2026

Bezpieczeństwo danych

ZAGROŻENIA ZWIĄZANE ZE STARYMU KONTAMI. ATAKI SOCJOTECHNICZNE. ATAKI WYKORZYSTUJĄCE WIADOMOŚCI TEKSTOWE. ZASADY BEZPIECZNYCH ROZMÓW.

SŁAWOMIR BILIŃSKI

1. Zagrożenia związane z zapomnianymi kontami[1]

a) Dlaczego stare konta są ryzykowne i warto zwrócić na nie uwagę:

Każde konto, które tworzysz, bez względu na to, jak błahe może się wydawać w danej chwili, przechowuje pewnego rodzaju dane osobowe. Może to obejmować Twoje imię i nazwisko, adres e-mail, datę urodzenia, numer telefonu, adres zamieszkania.

Stare konta mogą znajdować się na platformach, które nie są już wspierane, a przestarzałe zabezpieczenia sprawiają, że Twoje dane nie są bezpieczne.

Gdy takie witryny zostaną przejęte, hasła i dane osobowe będą narażone na ujawnienie. Jeśli używasz tego samego hasła w wielu serwisach, narażasz się na większe niebezpieczeństwo. Cyberprzestępcy często wykorzystują skradzione hasła z jednego konta i próbują użyć ich celem przejęcia innych kont.

b) Jak znaleźć stare konta:

Być może nie pamiętasz każdej witryny, na której się zarejestrowałeś, ale istnieją sposoby, aby je odkryć:

- **Przeszukaj swoją skrzynkę e-mail**: Wyszukaj wiadomości e-mail zawierających frazy takie jak: ***witaj w,*** "***zweryfikuj swój e-mail,***" "**faktura,**" lub "***zresetuj swoje hasło.***" Mogą one pomóc w identyfikacji zapomnianych kont.
- **Sprawdź menedżer haseł**: Jeśli używasz menedżera haseł, sprawdź zapisane hasła. Prawdopodobnie będą tam informacje o kontach utworzonych w przeszłości. Często możesz filtrować wyniki według najstarszych kont lub tych, do których nie uzyskiwano dostępu przez ponad rok.
- **Przejrzyj swoje urządzenie mobilne**: Przejrzyj wszystkie swoje aplikacje mobilne, aby znaleźć konta, których już nie używasz.

c) Co zrobić ze starymi kontami:

Gdy znajdziesz stare lub nieużywane konta, należy podjąć następujące działania:

- **Usuń konta, których nie używasz:** Jeżeli nie korzystasz już z konta, zaloguj się i usuń je lub dezaktywuj. Jeśli platforma nie pozwala Ci usunąć konta, zmień hasło, a następnie usuń z profilu wszelkie dane osobowe, takie jak imię i nazwisko i adres;
- **Zaktualizuj/popraw hasła do kont, które posiadasz:** W przypadku kont, z których nadal korzystasz, upewnij się, że każde z nich ma silne, unikalne hasło. Użyj menedżera haseł, który ułatwi Ci zarządzanie hasłami. Większość menedżerów haseł wyświetli ostrzeżenie, jeśli dwa lub więcej kont korzysta z tego samego hasła;
- **Włącz uwierzytelnianie wieloskładnikowe:** W przypadku istotnych kont, takich jak poczta e-mail, bankowość internetowa czy media społecznościowe, włącz uwierzytelnianie wieloskładnikowe. Zapewni Ci to dodatkową ochronę, nawet jeśli Twoje hasło zostanie ujawnione. Jeśli to możliwe, włącz uwierzytelnianie wieloskładnikowe na każdym koncie, które je obsługuje;

Pamiętaj, zastanów się zanim gdziekolwiek się zarejestrujesz. Twórz nowe konta tylko wtedy, gdy będzie to konieczne. Jeśli korzystasz z witryny tylko raz, skorzystaj z opcji płatności jako gość zamiast zakładać nowe konto.

Raz na jakiś czas zrób przegląd swoich kont, pod kontem siły hasła, przestarzałych/aktualnych zabezpieczeń.

[1] Źródło materiału: CERT Polska.

2. Ataki socjotechniczne.

Powszechnym (błędnym) przekonaniem na temat cyberprzestępców jest to, że używają oni wyłącznie wysoce zaawansowanych narzędzi i technik do włamywania się do komputerów lub kont użytkowników.

