Cyberbezpieczeństwo

Cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Rodzaje cyberataków:

Malware, czyli złośliwe oprogramowanie, które bez zgody i wiedzy użytkownika wykonuje na komputerze działania na korzyść osoby trzeciej.

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).

Cross site scripting polegający na umieszczeniu na stronie internetowej specjalnego kodu, którego kliknięcie przez użytkownika powoduje przekierowanie na inną stronę internetową (np. na witrynę konkurencji).

Phishing jest to atak polegający na dokonywaniu prób przejęcia haseł służących użytkownikowi do logowania na np. portalach społecznościowych, do których dostęp umożliwia atakującym uzyskanie danych osobowych użytkownika.

DDoS, czyli atak, którego celem jest zablokowanie możliwości logowania użytkownika na stronę internetową poprzez jednoczesne logowanie na tę samą stronę się wielu użytkowników. Wywoływany w ten sposób sztuczny ruch wzmacnia zainteresowanie użytkowników np. produktem dostępnym w sklepie internetowym.

SQL Injection jest atakiem polegającym na wykorzystywaniu przez przestępców luk występujących w zabezpieczeniach np. aplikacji i pozwalającym na uzyskanie przez osoby nieuprawione danych osobowych.

Ransomware to rodzaj ataku, którego celem jest przejęcie i zaszyfrowanie danych użytkownika po to aby w następnym kroku udostępnić te same dane użytkownikowi pod warunkiem wniesienia przez niego “okupu”.

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.

Realizując zadania wynikające z Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, przekazujemy dostęp do informacji zawierających wiedzę o zagrożeniach cyberbezpieczeństwa i stosowaniu skutecznych sposobów zabezpieczania się przed tymi zagrożeniami. Zachęcamy do śledzenia materiałów edukacyjnych udostępnianych bezpłatnie przez instytucje rządowe i administrację publiczną na stronie internetowej: https://www.gov.pl/web/baza-wiedzy oraz informacji publikowanych w szczególności na stronach zespołów reagowania na incydenty bezpieczeństwa informatycznego, np.:

- na stronie internetowej pierwszego w Polsce zespołu reagowania na incydenty informatyczne CERT.PL: https://www.cert.pl/
- przygotowanych przez CERT.PL publikacji: https://www.cert.pl/publikacje/
- cyklicznego, bezpłatnego biuletynu porad bezpieczeństwa dla użytkowników komputerów OUCH!: https://www.cert.pl/ouch/
- biuletynu informacyjnego systemu reagowania na incydenty komputerowe: http://csirt-mon.wp.mil.pl/pl
- na stronie zespołu ekspertów Naukowej i Akademickiej Sieci Komputerowej: https://dyzurnet.pl/