

Cyberbezpieczeństwo

Treść

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak przeciwdziałać tymi zagrożeniom.

1. Stosuj zasadę ograniczonego zaufania do odbieranych wiadomości email, 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. Nie ujawniaj danych osobowych w tym danych autoryzacyjnych dopóki nie ustalisz czy rozmawiasz z osobą uprawnioną do przetwarzania Twoich danych.
3. Instaluj aplikacje tylko ze znanych i zaufanych źródeł.
4. Nie otwieraj wiadomości e-mail i nie korzystaj z przesłanych linków od nadawców, których nie znasz.
5. Każdy email można sfałszować, sprawdź w nagłówku wiadomości pole Received: from (ang. otrzymane od) w tym polu znajdziesz rzeczywisty adres serwera nadawcy.
6. Porównaj adres konta email nadawcy adresem w polu „From” oraz „Reply to” – różne adresy w tych polach mogą wskazywać na próbę oszustwa.
7. Szyfruj dane poufne wysyłane pocztą elektroniczną.
8. 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.

9. Jeśli na podejrzanej stronie podałeś swoje dane do logowania lub jeżeli włamano się na Twoje konto email – jak najszybciej zmień hasło.

10. Chroń swój komputer, urządzenie mobilne programem antywirusowym zabezpieczającym przed zagrożeniami typu; wirusy, robaki, trojany, robakami, niebezpiecznymi aplikacjami typu ransomware, adware, keylogger, spyware, dialer, phishing, narzędziami hakerskimi, backdoorami, rootkitami, bootkitami i exploitami.

11. 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.

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. Regularnie zmieniaj hasła.

16. Nie udostępniaj nikomu swoich haseł.

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 przeglądarka 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, aktywuj funkcję Gościnną Sieć Wi-Fi „Guest Network”).
25. Szyfruj dyski twarde komputera, przenośne.

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/>

Zgłaszanie incydentów bezpieczeństwa: <https://incydent.cert.pl/>