Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu

- **Silne ale łatwe do zapamiętania hasło**
- **Dobre praktyki ochrony haseł**
- **Bezpieczne używanie haseł**

Bezpieczne i silne hasła

REDAKTOR GOŚCINNY

Majowe wydanie miesięcznika OUCH! powstało dzięki pomocy doktora Erica Cole'a. Dr Cole jest założycielem firmy Secure Anchor Consulting oraz wieloletnim współpracownikiem SANS Institute. Od wielu lat z pasją uczestniczy we wdrażaniu polityk bezpieczeństwa w wielu znanych firmach i organizacjach. Więcej informacji o działalności dr Cole'a można znaleźć na jego stronie internetowej http://www.securityhaven.com/.

WPROWADZENIE

Hasło jest kluczem do Twojego „królestwa". Wraz z nazwą użytkownika (tzw. loginem) stanowi najpopularniejszy sposób weryfikacji tożsamości i umożliwia zalogowanie się do komputera czy serwisu internetowego. Niestety bardzo często nie doceniamy wagi jaką ma hasło. Zazwyczaj stanowi ono jedyne zabezpieczenie przed niepowołanym dostępem do naszych kont bankowych, czy poczty elektronicznej. Używanie zbyt prostych haseł, np. „qwerty", „123456" lub „abc123" niesie za sobą ryzyko uzyskania nieuprawnionego dostępu do konta, co może doprowadzić do ogromnych strat. Za słabe uważane są również hasła bazujące na imionach bliskich osób, nazwach ulubionych zespołów czy imieniu pupila. Takie informacje są z reguły łatwo dostępne w Internecie lub nawet publikowane przez samego użytkownika, np. na portalach społecznościowych. Jeżeli przestępca zdobędzie nasze hasło może to doprowadzić do kradzieży naszej cyfrowej tożsamości, uzyskania dostępu do konta bankowego lub do poufnych danych pracodawcy powodując ogromne straty. Pamiętaj, że jeśli Twoje hasło zostanie skradzione, to Ty możesz stać się odpowiedzialny za wszystkie czynności wykonane z wykorzystaniem Twojego konta! W tym numerze miesięcznika OUCH! przedstawiamy prosty sposób tworzenia silnych, a jednocześnie łatwych do zapamiętania haseł oraz prezentujemy sposoby bezpiecznego ich używania.

SILNE HASŁA

Internetowi przestępcy opracowali wiele metod mających pomóc im w szybkim złamaniu hasła użytkownika i przejęcia dostępu do jego danych. Opierają się one głównie na atakach słownikowych (http://tinyurl.com/atak-slown) lub próbie ślepego odgadnięcia hasła (http://tinyurl.com/atak-brute). Aby uniemożliwić lub utrudnić atakującemu odgadnięcie hasła, powinno ono być ciągiem znaków, którego nie można znaleźć w słowniku oraz być na tyle długie, aby atak na ślepo był nieefektywny. Poniżej prezentujemy kilka wskazówek jak zbudować silne hasło.

Bezpieczne i silne hasła

Dobre hasło powinno:

- zawierać co najmniej jedną cyfrę
- zawierać co najmniej jedną dużą literę
- składać się z co najmniej jednego symbolu (np. #$%&:)
- mieć długość conajmniej 12 znaków,

a dla zabezpieczenia danych o wyjątkowym znaczeniu minimum 15 znaków

Na pierwszy rzut oka spełnienie wszystkich wymagań wydaje się być bardzo trudne, a hasło zbudowane w ten sposób niemożliwe do zapamiętania. Nie musi tak być, jeżeli zastosujemy prostą sztuczkę z dziedziny nauki zwanej mnemotechniką (http://tinyurl.com/haslo-mnemo). Przyjrzyjmy się prostemu przykładowi.

Mój syn urodził się w Warszawie 14 maja o 20:05

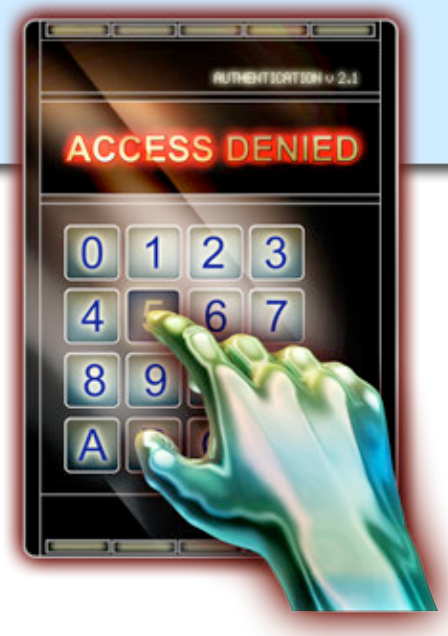
Takie zdanie jest bardzo proste do zapamiętania. Na jego podstawie możemy zbudować hasło, które spełni wcześniej założone kryteria i będzie trudne do odgadnięcia.

