NASK

Cyberoszustwa bazują na socjotechnice i psychologicznych pułapkach

JAK NIE DAĆ SIĘ OSZUKAĆ W INTERNECIE

Fot. https://pixabay.com/pl/illustrations/haker-bezpieczeństwo-cybernetyczne-8033977/

Anna Kwaśnik

Państwowy Instytut Badawczy NASK

Obraz cyberprzestępcy utrwalony w kulturze masowej przedstawia osobę o wyjątkowych kompetencjach technologicznych, piszącą na klawiaturze w tempie karabinu maszynowego i w kilka minut włamującą się do systemów FBI i Pentagonu. Rzeczywistość jest inna – oszuści najchętniej posługują się działaniami, które nie wymagają szczególnych umiejętności technicznych, za to bazują na psychologii i socjotechnice.

W 2022 r. zespół CERT Polska, działający w strukturach Państwowego Instytutu Badawczego NASK, zarejestrował ponad 39 tysięcy incydentów bezpieczeństwa. Aż 65,7% to ataki zakwalifikowane jako phishing. Dane z 2023 r. potwierdzają ten trend – choć liczba wszystkich odnotowanych incydentów znacznie się zwiększyła, nadal większość z nich (ponad 40 tys. przypadków) stanowił phishing. Podsumowując, większość zagrożeń, z jakimi można spotkać się w przestrzeni cyfrowej, nie jest związana z wykorzystywaniem zaawansowanych, szkodliwych aplikacji, ale z oszustwami i wyłudzeniami bazującymi w znacznej mierze na psychologii.

Sprawcy ataków opartych na socjotechnice wykorzystują nasze słabości

Socjotechnika i inżynieria społeczna to, najprościej mówiąc, każda forma manipulacji i triki psychologiczne. Mają nakłonić człowieka do podjęcia określonych działań, które najczęściej skutkują wyłudzeniem poufnych informacji, utratą danych, a to z kolei prowadzi do utraty pieniędzy. Ataki socjotechniczne zwykle nie są celem same w sobie, a elementem większego planu, za pomocą którego cyberprzestępcy realizują swoje cele.

Sprawcy ataków opartych na socjotechnice są bardzo kreatywni, a sposoby ich działania coraz bardziej wyrafinowane. Przestępcy wykorzystują słabości natury ludzkiej – emocje, presję czasu, stres. Poza tym wzbudzają u osoby, którą chcą oszukać, zaufanie lub poczucie komfortu. Dzięki temu osoby te stają się bardziej podatne na różnego rodzaju manipulacje, a przedstawione przez oszustów historie i scenariusze mogą wydawać się prawdziwe.

Phishing – najchętniej wykorzystywany atak socjotechniczny

Najpopularniejszą i niezwykle skuteczną formą ataku z wykorzystaniem socjotechniki jest phishing, który opiera się głównie na podszywaniu pod znaną firmę, instytucję lub bliską osobę, a także na manipulacji, opowiadaniu odpowiednich historii oraz wywieraniu presji. Cyberprzestępcy często kontaktują się z ofiarami za pomocą różnych środków komunikacji, takich jak e-maile, komunikatory, wiadomości SMS czy połączenia głosowe, QR kody, ale wszystkie próby oszustwa opierają się na tym samym mechanizmie. Chodzi o to, by osoba, którą wybrali oszuści, uwierzyła w fałszywą historię i podążała za wskazówkami rozmówcy.
Aby przyciągnąć uwagę potencjalnej ofiary, przestępcy stosują różne sztuczki – przedstawiają obietnicę korzyści lub wzbudzają strach przed stratą i często wywierają presję na szybką decyzję. Ponadto ataki te często wydają się autentyczne, ponieważ zawierają oficjalne logo, podpis osoby zarządzającej instytucją, a numer kontaktowy wygląda na prawdziwy.
Celem tych ataków jest zazwyczaj uzyskanie poufnych informacji, takich jak hasła do logowania czy dane karty płatniczej albo nakłonienie użytkownika do wykonania określonych działań, na przykład otwarcia zainfekowanego załącznika.

