Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu

- **Problem**
- **Rozwiązanie**
- **Przykład**

Dwustopniowe uwierzytelnianie

REDAKTOR GOŚCINNY

Fred Kerby jest redaktorem gościnnym tego wydania. Zarządzał bezpieczeństwem informacji w Naval Surface Warfare Center w oddziale w Dahlgren. Jest także starszym instruktorem SANS i prowadzi tam kurs „Wstęp do bezpieczeństwa informacji" (SEC 301).

PROBLEM

Żeby korzystać z usług dostępnych w Internecie, takich jak e-mail, bankowość elektroniczna lub zakupy on-line, musisz najpierw udowodnić, że jesteś tym za kogo się podajesz. Proces udowadniania swojej tożsamości nazywa się uwierzytelnieniem. Uwierzytelnienie odbywa się przy użyciu czegoś co wiesz (np. hasła), czegoś co masz (np. smartfona), lub czegoś unikalnego dotyczącego Ciebie (np. obrazu siatkówki lub odcisku palca). Tradycyjnie jednym z najbardziej powszechnych sposobów uwierzytelniania jest nazwa użytkownika i hasło. Jednak użycie wyłącznie hasła sprawia, że atakujący musi je jedynie zgadnąć lub wykraść, aby zyskać natychmiastowy dostęp do Twojego konta i wszystkich informacji do niego przypisanych. Jeśli używasz tej samej nazwy użytkownika i hasła do wielu kont, straty mogą być znacznie większe. Aby lepiej chronić konta internetowe, usługodawcy coraz częściej wykorzystują silniejsze metody weryfikacji tożsamości użytkownika, które wymagają użycia więcej niż jednego czynnika w celu uwierzytelniania. Poniżej wyjaśnimy czym jest dwustopniowe uwierzytelnianie, jak działa i dlaczego warto go używać.

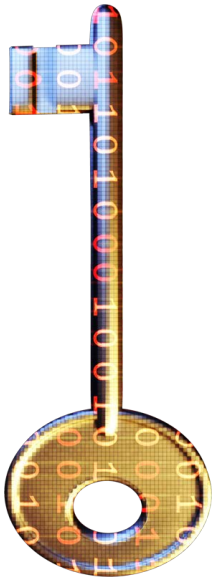
ROZWIĄZANIE

Silniejsze uwierzytelnianie wykorzystuje więcej niż jeden składnik. Oznacza to, że trzeba nie tylko podać hasło, ale również posiadać rzecz, która weźmie udział w uwierzytelnianiu (np. smartfon, token) lub przedstawić coś unikalnego wyłącznie dla Ciebie (np. odciski palców). Do dwuskładnikowego uwierzytelnienia, jak sama nazwa wskazuje, aby udowodnić kim jesteś, potrzebne są dwa czynniki. Typowym przykładem dwuskładnikowego uwierzytelnienia jest karta bankomatowa. Aby uzyskać dostęp do bankomatu trzeba coś mieć (karta bankomatowa) i trzeba coś wiedzieć (kod PIN). Jeśli karta bankomatowa zostanie skradziona, nie jest w pełni

Dwustopniowe uwierzytelnianie

użyteczna, chyba że złodziej zna także kod PIN (dlatego właśnie nigdy nie należy pisać swojego kodu PIN na karcie). Stosowanie dwóch czynników do uwierzytelniania zapewnia lepszą ochronę niż ograniczenie się tylko do jednego.

Dwuskładnikowe uwierzytelnianie w Internecie działa w sposób podobny do karty bankomatowej i kombinacji PIN. Aby uzyskać dostęp do swoich kont internetowych wykorzystywana jest nazwa użytkownika i hasło. Jednak po pomyślnym wpisaniu poprawnego hasła, zamiast przejść bezpośrednio do konta, strona wymaga podania drugiego czynnika uwierzytelniania, takiego jak kod weryfikacyjny lub odcisk palca. Jeśli nie posiadasz drugiego czynnika, nie uzyskasz dostępu do konta. Właśnie ten drugi krok znacząco zwiększa Twoje bezpieczeństwo. Nawet jeśli napastnik wszedł w posiadanie hasła, Twoje konto jest nadal bezpieczne ponieważ nie może on zakończyć kolejnego etapu uwierzytelniania bez drugiego czynnika.



