Biuletyn Informacji Publicznej Starostwo Powiatowe we Wrocławiu

Adres artykułu: http://sbip125.lo.pl/artykul/cyberbezpieczenstwo

Cyberbezpieczeństwo

Cyberbezpieczeństwo

W związku z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa przekazujemy Państwu informacje dotyczące cyberbezpieczeństwa, czyli zagrożeń, z którymi możecie Państwo spotkać się w sieci oraz przedstawiamy sposoby zabezpieczenia się przed nimi.

Cyberbezpieczeństwo to odporność systemów informatycznych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Najprościej mówiąc jest to ogół technik, procesów i praktyk stosowanych w celu ochrony sieci informatycznych, urządzeń, programów i danych przed atakami, uszkodzeniami lub nieautoryzowanym dostępem.

Jest wiele zagrożeń i niebezpieczeństw w świecie cyberprzestrzeni na jakie może się natknąć użytkownik urządzeń elektronicznych podpiętych do Internetu. Do najbardziej popularnych zagrożeń obecnie spotykanych możemy zaliczyć:

1. kradzież tożsamości - polega na tym, iż sprawca lub grupa sprawców w sposób bezprawny (a najczęściej podstępny) wchodzi w posiadanie danych osobowych poszczególnych osób takich jak: imię i nazwisko, adres, pesel, data urodzin, nr karty kredytowej etc. Powyższe dane są uzyskiwane po to, aby były wykorzystane w celach przestępczych (np. wyłudzeniu kredytu) lub celach związanych z popełnianiem przestępstw (np. wynajmowanie lokali przeznaczonych na przechowywanie kradzionych towarów na nazwisko “ofiar”)

2. Inne kradzieże typu wyłudzenia – phishing, smishing, vishing:

- Najczęściej wiadomości phishingowe to fałszywe powiadomienia z banków,komunikaty od dostawców systemów e-płatności, urzędów i innych organizacji.Czytając e-mail lub SMS, odbiorca zawsze jest zachęcany, aby pilnie wprowadził czy zaktualizował swoje poufne dane. W przeciwnym razie „grozi mu”

utrata konta, pieniędzy, zablokowanie systemu itp. Wiadomości mogą też sugerować konieczność potwierdzenia danych w celu ochrony przed pishingiem. Aby uzupełnić wymagane informacje, wystarczy kliknąć w przesłany link, który przekieruje bezpośrednio w odpowiednie miejsce na stronę instytucji. Problem w tym, że strona łudząco przypomina oryginalną. Wszystko, co tam wpiszemy zostanie wysłane do twórcy, wraz z loginem i hasłem do zaufanej, prawdziwej strony. Phisher uzyskując dostęp do konta, może wykorzystać go na różne sposoby, zależnie od typu konta.

- Szczególnym rodzajem oszustwa jest smishing. Nazwa powstała z połączenia dwóch słów: SMS i phishing. Oznacza nic innego jak kradzież z wykorzystaniem spreparowanych wiadomości SMS. Użytkownik otrzymuje SMS w tonie, który ma go zaniepokoić i namówić do podjęcia natychmiastowego działania. Oszuści najczęściej korzystają z internetowych bramek umożliwiających spoofing SMS. Dzięki nim mogą tak skonfigurować wysyłaną wiadomość, żeby na ekranie naszego telefonu w polu nadawcy ukazał się wybrany przez nich tekst. W ten sposób podszywają się pod banki czy operatorów telekomunikacyjnych. Najczęstszym scenariuszem jest próba podszycia się pod bank:
    - Użytkownik dostaje wiadomość z informacją o rzekomej blokadzie karty płatniczej ze względów bezpieczeństwa. Aby ją odblokować, musi zadzwonić pod podany w wiadomości numer. Jeśli nawiąże połączenie, usłyszy nagraną wiadomość, po której będzie musiał podać dane karty, by ją odblokować.
    - SMS może zawierać prośbę o zmianę danych logowania do bankowości internetowej. Swój dotychczasowy login i hasło – rzekomo w celu weryfikacji – trzeba będzie podać, dzwoniąc pod podany numer.

      Oba przypadki kończą się przekazaniem oszustom swoich prywatnych danych, dzięki którym otrzymają bezpośredni dostęp do naszych pieniędzy.

