» Leto nevarnega (IT) življenja

Esad Jakupović

V današnjem digitalnem svetu se vsi soočamo s kibernetskimi napadi. Letos bo za informacijsko varnost porabljeno skoraj 100 milijard dolarjev, v obdobju 2016–2021 pa skoraj bilijon. Kako bo potekal boj proti grožnjam?

Dejstva o informacijski (ne)varnosti so zelo zaskrbljujoča: vsaj 58 podjetij v svetu je v zadnjih 12 mesecih doživelo najmanj en vdor v podatke, polovica teh pa je zabeležila tudi vsaj en notranji varnostni dogodek, poroča analitsko podjetje Forrester Research na podlagi svoje obsežne raziskave. Pri tem so bili v več kot tretjini vseh vdorov vključeni tudi poslovni partnerji ali dobavitelji.

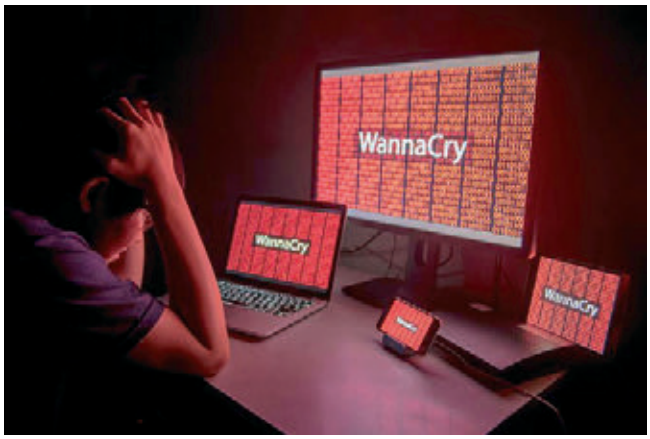
Hitro odpravljanje ranljivosti

Pozorni moramo biti tudi na podrobnost, ki jo v svoji globalni raziskavi poudarja Forrester Research: v 41 odstotkih primerov zunanjih napadov so vrata IT-vlomilcem odprle ranljivosti v programski opremi, ki so bile že znane. Pošastni primer je zaporedje dogodkov po uhajanju »izkoriščevalca« EternalBlue, ki ga je domnevno razvila ameriška Agencija za domovinsko varnost (NSA), do katerega je prišlo 14. aprila 2017. EternalBlue izrablja Microsoftovo storitev Server Message Block (SMBv1), ki jo Microsoft že desetletja vgrajuje v vsak operacijski sistem Windows. Kljub takojšnjim Microsoftovim popravkom je bila ranljivost izrabljena za množični vdor izsiljevalskega virusa WannaCry v 230.000 računalnikov v 150 državah v samo 24 urah, kar je povzročilo škodo med nekaj sto milijoni in štirimi milijardami dolarjev. Približno mesec dni potem je izsiljevalski virus NotPetya povzročil še okrog 300 milijonov škode.

» *Življenje z grožnjami: za IT-varnost bo letos porabljenih 96,3 milijarde dolarjev, 8 odstotkov več kot leta 2017.*

» *Boj brez konca: notranji in zunanji nepridipravi bodo vedno iskali načine, da bi poškodovali, popačili ter ponaredili podjetniške sisteme in podatke.*

Podatek, ki dobesedno straši profesionalce s področja kibernetske varnosti, je dejstvo, da je do napada prišlo 60 oz.90 dni potem, ko je Microsoft popravil ranljivost. Drugače povedano, ranljivosti praktično sploh ne bi bilo, če bi vsi redno in takoj posodabljali operacijski sistem in ključne aplikacije. Zato bo v letu 2018 upravljanje varnosti in ranljivosti (SVM) ključnega pomena za profesionalce, ki skrbijo za varnost, opozarja Forrester. Upravljanje varnosti/ranljivosti se je našlo tudi na prvem mestu na seznamu vodilnih groženj, ki ga je analitsko podjetje sestavilo po obsežni raziskavi med več kot 600 odločevalci, ki skrbijo za omrežno varnost v podjetjih z več kot 1000 zaposlenimi. Na drugem mestu groženj so se znašle nezavarovane storitve v oblaku, ki že več let povzročajo odtekanje občutljivih podatkov. Zadnja leta je zabeležena vrsta velikih odtekanj zaradi napačno konfiguriranih storitev v oblaku, kot sta MongoDB in Amazonov Simple Storage Service (S3). Samo v tretjem trimesečju 2017 so zaradi takšne vrste odtekanja podatkov Time Warner, Verizon in Viacom izgubili šifrirne ključe, detajle računov strank in druge občutljive podatke.



