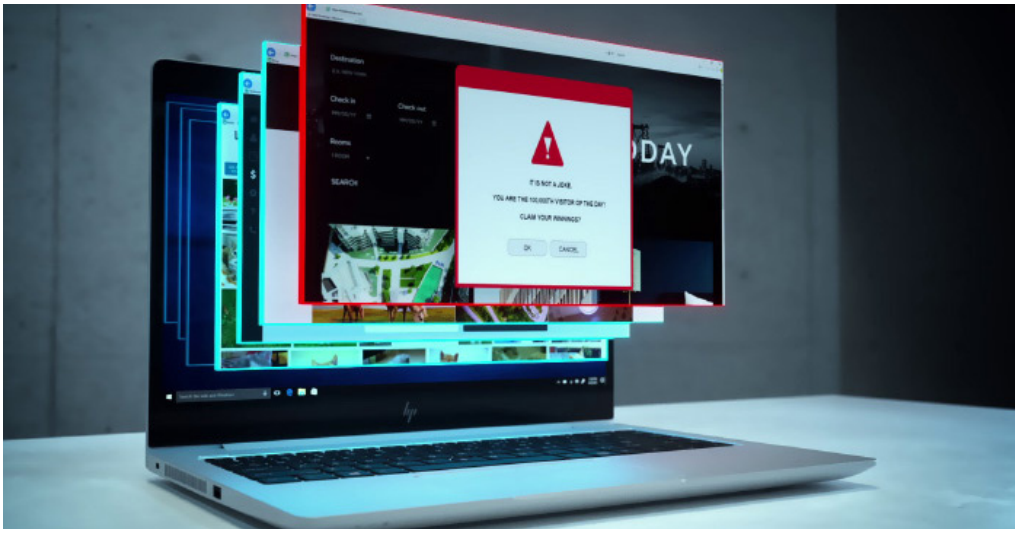
التصيد الاحتيالي لم يعُد يستهدف رسائل البريد الإلكتروني فحسب

بقلم: سكينة الإدريسي

Learn more



متصفح الويب هو بوابة مفتوحة على عالم من المعلومات... والتهديدات أيضًا. ولهذا، ما الذي يمكنك فعله كي تحمي شركتك؟

متصفحات الويب أمامها الكثير لتواجهه. في استبيان حديث مع 400 من مديري أقسام تكنولوجيا المعلومات، صرّحَ 68% منهم أنّ الجرائم الإلكترونية صارت الآن أكثر تعقيدًا, وأنّ فرق عملهم تكافح للتمييز بين المواقع الآمنة وغير الآمنة[1]. ولهذا السبب ليس من المستغرب أن نعرف أنّ 70% من متخصصي تكنولوجيا المعلومات يواجهون هجمات تصيد احتيالي أسبوعيًا – وليس عبر البريد الإلكتروني فقط[2]. فالقراصنة المحترفون يستخدمون الآن شبكات التواصل الاجتماعي، والإعلانات، والتهجئة الخاطئة لأسماء المواقع الإلكترونية الشهيرة كي يخدعوا الموظفين ويجعلوهم يُفصحون عن معلوماتهم الشخصية الحساسة. تزداد صعوبة التعرف على عمليات التصيد الاحتيالي يومًا بعد يوم، والشركات تعاني من أجل حماية موظفيها من هذه الهجمات.

فعلى الرغم من زيادة الوعي والاستثمار في برامج الحماية وتدريب الموظفين، إلّا أنّ هناك قفزة بلغت نسبتها 232% في عدد الهجمات الإلكترونية على أجهزة الكمبيوتر المحمولة وأجهزة الكمبيوتر المكتبية على مدار السنوات الست الماضية[3]. فالقراصنة الإلكترونيون ما زالوا يُحرزون تقدمًا؛ لأنّ الأرقام تشير إلى ذلك. و من هنا، تبذل الشركات جهدًا مهولاً كي تحمي بياناتها، ثم تأتي نقرة واحدة من أحد الموظفين على رابط ضار فيُهدَم كل هذا الجهد وتنهار شركتك أمام الهجمة الإلكترونية.

الهجمات الإلكترونية عبر وسائل التواصل الاجتماعي تحتل الجزء الأكبر من هذه المشكلة. فشبكات التواصل الاجتماعي، مثل فيسبوك وتويتر، تُعد بيئة خصبة للمجرمين الإلكترونيين. فهي ليست مصممة للتفاعل والتواصل فقط، بل هي أيضًا سهلة الاستخدام ويمكن الوصول إليها بأقل التكاليف. من السهل جدًا إنشاء حسابات مزيفة وبدء نشر محتوى ضار، يتنوّع ما بين الروابط الضارة وجمع البيانات، وحتى الصفحات الرئيسية للمواقع المشتملة على نوافذ منبثقة غير موثوق بها.

