Cyberbezpieczeństwo

Cyberbezpieczeństwoto odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy (zgodnie z art. 2 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa).

Zgodnie z art. 22 ust. 1 pkt 4 wyżej wymienionej ustawy podmiot publiczny zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej.

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. 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 w tym polu znajdziesz rzeczywisty adres serwera nadawcy.
6. Porównaj adres konta e-mail 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 e-mail – jak najszybciej zmień hasło.
10. Chroń swój komputer, urządzenie mobilne programem antywirusowym zabezpieczającym przez zagrożeniami typu: wirusy, robaki, trojany, niebezpieczne aplikacje (ransomware, adware, keylogger, spyware, dialer, phishing), narzędziami hakerskimi, backdoorami,rootkitami, bootkitami i exploitami.
11. Aktualizuj swój system operacyjny, aplikacje użytkowe, programy antywirusowe. Brak aktualizacji zwiększa podatność na cyberzagrożenia.
12. Logowanie do e-usług publicznych, bankowości elektronicznej bez aktualnego (wspieranego przez producenta) systemu operacyjnego także zwiększa ryzyko cyberzagrożeń.
13. Korzystaj z różnych haseł do różnych usług elektronicznych.
14. Tam gdzie to możliwe stosuj dwuetapowe uwierzytelnienie za pomocą np. sms, pin, itp.
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 na Twoim komputerze.
21. Kontroluj uprawnienia instalowanych aplikacji.
22. Unikaj korzystania z otwartych sieci Wi-Fi.
23. Podając poufne dane sprawdź czy strona internetowa posiada certyfikat SSL. Protokół SSL to standard kodowania 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, aktywuj funkcję Gościnna Sieć Wi-Fi „Guest Network".
25. Szyfruj dyski twarde komputera, dyski przenośne.
26. Pamiętaj, aby chronić swój telefon przed osobami trzecimi – stosuj blokadę ekranu oraz pin do karty sim.

Więcej informacji na tematcyberbezpieczeństwia można uzyskać:
https://uodo.gov.pl/pl/138/2634
https://www.gov.pl/web/baza-wiedzy/aktualnosci
https://cert.pl/ouch/
https://www.cert.pl/
Zgłaszanie incydentów bezpieczeństwa:
https://incydent.cert.pl/