Ministerstwo Cyfryzacji

PORADNIK – PRCyber-01

Cyberbezpieczeństwo – jak chronić nasze informacje przed atakami w cyberprzestrzeni ?

(Wydanie 1 - maj 2020 r.)

Departament Cyberbezpieczeństwa
Ministerstwo Cyfryzacji - CyberJST@mc.gov.pl

Cyberbezpieczeństwo – czy mnie to dotyczy ?

Cyberbezpieczeństwo jest ważne, ponieważ smartfony, komputery i Internet są obecnie tak fundamentalną częścią współczesnego życia, że trudno sobie wyobrazić, jak moglibyśmy bez nich funkcjonować, w szczególności w stanie epidemii, gdy musimy ograniczyć swoje fizyczne kontakty. Dlatego też szczególnie dziś ważne jest, aby w ramach kilku kroków ograniczyć cyberprzestępcom zdobycie dostępu do zawartości naszych urządzeń – smartfonów i komputerów – za ich pośrednictwem do naszych kont bankowych, kont w portalach społecznościowych, skrzynek poczty elektronicznej – zarówno prywatnych jak i służbowych.

Niezależnie od wielkości i rodzaju organizacji, w której pracujesz, ważne jest, aby zrozumieć, dlaczego możesz być podatny na cyberataki i sposoby obrony przed nimi. Te podstawowe porady dotyczą zarówno twojego życia zawodowego, jak i prywatnego.

Jak bronić się przed najpopularniejszymi atakami w cyberprzestrzeni i co to jest phishing oraz ransomware ?

Phishing to jeden z najpopularniejszych typów ataków opartych o wiadomości e-mail lub SMS. Wykorzystuje inżynierię społeczną, czyli technikę polegającą na tym, że przestępcy internetowi próbują Cię oszukać i spowodować, abyś podjął działanie zgodnie z ich zamierzeniami. Cyberprzestępcy podszywając się m.in. pod firmy kurierskie, urzędy administracji, operatorów telekomunikacyjnych, czy nawet naszych znajomych, starają się wyłudzić nasze dane do logowania np. do kont bankowych lub używanych przez nas kont społecznościowych, czy systemów biznesowych.

Nazwa *phishing* budzi dźwiękowe skojarzenia z *fishingiem* – czyli łowieniem ryb. Przestępcy, podobnie jak wędkarze, stosują bowiem odpowiednio przygotowaną „przynętę". Do tego wykorzystują najczęściej **sfałszowane e-maile i SMS-y.** Coraz częściej oszuści działają także za pośrednictwem komunikatorów i portali społecznościowych (np. poprzez „metodę na BLIKa").

Wiadomości phishingowe są tak przygotowywane przez cyberprzestępców aby wyglądały na autentyczne, ale w rzeczywistości są fałszywe. Mogą próbować skłonić Cię do ujawnienia poufnych informacji, zawierać linki do stron internetowych zainfekowanych szkodliwym oprogramowaniem, fałszywych stron płatności elektronicznych lub zawierać załącznik wyglądający jak interesujący dokument, który jednak w swojej treści zawiera złośliwy kod w celu przejęcia kontroli nad Twoim urządzeniem.

Szczególnym rodzajem phishingu – zdecydowanie bardziej niebezpiecznym – jest tzw. spear-phishing, czyli atak ukierunkowany na KONKRETNEGO adresata, mający na celu wywarcie określonego wpływu lub wymuszenia działania w stosunku do odbiorcy. Przestępcy mogą podszywać się pod naszych kolegów z urzędu, partnerów biznesowych, z którymi współpracujmy, a wiadomość jest spersonalizowana tzn. bezpośrednio odwołuje się do naszych relacji. Taki typ ataku jest często poprzedzony dokładnym rozpoznaniem przez

atakującego naszego urzędu, naszej organizacji, a także zebraniem i analizą informacji dostępnych o Tobie w mediach społecznościowych

Jak radzić sobie z fałszywymi wiadomościami?

Jeśli nie kliknąłeś w żaden link w wiadomości e-mail, to dobrze.
Dopóki nie masz pewności, że nadawca jest prawdziwy, nie powinieneś klikać w żadne linki ani na nie odpowiadać. W wiadomościach SMS lub mailach często wykorzystywane są tzw. tiny-URL, czyli skrócone adresy stron internetowych. Stąd też zalecamy zwracanie szczególnej uwagi na nazwy stron internetowych, które przesyłane są w podejrzanych mailach czy SMSach np. zamiast www.allegro.pl wykorzystywany może być fałszywy adres www(.)allegrosklep(.)online itp.

Następną rzeczą jest ustalenie, czy wiadomość e-mail jest autentyczna i nie jest oszustwem.

Jak rozpoznać e-mail wyłudzający informacje?

