Moje geslo je ...

Dr. Lorena Mihelač

ŠC Novo mesto

Zakaj redno menjati gesla? Glavni razlog redne menjave gesla je zmanjšati možnost kraje identitete. Glede na to, da veliko storitev opravljamo preko računalnika, se naša identiteta dopolnjuje z omrežnimi komponentami.

Kratka zgodovina uporabe gesla in šifriranja

Uporaba gesla in šifriranje podatkov nista vezana samo za sodobni čas. Gesla in šifrirana sporočila so dobrih 2000 let nazaj uporabljala stara ljudstva, ki so želela na ta način varovati svoje skrivnosti. Pri tem je bilo vedno v ospredju, kako narediti dostop do določenih podatkov čim bolj težaven, oziroma kako šifrirati neko geslo, s katerim se omogoča dostop do strogo varovanih podatkov nekemu posamezniku ali manjši skupini ljudi, ki delijo isto skrivnost. Čeprav so o tem dobrih 2000 let nazaj razmišljala različna stara ljudstva, se Hebrejci omenjajo kot prvi, ki so razvili šifriranje, imenovano »atbash«. Sam princip šifriranja je temeljil na zamenjavi črk (Miller, 2005). Izredno dober sistem uporabe gesla so razvili tudi špartanski vojaki okoli leta 400, in sicer samo z uporabo palice in usnjenega traka (Sabadin, 2006). Uporabo gesel in šifriranje zasledimo v Evropi v srednjem veku zlasti v Italiji. Veliki napredek na tem področju pripisujemo nemškim nacistom, ki so razvili stroj Enigma, s katerim so varovali svoje skrivnosti in imeli možnost šifrirati vsa sporočila. Uporabo gesla na računalniku zasledimo leta 1961 na ameriški univerzi Massachusetts Institute of Technology, ko velika večina ljudi še sploh ni videla računalnika. Naslednja prelomnica so sedemdeseta leta, ko so se prvič pojavile potrebe po kriptografskih metodah za varovanje in skrivanje podatkov (gesel, osebnih podatkov), saj v tem času ni bilo nekih javnih standardov za enkripcijske tehnike. Tako so leta 1979 razvili prvi enkripcijski standard imenovan DES (Data encryption standard). Leta 2001 se prvič uporabi Napredni standard šifriranja (AES), obliko šifriranja, ki jo je sprejela vlada Združenih držav Amerike. Ta standard omogoča varnejše šifriranje kot prejšnji standard šifriranja podatkov (DES) in jo uporablja tudi sistem Windows. Mogoče še nekaj besed o testu CAPCTHA (Completely Automated Public Turing test to tell Computers and Humans Apart). Ta test se pogosto uporablja pri prijavi v forumih in v sistemih, v katerih si ustvarimo brezplačen elektronski naslov. Test je izumljen z namenom, da ugotovi, ali je določen uporabnik človek ali program (stroj). Test CAPCTHA temelji na načelu »poziv-odgovor«, kar pomeni, da spletna stran uporabniku prikaže sliko, na kateri je zaporedje znakov (lahko tudi beseda), in ga pozove, naj znake s slike vpiše v ustrezno pozivno okno. Za izvedbo testa CAPTCHA torej potrebujemo strežnik in uporabnika. Test CAPTCHA sicer naredi (generira) sam računalnik in lahko tudi oceni, ali ga je uporabnik pravilno rešil, ne more pa ga rešiti sam. In prav to omogoča, da lahko na podlagi testa CAPTCHA razločimo med človeškimi in nečloveškimi uporabniki.

Zakaj in kako pogosto menjati gesla?

