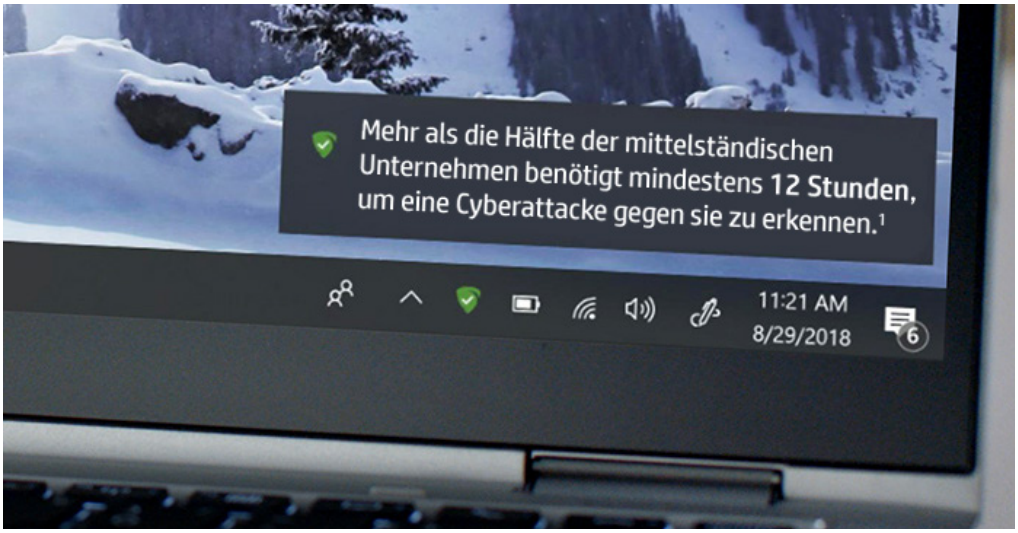
Phishing beschränkt sich nicht nur auf E-Mails

Erfahren Sie mehr



Ein Internetbrowser ist das Tor zu einer Welt voller Informationen ... und Gefahren. Was können Sie tun, um Ihr Unternehmen zu schützen?

Internetbrowser können tückisch sein. In einer aktuellen Studie mit 400 CIOs sagten 68 %, dass Cyberkriminelle inzwischen so raffiniert seien, dass ihre Mitarbeiter Schwierigkeiten hätten, zwischen sicheren und unsicheren Websites zu unterscheiden.[2] So ist es nicht verwunderlich, dass 70 % der IT-Fachkräfte wöchentlich mit Phishingangriffen zu tun haben – und das nicht nur in Verbindung mit E-Mails[3]. Raffinierte Hacker verwenden nun Social Media, Werbeanzeigen und gängige Falschschreibungen von Websites, um Mitarbeitern sensible personenbezogene Daten zu entlocken. Da es zunehmend schwierig wird, Phishing-Betrug zu erkennen, haben Unternehmen große Mühe, ihre Mitarbeiter vor diesen Angriffen zu schützen.

Trotz der vermehrten Sensibilisierung und Investition in Sicherheitssoftware und Mitarbeiterschulungen ist die Anzahl der Cyberattacken auf Notebooks und Desktops um mehr als 100 % gestiegen.[4] Cyberkriminelle gelangen immer noch auf Ihren PC, die Zahlen sprechen für sich. Es ist sehr mühselig, Daten zu sichern. Ein einziger Mitarbeiter reicht aus, um Ihr Unternehmen über einen schädlichen Link zu Fall zu bringen.

Cyberangriffe über Social Media sind ein großer Teil dieses Problems. Plattformen wie Facebook und Twitter sind ein erfolgsversprechendes Jagdrevier für Cyberkriminelle. Sie sind nicht nur prädestiniert für Engagement und Kommunikation, sondern auch einfach in der Anwendung und günstig im Unterhalt. Es ist unglaublich einfach, betrügerische Accounts einzurichten und schadhaften Inhalt zu posten. Das können Links, Formulare bis hin zu Landing-Pages mit außergewöhnlichen Pop-ups sein.

Ein Großteil dieser Online-Aktivitäten basiert auf Phishingmethoden, die früher nur über E-Mails stattfanden. Social Media dient der Vernetzung von Personen und es bedarf nicht viel, um eine glaubwürdige Persona zu erfinden und echten Nutzern auf den Plattformen zu folgen.

Für die meisten Unternehmen, die Opfer eines Phishingangriffs sind, können die Konsequenzen schädlich und dauerhaft sein. Diese Angriffe können nicht nur zum Verlust der Mitarbeiterproduktivität und Kundendaten führen, sondern auch zum Verlust der Kunden selbst. Das Vertrauen Ihrer Kunden in Ihr Unternehmen kann durch eine Sicherheitsverletzung enorm beeinträchtigt werden. Ab diesem Moment haben sie nicht mehr das Gefühl, ihre Daten seien bei Ihnen in guten Händen. Auch wenn sich die Situation retten lässt, die Auswirkungen bleiben häufig dauerhaft.

Phishing beschränkt sich nicht mehr nur auf E-Mails

Im 4. Quartal 2017 stiegen Phishingangriffe über Social Media auf 500 %, wobei der Trend zu Fake-Accounts geht, die sich als Kundensupport für namhafte Marken ausgeben[5]. Diese Entwicklung nennt man Angler-Phishing, da Hacker einen Köder auswerfen und warten, bis Social-Media-Nutzer anbeißen. Mit demselben Markennamen und einem authentisch wirkenden Account-Namen fallen Millionen Nutzer häufig auf diese überzeugenden Angriffe herein. Sobald ein Nutzer eine Nachricht schreibt oder anderweitig aktiv wird, sendet ihm der Fake-Account einen Link zu einer Phishing-Seite und bittet darum, sich anzumelden. Dadurch erreicht der Phisher sein eigentliches Ziel, private Daten auszuspionieren.