- Wiele wiadomości phishingowych ma niepoprawną gramatykę, interpunkcję, pisownię, czy też bak jest polskich znaków diakrytycznych np. nie używa się „ą", „ę" itd.
- Sprawdź, czy mail pochodzi z organizacji, na którą powołuje się nadawca. Często adres mailowy nadawcy jest zupełnie niewiarygodny, czy też nie jest tożsamy np. z podpisem pod treścią maila.
- Oceń, czy wygląd i ogólna jakość e-maila może pochodzić z organizacji / firmy, od której powinna pochodzić taka wiadomość np. użyte logotypy, stopki z danymi nadawcy itd.
- Sprawdź, czy e-mail jest adresowany do Ciebie z imienia i nazwiska, czy odnosi się do „cenionego klienta", „przyjaciela" lub „współpracownika"? Może to oznaczać, że nadawca tak naprawdę cię nie zna i że jest to część oszustwa typu phishing.
- Sprawdź, czy e-mail zawiera **ukryte zagrożenie**, które wymaga natychmiastowego działania? **Bądź podejrzliwy w stosunku do słów typu** „**wyślij te dane w ciągu 24 godzin**" lub „**padłeś ofiarą przestępstwa, kliknij tutaj natychmiast**".
- Spójrz na nazwę nadawcy, czy wygląda na prawdziwą, czy może tylko naśladuje kogoś, kogo znasz.
- Jeśli wiadomość brzmi zbyt dobrze, aby mogła być prawdziwa, prawdopodobnie nie jest ona prawdziwa. Jest mało prawdopodobne, aby ktoś chciał Ci dać pieniądze lub dostęp do tajnej części Internetu.
- Twój bank lub jakakolwiek inna instytucja nigdy nie powinna prosić Cię o podanie w wiadomości e-mail danych osobowych.
- Urzędy administracji publicznej nigdy nie proszą Cię przy pomocy SMS, czy maili o dopłatę do szczepionki, czy uregulowanie należności podatkowych.
- Sprawdź wszelkie polecenia lub pytania w wiadomości e-mail na przykład dzwoniąc do banku z pytaniem czy rzeczywiście wysłana została do Ciebie taka wiadomość lub wyszukaj w wyszukiwarce Google (lub podobnej) wybrane słowa użyte w wiadomości e-mail.
- Zwracaj uwagę na linki przekazywane również między znajomymi, sprawdź czy link faktycznie prowadzi do właściwej strony. Coraz częściej przestępcy uzyskując w nielegalny sposób kontrolę nad naszymi kontami społecznościowymi podszywając się pod naszych znajomych i rodzinę.

- Uważaj na skrócone linki, jeśli nie masz pewności dokąd poprowadzi Cię link, najedź wskaźnikiem myszy na link (nie klikaj), a na dole przeglądarki zostanie wyświetlony pełen adres linku.

Jeśli zauważysz podejrzanego e-maila, oznacz go w skrzynce odbiorczej jako **spam** lub **wiadomości śmieci** lub **podejrzany**. Spowoduje to usunięcie go ze skrzynki odbiorczej, a także poinformowanie dostawcy poczty e-mail, że zidentyfikowałeś go jako potencjalnie niebezpieczny.

Poza próbą wyłudzenia dostępu do Twoich danych ataki phishingowe są coraz częściej wykorzystywane do zainfekowania Twoich urządzeń oprogramowaniem szyfrującym Twoje dane w celu wymuszenia okupu za udostępnienie klucza do ich odszyfrowania – są to tzw. ataki ransomware (od angielskiego słowa „ransom" – okup).

Zabezpiecz swoje dane

Zastanów się, jak bardzo zależy Ci na swoich prywatnych danych cyfrowych (np. dokumentach, zdjęciach) ? Pomyśl też, czy zależy Ci na danych służbowych, takich jak dane klientów (mieszkańców Twojej gminy), usług, zamówienia i szczegóły płatności. Teraz wyobraź sobie, jak długo byłbyś w stanie działać bez nich.

Najlepszą praktyką, niezależnie od wielkości organizacji czy jednostki organizacyjnej, jest regularne wykonywanie kopii zapasowych ważnych danych i upewnianie się, że są one aktualne i można je przywrócić. Dzięki temu masz pewność, że Twoja jednostka może nadal funkcjonować po zdarzeniach losowych oraz cyberatakach. Ponadto, jeśli masz zapasowe kopie danych, które możesz szybko odzyskać, nie będziesz podatny na szantaż po atakach ransomware – jednym z przykładów był atak na Urząd Gminy w Kościerzynie[1].

Jak wykonywać bezpieczne kopie danych ?