- Vishing, czyli voice phishing, to kolejny rodzaj oszustwa. Cyberprzestępcy wyłudzają dane wykorzystując połączenia głosowe. Często są to nieświadomi zagrożenia rozmówcy. Podobnie jak w smishingu chodzi o kradzież osobistych, bardzo istotnych informacji. Naciągacz podający się np. za pracownika banku poprosi o hasła dostępu, loginy czy numery kart kredowych bądź debetowych. Przykładowo przekonuje, że ktoś w danym momencie podjął próbę wypłaty czy transakcji internetowej za pośrednictwem naszej karty. Częstym przykładem vishingu jest wyłudzenie kodu Blik. Po jego otrzymaniu oszust pobiera pieniądze z bankomatu. Oszuści podszywają się nie tylko pod pracowników banków. W danej chwili mogą przedstawić się jako pracownik urzędu czy po prostu przedstawiciel handlowy. Słysząc miły głos, informujący o blokadzie naszego konta trudno nam zweryfikować czy dzwoniąca osoba jest na pewno tą, za którą się podaje. Oszuści brzmią przekonująco, są przygotowani. Należy zachować rozsądek. Jeśli rozmówca

budzi naszą wątpliwość, rozłączmy się. Zadzwońmy do danej placówki i potwierdźmy przekazane informacje.

3. Fałszywe oferty pracy – Do tego typu przestępstw dochodzi często poprzez przesłanie do użytkowników ofert atrakcyjnej pracy. Sprawcy zazwyczaj oferują wysokie wynagrodzenia lub proponują pracę nie wymagającą od przyszłych „pracowników" dużego wysiłku. Oferty pracy przychodzą na adresy mailowe w postaci spamu lub ogłoszeń, itp. Ofiara wysyła swoje CV, kopię dokumentów tożsamości, numer swojego konta bankowego i telefon kontaktowy. Zdarzają się nawet przypadki gdzie oszust wymaga od aplikantów założenia konta bankowego na swoje dane osobowe, a następnie wysłanie otrzymanej karty bankomatowej wraz z kodem PIN. Jeżeli użytkownik spełni wymagania, oszust ma wszystko co potrzebne aby posłużyć się tożsamością ofiary do popełniania innych przestępstw. Po wyłudzeniu tych informacji oszust może dalej wykorzystywać nieświadomość użytkownika. W przypadku fałszywych ofert pracy, zadaniem ofiary jest zazwyczaj przesyłanie pieniędzy, wpływających na konto, do wskazanych przez oszustów osób czy banków. Przy czym przesyłanie pieniędzy odbywa się za pośrednictwem systemu płatności uniemożliwiającego identyfikację odbiorcy, np. Western Union. Ofiara jest przekonana, że pieniądze pochodzą z legalnie działających firm, przesyła pieniądze w żądane miejsce za co pobiera prowizję. Ofiary nie zdają sobie sprawy, że uczestniczą w procesie tzw. „prania pieniędzy", pochodzących z przestępstwa. Slangowo osoba zajmująca się przesyłaniem pieniędzy nazywa się money mule (muł pieniężny) -takie działanie w myśl przepisów polskiego prawa również jest karalne. Inny sposób to tzw . „oszustwa nigeryjskie". Oszust wysyła bardzo korzystną ofertę pracy za granicą. Ofiara odpowiada na ofertę, bardzo łatwo przechodzi rekrutację, a następnie ma zgłosić się do pracy. Oszust zapewnia, że wszystko jest już załatwione, prosi jedynie o wpłacenie niewielkiej kwoty np. na zakup biletu lotniczego, wykupienia wizy, pozwolenia na pracę czy opłacenia wynajętego mieszkania.

4. Modyfikowanie danych, niszczenie danych, blokowanie dostępu, - Zagrożenia tego typu określane są nazwą Ransomware. W szeroko rozumianym pojęciu ransomware jest kategorią złośliwego oprogramowania, zaprojektowanego aby blokować dostęp do komputera, dopóki odpowiednia suma okupu nie zostanie uiszczona na konto przestępcy. Obecnie znane są trzy różne rodzaje ransomware:

- Najmilszy z nich to screen-locker, który blokuje użytkownikowi dostęp do urządzenia poprzez zablokowanie ekranu. Dosyć irytujący, lecz można się go pozbyć bez płacenia atakującemu, jeśli ofiara posiada wystarczającą wiedzę techniczną.
- Screen-locek nie szyfrował plików i okazał się nieefektywny w wyłudzaniu pieniędzy, dlatego też został zastąpiony przez crypto-ransomware**.** Jest to

wyjątkowo efektywna odmiana tego oprogramowania z racji tego, że szyfruje lokalne pliki ofiary jak i również pliki w chmurze. Następnie oferuje deszyfrator za uiszczeniem odpowiedniej opłaty, przeważnie oscylującej między $300-$900 dolarów. Ponieważ crypto-ransomware wykorzystuje ten sam typ szyfrowania co oprogramowanie chroniące transakcje bankowe lub wojskową komunikacje, zaszyfrowane pliki są praktycznie nie do odzyskania, bez opłacenia okupu. Rodzina oprogramowania crypto-ransomware jest odpowiedzialna za wyłudzenie ponad miliarda dolarów co roku od ofiar.

