Poznaj 5 zasad "cyber-BHP", by nie paść ofiarą internetowych przestępców

Data publikacji: 26.04.2023 14:46

Liczba cyberataków rośnie w lawinowym tempie. W sieci zagrożone są nasze dane osobowe, prywatność i pieniądze. Możemy też zostać wykorzystani do ataku na organizację, w której pracujemy. Jak wynika z badań dla BIK, przekonało się o tym już 4 na 10 Polaków. Sam strach w starciu z przestępcami nie wystarczy. Aby pozostać bezpiecznym warto wyrobić sobie kilka dobrych nawyków i odpowiednio się zabezpieczyć. Poznaj 5 zasad „cyber-BHP".

Miniony rok obfitował w zagrożenia w sieci. Było ich prawie trzy razy więcej niż w 2021. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CERT) zanotował ponad 320 tys. takich przypadków. Eksperci są zgodni, za chwilę padną kolejne rekordy.

Zdaje sobie już z tego sprawę duża część społeczeństwa. Z badania na temat cyberbezpieczeństwa przeprowadzonego przez Quality Watch na zlecenie Biura Informacji Kredytowej wynika, że rośnie obawa Polaków, że padną ofiarą kradzieży w wyniku wyłudzenia ich danych. Wiosną ubiegłego roku wykorzystania informacji o sobie przez przestępców bało się 54 proc. ankietowanych, a jesienią już 64 proc. Z jednej strony narasta świadomość problemu, a z drugiej poprawia się skuteczność przestępców. Co prawda wciąż nagminnie zdarza się im rozsyłać przetłumaczone przez automat, niezbyt wiarygodne maile, ale potrafią wykazać się również wyrafinowanymi technikami.

Przyjrzyj się uważnie, kto to i jaki ma adres

Pierwsze co należy robić wchodząc do sieci, to sprawdzić z kim mamy do czynienia, czyli dokładnie przyjrzeć się adresowi, z którego została wysłana wiadomość. Z pewnością będzie przypominać ten, z którego korespondencję przesyła nam zaufana firma, ale nie będzie taki sam. I już na tym wstępnym etapie wielu atakowanych niestety oddaje pole przestępcom.

BIK w swoim badaniu o cyberbezpieczeństwie przeprowadziło quiz na to jak radzimy sobie z rozpoznawaniem adresów stron, które nie budzą zaufania. Poprawnie rozwiązało go... jedynie 20 proc. ankietowanych. Tymczasem według raportu „Threat Landscape 2022" przygotowanego przez Agencję UE ds. Cyberbezpieczeństwa (ENISA), ataki wykorzystujące socjotechnikę, podstępem nakłaniające do otwierania złośliwych dokumentów, plików lub wiadomości e-mail, odwiedzania stron internetowych, to aż 60 proc. wszystkich naruszeń cyberbezpieczeństwa.

To zagrożenie nie tylko dla użytkowników prywatnych, ale niebezpieczeństwo dla organizacji. Przestępcy mogą w ten sposób zdobyć dostępy do wewnętrznej sieci instytucji, poczty, aplikacji czy wreszcie do danych jej klientów. Wykorzystują phishing (fałszywe maile, komunikaty na portalach społecznościowych), smishing (fałszywe wiadomości na telefon) i inne taktyki socjotechniczne nakłaniając pracowników do otwarcia niebezpiecznych załączników lub podania danych uwierzytelniających do kont i systemów.

W minionym roku w Polsce zostało zgłoszonych niemal 35 tys. tego typu ataków, o jedną trzecią więcej niż w 2021 roku – informuje CERT.

Chroń swoje dane

Dla przestępców cenne są dane, na podstawie których są w stanie zaciągnąć na nasze konto różne zobowiązania finansowe. Mogą wypożyczyć samochód, wziąć kredyt czy podpisać długoterminową umowę abonamentową z operatorem telefonii komórkowej, a otrzymanego w zamian smartfona sprzedać. Tymczasem my zostaniemy z długiem, którego nie zaciągaliśmy.

Możemy się od tego uwolnić, jeśli skierujemy sprawę do sądu, a on nam uwierzy i unieważni umowę. Jednak zanim zorientujemy się, że padliśmy ofiarą oszustwa, możemy mieć kontakt z windykatorami czy nawet z komornikiem.

