Zagrożenia w cyberprzestrzeni

Realizując zadania, wynikające z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa, przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skutecznie stosować sposoby zabezpieczania się przed tymi zagrożeniami.

Cyberbezpieczeństwo, zgodnie z art. 2 pkt 4 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa, 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:

- ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki, itp.),

- kradzieże tożsamości, kradzieże mienia (wyłudzenia), modyfikacje bądź niszczenie danych,
- blokowanie dostępu do usług,

- spam (niechciane lub niepotrzebne wiadomości elektroniczne),
- ataki socjotechniczne (np. phishing, czyli wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję).

Sposoby zabezpieczenia się przed zagrożeniami:

- zainstaluj i używaj oprogramowania przeciw wirusom. Stosuj ochronę w czasie rzeczywistym,

- aktualizuj system operacyjny i aplikacje bez zbędnej zwłoki,
- aktualizuj oprogramowanie antywirusowe oraz bazy danych wirusów (dowiedz się czy twój program do ochrony przed wirusami posiada taką funkcję i czy robi to automatycznie),

- nie otwieraj plików nieznanego pochodzenia,
- nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu SSL,

- nie używaj niesprawdzonych programów zabezpieczających lub do publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony),
- skanuj komputer i sprawdzaj procesy sieciowe – 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,

- 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,
- sprawdzaj pliki pobrane z Internetu za pomocą skanera antywirusowego,

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

- nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich,
- pamiętaj o uruchomieniu firewalla na każdym urządzeniu,

- wykonuj kopie zapasowe ważnych danych.
Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie sposobów zabezpieczania się przed zagrożeniami, to wiedza niezbędna każdemu użytkownikowi komputera, smartphona czy też usług internetowych.

Dodatkowych informacji uzyskają Państwo na poniżej wskazanych stronach:

- zestaw porad bezpieczeństwa dla użytkowników komputerów prowadzony na witrynie internetowej CSIRT NASK – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym https://www.cert.pl/ouch/

- poradniki na witrynie internetowej Ministerstwa Cyfryzacji https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo

- publikacje z zakresu cyberbezpieczeństwa https://www.cert.pl/

- strona internetowa kampanii STÓJ. POMYŚL. POŁĄCZ. mającej na celu zwiększanie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni https://stojpomyslpolacz.pl/stp/