- Trzeci rodzaj ransomware to tzw.: disk-encryptor. W odróżnieniu od crypto-ransomware disk-encryptor zaszyfrowuje cały dysk ofiary i nie pozwala na uruchomienie się systemu operacyjnego.

  Przeważnie ransomware rozprzestrzenia się podszywając się pod fakturę, informacje o dostawie zamówienia lub załączone CV. Często też znajdują się w załącznikach w pieczołowicie wykonanych mailach ze spamem. Kiedy użytkownik otworzy załącznik, rozpoczyna się proces szyfrowania. Kiedy proces szyfrowania dobiegnie końca, ofiara widzi na ekranie powiadomienie z instrukcjami jak zapłacić okup i otrzymać klucz do deszyfracji. Innym razem, cyber-złoczyńcy kupują reklamy na stronach o dużej popularności. Te reklamy nie są normalnymi ogłoszeniami, lecz służą do wykorzystania słabości przeglądarki i ich wtyczek. Kiedy przeglądarka (lub znana wtyczka) ulegnie crashowi, komponent z ransomware automatycznie się instaluje. W taki sposób cyber-przestępcy wykorzystujący ransomware mają okazje zarazić ofiarę, nawet jeśli ta wie jak zachować się wobec ransomware w wiadomościach mailowych.

5. Ataki szkodliwych oprogramowań typu wirusy, robaki, konie trojańskie, exploit, rootkit i wiele innych, które maja na celu nadpisanie lub zmianę innych programów, umożliwienie otwarcie portów komputera, umożlwiające bezpośrednie włamanie do komputera, kradzież danych.

Jak w takim razie jesteśmy w stanie zabezpieczyć się przez potencjalnymi zagrożeniami?

Najlepszą metodą jest zapobieganie. Podstawową metodą uniknięcia zagrożenia wydaje się być nieotwieranie plików nieznanego pochodzenia. Takie materiały najlepiej od razu usuwać. Z pewnością systematyczne aktualizowanie systemu operacyjnego i aplikacji zwiększy poziom naszego bezpieczeństwa. Konieczna będzie również instalacja i użytkowanie oprogramowań przeciw wirusom, czy spyware. Zapora sieciowa typu firewall to jedna z najpopularniejszych metod zabezpieczenia swojej sieci – co ważne skuteczna przeciwko wielu zagrożeniom. Systematyczne skanowanie komputera i weryfikowanie procesów sieciowych jest kolejnym istotnym elementem

zabezpieczenia. Czasami złośliwe oprogramowanie nawiązujące własne połączenia z internetem, wysyłając hasła i inne prywatne dane do sieci, które mogą zostać zainstalowane nawet mimo dobrej ochrony. Nie zaleca się stosowania niesprawdzonych programów zabezpieczających czy też programów do publikowania własnych plików w internecie mogących np. podłączać niechciane linijki kodu do źródła strony. Bardzo istotnym elementem jest dbałość o aktualizację oprogramowania antywirusowego oraz baz danych wirusów. Rozwaga w internecie – nie należy zostawiać danych osobowych w niesprawdzonych serwisach i na stronach internetowych, jeżeli nie ma się pewności, że nie są one widoczne dla osób trzecich oraz nie wysyłanie w wiadomościach e-mail żadnych poufnych danych w formie otwartego tekstu. Dane powinny być zabezpieczone hasłem i zaszyfrowane. Hasło powinno być przekazywane w sposób bezpieczny przy użyciu innego środka komunikacji. Wykonywanie regularnych kopii zapasowych ważnych danych z pewnością nam pomoże w przypadku ich utraty. Dobrą praktyką jest nieotwieranie stron internetowych, które zawierają „podejrzane atrakcje” (łatwy zarobek, darmowe filmiki itp. - często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia).

Pamiętajmy, że żadna instytucja publiczna (urzędy czy banki) nie będą nam wysyłać wiadomości z prośbą do podanie loginu lub hasła celem ich weryfikacji.

Poniżej znajdują się treści, z którymi zachęcamy się zapoznać:

- Ministerstwo Cyfryzacji - Dla każdego cyberhigiena
- Zestaw porad bezpieczeństwa dla użytkowników komputerów CSIRT NASK

Metryczka

Odpowiedzialny za treść:	Admin BIP
Data wytworzenia:	29.01.2026
Opublikował w BIP:	Zespół Administratorów
Data opublikowania:	29.01.2026 09:19
Liczba wyświetleń:	2