Cyberbezpieczeństwo - jak skutecznie zabezpieczyć się przed zagrożeniami

Realizując zadania, wynikające z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369, z późn.zm.), przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skuteczne stosować sposoby zabezpieczenia się przed tymi zagrożeniami.

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), 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.

Sposoby zabezpieczenia się przed zagrożeniami:

1. 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.

2. Nie ujawniaj danych osobowych w tym danych autoryzacyjnych dopóki nie ustalisz czy rozmawiasz z osobą uprawnioną do przetwarzania Twoich danych.
3. Instaluj aplikacje tylko ze znanych i zaufanych źródeł.
4. Nie otwieraj wiadomości e-mail i nie korzystaj z przesłanych linków od nadawców, których nie znasz.
5. Każdy e-mail można sfałszować, sprawdź w nagłówku wiadomości pole Received: from (ang. otrzymane od) w tym polu znajdziesz rzeczywisty adres serwera nadawcy.
6. Porównaj adres konta e-mail nadawcy adresem w polu „From" oraz „Reply to" – różne adresy w tych polach mogą wskazywać na próbę oszustwa.
7. Szyfruj dane poufne wysyłane pocztą elektroniczną.
8. 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.
9. Jeśli na podejrzanej stronie podałeś swoje dane do logowania lub jeżeli włamano się na Twoje konto e-mail – jak najszybciej zmień hasło.
10. Chroń 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.
11. 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.
12. Logowanie do e-usług publicznych, bankowości elektronicznej bez aktualnego (wspieranego przez producenta) systemu operacyjnego to duże ryzyko.
13. Korzystaj z różnych haseł do różnych usług elektronicznych.

14. 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.
15. Regularnie zmieniaj hasła.
16. Nie udostępniaj nikomu swoich haseł.
17. Pracuj na najniższych możliwych uprawnieniach użytkownika.
18. Wykonuj kopie bezpieczeństwa.
19. Skanuj podłączane urządzenia zewnętrzne.
20. Skanuj regularnie wszystkie dyski twarde zainstalowane na Twoim komputerze.
21. Kontroluj uprawnienia instalowanych aplikacji.
22. Unikaj z korzystania otwartych sieci Wi-Fi.
23. Podając poufne dane sprawdź czy strona internetowa posiada certyfikat SSL. Protokół SSL to standard kodowania (zabezpieczania) przesyłanych danych pomiędzy przeglądarka a serwerem.
24. 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".
25. Szyfruj dyski twarde komputera, przenośne.

Informacje i porady dotyczące cyberbezpieczeństwa:

- https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo
- https://www.cert.pl/publikacje/
- https://akademia.nask.pl/publikacje/
- https://stojpomyslpolacz.pl/
- https://dyzurnet.pl/

Zgłaszanie incydnetów:

- https://incydent.cert.pl/

Czym są wirusy komputerowe?

Wirus komputerowy to program, który dostaje się bez wiedzy

użytkownika do jego komputera. Powiela się jak wirusy, stąd ta nazwa. Niektóre z nich nie są groźne, jednak zdecydowana większość chce zdobyć dane, pieniądze, lub doprowadzić do zniszczenia komputera.

Jak rozpoznać wirusa?
Wirusa rozpoznać można po tym, że komputer może działać powoli lub połączenie z internetem może nie być stabilne. Wirus może również wyłączyć firewalla i program antywirusowy.

Niektóre rodzaje maili z potencjalnym wirusem:

- maile wysłane dotyczące kontroli np. kontrola skarbowa (strach),
- faktury zamieszczone w załączniku na dużą kwotę (ciekawość),
- maile z załączonym życiorysem (ufność),
- wygrana w loterii (radość).

Przesyłane maile wpływają na ludzkie cechy charakteru takie jak podane powyżej. Hakerzy specjalnie tak układają swoje maile, żeby wpłynąć na nas w taki sposób, byśmy kliknęli w ich maila. Niekiedy właśnie to sprawia, że otwieramy wiadomości, które mogą zawierać

Jak rozpoznać oszusta?
Jednym z najprostszych sposobów na zauważenie oszustwa jest angielski, jakim niekiedy posługują się hakerzy - łamany i niespójny. Zawsze warto zobaczyć adres, z jakiego wysłany został mail. Jeżeli z adresu, z jakim nie utrzymujemy kontaktu lepiej w niego nie wchodzić. Należy również uważać w różnego rodzaju skrócone linki, ponieważ te mogą doprowadzić do wycieknięcia naszego adresu IP. Zaleca się również skanować wszystkie załączniki zawarte w mailach oraz nieotwieranie plików z niektórymi rozszerzeniami.

Profilaktyka
Aby jak najskuteczniej obronić się przed wirusami, zaleca się używanie programów antywirusowych, programów usuwających adware i spyware, wykonywania częstych kopii zapasowych oraz przechowywania część plików w chmurze. Dodatkowo nie należy pobierać plików z niezabezpieczonych stron, ponieważ może to skutkować w większości przypadków wirusem.