Večina podjetij bi pri inf varnosti prejela oceno n

S strokovnjaki za kibernetsko varnost smo govorili o sposobnostih po grožnjami, zakrpajo ranljivosti in kljubujejo dogodkom, ki tako rekoč

Minulo leto je nagnalo strah v kosti tudi izkušenim varnostnim inženirjem po vsem svetu. Najprej je maja napad z izsiljevalskim virusom WannaCry ohromil milijone podjetij po svetu in v jok spravil še precej več posameznikov, konec leta pa so razkrite ranljivosti v procesorjih podjetja Intel, ki z njimi zalaga več kot 90 odstotkov trga osebnih in prenosnih računalnikov, šokirale tako strokovno kot laično javnost. Ker jih v celoti vsaj pri starejših modelih ni mogoče programsko zakrpati, lahko širokopotezne napade, ki bi izkoriščali omenjene ranljivosti, šele pričakujemo – najbrž že letos.

THINKSTOCK

Slovenska in tudi vsa druga podjetja so sicer letos varnosti namenila precej več poudarka kot prejšnja leta, za kar je zaslužna predvsem nova evropska splošna uredba na področju varovanja osebnih podatkov – GDPR, ki poskuša varnostno higieno dvigniti na višjo raven.

»V Sloveniji sicer nismo imeli napadov, ki bi odmevali v javnosti, a sezono 2017/2018 vseeno ocenjujem kot prelomno. Podjetja so se začela precej bolj zavedati pomena varnosti informacijskih sistemov. Na to kaže povečano zanimanje za izvajanje različnih varnostnih pregledov IT-okolij, sistemov in aplikacij,« pravi Vladimir Ban, strokovnjak za kibernetsko varnost v podjetju Smart Com.

Ni dovolj poznati temeljna načela varnosti, treba jih je tudi upoštevati

Najlažje se je braniti pred napadalcem, ki ga podjetja vidijo oziroma poznajo. Osnovna načela in dobre prakse zagotavljanja varnosti pozna vsak skrbnik informacijskega sistema, a če jih ne upošteva, je informacijska varnost v podjetju na precej nižji ravni. Napadalec namreč za zlorabo ne potrebuje visokotehnoloških znanj in orodij, ampak največkrat zadošča že pravi motiv.

Zadevo lahko primerjamo z varovanjem stanovanja. Že od mladih nog nas učijo, da stanovanja ne puščamo odklenjenega in ključa ne spravljamo pod predpražnik. Zgolj upanje, da nismo zanimivi za napadalce oziroma da bo napadalec raje izbral soseda, ni dovolj, je precej neodgovorno početje. Tudi izgovarjanje na teoretično možnost, da lahko ključ izgubimo in nam bo rezervni pod predpražnikom omogočil vstop v stanovanje, ni dovolj dober za takšno početje.

Digitalna vhodna vrata je treba zaklepati

»Čeprav bi si v domačih podjetjih želeli visoko ozaveščenost o informacijski varnosti, praksa kaže nasprotno. Marsikatero podjetje še vedno ne zaklepa digitalnih vhodnih vrat oziroma pušča ključ pod predpražnikom. Razlogov za takšno početje je več, včasih je to neznanje, včasih nezavedanje, včasih pa podjetje preprosto 'nima časa' urediti zadev,« ugotavlja Ban.

Vladimir Ban, Smart Com:
Upam si trditi, da so podjetja, ki so opravila varnostni pregled, precej varnejša v primerjavi s podjetji, ki tega še niso storila.

Boštjan Špehonja, Unistar PRO:
Najpogostejša ranljivost, ki jo odkrivamo med varnostnimi pregledi, je raba privzetih uporabniških imen in gesel.

Uroš Majcen, S & T Slovenija:
Po naših izkušnjah niti ena aplikacija, ki smo jo pregledali, ni bila brez varnostnih lukenj.

Kakšne napake delajo podjetja? Predvsem so IT-viri v lokalnem omrežju zaposlenim dostopni brez kakršnihkoli omejitev, torej tudi brez mehanizmov večnivojske avtentikacije uporabnikov. Ker želi vse več podjetij zaposlenim omogočiti tudi delo in dostop na daljavo, so številna prijavna okna v sisteme dostopna prek interneta. Uporabnik tako kot napadalec potrebuje zgolj uporabniško geslo za prijavo, če je to za nameček še privzeto od namestitve sistema, je napad na podjetje otročje lahek.

Tovarniško nastavljena gesla je treba takoj spremeniti

»Najpogostejša ranljivost, ki jo odkrivamo med varnostnimi pregledi, je raba privzetih uporabniških imen in gesel. Zelo pogosta težava so tudi šibka gesla. Velikokrat se zgodi, da pri varnostnem pregledu pridobimo skrbniški dostop do naprave s privzetimi nastavitvami, na primer uporabniškim imenom in geslom 'admin'. Gre za tovarniško nastavitev, ki ob namestitvi naprave ni bila spremenjena in pomeni kritično varnostno tveganje. Pri takšni ranljivosti napadalec ne potrebuje tehničnega znanja, le nekaj iznajdljivosti. Pridobi pa lahko popoln nadzor nad napravo ali sistemom,« razlaga Boštjan Špehonja, višji svetovalec na področju informacijske varnosti v podjetju Unistar PRO in certificirani etični heker.

Redno posodabljanje kritičnih sistemov mora priti v kri

Čeprav se proizvajalci strojne in programske opreme trudijo čim prej zakrpati odkrite ranljivosti in o njih obvestiti javnost, v marsikaterem podjetju redno posodabljanje za poslovanje kritičnih sistemov informatikom še ni prišlo v kri. »Odkrivamo tako zastarele operacijske sisteme kot tudi vse storitve, ki tečejo na njih,« razlaga Špehonja. Pojasnjuje, da je za organizacijo zelo veliko tveganje, če se v internetu pojavi naprava, ki nima nameščenih varnostnih popravkov. Zato je redno nameščanje varnostnih popravkov in drugih posodobitev več kot priporočljivo. Pri nekaterih IKT-sistemih je to zaradi narave delovanja aplikacij teže izvedljivo, a je v takšnih primerih strežnike in aplikacije treba varovati z drugimi varnostnimi mehanizmi. »Čeprav je bilo o tem že veliko napisanega, je to še vedno huda težava skoraj vsake organizacije. Zadnje leto smo denimo prejeli veliko klicev organizacij, ki so bile okužene z izsiljevalskim virusom,« pravi Špehonja.

Prehod v oblak lahko poveča tveganje

Še precej trši oreh za podjetja so ranljivosti, ki so tudi informatikom bistveno bolj prikrite. Gre za kompleksnejše ranljivosti, pri katerih napadalec potrebuje več dela in znanja, da jih najprej sploh identificira in zatem še izrabi. Večina tovrstnih ranljivosti ni povezana z omrežjem oziroma sistemi,

Marjana Senčar Srdič, višja produktna vodja za področje digitalne preobrazbe in inovacij v družbi A1 Slovenija:
Uspeh uvedbe katerekoli rešitve MDM je odvisen od končnih uporabnikov. Tudi najboljša rešitev, ki ne ponuja nobene vrednosti zaposlenim, je obsojena na propad še pred začetkom projekta.

Četrtek, 12. julija 2018, št. 131 **www.finance.si**

...formacijski ...nezadostno

...odjetij, da se ubranijo pred različnimi ...ž vsako leto pretresejo svet IT

Kaj podjetja počnejo narobe?

1 Največja težava podjetij in organizacij so ranljivosti, ki se jih v teh niti ne zavedajo. Statistika ponudnikov varnostnih rešitev kaže, da so v podjetjih, ki so bila napadena, napadalci v omrežju in sistemih v povprečju »brezskrbno« prebili več kot tri mesece, preden so jih zaznali oziroma odkrili. Velika težava sodobnih podjetij je po ocenah varnostnih strokovnjakov že dejstvo, da nimajo vpeljanih procesov in rešitev za spremljanje varnostnih dogodkov – nihče pač ni pristojen za to. »Zavedati se moramo, da je skoraj nemogoče vnaprej odpraviti vse varnostne ranljivosti, vendar enako velja, da je za napadalca skoraj nemogoče, da napad izvede, ne da bi se izpostavil – včasih ga izda že kaka banalna zadeva. Za zaznavo takšnih dogodkov tehnično ne potrebujemo kompleksnih sistemov, a jih podjetja kljub temu ne zaznajo pravočasno, ker nimajo postavljenih pravil o tem, kdo kaj spremlja,« pojasnjuje Vladimir Ban iz podjetja Smart Com.