Pierwszym krokiem jest identyfikacja niezbędnych danych. Informacje, bez których Ty i Twoja jednostka nie mogłaby funkcjonować. Zwykle będą to dokumenty, zdjęcia, e-maile, kontakty i kalendarze, z których większość przechowywana jest w kilku wspólnych folderach na komputerze, telefonie, tablecie lub w sieci.
Następnie oddziel kopię zapasową od komputera/smartfona, z których je kopiowałeś. Bez względu na to, czy kopia znajduje się w zewnętrznej pamięci USB, na oddzielnym dysku, czy na oddzielnym komputerze, dostęp do kopii zapasowych danych powinien być ograniczony, aby, nie były one dostępne dla osób nieuprawnionych.
Złośliwe oprogramowanie często może automatycznie przenosić się do podłączonej pamięci, co oznacza, że każda taka kopia zapasowa może być również zainfekowana, uniemożliwiając odzyskanie kopii zapasowej. Aby uzyskać większą odporność, należy rozważyć

[1] https://www.polskieradio24.pl/42/273/Artykul/2416518,Hakerzy-chca-okupu-od-urzednikow-z-Koscierzyny-Czym-jest-ransomware

przechowywanie kopii zapasowych w innym miejscu, aby pożar lub kradzież nie spowodowały utraty obu kopii.
Dobrym rozwiązaniem jest przechowywanie danych na dysku w chmurze. Korzystanie z magazynu w chmurze (w którym dostawca usług przechowuje dane w swojej infrastrukturze) oznacza, że dane są fizycznie oddzielone od Twojej lokalizacji. Będziesz także korzystać z wysokiego poziomu dostępności. Dostawcy usług chmurowych mogą zapewnić przechowywanie danych i usługi sieciowe bez konieczności inwestowania z góry w drogi sprzęt. Większość dostawców oferuje ograniczoną ilość miejsca za darmo i większą pojemność przy minimalnych kosztach dla małych organizacji. Podmioty publiczne mogą korzystać z usług chmurowych oferowanych przez komercyjnych dostawców w ramach inicjatywy Wspólnej Infrastruktury Informatycznej Państwa (WIIP) – więcej informacji pod adresem http://chmura.gov.pl/

Zabezpiecz swoje urządzenia

Smartfony, tablety, laptopy lub komputery stacjonarne, których używasz, mogą być celem ataków w cyberprzestrzeni, a także ataków fizycznych – np. kradzieży. Jak się chronić przed takimi atakami na urządzenia:

- Nie ignoruj aktualizacji oprogramowania - zawierają poprawki i nowe funkcje, które chronią przed najnowszymi zagrożeniami. Jeśli pojawi się monit o zainstalowanie aktualizacji, upewnij się, czy faktycznie zostały one zaktualizowane.
- Zawsze blokuj urządzenie, gdy go nie używasz. Użyj kodu PIN, hasła lub odcisku palca. Utrudni to atakującemu wykorzystanie urządzenia, jeśli zostanie ono zgubione lub skradzione.
- Unikaj pobierania aplikacji, których reputacji nie jesteś pewien. Używaj tylko oficjalnych sklepów z aplikacjami (takich jak Google Play lub Apple App Store), które zapewniają większą ochronę przed złośliwym oprogramowaniem. Nie pobieraj aplikacji od przypadkowych źródeł, tylko dlatego, że ktoś do tego zachęca na mediach społecznościowych.

Używaj silnych haseł i używaj różnych haseł do różnych kont

Atakujący wypróbują najpopularniejsze hasła (np. 12334, abcd. itp.) lub wykorzystają publicznie dostępne informacje, aby uzyskać dostęp do Twoich kont. Jeśli się im powiedzie, mogą użyć tego samego hasła, aby uzyskać dostęp do innych Twoich kont.

- Utwórz silne i łatwe do zapamiętania hasło do ważnych kont, na przykład używając trzech losowych słów. Unikaj używania przewidywalnych haseł, takich jak daty, nazwisko i imię czy imię Twojego zwierzaka.
- Używaj osobnego hasła do konta służbowego. Jeśli prywatne konto internetowe zostanie przejęte, nie chcesz, aby osoba atakująca znała również twoje hasło służbowe.
- Jeśli zapisujesz swoje hasła, przechowuj je bezpiecznie z dala od urządzenia. Nigdy nie ujawniaj nikomu swojego hasła. Jeśli korzystasz z zarządzanego urządzenia Twój

administrator, zespół bezpieczeństwa lub zewnętrzny dostawca usług bezpieczeństwa będzie pomoże Ci zresetować hasło w razie potrzeby – w przypadku .

- Użyj wieloskładnikowego uwierzytelniania (MFA – Multi-Factor Authentication) w ważnych usługach online, takich jak bankowość i poczta e-mail, jeśli masz taką opcję. MFA zapewnia sposób co najmniej „podwójnego sprawdzenia", że naprawdę jesteś osobą, za którą się podajesz, gdy korzystasz z usług online.

W razie wątpliwości, zgłoś podejrzane działania do zespołu reagowania na incydenty bezpieczeństwa CSIRT NASK

Zgłaszanie informacji o podejrzanych działaniach w cyberprzestrzeni może znacznie zmniejszyć potencjalne szkody powodowane przez cyberataki.

- Cyberataki mogą być trudne do wykrycia, więc nie wahaj się prosić o dalsze wskazówki lub wsparcie, gdy coś wydaje się podejrzane lub niezwykłe.
- Zgłoś ataki jak najszybciej - nie zakładaj, że zrobi to ktoś inny – zgłoszenia możesz dokonać pod adresem https://incydent.cert.pl/