غالبية هذه الأنشطة الإلكترونية تقوم على تقنيات التصيد الاحتيالي، والتي اعتدنا سابقًا أن تكون مع رسائل البريد الإلكتروني فقط. تفتح وسائل التواصل الاجتماعي قنوات تواصل بين الأشخاص، ولا يتطلب الأمر جهدًا كبيرًا للتأسيس لشخصية ما ذات مصداقية ومتابعتها بواسطة مستخدمين حقيقيين في تلك الشبكات.

كانت شركة "فيفو" المتخصصة في بث الفيديو على الإنترنت هي آخر ضحايا الخرق الهائل للبيانات. فلقد تم استهداف أحد موظفيها عن طريق حيلة تصيّد على شبكة التواصل المهني "لينكد إن"، وهو ما أدّى إلى تسريب حوالي 3.12 تيرابايت من الملفات الداخلية للشركة على الإنترنت. والتي اشتملت على فيديوهات، ومستندات مكتبية، ومواد إعلانية، ومحتوى لوسائل تواصل اجتماعي كان مجهزًا للاستخدام لاحقًا، ومعلومات عن المطربين المُوقّعين مع شركات التسجيل المُشارِكة[4].

ولقد أعلن فريق القرصنة OurMine (آورماين) مسؤوليته عن تلك الهجمة، وذلك بعد مشادة حدثت عبر البريد الإلكتروني مع أحد الموظفين في شركة فيفو. وهذا يُرينا مدى خطورة التصيد الاحتيالي المُوجّه، وهو هجمة موجهة يحاول القرصان من خلالها سرقة بيانات معيّنة من شخص مستهدف معين. عادةً ما يتخفّى القرصان خلف ستار الصداقة أو المصادر الموثوق فيها (مثلا، المصرف الذي تتعامل معه) كي يخدع الشخص المستهدف ليُفشي المعلومات الخاصة به؛ وهذه الحيلة كانت السبب وراء 91% من الهجمات.

بالنسبة إلى غالبية الشركات التي تقع فريسة لمثل هذه الهجمات، مثل شركة فيفو، فإنّ العواقب قد تكون كارثية وتدوم لفترة طويلة. فهي قد لا تتسبب في ضياع مجهودات الموظفين وبيانات العملاء فحسب، ولكن أيضًا في ضياع العملاء أنفسهم. وذلك لأنّ ثقة عملائك في شركتك قد تهتز بصورة كبيرة جرّاء خرق أمني مثل هذا – فبالنسبة لهم لم تعُد تستحق الثقة الموضوعة فيك للاحتفاظ بمعلوماتهم. وعلى الرغم من إمكانية معالجة ذلك في أغلب الأحيان، إلّا أنّ آثاره تكون دائمة.

في الربع الأخير من عام 2017، ارتفع معدل هجمات التصيد الاحتيالي عبر وسائل التواصل الاجتماعي إلى 500%، والتي كانت غالبيتها عبارة عن حسابات مزيفة تدّعي من خلال منشوراتها أنّها حسابات خدمة عملاء لعلامات تجارية شهيرة[5]. وهذا التطور صار يُسمّى بالتصيد الاحتيالي بأسلوب الصنارة، وذلك لأنّ القرصان يقوم بإعداد طُعم وانتظار التقاط مستخدمي وسائل التواصل الاجتماعي له. ولاستخدامه نفس العلامة التجارية واسم حساب يظهر بمظهر الحساب الأصلي، يقع ملايين من الأشخاص الذين يعتمدون على وسائل التواصل الاجتماعي القائمة على الويب فريسة لمثل هذه الهجمات المُقنعة. وبعد ذلك، بمجرد أن يتفاعل المستخدم، يقوم الحساب المزيّف بإرسال موقع احتيال ويطلب من المستخدم تسجيل الدخول فيه، وهو ما يُتيح للشخص المحتال أن يصل إلى صيده الكبير، وهو الحصول على البيانات الخاصة.

