Cyberbezpieczeństwo- informacje dla klientów podmiotów publicznych

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.

Czym jest incydent i gdzie go zgłaszać

Incydent to zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo.

Ustawodawca w przepisach ustawy o krajowym systemie cyberbezpieczeństwa zdefiniował kilka rodzajów incydentów. Najważniejszymi z punktu widzenia interesanta podmiotu publicznego są:
1) **incydent w podmiocie publicznym** - incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.

2) **incydent krytyczny** - incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT w tym CSIRT NASK.

Zgłoszenie incydentu cyberbezpieczeństwa, którego ofiarą padł podmiot publiczny, może nastąpić poprzez przygotowany przez CSIRT NASK specjalnie do tego celu portal www.incydent.cert.pl, który umożliwia zgłaszanie incydentów zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa.

Zagrożenia nakierowane na przełamanie zabezpieczeń cyberbezpieczeństwa mogą godzić także w ochronę danych osobowych obywateli przechowywanych na serwerach urzędów lub innych podmiotów publicznych. W przypadku naruszenia ochrony takich danych, podmiot publiczny oprócz zgłoszenia incydentu do CSIRT NASK, zobowiązany jest w terminie 72 godzin po stwierdzeniu naruszenia zgłosić je organowi nadzorczemu. Organem właściwym do zgłaszania naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO).
Zgłoszenia administrator danych może dokonać na 5 sposobów:
1) poprzez stronę internetową Urzędu Ochrony Danych Osobowych (Urzędu) https://uodo.gov.pl/, wchodząc w podlink „Zgłoszenie naruszenia ochrony danych osobowych", znajdujący się u dołu strony internetowej;

2) elektronicznie poprzez wypełnienie dedykowanego formularza elektronicznego dostępnego bezpośrednio na platformie https://biznes.gov.pl odwzorowującego formularz dostępny na stronie internetowej Urzędu;

3) elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: /UODO/SkrytkaESP;

4) elektronicznie poprzez wysłanie wypełnionego formularza za pomocą pisma ogólnego dostępnego na platformie https://biznes.gov.pl;

5) tradycyjną pocztą, wysyłając wydrukowany i wypełniony formularz znajdujący się na stronie internetowej https://uodo.gov.pl/ na adres Urzędu.

Adres:
Urząd Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa

Jak bezpiecznie korzystać z Internetu i nie stać się ofiara cyberprzestępcy

Internet - jako ogólnoświatowy system połączeń między komputerami - niesie za sobą wiele zagrożeń, z których nie zawsze jako korzystający zdajemy sobie sprawę. Tak jak przy wykonywaniu każdej czynności, tak samo korzystając z Internetu należy zachować ostrożność, by skutecznie ograniczać ryzyko stania się ofiarą cyberprzestępcy. Bezpieczeństwa w sieci internetowej nie można zdecydowanie ograniczyć jedynie do ochrony technologicznej.

Cyberprzestępcy podejmują się najróżniejszych sposobów w tym zwykłej socjotechniki w celu nakłonienia użytkownika Internetu do wykonania czynności, które ujawnią informacje o hasłach i stosowanych przez niego zabezpieczeniach, wykorzystując zainfekowane załączniki, fałszywe strony www i wiadomości e-mail, łudząco podobne do prawdziwych.

Aby zminimalizować ryzyko stania się ofiarą cyberprzestępcy należy w szczególności:

1) korzystać z e-usług lub portali internetowych tworząc długie i skomplikowane hasła dostępu – co najmniej ośmioznakowe zawierające małe, wielkie litery, znaki specjalne lub cyfry. Dobrym rozwiązaniem jest korzystanie z tzw. haseł frazowych poprzez np zestawienie pięciu wyrazów niepowiązanych ze sobą i nieoddzielonych spacją

2) dokonywać cyklicznych zmian haseł (średnio co 60 dni) oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione osobie nieuprawnionej,

3) pliki zawierające Twoje dane osobowe przesyłać innym użytkownikom sieci za pośrednictwem poczty e-mail w formie zabezpieczonej hasłem, natomiast samo hasło przekazywać innym środkiem przekazu np. wiadomością sms, bądź podczas rozmowy telefonicznej po uprzednim zweryfikowaniu tożsamości adresata,

4) logując się na nieznane strony internetowe zwracać uwagę na poziom bezpieczeństwa danej strony – symbolami znaczącymi o bezpieczeństwie są m.in. „zielona kłódka" informująca, że strona jest wyposażona w sprawdzony i ważny certyfikat lub element „https", oznaczający, że strona jest szyfrowana. Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel,

5) w przypadku spostrzeżenia w adresie strony internetowej czerwonej kłódki ze znakiem krzyżyka, zachować szczególną ostrożność i powstrzymać się od wprowadzania danych, gdyż istnieje możliwość, iż ktoś podszywa się pod daną witrynę, aby przechwycić cenne informacje,

6) unikać umieszczania w tzw. publicznej chmurze plików i informacji zawierających wrażliwe dane na Twój temat;

7) unikać logowania się na swoje konta internetowe przy pomocy publicznego wifi lub na publicznych komputerach,

8) uważać na strony internetowe, które wymagają instalacji oprogramowania - w takim przypadku najlepiej uprzednio przeskanować wszystkie programy pobierane z Internetu za pomocą aktualnego oprogramowania antywirusowego,

9) unikać otwierania nieznanych linków i załączników w wiadomościach e-mail;

10) unikać korzystania ze stron internetowych, w szczególności o charakterze przestępczym, hackerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu może być zaimplementowany złośliwy kod, który może automatycznie zainfekować system operacyjny komputera w sposób niewidoczny dla użytkownika) oraz zwracać uwagę na reklamy wyświetlane na innych stronach internetowych które są przeglądane.

11) zwracać uwagę i upewnić się czy osoba, z którą nawiązywany jest kontakt jest tym, za kogo się podaje;

12) zwracać uwagę na wiadomości z prośbą o podanie szczegółów konta, gdyż instytucje finansowe oraz urzędy unikają takich sytuacji ze względów bezpieczeństwa;

13) zainstalować oprogramowanie antywirusowe i na bieżąco je aktualizować;

14) korzystać z najnowszych i zaktualizowanych wersji przeglądarek internetowych;

15) zapewnić, by system operacyjny posiadał włączoną funkcję automatycznych aktualizacji i instalować wszelkie aktualizacje zaraz po ich udostępnieniu przez producenta.

Bieżące informacje na temat złośliwych kampanii lub zagrożeń bezpieczeństwa można znaleźć na stronie NASK-u na Facebooku https://pl-pl.facebook.com/NASKpl/?hc_location=ufi

Zachęcamy również do śledzenia informacji publikowanych na poniższych stronach:

- https://www.cert.pl/publikacje/
- https://www.cert.pl/ouch/

Dodatkowe informacje można uzyskać pod adresem mailowym : koordynatorksc@pgkkrasnystaw.pl