Używaj dwustopniowego uwierzytelniania kiedy tylko to możliwe. To jeden z najsilniejszych sposobów aby chronić dostęp do Twoich kont i informacji.

PRZYKŁAD

Prześledźmy na przykładzie jak może działać dwuskładnikowe uwierzytelnianie. Jedną z najczęściej używanych usług online jest poczta elektroniczna Gmail. Wiele osób uwierzytelnia ich konta Gmail lub innych usług Google przy użyciu nazwy użytkownika i hasła. Google oferuje obecnie większe bezpieczeństwo w postaci dwuskładnikowego uwierzytelniania, lub, jak Google to nazywa, dwuetapowej weryfikacji. Dwuetapowa weryfikacja Google wymaga dwóch rzeczy do uwierzytelniania: Twojego hasła (czegoś co wiesz) i smartfona (czegoś coś co masz). Aby udowodnić, że masz smartfon, Google wyśle w wiadomości SMS jednorazowy, unikalny dla Ciebie kod weryfikacyjny. Następnie należy wprowadzić kod na stronie. Ponadto, jeśli wolisz, zamiast przesyłania przez Google jednorazowego kodu weryfikacyjnego za pomocą wiadomości SMS, można zainstalować aplikację, która wygeneruje taki unikalny kod. W ten sposób nie trzeba mieć nawet połączenia z operatorem telefonii komórkowej, wystarczy tylko smartfon. Ogromną zaletą takiego silniejszego uwierzytelniania jest to, że nawet gdy atakujący poznał Twoje hasło, nie może on uzyskać dostępu do konta Google, chyba że on również ma fizyczny dostęp do urządzenia typu smartfon. Zatem Ty i Twoje cenne informacje jesteście chronieni.

Dwustopniowe uwierzytelnianie

Pamiętaj, że wszystkie kody weryfikacyjne wysyłane na smartfon są niepowtarzalne, inne dla każdej próby uwierzytelnienia. Taki proces dwustopniowej weryfikacji trzeba będzie przejść za każdym razem, kiedy będziesz logował się do konta Google. Ponadto, funkcja ta nie jest domyślnie włączona. Aby ją włączyć, należy zalogować się na swoje konto Google, wejdź w swoje „Ustawienia konta", wybierz „Bezpieczeństwo" i zaznacz opcję dwuetapowej weryfikacji.

Inne witryny internetowe, takie jak Dropbox, Paypal lub witryny banków, również oferują dwuskładnikowe uwierzytelnianie. Niektóre z tych usług mogą obsługiwać wysyłanie kodów na telefon, podczas gdy inne, takie jak PayPal, mogą wysłać specjalny token do generowania unikatowych kodów weryfikacyjnych. Wreszcie można także wykorzystywać specjalne urządzenia, które podłącza się do portu USB w komputerze, taki jak Yubikey. Jeśli którakolwiek z usług internetowych z których korzystasz oferuje dwuskładnikowe uwierzytelnianie, zalecamy je włączyć i używać.

ŹRÓDŁA

W celu poprawy czytelności tekstu niektóre odnośniki w biuletynie zostały skrócone przy użyciu usługi TinyURL. Dla zachowania bezpieczeństwa, OUCH! używa funkcji podglądu TinyURL, która pozwala podejrzeć docelowy adres odnośnika oraz pyta o pozwolenie przed wejściem na stronę o docelowym adresie.

Weryfikacja dwuetapowa Google:
http://preview.tinyurl.com/cncte9n

Klucz bezpieczeństwa PayPal
http://preview.tinyurl.com/838dpds

Słownik pojęć bezpieczeństwa (EN):
http://preview.tinyurl.com/6wkpae5

Porada dnia SANS Security (EN):
http://preview.tinyurl.com/6s2wrkp

DOWIEDZ SIĘ WIĘCEJ

Zasubskrybuj comiesięczny Biuletyn Bezpieczeństwa Komputerowego – SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS z zakresu bezpieczeństwa komputerowego i osobowego. Odwiedź http://www.securingthehuman.org i dowiedz się więcej.

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

Redakcja: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz