IZZIVI KIBERNETSKE VARNOSTI

Kibernetska varnost je del sodobnega poslovanja

Poleg poslovne bodo podjetja potrebovala tudi kibernetsko higieno, za kar pa jim manjka več tisoč strokovnjakov. K sreči pa k boljši kibernetski odpornosti največ prispevajo prav izobraženi zaposleni.

Miran Varga, foto: Kraftart

Vsakih 39 sekund se zgodi kibernetski napad, vsako peto podjetje je že bilo tarča napada, obeti za prihodnost prav tako niso rožnati – napadenih podjetij kmalu ne bo več, bodo le tista, ki se tega, da so bila napadena, sploh ne bodo zavedala. Zlonamerna programska oprema, izsiljevalski virusi in onemogočanje dostopa do storitev so le nekateri izmed razlogov, zakaj je informacijska varnost vsak dan na preizkušnji in je treba zanjo ustrezno poskrbeti, če želi podjetje poslovati v digitalnem svetu.

Za zagotavljanje kibernetske varnosti poslovanja so ključnega pomena ljudje.

»Pri zagotavljanju kibernetske varnosti v podjetjih sta pomembna tako razumevanje kibernetskih tveganj, ki jim je podjetje izpostavljeno, kot tudi poznavanje možnosti za racionalno in učinkovito preventivno delovanje ali pa odpravo posledic kibernetskega napada. V Sekciji za kibernetsko varnost si prizadevamo za dvig uveljavitve ukrepov kibernetske varnosti v podjetjih,« je rdečo nit dogodka, naslovljenega »Izzivi kibernetske varnosti – od groženj do implementacije ukrepov«, ki sta ga organizirala Združenje za informatiko in telekomunikacije ter IKT horizontalna mreža na Gospodarski zbornici Slovenije, povzel **predsednik Sekcije za kibernetsko varnost Mihael Nagelj** in nadaljeval: »Ključna zgodba konference je: Ukrepe kibernetske varnosti je potrebno načrtovati in izvajati celovito, ne glede na to, ali gre za organizacijske, tehnične ali pa ukrepe, povezane z uporabniki. Kibernetska varnost mora biti del vseh projektov digitalne preobrazbe poslovanja in to že od samega začetka, saj iskanje in krpanje morebitnih ranljivosti ob že implementiranih rešitvah lahko močno poveča stroške slehernega projekta.«

Kibernetska varnost skrbi celo Evropo

Vzpostavitev enotnega digitalnega trga (DSM) je eden najpomembnejših strateških ciljev Evropske unije. Da bi podprla ta cilj, je Evropska komisija kibernetsko varnost prepoznala kot eno ključnih področij, ki potrebuje takojšnje ukrepanje na evropski ravni, zlasti vzpostavitev močnih evropskih rešitev kibernetske varnosti za vzpostavitev zaupanja. Ker mala in

Na konferenci je spregovoil Mihael Nagelj, vodja sekcije za kibernetsko varnost (SeKV/ZIT).

srednje velika podjetja predstavljajo kar 99,8 % vseh podjetij v Evropi, se je treba osredotočiti predvsem nanje. Tudi zato, ker večinoma niso (ustrezno) pripravljena na kibernetske napade in druge nevarnosti digitalnega sveta. »Podjetja vseh velikosti so danes tarče hekerskih napadov. Prav zato sta zasnova in izvedba učinkovitega ekosistema na regionalni ravni bistvenega pomena za delitev stroškov in najboljših praks, izmenjavo visokokvalificiranega osebja in izkoriščanje potencialnih sinergij med različnimi deležniki, kot so univerze, javni organi, telekomunikacijski operaterji, podjetja, specializirana za kibernetsko varnost itd.,« je izzive kibernetske varnosti na ravni EU predstavil **Luigi Rebuffi, generalni sekretar Evropske organizacije za kibernetsko varnost (ECSO)**.

