Cyberbezpieczeństwo

Realizując obowiązek wynikający z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560) zachęcamy Państwa do zapoznania się z informacjami, które przybliżą i pozwolą zrozumieć Państwu zagrożenia związane z cyberbezpieczeństwem.

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).

Do najpopularniejszych zagrożeń w cyberprzestrzeni możemy zaliczyć:

- Ataki z użycie szkodliwego oprogramowania,
- Kradzieże tożsamości
- Ataki mające na celu wyłudzenie lub zniszczenie danych,
- Blokada dostępu do usług,
- Niechciana poczta (SPAM),
- Socjotechnika,
- Phishing.

W celu ochrony przed zagrożeniami należy stosować zabezpieczenia:

- Używaj aktualnego oprogramowania antywirusowego - stosuj ochronę w czasie rzeczywistym, włącz aktualizacje automatyczne,
- Skanuj oprogramowaniem antywirusowym wszystkie urządzenia podłączane do komputera - pendrivy, płyty, karty pamięci,
- Aktualizuj system operacyjny i posiadane oprogramowanie,
- Nie otwieraj plików nieznanego pochodzenia,
- Wszystkie pobrane pliki skanuj programem antywirusowym,
- Nie korzystaj ze stron banków, poczty elektronicznej, które nie mają ważnego certyfikatu bezpieczeństwa,
- Cyklicznie skanuj komputer oprogramowaniem antywirusowym i sprawdzaj procesy sieciowe,
- Nie odwiedzaj stron oferujących darmowe filmy, muzykę albo łatwe pieniądze - najczęściej na takich stronach znajduje się złośliwe oprogramowanie,
- Nie podawaj swoich danych osobowych na stronach internetowych, co do których nie masz pewności, że nie są one widoczne dla osób trzecich,
- Zawsze weryfikuj adres nadawcy wiadomości e-mail,
- Zawsze zabezpieczaj hasłem lub szyfruj wiadomości e-mail zawierające poufne dane - hasło przekazuj innym sposobem komunikacji,
- Cyklicznie wykonuj kopie zapasowe ważnych danych,
- Zawsze miej włączoną - zaporę sieciową "firewall"
- Zwracaj uwagę na komunikaty wyświetlane na ekranie komputera.

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.

Warto również zapoznać się z informacjami poniżej:

1. STÓJ. POMYŚL. POŁĄCZ. jest polską wersją międzynarodowej kampanii STOP. THINK. CONNECT.™, mającej na celu podnoszenie poziomu świadomości społecznej w obszarze cyberbezpieczeństwa poprzez informowanie o zagrożeniach i sposobach radzenia sobie z nimi, promowanie zachowań służących poprawie bezpieczeństwa internautów, ich rodzin i otoczenia. ***Materiały do pobrania***
2. OUCH! To cykliczny, darmowy zestaw porad bezpieczeństwa dla użytkowników komputerów. Każde wydanie zawiera krótkie, przystępne przedstawienie wybranego zagadnienia z bezpieczeństwa komputerowego wraz z listą wskazówek jak można chronić siebie, swoich najbliższych i swoją organizację.
3. Zespół CERT Polska działa w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej) - państwowego instytutu badawczego prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne. ***CERT*** to pierwszy powstały w Polsce zespół reagowania na incydenty, zagrożenia w sieciach komputerowych. Zapoznaj się z rocznymi raportami z działalności CERT Polska zawierającymi zebrane dane o zagrożeniach dla polskich użytkowników Internetu, w tym również opisy najciekawszych nowych zagrożeń i podatności.

Podmioty oraz firmy zajmujące się cyberbezpieczeństwem:

- Ministerstwo Cyfryzacji,
- CERT Polska,
- CSIRT GOV,
- CSIRT NASK,
- CSIRT GOV,
- Niebezpiecznik.pl,
- CyberDefence24,
- Cyberrescue,