Z vdiranjem v računalnik, z okužbo (trojanski konji) ali z izkoriščanjem naše lastne nepazljivosti nam naše računalniške identifikatorje tujci lahko ukradejo. V nevarnosti je naša elektronska pošta, osebni podatki na socialnih omrežjih (Facebook, Twitter), bančni račun, kreditne kartice, s katerimi plačujemo storitve, ali izdelek na neki spletni strani. Načini kraje so čedalje bolj pretkani, vendar tatovi na prvem mestu izkoriščajo našo nepazljivost, ko jim po nesreči ali celo namenoma razkrijemo svoje geslo. Prav posebno mesto ima t. i. »ribarjenje«, ko nas neznanec preko lažnih elektronskih sporočil preusmeri na ponarejene spletne strani, kjer vpišemo svoje geslo, ki se nato pošlje neznancu. Posebna zgodba so tudi internetne točke, kjer so pogosto okuženi računalniki, ki jih uporabimo na svojem potovanju, da bi plačali račun, pogledali elektronsko pošto ali preverili stanje na bančnem računu. Če nismo prepričani o tem, ali nam je nekdo ukradel identiteto, to lahko preverimo tudi na spletni strani (https://www.ip-rs.si/kraja-identitete/test/index.html). Da kraja identitete dosega skrb vzbujajoče razsežnosti, kaže primer zgodbe verige trgovin, npr. Maxx in Marshall's, ko je bilo v osemnajstmesečnem obdobju ukradenih 45,7 milijonov kreditnih kartic, 450.000 ljudem pa osebni podatki (nekaterim celo številka vozniškega dovoljenja!). Seveda prepogosta menjava gesla ni zaželena, ker se lahko zgodi, da bo novo geslo manj močno kot prejšnje geslo, oziroma si je težko zapomniti toliko novih gesel. Sistemi nekaterih omrežij (npr. spletne učilnice na univerzah, e-redovalnice) na določena časovna obdobja sami predlagajo menjavo oziroma nas opominjajo, da se izteka čas veljavnosti našega gesla in nas opozarjajo, da zamenjamo geslo v čim krajšem času.

Koliko pogosto menjavati geslo?

Odvisno od tega, za kar se bo geslo uporabljalo; za dostop do računa na banki, za dostop do zelo bistvenih dokumentov ali mogoče za dostop na socialno omrežje (Facebook, Twitter)? Na spletnih straneh, ki so močno varovane, ni treba prepogosto menjavati gesla, vendar tudi to ni pravilo, ker so hekerji vse bolj iznajdljivi v tem, kako priti do gesla in si prisvojiti denar, podatke, identiteto ipd. Zelo priporočljivo je zamenjati vsa gesla predvsem v primeru, če smo z nekom delili isti računalnik in ga zaradi takšnih ali drugačnih razlogov več ne delimo.

Dolžina in vsebina gesla – kako sestaviti dobro geslo?

Če človeški spomin ne bi bil omejen, bi bila dolžina gesla po vsej verjetnosti tako dolga,

koliko to dovoljuje sistem, v katerega vpisujemo geslo. Vendar raziskave kažejo, da je naš kratkoročni spomin vezan za sedem znakov plus minus dva znaka (Miller, 1956). Najlažje in najdlje si zapomnimo tista gesla, ki so za nas smiselna in sestavljena iz znanih besed ali številk. To pomeni, da je včasih treba narediti kompromis glede dolžine in vsebine gesla, kar pomeni, da mora biti dolžina gesla ustrezno dolga, vsebina pa sestavljena iz smiselnih in znanih besed, ki se jih ne glede na to težko ugane. Kako se torej lotiti ustvarjanja novega gesla? Mogoče vam bodo pomagali spodaj navedeni predlogi (ko smo sestavili svoje novo geslo, lahko še preverimo, kako močno je, in sicer kar na spletni strani s »password meter« programom - www.passwordmeter.com):

