

## Cyberbezpieczeństwo

Realizując zadania wynikające z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, przekazujemy informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.

Zgodnie z art. 2 pkt 4 ww. ustawy cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Najpopularniejsze zagrożenia w cyberprzestrzeni to:

- ataki socjotechniczne (np. phishing - nazwa pochodzi od password ("hasło") oraz fishing ("wędrowanie"). Istotą ataku jest próba pozyskania hasła użytkownika, które służy do logowania się na portalach społecznościowych bądź do serwisów. Po uzyskaniu dostępu, przestępca może wykraść dane osobowe i w tym celu dokonywać oszustw);

- kradzieże (wyłudzenia), modyfikacje lub niszczenie danych;

- kradzieże tożsamości;

- ataki z użyciem szkodliwego oprogramowania (wirusy, robaki, malware - to zbitka wyrazowa pochodząca od wyrażenia malicious software ("złośliwe oprogramowanie"). Wspólną cechą programów uznawanych za malware jest fakt, że wykonują działania na komputerze bez jego zgody i wiedzy użytkownika, na korzyść osoby postronnej. Działania tego typu obejmują np. dołączenie maszyny do sieci komputerów "zombie", które służą do ataku na organizacje rządowe, zdobywanie wirtualnych walut lub kradzieży danych osobowych i informacji niezbędnych do logowania do bankowości elektronicznej.);

- blokowanie dostępu do usług;

- spam (niechciane lub niepotrzebne wiadomości elektroniczne mogące zawierać odnośniki do szkodliwego oprogramowania).

Przykładowe sposoby zabezpieczenia się przed zagrożeniami:

- aktualizowanie systemu operacyjnego i aplikacji bez zbędnej zwłoki;

- instalacja i uaktualnianie oprogramowania przeciw wirusom i spyware. Najlepiej stosować ochronę w czasie rzeczywistym;

- aktualizacja oprogramowania antywirusowego oraz bazy danych wirusów;

- sprawdzanie plików pobranych z Internetu za pomocą programu antywirusowego;

- pamiętanie o uruchomieniu firewalla;

- nieotwieranie plików nieznanego pochodzenia;

- korzystanie ze stron banków, poczty elektronicznej czy portali społecznościowych, które mają ważny certyfikat bezpieczeństwa;

- regularne skanowanie komputera i sprawdzanie procesów sieciowych;

- nieużywanie niesprawdzonych programów zabezpieczających;

- regularne wykonywanie kopii zapasowych ważnych danych;

- nieodwiedzanie stron, które oferują niesamowite atrakcje (darmowe filmiki, muzykę, albo łatwy zarobek) - często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia;

- niezostawianie danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie ma się absolutnej pewności, że nie są one widoczne dla osób trzecich oraz nie wysyłanie w wiadomościach e-mail ważnych poufnych danych w formie otwartego tekstu;

- pamiętanie, że żaden bank czy Urząd nie wysyła e-maili do swoich klientów/interesantów z

prośbę o podanie hasła lub loginu w celu ich weryfikacji.

Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie sposobów zabezpieczania się przed zagrożeniami to wiedza niezbędna każdemu użytkownikowi komputera, smartphona czy usług internetowych.

Zachęcamy do regularnego zapoznawania się z treściami dotyczącymi cyberbezpieczeństwa zawartymi m.in. na stronach: Ministerstwa Cyfryzacji czy państwowego instytutu badawczego NASK.

## Metryczka

<b>Wytworzył:</b>	Maria Wojcińska
<b>Data utworzenia:</b>	17.05.2022
<b>Opublikował w BIP:</b>	Aneta Witkowska
<b>Data opublikowania:</b>	17.05.2022 11:03
<b>Liczba wyświetleń:</b>	137