Cyberbezpieczeństwo

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. 2 pkt.4) Ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018r.poz. 1560).

Najpopularniejsze zagrożenia w cyberprzestrzeni:

- Ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki itp.),
- Kradzieże tożsamości,
- Kradzieże (wyłudzenia), modyfikacje bądź niszczenie danych,
- Blokowanie dostępu do usług,
- Spam (niechciane lub niepotrzebne wiadomości elektroniczne),
- Ataki socjotechniczne (np. phishing, czyli wyłudzenie informacji przez podszywanie się pod godną zaufania osobę lub instytucję.

Sposoby zabezpieczenia się przed zagrożeniami:

- 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.
- Nie ujawniaj danych osobowych w tym danych autoryzacyjnych dopóki nie ustalisz czy rozmawiasz z osobą uprawnioną do przetwarzania Twoich

danych.

- Instaluj aplikacje tylko ze znanych i zaufanych źródeł.
- Nie otwieraj wiadomości e-mail i nie korzystaj z przesłanych linków od nadawców, których nie znasz.
- Każdy e-mail można sfałszować, sprawdź w nagłówku wiadomości pole Received: from (ang. otrzymane od) w tym polu znajdziesz rzeczywisty adres serwera nadawcy.
- Porównaj adres konta e-mail nadawcy adresem w polu „From” oraz „Reply to” – różne adresy w tych polach mogą wskazywać na próbę oszustwa.
- Szyfruj dane poufne wysyłane pocztą elektroniczną.
- 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.
- Jeśli na podejrzanej stronie podałeś swoje dane do logowania lub jeżeli włamano się na Twoje konto e-mail – jak najszybciej zmień hasło.
- 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.
- 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.
- Logowanie do e-usług publicznych, bankowości elektronicznej bez aktualnego (wspieranego przez producenta) systemu operacyjnego to duże ryzyko.
- Korzystaj z różnych haseł do różnych usług elektronicznych.
- 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.
- Regularnie zmieniaj hasła.
- Nie udostępniaj nikomu swoich haseł.
- Pracuj na najniższych możliwych uprawnieniach użytkownika.
- Wykonuj kopie bezpieczeństwa.

- Skanuj podłączane urządzenia zewnętrzne.
- Skanuj regularnie wszystkie dyski twarde zainstalowane na Twoim komputerze.
- Kontroluj uprawnienia instalowanych aplikacji.
- Unikaj z korzystania otwartych sieci Wi-Fi.
- Podając poufne dane sprawdź czy strona internetowa posiada certyfikat SSL. Protokół SSL to standard kodowania (zabezpieczania) przesyłanych danych pomiędzy przeglądarka a serwerem.
- 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”.
- 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/