Kvantum tolažbe

So stvari, za katere je škoda trošiti moč človeških rok in čas inteligentnih umov. Recimo za kopanje jarkov, košnjo trave, izračun milijonte decimalke Ludolfovega števila ali ročno prepisovanje knjig. Zato smo si za neprijetna dela zvito umislili stroje, računalnike, robote, programe in podobno tehnično pomoč, ki vse naredi sama. Ko bi le za vse neprijetne stvari v življenju imeli kak magični gumb.

Vsak resen šef ITja, ki kaj da na ugled svojega podjetja, je tako že pred časom nakupil vse potrebne požarne pregrade, protivirusne zaščite in rešitve za boj z e-slamo. Ne znam si ga predstavljati junaka, ki se mu ne bi zasvetile oči ob ponudbi, da z eno samo ne preveliko investicijo za dalj časa kupi mir, občutek varnosti in reši večino svojih varnostnih problemov. Resnično napredne šefe sem videla odpirati denarnice za sisteme za odkrivanje in preprečevanje napadov ter nakupovati limanice za nesposobne hekerje. S tako odločitvijo ne morete pihniti zelo mimo, vedno jo lahko zagovorite pri šefih, marketing oddelek ima argumente za prepričevanje javnosti, pa niti predrago ne zgleda. Postavite škatlo pod pisalno mizo, namestite programski paket, malo povrtate po nastavitvah, zaženete binarije in ste varni. Sistem dela sam, alarmi se že oglašajo. Virusi, nimate vstopa. Skriptni mulc, boš moral še malo povaditi. Sledi napadov polnijo diskovje z gigabajti forenzičnih dokazov.

Pa se je izkazalo, da so se nekje v igri spremenila pravila. Skriptni mulci so odrasli, denar jim je pomembnejši od časti, posel v ilegali je odličen. Topove so zamenjali z natančno namerjenimi laserskimi žarki. Izklopili so grobo računalniško moč in vklopili intelekt, domišljijo in talente. Z vso silo so napadli najšibkejše člene sistemov – predvsem ranljivo programsko opremo, še posebej tisto, ki se pogovarja s spletom. Ranljivih tarč je za vse dovolj.

V velikem daljnem svetu na drugi strani luže, kjer nameravajo v naslednjem letu za informacijsko varnost zapraviti vsaj 10% IT proračuna, so v odgovor presenetili z vklopom grobe računalniške moči in izklopom večine talenta, domišljije in intelekta. Kot protiukrep hekerjem na njihovo drezanje v aplikacijske rane so se opremili z raznolikimi avtomatskimi in polavtomatskimi pripomočki, takimi z magičnimi gumbi na klik. Z njimi natančno prevohajo vsako ničlo in enico, ki pride v sistem ali iz njega. Prav vsako, nobena ne uide. Tako pikolovsko preskenirajo vseh 100 odstotkov ničel in enic, ne enkrat, nekajkrat. Z enako natančnostjo se lotijo prav vseh vrstic programske kode – tako izvorne kot izvršljive, vseh 20 milijonov, če je treba. Le kje boste našli tako vzdržljivo skupino za testiranje, ki ne bo umrla od dolgčasa, ko bo v neskončnost vrtela iste preizkuse? In kateri superheker bo sam sposoben tega? Tako je nabava orodij ali storitev za iskanje ranljivosti v programski opremi postala pravi nakupovalni hit, a kljub temu ni videti, da smo kaj bistveno bolj varni. Še sreča, da nekateri zaradi novih igračk vseeno bolje spijo, kar vsaj malo opraviči njihove stroške.

A hekerji še bolj učinkovito pikajo v varnostne luknje programske opreme. Razlogov za to je več. Tudi najbolj napredna orodja je potrebno odlično umeriti, da dajejo pametne rezultate, kar je delo za (primerno usposobljenega) strokovnjaka. Računalnik zna mojstrsko iskati vnaprej določene, dobro znane in »sumljive« vzorce v ogromnem kupu naključnih znakov in seveda pričakujete, da dosledno najde vse. Potem se je treba pregristi skozi neskončno dolgočasne sume o potencialnih ranljivostih, od katerih je morda le vsak stoti resnični varnostni problem, analiza vseh ostalih pa vam vzame nesorazmerno veliko dragocenega časa. Tudi najbolj glasne rdeče alarme počasi preslišite, ko jih (lažne) danes vidite že stotič. Ob takem delu se človek hitreje postara. Pa še po nepotrebnem strašite ljudi z nevarnostmi, ki to sploh niso in tvegate, da tudi vas naslednjič ne bodo jemali resno. Nekateri programi pa so celo toliko specifični, da si z avtomatiko sploh ne morete pomagati, ker ne prileze veliko dlje kot do vstopne strani v sistem - če ste kdaj poskušali avtomatizirati testiranje uporabniških vmesnikov, veste, o čem govorim. Zato začnete počasi izklapljati iskanje neučinkovitih vzorcev, vaša raziskovalna vnema popusti in na disku se nabirajo revizijski zapisi, ki nikogar ne zanimajo. Na računalniku pod mizo se nabere debela plast prahu. Zaljubljenost v kraljico drame se je ohladila, ne ljubi se vam je več ujčkati.

Najslabše pa je to, da **avtomatsko orodje spregleda veliko večino resnih varnostnih problemov, medtem ko vas zaposluje z morjem manj pomembnih.** Z avtomatiko pač ne morete najti napak, ki zahtevajo sposobnost logičnega razmišljanja, take pa so najbolj resne in z njimi pride do največ škode. Orodja tudi niso dovolj dobra, da najdejo prav vse, tudi bolj zapletene pojavne oblike napak, za katere so specializirana, tako da se moti tisti, ki zagotavlja, da njegovo orodje najde vsa SQL vrivanja. Če bi se vsaj malo zanesli na človeški intelekt, domišljijo in talente, bi po poročilu WASC našli vsaj dvanajstkrat več resnih napak kot jih najdete s klikom na gumb avtomatskega orodja. Verjetnost, da s pomočjo razuma najdete resno ranljivost na poljubni spletni strani, bi se iz 8% dvignila kar na alarmantnih 96 %.

Tako se izkaže, da je skupni strošek lastništva avtomatskega orodja precej draga stvar, namesto katere bi si lahko privoščili zajeten kolač drugih, varnostno bolj učinkovitih aktivnosti. Nedvomno je v avtomatiziranju varnosti drobec učinkovitosti. Bolje to kot nič. Iz naših računalniških sistemov in aplikacij odstranimo vsaj najbolj očitne varnostne težave in povečamo robustnost sistema. Tudi taki pristopi prinesejo svoj kvantum varnosti.

In kvantum lažne tolažbe.

Stanka Šalamun, Sistem, oktober 2008