

Cyberbezpieczeństwo

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skutecznie stosować sposoby zabezpieczenia się przed tymi zagrożeniami. Cyberbezpieczeństwo 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 2018r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369 z późn.zm)).

Do najpopularniejszych zagrożeń w cyberprzestrzeni należą:

- ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki, itp.),
- kradzieże tożsamości,
- kradzieże (wyłudzenia), fałszowanie bądź niszczenie danych,
- blokowanie dostępu do usług,
- spam (niechciane lub niepotrzebne wiadomości elektroniczne),
- ataki socjotechniczne (np. phishing, czyli wyłudzenie poufnych informacji, np. danych do logowania) poprzez podszywanie się pod instytucję lub osobę godną zaufania, np. urzędy, banki, portale społecznościowe, znajomych).

Niektóre sposoby zabezpieczenia się przed zagrożeniami:

- Używaj tylko silnych, indywidualnych dla każdego systemu haseł i nie udostępniaj ich nikomu.
- Zainstaluj i używaj oprogramowania antywirusowe. Najlepiej stosuj 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 internetowych (zwłaszcza 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 do publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony).
- Regularnie 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 programu antywirusowego.
- Unikaj odwiedzania stron, które oferują wyjątkowe atrakcje (darmowe filmiki, muzykę, łatwy zarobek, cudowną dietę) – 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 (np. danych osobowych, logowania, karty kredytowej) w formie otwartego tekstu – powinny być zabezpieczone hasłem i zaszyfrowane – hasło przekazuj w sposób bezpieczny, tj. innym kanałem niż dane.
- Pamiętaj o uruchomieniu firewalla.
- Wykonuj kopie zapasowe ważnych danych.
- Pamiętaj, że żaden bank czy Urząd nie wysyła e-maili do swoich klientów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.
- Zwracaj uwagę na komunikaty pojawiające się na ekranie i nigdy nie ignoruj ostrzeżeń dotyczących bezpieczeństwa.

Więcej wskazówek na temat zabezpieczenia danych można znaleźć pod linkami:

- [Bezpieczeństwo w sieci](#)
- [Cyberbezpieczeństwo od A do Z](#)

Jeżeli chcesz anonimowo i łatwo zgłosić nielegalne i szkodliwe treści, na które natknąłeś się w sieci możesz zrobić to wchodząc na stronę:

[Zgłaszanie nielegalnych i szkodliwych treści](#)