2 Dodatna težava podjetij je tudi manko zavedanja zaposlenih o informacijski varnosti. Številna nimajo opredeljenih postopkov odzivanja na zaznane »sumljive« dogodke. Napadalci se s prevarami več uporabnikov – tudi tako preprostimi, kot je pošiljanje e-pošte s povezavo na s škodljivo kodo okuženo ali prevarantsko spletno stran – dokopljejo do več uporabniških imen in gesel, preden kateri od zaposlenih le prijavi sumljive aktivnosti IT-oddelku. Njegov odziv sicer prepreči nadaljnje napade, nihče pa ne popravi »škode za nazaj« in ne zamenja prvotno pridobljenih gesel, kar je po Banovih besedah šokantno.

3 Marsikatero podjetje v želji po dvigu ravni informacijske varnosti najame zunanje specializirane izvajalce, kar je hvalevredno. A se kot varnostna pomanjkljivost pogosto pokaže slabo opredeljena odgovornost glede zagotavljanja varnosti med podjetjem in zunanjimi izvajalci. »Tipičen primer so varnostni sistemi. Postavi jih zunanji izvajalec, ki sistem morebiti tudi še naprej vzdržuje. Podjetje si pogosto predstavlja, da 'vzdrževanje' vključuje tudi proaktivno spremljanje in razmišljanje o varnosti, kar pa ni nujno res. In potem ob neželenem varnostnem dogodku kažejo s prstom drug na drugega,« dodatno težavo opisuje Ban.

ampak z aplikacijami. Ker tudi v Sloveniji zaznavamo očitno težnjo prehajanja aplikacij na spletne tehnologije, lahko govorimo o pogostih ranljivostih spletnih oziroma oblačnih aplikacij.

V Smart Comu so kot najpogostejše opredelili ranljivosti križno izvajanje skriptov (cross-site-scripting), injiciranje kode SQL in različne slabe nastavitve (piškotki, protokol SSL ...). »Te ranljivosti smo pogosto identificirali tudi na klasičnih spletnih straneh, kar pomeni, da obstajajo v tako rekoč vseh okoljih, in ne zgolj v posebnih okoljih s posebnimi aplikacijami, kot si to skrbniki mnogokrat predstavljajo. Omenjene ranljivosti so v marsikaterem okolju lahko zelo hude,« pojasnjuje Ban.

Pri razvoju lastnih aplikacij varnost pogosto ni na prvem mestu

»Zavedanje o pomembnosti informacijske varnosti se sicer povečuje, vendar je to spremembo v razmišljanju opaziti bolj pri načrtovanju in implementaciji infrastrukture kot pri razvoju aplikacij. Razlog je verjetno v tem, da večino infrastrukture testirajo in verificirajo proizvajalci in neodvisne hiše, medtem ko gre pri aplikacijah najpogosteje za lasten razvoj, pri katerem varnost ni na prvem mestu,« izkušnje iz prakse povzema Uroš Majcen, svetovalec za informacijsko varnost v družbi S & T Slovenija. Po njihovih opažanjih so precej varnejše tiste aplikacije, pri katerih je bil varnostni pregled izvorne kode vključen že v proces razvoja aplikacije. »Poleg tega vključevanje varnostnih pregledov v razvoj aplikacij pozitivno vpliva tudi na to, da se razvijalci naučijo pisati bolj varno kodo, kar je pravzaprav za podjetja, katerih glavna dejavnost je razvoj aplikacij, dolgoročna naložba.«

Varnostni pregled naj bo prvi korak

Kako varno je posamezno informacijsko okolje, lahko podjetjem pokaže šele iskrena analiza – temeljit varnostni pregled. Varnostni pregledi niso usmerjeni zgolj v identifikacijo posameznih tehničnih ranljivosti, temveč lahko obsegajo tudi delo z zaposlenimi, saj so pogosto prav ti tarča prevar in napadov z metodo socialnega inženiringa, ko napadalci od njih pridobijo podatke in informacije, ki jih potrebujejo za uspešno izvedbo napada. Varnostni pregled je torej prelomnica, ko podjetja spoznajo, kje so varnostno šibka, in ranljiva področja lahko uredijo. »Upam si trditi, da so podjetja, ki so izvedla varnostni pregled, precej varnejša v primerjavi s tistimi, ki tega še niso storila,« je prepričan Ban.

Posebno poglavje so brezžična omrežja podjetij

V podjetju Unistar PRO vsak varnostni pregled opravijo vsaj v dveh fazah. Najprej se lotijo iskanja osnovnih varnostnih napak v IKT-sistemih. V tej fazi najpogosteje odkrijejo privzeta ali šibka uporabniška imena in gesla, ki napadalcem omogočajo nadzor nad napravo brez naprednejših hekerskih tehnik. Velikokrat odkrijejo sisteme, ki nimajo nameščenih varnostnih popravkov.

Poglavje zase so tudi brezžična omrežja podjetij, saj številna ne sledijo priporočilom, naj bodo povsem ločena od notranjega omrežja podjetja. »Ko govorimo o notranjem omrežju organizacije, nam delo velikokrat olajša to, da organizacije nimajo mehanizma, ki bi neznanim elektronskim napravam onemogočal priklop v lokalno omrežje prek kabla. V takem primeru potrebujemo največ dva dni, da sami pridobimo veljavne domenske uporabniške račune in prevzamemo nadzor nad ključnimi sistemi v organizaciji,« pravi Špehonja.

Sledi naprednejši varnostni pregled oziroma penetracijski test. V tej fazi varnostni strokovnjaki uporabljajo kompleksnejše hekerske metode, s katerimi »vdirajo« v sisteme, spletne strani in aplikacije – pogosto prelahko. »Največkrat gre za možnost dostopa v dele sistema ali aplikacije, za katere naj ne bi imeli pravic, možno je onemogočiti aplikacijo ali izkoristiti napačno logiko delovanja aplikacije. Najhujši scenarij je ranljiva spletna aplikacija, prek katere prevzamemo nadzor nad strežnikom in dostopamo do notranjega omrežja in informacij podjetja,« pojasnjuje sogovornik.

Skoraj ni aplikacije brez pomanjkljivosti

Vsi domači ponudniki varnostnih storitev so v zadnjih letih zaznali povečano povpraševanje po varnostnih pregledih, kar pomeni, da se tudi slovenska podjetja bolj zavedajo potencialnih ranljivosti oziroma ogroženosti. Je pa delež podjetij, ki dejansko in redno naročajo varnostne preglede, še vedno razmeroma majhen.

»Opažamo, da se naročniki varnostnih pregledov prepogosto odločajo za cenovno ugodnejše varnostne preglede, kar pomeni tudi nižjo kakovost pregleda. Po naših izkušnjah niti ena aplikacija, ki smo jo pregledali, ni bila brez varnostnih lukenj, zato razvijalcem aplikacij svetujemo, naj se pri izbiri ponudnika raje kot na ceno pregleda osredotočijo na njegovo kakovost in izkušnje,« dodaja Majcen. Ugotovitev je potrdil tudi Špehonja: »Z ekipo sodelavcev še nismo naleteli na aplikacijo, ki so jo razvila domača podjetja in pri kateri ne bi odkrili varnostnih pomanjkljivosti.«

IKT-informator je oglasna priloga časnika Finance. Izhaja enkrat na mesec.

Urednik priloge:
Branko Žnidaršič
Tel.: (01) 30 91 526
E-pošta: branko.znidarsic@finance.si

Stalna zunanja sodelavca:
Esad Jakupović
Tel.: 040 296 184
E-pošta: esad.jakupovic@finance.si

Miran Varga
Tel.: 040 427 333
E-pošta: miran.varga@finance.si

Trženje:
Mateja Habjan Pejić
Tel.: (01) 30 91 534
E-pošta: mateja.pejic@finance.si

Prelom: Finance

Lektoriranje: Finance

Urednik oglasnega uredništva:
Branko Žnidaršič

Naslednji IKT-informator bo izšel 29. avgusta 2018.