Cyberprzestępcy wiedzą, że najłatwiejszym sposobem na kradzież informacji, zhakowanie konta lub zainfekowanie systemu jest po prostu nakłonienie Cię do zrobienia tego czego chcą, ale z wykorzystaniem techniki, która nosi nazwę socjotechniki.

Poniżej przedstawiono, jak działają te ataki i co możesz zrobić, aby się chronić.

a) Czym jest socjotechnika

Socjotechnika to atak psychologiczny, w ktorym atakujący nakłania Cię do zrobienia czegoś, czego niestety nie powinieneś robić, za pomocą rożnych technik manipulacji.

Dzisiejsza technologia ułatwia każdemu napastnikowi, który znajduje się w dowolnym miejsca na świecie podszywanie się pod jakąkolwiek osobę i tym samym atakowanie każdego z nas.

Oto dwa przykłady:

Otrzymujesz telefon od osoby, która twierdzi, że dzwoni z Urzędu Skarbowego z informacją, że masz zaległości podatkowe i jeśli ich nie zapłacisz od razu, zostaniesz ukarany grzywną. Następnie naciska, abyś zapłacił przez telefon, kartą kredytową, kartą podarunkową lub przelewem, ostrzegając, że jeśli nie zapłacisz, spotkają Cię konsekwencje.

Dzwoniący nie jest tak naprawdę z urzędu skarbowego, tylko przestępcą, który próbuje nakłonić Cię do przekazania mu pieniędzy.

Innym przykładem jest atak zwany phishingiem.

Atakujący tworzy wiadomość e-mail, którą próbuje nakłonić Cię do podjęcia działania, takiego jak: otwarcie zainfekowanego załącznika, kliknięcie złośliwego łącza lub podanie poufnych informacji

Przykładem mogą być te, które sugerują, że pochodzą z banku. Innym razem e-maile phishingowe mogą być spersonalizowane i ukierunkowane, ponieważ atakujący najpierw sprawdzają/obserwują swoje cele (wcześniej włamują się na Twoją skrzynkę pocztową), na przykład email sugerujący, że pochodzi od szefa lub współpracownika, lub firmy do której złożyłeś CV.

Należy pamiętać, że takie ataki socjotechniczne nie ograniczają się do rozmów telefonicznych lub e-maili. Mogą się zdarzyć w dowolnej formie, w tym SMS-em, w mediach społecznościowych, a nawet poprzez kontakt osobisty - twarzą w twarz.

b) Na co wobec tego należy zwrócić uwagę.

- Zachowaj dużą czujność. Atakujący próbują zmusić cię do popełnienia błędu. Im większe poczucie pilności, tym większe prawdopodobieństwo ataku;
- Atakujący naciskają na omijanie lub ignorowanie zasad lub procedur bezpieczeństwa, których masz przestrzegać w pracy;
- Prośby o podanie poufnych informacji, do których nikt nie powinien mieć dostępu, takich jak numery kont, peselu, itp.;
- E-mail lub wiadomość od znajomego lub współpracownika, którego znasz, ale wiadomość nie brzmi tak jakby to oni ją wysłali – np. zawiera dziwne sformułowanie lub nieprawidłowy podpis;
- E-mail, który wydaje się, iż pochodzi od współpracownika lub legalnej firmy, ale jest wysyłany przy użyciu osobistego adresu e-mail, takiego jak: @gmail.com;
- Granie na twojej ciekawości lub naiwności (coś jest zbyt piękne, aby mogło być prawdziwe) – przykładowo otrzymasz powiadomienie, że przesyłka została opóźniona, mimo że nigdy nie zamówiłeś paczki, lub że wygrałeś nagrodę w konkursie, w którym nigdy nie uczestniczyłeś.

3. Ataki wykorzystujące wiadomości tekstowe.

a) Czym są ataki wykorzystujące wiadomości tekstowe?

Smishing (połączenie słów SMS i phishing) to atak, w którym cyberprzestępcy używają SMS-ów i innych technologii przesyłania wiadomości, aby nakłonić Cię do podjęcia działania, którego nie powinieneś podejmować.

Mogą nakłonić Cię do podania danych karty kredytowej, zadzwonienia pod numer telefonu w celu uzyskania informacji bankowych lub wypełnienia ankiety online w celu zebrania danych osobowych.

Podobnie jak w przypadku phishingu rozpowszechnianego drogą mailową, atakujący często grają na emocjach, aby skłonić do działania, na przykład tworząc poczucie obowiązku lub ciekawości.

