Cyberbezpieczeństwo

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa 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. 22 pkt. 4. ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz.U. z 2024 r .poz. 1077).

Co to jest **Incydent cyberbezpieczeństwa?** To pojedyncze zdarzenie lub seria zdarzeń, które mają lub mogą mieć negatywny wpływ na cyberbezpieczeństwo. Dotyczy to naruszenia poufności, integralności lub dostępności informacji

i zasobów cyfrowych. Innymi słowy, jest to sytuacja, w której doszło do naruszenia zasad bezpieczeństwa systemów informatycznych.

Najpopularniejsze przykłady incydentów cyberbezpieczeństwa i zagrożeń w cyberprzestrzeni:

- Ataki złośliwego oprogramowania (malware).
- Phishing i ataki socjotechniczne.
- Ataki DDoS (Distributed Denial of Service).
- Nieautoryzowany dostęp.
- Wycieki danych.
- Naruszenia integralności danych.
- Kradzież lub utrata sprzętu.
- Kradzieże tożsamości.
- Luki w oprogramowaniu (exploitowanie podatności).
- Spam (niechciane lub niepotrzebne wiadomości elektroniczne).
- Blokowanie dostępu do usług.

Sposoby zabezpieczenia się przed zagrożeniami:

1. Instaluj aplikacje tylko ze znanych i zaufanych źródeł.
2. Nie ujawniaj danych osobowych w tym danych autoryzacyjnych, dopóki nie ustalisz, czy rozmawiasz z osobą uprawnioną do przetwarzania Twoich danych.
3. 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.

4. Chroń swój komputer, urządzenie mobilne programem antywirusowym zabezpieczającym przed zagrożeniami typu: wirusy, robaki, trojany, niebezpieczne aplikacje (typu ransomware, adware, keylogger, spyware, dialer), phishing, narzędziami hakerskimi, backdoorami, rootkitami, bootkitami i exploitami.
5. Bezpieczeństwo wiadomości tekstowych (SMS) - sprawdź adres url z którego domyślnie dany podmiot/instytucja wysyła do Ciebie smsy, cyberprzestępca może podszyć się pod dowolną tożsamość (odpowiednio definiując numer lub nazwę), otrzymując smsa, w którym cyberprzestępca podszywa się pod numer zapisany w książce adresowej, telefon zidentyfikuje go jako nadawcę wiadomości sms.
6. Aktualizuj system operacyjny, aplikacje użytkowe, programy antywirusowe. Brak aktualizacji zwiększa podatność na cyberzagrożenia. Hakerzy, którzy znają słabości systemu/aplikacji, mają otwartą furtkę do korzystania z luk w oprogramowaniu.
7. Każdy e-mail można sfałszować, sprawdź w nagłówku wiadomości pole Received: from (ang. otrzymane od) w tym polu znajdziesz rzeczywisty adres serwera nadawcy.
8. Nie otwieraj wiadomości e-mail i nie korzystaj z przesłanych linków od nadawców, których nie znasz.
9. Jeśli na podejrzanej stronie podałeś swoje dane do logowania lub jeżeli włamano się na Twoje konto e-mail –

jak najszybciej zmień hasło.

10. Porównaj adres konta e-mail nadawcy adresem w polu „From” oraz „Reply to” – różne adresy w tych polach mogą wskazywać na próbę oszustwa.
11. Szyfruj dane poufne wysyłane pocztą elektroniczną.
12. Logowanie do e-usług publicznych, bankowości elektronicznej bez aktualnego (wspieranego przez producenta) systemu operacyjnego to duże ryzyko.
13. Korzystaj z różnych haseł do różnych usług elektronicznych.
14. Tam, gdzie to możliwe (konta społecznościowe, konto email, usługi e-administracji, usługi finansowe) stosuj dwuetapowe uwierzytelnienie za pomocą np. sms, pin, aplikacji generującej jednorazowe kody autoryzujące, tokenów, klucza fizycznego.
15. Nie udostępniaj nikomu swoich haseł.
16. Regularnie zmieniaj hasła.
17. Pracuj na najniższych możliwych uprawnieniach użytkownika.
18. Wykonuj kopie bezpieczeństwa.
19. Skanuj podłączane urządzenia zewnętrzne.
20. Skanuj regularnie wszystkie dyski twarde zainstalowane na Twoim komputerze.
21. Kontroluj uprawnienia instalowanych aplikacji.
22. Unikaj z korzystania otwartych sieci Wi-Fi.
23. Podając poufne dane sprawdź czy strona internetowa posiada certyfikat SSL. Protokół SSL to standard kodowania (zabezpieczania) przesyłanych danych

pomiędzy przeglądarką a serwerem.

24. Zadbaj o bezpieczeństwo routera (ustal silne hasło do sieci WI-FI, zmień nazwę sieci WI-Fi, zmień hasło do panelu administratora, ustaw poziom zabezpieczeń połączenia z siecią Wi-FI np. WPA2 i wyższe, aktualizuj oprogramowanie routera, wyłącz funkcję WPS).
25. Szyfruj dyski twarde komputera oraz pamięci przenośne.

Zgłaszanie incydentów bezpieczeństwa:

https://incydent.cert.pl/

Więcej informacji porad o cyberbezpieczeństwie uzyskasz na stronach:

- https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo
- https://www.cert.pl/publikacje/
- https://akademia.nask.pl/publikacje/
- https://stojpomyslpolacz.pl/
- https://dyzurnet.pl/

Metryczka

Odpowiedzialny za treść:	Barbara Kurasińska
Data wytworzenia:	14.05.2025
Opublikował w BIP:	Daniel Skrobacki
Data opublikowania:	14.05.2025 08:43
Liczba wyświetleń:	28