Problem jest poważny, bowiem aż 11 proc. z nas doświadczyło wycieku danych osobowych – podaje wspomniane już badanie na zlecenie BIK. 41 proc. zetknęło się natomiast z różnymi próbami wyłudzenia, nie tylko przez kradzież danych.

Nie otwieraj odruchowo załączników

Kolejnym zagrożeniem jest włamanie na nasze konto bankowe. To niemal niemożliwe bez naszej pomocy. Przestępcy muszą uzyskać od nas informacje dotyczące logowania, a bez dodatkowej weryfikacji nie dokonają przelewu. Mogą wyłudzić od nas niezbędne dane albo zainstalować nam złośliwe oprogramowanie, które pozwoli na śledzenie naszych poczynań w sieci i wyczyszczenie rachunku.

Zmorą dużych i małych firm, a także zupełnie przypadkowych użytkowników, są programy szyfrujące dyski. Pobieramy taki np. poprzez otwarcie załącznika w mailu czy kliknięcie w link. W zamian za odszyfrowanie firmowego dysku przestępcy żądają pieniędzy. Najgorsze w tym procederze jest to, że zapłacenie okupu nie zawsze kończy się rozwiązaniem problemu. Zostajemy z zaszyfrowanymi dyskiem i bez pieniędzy.

Czy warto o tym przypominać? Na pewno, 34 proc. z nas otwiera załączniki od nieznanych nadawców i klika w linki od nich.

Nie jest prawdą, że ofiarami cyberprzestępców padają tylko osoby, które słabo radzą sobie z nowymi technologiami. Każdy z nas może się nią stać, wystarczy działanie w pośpiechu, bez zastanowienia, czasami z ciekawości, czy zwykła chwila roztargnienia.

Twoje „Cyber – BHP" w internecie:

1. **Unikajmy stosowania jednego hasła do wielu serwisów**. Stosujmy hasła długie, które jednocześnie są dla nas łatwe do zapamiętania. Może to być miejsce, w którym spędziliśmy najlepsze wakacje i rok tego wydarzenia. Jeśli w 2017 r. byliśmy w górach, to hasło „KotlinaKlodzka2017?!" jest nie do złamania, a ściślej, jego złamanie zajęłoby przestępcom od kilkudziesięciu do kilkuset lat.
2. **Używajmy programów chroniących** nasze urządzenia przed atakami. Może to być nawet domyślny bezpłatny program, który mamy wraz z systemem operacyjnym. Ważne, aby był włączony i codziennie aktualizowany (automatycznie).
3. **Uważajmy na reklamy oraz na różnego rodzaju ankiety i ogólnodostępne bardzo atrakcyjne oferty pracy.** Nie podawajmy żadnych danych osobowych ani informacji finansowych.
4. **Bądźmy uważni** - dokładnie czytajmy i sprawdzajmy adresy URL. Zamiast działać odruchowo, zachowujmy dystans do wszelkiego rodzaju linków i załączników w mailach - nie klikajmy w nie bez zastanowienia.
5. **Włączmy usługę ostrzegającą** przed próbą wyłudzenia kredytów na nasze konto. **Alerty BIK** to rozwiązanie, które informuje SMS-em lub mailem o każdym zapytaniu do bazy Biura Informacji Kredytowej oraz Rejestru Dłużników BIG InfoMonitor. Takie zapytanie to standardowa procedura przy sprawdzaniu wiarygodności kredytowej przed udzielaniem pożyczki, podpisaniem umowy abonamentowej czy zakupem sprzętu na raty. Jeśli to nie my złożyliśmy wniosek o kredyt czy pożyczkę, to taki SMS, mail jest informacją, że ktoś dokonuje wyłudzenia na nasze dane. Przy odpowiednio szybkiej reakcji jesteśmy w stanie uniemożliwić oszustowi zaciągnięcie zobowiązania na nasze personalia.

***

Biuro Informacji Kredytowej jest inicjatorem programu edukacyjnego Nowoczesne Zarządzanie Biznesem i partnerem w module „Zarządzanie ryzykiem finansowym w biznesie i życiu osobistym".

Więcej: www.nzb.pl oraz www.facebook.com/NowoczesneZarzadzanieBiznesem