Nevarnosti digitalnega sveta

Ključne trende na področju kibernetske varnosti in kibernetske grožnje so predstavila slovenska podjetja. **Dr. Andrej Rakar, vodja informacijske varnosti v družbi Petrol**, je izpostavil, da so trn v peti varnostnih strokovnjakov že desetletja predvsem tehnike socialnega inženiringa, s katerimi napadalci pretentajo zaposlene v podjetjih, da jim (nevede) odprejo vrata do sistemov, aplikacij in omrežja podjetja (beri: omogočijo zastonj). Predstavil je tipične primere napadov v jadranski regiji, kot so napadi, ki so ohromili poslovanje podjetij Lekarna Ljubljana, ProPlus, Revoz, Knauf Insulation in drugih ter organizacij, kot sta Uprava RS za zaščito in reševanje ter Slovenska policija. Večinoma prav na račun spletnih prevar in škodljivih kod ter izsiljevalskih virusov. Za hekerje je lahko tudi informacijski oblak zlata jama – namesto, da cilja na posameznika v podjetju, lahko z vdorom v oblak prevzame nadzor nad več tisoč uporabniškimi računi in podatki. Dr. Rakar je osvetlil tudi minimalne varnostne ukrepe, ki bi jih po njegovem mnenju potrebovalo vsako podjetje, ter izpostavil področja, ki jih podjetja pogosto spregledajo, kot so aktivno zaznavanje varnostnih incidentov, opredelitev varnostnih zahtev za (ključne) dobavitelje ter zagotavljanje integritete kadrov in njihove ozaveščenosti glede informacijske varnosti. Dejstvo, da se napadalci v omrežjih in sistemih podjetja lahko skrivajo tudi po več mesecev, preden so odkriti, ni sprejemljivo.

Dalibor Vukovič, specialist kibernetske varnosti v podjetju Telekom Slovenije, je poudaril, da velja več sredstev in človeških virov v podjetjih nameniti preventivni (prediktivni) varnosti, namesto rešitvam za reaktivno varovanje, ko do težav že pride. T. i. obveščevalne informacije podjetjem lahko povedo, kateri napadi in napadalci ciljajo nanje, kaj velja takoj posodobiti, ker je posodobitev na voljo ipd. Vukovič je izpostavil, da na podjetja danes prežijo predvsem štiri vrste nevarnosti, ki se od napadov z izsiljevalskimi virusi (šifriranje podatkov) stopnjujejo še na krajo podatkov, napade z onemogočanjem storitev ter grožnje strankam podjetja (na podlagi podatkov, ki so jih napadalci ukradli podjetju).

Skrb za kibernetsko odpornost

Do varnostnih incidentov bo vedno prihajalo, pomembno je, da je podjetje sposobno pravilnega in hitrega odziva. Tu lahko podjetjem pomagajo standardi. Standardi na področju kibernetske varnosti posredujejo znanje za celovito obvladovanje kibernetskih tveganj, kar zmanjšuje stroške implementacije in dviguje raven t. i. kibernetske odpornosti.

Idealna rešitev bi bila, da ima vsako podjetje lasten varnostno-operativni center (SOC), v katerem deluje visoko usposobljena ekipa varnostnih strokovnjakov in analitikov ter zagotavlja hitro reakcijo na napade. Seveda si lasten SOC lahko privoščijo le velika podjetja, k sreči pa SOC svoje znanje in sposobnosti podjetjem nudijo v obliki storitev, ki so bistveno dostopnejše. Kakšen varnostno-operativni center izbrati? Predvsem takšnega, ki pozna okolje panoge, v kateri deluje podjetje, saj bo tako poznal tudi potencialne ranljivosti in grožnje.

Napadalci so v omrežjih in sistemih podjetja lahko skriti tudi po več mesecev, preden jih odkrijejo.

Sodelujoči na konferenci so se posvetili tudi ključnim trendom na področju kibernetske varnosti in obvladovanju kibernetskih tveganj.