Fakt, że w wiadomościach SMS jest znacznie mniej informacji niż w wiadomości e-mail usypia naszą czujność i sprawia, że ataki tego typu są bardziej niebezpieczne, ponieważ trudniej wykryć, że coś jest nie tak.

Powszechnym oszustwem jest wiadomość informująca o wygraniu m.in. telefonu komórkowego - wystarczy kliknąć w link i wypełnić ankietę, aby go odebrać.

W rzeczywistości do wygrania nie ma żadnego telefonu, a ankieta ma na celu zebranie danych osobowych.

Innym przykładem może być wiadomość informująca, że paczka nie mogła zostać dostarczona do adresata z powodu niedopłaty. Link do strony przekierowuje do fałszywego panelu logowania do bankowości internetowej, w którym użytkownik jest proszony o podanie informacji potrzebnych do zalogowania się na konto bankowe.

W niektórych przypadkach strony mogą nawet nakłaniać do zainstalowania szkodliwej aplikacji mobilnej, która przejmuje kontrolę nad naszym urządzeniem.

Czasami atakujący łączą nawet ataki na telefon z wiadomościami SMS. Na przykład możesz otrzymać SMSa z banku z pytaniem, czy autoryzowałeś płatność.

Nadawca wiadomości poprosi o odpowiedź TAK lub NIE. Jeśli odpowiesz, atakujący zadzwoni do Ciebie, podszywając się pod pracownika banku.

Następnie spróbuje wyciągnąć od Ciebie informacje, takie jak login i hasło do konta bankowego.

b) Wykrywanie i zatrzymywanie ataków w wiadomościach tekstowych.

Oto kilka pytań, które należy sobie zadać, aby uchronić się przed utratą danych:

- Czy wiadomość wywołuje poczucie obowiązku i sprawia, że robisz jakieś działania w pośpiechu?
- Czy linki w wiadomości prowadzą do witryn, które nakłaniają do podania danych osobowych, karty kredytowej, hasła lub innych poufnych informacji, do których nikt oprócz Ciebie nie powinien mieć dostępu?
- Czy wiadomość brzmi zbyt dobrze, by mogła być prawdziwa? Czy tak naprawdę wygranie iPhone'a, Samsunga w podejrzanej loterii może być realne?
- Czy podlinkowana strona lub usługa zmuszają Cię do płacenia za pomocą niestandardowych metod, takich jak Bitcoin, karty podarunkowe lub przelewu Western Union?
- Czy w wiadomości pojawia się pytanie o wieloskładnikowy kod uwierzytelniający, który został wysłany na Twój numer telefonu lub wygenerowany przez aplikację?
- Czy wiadomość wygląda jakby została wysłana do nieodpowiedniej osoby?

Jeśli tak, nie powinieneś odpowiadać na takie wiadomości ani kontaktować się z nadawcą. Najlepiej będzie jeżeli takie wiadomości usuniesz.

Jeśli otrzymasz wiadomość od oficjalnej firmy, oddzwoń bezpośrednio na infolinię tej firmy. Do kontaktów używaj wyłącznie numerów telefonu podanych na oficjalnej stronie internetowej. Jeśli otrzymujesz wiadomość o problemie z kontem bankowym, z kartą kredytową, skontaktuj się bezpośrednio ze swoim bankiem lub firmą, która obsługuje kartę kredytową. Numer telefonu znajduje się

na oficjalnej stronie internetowej banku lub na odwrocie karty kredytowej. Pamiętaj też, że większość instytucji rządowych, finansowych nigdy nie skontaktuje się z Tobą za pomocą wiadomości tekstowych. Zazwyczaj będą wybierać inną drogę komunikacji, np. za pomocą poczty.

4. Zasady bezpiecznych rozmów.

Wiadomości są podstawowym sposobem komunikacji zarówno w życiu osobistym, jak i zawodowym. Często jednak osobami, które stwarzają największe niebezpieczeństwo podczas komunikowania się, jesteśmy my sami.

Poniżej przedstawiono najczęstsze błędy popełniane przez ludzi i informacje, jak można ich uniknąć.

a) Autouzupełnianie.

Automatyczne uzupełnianie to powszechna funkcja wielu aplikacji. Gdy wpiszesz imię i nazwisko osoby, do której chcesz wysłać wiadomość, aplikacja może automatycznie wybrać tę osobę.

