12 września 2022

O cyberbezpieczeństwie

Cyberbezpieczeństwo (ang. cybersecurity) stanowi zespół zagadnień związanych z zapewnianiem ochrony w obszarze cyberprzestrzeni. Z pojęciem cyberbezpieczeństwa związana jest między innymi ochrona przestrzeni przetwarzania informacji oraz zachodzących interakcji w sieciach teleinformatycznych. Cyberprzestrzeń rozumiana jest natomiast jako przestrzeń przetwarzania i wymiany informacji, tworzona przez systemy teleinformatyczne, wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami.
Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego (2013), Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Warszawa

Cyberbezpieczeństwo odnosi się do szerokiego zakresu różnych działań przestępczych, w których jako podstawowe narzędzie lub jako główny cel wykorzystywane są komputery i systemy informacyjne. Może ona obejmować przestępstwa tradycyjne takie jak oszustwo, fałszerstwo, czy też kradzież, bądź może dotyczyć również przestępstw powiązanych z zakazaną prawem treścią jak nawoływanie do nienawiści. Najczęstsze jednak skojarzeniee z incydentami mającymi miejsce w świecie wirtualnym stanowią przestępstwa charakterystyczne wyłącznie dla komputerów i systemów informacyjnych jak ataki na systemy informatyczne, ataki odmowy usług, przejmowanie mocy obliczeniowej lub tworzenia i dystrybucja złośliwego oprogramowania

Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, K. Czaplicki (red.), Warszawa, Wolters Kluwer 2019 r., s. 17

Celem cyberprzestępców zwykle jest kradzież danych użytkowników. Kradzież odbywać się może podczas niewielkich, dyskretnych ataków na pojedyncze ofiary lub podczas masowych operacji cyberprzestępczych na dużą skalę z wykorzystaniem stron internetowych www. i włamań do baz danych. Metody mogą być różne, ale cel pozostaje ten sam. W większości przypadków napastnicy próbują w pierwszej kolejności dostarczyć na komputer ofiary rodzaj szkodliwego oprogramowania, jako że jest to najkrótsza droga pomiędzy nimi a danymi użytkownika. Zamiary cyberprzestępcy ukierunkowane mogą być również na dokonanie strat finansowych w atakowanej instytucji lub utraty reputacji konkurencji, która zostaje sparaliżowana przez niedostępność usług, bądź w celu uzyskania okupu.

RODZAJE ZAGROŻEŃ CYBERBEZPIECZEŃSTWA

Phishing – Jest to metoda oszustwa, oznaczająca w tradycyjnym rozumieniu tego słowa podszywania się (przede wszystkim z wykorzystaniem poczty elektronicznej i stron internetowych www.) pod inną osobę, instytucję lub znane marki, w celu wyłudzenia określonych informacji takich jak numery oraz hasła PIN kart płatniczych, hasła logowania do urzędów czy też płatności internetowej banków lub szczegółów karty kredytowej w celu wyłudzenia danych. Jest to rodzaj ataku oparty na tzw. inżynierii społecznej.
Atak DDoS atak na system komputerowy lub usługę sieciową w celu uniemożliwienia świadczenia tejusługi (odmowy jej realizacji) polegający na zablokowaniu działania poprzez zajęcie wszystkich wolnych zasobów, przeprowadzany równocześnie z wielu komputerów. Ataki te nie uszkadzają danych, gdyż ich celem jest utrudnienie lub uniemożliwienie dostępu do nich, co może skutkować równie kosztownymi stratami co utrata danych. Ataki te są stanowią jeden z najprostszych sposobów paraliżowania infrastruktury sieciowej oraz aplikacji, jednakże wymagają użycia równocześnie kilku tysięcy urządzeń. Do przeprowadzenia ataku służą najczęściej komputery, nad którymi przejęto kontrolę przy użyciu specjalnego oprogramowania, i które na dany sygnał zaczynają jednocześnie atakować system ofiary, zasypując go fałszywymi próbami skorzystania z usług, jakie oferuje.
Złośliwe oprogramowanie (Malware) – To określenie opisuje całą gamę szkodliwych programów i aplikacji, które po uzyskaniu dostępu do sieci podmiotu lub instytucji może poczynić wiele szkód. Złośliwe oprogramowanie może przyjąć formę wirusów, robaków, koni trojańskich i innych,
Atak Key Logger (ang. Key Logger Attack) – Cyberprzestępcy używają programów, które mogą zapisywać naciśnięcie każdego klawisza na klawiaturze. Dzięki temu mogą poznać login i hasło użytkownika zainfekowanego komputera. Wystarczy raz zalogować się do danej usługi żeby dostarczyć przestępcom pełne dane.
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.
Ransomware to rodzaj złośliwego oprogramowania, które infekując urządzenie lub komputer blokuje jego podstawowe funkcje i wymusza użytkownika do zapłacenia haraczu, w zamian za przywrócenie kontroli nad systemem operacyjnym i umożliwienia dostępu do danych zgromadzonych na komputerze. Zagrożenie może dostać się do komputera za pośrednictwem pobranego

pliku, wykorzystując niespójności w strukturze ochrony lub nawet przez wiadomość tekstową.
Czym się różni od typowego złośliwego oprogramowania?
• Nie kradnie danych użytkownika, lecz je szyfruje.
• Wymusza płatność okupu, zazwyczaj w dolarach lub Bitcoinach.
• Jest relatywnie łatwy do stworzenia – istnieje wiele bardzo dobrze udokumentowanych cryptobibliotek.