Nič več brezplačnih kosil

Predstavljajte si, da drago kupite varen avto, potem pa se izkaže, da v ključnih trenutkih zračna blazina ne dela ali da popustijo zavore - kljub vsem dragim servisom in zagotovilom, da je varnost na vrhunskem nivoju. A ne bi bili vsaj malo hudi, da vas je proizvajalec vlekel za nos?

Jaz bi bila. Še posebej bi me jezilo, če bi se to dogajalo pogosto, kljub dolgotrajnim opozorilom strokovnjakov in če bi šlo za sorazmerno banalne vzroke s preprostimi rešitvami. Če bi lahko, bi seveda zamenjala vozilo, a pogosto to iz različnih razlogov ni mogoče. In ne, nikakor ne bi pristala na to, da mi bodo za obljubljeno boljšo varnost dodatno zaračunali, saj sem jo v dobri veri plačala ob nakupu.

Pri drugi vrsti izdelkov, recimo aplikacijah, se uporabniki obnašamo bolj brezbrižno. Kot da še nismo povsem doumeli, da lahko zaradi lukenj v programski opremi prav tako umremo kot zaradi pokvarjenih zavor, prav tako nam uplenijo denar ali, kar je za marsikogar dandanes še nepomembno, ukradejo identiteto ali zasebnost. In vse zaradi veliko malih površnosti, ki se jih nekomu ne splača temeljito odstraniti. Tako veliki proizvajalci programske opreme še naprej vrtijo svojo pokvarjeno ploščo ignorance in le peščica zagnancev – neodvisnih varnostnih raziskovalcev - na glas kriči, da nekaj tu ni prav.

Raziskovalci zagotovo nosijo svoj delež greha v tej zgodbi. V dobri veri, da bodo z odgovornim razkritjem pomagali zmanjšati skupno varnostno izpostavljenost uporabnikov, so proizvajalce, le za čast in slavo, razvadili z brezplačnim obveščanjem o ranljivostih. S tem so razvrednotili pomembnost odpravljanja ranljivosti (ker so bili proizvajalcem le škodljiva motnja), odvzeli varnostnim napakam njihovo pravo ceno in skoraj popolnoma uničili njihov legalni trg. Hkrati se je razcvetelo črno trgovanje, ker so proizvajalci družno sklenili, da ranljivosti ne bodo odkupovali.

Morda se vam zazdi, da ta tematika ni za našo Betajnovo, saj lahko na prste ene roke naštejemo sodržavljane, ki se jim je že kaka velika firma zahvalila za odgovorno razkritje ranljivosti. Tudi domači proizvajalci so pretežno še v infantilni fazi, ki bi jo lahko na kratko opisali z »Mi pa ne delamo varnostnih napak!«. A brez skrbi, tudi to bomo prerasli. Ne morete pa mimo dejstva, da ste uporabniki, naročniki in plačniki, če že ne drugače, vsaj kje kakega operacijskega sistema. Zato bi vas moralo globoko zaskrbeti dejstvo, da **nekateri največji svojih znanih ranljivosti niso odpravili že več kot 1000 dni in da ves svet to ve**. Hkrati taisti na veliko služijo z lastnimi varnostnimi rešitvami in storitvami (kot recimo HP in IBM) in bi morali biti pri odpravljanju lastnih varnostnih lukenj še posebej dosledni.

A še bolj neetično je, da proizvajalci drago prodajajo rešitve, ki ne vključujejo tega, kar oglašujejo (torej varnosti), ter pričakujejo, da se bo dalo še naprej brezplačno »šlepati« na tujem, težko pridelanem znanju raziskovalcev. Saj delež svojih ranljivosti zagotovo najdejo in odpravijo sami, a jih očitno vse preveč pustijo v kodi. Zato bi prav vsem koristilo, če se bi naučili določiti pošteno ceno za ranljivosti in omogočili delovanje trga. Tako bomo s skupnimi močmi precej hitreje poiskali luknje v softveru in jih tudi prej odpravili.

Raziskovalcem trenutna situacija ni naklonjena: nekaj sprevrženega je ponuditi storitev in zahtevati plačilo, če je naročnik ni naročil - a če jih ne bi bilo, bi imel vaš računalnik še precej več lukenj. Raziskovalna srenja je tudi utrujena od že vsaj petnajstletnega jalovega boja z brezplačnimi dokazovanji banalnih prekoračitev vmesnikov, sql vrivanj in podobnih osnovnih napak, počasi so porabili ves zagon. A po novem se upirajo. Spreminjajo svoj odnos do lastnega dela in znanja. Končno jim, po letih družbenega dobrodelništva, ki so jim ga vsilili (večinoma precej premožni) proizvajalci programske opreme, ni več vseeno, da brezplačno opravljajo težaška dela za tiste, ki poberejo ves denar. Zakaj bi proizvajalce obveščali odgovorno, če pri teh traja povprečen odpravek ranljivosti neodgovorno dolgo? In kaj je v tem dobrega za njih? Dobrodelnost pač ne plačuje recesijskih položnic.

Zato beli trg ranljivosti nastaja obotavljajoče, a zagotovo. Na eBayu so v preteklosti že prodajali ranljivosti, prav tako jih odkupujejo posredniki. Google je za napako v spletnem brskalniku Chrome ponudil nespodobnih 500$. Resni raziskovalci pravijo, da je cena žaljivo nizka, kar lahko potrdi vsak, ki je že kdaj odgovorno raziskoval in javil resno ranljivost. A če želite res dobro zaslužiti in imate potreben pogum in zveze, poskusite pri vladnih agencijah. Šušlja se, da jim je milijonček za kritično ranljivost ob vseh njihovih dnevnih stroških omembe nevreden drobižek. Kaže torej, da se časi podarjanja ranljivosti za zmeraj končujejo.

Stanka Šalamun, Sistem, marec 2010