CYBERBEZPIECZEŃSTWO

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczenstwa 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 2018 r. poz. 1560).

Najpopularniejsze zagrożenia w cyberprzestrzeni:

- **Malware** - oprogramowanie, które wykonuje złośliwe zadanie na urządzeniu docelowym lub w sieci, np. uszkadza dane lub przejmuje system.
- **Phishing** - podszywanie się pod godną zaufania osobę lub instytucję - atak za pośrednictwem poczty e-mail polegający na nakłonieniu odbiorcy wiadomości e-mail do ujawnienia poufnych informacji lub pobrania złośliwego oprogramowania.
- **Spear Phishing** - bardziej wyrafinowana forma phishingu, w której napastnik podszywa się pod osobę bliską osoby atakowanej.
- **Atak typu "Man in the Middle" (MitM)** - atak ten wymaga, aby napastnik znalazł się między dwiema stronami, które się komunikują i był w stanie przechwytywać wysyłane informacje.
- **Trojan - (koń trojański)** - oprogramowanie, które podszywa się pod przydatne lub ciekawe dla użytkownika aplikacje, implementując szkodliwe, ukryte przed użytkownikiem różne funkcje (oprogramowanie szantażujące - ransomware, szpiegujące - spyware etc.).
- **Ransomware** - atak polegający na zaszyfrowaniu danych w systemie docelowym i zażądaniu okupu w zamian za umożliwienie użytkownikowi ponownego dostępu do danych. Często te dane są uszkadzane i nawet po opłaceniu nie da się ich odzyskać.
- **Atak DoS lub DDoS** - atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów i blokowanie dostępu do usług. DDoS atakuje z wielu miejsc równocześnie.
- **Ataki IoT w Internecie rzeczy** - atak polegający na przejmowaniu kontroli nad urządzeniami w sieci Internet: inteligentnymi domami, budynkami, sieciami energetycznymi, urządzeniami gospodarstwa domowego - przemysłu etc.).
- **Data Breaches (naruszenie danych)** - atak tego typu polega na kradzieży danych. Motywy naruszeń danych obejmują przestępstwa: (tj. kradzieży tożsamości, chęci zawstydzenia instytucji, szpiegostwo i inne).
- **Malware w aplikacjach telefonów.** Urządzenia mobilne są szczególnie podatne na ataki złośliwego oprogramowania, a efektem mogą być objawy: telefon zaczyna się przegrzewać, błyskawiczne wyczerpywanie baterii, wciąż wyskakujące reklamy, zwiększone użycie danych bez wyraźnego powodu, aplikacje, które bardzo często ulegają awariom a nawet bardzo wysoki rachunek za telefon.
- **Spam** (niechciane lub niepotrzebne wiadomości elektroniczne- zbyt wiele może zablokować dostęp do twojej poczty)

Sposoby zabezpieczenia się przed zagrożeniami:

- zainstaluj i używaj oprogramowania przeciw wirusom i spyware. Najlepiej stosuj aktywną 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 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, lub 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,
- stosuj odpowiednie, złożone hasło: min. 8 znakowe, cyfry, znaki szczególne oraz wielkie i małe litery, pamiętaj o ich zmianie**,**
- 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,

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

Wszelkie porady bezpieczeństwa dla użytkowników komputerów dostępne są na:

- witrynie internetowej CSIRT NASK – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym pod adresem: https://www.cert.pl/ouch;
- witrynie internetowej Ministerstwa Cyfryzacji pod adresem: https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo;
- publikacje za zakresu cyberbezpieczeństwa dostępne pod adresem: https://www.cert.pl;
- stronie internetowej kampanii STÓJ. POMYŚL. POŁĄCZ po adresem: https://stojpomyslpolacz.pl/stp/.

Kampania ma na celu zwiększanie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni.