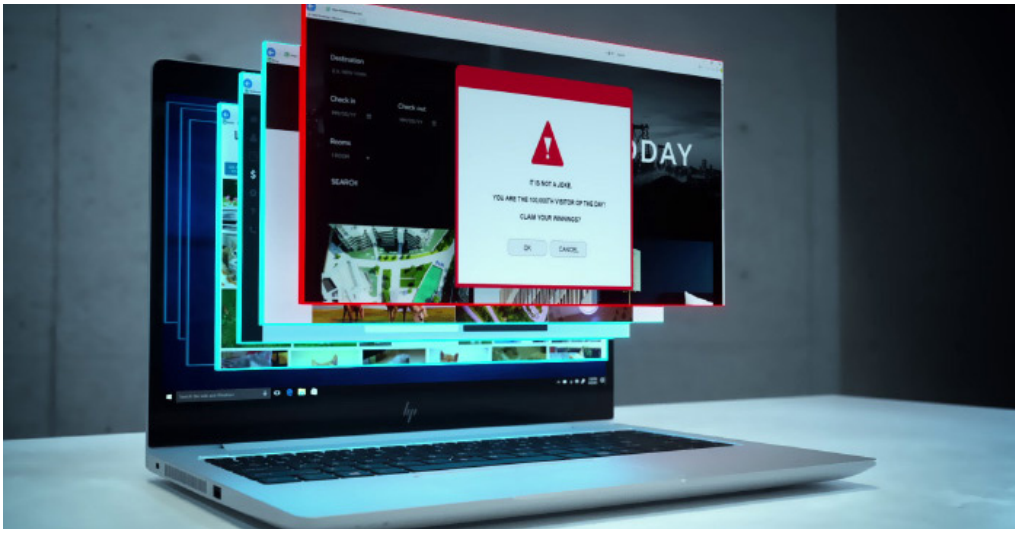
Phishing nie dotyczy już tylko wiadomości e-mail

Napisane przez Luizę Dzienkiewicz-Kobus

Dowiedz się więcej



Przeglądarka internetowa to portal wprowadzający w świat informacji... i zagrożeń. Co zatem możesz z tym zrobić, aby chronić swoją firmę?

Przeglądarki internetowe są miejscem, w którym dochodzi do wielu ataków. W ramach niedawno przeprowadzonej ankiety, w której udział wzięło 400 dyrektorów ds. informatyki, 68% respondentów powiedziało, że cyberprzestępcy są teraz bardziej wyrafinowani, a ich pracownicy z trudem odróżniają bezpieczne witryny od niebezpiecznych1. Mając to na względzie, nie należy się dziwić, że 70% informatyków doświadcza ataków phishingowych w każdym tygodniu – i nie są one przeprowadzane tylko przez pocztę elektroniczną[2]. Wyrafinowani hakerzy nakłaniają teraz podstępem pracowników do ujawniania wrażliwych danych osobowych, korzystając z mediów społecznościowych, reklam i adresów popularnych stron internetowych z błędami w pisowni. Ponieważ wykrycie phishingu jest coraz trudniejsze, firmy mają problemy z ochroną swoich pracowników przed tymi atakami.

Pomimo większej świadomości i większych inwestycji w oprogramowanie zabezpieczające i edukację pracowników, w ciągu ostatnich sześciu lat liczba cyberataków na notebooki i komputery stacjonarne wzrosła o 232%[3]. Cyberprzestępcy wciąż realizują swoje cele, ponieważ mają po swojej stronie liczby. Zabezpieczenie danych wymaga ogromnego nakładu pracy, a wystarczy, że jeden pracownik kliknie jedno złośliwe łącze, aby sparaliżować całą firmę.

W dużej mierze za ten problem odpowiadają cyberataki za pośrednictwem mediów społecznościowych. Platformy, takie jak Facebook i Twitter, są obfitym terenem łowieckim dla cyberprzestępców. Oprócz tego, że służą one do kontaktów i komunikacji, są one także łatwe w użyciu i tanie w utrzymaniu. Założenie oszukańczych kont i rozpoczęcie publikowania złośliwych treści, od łączy i zbierania danych do stron docelowych z niepewnymi wyskakującymi okienkami, jest niewiarygodnie łatwe.

Większość tych działań podejmowanych w Internecie opiera się na technikach phishingu, które kiedyś były zarezerwowane dla poczty elektronicznej. Media społecznościowe umożliwiają ludziom łączenie się ze sobą, a stworzenie poważnej i wiarygodnej postaci oraz obserwowanie autentycznych użytkowników platform nie wymaga wiele wysiłku.

Vevo, serwis streamingowy, padł ostatnio ofiarą masowego naruszenia danych. W jednego z jego pracowników wymierzony został atak phishingowy za pośrednictwem serwisu LinkedIn, w wyniku którego do Internetu wyciekło 3,12 TB plików wewnętrznych. Wśród nich znajdowały się filmy, dokumenty biurowe, materiały promocyjne, treści, które dopiero miały zostać opublikowane w mediach społecznościowych, oraz informacje na temat artystów korzystających ze studiów nagraniowych, które współpracują z tym serwisem[4].

Po sprzeczce z pracownikiem Vevo, która miała miejsce za pośrednictwem poczty elektronicznej, do ataku przyznała się grupa hakerska OurMine. Pokazuje to niebezpieczeństwo **spear-phishingu**, czyli odpowiednio wymierzonego ataku, którego celem jest kradzież określonych informacji znajdujących się w posiadaniu wyznaczonego celu. Najczęściej hakerzy podszywają się pod znajomego lub zaufane źródło (np. bank), aby podstępem namówić wyznaczony cel do ujawnienia informacji – co odpowiada za 91% ataków.