MsuswW14mo20:05

Hasło powstało poprzez użycie pierwszych liter z każdego z wyrazów oraz wszystkich liczb. Dodatkowo, jeżeli chcemy jeszcze bardziej je skomplikować możemy spójniki w zdaniu zamienić na ich angielskie odpowiedniki w postaci symboli, np. @ może odpowiadać spójnikom „w”, „na”, „o”, itp., a symbol & spójnikowi „i”. Nasze hasło przybierze wtedy nową formę, która będzie jeszcze trudniejsza do odgadnięcia dla atakującego, ciągle pozostając prosta do zapamiętania dla twórcy:

Msus@W14m@20:05

Bezpieczne hasło powinno być trudne do odgadnięcia, łatwe do zapamiętania, unikalne i prywatne.



OCHRONA HASEŁ

Pamiętaj, że silne hasło to nie wszystko. Każde z haseł, które chroni nasze dane przed dostępem niepowołanych osób, jesteśmy zobowiązani przechowywać w sekrecie. Nie ważne jak silne jest hasło i jak wiele trudu włożyliśmy w jego wymyślenie – nasze dane mogą ciągle paść łupem przestępców. Kilka prostych rad przedstawionych poniżej może w znacznym stopniu podnieść poziom bezpieczeństwa i utrudnić przestępcom zdobycie informacji potrzebnych do przejęcia naszej cyfrowej tożsamości:

1. Chroń komputer przed wirusami. Jedną z najpopularniejszych metod wykradania poufnych danych to infekcja komputerów oprogramowaniem, które zbiera

Bezpieczne i silne hasła

wszystko, co użytkownik wprowadza za pomocą klawiatury, w tym także loginy i hasła. Następnie są one przesyłane do atakującego, który może w ten sposób przejąć kontrolę nad kontami użytkownika. Aby ograniczyć możliwości infekcji musimy regularnie aktualizować oprogramowanie antywirusowe oraz aplikować poprawki do aplikacji, których używamy na co dzień.

2. Używaj różnych haseł dla różnych serwisów. Wówczas jeżeli nawet jeden z serwisów zostanie zaatakowany, a dane użytkowników przejęte – dane na innych serwisach pozostaną bezpieczne.

3. Nie udostępniaj haseł do swoich serwisów nikomu, nawet administratorom sieci. Hasło jest sekretem i powinno być chronione. Jeżeli podejrzewasz, że ktoś mógł poznać Twoje hasło, jak najszybciej zmień je na inne.

4. Nigdy nie używaj publicznych komputerów dostępnych np. w hotelach czy kafejkach internetowych do logowania się do ważnych usług takich jak banki, czy konta pocztowe. Komputery w takich miejscach są z reguły pod słabym nadzorem i bardzo często są zainfekowane oprogramowaniem szpiegującym.

5. Większość z nas korzysta w wielu serwisów, które wymagają podania loginu i hasła. Zapamiętanie oddzielnego hasła dla każdego z nich może z czasem stać się problematyczne. Na szczęście z pomocą przychodzą specjalnie stworzone do tego celu programy do bezpiecznego przechowywania haseł. Zapisują one wszystkie informacje w formie zaszyfrowanej, praktycznie niemożliwej do odtworzenia bez znajomości tzw. hasła głównego. Użytkownik jest wtedy zobowiązany zapamiętać jedno hasło do programu, który wprowadzi odpowiednie hasło w serwisie, do którego chcemy się zalogować. Programy do przechowywania haseł możemy znaleźć pod wymienionymi odnośnikami: http://tinyurl.com/622v9m2 oraz http://tinyurl.com/2p385o.

6. Prawie każdy z serwisów udostępnia funkcjonalność podpowiedzi do haseł w momencie gdy nie jesteśmy w stanie przypomnieć sobie właściwego. Podpowiedzi najczęściej są ustalane w momencie rejestracji w danym portalu lub usłudze. Należy być niezwykle rozważnym ustalając taką podpowiedź i podać informację, której nikt inny nie będzie w stanie odgadnąć. Przede wszystkim należy unikać ustalania podpowiedzi do haseł na podstawie informacji, które udostępniamy w portalach społecznościowych lub są o nas powszechnie znane (np. nasz ulubiony kolor lub imię zwierzaka).

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 reagownia 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, Carmen Ruyle Hardy
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz, Łukasz Juszczyk