Standardizirana nevarnost

Nekaj dni nazaj me je nostalgija po še več Prvinskega nagona privabila v temine udobne kinodvorane. Kokice, kristalno blond Catherine Tramell in londonske nepremičnine niso razočarale, le da prvo tretjino filma nisem bila povsem prepričana, ali gledam napet erotični triler ali kakšno obskurno podtalno ekranizacijo varnostnega standarda BS 7799. Tako film kot standard sta popularna, pa še besed o obvladovanju tveganja in nagnjenju k tveganju je bilo nestandardno veliko. In ker se prvinski nagoni vse prevečkrat zapletejo v kri, nevarnost in težave, se nisem mogla otresti misli na to, da se lahko nekaj podobnega zgodi tudi pri varnostnih standardih. Morda zato, ker želimo med vrsticami standardov slišati, da če bomo usklajeni, bomo v resnici varni. Kar je svetlobna leta daleč od resnice.

Standardi so pravzaprav precej krasna stvar. Če hočemo sebi in svetu razložiti, da smo glede kakšne sorazmerno subjektivne tematike, kot sta recimo kakovost ali varnost, v lokalnem ribniku alfa in omega, potem brez usklajenosti s pravimi standardi skoraj ne bo šlo. Ko želimo utišati nadležne nadzornike ali zadovoljiti tiste, ki nam dajejo licenco za delo, se lahko udobno zatečemo v široka, topla nedrja trenutno popularnega standarda. Če želimo privabiti množice strank, pomahamo s papirjem, kjer na veliko piše »usklajeni«. Vsaj v informacijski varnosti imamo izbire kar nekaj: BS7799, CobiT, SOX, FSA, COSO, CMM-S, FSA ali ISO15408, če se malo poigram z najbolj popularnimi kraticami na tem področju. Lahko so učinkovito orodje vsakega varnostnozavednega vodja IT, ki varnostno besedo širi med vse svoje uporabnike. Ko nam ni čisto jasno, kje bi morali začeti graditi varnost, sledimo napotkom standardov. In potem lahko rečemo, da smo stvari naredili dobro, ker standardi pravijo tako. Dajo nam prave smernice ter zahtevajo razmislek o stvareh, ki niso povsem intuitivne.

Ampak ali to, da smo usklajeni z varnostnimi standardi, v resnici pomeni, da je za varnost poskrbljeno po najvišjih merilih? Da zagotavljamo dejansko varnost podatkov, ki jih zbiramo? Da smo lahko popolnoma prepričani, da ne bomo nehote kršili zakonodaje o varovanju osebnih podatkov? Da nam res ne bo nihče nepooblaščeno brskal po, recimo, naši najpomembnejši podatkovni bazi? Da smo se učinkovito ubranili hekerjev, ker po varnostni politiki redno posodabljamo programsko opremo in zaganjamo protivirusno zaščito? Ali lahko zaradi upoštevanja standardov res trdimo, da smo zelo varni? Bojim se, da ne. Standardi se oblikujejo leta, akademsko, s konsenzom velikega števila strokovnjakov. Postavljajo splošne smernice in si ne morejo privoščiti posebej natančnih napotkov o izvedbi. Kot taki nas težko ubranijo pred najnovejšimi izmišljotinami hitrih, prefriganih, tehnično usposobljenih, ne pretirano moralnih tatinskih umov. Ponavadi nas tudi usmerijo, da si sami določimo sebi optimalni nivo varnosti in nam dovoljujejo, da smo zadovoljni s sabo, če jih dosegamo. Kar lahko v praksi tudi pomeni, da če v varnostno politiko zapišemo, da bomo skrbeli za svoje podatke po najboljših močeh, in smo hkrati bolj šibki ali slabovidni, bo z našo varnostno politiko še vedno vse OK, čeprav nam bodo ukradli čevlje z nog. Preveč je podjetij, ki se hvalijo z varnostnimi standardi že, ko so šele zagrizli v »*PLAN*« del slavnega Demingovega kroga »*PLAN-DO-CHECK-ACT*« in jim je »*DO*« znanstvena fantastika. Za takšne je vprašanje, kako vedo, da njihova varnostna politika deluje, bogokletno in so me zanj sposobni skuriti na grmadi. Morda bom v prihodnje vse take izzvala s stavo za milijon dolarjev, da se jim da vdreti v sistem. Me zanima, če bodo v takem stresu kot pri pripravah na napovedan obisk revizorja.

Ne želim podžigati stare vojne med Windows in Unix svetom, pa tudi o Microsoftovi zavzetosti za varnost ne želim polemizirati, a mimo naslednjega draženja ne morem: dvignite roko tisti, ki se vam zdi, da je MS Windows XP SP2 med 200 najvarnejšimi komercialnimi programskimi izdelki na svetu. Če se z izjavo ne strinjate, naj vam povem, da je Microsoft zanj prejel certifikat svetovno priznanega standarda za aplikacijsko varnost, ISO 15408 ali »Common Criteria«, na nivoju EAL4. Bolj varno in eminentno na tem področju ne gre. Če ste uporabnik, se zaradi tega počutite kaj bolj varovani? In če ste bili skeptik, se vam zdijo napori, varnostne akcije in vložena sredstva učinkovito vloženi? Četudi je po pridobitvi certifikata proizvajalec izdal varnostni popravek, pa še enega, pa naslednjega, ...? Kakšna je torej vrednost takega certifikata?

Kar se varnostne zrelosti tiče, smo, čeprav nam je vsaj BS 7799 znan že leta, precej na začetku. Če bi bili dlje, bi nam bilo jasno, da sta varnostna politika in ocena tveganja pomembna, a le prva koraka. Dokler ne bomo zavrteli magičnega Demingovega kroga hitreje in bolj ambiciozno, nas bo za razliko od Trnuljčice iz varnih sanj prebudil vdor hekerja, zaradi katerega smo zapisali tisti debeli špeh varnostne politike. Če se postopkov občasno drži vsak tretji v podjetju, če svojih varnostnih politik ne bomo upali pokazati svojim strankam, če bomo pred prihodom revizorjem uredili papirologijo, da bo ja vse OK, smo zgrešili osnovni namen najboljšega, kar nam standardi v resnici ponujajo. Tega, da bi si kot Slavko v Dolly Bell lahko rekli: »Svakog dana u svakom pogledu...«. Če ne pridemo tja, smo samo standardizirali nevarnost.

Stanka Šalamun, Sistem, maj 2006