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. Wszelkie zdarzenia mające lub mogące mieć niekorzystny wpływ na cyberbezpieczeństwo nazywane są zagrożeniami lub incydentami.

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 wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję).

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, które żądają podania danych autoryzacyjnych lub nakłaniają 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 linków przesłanych od nadawców, których nie znasz.
5. Każdy e-mail można bardzo łatwo sfałszować. To, że w polu nadawca jest znany ci adres wcale nie oznacza, że ten nadawca go wysłał.
6. Porównaj w źródle wiadomości adres konta e-mail nadawcy z adresem w polu „*From" oraz „Reply to"* – różne adresy w tych polach mogą wskazywać na próbę oszustwa.
7. Szyfruj dane poufne wysyłane pocztą elektroniczną. Hasło do odszyfrowania najlepiej wyślij inną drogą (np. sms'em).
8. Bezpieczeństwo wiadomości tekstowych (SMS) - sprawdź adres url, z którego domyślnie dany podmiot/instytucja wysyła do Ciebie sms-y, cyberprzestępca może podszyć się pod dowolną tożsamość (odpowiednio definiując numer lub nazwę), otrzymując sms-a, w którym cyberprzestępca podszywa się pod numer zapisany w książce adresowej, telefon zidentyfikuje jako zaufanego 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 przed zagrożeniami typu: wirusy, robaki, trojany, niebezpieczne aplikacje (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 (2FA) 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 w systemach na najniższych możliwych uprawnieniach użytkownika.
18. Wykonuj kopie bezpieczeństwa.
19. Skanuj podłączane urządzenia zewnętrzne.
20. Skanuj regularnie wszystkie dyski twarde zainstalowane w Twoim komputerze.
21. Kontroluj uprawnienia instalowanych aplikacji.
22. Unikaj korzystania z otwartych (publicznych) sieci Wi-Fi.
23. Podając poufne dane sprawdź czy strona internetowa posiada certyfikat SSL. Protokół SSL to standard szyfrowania (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 domyślne 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. Pamiętaj, że żaden bank czy 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 skutecznych sposobów zabezpieczania się przed tymi zagrożeniami to wiedza niezbędna każdemu użytkownikowi komputera, smartphona czy usług internetowych.