Kavo s smetano, prosim!

Sedim ob kavi, prebiram kupe strani enega najnovejših javnih razpisov za nabavo pomembne narodove programske opreme. Kava je sladka, vroča, z dobro smetano, razpis pa najmanj eno od naštetega. Boleče očitno je, da bo kave do konca prebiranja dokumentov zmanjkalo. A če bi bila smetana na kavi razpisa varnost, bi jo pila ledeno doooolgo črno. S kapljicami mleka.

Razpis nikakor ni prvi, ki se je zataknil na moji mizi. Morda je samo malo bolj pomemben, malo bolj kompleksen, malo dražji od drugih. Veliko jih deli podobno usodo - zaradi mešanice nostalgije, profesionalne radovednosti in ker so pač očitno vsem na razpolago. Če gre za izdelavo pomembne programske opreme, ki je po varnostni plati za naš dvomilijonski narod lahko kjučna, mi nozdrvi zaplapolajo, oči izstopijo, prsti divje klikajo med stranmi. Brskam za opisom varnostnih zahtev v bodočih projektih, odkrivam globino razumevanja varnostnih problemov, ugotavljam sposobnost prevzema odgovornosti odgovornih za varnost.

Ne tako izrazito paranoični umni ljudje iz moje družbe me včasih prijazno obvestijo, da sem morda v svojih željah po dobri kavi s smetano in varnem digitalnem svetu prezahtevna. Nočno prebiranje B. Schneierja in podobnih posebnežev na dolgi rok lahko zaškodi. A ko tako po javnih razpisih kupčkam točke, ki bi z dobrimi merili spodbudile proizvajalce varnostne opreme k bolj pravim, v svetu in z izkušnjami potrjenimi varnostnimi praksami, zasumim, da nekaj ključnega, s čimer bi se morali ukvarjati že v računalniški prazgodovini, manjka: manjka resnost pri zahtevanju tistega, zaradi česar so sistemi bolj varni.

Vrnimo se za trenutek nazaj k naslovni temi tega razmišljanja. Kdaj lahko za neko kavo s smetano zagotovimo, da zadovoljivo ustreza zahtevam in da je med vsemi razpoložljivimi najbolj primerna kava s smetano? Če bi jo iskali z javnim razpisom, bi morda v razpisne pogoje zapisali, da damo vsaki črni brozgi, ki pridiši mimo, po eno točko. Nato naslednji dve, če nam jo prinese slovensko govoreč natakar. Še dodatno točko, če tista bela stvar na vrhu, ki se dela, da je smetana, ne teče čez rob skodelice. Število vseh točk delimo s ponujeno ceno brez DDV. Zmaga tista kandidatka za kavo s smetano, ki jih zbere največje število. Ko povemo, da hočemo samo alpsko stepeno smetano, lahko pričakujemo uradne pritožbe vseh kav, ki bi želele ponuditi nealpske ali nestepene smetane. Dovolj preprosto, ne? Zakaj ne bi na podoben način poskusili oceniti tudi javnih razpisov za nabavo državnega softvera? Naj zmaga tisti razpis, ki bo prerastel naštevanje zahtevanih varnostnih mehanizmov in bo znal najbolje določiti merila za zadovoljivo varnost končnega izdelka. Če lahko v javnih razpisih precej dobro določijo, kako si predstavljajo vsebine posameznih spletnih form, bi se morda v njih lahko znašle tudi napredne in zrele ideje o dejanski varnosti končnega izdelka.

Najprej pričakujem, da je za projekte nad milijon evrov varnost ena izmed ključnih funkcij. S tem naročniki svojim državljanom in njihovim dobaviteljem smrtno resno povedo, da sprejemajo polno odgovornost za naše osebne podatke in denar, ki ga v našem imenu porabljajo. Ker bodo v razpisu objavili zelo veliko operativnih podrobnosti bodočega programja, morajo nadzirati, kdo vse ga prebira in ga zato ne smejo kar tako nalepiti na Internet. Zahtevati morajo, da v projektu sodeluje vsaj en, še bolje pa več, preizkušenih specialistov za informacijsko varnost - pa naj bodo mojstri vgrajevanja varnostnih čudes ali ponosni lastniki svetovno priznanega varnostnega certifikata. Zapovedati morajo izdelavo varnostnega profila in modela groženj aplikacije. Razvpitim varnostnim mehanizmom (ja, tudi šifiriranju, pametnim karticam, nadomestnim lokacijam in revizijskim sledem) je v velikem svetu že davno potekel status varnostnih megazvezd, so pa v skupini »nujni na projektu«, tako kot voda v kavi in o tem dovolj besedi. Prav tako je igre konec, če v razpisu ni zahteve po vodenju seznama odprtih in zaprtih ranljivosti - takrat se ranljivosti ponavadi iščejo po neučinkovitem principu »tudi slepa kura včasih zrno najde«. Naslednja nujna zahteva je, da naj varnostne luknje sistematično iščejo potrjeni strokovnjaki, taki, ki so kdaj kakšno že prav zares sami našli. Pravzaprav je vsak razpis, ki ne zahteva, da naj si dobavitelj vzame za varnostno testiranje vsaj toliko časa kot povprečen potencialen napadalec, milo rečeno osebna žaljitev pomembnosti naših podatkov. Razpis mora tudi zagroziti z resnim neodvisnim varnostnim preverjanjem ali podeliti bonus točke, če kaj takega organizira dobavitelj sam.

Kot pri vseh dobrih javnih razpisih mora biti tudi tu zelo pomemben kriterij cena, a tokrat malo drugače: višja ko je, več dela je v rešitvi, večja je kompleksnost izdelka, več ljudi se bo večkrat zmotilo, več hekerjev bo večkrat lahko izrabilo ranljivost - torej mora biti odpravljanju teh napak posvečenih več naporov. Dodatne točke podelim za iniciativo po preganjanju najbolj razvpitih programerskih napak ter za spremljanje krivulje odkrivanja ranljivosti. Za vsak dokaz zahteve po uporabi varnostnega inženirskega pristopa, lahko tudi kopiran po MS SDL, zapišem pisno pohvalo in jo objavim v Uradnem listu. Izkazovanju znanja, da varnostno testiranje ni enako testiranju varnostnih funkcij, namenim poznavalski poklon, kot tudi zahtevi po izdelavi načrta testiranja varnostnih funkcij. Vsaka zahteva za varnostno izobraževanje zaposlenih pri naročniku ali dobavitelju prinese dodatnih nekaj točk. Pa še bi lahko naštevala, a bom raje srknila poslednji požirek z dna skodelice.

In vzdihnila ob preblisku, da so moje želje še neskončno daleč od uresničitve. Tolaži dejstvo, da sem v njih vedno manj sama. Vedno manj ljubiteljev dobre kave s smetano se bo pustilo prepričati, da je vsaka črna brozga s sledmi mlečne maščobe res kava s smetano.

A nekega lepega dne se bo končno zgodilo - po neslišanih milijonkrat ponovljenih besedah, po popitih hektolitrih in tisoč nepripisanih točkah. Naučili se bomo bolje zahtevati, kar nam pripada. Nekdo bo končno rekel: vročo kavo s pravo sladko alpsko stepeno smetano prosim. Nič slabše kot to!

Stanka Šalamun, Sistem, mar 2008