Kolumna (n)e-varnost
(razmišljanje o učinkoviti digitalni nevarnosti)

Prosimo, odtisnite vaše geslo tukaj!

O tem, kako lahko izgubimo prst.

Malezija, kak mesec nazaj. Računovodja, ponosni lastnik Mercedesa razreda S z vgrajenim sistemom za prepoznavanje prstnih odtisov, po težkem delovnem dnevu koraka proti svojemu avtomobilu. K njemu pristopijo štirje gangsterji z mačetami, ki vztrajajo, da ga peljejo. Po nekaj kilometrih divje vožnje ustavijo, gospoda slečejo, vržejo z njegovega avtomobila in mu z mačeto odsekajo kazalec, saj ga potrebujejo, da sami odpeljejo avto neznano kam.

Barvita, a resnična zgodba, ki kaže na to, da biometričnim mehanizmom vse preveč pripisujemo vlogo avtentikatorjev in ne identifikatorjev, kar so v resnici. Preprosto povedano: od prstnih odtisov, šarenic, vzorcev ožilja na dlaneh, obraznih potez, govora, DNK-ja, vonja in podobnih bioloških izkazov pričakujemo, da igrajo vlogo gesla in ne uporabniškega imena, a je tehnologija za te namene precej neprimerna. Pri vsakem sistemu, ki temelji na tem, da potencialnemu uporabniku dovoli dostop do podatkov predvsem na podlagi njegovih fizičnih lastnosti, postavimo v nevarnost predvsem uporabnike. In ker bodo tovrstne rešitve verjetno uporabljali tudi ljudje s fizičnimi okvarami, bodo morali razvijalci za njih priskrbeti »stranska vrata« in jih tudi nadzorovati, kar bo povečalo kompleksnost sistema. Takšna stranska vrata pa so praviloma šibkejši člen celotnega sistema. Ste že slišali za lopova, ki bi si ob tatvini načrtno izbral težjo pot?

Če že v praksi uporabljamo biometrijo namesto gesel, brez kombiniranja z drugimi varnostnimi metodami, ki bi opravljale funkcijo avtenticiranja, razmislimo vsaj, s kako močnim orožjem si pomagamo. Ptički že čivkajo o tem, da moramo uporabniki izbrati močno, težko uganljivo geslo in da ga naj pogosto menjamo. Prav tako velja, da je gesla potrebno skrbno varovati.

In kako se pri teh zahtevah obnese biometrija? Daleč najbolj popularna biometrična metoda je uporaba prstnih odtisov. Prstni odtis je osebni pečat, ki ga vsak dan odtisnemo na desettisoč mestih. Po kljukah, kozarcih, vratih, stikalih, računalnikih, torbah. Ko nekomu izročite svojo vizitko, mu skoraj zagotovo podarite še prstni odtis. Ironično, pustimo jih tudi na pravih ali sovražnih čitalcih prstnih odtisov. Praktični preizkusi kažejo, da jih je sorazmerno preprosto ponarediti. Če bi morali upoštevati pravilo pogostega menjavanja, recimo enkrat na mesec, bi si, če uporabite poleg prstov na rokah še nožne, že po dveh letih morali odtise sposojati pri sosedih. Še bolj absurdno bi bilo upoštevanje varnostne prakse v točki, ki govori o skrbnem varovanju gesla. Predstavljajte si, da bi, da ne trosite prstnih odtisov, morali vedno nositi rokavice in da ne bi smeli gledati naokrog, da vam kdo ne posname šarenice. Hudo praktično! Zdaj vam je verjetno že jasno, da pri nas doma ne bomo kmalu investirali v novo biometrično ključavnico na vratih.

Ob vseh dvomih v biometrijo kot zanesljivo varnostno metodo pa vseeno obstajajo področja, kjer je lahko zelo uporabna. Zagotovo bomo povečali varnost v sistemih, če jo bomo uporabili kot dodatni varnostni mehanizem ali pa, samostojno, v ne posebej varnostno kritičnih sistemih, kjer potencialna škoda ob zlorabi ni omembe vredna, uporaba pa je zelo priročna. Tudi tam, kjer bomo zamenjali manj zanesljivo »človeško« biometrijo z bolj zanesljiivo »računalniško«, nam zna priti zelo prav. Včeraj so policisti in cariniki preverjali, če slika v potnem listu ali vozniški ustreza določeni osebi, danes pa naprava preveri, če slika pravkar posnete mrežnice ustreza zapisu mrežnice v osebnem dokumentu. Pravzaprav je biometrija lahko učinkovita v tistih primerih, ko na podlagi fizikalnih lastnosti ugotovimo značilnosti skupine, v katero oseba spada, torej ko jo identificiramo, ko oseba zase reče: jaz sem pa tainta. Da pa ji sistem dovoli pristop – torej da osebo avtenticira, se mora odločilno preverjanje zgoditi drugje. Pri tej odločitvi bo imel še vedno glavno besedo človek.

Véliki Bruce Schneier pravi v enem od svojih slavnih Kriptogramov: vsaka nova varnostna metoda spremeni načine napadov. To je začaran krog. V primeru gospoda računovodje, ki verjetno ni več lastnik tistega sanjskega avta, je resničnost še bolj kruta: prej je bila tarča napadov naprava, zdaj je človek. Če je vaš prstni odtis edini ali odločujoči element odločitve, da smete dostopati do varnostno kritičnega sistema, ste najšibkejši in najranljivejši člen vi. Zato pomislite, ko nekdo naslednjič zahteva košček vas na način: prosimo, odtisnite vaše geslo tukaj. Naj bo vaš prstni odtis pripomoček za to, da vas identificirajo, ne pa tudi avtenticirajo. Vaša digitalna identiteta bo tako veliko bolj varna. Vaši prsti tudi.

Stanka Šalamun
Objavljeno v reviji Sistemi (priloga revije Monitor), julij-avgust 2005