Informacijska varnost sloni na ljudeh in znanju

UVODNIK
Miran Varga

miran.varga@finance.si

Številna podjetja skozi bolečo prakso odkrivajo, da jim v primeru IT-varnosti največje težave povzročajo najpreprostejše stvari. Omrežje podjetja je varno le toliko, kolikor je varen njegov najšibkejši člen. Večina hekerjev se vendarle ne ukvarja z naprednimi grožnjami in napadi, ki bi izkoriščali tako imenovane ranljivosti ničtega dne – tipični hekerji ne kompliciraju niti ne izgubljajo časa in denarja z naprednimi napadi, temveč le iščejo najlažjo točko za vstop v omrežja in sisteme.

Najpogostejša tarča in hkrati ranljivost so zaposleni. Lansko poročilo Data Breach Investigations Report ameriškega telekomunikacijskega velikana Verizon je kar 81 odstotkov vdorov pripisalo napakam ljudi – najpogosteje je šlo za ukradena ali šibka gesla. Ljudje smo tisti, ki se motimo, smo (pretirano) čustveni, zato tudi redna izobraževanja in usposabljanja glede informacijske varnosti niso vsemogočna.

V dobi povsod navzoče povezljivosti in informacij napadalci vse lažje najdejo poslovne, osebne in politične informacije, ki jih izrabijo za pripravo sporočil, na katera se bomo ljudje odzvali – najverjetneje s klikom na okuženo povezavo. In že so notri – v omrežju, sistemu, aplikaciji, podatkovni bazi. V času vse bolj spretno pripravljenih pasti in prevar mora tudi izobraževanje glede informacijske varnosti narediti korak naprej – če želimo dobiti to bitko, moramo sodelovati vsi.

Ljudje smo tisti, ki odločamo o tem, ali bomo najšibkejši ali pa najmočnejši del varnostne verige.

Za zdaj se zdi, da bitke dobivajo predvsem napadalci. Na strani obrambe namreč primanjkuje borcev. ISACA, neprofitna organizacija s področja informacijske varnosti, je objavila oceno, da bo že prihodnje leto po svetu primanjkovalo dva milijona strokovnjakov s področja kibernetske varnosti. Torej za vso Slovenijo varnostnih strokovnjakov! Pomanjkanje usposobljenih varnostnih analitikov bo še stopnjevalo težave, s katerimi se bodo spopadala podjetja in posamezniki. Oddelek informatike, ki je v marsikaterem podjetju danes odgovoren za varovanje njegove digitalne krajine, je preobremenjen, ne le z drugim delom, temveč tudi številom in obsegom varnostnih groženj in incidentov. Zaposleni v varnostnih ekipah dobesedno izgorevajo, podjetja pa so vse bolj ranljiva.

Kaj nam je storiti? Če želijo podjetja ostati korak pred napadalci, ki se hočejo prebiti v njihova omrežja, sisteme in naprave, morajo razumeti razmišljanje in delovanje hekerjev. To se seveda, podobno kot varnostne grožnje, skozi čas spreminja, zato je nujno osvajanje novih znanj – varnostni strokovnjaki se morajo stalno izobraževati, če naj ustrezno zaščitijo podjetje ali organizacijo.

Varnostne ekipe za učinkovito delo potrebujejo orodja, s katerimi bodo uspešno odkrivale in preiskovale varnostne incidente ter se nanje hitro in učinkovito odzivale. Ker večina podjetij zaradi očitnih izzivov, povezanih s kadri in denarjem, lastnih vrhunskih varnostnih ekip nikoli ne bo imela, se zdi najem storitev varnostno-operativnih centrov še najboljša rešitev – poleg stalnega izobraževanja in ozaveščanja vseh zaposlenih, se razume.

www.finance.si
Četrtek, 12. julija 2018, št. 131

KOLEDAR IKT-DOGODKOV

OD 12. JULIJA DO 30. SEPTEMBRA

Navedeni so naziv in opis, organizator, mesto, datum in kraj dogodka ter spletna stran za dodatne informacije.

EdIT 2018 (Education for Inovative Thinkers), poletna šola v okviru mednarodno-izobraževalnega programa v treh državah (Sloveniji, Srbiji ter Bosni in Hercegovini), Comtrade, **Ljubljana, 16.–27. julija** (Z zabavo do zmage: Zgradi platformo za interakcijo s potniki), **Maribor, 16.–27. julija** (Podatkovna zgodba: Gradnja igralniških vizualizacij) (www.comtrade.com/si)
Microsoft Power BI, poročila na dlani, tehnični dogodek oziroma predstavitev orodja Microsoft Power BI, SRC, **Ljubljana, 17. julija**, MatrixRoom podjetja SRC (www.src.si)
Poletni tabor računalništva 2018, ZOTKS in Šola prihodnosti Maribor, **Gorenje pri Zrečah, 11. avgusta**, CŠOD Gorenje (www.zotk.si)
Gamescom 2018, največji svetovni sejem interaktivnih iger, Kölnmesse, **Köln, 21.–28. avgusta**, Kölnmesse (gamescom.de)
VMworld 2018, letna konferenca strokovnjakov za virtualizacijo in oblak, VMware, **Las Vegas, 26.–30. avgusta**, Mandalay Bay Convention Center (www.vmworld.com)
IFA 2018, mednarodni sejem potrošniške elektronike in hišnih aparatov, Messe Berlin in gfu, **Berlin, od 31. avgusta do 5. septembra**, Messe Berlin (www.ifa-berlin.com)
CIO leta 2018, slovesna razglasitev 12. dobitnika priznanja, CIO odbor in Housing Co., **Brdo pri Kranju, 7. septembra**, Kongresni center Brdo (www.cio.si)
Gartner Security & Risk Management Summit 2018, konferenca o najnovejših grožnjah in pripravi na prihajajoče tehnologije, kot so AI, strojno učenje, veriženje blokov in napredna analitika, Gartner, **London, 10. in 11. septembra**, InterContinental London The O2 Hotel (www.gartner.com)
Digitalizacija: Spremembe v poslovnem in tehnološkem okolju, osnovni pojmi, tehnologije in trendi v digitalni transformaciji (uvodna delavnica), ICT Academy, **Ljubljana, 10. in 11. septembra**, Fakulteta za elektrotehniko (www.ict-academy.eu)
ITU Telecom World '18, svetovni kongres in sejem telekomunikacij, ITU, **Durban, 10.–13. septembra**, Durban International Convention Centre (https://telecomworld.itu.int)
HTML5, osnovna znanja o HTML5 in njegovi uporabi pri zasnovi sodobnih spletnih aplikacij, ICT Academy, **Ljubljana, 11. septembra**, Fakulteta za elektrotehniko (www.ict-academy.eu)
DMEXCO 2018, mednarodni sejem digitalne ekonomije in marketinga, Kölnmesse in Bundesverband Digitale Wirtschaft (BVDW), **Köln, 12. in 13. septembra**, Kölnmesse (dmexco.de)
Shranjevanje podatkov in podatkovne baze: plačljive in brezplačne podatkovne baze in orodja za delo z njimi, možnosti shranjevanja podatkov in uporabe podatkovnih baz, ICT Academy, **Ljubljana, 12. in 13. septembra**, Fakulteta za elektrotehniko (www.ict-academy.eu)
Mobile World Congress Americas 2018, sejem mobilnih rešitev v informacijskih tehnologijah in uporabniški elektroniki, CTIA in GSMA, **Los Angeles, 12.–14. septembra**, Los Angeles Convention Center (LACC) (www.supermobilityweek.com)
IT-vizija 2018, strokovna konferenca o aktualnih trendih na področjih tehnologije in poslovanja, NIL, **Ljubljana, 13. septembra**, Ljubljanski grad (www.nil.com/sl/dogodki/it-vizija-2018)
IBC 2018, konferenca in razstava o ustvarjanju, upravljanju in distribuciji vsebin v zabavni industriji, IBC London, **Amsterdam, 13.–18. septembra**, RAI Amsterdam (http://ibc2018.online)
Uskladitev med marketingom in prodajo, tematski zajtrk, FrodX, **Ljubljana, 14. septembra**, prostori podjetja FrodX (frodx.com/seminarji/frodx-akademija)
Varnost v omrežjih IP: postopki in mehanizmi kriptiranja podatkov ter uveljavitev varnosti komunikacijskih storitev, naprav in sistemov, **Ljubljana, 18. in 19. septembra**, Fakulteta za elektrotehniko (www.ict-academy.eu/sl-SI/upcoming-events)
Razvoj decentraliziranih aplikacij za Ethereum: glavni vidiki delovanja, arhitekture, aplikacije za Ethereum v končnih napravah in uporabniških vmesnikih, ICT Academy, **Ljubljana, 20. in 21. septembra**, Fakulteta za elektrotehniko (www.ict-academy.eu/sl-SI/upcoming-events)
SAP TechED 2018, tehnološka konferenca podjetja SAP, partnerjev in strank, SAP, **Barcelona, 23.–25. septembra**, Fira de Barcelona – Gran Via (events.sap.com)
Nove blockchain in finančne tehnologije, konferenca na temo veriženja blokov, tehnologij fintech in insuretech, kriptovalut ter novodobnega bančništva, Palsit, **Brdo pri Kranju, 25. septembra** (www.palsit.com)

