**Ponad pół miliona incydentów dziennie w czasie urlopów. Jak zmniejszyć ryzyko cyberataków na firmy?**

* **Liczba cyberataków phishingowych wzrasta w sezonie urlopowym – w 2022 r. było ich w wakacje niemal dwukrotnie więcej w porównaniu z resztą roku. Pośrednio doprowadziło to do wzrostu strat finansowych organizacji aż o 76% r/r.**
* **Nie tylko letnie rozkojarzenie pracowników sprzyja hakerom. Znaczenie mają też ryzykowne praktyki związane z cyberbezpieczeństwem.**
* **Jednym ze sposobów na aktualizację wiedzy o zagrożeniach wśród osób zatrudnionych w organizacji są szkolenia w zakresie cyberbezpieczeństwa.**

Z raportu Proofpoint „2023 State of the Phish report” wynika, że liczba ataków phishingowych za pośrednictwem telefonów, wzrosła do 600 tys. dziennie w sierpniu 2022 roku. W pozostałych miesiącach utrzymywała się ona na poziomie 300-400 tys. dziennie. Oznacza to niemal 100% wzrostu w sezonie urlopowym. Pozwala to przypuszczać, że latem jesteśmy szczególnie rozkojarzeni.

*–* *To tylko potwierdza fakt, że choć poziom wiedzy na temat ataków wśród pracowników jest niezły, to nadal mamy trochę do nadrobienia w tym zakresie. Dodam, że bardzo łatwo paść ofiarą ataku phishingowego – wystarczy kliknąć w fałszywy link, który otwiera hakerom dostęp nie tylko do naszego urządzenia, ale także danych wrażliwych. W tym przypadku zagrożone mogą być także dane firmowe, nawet jeżeli zainfekowano nasz prywatny sprzęt. Phishing może utorować hakerowi drogę do firmowej sieci IT, jeśli nie dbamy o bezpieczeństwo haseł i danych logowania lub korzystamy ze służbowego sprzętu w celach prywatnych i na odwrót. Ten rodzaj ataku może przybierać różne formy i często poprzedza atak ransomware, czyli zablokowanie dostępu do danych z użyciem złośliwego oprogramowania. W ten sposób przestępcy mogą m.in. żądać okupu za odblokowanie dostępu –* mówi Patrycja Tatara, ekspertka ds. cyberbezpieczeństwa w Sprint S.A.

**Czy wiemy, co to jest phishing?**

W tym samym raporcie czytamy, że 58% ankietowanych pracowników wie, czym jest phishing, choć poziom tej wiedzy i tak spadł o 3 punkty procentowe w stosunku do 2019 roku. A czym jest ten atak? Jego nazwa brzmi podobnie jak angielskie słowo *fishing,* czyli *łowić.* Polega ono na pozyskiwaniu danych dostępowych poprzez rozsyłanie wiadomości z fałszywymi linkami. Po kliknięciu ofiara otwiera hakerowi dostęp do swojego urządzenia, a to już prosta droga do wykradania i blokowania rozmaitych danych. Aby oszukać potencjalną ofiarę, cyberprzestępcy stosują wiele praktyk mających na celu uśpienie czujności atakowanej osoby. W tym celu podszywają się np. pod kuriera wysyłającego link do śledzenia paczki przez SMS (*smishing*)*,* udają pracowników banków lub przełożonych z użyciem programów zmieniających głos (*vishing*), a nawet dzwonią ze znanego ofierze numeru telefonu (*spoofing telefoniczny*). Dane wykradzione tymi sposobami służą hakerom do dalszych działań i przeprowadzania głównie ataków ransomware. Według danych „2023 State of the Phish report”, w 2022 roku 76% organizacji odnotowały próby tych ataków, z czego 64% okazało się skutecznych. Co więcej, straty firm z tego tytułu wzrosły o 76% r/r.

**Szkolenia zminimalizują ryzyko**

Zróżnicowany poziom wiedzy na temat cyberzagrożeń może prowadzić do ryzykownych zachowań lub niewłaściwych praktyk, które mogą zostać wykorzystane przez hakerów. 78% badanych pracowników używa sprzętu służbowego w celach prywatnych, a 72% – prywatnego w celach służbowych. Z kolei 48% pozwala skorzystać ze służbowego telefonu lub komputera członkom rodziny, a nawet znajomym. Wiedza na temat bezpieczeństwa haseł w 2022 roku pozostała na tym samym poziomie, co rok wcześniej – 31% pracowników używa jednego hasła do wszystkich kont służbowych, a 27% robi to samo w przypadku kont do prywatnego użytku. 26% pracowników pozwala też przeglądarkom na używanym w urządzeniach służbowych, do zachowywania danych logowania. I na koniec bezpieczeństwo w pracy hybrydowej lub zdalnej – aż 80% pracowników nie zmienia domyślnych nazw i haseł w domowym routerze WiFi[[1]](#footnote-1).

– *Jednym ze sposobów na zmianę wspomnianych zachowań i minimalizację ryzyka ataku, są cykliczne szkolenia pracowników w zakresie cyberbezpieczeństwa. Hakerzy stale doskonalą swoje metody działania, ale też wiedzą sporo o zachowaniu ludzkiej psychiki. Umieją wywierać presję, ale też wzbudzać zaufanie. W czasie szkoleń przeprowadzane są symulowane ataki, które umożliwiają zdobycie wiedzy na temat tego, jak zachować się w takiej sytuacji i nie dać zmanipulować. Kolejny aspekt to informowanie o dobrych praktyk i wskazywanie na popełniane błędy, jak choćby bezpieczeństwo haseł. Ważne, aby szkolenia odbywały się cyklicznie i były przeprowadzane przez specjalistów* –dodaje Patrycja Tatara ze Sprint S.A.

Źródło: Sprint S.A.

1. dane z „2023 State of the Phish report” [↑](#footnote-ref-1)