

Cyberbezpieczeństwo

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skutecznie stosować sposoby zabezpieczenia się przed tymi zagrożeniami.

Cyberbezpieczeństwo zgodnie z obowiązującymi przepisami to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy” – art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, ze zm.).

Celem cyberprzestępców zwykle jest kradzież naszych danych. Do tego celu wykorzystywane są różne techniki mające na celu nakłonienie nas do wykonania czynności, wskutek których ujawnione zostaną nasze hasła i stosowane zabezpieczenia. Wśród tych technik są między innymi: zainfekowane załączniki, fałszywe strony internetowe i wiadomości e-mail, łudząco podobne do prawdziwych.

Najpopularniejsze rodzaje zagrożeń w cyberprzestrzeni:

Malware, czyli złośliwe oprogramowanie, które bez naszej zgody i wiedzy wykonuje na komputerze działania na korzyść osoby trzeciej. Działania tego typu obejmują między innymi zdobywanie wirtualnych walut, kradzież danych osobowych i informacji niezbędnych do logowania do bankowości elektronicznej. Złośliwe oprogramowanie może przyjąć formę wirusów, robaków, koni trojańskich i innych.

Phishing to jeden z najpopularniejszych typów ataków dokonywanych przy użyciu wiadomości e-mail, rozmów telefonicznych czy wysyłanych wiadomości SMS. Cyberprzestępcy podszywając się pod różne instytucje (np. firmy kurierskie, urzędy, operatorów telekomunikacyjnych, banki) a nawet naszych znajomych, starają się wyłudzić nasze dane do logowania np. do kont bankowych lub używanych przez nas kont społecznościowych. Wiadomości phishingowe są tak przygotowywane, aby wyglądały na autentyczne.

Man in the Middle jest rodzajem ataku, w którym cyberprzestępca uczestniczy w komunikacji między osobami, bez ich wiedzy. Wydaje nam się, że połączenie jest bezpośrednie i prywatne, natomiast w rzeczywistości ktoś potajemnie uczestniczy w komunikacji i ją zmienia. Celem takich ataków jest przechwycenie informacji lub środków pieniężnych (np. uzyskanie danych niezbędnych do logowania w systemie bankowości elektronicznej).

Ransomware to rodzaj ataku, którego celem jest przejęcie i zaszyfrowanie danych zgromadzonych na komputerze a następnie zażądanie okupu za ich odzyskanie. Zagrożenie może dostać się do komputera za pośrednictwem pobranego pliku lub nawet przez wiadomość tekstową. Atak nie ma na celu kradzieży danych, lecz wymuszenie okupu.

Malvertising pozwala przestępcom na dotarcie do nas poprzez reklamy udostępniane nam na przeglądanych zaufanych stronach internetowych. W następnym kroku atakujący instaluje, bez naszej wiedzy i zgody, złośliwe oprogramowanie na urządzeniach.

Sposoby zabezpieczenia się przed zagrożeniami:

Zainstaluj i używaj oprogramowania przeciw wirusom i spyware. Najlepiej stosuj ochronę w czasie rzeczywistym.

Aktualizuj oprogramowanie antywirusowe oraz bazy danych wirusów (dowiedz się czy twój program do ochrony przed wirusami posiada taką funkcję i robi to automatycznie).

Aktualizuj system operacyjny i aplikacje bez zbędnej zwłoki.

Nie otwieraj plików nieznanego pochodzenia.

Nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu, chyba, że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna.

Nie używaj niesprawdzonych programów zabezpieczających czy też do publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony).

Co jakiś czas skanuj komputer i sprawdzaj procesy sieciowe – jeśli się na tym nie znasz poproś o sprawdzenie kogoś, kto się zna. Czasami złośliwe oprogramowanie nawiązujące własne połączenia z Internetem, wysyłające twoje hasła i inne prywatne dane do sieci może się zainstalować na komputerze mimo dobrej ochrony – należy je wykryć i zlikwidować.

Sprawdzaj pliki pobrane z Internetu za pomocą skanera.

Staraj się nie odwiedzać zbyt często stron, które oferują niesamowite atrakcje (darmowe filmiki, muzykę, albo łatwy zarobek przy rozsyłaniu spamu) – często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia.

Nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich.

Nie wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu – niech np. będą zabezpieczone hasłem i zaszyfrowane – hasło przekazuj w sposób bezpieczny.

Pamiętaj o uruchomieniu firewalla.

Wykonuj kopie zapasowe ważnych danych.

Pamiętaj, że żaden bank czy Urząd nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.

Pamiętaj, że zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie sposobów zabezpieczania się przed zagrożeniami to wiedza niezbędna każdemu użytkownikowi komputera, telefonu komórkowego czy też usług internetowych.

Więcej informacji na temat cyberbezpieczeństwa można znaleźć na następujących stronach:

[Baza wiedzy w serwisie gov.pl](#)

[CERT Polska](#)

[Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT](#)

[CSIRT NASK](#)

[CSIRT MON](#)

Metryczka

Podmiot udostępniający:	Prezydent Miasta Inowrocławia
Wytworzył:	Inspektor Ochrony Danych
Data wytworzenia:	01.09.2022

Opublikował w BIP:	Jarosław Osiński
Data opublikowania:	01.09.2022 08:11
Ostatnio zaktualizował:	Jarosław Osiński
Data ostatniej aktualizacji:	01.09.2022 08:19
Liczba wyświetleń:	365