Częste scenariusze phishingowe

Wiadomości phishingowe rozsyłane przez cyberprzestępców są coraz trudniejsze do zweryfikowania. Do złudzenia potrafią przypominać oficjalną korespondencję z banków, sklepów czy instytucji publicznych. Dokładnie odtworzona forma graficzna strony lub wiadomości, stopka nadawcy i ukrycie adresu, z którego pochodzi wiadomość to podstawowe triki oszustów. Dlatego zawsze po otrzymaniu nietypowej wiadomości lub połączenia telefonicznego należy się zastanowić, czy przedstawiona historia jest prawdziwa. I najlepiej ją zweryfikować przez bezpośredni kontakt z firmą, podmiotem lub osobą prywatną, od której rzekomo otrzymano wiadomość.
Do najczęściej wykorzystywanych scenariuszy wiadomości phishingowych należą: niezapłacona faktura, dopłata do paczki, wyjątkowe oferty sklepów lub funduszy inwestycyjnych, zagrożenie życia bliskich osób, blokada konta bankowego lub podejrzane transakcje, opłata mandatu. Należy jednak pamiętać, że oszuści są bardzo kreatywni, zatem scenariusze przedstawiane przez nich mogą być bardzo różne.

Ataki masowe i *spear phishing*

Większość ataków phishingowych ukierunkowanych jest na masową wysyłkę i przypadkowych użytkowników internetu. Socjotechnika może być jednak wykorzystywana również w atakach ukierunkowanych na konkretne organizacje czy jednostki, takie jak dyrektorzy, menedżerowie i pracownicy firm, korporacji, instytucji.
W ataku typu *spear phishing*, czyli ukierunkowanym na konkretną osobę, wykorzystuje się presję autorytetu i czasu, aby skłonić potencjalną ofiarę do podjęcia działania, które może mieć negatywne konsekwencje dla firmy. Aby taki atak był skuteczny, oszuści muszą wcześniej poznać ofiarę i zebrać o niej informacje. Najczęściej pochodzą one z otwartych źródeł w internecie, w tym także z profili w mediach społecznościowych. Każda zdobyta informacja o celu ataku zwiększa szansę na uwiarygodnienie się sprawcy i sukces jego działań.
Najczęstszym sposobem ataku ukierunkowanego są wiadomości e-mail, których treść sugeruje, że zaistniała konieczność natychmiastowej weryfikacji stanu konta, uaktualnienia danych do przelewu, które w rzeczywistości należą do oszusta, i wykonanie przelewu. Sprawa może dotyczyć zarówno konta osobistego, jak i konta instytucji, z którego należy wykonać transakcję. Wiadomości najczęściej wymagają szybkiego działania, a zaufanie, jakim pracownik darzy swojego przełożonego, mogą przyczyniać się do skuteczności ataku.

Jak rozróżnić fałszywą wiadomość?

Nadawca. Sprawdź adres e-mail nadawcy. Czy wygląda autentycznie? Czy pasuje do firmy czy instytucji, z której rzekomo pochodzi wiadomość?

Nieoczekiwane i nietypowe wiadomości. Otrzymanie wiadomości e-mail, SMS-a lub innej formy komunikatu, którego nie oczekiwałeś, może być podejrzane.

Presja czasu i emocje. Wiadomości mogą zawierać stresujące lub niepokojące treści, takie jak informacje o blokadzie konta bankowego lub groźby utraty dostępu do konta.

Linki URL. Sprawdź dokładnie linki zawarte w wiadomości. Czy prowadzą do autentycznej strony internetowej? Czy jest jakiś subtelny błąd w adresie URL, który sugeruje, że może to być fałszywa strona?

Prośby o poufne informacje. Ostrożnie z wiadomościami, które proszą o podanie poufnych informacji, takich jak hasła, numery kart kredytowych czy dane osobowe. Autentyczne firmy rzadko kiedy proszą o takie informacje drogą mailową.

Niepoprawna gramatyka i ortografia. Mimo, że wiadomości phishingowe są coraz lepiej przygotowywane, stale mogą zawierać błędy gramatyczne i ortograficzne. Autentyczne komunikaty od renomowanych firm zwykle są starannie sformułowane.

Podsumowując: na ataki socjotechniczne narażony jest każdy użytkownik internetu. Aby skutecznie się przed nimi bronić, niezwykle ważne jest, aby stale budować świadomość z zakresu cyberbezpieczeństwa i przestrzegać zasady cyberhigieny.

JAK SIĘ CHRONIĆ PRZED CYBERATAKAMI?

Nigdy nie podejmuj działań pod wpływem emocji i presji czasu. Zanim podejmiesz jakiekolwiek działania, zweryfikuj autentyczność zdarzenia.

