SANS SECURITY AWARENESS

OUCH!

Biuletyn Bezpieczeństwa Komputerowego

CEO Fraud

Czym jest oszustwo na wiadomość od prezesa (ang. CEO Fraud / Business Email Compromise)?

Cyberprzestępcy ciągle atakują organizacje za pomocą fałszywych wiadomości podszywających się pod komunikację biznesową, co nazywamy także oszustwem na wiadomość od prezesa (CEO Fraud). Celem ataku zwykle są pieniądze a przestępcy za pomocą fałszywych wiadomości manipulują odbiorcą tak aby zrobił coś czego nie powinien. Atak tego rodzaju jest szczególnie niebezpieczny bo przestępcy wyszukują informacje na temat ofiary aby stworzyć jak najbardziej wiarygodną wiadomość. Wykrycie oszustwa na wczesnym etapie jest trudne także ze względu na brak szkodliwego oprogramowania w załączniku wiadomości, brak też w treści podejrzanych linków. Taki atak przebiega według scenariusza o kilku charakterystycznych cechach.

Cyberprzestępca na podstawie informacji dostępnych w internecie wyszukuje ofiarę oraz osoby, z którymi ofiara komunikuje się w pracy. Dla przykładu, chcąc zaatakować Ciebie, sprawdzi kto jest Twoim kierownikiem i zapozna się ze strukturą firmy, w której pracujesz. Na podstawie tych informacji przestępca stworzy wiadomość mailową naśladująca korespondencję, która mogłaby w rzeczywistości pojawić się podczas komunikacji ze współpracownikami. Zazwyczaj wiadomości od przestępców mają wywoływać poczucie pośpiechu, nakłaniając odbiorcę do podjęcia natychmiastowych działań takich jak dokonanie płatności za fakturę, zmianę danych osobowych odbiorcy przelewu czy przesłania wrażliwych dokumentów. Przestępcza wiadomość wywiera presję, której ulegnie ofiara. Przykłady:

Przelew: Przestępca chce wyłudzić pieniądze. Zbiera w tym celu informacje o firmie, stara się określić kto jest odpowiedzialny za księgowość oraz rozliczenia lub z innego powodu może mieć uprawnienia do realizowania przelewów. W następnym kroku, atakujący wysyła do takich osób wiadomości mailowe podając się za ich przełożonego lub dyrektora. Wiadomość zawiera informację o wystąpieniu wyjątkowej sytuacji i konieczności wykonania natychmiastowego przelewu na nowe konto bankowe. Ofiara myśląc, że wypełnia polecenie służbowe w rzeczywistości wykonuje przelew na konto przestępców.

Wyłudzenie informacji: Atakujący chce uzyskać informacje przydatne do przeprowadzenia oszustwa podatkowego. Najszybszym sposobem jest zazwyczaj kradzież informacji na temat pracowników danej firmy. Cyberprzestępcy identyfikują pracownika działu kadr, a następnie wysyłają mu wiadomość podając się za pracownika wyższego szczebla lub działu prawnego. Przesłana prośba o udostępnienie danych uzasadniona jest pilną potrzebą uzupełnienia dokumentów podatkowych. Pracownicy zespołu zarządzania personelem są przekonani, że w odpowiedzi na zapytanie, wysyłają wrażliwe dane do przełożonego. Rzeczywistym adresatem wiadomości są jednak przestępcy.

Metody ochrony

Jakie są w takim razie najskuteczniejsze sposoby ochrony? Najlepszą ochroną jest zachowanie zdrowego rozsądku. Warto mieć na uwadze wskazówki, które mogą być pomocne w wykryciu próby ataku.

- Email jest bardzo krótki (zazwyczaj jest to zaledwie kilka zdań), napisany jest w sposób sugerujący potrzebę pośpiechu, oraz opatrzony jest podpisem informującym o wysłaniu wiadomości z urządzenia mobilnego.
- Wydźwięk wiadomości sugeruje niezwłoczne podjęcie działania oraz pominięcie obowiązujących procedur i polityk pracodawcy. Nigdy nie należy ignorować procedur wdrożonych w firmie, nawet jeśli email podpisany jest rzekomo przez osobę wyższego szczebla lub działu prawnego.
- Wiadomość ma związek z obowiązkami służbowymi, ale w adresie nadawcy znajduje się mail prywatny, np. @gmail.com lub @wp.pl
- Ton i charakter wiadomości nie pasuje do osoby, która wpisana jest jako nadawca wiadomości.
- Załączone instrukcje dotyczące wykonywania płatności różnią się od stosowanych już procedur lub płatność ma zostać wykonana na inny numer konta bankowego niż zazwyczaj.

Jeżeli podejrzewasz, że korzystając ze służbowej poczty mogłeś stać się celem ataku, nie podejmuj kontaktu z nadawcą podejrzanej wiadomości i poinformuj swojego przełożonego o incydencie inną drogą. Jeśli atak nastąpił poza pracą i dokonałeś przelewu na konto przestępców, niezwłocznie poinformuj o tym bank, a w następnej kolejności organy ścigania.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK, powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.
WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Redaktor Gościnny

Don Cavender *to były agent specjalny FBI posiadający ponad 22 lata doświadczenia w zakresie informatyki śledczej oraz walki z cyberprzestępczością. Swoje doświadczenie wykorzystuje w prowadzonych szkoleniach oraz badaniach. Udziela się na Twitterze jako* @don_cavender a jego profil na Linkedin ma adres https://www.linkedin.com/in/donald-cavender.

Przydatne linki

Inżynieria społeczna:	https://www.sans.org/u/HE3
Powstrzymać phishing:	https://www.sans.org/u/HE8
Ochrona przed złośliwym oprogramowaniem:	https://www.sans.org/u/HEd
Bezpieczne logowanie:	https://www.sans.org/u/HEi