Cyberbezpieczeństwo - baza wiedzy

Realizując zadania, wynikające z art. 9 ust. 1 pkt 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, dbając o bezpieczeństwo Państwa danych przygotowaliśmy zbiór porad bezpiecznego korzystania z sieci.

Cyberbezpieczeństwo, zgodnie z obowiązującymi przepisami oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami (art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa).

Najpopularniejsze zagrożenia w cyberprzestrzeni:

- ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki, itp.);
- kradzieże tożsamości, kradzieże (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 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 czy też 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;

- 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, smartphona czy też usług internetowych.

Aktualne i pełne informacje na temat cyberbezpieczeństwa znajdziemy na stronach:

- https://www.cert.pl/ouch/- zestaw porad bezpieczeństwa dla użytkowników komputerów prowadzony na witrynie internetowej CSIRT NASK – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym;
- https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo/ poradniki na witrynie internetowej Ministerstwa Cyfryzacji;
- https://www.cert.pl/ publikacje z zakresu cyberbezpieczeństwa.

Zgłaszanie incydentów bezpieczeństwa: https://incydent.cert.pl/