Twórz silne i unikalne hasła. Dobre hasło powinno być długie, zawierać co najmniej 14 znaków. Zaleca się, by były to całe frazy lub zdania, minimum cztery losowe wyrazy, które będą trudne do złamania. Zawsze stosuj zasadę jedno hasło = jedno konto. Więcej o hasłach w materiale CERT Polska [https://cert.pl/hasla/].

Zawsze sprawdzaj adres URL strony, na której się znajdujesz, upewniając się, że jest zgodny z oficjalnym adresem strony internetowej firmy lub instytucji. Bądź ostrożny wobec skróconych linków, które możesz otrzymać, na przykład w wiadomościach SMS.

Dokładnie sprawdź nadawcę wiadomości, szczegółowo analizując adres e-mail, z którego została wysłana do Ciebie wiadomość. Porównaj go z innymi, otrzymanymi od banku lub innej instytucji. Jeśli coś budzi Twoje wątpliwości, lepiej zignorować tę wiadomość.

Uważnie czytaj powiadomienia dotyczące potwierdzenia transakcji i operacji bankowych, nie zatwierdzając ich pochopnie. Skup się na treści i kwocie transakcji.

Nigdy nie udostępniaj numeru karty płatniczej ani danych logowania osobom trzecim, zwłaszcza, gdy oczekujesz na płatność. Te dane służą do wykonywania transakcji i przelewów, a nie do odbierania płatności.

Włącz weryfikację dwuetapową wszędzie tam, gdzie jest to możliwe. Rozważ użycie menedżera haseł.

Jeśli korzystasz często z usług firm kurierskich, warto rozważyć korzystanie z ich aplikacji. Dzięki temu będziesz mógł otrzymać informacje o każdej przesyłce bezpośrednio na swoje urządzenie.

Jeśli otrzymasz nietypową wiadomość SMS, zgłoś ją na numer 8080. Wszystkie incydenty związane z Twoim bezpieczeństwem w sieci zgłaszaj do CERT Polska.

Baza wiedzy:

Bezpieczny Miesiąc, https://bezpiecznymiesiac.pl/bm/baza-wiedzy.
Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/baza-wiedzy/aktualnosci.
Biuletyn OUCH!, https://cert.pl/ouch/.
CERT Polska, https://cert.pl/.

Bibliografia:

Bezpieczny Miesiąc, *Ataki socjotechniczne, czyli umysł w niebezpieczeństwie,* https://bezpiecznymiesiac.pl/bm/baza-wiedzy/844,Ataki-socjotechniczne-czyli-umysl-w-niebezpieczenstwie.html [dostęp: 11.03.2024 r.].
CERT Polska, *Ataki spear phishing na pracowników polskich firm i instytucji publicznych,* https://cert.pl/posts/2023/03/spear-phishing/ [dostęp: 11.03.2024 r.].
Biuletyn OUCH! *Ataki phishingowe*, https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt1342ae6456b825c1/62b24560ce3d8856b19fcc1f/ouch!_july_2022_polish_phishing_attacks_are_getting_trickier.pdf [dostęp: 11.03.2024 r.].
CERT Polska, *Kompleksowo o hasłach,* https://cert.pl/posts/2022/01/kompleksowo-o-haslach/ [dostęp: 11.03.2024 r.].

Summary

Cyberfraud is based on social engineering and psychological traps. How not to get scammed on the Internet

Cyberfraud can affect anyone: companies, organisations and a mere user of the Internet. There are known cases of great ”phishing campaigns” reaching a very large number of people and ending with the loss of money accumulated in accounts for many years. In different publications or multimedia the image of a cybercriminal is presented in the usual way. Meanwhile, what should be kept in mind and clearly emphasised, is the fact that not only technical skills determine the commission of this type of crime. While deceiving, fraudsters primarily use psychology and social engineering. The article explains the specifics of the actions undertaken by cybercriminals, who choose the most common form of social engineering attack, i.e. phishing. The paper describes how attacks that exploit our weaknesses are performed, as well as what a mass attack and spear phishing are. In the final part of the article there are practical tips on how to recognize that the message is fake and how to protect yourself from cyberattacks. The entire article closes with a database of publications – studies prepared, among others, by experts of the National Research Institute NASK

Tłumaczenie: Katarzyna Olbryś