1. najenostavnejše geslo je sestavljeno iz treh besed, ki nam nekaj pomenijo, npr. »hranapesotrok«. Geslo bo bistveno bolj varno, če uporabimo velike in male črke, npr. »hranapEsoTrok«;
2. geslo lahko sestavimo tako, da uporabimo eno ali dve najljubši števili, eden ali dva najljubša simbola in eno ali dve najljubši besedi, npr. »13*hranaPes/«;
3. geslo lahko sestavimo iz besede ali krajšega stavka in umaknemo samoglasnike, pri čemer »hranapesotrok« postane »hrnpstrk« (pri tem je seveda treba paziti na ustrezno dolžino gesla);
4. pri sestavljanju gesla lahko zamenjamo samoglasnike z ustreznimi številkami, npr. »a« je »1«, »e« je »2«, »i« je »3«, kar pomeni, da bi geslo »hranapesotrok« postalo »hr1n1p2s4tr4k«, z uporabo velikih črk pa »Hr1n1p2s4tr4K«;
5. geslo lahko sestavimo iz prvih črk krajšega stavka, ki nam nekaj pomeni, npr. stavek »po koroškem po kranjskem že ajda zori« postane kot geslo »pkpkžaz«, z uporabo velikih in malih črk pa »PkpKžaZ« (pri tem je seveda treba paziti na ustrezno dolžino gesla);
6. geslo lahko sestavimo iz dveh besed in pri tem kombiniramo njihove črke, npr. ena črka iz prve besede, druga črka iz druge besede in tako dalje, npr. beseda »hrana« in »otrok« postane novo geslo: »hortarnoak«;
7. pri sestavljanju gesla lahko uporabimo tekoče leto in prve tri črke tekočega meseca, npr. 2012okt, in temu dodamo našo najljubšo besedo »otrok« ter dobimo »2012oktotrok«;
8. geslo je lahko sestavljeno iz datuma, ki nam nekaj pomeni in katerega umestimo znotraj svoje najljubše besede, npr. datum 03.01.2013 umestimo znotraj besede »otrok« in dobimo »ot03.01.2013rok«,
9. za geslo lahko uporabimo tudi prve črke besed iz dobro poznanega dolgega stavka, ki si ga lahko zapomnimo, npr. iz »pravljica pripoveduje o deklici, ki je med pometanjem našla krajcar« dobimo geslo »PpodkjmpnK«;
10. geslo je lahko sestavljeno iz dveh besed, ki jih združimo in obrnemo, npr. beseda »Hiša« in »Otrok«, ki postaneta združeno novo geslo »HišaOtrok«. Če te dve besedi obrnemo dobimo končno geslo »KortoAšiH«.

Kaj se zgodi z gesli, ko umremo?

Možni odgovori so: a) tudi gesla »umrejo« s posameznikom, ki je umrl; b) gesla po določenem času postanejo neuporabna, ker posameznik ni spremenil starega gesla v novega, c) posameznik je v oporoki določil, kdo je zadolžen za izbris gesel in profilov na internetnih straneh. V Združenih državah Amerike so na razpolago celo podjetja (http://legacylocker.com/company/about in http://www.securesafe.com/en/partners/entrustet.html.), ki imajo strokovnjake, t. i. digital executorje, za izbris vseh gesel in slik umrlih oseb. Kako vemo, da je neka oseba umrla? Odvisno od države. Na Švedskem se tedensko preverja register živečih oseb in se ugotavlja, kdo je umrl. V Združenih državah Amerike pa vam ponudijo celo možnost, da pri ustvarjanju novega gesla izberete dve osebi, ki bosta o vaši smrti obvestili lastnika spletne strani, pri katerem ste se vpisal z geslom.

Zaključek

Na koncu tega prispevka še ena zanimivost, in sicer 25 najslabših gesel, ki so bila uporabljena in s strani nepridipravov seveda brez težav odkrita v letu 2011: »password«, »123456«, »12345678«, »qwerty«, »abc123«, »monkey«, »1234567«, »letmein«, »trustno1«, »dragon«, »baseball«, »111111«, »iloveyou«, »master«, »sunshine«, »ashley«, »bailey«, »passw0rd«, »shadow«, »123123«, »654321«, »superman«, »qazwsx«, »michael«, »football«. •

Literatura

- Corporate Owner of T.J. Maxx, Marshall's Says Information for 45.7 Million Cardholders Stolen. Pridobljeno na http://www.foxnews.com/story/0,2933,262300,00.html#ixzz29JKePerX
- Yan, J. et al. (2000). The memorability and security of passwords – some empirical results. Pridobljeno iz http://www.cl.cam.ac.uk/TechReports
- Miller, G. A. (1956). The magical number seven, plus or minus two: Limits on our capacity for processing information«. Psychological Review, 63, 81-87.
- Sabadin, R. (2006). Kriptografija in varnost slovenskih e-trgovin. Magistrsko delo. Ljubljana: Univerza v Ljubljani, Ekonomska fakulteta.
- 25 Worst Passwords of 2011 (Study). Pridobljeno iz http://mashable.com/2011/11/17/worst-internet-passwords/.
- Password researchs. Pridobljeno iz http://www.passwordresearch.com/stats/statindex.html.