

Z obowiązku wynikającego z ustawy z dnia 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369) chcielibyśmy przekazać informacje, które pozwolą Państwu zrozumieć zagrożenia występujące w cyberprzestrzeni jak i poradzić jak skutecznie stosować sposoby zabezpieczania się przed tego typu zagrożeniami.

Do najczęstszych zagrożeń związanych z cyberprzestrzenią, z którymi mogą się Państwo zetknąć, należą:

- ataki używające szkodliwego oprogramowania (wirusy, malware ,robaki, itp.),
- ataki typu phishing, czyli wyłudzenie poufnych informacji poprzez podszywanie się pod godną zaufania instytucję lub osobę).
- spam (niechciane / niepotrzebne wiadomości elektroniczne),
- kradzieże tożsamości,
- blokowanie dostępu do usług internetowych (ataki typu DDOS).

Sposoby zabezpieczenia się przed zagrożeniami:

- Instalacja i używanie oprogramowania przeciw wirusom i programom śledzących (antywirusy). Zaleca się ochronę w czasie rzeczywistym.
- Aktualizacje bazy danych wirusów.
- Częste aktualizuje oprogramowania na komputerze a w szczególności oprogramowania internetowych przeglądarek.
- Oprogramowanie to może zawierać stworzone przez hakerów wirusy, które pomogą im w opanowaniu naszego komputera, wyłudzeniu danych itp.
- Nie otwieraj wiadomości a w szczególności dołączonych do nich załączników z nieznanych źródeł, zazwyczaj w takich załącznikach ukryte jest złośliwe oprogramowanie.
- Pamiętaj o uruchomieniu firewalla.
- Pamiętaj o regularnej zmianie hasła do komputera oraz dostępu do kont internetowych. Hasła powinny być trudne składające się z dużych i małych liter oraz znaków specjalnych.
- Nie zaleca się instalacji na komputerze nielegalnego oprogramowania.
- Nie otwieraj plików, których pochodzenia nie znamy albo nie jesteśmy pewni.
- Pliki pobrane z Internetu należy przed ich instalacją przeskanować programem antywirusowym w celu wykrycie ewentualnego zagrożenia.
- Nie korzystaj ze stron internetowych banków, portali społecznościowych, czy poczty e-mail, które nie posiadają ważnego certyfikatu SSL, chyba, że mamy 100% pewność, że strona taka jest bezpieczna.
- Płatności wykonuj tylko z własnego komputera lub telefonu. Nie korzystaj do tych celów z publicznej sieci Wi-fi
- Pamiętaj, że żaden bank czy Urząd nie wysyła e-maili do swoich klientów prosząc o podanie hasła / loginu w celu weryfikacji.
- 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 poufnych danych w formie otwartego tekstu.
- Wykonuj kopie zapasowe oprogramowania i innych danych.

Podmiot publikujący Urząd Gminy

Wytworzył Michał Kocunik - Informatyk 2022-08-24

Publikujący Michał Kocunik - Informatyk 2022-08-24 14:12

Modyfikacja Michał Kocunik - Informatyk 2022-08-24 14:15