Realizując zadania wynikające z ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa przekazujemy Państwu podstawowe informacje dotyczące cyberbezpieczeństwa , zagrożeń i sposobów zabezpieczania się przed nimi.

Cyberbezpieczeństwo, zgodnie z art. 2 pkt 4 ustawy 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”*.

Do najpopularniejszych <u>zagrożeń</u> w cyberprzestrzeni należą:

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

Przykładowe sposoby <u>zabezpieczenia</u> przed potencjalnymi zagrożeniami:

- Używanie tylko silnych, indywidualnych dla każdego systemu haseł i nie udostępnianie ich nikomu.
- Zainstalowanie i używanie oprogramowania antywirusowego. Stosowanie ochrony w czasie rzeczywistym!
- Aktualizowanie oprogramowania antywirusowego oraz bazy danych wirusów (dowiedz się czy twój program do ochrony przed wirusami posiada taką funkcję i robi to automatycznie).
- Regularne aktualizowanie systemu operacyjnego i aplikacji.
- Nie otwieranie plików nieznanego pochodzenia.
- Nie korzystanie ze stron internetowych (zwłaszcza ze stron banków, poczty elektronicznej czy portali społecznościowych), które nie mają ważnego certyfikatu SSL, chyba że masz stuprocentową pewność z innego źródła, że dana strona jest bezpieczna.
- Nie używanie niesprawdzonych programów zabezpieczających.
- Należy regularnie skanować komputer i sprawdzać zachodzące procesy sieciowe – jeśli się na tym nie znasz, poproś o sprawdzenie kogoś doświadczonego w tym zakresie.
- Sprawdzanie plików pobranych z Internetu za pomocą programu antywirusowego.
- Unikanie odwiedzania stron, które oferują wyjątkowe atrakcje (darmowe filmiki, darmową muzykę czy łatwy zarobek) – często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia.
- Nie wpisywanie danych osobowych w niesprawdzonych serwisach.
- Nie wysyłanie w wiadomościach e-mail żadnych poufnych danych (np. danych osobowych, danych logowania, skanu karty kredytowej) w formie otwartego tekstu – powinny być zabezpieczone hasłem i zaszyfrowane – hasło przekazujemy w sposób bezpieczny, tj. innym kanałem niż dane.
- Pamiętanie o uruchomieniu firewalla.
- Wykonywanie kopii zapasowych ważnych danych.

- Należy pamiętać, iż żaden bank czy urząd nie wysyła e-maili do swoich klientów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.
- Zwracanie uwagi na komunikaty pojawiające się na ekranie oraz nie ignorowanie ostrzeżeń dotyczących bezpieczeństwa.

Więcej informacji na temat zabezpieczeń w cyberprzestrzeni można znaleźć pod linkiem:

https://cert.pl/

https://cert.pl/ouch/ - porady bezpieczeństwa

https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo