Zagrożenia w cyberprzestrzeni

Realizując zadania, wynikające z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. 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 r. 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".

W sieci codziennie możemy stać się ofiarą różnych prób cyberataków, dlatego warto na bieżąco śledzić informacje na temat metod stosowanych przez oszustów.

Najpopularniejsze zagrożenia w cyberprzestrzeni to:

- ataki z użyciem szkodliwego oprogramowania (wirusy, trojany, robaki, itd.),
- kradzieże tożsamości, kradzieże mienia (wyłudzenia), modyfikacje bądź niszczenie danych,
- blokowanie dostępu do usług,
- spam (niechciane lub niepotrzebne wiadomości przesyłane drogą e-mailową, SMS-ową lub za pośrednictwem serwisów społecznych),
- ataki socjotechniczne (np. phishing czyli wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę, firmę z których usług korzystamy na co dzień).

Sposoby zabezpieczenia się przed zagrożeniami:

- zainstaluj i używaj oprogramowania przeciw wirusom, stosuj ochronę w czasie rzeczywistym,
- systematycznie aktualizuj oprogramowanie czyli instalację jego nowszych, poprawionych wersji – to podstawa i pozwalają chronić urządzenia i dbać o Twoje bezpieczeństwo w sieci,
- 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 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 zainstalować na komputerze pomimo dobrej ochrony – należy je wykryć i zlikwidować,
- nie podłączaj do swoich urządzeń USB niewiadomego pochodzenia,

- pamiętaj, że żaden bank czy urząd nie wysyła e-maili do swoich klientów 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, 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 – np. niech 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,
- pobieraj aplikacje tylko z oficjalnych, bezpiecznych źródeł, czyli ze sklepów z aplikacjami przeznaczonymi dla odpowiednich systemów operacyjnych. Pamiętaj o ograniczeniu uprawnień aplikacji. Nie podawaj swoich danych na nieznanych urządzeniach.
- chcąc zachować anonimowość online zwracaj również uwagę na publikowane treści m. in. w media społecznościowych (nigdy nie udostępniaj tam np. skanów dokumentów lub innych wrażliwych informacji),
- otrzymując wiadomość na wirtualną skrzynkę, zawsze bądź ostrożny. Uważaj na te oznaczone jako spam, nie klikaj w żadne podejrzane linki zawarte w ich treści i nie pobieraj załączników. Najpierw upewnij się, że nadawca rzeczywiście jest tym, za kogo się podaje i nie ma złych intencji.
- 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, telefonu czy też usług internetowych.

Każdego dnia powinniście Państwo pamiętać o zachowaniu bezpieczeństwa w sieci.

Dodatkowe informacje 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/),
- ,,ABC cyberbezpieczeństwa” - nowy poradnik przygotowany przez NASK-PIB (https://it-szkola.edu.pl/news,art,514).