» Nemarnost plačana z najmanj 300 milijoni dolarjev: virus NotPetya se je razširil po svetu kljub izkušnjam z virusom WannaCry in kljub dobro znanemu popravku ranljivosti.

Škodljivci pod povečalom

Razvijalec varnostne programske opreme Kaspersky Lab poroča, da so lani zaznali v povprečju 360.000 novih zlonamernih datotek na dan, 11,5 odstotka več kot v letu 2016. Po rahlem upadu v letu 2015 se je število zaznanih zlonamernih datotek tako že drugo leto zapored povečalo. Število odraža aktivnost kibernetskih kriminalcev, ki ustvarjajo in razširjano zlonamerno programsko opremo. Pri prvem izračunavanju, v letu 2011, je bilo zaznano 70.000 datotek na dan, v naslednjih letih pa se je število povečalo za več kot petkrat. Večina nevarnih datotek spada v skupno kategorijo zlonamerne programske opreme (78 odstotkov). Virusi, katerih prisotnost se je zaradi kompleksnega razvoja in majhne učinkovitosti pred petimi do sedmimi leti precej zmanjšala, še vedno povzročijo 14 odstotkov vseh zaznavanj. Preostanek (8 odstotkov) predstavljajo oglaševalski programi, ki niso privzeto zlonamerni, ampak lahko v številnih primerih povzročijo razkritje zasebnih informacij in druga tveganja. Približno 20.000 vseh dnevno zaznanih nevarnih datotek je prepoznal strojno učeči sistem Kaspersky Laba za analizo zlonamerne programske opreme Astraea, ki samodejno identificira in blokira zlonamerno programsko opremo.

»Leta 2015 smo bili priče upadu dnevno zaznanih zlonamernih datotek – tako smo celo domnevali, da je nova zlonamerna programska oprema manj privlačna za spletne nepridiprave, ki so raje še naprej uporabljali starejše pristope,« razlaga Vyacheslav Zakorzhevsky, vodja raziskovalne skupine za preprečevanje napadov pri družbi Kaspersky Lab. Na žalost je zadnji dve leti število odkrite nove zlonamerne programske opreme znova naraslo, kar je znak, da med kriminalci obstaja interes za ustvarjanje novih zlonamernih kod. »Veliko naraščanje napadov z izsiljevalskimi virusi v zadnjih letih se bo nadaljevalo, saj je v ozadju velikanski kriminalni sistem, ki dnevno ustvari več sto primerkov tega tipa grožnje,« opozarja Zakorzhevsky. Vzporedno z naraščajočo priljubljenostjo kriptovalut so lani pri Kaspersky Labu opazili tudi vzpon t. i. rudarjev, ki tuje računalnike nepooblaščeno uporabljajo za »rudarjenje« za kriptokovanci (v svetu bitcoinov in drugih kriptovalut denar ni natisnjen, ampak se odkriva). Podjetje še opozarja, da lahko razlog za povečanje zaznav v letu 2017 deloma pripišemo nenehnim izboljšavam varnostnih tehnologij, ki prispevajo k boljši identifikaciji zlonamerne programske opreme.

› Nekaj nasvetov Kaspersky Laba proti grožnjam

- Bodite pozorni in ne odpirajte sumljivih datotek ali priponk od neznanih pošiljateljev.
- Ne nameščajte aplikacij, ki ste jih prejeli od nezanesljivih virov.
- Ne odpirajte spletnih povezav, ki ste jih dobili od neznanih virov in v sumljivih spletnih oglasih.
- Uporabljajte močna gesla in jih redno spreminjajte.
- Redno nameščajte posodobitve. Veliki izbruhi izsiljevalskih virusov, kot sta bila WannaCry in ExPetr, so pokazali, da lahko nameščanje popravkov traja tudi več mesecev.
- Nikoli ne upoštevajte sporočil, ki od vas zahtevajo, da onemogočite protivirusno programsko opremo ali varnostne sisteme za Office.
- Namestite varnostno rešitev, ki je primerna za vašo vrsto naprave in sistem.