Poslovne mobilne naprave so vse bolj zaščitene, a še ne dovolj

Skoraj ni več podjetja, ki ne bi uporabljalo mobilnega poslovanja. Prav tako skoraj ni več podjetja, ki ne bi bilo žrtev napadov zlonamernih programov na mobilne naprave. Poletna mobilnost varnostna tveganja za poslovne mobilne naprave še povečuje.

■ **Finančne posledice in pogostost varnostnih napadov na mobilne naprave so v svetu lani že presegle posledice in število napadov na računalnike.**

V nedavni anketi Oxford Economics je izmed 500 poslovnih in IT-vodij kar 80 odstotkov izjavilo, da zaposleni ne morejo učinkovito opravljati svojega dela brez pametnih telefonov. Tri četrtine anketiranih je ocenilo, da so mobilne naprave odločilne za učinkovit potek dela. »Uspešna delovna sila sodobnega podjetja je mobilna delovna sila,« poudarja raziskava. Pri tem so mobilne naprave v večini organizacij zelo različne, saj jih je le v redkih primerih kupilo samo podjetje.

Večinoma gre za kombinacijo poslovnih in osebnih naprav zaposlenih, pojasnjuje Oxford Economics. Ob tem ocenjuje, da je takšen hibridni model najboljši, saj povečuje zadovoljstvo zaposlenih z mobilnimi napravami kot poslovnim orodjem, izboljšuje medsebojno sodelovanje, uporabo poslovnih aplikacij dela bolj učinkovito in povečuje mobilno varnost. Da bi organizacije bolje izkoristile zmožnosti svoje delovne sile, morajo razviti premišljeno, načrtno in usklajeno strategijo, ki učinkovito podpira mobilne naprave in zagotavlja njihovo varnost.

Mobilne naprave že bolj ogrožene kot računalniki

Danes ni več podjetja, ki ne bi bilo žrtev napadov zlonamernih programov na mobilne naprave, pri čemer je operacijski sistem Android pogostejša tarča, kot sta iOS ali Windows Mobile, ugotavlja študija podjetja Nokia. Analitska podjetja med tem ocenjujejo, da so finančne posledice in pogostost varnostnih napadov na mobilne naprave v svetu lani že presegle posledice in število napadov na računalnike. Raziskava varnostnega podjetja Check Point Software je pokazala povprečno 54 napadov »mobilne« zlonamerne programske opreme na podjetje oziroma ustanovo.

Kar 89 odstotkov napadov je bilo izvedenih prek radijskih omrežij, v katera uporabniki nepremišljeno vstopajo. »Vse kaže, da so mobilne naprave pravzaprav postale nova stranska vrata za kibernetske kriminalce,« meni Michael Shaulov, vodja za mobilno varnost pri Check Pointu.

Varnostna tveganja razumemo, upoštevamo pa ne

Poslovni in IT-vodje danes dobro razumejo velikanska varnostna tveganja, s katerimi se spopadajo podjetja in ustanove, ocenjuje varnostno podjetje Code4. »Kljub temu 75 odstotkov direktorjev in 52 odstotkov drugih odločevalcev še vedno uporablja aplikacije in programe, ki jih niso potrdili njihovi IT-oddelki,« dodajajo.

Večina kot razlog navaja željo po hitrem izboljšanju produktivnosti. Pri tem 91 odstotkov omenjenih direktorjev in 83 odstotkov drugih odločevalcev priznava, da uporaba nepotrjene opreme pomeni varnostno tveganje. Ni čudno, da je skoraj polovica podjetij, ki jih je anketiral Code4, v zadnjem poldrugem letu izkusila varnostne vdore.

Visoko raven zaščite omogočijo že osnovni varnostni ukrepi

»Pri zaščiti mobilnih aplikacij je večino pozornosti še vedno treba posvečati osnovnim varnostnim ukrepom, ki zagotavljajo visoko raven zaščite,« poudarja Andrej Zimšek, odgovorni poslovni arhitekt v podjetju Brihteja. Mednje sodijo nameščanje popravkov operacijskega sistema na mobilnih napravah, zaklepanje telefona (čeprav je lahko to včasih nadležno), nastavitev dostopa do zaupnih službenih vsebin prek varnih povezav ter upoštevanje navodil administratorjev v podjetju in tudi navodil varnostne politike podjetja.

Zimšek razlaga, da med osnovne varnostne ukrepe sodi tudi nastavitev podatkov o lastniku telefona – ko telefon najde pošteni najditelj in ga želi vrniti lastniku (Zimšek omenja dobro lastno izkušnjo na letališču) – ter šifriranje zaupnih vsebin (bodisi prek vgrajenih programov in možnosti telefona bodisi z uporabo posebnih aplikacij). Opozarja tudi, da je priklop mobilne naprave na USB-polnilnike na javnih mestih izredno tvegan, saj so takšni polnilniki lahko povezani še s čim drugim kot le z napajanjem. Odsvetuje tudi odgovarjanje na klice z neznanih številk (na primer iz Afrike) ali na SMS-sporočila iz neznanih virov. »Niti ne odpirajte jih, ker lahko vsebujejo kakšno povezavo na zlonamerno programsko opremo,« opozarja Zimšek.

Andrej Zimšek, odgovorni poslovni arhitekt v podjetju Brihteja:
Pri zaščiti mobilnih aplikacij je večino pozornosti še vedno treba posvečati osnovnim varnostnim ukrepom, ki zagotavljajo visoko raven zaščite.

Boj med produktivnostjo in varnostjo

■ Danes se samo polovica poslovnih podatkov hrani v podatkovnih centrih in na strežnikih, druga polovica pa je na manj varnih prenosnih in namiznih osebnih računalnikih. V raziskavi podjetja Code4 je večina organizacij potrdila, da ima nameščen sistem za izdelavo varnostnih kopij za prenosne in namizne računalnike kot glavno zaščito pred napadi, samo 13 odstotkov direktorjev in osem odstotkov IT-odločevalcev pa je potrdilo, da sistem tudi preverjajo.
■ V anketi 63 odstotkov direktorjev ocenjuje, da lahko izguba podjetniških podatkov uniči njihovo poslovanje. Približno 50 odstotkov IT-odločevalcev pa meni, da je njihova sposobnost zaščite poslovnih podatkov in strank vitalna za blagovno znamko in ugled podjetja. Kljub temu zavedanju 75 odstotkov direktorjev in 52 odstotkov drugih odločevalcev zaradi hitrejšega izboljšanja produktivnosti tvega z nepotrjenimi aplikacijami in programi. »Sodobna podjetja vodijo notranji boji med potrebo po produktivnosti in potrebo po varnosti,« komentira Rick Orloff, vodja raziskave v podjetju Code4.

Kaspersky Lab ugotavlja: Polovica ljudi pametnih telefonov ne zaščiti z geslom

■ 52 odstotkov ljudi svojih osebnih pametnih telefonov ne zaščiti z geslom.
■ 22 odstotkov jih uporablja varnostno rešitev za zaščito naprav proti kraji.
■ 68 odstotkov jih svoj pametni telefon redno uporablja za dostop do interneta.
■ 14 odstotkov jih šifrira datoteke in mape.
■ 41 odstotkov jih naredi varnostno kopijo svojih podatkov.

