ZAGROŻENIA CYBERBEZPIECZEŃSTWA:

Realizując zadania wynikające z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, przekazujemy informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.
Zgodnie z art. 2 pkt 4 ww. ustawy ***cyberbezpieczeństwo*** *to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy*.

Najpopularniejsze zagrożenia w cyberprzestrzeni:

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

  Phishing – nazwa pochodzi od password („hasło") oraz fishing („wędkowanie"). Istotą ataku jest próba pozyskania hasła użytkownika, które służy do logowania się na portalach społecznościowych bądź do serwisów. Po uzyskaniu dostępu, przestępca może wykraść dane osobowe i w tym celu dokonywać oszustw.

  Jak się bronić? Ataki tego typu wymagają bardzo często interakcji ze strony człowieka w postaci odebrania maila lub potwierdzenia logowania.

  Malware – zbitka wyrazowa pochodząca od wyrażenia malicious software („złośliwe oprogramowanie"). Wspólną cechą programów uznawanych za malware jest fakt, że wykonują działania na komputerze bez jego zgody i wiedzy użytkownika, na korzyść osoby postronnej. Działania tego typu obejmują np. dołączenie maszyny do sieci komputerów „zombie", które służą do ataku na organizacje rządowe, zdobywanie wirtualnych walut lub kradzież danych osobowych i informacji niezbędnych do logowania do bankowości elektronicznej.

  Jak się bronić? Najskuteczniejszą obroną przed malware jest dobry system antywirusowy oraz regularnie aktualizowane oprogramowanie.

  Ransomomware – Celem ataku jest zaszyfrowanie danych użytkownika, a następnie ponowne ich udostępnienie w zamian za opłatę. Odbywa się głównie za sprawą okupu. Ataki tego typu działają na szkodę osoby fizycznej, jak i przedsiębiorców.

  Jak się bronić? Należy stosować aktualne oprogramowania antywirusowe oraz dokonywać regularnych aktualizacji systemu

  Man In the Middle – zwany „człowiekiem pośrodku", jest to typ ataku, w ramach, którego w transakcji lub korespondencji między dwoma podmiotami (na przykład sklepem internetowym i klientem) bierze udział osoba trzecia. Celem takich ataków jest przechwycenie informacji lub środków pieniężnych. Celem może być również podsłuchanie poufnych informacji oraz ich modyfikacja.

Jak się bronić? Szyfrowanie transmisji danych, certyfikaty bezpieczeństwa.

Cross-site scripting – jest to atak, który polega na umieszczeniu na stronie internetowej specjalnego kodu, który może skłonić ich do wykonania działania, którego nie planowali.

Jak się bronić? Przede wszystkim korzystanie z zaufanego oprogramowania oraz dobrego programu antywirusowego.

DDos (distributed denial of service) – rozproszona odmowa usługi jest to atak polegający na jednoczesnym logowaniu się na stronę internetową wielu użytkowników, w celu jej zablokowania. Głównie wykorzystywana jest w walce politycznej oraz w e-commerce, gdy w czasie szczególnie atrakcyjnej promocji konkurencja wzmacnia sztucznym ruchem naturalne zainteresowanie użytkowników, by w ten sposób unieszkodliwić sklep.

Jak się bronić? Przed atakami DDoS brakuje skutecznych narzędzi ochrony, oprócz dobrze skonfigurowanemu firewallowi u dostawcy usług internetowych.

SQL Injection – atak tego rodzaju polega na uzyskaniu nieuprawnionego dostępu do bazy danych poprzez lukę w zabezpieczeniach aplikacji, na przykład systemu do obsługi handlu internetowego. Dzięki temu, cyberprzestępca może wykraść informacje od firmy, na przykład dane kontaktowe klientów.

Jak się bronić? Odpowiednie zabezpieczenia na poziomie bazy danych.

Malvertising – zalicza się do szczególnie złośliwego ataku, ponieważ pozwala dotrzeć do użytkowników przeglądających jedynie zaufane strony internetowe. Ich nośnikiem są reklamy internetowe wyświetlane poprzez sieci takie jak np. Google Adwords. Poprzez reklamy może być zainstalowane złośliwe oprogramowanie na komputerze. Takie oprogramowania wykorzystywane są również do wydobywania krypto walut poprzez urządzenia przeglądających.

Jak się bronić? Należy stosować filtry blokujące reklamy.

<u>Sposoby zabezpieczenia się przed zagrożeniami</u>:

- Zainstaluj i używaj oprogramowania przeciw wirusom i spyware. Najlepiej stosuj ochronę w czasie rzeczywistym.
- Aktualizuj oprogramowanie antywirusowe oraz bazy danych wirusów (dowiedz się czy twój program do ochrony przed wirusami posiada taką funkcję i robi to automatycznie).
- Aktualizuj system operacyjny i aplikacje bez zbędnej zwłoki.
- Nie otwieraj plików nieznanego pochodzenia.
- Nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu, chyba, że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna.
- Nie używaj niesprawdzonych programów zabezpieczających czy też do publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony).
- Co jakiś czas skanuj komputer i sprawdzaj procesy sieciowe – jeśli się na tym nie znasz poproś o sprawdzenie kogoś, kto się zna. Czasami 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.

- Sprawdzaj pliki pobrane z Internetu za pomocą skanera.
- Staraj się nie odwiedzać zbyt często 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 zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich.
- Nie wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu – niech np. będą zabezpieczone hasłem i zaszyfrowane – hasło przekazuj w sposób bezpieczny.
- Pamiętaj o uruchomieniu firewalla.
- Wykonuj kopie zapasowe ważnych danych. 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 sposobów zabezpieczania się przed zagrożeniami to wiedza niezbędna każdemu użytkownikowi komputera, smartphona czy też usług internetowych.

Zachęca się do regularnego zapoznawania się z treściami dotyczącymi cyberbezpieczeństwa zawartymi na stronach: Ministerstwa Cyfryzacji,
Porady bezpieczeństwa dla użytkowników komputerów udzielanych przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym, np.:
NIE BĄDŹ OBOJĘTNY! ZGŁASZAJ PRZESTĘPSTWA DOKONYWANE W SIECI! https://www.nask.pl/pl/aktualnosci/4260,Nie-badz-obojetny-Zglaszaj-przestepstwa-dokonywane-w-sieci.html?search=44301045967078