Sto milijard za varnost

Za IT-varnost bo letos porabljenih 96,3 milijarde dolarjev, 8 odstotkov več kot leta 2017, poroča analitsko podjetje Gartner. Razlogi za rast so poostreni predpisi, večje zavedanje o nevarnostnih, razvoj strategij digitalnega poslovanja in tehnološki napredek. »Rast porabe je reakcija na povečane varnostne težave in višji profil kibernapadov,« pravi Ruggero Contu, raziskovalni direktor pri Gartnerju. »Izbruhi, kot so WannaCry in NotPetya ter novejši Equifax, so neposredno vplivali na potrošnjo za varnost, ker so trajali več kot tri leta,« je povedal. To potrjuje tudi Gartnerjeva raziskava med 512 anketiranci v osmih državah

(Avstraliji, Kanadi, Franciji, Nemčiji, Indiji, Singapurju, Veliki Britaniji in ZDA), v kateri je 53 odstotkov udeležencev postavilo varnostna tveganja na prvo mesto med gonili potrošnje za varnost. Največjo rast in največji delež bosta zabeležila segmenta zaščite infrastruktur in varnostnih storitev. K rasti potrošnje za varnostne rešitve so zadnja tri leta pomembno prispevali regulatorni predpisi v ZDA in Indiji, na Kitajskem ter sedaj v Evropi (Splošna uredba o varstvu podatkov, GDPR, ki bo začela veljati 28. maja).

Poraba posebej raste v podsegmentih varnostnega testiranja, orodij za varnost podatkov, zunanjega izvajanja, upravljanja privilegiranega dostopa (PAM) ter upravljanja varnostnih informacij in dogodkov (SIEM). Leta 2020 bo več kot 60 odstotkov organizacij (danes približno 35 odstotkov) investiralo sredstva v večkratno zaščito podatkov – za orodja za preprečevanje izgube podatkov, zaščito podatkov in šifriranje. Pomanjkanje veščin, tehnična kompleksnost in raznovrsnost groženj spodbujajo tako širjenje avtomatizacije na področju varnosti kot tudi angažiranja zunanjih varnostnih svetovalcev, ponudnikov upravljane varnosti in na splošno zunanjega izvajanja. Gartner ocenjuje, da se bo letos poraba za varnostne storitve zunanjega izvajanja povečala za 11 odstotkov, na 18,5 milijarde dolarjev. »Zunanje IT-izvajanje je drugi največji segment porabe za varnost, po svetovanju,« poudarja Ruggero Contu. Leta 2019 se bo potrošnja za zunanje varnostne storitve povečala na 75 odstotkov porabo za strojne in programske varnostne produkte, ki je v letu 2016 znašala 63 odstotkov. Proračuni za varnost v podjetjih rastejo posebej v segmentu odkrivanja in odzivov, kar bo v prihodnjih petih letih gonilo rasti varnostnega trga.

› Kaj bo letos najbolj skrbelo strokovnjake za IT-varnost

Vzporedno z razvojem IT-sistemov v pisarnah, proizvodnih prostorih, prometnih sistemih, domovih in drugod se nadaljuje neustavljivi boj med varnostnimi strokovnjaki ter rastočimi in nenehno se spreminjajočimi skupinami nepridipravov. Te se poskušajo vtihotapiti v omrežja in odtujiti občutljive podatke, da bi z njimi izsiljevali, jih prodajali in jih kako drugače zlorabljali s ciljem zaslužka ali povzročanja škode. V znanem spletnem portalu TechRepublic so analizirali 518 napovedi v 46 kategorijah kibernetske varnosti, ki jih je objavilo 83 organizacij. Iz njihovih ocen so izdelali zbirno preglednico, ki predstavlja objektiviziran pregled IT-nevarnosti v letu 2018 (podatki so v odstotkih):

