالجة جميع معلومات الضحية

هجوم قطع الخدمة

يغمر هجوم قطع الخدمة الأنظمة أو الخوادم أو الشبكات بحركة البيانات لاستنفاذ الموارد و حزم مرور المعلومات ونتيجة لذلك يصبح النظام غير قادر على تلبية الطلبات الصحيحة ويمكن للمهاجمين أيضاً استخدام العديد من الأجهزة المخترقة لشن هذا الهجوم و يعرف هذا بهجوم قطع الخدمة الموزع (DdoS).

حقن SQL

يحدث الحقن في لغة (SQL) عندما يقوم المهاجم بإدخال تعليمات برمجية ضارة في خادم يستخدم SQL ويجبر الخادم على الكشف عن معلومات لا يفعلها عادة حيث يمكن للمهاجم تنفيذ حقنة SQL ببساطة عن طريق إرسال تعليمات برمجية ضارة في مربع بحث موقع ويب ضعيف.

استغلال يوم الصفر Zero-day exploit

عند الإعلان عن ثغرة أمنية ولكن قبل تحديث التصحيح أو حل المشكلة يستهدف المهاجمون الثغرة الأمنية التي تم الكشف عنها خلال هذه الفترة الزمنية يتطلب اكتشاف تهديدات الثغرات الأمنية في اليوم الصفري اهتماماً دائماً و بحث مستمر عن الثغرات.

نفق DNS

يستخدم بروتوكول DNS لتوصيل حركة مرور DNS عبر البورت ٥٣ و يرسل HTTP و بروتوكولات أخرى عبر DNS هناك العديد من الأسباب لاستخدام نفق DNS بشكل عام ومع ذلك هناك أيضاً ضرر في استخدام خدمات DNS Tunneling VPN حيث يمكن استخدامها لإخفاء حركة المعلومات الصادرة واخفاء البيانات التي تتم مشاركتها عادةً من خلال اتصال الإنترنت. للاستخدام الضار يتم التلاعب بطلبات DNS لاستخراج البيانات من نظام مخترق إلى البنية التحتية للمهاجم حيث يمكن استخدامه أيضاً لعمليات استرجاع الأوامر والتحكم في البنية التحتية.

الفيروسات والبرامج الضارة

البرامج الضارة Malware

وهي أي برامج تطفلية طورها مبرمجون لسرقة البيانات وإتلاف أو تدمير أجهزة الكمبيوتر وأنظمة الكمبيوتر وأكثر البرامج الضارة الشائعة الفيروسات والديدان وفيروسات أحصنة طروادة وبرامج التجسس والبرامج الإعلانية وبرامج الفدية

الحماية منها :

عادة ما تركز الشركات على الأدوات الوقائية لوقف البرامج الخبيثة و مع ذلك ستشق بعض البرامج الضارة المتقدمة طريقها في النهاية إلى الشبكة فنتيجة لذلك من المهم نشر التقنيات التي تراقب وتكشف باستمرار البرامج الضارة التي تهربت من الدفاعات الأولية و تتطلب الحماية الكافية من البرامج الضارة المتقدمة طبقات متعددة من الضمانات جنباً إلى جنب مع مستوى عالي من الذكاء ومراقبة الشبكة بشكل دائم.

اكتشاف البرامج الضارة :

سوف تخترق البرامج الضارة الشبكة حتماً لذا يجب أن يكون لدينا دفاعات توفر رؤية واضحة واكتشاف الخروقات و لإزالة البرامج الضارة يجب أن تكون قادراً على التعرف عليها بسرعة و هذا يتطلب مسحاً ثابتاً للشبكة وبمجرد تحديد التهديد يجب إزالة البرامج الضارة من الشبكة ولا تكفي منتجات مكافحة الفيروسات الحالية للحماية من التهديدات الإلكترونية المتقدمة

أشهر الأنواع

1- الفيروسات

هي مجموعة فرعية من البرامج الضارة فالفيروس هو برنامج ضار مرفق بمستند أو ملف يدعم وحدات الماكرو لتنفيذ التعليمات البرمجية الخاصة به والانتشار من مكان لآخر بمجرد تنزيله سيظل الفيروس خامداً حتى يتم فتح الملف واستخدامه حيث تم تصميم الفيروسات لتعطيل قدرة النظام على العمل لذلك يمكن أن تتسبب الفيروسات في حدوث مشكلات تشغيلية كبيرة وفقدان كبير في البيانات.

٢- الديدان

هي برامج ضارة تتكاثر بسرعة وتنتشر إلى أي جهاز داخل الشبكة على عكس الفيروسات لا تحتاج الديدان إلى برامج مضيفة لنشرها فهي تصيب جهازاً عبر ملف تم تنزيله أو اتصال شبكة قبل أن يتكاثر ويتشتت بمعدل أسي مثل الفيروسات يمكن للديدان أن تعطل بشدة عمليات الجهاز وتتسبب في فقد البيانات.

٣- حصان طروادة

يتم إخفاء فيروسات أحصنة طروادة فتبدو كبرامج مفيدة ولكن بمجرد قيام المستخدم بتنزيله يمكن الحصان طروادة الوصول إلى البيانات الحساسة ثم تعديل البيانات أو حظرها أو حذفها وهذا يمكن أن يكون ضاراً للغاية بأداء الجهاز على عكس الفيروسات والديدان العادية لم يتم تصميم فيروسات أحصنة طروادة للتكرار الذاتي.

