CYBERBEZPIECZEŃSTWO

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa (art. 22 ust. 1 pkt 4) przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak przeciwdziałać tym zagrożeniom.

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 2018r. o krajowym systemie cyberbezpieczeństwa.

Najpopularniejsze zagrożenia w cyberprzestrzeni:

1. Ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki itp.).
2. Kradzieże tożsamości, kradzieże (wyłudzenia), modyfikacje bądź niszczenie danych.
3. Blokowanie dostępu do usług.
4. Spam (niechciane lub niepotrzebne wiadomości elektroniczne).
5. Ataki socjotechniczne (np. phishing, czyli wyłudzenie informacji przez podszywanie się pod godną zaufania osobę lub instytucję).

Sposoby zabezpieczenia się przed zagrożeniami:

1. Stosuj zasadę ograniczonego zaufania do odbieranych wiadomości e-mail, sms, stron internetowych nakłaniających do podania danych osobowych, osób podających się za przedstawicieli firm, instytucji, którzy żądają podania danych autoryzacyjnych lub nakłaniających do instalowania aplikacji zdalnego dostępu.
2. Zainstaluj i używaj programu antywirusowego zabezpieczającego przed zagrożeniami typu: wirusy, robaki, trojany, niebezpieczne aplikacje itp.
3. Aktualizuj system operacyjny, aplikacje użytkowe i programy antywirusowe.
4. Instaluj aplikacje tylko ze znanych i zaufanych źródeł.
5. Nie otwieraj plików nieznanego pochodzenia.
6. Szyfruj dane poufne wysyłane poczta elektroniczną.
7. Regularnie zmieniaj hasła.
8. Nie udostępniaj nikomu swoich haseł.
9. Wykonuj kopie bezpieczeństwa.
10. Skanuj podłączone urządzenia zewnętrzne.
11. Unikaj korzystania z otwartych sieci Wi-Fi.

12. Podając poufne dane sprawdź czy strona internetowa posiada certyfikat SSL. Protokół SSL to standard zabezpieczeni przesyłanych danych pomiędzy przeglądarką a serwerem.
13. Pracuj na najwyższych możliwych uprawnieniach użytkownika.

Więcej informacji i porad o cyberbezpieczeństwie uzyskasz na stronach:

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

https://www.cert.pl/publikacje/

https://akademia.nask.pl/publikacje/

https://stojpomyslpolacz.pl/