Twój szef może być hakerem. Tylko co piąty e-mail phishingowy jest wychwytywany

Kategoria: Styl życia
Opublikowano: wtorek, 10, październik 2017 12:15
Artur Duda

Na każde 5 ataków, które zostaną zidentyfikowane jako phishing, przypada 20, które ominęły zabezpieczenia - wynika z danych Ironscale. W 95% przypadków, złodzieje wysyłają indywidualne wiadomości, które do złudzenia przypominają codzienną korespondencję.

Phishing to w głównej mierze próba przejęcia informacji wrażliwych, czyli haseł lub tajemnic handlowych, których posiadanie pozwala m.in. na kradzież pieniędzy. Już teraz niemal 95% prób phishingu jest wysoce celowanych. Złodzieje atakują pojedyncze skrzynki odbiorcze, wcześniej zbierając szczegółowe informacje o właścicielu danego adresu e-mail. I tak w przypadku odbiorców usług takich jak telewizja czy internet, złodzieje wiedzą doskonalone z jakiej firmy korzysta dana osoba i w którym dniu otrzymuje fakturę. Natomiast w przypadku pracowników, przestępcy podszywają się pod zespół komunikacji wewnętrznej czy przełożonego. Co ważne, wiadomości do złudzenia przypominają codzienne e-maile. Złodzieje powielają już nie tylko styl i szablony językowe powszechnie używane w danej branży, lecz także coraz częściej korzystają z rzeczywistych szczegółów wyróżniających daną firmę – kopiują stopki mailowe, logotypy, a także dbają o wiarygodne tematy e-maili, zgodne z profilem działalności firmy. Przestępcy załączają też pliki czy linki chronione hasłem. Tym samym podkreślają ich znaczenie i poufność. Tak podrobione wiadomości rozsyłane są nie tylko wewnątrz przedsiębiorstwa lecz także do aktualnych i potencjalnych partnerów.

- *Wykorzystanie wizerunku znanych firm w atakach phishingowych to częsta praktyka. Bez podszycia się pod instytucje wzbudzające zaufanie, ataki tego typu nie byłyby skuteczne. Dlatego tak istotne jest, aby przedsiębiorcy zadbali o własne bezpieczeństwo i wdrożyli odpowiednie zabezpieczenia. Firmy mogą m.in. włączyć funkcję, która spowoduje, że przy każdym e-mailu pojawi się specjalny znaczek uwierzytelniający* – mówi Michał Walachowski, dyrektor zarządzający z EmailLabs.

Cyberprzestępcy doskonale wiedzą, iż najsłabszym ogniwem w łańcuchu bezpieczeństwa internetowego jest człowiek. W danej firmie wystarczy kilku nieświadomych zagrożenia pracowników, którzy klikną na zainfekowany link, aby zdobyć dane wrażliwe. Co istotne, wirusy są instalowane na komputerach na długi okres. Jak podaje Ironscale, czas od naruszenia do wykrycia niebezpieczeństwa wynosi średnio 146 dni.

- *Newralgicznym punktem dla cyberbezpieczeństwa jest moment podejmowania decyzji przez pracownika czy otworzyć zawartość danego e-maila. Osobę świadomą zagrożenia trudniej będzie oszukać, dlatego tak istotna jest ciągła edukacja w tym zakresie. Nie można jednak pomijać znaczenia odpowiednich rozwiązań systemowych. To właśnie one są w stanie ochronić najważniejsze dane przed wyciekiem. Trzymając kluczowe informacje w chmurze możemy spać spokojnie, bo skompresowane i zaszyfrowane kopie dokumentów, umieszczane są w różnych lokalizacjach geograficznych. Dzięki temu są bezpieczne. Warto też oczywiście regularnie aktualizować oprogramowanie* – podsumowuje Jakub Hryciuk, dyrektor zarządzający Onex Group.

Źródło: newsrm.tv