Naj mobilne naprave ne bodo najšibkejši člen varnostne verige

Informatiki imajo stvari radi pod nadzorom. Še toliko bolj, če gre za vprašanje informacijske varnosti. Varovati namreč pomeni obvladovati. Zadnja leta informatikom izziv pomeni predvsem varovanje mobilnih naprav v poslovnih okoljih in zunaj njih.

Pametni telefoni, tablice in prenosni računalniki so sestavni del tako poslovnih okolij kot gospodinjstev. Medtem ko so njihovo rabo nekdaj narekovala podjetja – šlo je za »službene« računalnike in telefone –, je danes ravno nasprotno. Zaposleni so tisti, ki v poslovna okolja prinašajo pogosto najnovejše pa tudi precej eksotične naprave.

Sodobne mobilne naprave so postale vsakodnevno orodje za izmenjavo najrazličnejših informacij (e-pošta, raba namenskih aplikacij), tudi takšnih, ki si zaslužijo oznako interno ali celo zaupno. Hkrati so glavno komunikacijsko sredstvo zaposlenih za stik s podjetjem (sodelavci) in strankami. Naprave in njihovo komunikacijo je zato treba ustrezno (za)varovati.

Zaposleni na dopustu, nepridipravi na preži

Na dopustu, podobno kot na službeni poti, lahko na poslovne uporabnike in njihove mobilne naprave preži precej več nevarnosti kot v domačem ali poslovnem okolju. Težave si pogosto nakopljejo zaposleni kar sami, saj morebitna večja sproščenost med dopustom lahko vodi do namestitve kakšne igrice (ne glede na to, ali jo namesti starš ali otrok) ali druge prikrito škodljive aplikacije, katere delovanje lahko ogrozi napravo in podatke, ki jih ta hrani. Prek okužene aplikacije oziroma naprave pa napadalci lahko dobijo dostop tudi do omrežja in drugih virov podjetja.

Varovanje naprav in komunikacije

Oddelki IT v podjetjih v želji po zmanjševanju varnostnih tveganj, zaščiti vsebin in elektronske komunikacije uvajajo orodja za upravljanje mobilnih naprav (angl. Mobile Device Management). Te rešitve poslovne podatke varujejo tako, da na mobilni napravi ustvarijo dodatno varovano področje (nekakšen sef) in poskrbijo za šifriranje komunikacije oziroma vzpostavitev varne povezave med napravo in omrežjem podjetja.

Rešitve MDM se zelo izkažejo tudi ob kraji ali izgubi mobilne naprave, saj jo lahko uporabnik sam ali pa skrbnik informacijskega sistema v podjetju zaklene na daljavo. Prav tako lahko z nje na daljavo izbriše vse občutljive podatke. Varnostna programska oprema dodatno okrepi boj proti virusom in škodljivim kodam, ki bi na najrazličnejše načine želeli okužiti mobilno napravo (poslovnega) uporabnika.

Oddelki IT v podjetjih v želji po zmanjševanju varnostnih tveganj, zaščiti vsebin in elektronske komunikacije uvajajo orodja za upravljanje mobilnih naprav.

Informatiki poznajo še nekaj zanimivih pristopov, kako doseči večjo varnost mobilnih naprav. Nekatera poslovna okolja so uvedla omejevanje funkcionalnosti, ko naprave zapustijo varno okolje oziroma omrežje podjetja. Med funkcijami, ki jih v omenjenih primerih pogosto onemogočijo, so prepošiljanje priponk, komunikacija med zasebnim in varnim delom mobilne naprave, zajem zaslonskega posnetka in podobne.

Po rešitve k specialistom

Uvajanja varovanja mobilnih naprav se podjetja lahko lotijo precej elegantno. Večina podjetij je v preteklosti že poskrbela za optimizacijo stroškov komuniciranja, zato ima le enega ponudnika telekomunikacijskih storitev. Prav zato naj bo prvi korak preverjanje, kaj na področju upravljanja in varovanja mobilnih naprav omogoča mobilni operater.

INTERVJU: Marjana Senčar Srdič o upravljanju mobilnih naprav

Uspeh uvedbe rešitve MDM je odvisen od končnih uporabnikov

Mobilne naprave, prek katerih dostopamo do občutljivih poslovnih podatkov, je treba varovati in upravljati. Marjana Senčar Srdič, višja produktna vodja za področje digitalne preobrazbe in inovacij v družbi A1 Slovenija, nam je predstavila izkušnje z namenskimi rešitvami MDM.

Rešitve za upravljanje mobilnih naprav (MDM) sodijo med varnostne rešitve. Medtem ko imajo zadnje implementirana skoraj vsa podjetja, je prvih le za vzorec. Zakaj?

Tradicionalno so se za delo s podatki v podjetjih uporabljali predvsem delovne postaje in prenosni računalniki, mobilne naprave pa so bile namenjene le klicem in brskanju po spletu. Položaj se je v zadnjih letih izrazito spremenil, zaposleni zdaj mobilne naprave množično uporabljajo v službene namene. V podjetjih, ki še niso podprla tovrstnega načina dela, zaposleni to vse pogosteje zahtevajo. Pridobivanje informacij iz sistemov podjetja ali celo aktivno delo na mobilni napravi je pač zelo priročno. Podjetja, ki so potrebo po mobilnem delu zaznala kot prva, na primer energetski sektor, zavarovalnice in številna podjetja z zaposlenimi na terenu, so večinoma že uvedla rešitve MDM, ta trend pa se zdaj širi tudi v druge panoge.

Raba lastnih naprav v poslovne namene (BYOD) se je zelo razširila. Kako naj podjetja obvladajo vse te naprave in želje zaposlenih po mobilnem dostopu?

Gre za precejšen izziv, saj res dobrih ponudnikov rešitev MDM ni veliko. Trg mobilnih operacijskih sistemov in aplikacij se hitro spreminja, sledenje novim različicam in funkcionalnostim pa zahteva veliko razvojnih virov. Le malo ponudnikov lahko podjetjem zagotovi podporo od ničtega dne, torej od trenutka, ko ponudnik predstavi novo različico sistema ali funkcionalnost. Za uspešno uveljavitev koncepta BYOD je treba izpolniti še dodaten pogoj – ponudnik rešitve MDM mora biti sposoben ponuditi možnost hranjenja podatkov podjetja znotraj zbirnika in tako ločiti upravljanje službenega dostopa in podatkov ter zasebni del mobilne naprave. Uporaba zbirnika prav tako omogoča, da se, če zaposleni zapusti podjetje, podatki podjetja enostavno odstranijo, ne da bi bilo treba zbrisati vse podatke na napravi.

> **Treba je najti ravnovesje med vrednostjo za uporabnike, njihovim udobjem in varnostjo podatkov podjetja.**

Katera je tista točka preloma, ko podjetje poseže po rešitvi MDM?

Takšnih točk je lahko več – na primer ko mora podjetje ponuditi dostop do svojih sistemov prek mobilnih naprav, ko želi imeti naprave popisane na enem mestu ali ko želi distribuirati in upravljati aplikacije na mobilnih napravah zaposlenih. Za nekatera podjetja je potreba po MDM prišla zelo naravno z novim projektom digitalne preobrazbe, vlakovodje so dobili tablice, prav tako zavarovalniški agenti in podobno. Dodatna ključna točka preloma je varnost, ko se podjetje zave, da so informacije, ki so shranjene na mobilnih napravah, občutne vrednosti in da so izpostavljene zlorabi, če niso primerno zavarovane.

> **Le malo ponudnikov lahko podjetjem zagotovi podporo od ničtega dne.**

Kako zahtevna je implementacija rešitve MDM, kakšni so stroški uvedbe in vzdrževanja?

Implementacija rešitev MDM je odvisna od načina namestitve – lokalno ali v oblaku. Če gre za oblak, je uvedba zelo preprosta, saj večji del rešitve implementira, vzdržuje in tudi nadgrajuje ponudnik. Ta v navezi s stranko poskrbi le za integracijo z zalednimi sistemi stranke, na primer z aktivnim imenikom in e-poštnim strežnikom. Tudi sam postopek namestitve na mobilne naprave ponudniki pogosto precej poenostavijo – uporabnik ali skrbnik le klikne na povezavo in namesti rešitev.