varnost IoT	43,2
GDPR	35,3
varnost v oblaku	25,4
kriptovalute in veriženje blokov	22,8
izsiljevalski virusi	22,7
usmerjeni kibernetski napadi	22,1
AI/ML in nastajoče kibervarnostne tehnologije	21,9
kibernetske aktivnosti na ravni držav	21,2
upravljanje pristnosti in identitet	20,3
teme CxO in poslovne kulture	18,7
varnostna avtomatizacija in orkestracija	16,1
digitalna varnost (kanali, zahteve, pravice)	16,0
socialni inženiring	16,0
aktivnosti hekerjev, politikov, ekstremistov, teroristov	14,6
zlonamerna raba AI/ML	14,2
operativne tehnološke in kritične infrastrukture	13,1
napadi prek družabnih medijev in lažne novice	12,0
notranje grožnje ter varnost končnih uporabnikov in končnih točk	11,2
mobilna in komunikacijska varnost	10,8
DevOps in DevSecOps	10,0
šifriranje	9,6
brezdatotečni napadi in APT	9,4

(Opomba: GDPR – Splošna uredba o varstvu osebnih podatkov, AI – umetna inteligenca, ML – strojno učenje, APT – napredne trajne grožnje)

» *Proti stopnjevanju napadov: vse več podjetij bo zmanjševalo tveganje z uvajanjem preizkušanih virov, kakovostne opreme in kvalificiranih strokovnjakov.*

Trendi, ki poganjajo porabo

Poraba za strojno in programsko opremo ter storitve, povezane z varnostjo, se bo v letu 2021 povečala na 119,9 milijarde dolarjev, napoveduje IDC. Zaradi dejstva, da bo skoraj vsaka industrija investirala v varnostne rešitve in tako odgovorila na širok spekter groženj, bo potrošnja v obdobju 2016–2021 rasla v povprečju 9,6 odstotka na leto (CAGR). Svetovna potrošnja za varnostne produkte in storitve se je lani povečala za 10,3 odstotka v primerjavi z letom 2016, na 83,5 milijarde dolarjev. »Trije splošni trendi poganjajo porabo za varnost: dinamična krajina groženj, rastoči regulatorni pritiski in arhitekturne spremembe, ki jih spodbujajo digitalne spremembe,« razlaga podpredsednik programa IDC za varnostne produkte Sine Pike. IDC ocenjuje, da so se varnostni stroški lani približno enakomerno razporedili na štiri industrijske sektorje: distribucijo in storitve (19,7 milijarde dolarjev), javni sektor (18,6 milijarde), proizvodnjo in vire (16,4 milijarde) ter finance (16,3 milijarde dolarjev). V letu 2021 se bo javni sektor s povprečno rastjo 10,3 odstotka skoraj izenačil s sektorjem distribucije, sektor financ pa bo s povprečno rastjo 10,2 odstotka prekosil sektor proizvodnje.

Na svetovni ravni so lani za varnostne produkte in storitve največ porabile banke, diskretna proizvodnja in državne

» *»Imamo vaše podatke – plačajte!«: ilustracija na temo izsiljevalskih virusov*

SEGMENT	2016	2017	2018
Upravljanje dostopnih identitet (AIM)	3,91	4,28	4,69
Zaščita infrastruktur	15,15	16,22	17,47
Oprema za omrežno varnost	9,80	10,93	11,67
Varnostne tsoritve	48,80	53,06	57,72
Progr. oprema za varnost uporabnikov	4,57	4,64	4,75
Skupaj	82,23	89,13	96,30

