CYBERBEZPIECZEŃSTWO

W związku z zadaniami wynikającymi z ustawy o krajowym systemie cyberbezpieczeństwa przedstawiamy Państwu podstawowe informacje dotyczące cyberbezpieczeństwa, zagrożeń i sposobów zabezpieczenia się przed nimi.

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. Wszelkie zdarzenia mające lub mogące mieć niekorzystny wpływ na cyberbezpieczeństwo nazywane są zagrożeniami lub incydentami.

Najpopularniejsze zagrożenia w cyberprzestrzeni to:

- ataki socjotechniczne (przykładowo phishing, czyli metoda polegająca na wyłudzaniu poufnych informacji przez podszycie się pod godną zaufania osobę lub instytucję);
- kradzieże (wyłudzenia), modyfikacje lub niszczenie danych;
- kradzieże tożsamości;
- ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki, itp.);
- 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 użytkowanie 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;
- nie otwieranie plików nieznanego pochodzenia;
- korzystanie ze stron banków, poczty elektronicznej czy portali społecznościowych, które mają ważny certyfikat bezpieczeństwa, chyba, że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna;
- regularne skanowanie komputera i sprawdzanie procesów sieciowych. Jeśli się na tym nie znasz poproś o sprawdzenie kogoś, kto się zna. Czasami złośliwe oprogramowanie nawiązujące własne połączenia z Internetem, wysyłając twoje hasła i inne prywatne dane do sieci. Może również zainstalować się na komputerze mimo dobrej ochrony;
- nie używanie niesprawdzonych programów zabezpieczających czy też do publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony);
- regularne wykonywanie kopii zapasowych ważnych danych;
- staranie się aby 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 zostawianie 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 żadnych poufnych danych w formie otwartego tekstu przykładowo dane powinny być zabezpieczone hasłem i zaszyfrowane. Hasło najlepiej przekazuj w sposób bezpieczny przy użyciu innego środka komunikacji;
- należy pamiętać, 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, smartphona czy też usług internetowych. Należy pamiętać, że najlepszym sposobem na ustrzeżenie się przed negatywnymi skutkami zagrożeń jest działalność zapobiegawcza.

Zachęcamy do zapoznania się z poniżej zawartymi treściami w celu uzyskania szczegółowych informacji dotyczących cyberbezpieczeństwa:

- Ministerstwo Cyfryzacji oraz baza wiedzy
- Zestaw porad bezpieczeństwa dla użytkowników komputerów CSIRT NASK – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym
- Publikacje z zakresu cyberbezpieczeństwa