Gre lahko pri uvedbi rešitve MDM v praksi kaj narobe?

Uspeh uvedbe katerekoli rešitve MDM je odvisen od končnih uporabnikov. Tudi najboljša rešitev, če zaposlenim ne ponuja nobene vrednosti, je obsojena na propad še pred začetkom projekta. Treba je najti ravnovesje med vrednostjo za uporabnike, njihovim udobjem in varnostjo podatkov podjetja. Gre za največji izziv vsakega projekta uvedbe MDM. Eden najbolj občutljivih delov rešitve je e-poštni odjemalec. Zaposleni bi radi dostopali do svojih sporočil enako kot pred uvedbo rešitve MDM, čeprav ta način morebiti ni varen. Ponudniki rešitev MDM se zato trudijo zagotoviti čim bolj podobno, a precej varnejšo uporabniško izkušnjo in jo celo nadgraditi, na primer z možnostjo prikaza zasebnega koledarja znotraj službenega, ter tako prepričati končne uporabnike.

Najrazličnejšim poslovnim rešitvam danes pomaga umetna pamet, kaj pa rešitvam MDM?

Ta trend v svetu rešitev MDM še ni tako pogost, se pa že pojavlja. IBM-ov Watson, ki je integriran v IBM MaaS360, lahko na primer deluje kot nekakšen umetni varnostni strokovnjak, ki so mu znana vsa potencialna varnostna tveganja po svetu in lahko to znanje aplicira na okolje podjetja. S tem je v dragoceno pomoč podjetju, saj njegovi sistemski ali varnostni skrbniki ne izgubljajo časa s proučevanjem vseh možnih varnostnih virov.

Bodo rešitve MDM v prihodnje postale sestavni del drugih celostnih varnostnih rešitev?

S tem ko mobilne naprave postajajo sestavni del omrežja podjetja, morajo rešitve MDM brez dvoma postati del širših varnostnih rešitev. Najboljše rešitve MDM so z njimi pravzaprav že integrirane, saj si tudi podjetja želijo centralno upravljati vse naprave, ki jih imajo, torej računalnike in delovne postaje, strežnike kot tudi pametne telefone in tablice, pa čeprav ti delujejo na zelo različnih strojnih in programskih platformah. Vse pogosteje se rešitve MDM v praksi integrirajo tudi z orodji za centraliziran varnostni nadzor (SIEM).

www.finance.si
Četrtek, 12. julija 2018, št. 131

Kaj vse krati spanec varnostnim strokovnjakom

Vodje oddelkov za informacijsko varnost so odgovorni za varno poslovanje podjetja, kar v luči čedalje trdovratnejšega kiberkriminala na eni in evropske uredbe GDPR na drugi strani postaja resničen izziv. Bojevati se morajo tako z zunanjimi napadalci kot morebitnimi notranjimi napakami.

Tradicionalno je za informacijsko varnost v podjetjih skrbel oddelek IT, danes pa vsaj večja podjetja in organizacije zaposlujejo specializirane strokovnjake s področja informacijske varnosti. Nekateri med njimi imajo celo vodstveno vlogo – gre za tako imenovane direktorje informacijske varnosti (Chief Information Security Officer – CISO). In prav ti zadnje čase spijo čedalje bolj nemirno. Breme odgovornosti je namreč skoraj v celoti na njihovih ramenih. Odgovorni so za varno poslovanje podjetja, kar z vidika vse trdovratnejšega in povsod navzočega kiberkriminala na eni in evropske uredbe GDPR na drugi strani postaja resničen izziv. Bojevati se morajo tako z zunanjimi napadalci kot morebitnimi notranjimi napakami. Predstavljamo tri glavne izzive, s katerimi se spopadajo.

Kako govoriti z vodstvom podjetja?

1 Čeprav kibernetska varnost v svetu postaja tema pogovorov v čedalje več upravah, je številni člani uprav in direktorji še vedno ne razumejo. Zaradi tega so vodje informacijske varnosti postavljeni pred dodaten izziv, kako zagotoviti ustrezna sredstva in druge vire za varovanje digitalnega in informacijskega premoženja podjetja. V praksi se položaj od leta 2016, ko je podjetje Cybersecurity Ventures objavilo poročilo, da več kot 90 odstotkov direktorjev podjetij ne razume varnostnih poročil, prav tolikšen delež podjetij pa ne bi bil kos večjemu kibernetskemu napadu, ni pomembneje spremenil. Je pa naloga CISO, da do lastnikov oziroma upraviteljev podjetij prenese informacijo o tem, kakšnim tveganjem je podjetje izpostavljeno in kako naj se zavaruje.

Ali res sprejemam pravilne odločitve?

2 Vodje oddelkov za informacijsko varnost stalno dvomijo o tehnologiji in zaposlenih. Pogosto se sprašujejo, ali so kupili pravo tehnologijo, jo ustrezno vpeljali, ali je vse zakrpano, bomo jutri še kos napadalcem … Vprašanje, ki načenja spanec, se glasi: »Kako res vem, da smo varni?«

Naloga CISO je torej v podjetje pripeljati varnostne strokovnjake z ustreznimi kompetencami, ki bodo pomenili intelektualno obrambo pred vse bolj premetenimi in spretnimi napadalci. Varnostnih strokovnjakov primanjkuje po vsem svetu, sploh izkušenih. Analitiki napovedujejo, da bo že leta 2021 globalno primanjkovalo kar 3,5 milijona varnostnih strokovnjakov, pri čemer je bil manko še leta 2014 ocenjen na milijon.

Bitka za talente in kompetence se bo še bolj zaostrila, varnostni strokovnjaki pa bodo za podjetja čedalje dražji, saj to področje tako rekoč ne pozna pojma brezposelnost. In prav to dodatno zvišuje raven tveganja – brez kakovostnih ljudi je težko postaviti učinkovite rešitve za zaščito in odziv na varnostne incidente. Tudi zunanji ponudniki varnostnih storitev, ki so ena elegantnejših rešitev za krpanje lukenj v znanju in delovanju, bodo kmalu razprodani.

Zagotavljanje skladnosti in zasebnosti

3 Uredba GDPR je varnostnim strokovnjakom naložila cel kup dodatnega dela. Kdor ga je opravil zgledno, danes predvsem nadzoruje informacijsko krajino, drugi pa si grizejo nohte in upajo, da se manjše razpoke ne bodo pokazale za usodne. Zagotavljanje skladnosti z različnimi zakonodajami bo tudi v prihodnje največje gonilo varnostne industrije, analitiki ocenjujejo, da že danes pomeni okoli polovico prihodkov ponudnikom varnostnih rešitev. A GDPR ni edina kratica, ki odmeva po svetu. Kdor posluje globalno, je verjetno že imel opravka z njenimi sestričnami, kot so DFARS, NYCRR 500, FISMA, GLBA, SOX in druge.

Glede na finančne in druge udarce, ki lahko podjetja doletijo zaradi nezdružljivosti, je jasno, da si CISO tovrstnih tveganj ne more privoščiti. Kaj naj torej stori? Izkušeni mački predlagajo, naj se obda z ustreznimi ljudmi in rešitvami. Poleg s hišnimi varnostnimi strokovnjaki lahko sodeluje s specializiranim ponudnikom rešitev in storitev s področja informacijske varnosti, poskrbi za ustrezen nadzor IT-okolja in upravljanje varnostnih tehnologij. Odveč ne bosta niti povezava s pravnimi svetovalci in opravljanje pregleda glede skladnosti in varnosti.

Kamorkoli brez strahu pred žeparji

Predstavljamo nahrbtnik Bobby, v katerega ni mogoče vdreti oziroma iz katerega ni mogoče ničesar ukrasti.

Sodobni človek je opremljen z vrsto digitalnih in analognih pripomočkov, brez katerih si ni mogoče prestavljati ne poslovnega ne zasebnega življenja. Pametni telefon, pametna ura, pametna zapestnica, prenosni računalnik, tablica, digitalni fotoaparat in denarnica oziroma kombinacija naštetih so del našega vsakdanjika. Izziv nastane, ko jih je treba prenašati okoli, posebej v poletnem času, ko že tradicionalno nosimo manj oblačil, predvsem takšnih z žepi. Takrat nam pridejo prav različne torbe in nahrbtniki, posebej če se odpravimo kam dlje.

