**Każdy jest pracownikiem działu IT, czyli jak skutecznie chronić firmę przed atakami hakerów**

* **Rośnie liczba incydentów związanych z bezpieczeństwem komputerowym. W pierwszym półroczu 2021 roku było ich ponad 9 tysięcy, czyli dwa razy więcej niż w całym roku 2019 – wynika z danych NASK.**
* **Hakerzy wykorzystują konteksty związane z pandemią i stosują rozmaite techniki – m.in. phishing, który wg danych CERT był dominującą formą ataków w ubiegłym roku.**
* **Nawet najprostszą infrastrukturę IT trzeba regularnie sprawdzać i serwisować, w czym pomagają audyty.**

Hakerzy atakują nie tylko prezesów i zarząd, ale za cel przyjmują też szeregowych pracowników. Infekując ich komputer, „wchodzą dalej w system". Wydobycie danych nie musi być trudne, wystarczy podszyć się pod jakąś osobę lub instytucję i w ten sposób wyłudzić dostęp do informacji. Właśnie tak działa phishing, który brzmi tak samo jak „fishing”, czyli z angielskiego „łowienie”.

Ta technika zdobywania danych przez hakerów była numerem jeden wśród wszystkich cyberataków w Polsce, jakie odnotowano w raporcie CERT Orange Polska. To niemal 35% wszystkich wykrytych incydentów.

– *Te dane dobitnie potwierdzają, że phishing oraz jego odmiany jak np. vishing, to najskuteczniejsza metoda stosowana przez hakerów. Dlaczego tak jest? Ich ofiarą często padają szeregowi pracownicy firm, którzy nie zawsze potrafią wykryć zagrożenie. Właściwie skonstruowana wiadomość e-mail lub sms z prośbą o podanie danych, w zupełności wystarczy. Podobnie jest w przypadku wspomnianego wcześniej vishing’u, czyli voice phishing’u. Haker dzwoni do ofiary, podszywając się np. pod kogoś z zarządu i prosi o podanie informacji –* wyjaśnia Michał Bukontt, Dyrektor Sprzedaży w Sprint S.A.

**Metoda „na prezesa”**

Znany jest przypadek sekretarki, która podała przez telefon dane kilku pracowników osobie podszywającej się pod bliskiego znajomego prezesa. Na szczęście był to ekspert działający na korzyść organizacji, więc tym razem nie doszło do wycieku informacji. Ten przykład pokazuje, jak ważne jest przeprowadzanie regularnych audytów firmowej infrastruktury i procedur IT.

– *Hakerzy zdają sobie sprawę ze słabych punktów ochrony infrastruktury teleinformatycznej, a najsłabsze ogniowo to najczęściej nieświadomi pracownicy. Wbrew pozorom, znaczenie ma nie tylko zabezpieczenie techniczne, jak choćby zastosowanie firewall’a lub innych narzędzi, ale też zbudowanie odporności pracowników na social engineering, czyli techniki manipulacyjne. Właściwie przeprowadzony audyt pozwala wykryć takie nieprawidłowości i przygotować wszystkich zatrudnionych do radzenia sobie w tego typu sytuacjach. Musimy mieć świadomość, że dzisiaj każdy jest pracownikiem działu IT –* dodaje Michał Bukontt ze Sprint S.A.

Audyt firmowej infrastruktury IT opiera się na testach zewnętrznych i wewnętrznych. W pierwszym przypadku specjaliści, stosując między innymi phishing i pochodne techniki, próbują uzyskać nieautoryzowany dostęp do danych firmy. Ataki wykonywane są z sieci zewnętrznej poprzez próby ataku na sieci bezprzewodowe oraz przez Internet. Z kolei test wewnętrzny pozwala „od środka” zebrać specjalistom wszelkie dane dotyczące działania urządzeń w firmie – jej słabych punktów lub nieprawidłowości w konfiguracji. Znaczenie audytu jest kluczowe dla bezpieczeństwa informatycznego całej organizacji, niezależnie od stopnia rozwinięcia infrastruktury IT. Sprawdza się nawet w przypadku firm obsługujących infokioski czy biletomaty i w niewielkich przedsiębiorstwach sektora MSP.

**Każdy kontekst dobry, a zagrożenie rośnie**

Z danych raportu CERT wynika, że najpopularniejszą formą phishing’u w 2020 roku, podobnie jak w poprzednich latach, było podszywanie się pod firmy kurierskie. Hakerzy wykorzystali tym razem kontekst pandemii, wysyłając wiadomości z żądaniem dodatkowej opłaty za dezynfekcję paczek. W obawie przed zakażeniem często klikano w umieszczone tam linki. Koronawirus spowodował też rozwój bombardowania Zoomem, czyli włamań za pośrednictwem popularnej platformy do spotkań online. Hakerzy utrudniali połączenia lub wykradali informacje dzięki upublicznionym linkom do spotkań. Niejednokrotnie, korzystając z opcji udostępniania ekranu, obciążali sieć. Odnotowano też przypadki nielegalnych klonów narzędzi tego typu, zarządzanych przez cyberprzestępców. Skorzystanie z fałszywego programu oznaczało szybki wyciek danych.

Według prognoz przedstawionych w raporcie CERT, w tym roku wzrastać będzie liczba ataków phishing’owych z wykorzystaniem mediów społecznościowych oraz incydentów z zastosowaniem vishing’u i smishing’u. Zmianie może ulec także stopień skomplikowania ataków phishing’owych, których wykrycie może być coraz trudniejsze. Niestety pandemia przyspieszyła rozwój działalności cyberprzestępców.

Te prognozy potwierdzają dane NASK. Między styczniem a czerwcem 2021 roku, instytucja obsłużyła 9167 incydentów skategoryzowanych jako oszustwa komputerowe. To więcej niż w całym roku 2020 (8310 incydentów) i ponad dwukrotność przypadków z roku 2019 (4016).

– *Choć w czasie pandemii wszyscy nauczyliśmy się nowego stylu pracy, to jednak nie znaczy, że skala zagrożenia atakami hakerskimi jest mniejsza. Przeciwnie, częstsza i długotrwała obecność pracowników w sieci oraz przyspieszona cyfryzacja wielu procesów w firmach, tworzy jeszcze większe luki w infrastrukturze IT, które cyberprzestępcy mogą wykorzystać. Tutaj po raz kolejny duży nacisk należy położyć na obronę przed social engineeringiem i edukację pracowników. Wiele organizacji nadal pracuje zdalnie lub w trybie hybrydowym. To oznacza również częstsze logowanie do firmowego oprogramowania z zewnętrznych sieci i dodatkowe, potencjalne zagrożenie, którego można uniknąć* – wskazuje Michał Bukontt ze Sprint S.A.

Źródło: Sprint S.A.