

Zgodnie z art. 22 ust. 1 pkt 4 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej jako „Ustawa”) przekazujemy Państwu niezbędne informacje w przedmiocie zagadnienia jakim jest cyberbezpieczeństwo.

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 2018 r. o krajowym systemie cyberbezpieczeństwa.

Najpopularniejsze zagrożenia w cyberprzestrzeni:

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

Sposoby zabezpieczenia się przed zagrożeniami:

- Zainstaluj i używaj oprogramowania antywirusowego. Stosuj ochronę w czasie rzeczywistym;
 - Aktualizuj na bieżąco system operacyjny i zainstalowane aplikacje;
 - Aktualizuj oprogramowanie antywirusowe oraz bazy danych wirusów (dowiedz się czy twój program do ochrony przed wirusami posiada taką funkcję i robi to automatycznie);
 - Nie otwieraj plików nieznanego pochodzenia;
 - Nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu SSL;
 - Nie używaj niesprawdzonych programów zabezpieczających czy też do publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony);
 - Skanuj komputer i sprawdzaj procesy sieciowe – złośliwe oprogramowanie nawiązujące własne połączenia z Internetem, wysyłające twoje hasła i inne prywatne dane do sieci może się zainstalować na komputerze mimo dobrej ochrony – należy je wykryć i zlikwidować;
 - 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;
 - Sprawdzaj pliki pobrane z Internetu za pomocą skanera antywirusowego;
 - Nie odwiedzaj stron, które oferują niesamowite atrakcje (darmowe filmiki, muzykę, albo łatwy zarobek przy rozsyłaniu spamu) – często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia;
 - Nie wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu – niech np. będą zabezpieczone hasłem i zaszyfrowane – hasło przekazuj w sposób bezpieczny;
 - Nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich;
 - Pamiętaj o uruchomieniu firewalla na każdym urządzeniu;
 - Wykonuj kopie zapasowe swoich ważnych danych.
- 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.
- Chronić 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 przeglądarką 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.

Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie sposobów zabezpieczania się przed zagrożeniami, to wiedza niezbędna każdemu użytkownikowi komputera, tabletu czy telefonu komórkowego.

Dodatkowe informacje znajdują się pod poniższymi adresami:

- <https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo>
- <https://www.cert.pl/publikacje/>