Cyberbezpieczeństwo

Treść

Realizując zadania wynikające z ustawy o Krajowym Systemie Cyberbezpieczeństwa przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skuteczne stosować sposoby zabezpieczenia się przed tymi zagrożeniami.

Cyberbezpieczeństwo zgodnie z ustawą o Krajowym Systemie Cyberbezpieczeństwa (art. 2 pkt 4) – cyberbezpieczeństwo to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy" Główne zagrożenia występujące w cyberprzestrzeni: ·**Kradzież tożsamości** - są dwa rodzaje kradzieży tożsamości. Pierwszy polega na wykorzystaniu Twoich danych osobowych do otwarcia nowego konta na Twoje nazwisko, np. w celu otrzymania karty kredytowej, lub zawarcia umowy z dostawcą usług komórkowych. Drugi polega na wykorzystaniu Twoich danych osobowych do uzyskania dostępu do Twoich kont w celu wykorzystania środków. Sposoby zdobycia Twojej tożsamości - infekowanie komputera wirusami, wysyłanie e-maili z próbami wyłudzenia haseł lub innych informacji, obserwowanie obecności online i rejestrowanie naciśnięć klawiszy na klawiaturze, a nawet monitorowanie aktywności sieciowej w celu zdobycia najważniejszych danych osobowych Jak zapobiegać? – nigdy nie ujawniaj swoich haseł, ani danych osobowych; sprawdzaj wszystko co pobierasz aby upewnić się czy nie jest to złośliwe oprogramowanie (malware); monitoruj konta bankowe; ustal dzienne limity transakcji

· Kradzieże (wyłudzenia), modyfikacje bądź niszczenie danych,

· Ataki z użyciem szkodliwego oprogramowania m.in.:

a) Ransomware – oprogramowanie szantażujące, napastnicy szyfrują dane użytkownika i żądają zapłaty za przywrócenie dostępu do danych. Zagrożenie może dostać się do komputera za pośrednictwem pobranego pliku, poprzez załącznik e-mail, przeglądarkę, jeśli odwiedzasz stronę , która jest zainfekowana lub nawet przez wiadomość tekstową. - **Jak zapobiegać?** - stosować aktualne oprogramowania antywirusowe oraz dokonywać regularnych aktualizacji systemu;

b) Malware – różnego rodzaju szkodliwe programy, których wspólną cechą jest fakt ,że potajemnie uzyskują dostęp do urządzenia bez wiedzy użytkownika. Hakerzy wykorzystują je do różnych celów – wykradania danych osobowych, haseł, pieniędzy oraz blokowania dostępu do urządzeń. Najczęściej dostaje się na urządzenie z Internetu i poczty elektronicznej. Może również pochodzić ze zhakowanych stron internetowych, wersji demo gier, plików muzycznych, pasków narzędziowych, oprogramowania, bezpłatnych subskrypcji lub innych plików pobranych z Internetu na urządzenie, które nie jest odpowiednio zabezpieczone. Rodzaje złośliwego oprogramowanie obejmują oprogramowanie szpiegujące (spyware), adware, wirusy, trojany, rootkity, zagrożenia typu ransomware oraz porywaczy przeglądarki - **Jak zapobiegać ?** – korzystać ze skutecznego antywirusa, nie otwierać załączników z niezaufanych źródeł;

c) SQL Injection jest atakiem polegającym na wykorzystywaniu przez przestępców luk występujących w zabezpieczeniach np. aplikacji i pozwalającym na uzyskanie przez osoby nieuprawione danych osobowych. -**Jak zapobiegać ?** - zapobieganie atakom typu SQL Injection to obowiązek właściciela strony internetowej lub aplikacji;

d) Malvertising pozwala przestępcom na dotarcie do użytkowników przeglądających zaufane strony internetowe poprzez nośniki jakimi są udostępniane na stronach internetowych reklamy, a następnie na instalowanie bez wiedzy i zgody użytkownika złośliwego oprogramowania na urządzeniach użytkownika. -**Jak zapobiegać ?** - nie klikać reklam, stosować filtry blokujące reklamy;

e) Man in the Middle jest rodzajem ataku polegającym na uczestniczeniu osoby trzeciej np. w transakcji pomiędzy sklepem internetowym a klientem. Celem takich ataków jest przechwycenie informacji lub środków pieniężnych (np. uzyskanie danych niezbędnych do logowania w systemie bankowości elektronicznej). -**Jak zapobiegać ?** - szyfrowanie transmisji danych, ważne certyfikaty bezpieczeństwa;

f) Cross sitescripting atak polegający na umieszczeniu na stronie internetowej specjalnego kodu, którego kliknięcie przez użytkownika powoduje przekierowanie na inną stronę internetową (np. na witrynę konkurencji). -**Jak zapobiegać ?** - korzystanie z zaufanego oprogramowania oraz dobrego programu antywirusowego;

