Data publikacji: 2024-10-07

Październik - Europejskim Miesiącem Cyberbezpieczeństwa

W świecie, gdzie codzienność przenosi się do Internetu, bezpieczeństwo w sieci staje się priorytetem. Każdego dnia jesteśmy narażeni na różnego rodzaju cyberzagrożenia, które mogą dotknąć każdego. Październik, Europejski Miesiąc Cyberbezpieczeństwa, to idealny moment, aby poznać najważniejsze zasady ochrony swoich danych i dowiedzieć się, jak skutecznie zabezpieczyć aktywności w sieci.

Pomyśl, zanim klikniesz! *(ang. Think Before U Click)* – to hasło przewodnie Europejskiego Miesiąca Cyberbezpieczeństwa w październiku. Z tej okazji w całej Europie odbywają się wydarzenia, których celem jestzwiększenie wiedzy dotyczącej cyberbezpieczeństwa i zagrożeń, które czyhają na nas w sieci.

Najczęstsze incydenty według raportu CERT Polska 2023
W 2023 roku, podobnie jak w latach poprzednich, najczęstszym typem cyberataków były incydenty phishingowe. Zarejestrowano 41 423 takich przypadków, co stanowiło ponad połowę wszystkich incydentów obsłużonych przez CERT Polska. To znaczący wzrost o 61 punktów procentowych w porównaniu do roku 2022. Najczęściej wykorzystywano wizerunek serwisów takich jak Allegro (11 161 przypadków), Facebook (5 308) oraz OLX (4 753).

Kolejną dużą grupę incydentów stanowiły oszustwa komputerowe, których odnotowano 34 304, co daje ponad 42% wszystkich incydentów. Do tej kategorii zaliczały się fałszywe sklepy internetowe oraz oszustwa finansowe, w których przestępcy podszywali się pod znane firmy i instytucje, m.in. w sektorze energetycznym, próbując wyłudzić pieniądze poprzez fałszywe programy inwestycyjne.

Trzecią najczęstszą kategorią było szkodliwe oprogramowanie. W 2023 roku zarejestrowano 1 650 takich przypadków, co oznacza spadek o połowę w porównaniu do poprzedniego roku, gdy takich incydentów było 3 409. Wśród nich były zarówno infekcje ransomware, jak i kampanie spamowe rozprzestrzeniające oprogramowanie takie jak Remcos czy Agent Tesla.

Phishing – najczęściej spotykana forma cyberataków
Obrona przed phishingiem nie wymaga zaawansowanej wiedzy technicznej ani specjalistycznego sprzętu. Oszuści zazwyczaj podszywają się pod znane instytucje lub osoby, aby zdobyć zaufanie i manipulować odbiorcami. Wiadomości phishingowe są wysyłane masowo, z nadzieją, że choćby niewielki odsetek osób padnie ofiarą oszustwa – na przykład ci, którzy czekają na przesyłkę, zwrot podatku lub korzystają z bankowości online.

Najlepszym sposobem obrony jest zachowanie spokoju i dokładna weryfikacja otrzymanych wiadomości poprzez inne źródła. Dzięki temu można uniknąć większości ataków. Przestępcy stale udoskonalają swoje metody, dlatego zaleca się regularne śledzenie informacji o zagrożeniach w sieci.

Ochrona prywatności w mediach społecznościowych
Media społecznościowe są przestrzenią, w której spotykają się użytkownicy o różnych poglądach, w różnym wieku i z różnymi zainteresowaniami. Niestety, wielu z nich nie zdaje sobie sprawy, jak łatwo mogą stać się ofiarami cyberoszustwa.

Tworząc konto na platformach takich jak Facebook czy Instagram, warto zastanowić się, kto będzie miał dostęp do naszych treści. Dzięki ustawieniom prywatności można kontrolować, kto zobaczy, polubi czy skomentuje posty i zdjęcia.

Niezwykle istotne jest też rozsądne podejście do zaproszeń do grona znajomych – nie akceptujmy próśb od osób, których nie znamy. Jeśli zauważymy niewłaściwe zachowania, takie jak nękanie czy propagowanie nienawiści, zawsze mamy możliwość zgłoszenia profilu lub jego zablokowania.

Zabezpieczenie kont przed cyberatakami
Konta w sieci mogą stać się celem ataków hackerskich. Aby minimalizować to ryzyko, eksperci rekomendują stosowanie dwuetapowej weryfikacji. To dodatkowe zabezpieczenie polega na konieczności podania drugiego elementu uwierzytelniania użytkownika podczas logowania, np. otrzymanego SMS-em, podczas logowania.

Ważne jest również stosowanie silnych i unikalnych haseł – każde z kont powinno mieć inne hasło. Pomocna będzie także instalacja programu antywirusowego, który pomoże chronić nasze urządzenia i dane przed zagrożeniami.

Nowe funkcje w aplikacji mObywatel 2.0
Ministerstwo Cyfryzacji, wychodząc naprzeciw potrzebom użytkowników, wprowadziło w aplikacji mObywatel 2.0 nową funkcję zgłaszania incydentów cyberbezpieczeństwa. Umożliwia ona raportowanie podejrzanych stron internetowych, e-maili czy SMS-ów. Zgłoszenia trafiają bezpośrednio do ekspertów z CERT Polska, którzy zajmują się analizą i eliminacją zagrożeń.

Wkrótce zostanie również uruchomiona baza wiedzy, w której znajdą się proste wskazówki dotyczące ochrony danych w sieci. Każdy użytkownik będzie mógł dowiedzieć się, na co zwracać szczególną uwagę, aby bezpiecznie korzystać z Internetu.

Polecamy ciekawy artykuł: Socjotechnika – sztuka manipulacji w świecie cyfrowym.

Zachęcamy do regularnego odwiedzania oficjalnych stron rządowych, gdzie można znaleźć informacje dotyczące różnych zagrożeń oraz sposobów ochrony przed przestępczością internetową:

- **GOV.PL**– strona rządowa z informacjami dotyczącymi m.in. aktualnych zagrożeń, szkoleń i rekomendacji związanych z cyberbezpieczeństwem

- **NASK.PL** - Państwowy Instytut Badawczym, którego misją jest poszukiwanie i wdrażanie rozwiązań, służących rozwojowi sieci teleinformatycznych w Polsce oraz poprawie ich efektywności i bezpieczeństwa. Instytut prowadzi badania naukowe, prace rozwojowe, a także działalność operacyjną na rzecz bezpieczeństwa polskiej cywilnej cyberprzestrzeni. Ważnym elementem działalności NASK jest też edukacja użytkowników oraz promowanie koncepcji społeczeństwa informacyjnego, głównie w celu ochrony dzieci i młodzieży przed zagrożeniami, związanymi z użytkowaniem nowych technologii.
- **CERT.PL** – CERT Polska to działający w ramach NASK zespół reagowania na incydenty związane z cyberbezpieczeństwem, gdzie pod linkiem https://incydent.cert.pl/ dostępny jest interaktywny formularz umożliwiający wysłanie zgłoszenia o potencjalnym oszustwie np. sms/mail z nieznanego źródła o zaległościach finansowych z linkiem do opłaty.

Źródło: Ministerstwo Cyfryzacji, bezpiecznymiesiac.pl