من أسهل الطرق لمنع موظفيك من الوقوع فريسة للاحتيال عبر وسائل التواصل الاجتماعي هي تحفيزهم على تغيير سلوكياتهم أثناء العمل. وهو ما ينبغي أن يساعد موظفيك على تجنُّب هذا النوع من الأخطاء البسيطة التي قد تؤدي إلى وقوع عواقب وخيمة على شركتك:

1. اقتصار التفاعل على المستخدمين الذين يمكنك الثقة فيهم
2. عدم الضغط على روابط قادمة من مصدر غير معتمد
3. عدم تحميل أي ملفات مرفقة عبر وسائل التواصل الاجتماعي
4. تمكين المصادقة بعاملَيْ أمان على جميع أجهزتك وحساباتك على وسائل التواصل الاجتماعي – فهذا سيُصعّب مهمة اختراقها
5. إخضاع الموظفين من ذوي امتيازات الوصول الخاص أو القائمين على حسابات التواصل الاجتماعي لتدريبات إضافية

وهناك جانب أساسي آخر من خطتك للأمان ينبغي عليك الالتفات إليه، وهو التقنيات التي تستخدمها للحفاظ على مرونتك في العالم الإلكتروني. فعائلة أجهزة HP Elite، على سبيل المثال، عبارة عن أجهزة كمبيوتر محمولة وأجهزة كمبيوتر مكتبية تم تصميمها على أساس الأمان من جميع الأوجه.

ومن بين هذه الميزات تقنية HP Sure Click، والتي تكون متاحة على أجهزة HP Elite مختارة، حيث تتعامل مع أمان التصفح بشكلٍ مختلف. فبدلاً من تمييز المواقع الخطيرة كي يتجنّبها المستخدمون فحسب، فهي تقوم أيضًا بمنع البرامج الضارة، وبرامج طلب الفدية مقابل المعلومات المسروقة، والفيروسات من إلحاق الضرر بعلامات تبويب المتصفح الأخرى والنظام بأكمله. فعند بدء المستخدم لجلسة عمل على المتصفح، فإنّ كل موقع يزوره يقوم بتشغيل تقنية HP Sure Click. على سبيل المثال، في كل مرة يقوم المستخدم بزيارة موقع إلكتروني، تقوم تقنية HP Sure Click بإنشاء جلسة عمل للتصفح معزولة وقائمة على المكونات الداخلية للجهاز، بحيث تعيق قدرة الموقع الإلكتروني على إلحاق الضرر بعلامات التبويب الأخرى أو النظام نفسه.

عندما يتعلق الأمر بتغيير الشركات لاستراتيجيتها المتعلقة بالأمان وامتلاك مثل تلك الأجهزة المتطورة، مثل سلسلة HP EliteBook 800 Series, المزوّدة اختياريًا بمعالجات Intel® Core™ من الجيل الثامن، فستشعر كأنّ الكلام رائع، ولكن التنفيذ صعب. وهنا يأتي دور حلٌ مثل. استخدام الأجهزة كخدمات من HP (DaaS)، وهو نموذج استهلاك لأجهزة الكمبيوتر حديث يُبسّط كيفية تزويد المؤسسات التجارية لموظفيها بالأجهزة والملحقات المناسبة، وإدارة أساطيل الأجهزة متعددة أنظمة التشغيل، والحصول على خدمات إضافية لإدارة دورة عمر الأجهزة. تقدم خدمة HP DaaS خططًا بسيطة مرنة، بسعر مُوحّد لكل جهاز، كي يظل كل شيء يعمل بسلاسة وكفاءة.

وفي نهاية المطاف، فإنّ حصولك على فريق جيد التدريب وأجهزة تم تطويرها لأغراض الأمان سيساعدك على مكافحة الجرائم الإلكترونية عبر وسائل التواصل الاجتماعي، والتي صارت من أكبر المخاطر الموجودة في الفضاء الإلكتروني. هذه المخاطر ستصبح أكبر وأكثر شراسة، ولذا، فقد حان الآن الوقت لترقية دفاعاتك.

التصيد الاحتيالي لم يعُد يستهدف رسائل البريد الإلكتروني فحسب

استكشف مزايا حلول الأمان المُقدَّمة من HP لشركتك.

المصادر:

1. https://www.bromium.com/company/press-releases/majority-cios-believe-they-are-losing-battle-against-cybercrime.html
2. https://www.engineering.com/DesignerEdge/DesignerEdgeArticles/ArticleID/8355/HP-Nearly-70-of-IT-Professionals-Experience-Weekly-Phishing-Attacks.aspx
3. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
4. https://www.zerofox.com/blog/vevo-hacked-via-linkedin-phishing-campaign/
5. https://www.infosecurity-magazine.com/news/social-media-phishing-attacks-soar/

4AA7-3218ARE, رايا 2018