Cyberbezpieczeństwo

Departament Informatyki Data publikacji: 13.03.2023 Data modyfikacji: 18.12.2023

Zgodnie z zapisami ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa zachęcamy do zapoznania się z materiałami i informacjami, które przybliżają i pozwalają zrozumieć zagrożenia związane z cyberbezpieczeństwem, a także zawierają wskazówki w zakresie stosowania skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.

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.

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.

Pamiętaj, że żaden 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, smartfona czy też portali internetowych.

Warto również zapoznać się z informacjami i poradnikami zamieszczonymi na stronach:

- https://stojpomyslpolacz.pl/
- https://cert.pl/
- https://akademia.nask.pl/
- https://www.saferinternet.pl/
- https://www.gov.pl/web/baza-wiedzy/aktualnosci

Rekomendacje dla obywateli

- Zapoznaj się z poradnikiem dotyczącym bezpieczeństwa skrzynek pocztowych i kont w mediach społecznościowych oraz zastosuj się do jego rekomendacji.
- Bądź wyczulony na sensacyjne informacje, w szczególności zachęcające do natychmiastowego podjęcia jakiegoś działania. Weryfikuj informacje w kilku źródłach. Upewnij się, że informacja jest prawdziwa przed podaniem jej dalej w mediach społecznościowych. Jeśli masz jakieś wątpliwości, wstrzymaj się.
- Uważaj na wszelkie linki w wiadomościach mailowych i SMS-ach, zwłaszcza te sugerujące podjęcie jakiegoś działania, np. konieczność zmiany hasła, albo podejrzaną aktywność na koncie. Obserwowaliśmy w przeszłości tego typu celowane ataki na prywatne konta, gdzie celem było zdobycie informacji zawodowych.
- Upewnij się, że posiadasz kopię zapasową wszystkich ważnych dla siebie plików i potrafisz je przywrócić w przypadku takiej potrzeby.

- **Zgłaszaj każdą podejrzaną aktywność przez formularz na stronie incydent.cert.pl lub mailem na cert@cert.pl. Podejrzane SMS-y prześlij bezpośrednio na numer 799 448 084. Rekomendujemy zapisanie go w kontaktach.**

Materiały

- Ustawa o Krajowym Systemie Cyberbezpieczeństwa (pdf, 1,28 MB)
- Najczęściej zgłaszane incydenty do CERT Polska w latach 2017-2020 (pdf, 1,15 MB)
- Przykłady zagrożeń (pdf, 1,40 MB)
- Poradnik dotyczący bezpieczeństwa skrzynek pocztowych i kont w mediach społecznościowych (pdf, 418 KB)