Eine der Möglichkeiten, Ihre Mitarbeiter davor zu bewahren, Phishing-Opfer über Social Media zu werden, ist eine Verhaltensänderung am Arbeitsplatz. So unterstützen Sie Ihre Mitarbeiter, einfache Fehler zu vermeiden, die für Ihr Unternehmen so verheerende Konsequenzen haben können:

1. Einschränkung der Interaktionen auf vertrauenswürdige Nutzer
2. Keine Klicks auf Links aus nicht verifizierter Quelle
3. Keine Downloads von Datenanhängen aus Social Media
4. Aktivierung der Zwei-Faktoren-Authentifizierung bei allen Social Media und Geräten, um das Hacking zu erschweren
5. Zusätzliche Schulungen für Mitarbeiter mit umfangreichen Zugriffsrechten und Kundenkontakt über Social Media

Ein weiterer wichtiger Aspekt, den Sie bei Ihrem Sicherheitsplan beachten müssen, ist die eingesetzte Technologie zum Schutz vor Cyberangriffen. Die HP Elite Familie ist z. B. eine Reihe von Notebooks, Desktop-PCs und Workstations, die von Grund auf unter Sicherheitsaspekten entwickelt wurden.

Eine der Sicherheitsfunktionen ist HP Sure Click[6]. Sie steht auf ausgewählten HP Elite Notebooks und Workstations zur Verfügung und verfolgt einen neuen Ansatz für sicheres Browsen. Anstatt lediglich zu kennzeichnen, welche Risiko-Seiten gemieden werden sollen, verhindert die Sicherheitsfunktion, dass Malware, Ransomware und Viren andere Browser-Tabs und das gesamte System befallen. Startet ein Nutzer eine Internetsitzung, wird bei jeder besuchten Website HP Sure Click aktiviert. Dabei erzeugt HP Sure Click eine hardwarebasierte isolierte Internetsitzung. Auf diese Weise wird verhindert, dass eine Website andere Tabs oder das System selbst infiziert.

HP Sure Click schützt die Nutzer sogar vor infizierter Malware, die in Office- und PDF-Dateien verborgen wurde. Wenn Ihre Mitarbeiter beispielsweise eine infizierte PDF-Datei per E-Mail erhalten haben, können sie diese ohne Risiko öffnen, da sie von HP Sure Click in einem hardwarebasierten Container isoliert wird, was eine Ausbreitung der Infektion unterbindet. Ist diese Sicherheitslösung in Ihre geschäftlichen PCs integriert, sind Onlinebedrohungen weniger besorgniserregend.

Doch oft können Unternehmen ihre Sicherheitsstrategie nicht so einfach ändern und zukunftweisende Geräte wie z. B. das HP EliteBook x360 mit optionalem Intel® Core™ i7-Prozessor der 8. Generation einsetzen. Genau hier kommen Lösungen wie HP Device as a Service (DaaS)[7] ins Spiel. Hierbei handelt es sich um ein modernes PC-Verbrauchsmodell, das es Unternehmen erleichtert, ihre Mitarbeiter mit der richtigen Hardware und Zubehör auszustatten, Geräte mit verschiedenen Betriebssystemen zu verwalten und zusätzliche Lebenszyklusservices zu erhalten. HP DaaS überzeugt mit einfachen, aber dennoch flexiblen Tarifen mit einem festen Preis pro Gerät, sodass ein reibungsloser und effizienter Betrieb garantiert ist.

Mit einem gut geschulten Team und sicherheitsoptimierten Geräten können Sie der Cyberkriminalität über Social Media, einer der größten Cyberbedrohungen, den Kampf ansagen. Die Zukunft bringt immer größere Gefahren mit sich, deshalb ist es jetzt an der Zeit, Ihre Verteidigung zu verstärken.

Entdecken Sie die Vorteile der HP-Sicherheitslösungen für Ihr Unternehmen.

Quellen:

1. Osterman Research, gesponsert von Malwarebytes „Second Annual State of Ransomware Report: US Survey Results“, Juli 2017
2. https://www.bromium.com/company/press-releases/majority-cios-believe-they-are-losing-battle-against-cybercrime.html
3. http://www8.hp.com/us/en/hp-news/press-release.html?id=1763561#.WLTLYjsrI2y
4. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
5. https://www.infosecurity-magazine.com/news/social-media-phishing-attacks-soar/

6. HP Sure Click ist auf den meisten HP-PCs verfügbar und unterstützt Microsoft® Internet Explorer, Google Chrome und Chromium™. Zu den unterstützten Anhängen gehören Microsoft Office (Word, Excel, PowerPoint) und PDF-Dateien im Schreibschutz-Modus, wenn Microsoft Office oder Adobe Acrobat installiert sind.

7. HP DaaS-Pakete und/oder enthaltene Komponenten können je nach Region oder nach autorisierten HP DaaS-Service-Partner variieren. Wenden Sie sich für genauere Details in Ihrer Region an Ihren HP-Vertreter oder den autorisierten DaaS-Partner vor Ort. HP Services unterliegen den jeweils geltenden allgemeinen Geschäftsbedingungen von HP, die dem Kunden zum Zeitpunkt des Kaufs bereitgestellt oder genannt werden. Möglicherweise haben Kunden nach lokal geltendem Recht zusätzliche Rechte. Diese Rechte sind in keinster Weise von den Geschäftsbedingungen von HP oder der eingeschränkten Gewährleistung Ihres HP-Produkts betroffen.

4AA7-317DEDE, April 2019