» *Potrošnja za varnost v svetu po segmentih 2016–2018 (v milijardah dolarjev). Vir: Gartner, 12/2017. Največja rast in delež: po potrošnji za varnost vodita segmenta zaščite infrastruktur in varnostnih storitev*

agencije, skupaj okrog 30 odstotkov skupne svetovne potrošnje. Banke in državne agencije bodo s povprečno rastjo 10,9 oz. 10,7 odstotka med panogami z največjo povprečno rastjo v petletnem obdobju. Največjo povprečno rast pa bo doživela industrija telekomunikacij, 12,6 odstotka, ki bo tako leta 2021 postala četrta največja industrija, ki bo tudi prekosila panoge procesne proizvodnje in profesionalnih storitev. V letu 2017 je bilo 80 odstotkov stroškov za varnost porabljeno za storitve in programsko opremo. Med storitvami sta bili vodilni kategoriji upravljanih varnostnih storitev (15,25 milijarde dolarjev) in integriranih storitev (12,5 milijarde). Potrošnja za programsko opremo je bila osredotočena na tri kategorije – varnost končne točke (podjetniškega omrežja, na katerega se brezžično povezujejo prenosniki, tablice in mobilni telefoni), upravljanje dostopnih identitet (AIM) ter upravljanje varnosti in ranljivosti (SVM). Na te kategorije je odpadlo 75 odstotkov skupne porabe za programsko opremo. Za strojno opremo je bila porabljena manj kot četrtina sredstev, največ pa za rešitve za omrežno varnost (13,7 milijarde dolarjev).

V ospredju naj bodo ljudje

Analitsko podjetje Information Management napoveduje, da bodo globalni stroški za informacijsko varnost v prihodnjih petih letih skupaj presegli bilijon dolarjev, medtem ko bo škoda zaradi kibernetskih napadov, vdorov, vpadov in vlomov ter izgub in kraj podatkov v letu 2021 presegla neverjetnih šest bilijonov dolarjev. Tako notranji kot tudi zunanji nepridipravi bodo vedno iskali načine, da poškodujejo, popačijo ter ponaredijo podjetniške sisteme in podatke. Organizacije morajo zato nenehno izboljševati obstoječe mere, postopke in sisteme zaščite ter uvajati nove, ki se osredotočajo na ljudi, procese in tehnologije. Analitsko podjetje predstavlja šest glavnih trendov na področju kibernetske varnosti, ki letos postajajo vsakdanji: pomanjkanje strokovnjakov, zunanje izvajanje, angažiranje žensk, avtomatizacijo in orkestracijo, socialni inženiring ter osredotočanje na ljudi. Pomanjkanje strokovnjakov: V svetu že danes doživljamo množično pomanjkanje kadrov za kibernetsko varnost. Leta 2017 je po svetu ostalo nezasedenih stotine tisoč varnostnih delovnih mest, samo v ZDA 350.000, letos pa se bo stanje še poslabšalo.

Širjenje zunanjega izvajanja: Zaradi pomanjkanja kadrov organizacije težko učinkovito rešujejo nastanke kibernetsko-varnostne škode, zato se bodo obračale na zunanje ponudnike upravljanja storitev. Ženske v kibervarnosti: Po najnovejših podatkih je ženske delovne sile v informacijski varnosti samo 11 odstotkov. Pomanjkanje varnostnih strokovnjakov prinaša veliko priložnosti za ženske, ki jim pomagajo organizacije, kot je Women's Society of Cyberjutsu (WSC). Avtomatizacija in orkestracija: Tudi organizacije, ki imajo ustrezne varnostne kadre, težko uspešno zmanjšajo povprečen čas odkrivanja vdora in saniranja škode, zaradi trajanja komunikacij in preprostih opravil. Vse več organizacij

» *V ospredju pozornosti: strokovnjaki za varnost so kot največjo skrb v letu 2018 izpostavili internet stvari.*

bo začelo uporabljati varnostno avtomatizacijo in orodja orkestracije, s čimer bi pospešili notranje procese in razširili linije komunikacij. Socialni inženiring: Za velik del varnostnih vpadov so krivi ljudje, zato je tudi logično, da je treba problem pomanjkanja kadrov reševati z izobraževanjem in treniranjem zaposlenih. Osredotočanje na ljudi: Lani je internet uporabljalo okrog 3,8 milijarde ljudi, v letu 2020 pa jih bo že 6 milijard. Podjetja bodo morala izbirati procese, v katerih bo lažje odkrivati grožnje, pospeševati poizvedovanje, preprečevati odtekanje podatkov in zagotavljati učinkovit odziv.