Password42

Ponavadi je menje v reviji namenjeno globokim, razmišljujočim mislim, a tokrat vas bom načrtno razočarala. Govorila bom o banalnostih. Na dan bom potegnila skrajno nadležno, vsakdanjo, a večno temo. Vprašala vas bom: kako lahko je ukrasti vaše službeno domensko geslo in kaj vam lahko z njim ušpičim?

Verjamem, da ga ni homo sapiensa digitalnega časa, ki ne bi bil primoran, da si vsaj enkrat v življenju zapomni kako geslo. Kaj enkrat v življenju, enkrat na leto, na mesec, na teden! In kaj eno, tri, pet, deset, morda celo več! Pomembnejši kot je, več gesel mora poznati. Vas kar vidim, kako štejete svoja: eno službeno domensko, pa za spletno banko, poštni nabiralnik, kak Google/Yahoo/iTunes uporabniški račun, geslo za dostop do spletnega albuma, pa do Amazonovega, Paypalovga, Ebayevega in Mimovrstnega računa, pa administratorsko od službenega računalnika (ki ga, ups, sploh ne bi smeli poznati), pa digitalnega potrdila, pa službenega računalnika, pa ženinega poštnega nabiralnika, pa ...

Seveda ni nikakršno presenečenje, da so zato naša gesla slaba. Kar slišim vas, kako pri sebi momljate, da to ni neka novost in da imate dovolj drugih pomembnejši izzivov v življenju. A sem vas opozorila, da bom težila z banalnostmi. Vem tudi, da to občasno počne kak zagnan mojster iz ITja ali njegova izvedba varnostne politike, ki od vas pričakujeta izvirno 16-mestno geslo, ki ga je treba menjati tako pogosto kot spodnjice. Kot kaže, vse to ni dovolj.

Čeprav si ljudje radi domišljamo lastno vsemogočnost, smo pravzaprav hudo omejena bitja. Povprečen človek ima po Millerju pomnilniško kapaciteto za obdelavo magičnih +-7 stvari, tako da se gesla za uporabniške račune kmalu začnejo čudežno ponavljati in reinkarnirati v lastni podobnosti. Da bi pretentali hudobno, omejujočo in nadležno varnostno politiko, postanemo ljudje pri izmišljanju novih gesel neverjetno iznajdljivi. Povečujemo zadnjo številko v geslu, dodajamo imena mesecev, letnico rojstva, morda celo vključimo ime svoje simpatije ali domačega ljubljenčka. ITjevci si izklopimo obvezno menjavo gesla (pa šefom tudi) in potem se na najbolj zanimive računalnike prijavljamo z najbolj uganljivimi in ponavljajočimi se gesli. Tako je večina gesel tega sveta prav nesrečno neposrečenih, tako zelo, da jih je, po izkušnjah s terena, približno 80% vseh v domenah možno razbiti prej kot v minuti.

V podjetjih kar nekako pozabljamo, da so gesla zaposlenih ključ do naših najpomembnejših podatkovnih dragocenosti. Najbolj sladko je uganjevati gesla močnih uporabnikov: administratorjev, šefov, tajnic, drugih ljudi z veliko dostopa. Če recimo pridemo do gesla domenskega administratorja, lahko z nekaj truda formatiramo vse diske v domeni, vključno z varnostnimi kopijami. Ali pa rodimo novega domenskega administratorja, ki počne, kar pač hoče. Ali pa nastavimo tako varnostno politiko, da morajo biti vsa gesla dolga 264 znakov in da morajo vsebovati same zvezdice, pa naj se uporabniki pritožujejo po mili volji. In kaj je najlepše? Za težave ne bomo krivi mi, temveč ubogi dejanski administrator.

Problem bi preprosto rešili, če bi pomebna gesla (domenska, administratorska, podatkovnih baz, aplikacijska) redno in učinkovito nadzorovali. Morda se kak potencialni izmuzljivec pritoži nad vdorom v zasebnost, a močnih gesel z rednim preventivnim razbijanjem z omejenimi sredstvi ne bi razkrivali. Tako bi ugotovili samo šibka, ki v sistemu sploh ne bi smela obstajati, lahko pa jih ugane še kdo, ki ga strah pred vdorom v zasebnost ne bi ustavil. Upamo sicer lahko, da bodo staromodna gesla kmalu masovno zamenjala druga, boljša orodja. Porekli boste, da vsak, ki kaj da nase, uporablja pametne kartice, biometrijo, enkratno prijavo in podobno, a če se ozrem naokrog, vseh teh novotarij v domenah nekako ne vidim v masovni uporabi. Zdi se, da jih podjetja najraje podtaknejo v uporabo svojim strankam (»za njihovo varnost«), medtem ko se v lastnih omrežjih z njimi ne trudijo posebej rada.

Zato ko boste naslednjič razmišljali o investiciji v nov milijonski superstroj za varnost, postojte za trenutek. Globoko vdihnite in preštejte do deset. Predstavljajte si denarce, ki vam šuštijo v rokah,

zavonjajte njihov neustavljiv vonj in pod prsti začutite njih bogato obarvan relief. Preden jih vržete skozi okno za naslednjo nemočno seksi varnostno igračko (recimo sistem za odkrivanje vdorov), se tiho vprašajte: jih ni škoda zapraviti, preden ste izčrpali občutno cenejše, učinkovitejše metode? Recimo preverili, če ima vaš administrator za domensko geslo password42, ker je fan Douglasa Adamsa ali pa zato, ker je pred dobrimi tremi leti začel s password1?

Stanka Šalamun, Sistem, september 2009