V podjetjih iz predala še vedno pogosto potegnejo star varnostni načrt, s katerim si nimajo kaj pomagati.«

»NAJBOLJ ME SKRBIJO NAPADI Z UMETNO INTELIGENCO.«

- Kako umetna inteligenca že pomaga pri varovanju v podjetjih?
- Zakaj bi se bilo dobro spomniti na staro akcijo Nič nas ne sme presenetiti?
- Ali bodo podjetja v prihodnje doletele kazni, če ne bodo priglasila incidentov?

Goran Novković
Foto: Barbara Reya

Branko Slak je predsednik Zbornice za razvoj slovenskega zasebnega varovanja. Tako je odličen poznavalec trendov na področju fizičnega, tehničnega in tudi kibernetskega varovanja.

Ali podjetja razumejo, da fizična in tehnična varnost nista več ločeni od kibernetske varnosti?

Mislim, da razumejo, ampak zavedanja še vedno ni dovolj. Številna podjetja varnost še vedno obravnavajo kot skupek ločenih področij – fizično, tehnično, informacijsko. V praksi pa so ti segmenti že dolgo prepleteni.

Ali zdaj podjetja za varovanje v sklopu svojih ponudb že ponujajo tudi varovanje pred kibernetskimi napadi?

Tega v ponudbah še ni, saj je šele v fazi razvoja. Paketi fizičnega, tehničnega in mehanskega varovanja pa so tudi pri nas zelo razviti že nekaj let. Tehnologija zelo hitro napreduje, od kamer do javljalnikov; vsako leto je revolucija. Kamere se integrirajo z različnimi sistemi, umetno inteligenco, z različnimi drugimi parametri.

Kako umetna inteligenca vpliva na varovanje? Kaj prinaša dobrega?

Veliko. Umetna inteligenca je izjemno pomembna pri analitiki. Vsaka kamera danes že vsebuje integralne sisteme, ti pa vključujejo umetno inteligenco, prepoznavanje različnih parametrov, obrazov, kretenj in zvokov.

V času, ko je velik izziv varnost v šolah, se v nekaterih šolah že zanimajo za kamere z umetno inteligenco, ki analizirajo gibanje, kretnje in zvoke ter ugotavljajo odstopanja od normalnih vsakodnevnih gibanj in izrazov. Kamere prepoznavajo tudi registrske tablice, štejejo ljudi, odkrivajo nenavadno gibanje, zapuščene predmete in podobno. Tako dajejo signale varnostnim službam, predvsem fizičnemu varovanju, kaj je treba pregledati, poostriti oziroma preveriti.

»Imamo težave pri javnih naročilih. Še vedno je pogosto merilo najnižja cena, kar pa se na področju varnosti ne bi smelo dogajati.«

Ali slovenska podjetja že naročajo takšno opremo v paketu?

Da, nekatera zelo. Premalo zavedanja je zlasti na strani države, v javni upravi. Imamo pa težave pri javnih naročilih. Prvič, ta javna naročila so slabo pripravljena. In drugič, še vedno je pogosto glavno merilo najnižja cena, kar pa se na tem področju ne bi smelo dogajati. Za najnižjo ceno seveda dobiš tisto, kar ni najboljše.

Kako se hibridne grožnje odražajo v praksi, pri fizičnem varovanju?

Hibridne grožnje pomenijo napade na več ravneh hkrati: fizični vdori, sabotaže, dezinformacije. Zelo so usmerjene tudi na zaposlene. Nepridipravi poskušajo z izsiljevanji, grožnjami in različnimi vabami prek njih priti v sistem in narediti škodo.



Tipičen primer je fizični vdor v objekt, da bi napadalci namestili zlonamerno strojno ali programsko opremo, ki jim omogoča oddaljen dostop do sistema. Tako napad postane bolj učinkovit, saj napadalci pridobijo notranjo točko dostopa in lažje obidejo digitalne zaščitne mehanizme.

Dezinformacije pa najpogosteje ciljajo na človeški faktor – vplivajo na odločanje zaposlenih, povzročajo paniko, preusmerjajo pozornost ali spodkopavajo zaupanje v varnostne procese. Ravno zato je nujno, da varnostno osebje ni samo tehnično opremljeno, temveč tudi usposobljeno za prepoznavanje širšega konteksta groženj.