A vsi nahrbtniki si niso enaki

Svojevrsten posebnež med njimi je nahrbtnik proizvajalca XD Design, ki so ga poimenovali Bobby, kar je v angleško govorečem svetu oznaka za policista. Še danes velja za nahrbtnik, ki je najbolj navdušil javnost, ko ga je prvič videla. Na spletni platformi za množično financiranje še danes drži rekord v svoji kategoriji. Podroben pogled hitro razkrije, zakaj.

Bobby ima vrsto patentiranih rešitev

Njegov največji adut je zasnova, ki je podrejena uporabnosti in predvsem varnosti. Snovalci so imeli v mislih predvsem uporabnike v urbanih središčih, kjer narašča število kraj in tatvin. V nahrbtnik Bobby namreč ni mogoče vdreti oziroma iz njega karkoli ukrasti, dokler ga nosimo na hrbtu. Materiali so odporni tako proti udarcem kot proti rezanju z nožem, odlična zadrga YKK pa je spretno skrita očem – nepridiprav, ki se uporabniku približa s hrbta ali strani, ne vidi niti ene zadrge ali žepa.

Notranjost nahrbtnika, ki je zgledno urejena s predelnimi predali, je dostopna šele, ko nahrbtnik snamemo. Da takšen pristop ne bi zmanjšal njegove uporabnosti, poskrbijo številne praktične rešitve, kot so skriti žepi za vizitke, bančne kartice ali telefon, ki so vgrajeni v izdatno nastavljive ramenske pasove. Bobby ima vgrajen tudi praktičen polnilni priklop z najbolj univerzalnim vmesnikom vseh časov – USB. Uporabnik svojo napravo polni tudi med nošenjem nahrbtnika.

Dodatna pasivna varnost in boljša ergonomija

Za varnost vsebine, ki jo prenašamo, skrbijo materiali, ki so odporni proti vodi, za dodatno pasivno varnost pa različni reflektivni dodatki, ki so vidni z vseh strani (brez mrtvega kota) – vozniki kolesarja z nahrbtnikom zato prej opazijo.

Veliko pozornosti so namenili tudi ergonomiji nošenja nahrbtnika – notranja ureditev skupaj s hrbtnim delom poskrbi, da se teža predmetov čim bolj prilega uporabnikovi hrbtenici. Obremenitev uporabnikovih ramen in hrbta je zato najnižja – v primerjavi s klasičnimi nahrbtniki je občutek ob prenašanju enako težkih predmetov v Bobbyju za petino boljši.

Nahrbtnik Bobby Bizz za poslovneže

Nad nahrbtnikom Bobby, ki se ponaša z oblikovalsko nagrado red dot, so se poleg splošne javnosti navdušili tudi poslovni uporabniki. V podjetju XD Design so jim prisluhnili in zanje pripravili posebno različico, prilagojeno navadam v poslovnem svetu. Bobby Bizz je tako popolnoma varen nahrbtnik za poslovneže, njegova posebnost pa je, da se lahko mimogrede spretno prelevi tudi v poslovni kovček.

Nahrbtnik Bobby v Sloveniji prodajajo v prodajalnah DZS, kjer je na voljo za 89,95 evra. Uporabnikom, ki si želijo bolj kompaktnega nahrbtnika (uporaben je tudi kot šolska torba), pa je na voljo model Bobby Compact, ki prinaša še več različnih barvnih kombinacij.

RT-TRI, d. o. o.
Borovec 31,
1236 Trzin
Tel.: (01) 53 04 000
E-pošta:
info@rt-tri.si

INTERVJU: Matevž Mesojednik, vodja varnostno-operativnega centra NIL

Ko pade človeški požarni zid, je edina varovalka zaznava

Človek je hkrati najšibkejši in najmočnejši člen kibernetske varnostne verige, poudarja Matevž Mesojednik, vodja varnostno-operativnega centra NIL. Zaposleni so pogosto tarče, varnostni analitiki v varnostno-operativnih centrih pa steber obrambe pred sodobnim kiberkriminalom.

■ Informacijska varnost je danes žgoča tema v poslovnih okoljih. Zakaj?
Uspešnost poslovanja organizacij, tujih ali domačih, je danes ne le podprta, temveč pogojena s stabilnim delovanjem informacijskega sistema. Okrnjenost delovanja njegovih vitalnih funkcij lahko privede do motenega ali povsem ustavljenega izvajanja ključnih poslovnih procesov organizacije. To pa boli. In bolečina ni prav nič manjša v primeru kibernetskega napada, katerega posledice so lahko katastrofalne, na primer ohromitev poslovanja ali izguba podatkov, ugleda in poslovnih partnerjev. Vrednotenje tveganj je že v svoji zasnovi povezano s tehtanjem pogostosti ter verjetnosti uresničitve groženj in z njimi povezanih posledic.

■ Kako se z zagotavljanjem informacijske varnosti soočajo slovenska podjetja?
Slovenska podjetja si prav tako kot tuja prizadevajo za intenzivnejše povezovanje informacijskih sistemov in njihovih uporabnikov, posledično pa odpirajo tudi nove priložnosti za kibernetske zlorabe. Pri tem poslovna tveganja obvladujejo različno preudarno, celostno in kontinuirano. Pisane strategije ciljev kibernetske varnosti pridobivajo pomen (tudi na državni ravni), podjetja se vse pogosteje odločajo za vzpostavitev sistemov upravljanja informacijske varnosti. Pomemben del nastalega dokumentarnega gradiva podjetja pripisujejo vzpostavljenim procesom in kontrolam preprečevanja varnostnih incidentov. Osebno v pobudah še vedno pogrešam akcijsko noto uresničevanja teh ciljev (kadri, znanja) ter več poudarka na zmogljivostih zaznave in odziva na napredne kibernetske grožnje.

■ Kako nevarni so v praksi različni napadi in škodljive kode – se domača podjetja pogosto znajdejo med žrtvami ali pa zaradi naše majhnosti za napadalce nismo zanimivi?
Napadalci postajajo vse pametnejši in nevarnejši, saj so dobro založeni z denarnimi spodbudami. Skupen zaslužek celotne palete kibernetskega kriminala – kamor štejemo tudi izsiljevalske viruse, kiberkriminal kot storitev, preprodajo podatkov – je po oceni profesorja kriminologije na Univerzi Surrey Michaela McGuireja, objavljeni v raziskavi »Into The Web of Profit«, v prejšnjem letu po svetu dosegel 1.500 milijard dolarjev. Konkretnih podatkov za Slovenijo ni, saj navadno podjetja javno ne govorijo o tem, da so bila napadena in da je bila ob tem na primer povzročena večmilijonska škoda. Nacionalni odzivni center za kibernetsko varnost SI-CERT v svojem zadnjem poročilu navaja, da je lani obravnaval 2.300 varnostnih incidentov, največ doslej.

■ Ali je Slovenija nezanimiva?
Lahko bi rekel, da heker ne izbira končne tarče, vendar bi bila to netočna izjava. Pravi napredni napadalec ne cilja v prazno in navadno, žal, tudi ne zgreši. Napadi so vse bolj lokalno organizirani, napadalci opravijo svojo domačo nalogo. Majhna Slovenija vsekakor je na njihovem radarju – kot primera bi lahko poudaril lanski DDoS-napad na banke ter izsiljevalski virus WannaCry. Predvsem zaradi svoje strateško zanimive geolokacije, saj pomeni odlično tarčo za povzročanje kakršnihkoli motenj – političnih, transportnih, gospodarskih in v dobi agresivne digitalizacije predvsem kibernetskih.