Ta funkcja może niestety prowadzić do błędów i wielu problemów, zwłaszcza gdy wiele kontaktów podobnie się nazywa. Wiadomość, która miała trafić do współpracownika, może zamiast tego trafić do osoby, która ma bardzo podobne nazwisko. Zawsze dokładnie sprawdź dane osoby, do której chcesz wysłać wiadomość, zanim naciśniesz przycisk „wyślij".

b) Odpowiadanie na wiadomości grupowe.

Czaty grupowe są bardzo popularne, ale zanim zaczniesz się w nich udzielać, upewnij się, że znasz wszystkich członków grupy biorących udział w rozmowie.

Wysyłane wiadomości muszą być odpowiednie dla wszystkich osób w tej grupie. Muszą dotyczyć tej grupy, a nie innej.

Częstym błędem jest przypadkowe odpowiadanie wszystkim członkom grupy zamiast konkretnej osobie. Nie spiesz się z odpowiedzią: Sprawdź swoją wiadomość zanim ją wyślesz.

c) Emocje.

Unikaj wysyłania wiadomości, gdy jesteś zły lub zdenerwowany. Ta wiadomość może wyrządzić ci krzywdę w przyszłości.

Zamiast tego poświęć chwilę i spokojnie uporządkuj swoje myśli. Jeśli nie możesz się powstrzymać, otwórz nową wiadomość bez wybranego odbiorcy, napisz dokładnie, co czujesz, a następnie odejdź od komputera.

Dobrym pomysłem może okazać się wyjście na spacer. Kiedy wrócisz, usuń wiadomość i zacznij od nowa. Prawdopodobnie będziesz wtedy spokojniejszy. Bezpośrednia rozmowa przez telefon lub na żywo będzie bardziej efektywna. Ludziom może być trudno określić ton i intencje w samej wiadomości tekstowej.

d) Prywatność.

Tradycyjnym wiadomościom SMS brakuje zabezpieczeń prywatności, ponieważ po jej wysłaniu tracisz kontrolę nad wiadomością.

Pamiętaj, że twoje wiadomości, mogą być przesyłane dalej, publikowane i udostępniane w postaci zrzutów ekranu.

W ważnych sprawach (wymagających poufności) najlepszy może okazać się telefon do danej osoby, lub rozmowa bezpośrednia.

Jeśli używasz urządzenia służbowego do wysyłania wiadomości, pamiętaj, że pracodawca może mieć prawo do monitorowania i potencjalnego odczytywania wiadomości na urządzeniach, z których korzystasz. Zawsze stosuj obowiązujące w miejscu racy zasady korzystania z urządzeń służbowych i zasad korespondencji.

e) Złośliwe wiadomości.

Podobnie jak w przypadku poczty elektronicznej, cyberprzestępcy próbują oszukiwać za pomocą SMS-ów.

Wiadomości te mogą zawierać złośliwe linki, prośby o udostępnienie danych osobowych lub naciski, abyś nawiązał kontakt z daną osobą inną drogą.

Otrzymanie dziwnej wiadomość tekstowej zawierającej tylko słowo „Cześć", oznacza, że cyberprzestępca próbuje rozpocząć z Tobą rozmowę, co często jest początkiem tzw. oszustwa nigeryjskiego.

Jeśli otrzymasz dziwne lub podejrzane wiadomości, po prostu je usuń. Ponadto, podobnie jak w przypadku e-maili, możliwe jest sfałszowanie źródła wiadomości SMS.

Zanim udostępnisz jakiekolwiek dane, upewnij się, że znasz osobę, z którą piszesz, zwłaszcza jeśli nie jesteś inicjatorem rozmowy. Możesz także zablokować niechciane lub podejrzane numery telefonów.

f) Bezpieczeństwo wiadomości.

Upewnij się, że aplikacja do przesyłania wiadomości, której używasz, jest zaktualizowana.

Powyższe zasady (omówione w niniejszym materiale) nie tylko uchronią Twoje dane osobowe, ale również dane służbowe, do których masz dostęp. W konsekwencji nieodpowiedzialnego zachowania (szczególnie w przypadku przetwarzania danych szczególnej kategorii, np. zdrowia) straty może ponieść również Twój pracodawca i osoby, których dane osobowe on przetwarza. Skala incydentu może iść wówczas nie tylko w dziesiątki osób ale setki.

Sławomir Biliński