Phishing nie dotyczy już tylko wiadomości e-mail

Konsekwencje ataku phishingowego w przypadku większości firm, takich jak Vevo, mogą zarówno wiązać się ze szkodami, jak i utrzymywać przez długi czas. Oprócz utraty wydajności pracowników i danych klientów, ataki te mogą także doprowadzić do utraty samych klientów. Naruszenie bezpieczeństwa może bardzo poważnie zaszkodzić zaufaniu, jakim klienci darzą Twoją firmę – nie będziesz już dla nich wiarygodnym podmiotem przechowującym informacje. Chociaż czasami udaje się odzyskać dobre imię, częściej konsekwencje utrzymują się przez cały czas.

W IV kwartale 2017 r. ataki phishingowe, przeprowadzane za pośrednictwem mediów społecznościowych, wzrosły do 500%, wykazując trend, zgodnie z którym fałszywe konta były wykorzystywane jako punkty wsparcia dla klientów, udostępniane rzekomo przez znane firmy[5]. Zjawisko to jest znane jako **angler-phishing**, ponieważ hakerzy zarzucają przynętę i czekają, aż zgłoszą się do nich użytkownicy mediów społecznościowych. Aby stworzyć przekonywujący atak, hakerzy często używają konta z tym samym brandingiem i o autentycznym wyglądzie, przez co udaje im się nabrać miliony użytkowników mediów społecznościowych. Następnie, gdy tylko użytkownik nawiąże kontakt, otrzymuje z fałszywego konta łącze do witryny phishingowej, na której jest on proszony o zalogowanie się, dzięki czemu autor ataku phishingowego osiąga swój ostateczny cel, jakim jest zdobycie prywatnych danych.

Jednym z najłatwiejszych sposobów, aby uchronić swoich pracowników przed atakiem phishingowym za pośrednictwem mediów społecznościowych jest namawianie ich do zmiany zachowania w pracy. Powinno to pomóc pracownikom unikać prostych błędów, które prowadzą do dewastujących konsekwencji dla Twojej firmy:

1. Ograniczyć interakcje do użytkowników, którym można ufać
2. Nie klikać łączy pochodzących z niezweryfikowanego źródła
3. Nigdy nie pobierać załączników w postaci plików z mediów społecznościowych
4. Włączyć uwierzytelnianie dwupoziomowe na wszystkich urządzeniach i kontach w mediach społecznościowych – dzięki temu trudniej będzie je zaatakować
5. Przeszkolić dodatkowo pracowników w zakresie rozszerzonych uprawnień dostępu lub ról obejmujących kontakt z mediami społecznościowymi

Innym, podstawowym aspektem Twojego planu bezpieczeństwa, któremu należy się przyjrzeć, jest technologia, której używasz, aby zapewnić sobie odporność w cyberprzestrzeni. Na przykład rodzina urządzeń HP Elite obejmuje laptopy i komputery stacjonarne, które zostały opracowane od podstaw zgodnie z zasadami bezpieczeństwa.

Jedną z tych funkcji jest HP Sure Click, która jest dostępna na wybranych platformach HP Elite i która wykorzystuje odmienny sposób podejścia do kwestii bezpiecznego przeglądania Internetu. Zamiast zwykłego oznaczania niebezpiecznych stron, aby użytkownicy mogli ich unikać, funkcja ta powstrzymuje także złośliwe oprogramowanie, ransomware oraz wirusy przed zainfekowaniem innych kart przeglądarki oraz większej części systemu. Po rozpoczęciu przez użytkownika sesji przeglądania Internetu każda odwiedzona strona powoduje uruchomienie funkcji HP Sure Click. Na przykład w przypadku każdej wizyty na stronie internetowej, w ramach funkcji HP Sure Click tworzona jest oddzielna, sprzętowa sesja przeglądania, w ramach której jedna strona internetowa nie jest w stanie zainfekować pozostałych kart ani samego systemu.

Jeśli chodzi o firmy zmieniające swoją strategię bezpieczeństwa i wyposażające się w te najnowocześniejsze urządzenia, takie jak HP EliteBook 800 Series z opcjonalnym procesorem Intel® Core™ 8. generacji, może wydawać się, że łatwiej jest to powiedzieć niż zrobić. W tym przypadku można skorzystać z pomocy takich rozwiązań jak HP Device as a Service (DaaS). Jest to nowoczesny model korzystania z komputerów, który upraszcza sposób, w jaki organizacje komercyjne wyposażają swoich pracowników w odpowiedni sprzęt i akcesoria, zarządzają flotami urządzeń z różnymi systemami operacyjnymi i korzystają z dodatkowych usług w ramach cyklu życia tych urządzeń. W ramach HP DaaS dostępne są proste, a zarazem elastyczne plany obejmujące jedną cenę dla każdego urządzenia, dzięki czemu wszystko będzie działało płynnie oraz wydajnie.

W końcu posiadanie dobrze przeszkolonego zespołu i urządzeń zoptymalizowanych pod kątem bezpieczeństwa pomoże Ci walczyć z cyberprzestępcami wykorzystującymi do swoich procederów media społecznościowe (jest to jedno z głównych zagrożeń występujących w cyberprzestrzeni). Zagrożenie to będzie jedynie się zwiększało i stawało się coraz bardziej złowieszcze, a zatem musisz teraz udoskonalić swoją ochronę.

Odkryj korzyści, jakie rozwiązania zabezpieczające firmy HP mogą zapewnić Twojej firmie.

Źródła:

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/

4AA7-3218PLE, Może 2018 r.