Aktualności

CYBERBEZPIECZEŃSTWO 2022-10-10

W świetle obowiązującej ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 art. 2 pkt 4). Podmiot publiczny w związku z obowiązkiem wypełnienia zadań wynikających z ustawy o krajowym systemie cyberbezpieczeństwa zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa

CZYM JEST CYBERBEZPIECZEŃSTWO

Cyberbezpieczeństwo działa jak tradycyjna ochrona – jego zadaniem jest zapewnienie bezpieczeństwa użytkownikom i ich systemom komputerowym. W prawdziwym świecie wystarczy Ci domofon i zamykane na klucz okna, ale w świecie wirtualnym nie jest to aż tak proste. Internetowi złodzieje mogą wejść w posiadanie Twoich danych na wiele sposobów. Mogą nawet przekonać Cię do przesłania ich dobrowolnie, jeśli nie zdajesz sobie sprawy, że właśnie padasz ofiarą oszustwa. Internet może być przerażającym miejscem, a samotne surfowanie po nim może być niebezpieczne. Dlatego musisz się upewnić, że korzystasz z odpowiedniej ochrony.

Motywacją cyberprzestępców są pieniądze, w związku z tym stworzyli oni setki różnych metod kradzieży. W niektórych przypadkach może to sprowadzać się po prostu do śledzenia Twojego konta bankowego, a w niektórych do kradzieży dowodu osobistego. W niektórych naprawdę przerażających sytuacjach cyberprzestępcy mogą zająć cały Twój komputer – to zupełnie tak, jakby przyszli do Twojego domu.

Rodzaje cyberataków

Złośliwe oprogramowanie

Złośliwe oprogramowanie to rodzaj programu, który hackerzy celowo instalują na Twoim komputerze. Złośliwe oprogramowanie często przedostaje się do komputerów, podszywając się pod zupełnie niewinne załączniki wiadomości e-mail lub fałszywe przyciski na stronach internetowych. Umożliwia mu to obejście zabezpieczeń sieci. Tego typu oprogramowanie, znane jako oprogramowanie szpiegujące, może również przesyłać Twoje dane osobowe, instalować kolejne złośliwe programy lub całkowicie wyłączać komputer. By zapewnić bezpieczeństwo komputera, powinno się pobierać wyłącznie te pliki, co do których mamy pewność.

Ransomware

Ransomware to rodzaj złośliwego oprogramowania szyfrującego wszystkie pliki. Trudno jest rozpoznać, że akurat pobiera się ransomware. Często wyląduje ono w Twojej skrzynce odbiorczej pod niewinną nazwą pliku od niewinnie brzmiącego nadawcy. Po jego otwarciu dostęp do plików stanie się niemożliwy, a by go odzyskać, trzeba będzie zapłacić okup. Możesz mieć jednak pewność, że nawet po jego zapłaceniu pozostanie Ci tylko lżejszy portfel i nieprzyjemne wspomnienie.

Phishing

Phishing ma z kolei miejsce wtedy, gdy oszust podszywa się pod wiarygodne źródło. Atak phishingowy może przybrać formę

wiadomości e-mail, wiadomości w mediach społecznościowych, a nawet rozmowy telefonicznej. Możesz na przykład otrzymać wiadomość od kogoś, kto podaje się za pracownika banku i prosi o potwierdzenie Twoich danych, podanie numeru karty kredytowej lub wykonanie przelewu. Następnie ta osoba wykorzysta Twoje dane w celu uzyskania nieautoryzowanego dostępu do Twoich kont. Czasami zdarza się również tak, że wiadomości phishingowe będą Cię oszukiwać i przekonywać, że, by uchronić się przed atakiem oszustów, należy kliknąć określony link lub podać dane swojego konta bankowego. Nigdy, przenigdy nie odpowiadaj na takie prośby. Bezpieczeństwo informacji jest dla banków najwyższym priorytetem, więc z pewnością nie będą one nagle rozsyłać wiadomości e-mail z prośbą o podanie jakichkolwiek danych. Jeśli masz wątpliwości odnośnie do jakiejś wiadomości, nie wykonuj żadnych zawartych w niej poleceń, tylko zadzwoń do banku i sprawdź, czy wiadomość naprawdę została przez niego wysłana.

Ataki DDoS (Denial of Service)

Atak DDoS ma miejsce wtedy, gdy Twoja sieć lub serwer są przeciążone i zalane dużą ilością danych internetowych. Przy tak wielkim nagromadzeniu danych wykorzystujących przepustowość sieci nie możesz normalnie z niej korzystać. Ten rodzaj ataku jest najczęściej kierowany na strony internetowe firm i organizacji. Celem tych ataków raczej nie są pieniądze (przynajmniej nie z punktu widzenia samego oszusta), a utrudnienie dostępu klientom i osobom odwiedzającym stronę. Działa to tak samo jak protest blokujący ulice – tylko online. Prawdopodobnie ataki DDoS wykorzystywane były „w dobrym celu", by zatrzymać działanie grup hejterskich blokujących dostęp do danych stron internetowych.

Atak Man-in-the-Middle

Do takiego ataku dochodzi, gdy atakujący umieszczony jest pomiędzy dwiema ofiarami. Jeśli na przykład rozmawiasz ze znajomym i chcesz, by oddał Ci za coś pieniądze, wysyłasz mu swój numer konta. Twój znajomy widzi wiadomość od Ciebie i przelewa pieniądze. Ty z kolei widzisz wiadomość, że znajomy już zwrócił należną kwotę. Nie zauważycie nawet, że znajduje się między Wami oszust, ponieważ podszywa się on zarówno pod Ciebie, jak i pod Twojego znajomego. A Ty nigdy nie odzyskasz pieniędzy, gdyż oszust zmienił Twoją wiadomość i podmienił numer konta na swój. Ten rodzaj kradzieży tożsamości może być kontynuowany przez kilka dni lub nawet tygodni – dopóki ktoś nie zorientuje się, że coś jest nie w porządku.

Dodatkowe informacje:

Cyberbezpieczeństwo- informacje dla klientów podmiotów publicznych

wszystkie aktualności