> **Za podjetja brez informatikov in specializiranih varnostnih strokovnjakov je najučinkovitejša rešitev najem storitev varnostno-operativnega centra.**

■ Kakšna bi morala biti minimalna varnostna higiena podjetij?
Tehnološko ima večina podjetij minimalne pogoje varnega elektronskega poslovanja že pri roki. V mislih imam nosilne, sistemske in varnostne gradnike informacijskega sistema z vlogo podpore poslovanju. Osebno bi več posluha namenil predvsem pobudam varnostnih inženirjev, ki si že po naravi ves čas prizadevajo ne le za ohranjanje, temveč tudi dvigovanje ravni informacijske varnosti. Operativnim skrbniškim ekipam kakovostnega časa za uresničevanje minimalnih varnostnih zahtev praviloma primanjkuje, torej tudi za pregledovanje, triažo in ukrepanje v primerih identificiranih varnostnih incidentov. Področji, ki sta v organizacijah (pre)pogosto podhranjeni ali nedotaknjeni, sta prav nadzorna in operativna komponenta zagotavljanja informacijske varnosti. Menim, da je organizacijsko nujna vzpostavitev kontinuiranih procesov zaznave in odziva na varnostne incidente, ki bodo kos tudi neljubim situacijam, ko – in ne če – preventiva pade. Ne le na papirju, v poročilih presojevalcem ali pristojnim službam, temveč tudi operativno – v izvajanju.

> **Najpogostejši vektor dostave škodljive kode ostaja e-pošta zaposlenemu.**

■ Večina večjih podjetij skrb za informacijsko varnost zaupa oddelku IT, kaj pa lahko storijo tista, ki informatikov sploh nimajo?
Glavno je zavedanje, da smo v podjetjih za izvajanje informacijske varnosti odgovorni prav vsi zaposleni, ne le oddelek IT. Stalni procesi ozaveščanja in izobraževanja zaposlenih so zato odločilni za dvig ravni informacijske varnosti. Najpogostejši vektor dostave škodljive kode ostaja e-pošta zaposlenemu. Napredne tehnike kibernetskih kriminalcev imajo sposobnost, da zaobidejo vzpostavljene IT-varnostne kontrole. Takrat je na preizkušnji človeški požarni zid, ki je pogosto zadnja organizacijska varovalka pred povzročitvijo poslovne škode. V tem kontekstu sta zato za podjetja, ki so potencialne tarče kibernetskih napadov, odločilna pravočasna zaznava in odziv na hekerske poskuse, tudi uspešne. Za podjetja brez informatikov in specializiranih varnostnih strokovnjakov je najučinkovitejša rešitev najem storitev varnostno-operativnega centra (Security Operations Center – SOC), saj ta stalno preži na pasti naprednih kibernetskih groženj in se zna nanje ustrezno odzvati.

> **V varnostno-operativnem centru je veliko bolje imeti vrhunske eksperte in analitike, ki uporabljajo povprečna orodja, kot pa povprečne analitike, ki uporabljajo najnovejša in najdražja orodja.**

■ So varnostno-operativni centri nekakšna tržna niša na področju varnostnih rešitev?
Morebiti so tržna niša le v kontekstu ponudnika varnostnih storitev, saj te rešitve nima vsak. Gre namreč za izredno kompleksno in drago naložbo, veliko se vlaga v specializiran kader, vrhunske tehnologije in varnostne procese. V Sloveniji prostora za veliko število varnostno-operativnih centrov ni, za zdajšnje ponudnike ti pomenijo strateške naložbe.

■ Kaj pravzaprav počne varnostno-operativni center?
Varnostno-operativni center strankam ponuja široko paleto storitev spremljanja, triaže, varnostne forenzike, varnostnega preverjanja in procesov odziva na kibernetske napade. Njegova naloga je, da zazna, torej odkrije in blokira morebitnega, tudi uspešnega napadalca, še preden bi ta lahko povzročil škodo. Anonimizirane statistike večjih ponudnikov varnostnih rešitev kažejo, da je lani v povprečju pri vseh napadenih podjetjih minilo več kot sto dni, preden je bila navzočnost napadalca v omrežju zaznana, pri čemer je po raziskavi inštituta Ponemon škoda kibernetskega napada glede na prejšnje leto zrasla za 23 odstotkov, na vrtoglavih 2,4 milijona dolarjev. V državah EU je povprečje še slabše, napadena podjetja napadalca v povprečju ne odkrijejo 150 dni. Varnostno-operativni center to številko precej zmanjša.

■ V Sloveniji se je v zadnjih dveh letih pojavilo več varnostno-operativnih centrov. Kako naj podjetje loči med njimi in prepozna kakovost ponudnika?
Pri izbiri ponudnikov najemnih storitev varnostno-operativnega centra svetujem preudarnost. Pomembno je, da je izvajalec kredibilen, torej da lahko ponujene storitve dejansko tudi zagotovi in dostavi. Preveriti je treba potrebne kadrovske zmogljivosti in strokovna znanja ponudnika. Priznan varnostni strokovnjak in Gartnerjev svetovalec Anton Chuvakin vedno znova poudarja, da je v varnostno-operativnem centru veliko bolje imeti vrhunske eksperte in analitike, ki uporabljajo povprečna orodja, kot pa povprečne analitike, ki uporabljajo najnovejša in najdražja orodja. Podjetja naj bodo pozorna še na varnostno-operativne centre, ki so ali bodo zrasli iz centrov pomoči uporabnikom. Taka praksa se morda na prvi pogled zdi smiselna, saj je režim delovanja »24 ur na dan vse dni v tednu« že vzpostavljen, vendar si kaže naliti čistega vina – gre za popolnoma drugo problematiko, druga znanja in predvsem druge odgovornosti.

■ Zakaj so se varnostno-operativni centri v Sloveniji pojavili šele v zadnjih letih?
Slovenski trg je izredno konservativen. Spomnim se besed ene od strank, ki mi je dejala, da je varnostno-operativni center NIL pravzaprav petelin, ki je prezgodaj zapel. Menim, da smo petelin, ki je zapel, vendar ne prezgodaj, temveč prvi. V tujini taki centri delujejo že vsaj desetletje, in to z razlogom. Kibernetski prostor je povezan, ne pozna klasičnih meja, zato napadalci tudi v primeru simpatične deželice na sončni strani Alp ne delajo izjem. Na NIL smo že navajeni, da smo pogosto prvi, ki orjemo ledino.

■ Boste svoj SOC torej tržili tudi v tujini, kjer je sicer več konkurence?
Bomo, saj se tako kot z drugimi storitvami vedno želimo pozicionirati tudi v tujini.

■ Kaj je trenutno vaš največji izziv?
Naši izzivi so povezani s pogosto stereotipnim obvladovanjem celostnega cikla zagotavljanja kibernetske varnosti. Zaščita pred naprednimi in vse pogostejšimi hekerskimi napadi ni nujno enaka naložbi v nova varnostna orodja, ki naj bi čudežno zagotavljala zanesljivo preventivo. Nobena tehnologija ne zagotavlja popolne varnostne imunitete. Je pa mogoče sodobna varnostna orodja ustrezno prilagoditi in uporabljati z največjim možnim izkoristkom. Cikel spremljanja in obravnave varnostnih dogodkov mora biti kontinuiran proces, kjer temeljno vlogo odigrajo specializirani strokovnjaki – analitiki varnostno-operativnih centrov. Vsak napreden kibernetski napad dirigira človek, zato je pomembno, da proces varnostne triaže in obrambe izvajajo pravi varnostni eksperti, ki pa jih ni veliko. Na NIL smo tudi zato ustanovili lastno akademijo za usmerjeno vzgajanje varnostnih analitikov, ki bodo že jutri lahko na voljo za nemoteno organsko rast našega varnostno-operativnega centra.

■ V svetu že lahko opazimo nov trend, in sicer panožno specializacijo varnostno-operativnih centrov. Ponudniki se denimo osredotočajo na varovanje bančnih okolij, energetike in podobno. Se boste tudi na NIL podobno profilirali ali boste ostali varnostni generiki?
V idealnem svetu bi vsako podjetje najprej moralo imeti svoj varnostno-operativni center, nad tem pa bi morali bedeti sektorski varnostno-operativni centri, ki bi delovali tudi kot izmenjevalci informacij glede groženj, specifičnih za določen sektor. Pri delovanju kompetentnega varnostno-operativnega centra je najprej pomembna ekspertiza oziroma razumevanje logike napadalca. Ta trenutek smo usmerjeni v naše stranke, ne glede na to, v kateri panogi delujejo. Sčasoma, ko bo trg tudi pri nas postal zrelejši, pa bomo svoja znanja dodatno širili še na specializirana okolja.