OUCH! Wrzesień 2021

SANS SECURITY AWARENESS

OUCH!

Biuletyn Bezpieczeństwa Komputerowego

Zabezpieczenie kont online

Czy masz czasami wrażenie, że cyberprzestępcy w magiczny sposób wkradają się do skrzynek elektronicznych czy kont bankowych, a Ty nic nie możesz zrobić aby ich powstrzymać? Czy nie byłoby wspaniale gdyby istniała jedna metoda, która pozwoliłaby ochronić te dane przed działaniem przestępców? Choć jeden krok to za mało na powstrzymanie atakujących, najważniejszym jaki możesz podjąć, jest włączenie uwierzytelniania dwuskładnikowego (czasem zwanego 2FA, weryfikacją dwuetapową lub uwierzytelnianiem wieloczynnikowym) na każdym z kont, gdzie jest to tylko możliwe.

Problem z hasłami

Do ochrony kont online prawdopodobnie używasz hasła dostępowego. W dużym uproszczeniu istnieje kilka metod na uwierzytelnienie się do konta, na podstawie: tego co masz, tego co znasz, kim jesteś i gdzie jesteś. Stosując więcej niż jedną metodę uwierzytelniania, dodajesz dodatkową warstwę ochrony przed cyberprzestępcami. Nawet jeśli złamią jedną metodę, nadal będą musieli ominąć dodatkowe mechanizmy, aby uzyskać dostęp do konta. Hasła służą do udowodnienia, że jesteś tym za kogo się podajesz. Niebezpieczeństwem związanym z hasłami jest fakt, że są jedynym zabezpieczeniem przed nieautoryzowanym dostępem. Jeśli ktoś jest w stanie odgadnąć albo pozyskać hasło, będzie również w stanie uzyskać dostęp do wszystkich informacji nim chronionych. Najnowsze technologie ułatwiają atakującym szybkie łamanie haseł. Na szczęście walka trwa i mamy do dyspozycji uwierzytelnianie dwuskładnikowe.

Uwierzytelnianie dwuskładnikowe

Dwuskładnikowe uwierzytelnianie jest dużo bezpieczniejszym rozwiązaniem niż używanie samego hasła. Zasada jest prosta, zamiast wykorzystywania tylko jednej metody uwierzytelniania, używane są obydwie. Dzięki tej metodzie, jeśli hasło trafi w ręce cyberprzestępców, konto nadal będzie chronione. Dobry przykładem może być wypłacanie pieniędzy z bankomatu. Kiedy wypłacasz pieniądze z bankomatu również używasz uwierzytelniania dwuskładnikowego. Aby uzyskać dostęp do swoich środków potrzebujesz dwóch rzeczy: karty bankomatowej oraz numeru PIN. Jeśli zgubisz kartę, żadna osoba która ją znajdzie nie będzie w stanie wypłacić pieniędzy nie znając kodu PIN. Podobnie jeśli ktoś zna kod PIN ale nie jest w posiadaniu karty bankomatowej, nie wypłaci środków. Atakujący musi posiadać obie rzeczy, aby uzyskać dostęp do konta. To właśnie sprawia, że dwuetapowa weryfikacja jest dużo bezpieczniejsza, składa się z dwóch warstw zabezpieczeń.

Używanie dwuskładnikowego uwierzytelnianie

Dwuskładnikowe uwierzytelnianie zazwyczaj jest domyślnie wyłączone i trzeba aktywować osobno dla każdego z kont.
W rzeczywistości to nic trudnego, zazwyczaj nie musisz robić nic więcej niż zsynchronizować telefon komórkowy z kontem. Dzięki temu, gdy chcesz zalogować się na swoje konto, nie tylko logujesz się za pomocą nazwy użytkownika i hasła, ale także używasz unikalnego kodu jednorazowego, który otrzymujesz na urządzenie mobilne. Idea tego rozwiązania polega na tym, że do zalogowania się wymagana jest kombinacja zarówno hasła, jak i unikalnego kodu. Zazwyczaj ten unikalny kod zostaje wysłany za pomocą wiadomości tekstowej na telefon komórkowy lub e-mail. Ale zamiast otrzymywać kod w wiadomości tekstowej, możesz zainstalować specjalną aplikację (np. Google lub Microsoft Authenticator). Taka aplikacja wygeneruje specjalny kod, za każdym razem kiedy chcesz się zalogować, nawet bez połączenia z internetem. Rozwiązanie to jest uważane za najbezpieczniejszą opcję uzyskania kodu.

Zazwyczaj podanie kodu do weryfikacji jest wymagane tylko przy pierwszym logowaniu z danego urządzenia. Przeglądarki często zapamiętują urządzenia, z którego wykonane było ostatnie logowanie i w takim przypadku wystarczy jedynie hasło, aby się zalogować. Natomiast gdy będziesz chciał się zalogować na konto z innego urządzenia, albo ktoś będzie chciał to zrobić, system ponownie będzie wymagał uwierzytelnienia dwuskładnikowego. Oznacza to, że jeśli cyberprzestępca zdobędzie hasło, nadal nie będzie mógł uzyskać dostępu do Twojego konta, ponieważ nie będzie miał dostępu do unikalnego kodu.

Pamiętaj, że uwierzytelnianie dwuskładnikowe zazwyczaj nie jest włączone domyślnie, więc będziesz musiał włączyć je samodzielnie dla każdego z najważniejszych kont, takich jak konta bankowe, inwestycyjne, społecznościowe czy osobiste konta e-mail. Na początku może się wydawać, że konfiguracja uwierzytelniania dwuskładnikowego może przysporzyć problemów i dodatkowej pracy, ale nic bardziej mylnego. Jest to bardzo łatwe w użyciu.

Redaktor gościnny

Lysandra Capella ma ponad 15-letnie doświadczenie w pracy w dziedzinie bezpieczeństwa informacji i technologii. Jest instruktorem Instytutu SANS dla kursu SANS AUD507, skupiającego się na pomiarze i zarządzaniu ryzykiem. W wolnym czasie Lysandra wspiera zespoły zarządzające w zakresie formułowania strategii, zapewniania bezpieczeństwa i zarządzania IT.
https://www.linkedin.com/in/lysandracapella/.

Źródła

Tworzenie haseł w prostszy sposób: https://www.sans.org/newsletters/ouch/making-passwords-simple/
Menedżer haseł: https://www.sans.org/newsletters/ouch/password-managers/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz