Cyberhigiena

Informacje dotyczące zagrożeń cyberbepieczeństwa i stosowania skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.

Realizując obowiązek wynikający z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbepieczeństwa, informujemy, że do najpopularniejszych zagrożeń w cyberprzestrzeni należą:

- kradzieże tożsamości;
- wyłudzenia danych uwierzytelniających (loginów, haseł);
- kradzieże, 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;
- ataki z użyciem szkodliwego oprogramowania (np. malware, wirusy, robaki).

Sposoby zabezpieczenia przed ww. zagrożeniami, to w szczególności:

- stosuj zasady 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 jedynie ze znanych i zaufanych źródeł;
- nie otwieraj wiadomości e-mail i nie korzystaj z przesłanych linków od nadawców, których nie znasz;
- nie otwieraj plików nieznanego pochodzenia, a wszystkie pobrane pliki skanuj programem antywirusowym;
- szyfruj dane poufne wysyłane pocztą elektroniczną (szczególne, które w razie nieuprawnionego ujawnienia mogą narazić na stratę Ciebie lub osobę do której, lub o której piszesz);
- sprawdzaj adres url, z którego domyślnie dany podmiot (instytucja) wysyła do Ciebie smsy – cyberprzestępca może podszyć się pod dowolną tożsamość (odpowiednio definiując numer lub nazwę);
- jeśli na podejrzanej stronie podałeś swoje dane do logowania lub jeżeli włamano się na Twoje konto e-mail – jak najszybciej zmień hasło;
- używaj aktualnego oprogramowania antywirusowego – stosuj ochronę w czasie rzeczywistym, włącz aktualizacje automatyczne, skanuj oprogramowaniem antywirusowym wszystkie urządzenia podłączane do komputera – pendrive, płyty, karty pamięci;
- aktualizuj system operacyjny, aplikacje użytkowe, programy antywirusowe – brak aktualizacji zwiększa podatność na cyberzagrożenia;
- nie korzystaj ze stron banków, poczty elektronicznej, które nie mają ważnego certyfikatu bezpieczeństwa;
- pamiętaj, że żaden bank czy urząd nie wysyła e-maili do swoich klientów z prośbą o podanie hasła lub loginu w celu ich weryfikacji;
- nie odwiedzaj stron oferujących darmowe filmy, muzykę albo „łatwe” pieniądze – najczęściej na takich stronach znajduje się złośliwe oprogramowanie;
- zwracaj uwagę na nazwę aplikacji, czy nie ma w niej błędów lub literówek – jeśli tak, może być fałszywa i podszywać się pod oficjalną wersję;
- zawsze weryfikuj adres nadawcy wiadomości e-mail;
- systematycznie wykonuj kopie zapasowe ważnych danych;
- zwracaj uwagę na komunikaty oraz czytaj treści wyświetlane na ekranie komputera;
- pamiętaj, aby chronić swój telefon przed osobami trzecimi – stosuj blokadę ekranu;
- nigdy nie instaluj aplikacji, do których namawiają cię nieznane osoby trzecie;
- korzystaj z różnych haseł do różnych usług elektronicznych;

- jeżeli masz taką możliwość (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;
- twórz silne hasła;
- nie udostępniaj nikomu swoich haseł;
- pracuj na najniższych możliwych uprawnieniach użytkownika;
- unikaj z korzystania otwartych sieci Wi-Fi;
- podając poufne dane sprawdź, czy strona internetowa posiada certyfikat SSL (SSL to standard kodowania 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 lub wyższy, aktualizuj oprogramowanie routera, wyłącz funkcję WPS, aktywuj funkcję Gościnna Sieć Wi-Fi „Guest Network”.

Szerszy zakres wiedzy o aktualnych zagrożeniach cyberbepieczeństwa i stosowania skutecznych sposobów zabezpieczania się przed tymi zagrożeniami dostępne są na stronach:

https://cert.pl/

https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo

Życzymy bezpiecznego korzystania z Internetu i komunikacji elektronicznej!