Cyberbezpieczeństwo

Cyberbezpieczeństwo

W dobie cyfryzacji, stajemy się wprost uzależnieni od otaczającej nas, dynamicznie rozwijającej się technologii informatycznej. Technologii, która uzyskała tak duży stopień skomplikowania, że staje się źródłem coraz to nowych podatności. Wykorzystują to międzynarodowe, zorganizowane grupy cyberprzestępców. Wsparte socjotechniką, wiedzą o najnowszych lukach w bezpieczeństwie oraz coraz bardziej zaawansowanymi technikami ataku, są w stanie włamać się do każdej organizacji. Wielomilionowe nieautoryzowane przelewy, paraliż tysięcy organizacji, odcięcie od prądu setek tysięcy gospodarstw – to przykłady skutków dzisiejszych ataków.

Co to jest cyberprzestrzeń?

Cyberprzestrzeń to sfera ludzkiej działalności, która wykształciła się dzięki powstaniu sieci komputerowych jednak nie jest tożsama tylko z Internetem. Cyberprzestrzeń to przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. Cyberprzestrzeń to nie tylko systemy, oprogramowania, Internet czy też przetwarzanie danych, to wirtualne odzwierciedlenie działalności człowieka. Jest to obszar wytworzony w oparciu o nowe technologie.

Co to jest cyberbezpieczeństwo?

Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa, poprzez cyberbezpieczeństwo należy rozumieć „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”. Cyberbezpieczeństwo to jeden ze strategicznych celów w obszarze bezpieczeństwa naszego Państwa w wyniku którego podejmowany jest całokształt działań w celu minimalizacji ryzyk, grożącym czynnościom (operacjom) dokonywanych w cyberprzestrzeni.

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 o krajowym systemie cyberbezpieczeństwa przekazujemy Państwu dostęp do informacji pozwalających na zrozumienie zagrożeń cyberbezpieczeństwa oraz jak stosować skuteczne sposoby zabezpieczenia się przed tymi zagrożeniami:

portale, których celem jest podnoszenie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni - stojpomyslpolacz.pl, it-szkola.edu.pl, www.cyber.mil.pl/edukacja/;

portale zawierające poradniki i porady z zakresu cyberbezpieczeństwa - www.cert.pl/ouch, www.cyber.mil.pl/edukacja/, www.gov.pl/web/cyfryzacja/edukacja/;

portale zawierające artykuły z zakresu cyberbezpieczeństwa - www.cert.pl, cyberpolicy.nask.pl, http://www.cyber.mil.pl

METRYKA:

Liczba wyświetleń:	2823
Utworzono dnia:	2021-11-04 11:00:00
Osoba wprowadzająca informację:	Piotr Michalski
Osoba odpowiedzialna:	Jan Kowalski