XML

Cyberbezpieczeństwo

Jak zrozumieć pojęcie cyberbezpieczeństwa?

Dla zrozumienia terminu cyberbezpieczeństwa niezbędne jest zdefiniowanie cyberprzestrzeni (z ang. cyberspace, cybernetics space), która to cyberprzestrzeń rozumiana jest jako "przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami”[1]. Zakres pojęciowy cyberbezpieczeństwa obejmuje więc zagadnienia związane z bezpieczeństwem cyberprzestrzeni, czyli zachodzących na jej obszarze procesów przetwarzania informacji i interakcji w sieciach teleinformatycznych.

Cyberbezpieczeństwo w wymiarze cyberprzestrzeni

Jest to proces polegający na korzystaniu przez pracowników z jak najbardziej aktualnych programów zabezpieczających dane przed zagrożeniami internetowymi. Cyberbezpieczeństwo w tym aspekcie opiera się również na niewchodzeniu na takie witryny internetowe, które są szczególnie narażone na ataki cyberprzestępców, a także na unikaniu podawania w Internecie do wiadomości publicznej szczegółowych danych firmy.

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.[

Cyberprzestępczość a kodeks karny

Przestępstwa przeciwko ochronie informacji zostały ujęte w XXXIII rozdziale kodeksu karnego. Przepisami sankcjonującymi naruszenia w cyberprzestrzeni są m. in.:

- Art. 267, w którym określona została penalizacja "hackingu” polegającego na włamywaniu się do systemów komputerowych po uprzednim pokonaniu zabezpieczeń,
- Art. 268 i art. 268 a sankcjonują naruszenia porządku w cyberprzestrzeni, które polegają na usuwaniu, modyfikacji i uszkadzaniu plików.

Ponadto Rozporządzeni o Ochronie Danych Osobowych przewiduje kary dla firm, które nie wprowadzają działań koniecznych do uzyskania bezpieczeństwa danych wewnętrznych. Akt prawny przewiduje dotkliwe kary za incydenty związane z

wyciekiem danych osobowych w firmie.[7]

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

Przedmiotem ustawy, która weszła w życie z dniem 28 sierpnia 2018 roku jest organizacja krajowego systemu cyberbezpieczeństwa i określenie zadań oraz obowiązków podmiotów wchodzących w jego skład. Ustawa reguluje również kwestie sprawowania nadzoru i kontroli przestrzegania jej przepisów oraz tryb ustanawiania Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej. Treść ustawy określa zarówno podmioty będące uczestnikami krajowego systemy cyberbezpieczeństwa jak i ich obowiązki.

Zachęcamy do zapoznania się z krótkim filmem na temat cyberbezpieczeństwa.
poniżej link do tego filmu

https://www.youtube.com/watch?v=wAt2mvdhknk

Podmiot publikujący	Urząd Miasta Krosna
Wytworzył	Marian Zoła 2022-10-06
Publikujący	Marian Zoła 2022-10-06 11:14
Modyfikacja	Marian Zoła 2022-10-06 11:18