Zgodnie z art. 2 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa pojęcie cyberbezpieczeństwo oznacza odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

W świetle art. 22 ust. 1 pkt 4 ww. ustawy podmiot publiczny zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej.

Stosownie do ww. wymogu przedstawiamy poniżej najważniejsze informacje i zasady zabezpieczenia się przed zagrożeniami w obszarze cyberbezpieczeństwa.

Do najpopularniejszych zagrożeń w cyberprzestrzeni możemy zaliczyć:

– kradzieże tożsamości, modyfikacje bądź niszczenie danych,

– ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki, itp.)

– 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.

Rodzaje cyberzagrożeń

Phishing – próba przekierowania na podrobione strony www za pomocą fałszywych e-maili lub sms, gdzie atakujący podszywa się pod znaną instytucję celem pozyskania od użytkownika danych do logowania.

Qrishing – analogiczny atak z wykorzystaniem przez atakującego fałszywych kodów QR, np. w celu zabezpieczenia swojego konta.

Spear-phishing – atak nakierunkowany na użytkownika z wykorzystaniem równocześnie maila i telefonu.

Malware – złośliwe oprogramowanie, które zostało stworzone z myślą o uszkodzeniu sprzętu lub kradzieży danych.

Deepfake – sfałszowane nagrania audio lub video zamieszczane w serwisach internetowych, czy portalach, gdzie atakujący podszywają się pod znane osoby nakłaniając użytkownika do pozostawienia swoich danych kontaktowych, zachęcając do przystąpienia do wysoko oprocentowanych inwestycji, czy programów rządowych.

Baiting – podrzucenie zainfekowanego urządzenia.

Sposoby zabezpieczenia się przed zagrożeniami:

- Zainstaluj i używaj oprogramowania antywirusowego i spyware. Zaleca się stosowanie ochrony w czasie rzeczywistym.
- Aktualizuj system operacyjny i aplikacje bez zbędnej zwłoki oraz oprogramowanie antywirusowe oraz bazy danych wirusów (zaleca się automatyczną aktualizację).
- Pamiętaj o uruchomieniu firewalla.
- Pobieraj oficjalne oprogramowanie tylko ze sprawdzonych źródeł.
- Sprawdzaj i weryfikuj, czy wchodzisz na zaufane strony www.
- Nie otwieraj plików nieznanego pochodzenia.
- Skanuj swój komputer i procesy sieciowe – celem zabezpieczenia swojego komputera przed złośliwym oprogramowaniem, które może wysyłać twoje hasła i inne poufne dane do sieci
- Sprawdzaj pliki pobrane z Internetu za pomocą skanera.
- Używaj wyłącznie osobistego loginu i hasła. Należy stosować złożone i unikalne hasła. Hasło powinno być trudne do odgadnięcia i zawierać duże/małe litery, cyfry oraz znaki specjalne – hasła z większą liczbą znaków są mniej podatne na złamanie w krótkim czasie. Nie stosuj haseł łatwych do odgadnięcia i jednakowych haseł w różnych aplikacjach i systemach. Nie zaleca się zapamiętywania haseł w pamięci przeglądarki lub w aplikacji na urządzeniu
- Chroń swoje konta w serwisach społecznościowych. Weryfikuj jakie informacje udostępniasz o sobie min. w mediach społecznościowych i aplikacjach i kto może mieć do nich dostęp. Zaleca się ograniczenie dostępu do konta (zasada ograniczonego zaufania). Zweryfikuj warunki korzystania z usługi. Zwracaj uwagę na fałszywe konta i zaproszenia od nieznanych użytkowników
- Nie pozostawiaj 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. Dane poufne powinny być spakowane i zahasłowane. Hasła nie należy przesyłać w tym samym lub kolejnym mailu, tylko innym kanałem, np. za pośrednictwem sms
- Regularnie wykonuj kopie zapasowe ważnych danych.
- Pamiętaj, że żadna instytucja nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji. Zawsze weryfikuj adres nadawcy.

- Bądź ostrożny w stosunku do wiadomości od nieznanych osób.
- Nie otwieraj podejrzanych załączników i nie klikaj w linki niewiadomego pochodzenia.
- Uważaj na publiczne lub niezabezpieczone połączenia internetowe. Nie loguj się do serwisów społecznościowych, banku lub poczty podczas korzystania z otwartych sieci, ponieważ może to grozić udostępnieniem Twoich danych cyberprzestępcom.
- Zabezpiecz swój router hasłem
- Pamiętaj, aby chronić swój telefon przed osobami trzecimi – stosuj blokadę ekranu oraz pin do karty sim

Więcej informacji i porad o cyberbezpieczeństwie:

- https://uodo.gov.pl/pl/138/2634
- https://www.gov.pl/web/baza-wiedzy/aktualnosci
- https://cert.pl/ouch/
- https://www.cert.pl/

Podmioty zajmujące się cyberbezpieczeństwem:

- Cyfryzacja KPRM, https://www.gov.pl/web/cyfryzacja/
- CERT Polska, https://cert.pl/
- CSIRT GOV, https://csirt.gov.pl/
- CSIRT NASK, https://www.nask.pl/pl/dzialalnosc/csirt-nask/3424,CSIRT-NASK.html

Zgłaszanie incydentów bezpieczeństwa:

- https://incydent.cert.pl/