٤- برامج التجسس

هي برامج ضارة يتم تشغيلها سراً على جهاز كمبيوتر وترسل تقارير إلى مستخدم بعيد بدلاً من مجرد تعطيل عمليات الجهاز تستهدف برامج التجسس المعلومات الحساسة ويمكن أن تمنح الوصول عن بعد إلى المحتالين و غالباً ما تستخدم برامج التجسس السرقة المعلومات المالية أو الشخصية وهنالك نوع معين من برامج التجسس

هو برنامج تسجيل ضغطات المفاتيح key logger والذي يسجل ضغطات المفاتيح كلها لكشف كلمات المرور والمعلومات الشخصية.

٥- برامج الإعلانات

هي برامج ضارة تستخدم لجمع البيانات حول استخدام الكمبيوتر الخاص بك وتقديم إعلانات مناسبة لك و على الرغم من أن برامج الإعلانات المتسللة ليست خطيرة دائماً إلا أنه في بعض الحالات يمكن أن تتسبب البرامج الإعلانية في حدوث مشكلات النظامك ويمكن لبرامج الإعلانات المتسللة إعادة توجيه متصفحك إلى مواقع غير آمنة كما يمكن أن تحتوي أيضاً على أحصنة طروادة وبرامج التجسس ويمكن أن تؤدي المستويات الكبيرة من البرامج الإعلانية إلى إبطاء نظامك بشكل ملحوظ نظراً لأن برامج الإعلانات المتسللة ليست كلها ضارة فمن المهم أن يكون لديك حماية تقوم بمسح هذه البرامج باستمرار وبذكاء.

٦- برامج الفدية

برامج الفدية هي برامج ضارة يمكنها الوصول إلى المعلومات الحساسة داخل النظام وتشفير هذه المعلومات بحيث لا يتمكن المستخدم من الوصول إليها ثم تطالب بتعويض مالي مقابل البيانات التي سيتم إصدارها وتعد برامج الفدية عادة جزء من عمليات الاحتيال حيث يتم بالنقر فوق ارتباط معين فيقوم المستخدم بتنزيل برنامج الفدية يواصل المهاجم تشفير معلومات محددة لا يمكن فتحها إلا من خلال مفتاح لدى المهاجم وعندما يتلقى المهاجم دفعات مالية يتم إلغاء قفل البيانات.

7- البرمجيات الخبيثة بل ملف

هي نوع من البرامج الضارة الموجودة في الذاكرة فهي تعمل من ذاكرة كمبيوتر الضحية وليس من الملفات الموجودة على محرك الأقراص نظراً لعدم وجود ملفات لفحصها يكون اكتشافها أصعب من اكتشاف البرامج الضارة التقليدية كما أنه يجعل عمليه مراقبتها أكثر صعوبة لأن البرامج الضارة تختفي عند إعادة تشغيل جهاز الكمبيوتر الضحية.

طرق الحماية من البرامج الخبيثة

• تحديث الدفاعات الأولية

الالتزام بالسياسات وأفضل الممارسات الخاصة بأمان التطبيقات والنظام والأجهزة وإنشاء كلمات مرور فريدة يبلغ طولها ١٦ حرفاً على الأقل واستخدام مدير كلمات المرور وتحديث الأنظمة بسرعة حيث تصبح الثغرات الأمنية معروفة جيدا بمجرد إصدار التحديثات

• نسخ احتياطي للبيانات واختبار إجراءات الاستعادة

عمليات النسخ الاحتياطي ضرورية للحماية من فقدان البيانات في عالم من الفيروسات المتنقلة لبرمجيات الفدية سريعة الحركة والقائمة على الشبكة والهجمات الإلكترونية المدمرة يجب عليك تمكين حل حماية البيانات.

• الحماية من البرامج الضارة

سيساعدك اتباع نهج متعدد المستويات مع أدوات مراقبة البرمجيات وجدران الحماية ونظام منع التطفل على نشر الأمان.

• توعية المستخدمين بمصادر التهديد

قم بتدريب المستخدمين على ما يجب أن يثقوا به وعلمهم ألا يقعوا في فخ الاحتيال أو غيره من المخططات واطلب منهم تثبيت المصادقة بخطوتين كخط دفاع أول.

• تقسيم الشبكة إلى شبكات فرعية

قلل من مخاطر التعرض لتفشي المرض عن طريق عزل الشبكة باستخدام تقسيم الشبكة.

• رفع مستوى أمان البريد الإلكتروني

تنتشر معظم الإصابات ببرامج الفدية من خلال مرفق بريد إلكتروني أو تنزيلات ضارة فيجب حجب مواقع الويب الضارة ورسائل البريد الإلكتروني والمرفقات بجدية من خلال سياسة أمان متعددة الطبقات وبرنامج مشاركة الملفات المعتمدة من الشركة.

• استخدام التحليلات الأمنية

مراقبة حركة مرور الشبكة عن طريق إجراء تحليلات أعمق وأكثر تقدماً لمعرفة كل ما يحدث عبرها و الاستفادة من معلومات التهديدات في الوقت الفعلي وفهم معلومات الأمان وتهديدات الأمن السيبراني الجديدة بشكل أفضل.

• إنشاء مجموعة من التعليمات لموظفي تكنولوجيا المعلومات

مراجعة وممارسة إجراءات الاستجابة الأمنية من خلال تطوير خطة الاستجابة للحوادث.

• ممارسة الوقاية والعلاج معاً

تعرف على حلول الأمان الإضافية وفكر فيها والتي ستعمل على حماية الشبكة بشكل أكبر بالإضافة إلى توسيع نطاق الرؤية و إجراء فحص أمني للخدمات المصغرة والخدمات السحابية وأنظمة إدارة التطبيقات.