· Blokowanie dostępu do usług m.in.: **DDoS**, czyli atak, którego celem jest zablokowanie możliwości logowania użytkownika na stronę internetową poprzez jednoczesne logowanie na tę samą stronę się wielu użytkowników **Jak zapobiegać ?** - Dla zwykłych użytkowników zabezpieczenie się przed atakiem DDoS jest niemożliwe, ponieważ jedynie administrator strony uzyskuje informacje o nagłych, niespodziewanych skokach w ruchu na stronie, na podstawie których może podejmować odpowiednie kroki;

· Ataki socjotechniczne m.in.: **Phishing**, przebiegła metoda, której używa haker, aby nakłonić użytkownika do ujawnienia informacji osobistych, takich jak hasła lub numery kart kredytowych, ubezpieczeń i kont bankowych. Robią to poprzez wysyłanie fałszywych e-maili, przekierowywanie na fałszywe strony internetowe lub podszywając się pod instytucję lub osobę godną zaufania, np. urzędy, banki, portale społecznościowe, znajomych -**Jak zapobiegać?** –nie otwieraj załączników w niechcianych e-mailach; chroń swoje hasła i nie ujawniaj ich nikomu; nie przekazuj nikomu poufnych danych — przez telefon, osobiście lub przez e-mail; sprawdzaj URL stron (adresy stron), dbaj o to, aby przeglądarka była cały czas zaktualizowana i korzystaj z poprawek zabezpieczeń;

·**Spam** - niechciane lub niepotrzebne wiadomości elektroniczne -**Jak zapobiegać?** – używanie skutecznego antywirusa oraz narzędzia antyspamowego; odznaczenie dodatkowych opcji przy rejestracji na kontach lub w usługach internetowych.

Elementarne sposoby zabezpieczenia się przed zagrożeniami:

· używanie silnych, indywidualnych dla każdego systemu haseł i nie nieudostępnianie ich nikomu; · regularne wykonywanie kopii zapasowych ważnych danych; · bieżące aktualizowanie systemu operacyjnego i aplikacji ; · instalacja i użytkowanie oprogramowania

przeciw wirusom i spyware - najlepiej stosować ochronę w czasie rzeczywistym; · aktualizacja oprogramowania antywirusowego oraz bazy danych wirusów; · sprawdzanie plików pobranych z Internetu za pomocą programu antywirusowego; · uruchomienie firewalla; · nie otwieranie plików nieznanego pochodzenia; · korzystanie ze stron banków, poczty elektronicznej czy portali społecznościowych, które mają ważny certyfikat bezpieczeństwa, chyba, że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna; · regularne skanowanie komputera i sprawdzanie procesów sieciowych - czasami złośliwe oprogramowanie nawiązuje własne połączenia z Internetem, wysyłając twoje hasła i inne prywatne dane do sieci; może również zainstalować się na komputerze mimo dobrej ochrony; · nie instalowanie aplikacji nieznanych producentów, bez autoryzacji sklepów z aplikacjami, aplikacje nieznanych producentów mogą prowadzić do wycieku danych; · unikanie 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; · niebezpieczne jest logowanie się do systemów z danymi wrażliwymi za pomocą publicznych sieci Wi-Fi; · nie zostawianie danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie ma się absolutnej pewności, że nie są one widoczne dla osób trzecich oraz nie wysyłanie w wiadomościach e-mail żadnych poufnych danych w formie otwartego tekstu przykładowo dane powinny być zabezpieczone hasłem i zaszyfrowane. Hasło najlepiej przekazuj w sposób bezpieczny przy użyciu innego środka komunikacji; · należy pamiętać, że żaden bank czy Urząd nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji; · zabezpieczenie urządzeń mobilnych- laptopy, smartfony i tablety należy zabezpieczać przy pomocy PINu, odcisku palca lub innych metod oferowanych przez producentów urządzeń. · zwracanie uwagi na komunikaty pojawiające się na ekranie oraz nie ignorowanie ostrzeżeń dotyczących bezpieczeństwa

Więcej informacji znajdziecie Państwo na stronach i portalach:

portale, których celem jest podnoszenie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni –

- www.cert.pl,
- https://cyberpolicy.nask.pl
- http://www.cyber.mil.pl ,
- https://www.gov.pl/web/cyfryzacja/cyberbezpieczenstwo.
- Baza wiedzy cyberbezpieczeństwa
- Narodowe Standardy Cyberbezpieczeństwa
- https://www.cyber.mil.pl/edukacja/
- www.cert.pl/ouch,
- https://stojpomyslpolacz.pl/stp/dobre-praktyki,