Šibkosti najmočnejših

Uspešen ropar je iskreno izdal naslednjo modrost: »Medtem ko ključavnice postajajo vse bolj zapletene, so vrata in podboji vedno bolj šibki. Le nekaj konkretnih sunkov na pravih mestih je potrebnih, pa sem v hiši.« To zelo diši po tem, kako dandanes pred napadalci poklekajo naši varni informacijski sistemi. Lahko bi v njih vdirali grandiozno, z velikim pompom in obiljem izredno zapletene tehnologije, pa ni tako. Ker to sploh ni potrebno in še dolgo ne bo. Smo pač še vse preveč ranljivi.

Na šibkosti najmočnejših sem trčila, ko sem prvič doživela in doumela vroče vznemirjenje pravega, globokega, uspešnega hekinga pri sodelovanju na mojem krstnem penetracijskem preizkusu. Od takrat se sprašujem, zakaj se vsi trudijo z neskončno zapletenimi in dragimi varnostnimi mehanizmi, če pa ob tem puščajo en kup zelo očitnih varnostnih lukenj, ki kar čakajo, da na široko odprejo zadnja vrata v informacijski sistem. Krilatica, da je varnost celotnega sistema le toliko močna, kot je močen njen najšibkejši člen, še ni uspela ubežati iz visokoletečih teoretičnih svetov v realnost, kjer bi že davno morala imeti pomembno mesto. Zgleda, kot da se lekcija nikogar ne prime, čeprav se zdi, da jo ljudje slišijo in se celo delajo, da jo v kakšnih resnično čudaških sanjah morda celo razumejo in upoštevajo.

Izvirni greh velike večine varnostnih problemov v naših informacijskih sistemih je v dvojnem, v osnovi nasprotujočem poslanstvu ljudi, ki odločajo o nivoju varnosti in skrbijo zanjo. Po eni strani morajo brezpogojno prepričevati uporabnike, naj zaupajo v varnost sistemov, saj jih bodo tako uporabljali bolj učinkovito. Vsem morajo jasno pokazati, da so močni, da so hkrati Ahili, Samsoni in Goljati današnjega časa. Po drugi strani morajo poskrbeti, da sistemi v resnici ne bodo pokleknili pred napadalci – torej se morajo skoraj o vsem o sebi iskreno vprašati, kje so najšibkejši: v peti, laseh, čelu ali kje drugje.

Ujeti prvi cilj je precej lažje in ceneje. Vsi se radi vidimo kot nepremagljivi heroji. Velike besede, kot so »popolne varnosti tako ali tako ni« ali »zelo dobro skrbimo za varnost«, celo močna in razvpita »nezlomljivo«, lahko zdrsijo lahkotno in ljubko iz ust kot morska voda po od sonca razgreti, s sončno kremo namazani vroči koži. Prav nič napačno ne delujejo, zaradi njih še nihče ni izgubil službe. Kar poskusite, prijetno in preprosto jih je izgovarjati, zato jih tudi velikokrat slišimo.

A priznati si vse svoje šibkosti in slabe navade, ki smo jih dosledno, velikokrat nezavedno nabirali ves čas, je bistveno težje delo. Še bolj naporno je odpraviti jih, dokončno, vsako zase. Iskanje šibkih členov sistema je pravzaprav zelo naporno, velikokrat enolično, duhamorno, prav nič zveličavno delo in zaradi njega se jih je le malo proslavilo. Za veliko stvari niti ne vemo, kako naj jih najdemo. In ko jih končno ugotovimo, se zavemo, da bo za odpravo potrebnih veliko doslednosti, nadzora, razlaganja, pregovarjanja in tudi nepopularnih sprememb. In nas malo mine volja.

Vdori se ponavadi zgodijo zaradi serije malih, na videz nepomembnih in nepovezanih slabosti v sicer močnih sistemih. Takih, ki bi jih vsako posebej lahko morda preprosto odpravili. Če napadalec izkoristi eno samo našo varnostno napako, je varne igre konec. Ko podatki enkrat uidejo iz sistema, so se razkropili za vedno in nikoli več jih ne moremo nadzorovati. Zato lahko naredimo sto stvari popolnoma prav in eno le malo narobe, pa več ne bo varno. Napadalca ne zanima število vgrajenih varnostnih mehanizmov, niti kako zelo moderni so, niti to, da jih zahteva EU, kaj šele, ali so certificirani. Zanima ga samo ena sama mala napakica, slab dan programerja ali administratorja, nedoslednost v našem kompleksnem sistemu, slabo nadzorovan vhodni vmesnik, en sam uporabnik s prehitrimi prsti. Išče samo najlažje, najbolj očitne poti - največje šibkosti sistema. In te so ponavadi banalne: uganljiva gesla, neuradne brezžične in telefonske vstopne točke, preprost fizični dostop do omrežne vtičnice v fotokopirnici naše najbolj zakotne izpostave, pozabljena odprta vrata na požarnih zidovih, naivni uporabniki, aplikacije z osnovnošolskimi ranljivostmi in skoraj popolnoma nezavarovani viri v varnem zaledju požarne pregrade.

Zato nehajmo sanjariti o tem, da bodo močni varnostni mehanizmi ustavili napade. Napadalci se jih niti lotili ne bodo. Zakaj bi razbijali 128-bitno šifriranje, če pa je lažje priti do istih podatkov s socialnim inženiringom? Zakaj bi se vdiralci po požarnem jašku prebijali do sobe s strežnikom in nato viseli z glavo navzdol na žici, če pa lahko dostopajo do njega po omrežju? Zakaj razbijati pametne kartice, če pa lahko bolj preprosto ukradejo uporabnikovo sejo ali še bolje, kar njegovo identiteto? Zakaj bi se izpostavljali in varnostniku v banki po filmsko podtikali nadzorne posnetke, medtem ko bodo v resnici grozili uslužbenki za bančnim pultom, če pa lahko s pravo kombinacijo napadov na ranljivo aplikacijo od daleč odpeljejo taiste dolarje?

Močne najbolj izpostavlja njihovo skoraj religiozno zaupanje v lastno moč. Zato bi bilo bolj varno, da namesto triumfiranja ob močnih členih končno začnemo odpravljati najšibkejše. Da ne bomo kot Ahil, ki se je po tem, ko

ga je smrtna puščica zadela v peto, lopnil po glavi in si rekel: oh neumnež jaz, mar bi na boj obul škornje namesto sandal!

Stanka Šalamun, Sistem, jun. 2007