»Zelo priporočljivo je, da posamezno podjetje vsaj enkrat letno najame strokovnjake, ki opravijo t. i. varnostni pregled. S tem nedestruktivnim napadom brez omejitev, ki preverja upoštevanje varnostne politike, ukrepov in rešitev ter celovito obravnava tehnologijo, procese in zaposlene – vendarle gre za najbolj realen scenarij vdora v organizacijo – podjetje pridobi temeljito poročilo glede ranljivosti in priporočila za njihovo odpravo,« je udeležencem konference zaupal **etični heker Elijah B. Hlastan**, ki sodeluje s

podjetjem **ProAstec**, in priporoča redno izvajanje kibernetskih vaj z zaposlenimi.

Znanje je najboljša obramba

Po vsem svetu po ocenah primanjkuje kar 3,5 milijona varnostnih strokovnjakov. In še zelo dragi so. Kako naj podjetja pridobijo ustrezne kadre? Kader s področja kibernetske varnosti se izobražuje dve do štiri leta (v primeru, da že ima računalniško podlago oz. predznanje), saj gre za zelo specifično področje znanja, ki ga fakultete pri nas (še) ne učijo. Najboljši recept je izobraževanje lastnega kadra, predvsem informatikov, ki bi radi okrepili znanje s področja kibernetske varnosti.

»Locked Shield je največja svetovna vaja s področja informacijske varnosti, v kateri sodelujejo malodane vsi mogoči strokovnjaki, ki rešujejo vprašanja kibernetske varnosti na številnih področjih, od telekomunikacijskih operaterjev, bank, energetike, komunale, bolnišnice, vojske do javne uprave. Več kot dva tisoč IT-inženirjev iz 32 držav je izvajalo številne naloge, eni v vlogi napadalcev in drugi v vlogi obrambe. To strokovnjakom daje možnost intenzivnega izobraževanja in preskusa zmožnosti. S tem države s podporo NATO kompetenčnega centra za kibernetsko varnost preizkušajo elemente kibernetske odpornosti držav. Slovenija je dosegla bistven napredek, saj se je uspešno udeležila dveh zadnjih tekmovanj z nadpovprečnimi rezultati, kar kaže na strokovnost posameznikov. Ti dve tekmovanji sta pokazali, da je mogoče sodelovanje javnega in zasebnega sektorja, ki je zaradi pomanjkanja kadra nujno. Sodelovanje v takšnem dogodku pa je pokazalo tudi na 'sistemske težave',« je povedal **Gregor Spagnolo, svetovalec s področja informacijske varnosti,** iz **podjetja SSRD**. Razvoj strokovnega kadra zahteva sistematičen pristop od mladih v šolah, univerzitetnega izobraževanja za vključevanje v začetne poklice karierne poti specialista kibernetske varnosti.

Kako dobro je posamezno podjetje pripravljeno na kibernetsko obrambo, je razvidno tudi iz t. i. IT zrelostnega modela podjetja. »Dokler je informatika v očeh (vodstva) podjetja samo ali predvsem strošek, ne moremo pričakovati dobre varnostne drže. Šele ko informatika postane področje, ki ustvarja dodano vrednost ali konkurenčno prednost, so navadno vlaganja v kibernetsko varnost in izobraževanje zaposlenih ustrezna,« je povzel **Miha Lavrič, tehnični direktor podjetja CREAplus**.

Kje začeti z gradnjo ali nadgradnjo kibernetske odpornosti? Predvsem s standardi (npr. ISO/IEC 27001 in 27002), ki vsebujejo temeljna znanja o celovitem pristopu, priporočila za načrtovanje in izvajanje ukrepov in dobrimi praksami, ki so na voljo za različna področja in vrste industrij. Velikih bližnjic ni. S pomočjo podjetij, ki izvajajo storitve v sektorju kibernetske varnosti od analize kibernetskih tveganj, izvajanja storitev varnostno operativnega centra, varnostnih preverjanj in testiranj do izobraževanja uporabnikov. Zavedati se je treba, da so tudi za zagotavljanje kibernetske varnosti poslovanja ključnega pomena ljudje in ne (zgolj) tehnologije. ■