Kako nepridipravi največkrat izkoristijo zaposlene?

Ni nujno, da grozijo. Lahko poskušajo z mehkimi metodami, torej različnimi ugodnostmi, a tudi z izsiljevanjem in podobno. Zelo pomembno je, da imajo podjetja nadzor nad svojimi zaposlenimi, da uvajajo varnostno kulturo. Tako varnost ni samo stvar vodstva in seveda varnostnih menedžerjev, ampak je ta varnostna kultura prisotna tudi pri zaposlenih.

Koliko podjetij si danes že privošči varnostnega menedžerja? Katera ga mogoče ne potrebujejo?

Kritična infrastruktura in vse organizacije, ki upravljajo pomembne informacije, bi ga morale obvezno zaposliti. Povprečna podjetja pa bi morala imeti nekoga, ki spremlja varnostne izzive. Ta oseba mora biti odgovorna tudi za informacijsko varnost. Glede na to, da je vse povezano v informacijske verige, je nujno, da ima pregled na tem, kako zaposleni ravnajo z njimi.

Ali podjetja v zadnjem času k podjetjem za varovanje pristopajo bolj proaktivno? Ali pa to še vedno večinoma storijo šele takrat, ko se zgodi incident?

V veliko manjših in srednjih podjetjih še vedno delujejo reaktivno. Reagirajo takrat, ko imajo problem, sicer pa to področje preveč zanemarjajo.

Je kakšna možnost, da bi se podjetja v državi varnostno okrepila tudi prek dvojnega namena za obrambna sredstva, ki bodo na voljo v EU? Če je lahko infrastruktura del tega programa, zakaj ne bi bila tudi varnostna obramba vsaj kritičnih podjetij? Se kaj dogaja na tem področju?

Mislim, da ne.

V katerih podjetjih ali organizacijah so v zadnjih letih uspešno preprečevali škodo, ker so bila dobro varovana ali pa so se varnostne službe dobro odzvale?

Zelo velika preprečitev okoljske in zdravstvene škode je bila zasluga varnostne službe ob požaru v Kemisu. Interventni varnostnik je v tem primeru v sedmih minutah prišel na kraj, zaprl vse glavne ventile in vse dovode ter tako preprečil veliko večjo škodo. Takratna škoda je bila sicer velika, a hkrati še vedno minimalna v primerjavi s tem, kaj bi se lahko zgodilo, če varnostna služba ne bi ukrepala tako, kot je.

Področje varovanja zelo hitro napreduje, tudi tehnično. Kako naj vodstva podjetij preverjajo, ali je vse varovano, kot je treba?

Z rednimi presojami ogroženosti. Ob tem je treba ves čas preverjati varnostna tveganja. Brez tega ne gre. Pomembni so predvsem standardi ISO 27001 (informacijska varnost), ISO 22301 (neprekinjeno poslovanje), pa tudi smernice, kot je EN 50600 za podatkovne centre. Certifikacija ni vedno nujna. Pomembno pa je, da podjetje deluje po teh načelih.

Na kaj ste že in boste v prihodnje še bolj pozorni pri varnostnih pregledih ali presojah?

Vsekakor so to informacijska veriga, informacijski sistemi, kibernetska varnost. Predvsem pa je treba nenehno posodabljati načrte varovanja. Ugotavljamo, da imajo podjetja pogosto zelo stare varnostne načrte, ki jih nihče ne preverja in posodablja. S takšnim zastarelim načrtom si nimajo kaj pomagati.

To je velik problem, še zlasti, če tudi tisti, ki so v podjetju odgovorni za varovanje, varnostnih načrtov ne poznajo. Tega je zelo veliko. Varnostni načrt je izjemno pomemben; je miselna vaja, miselni proces, kako se odzvati, ko pride do varnostnega problema.

»Interventni varnostnik je ob požaru v Kemisu v sedmih minutah prišel na kraj, zaprl vse glavne ventile in vse dovode ter preprečil veliko večjo škodo.«

V bistvu tako treniramo, kot v času slogana Nič nas ne sme presenetiti.

Tako je. V dejanskih primerih pa se odloča o življenjih.

Koliko podjetij že ima primerne standarde varnosti?

Precej podjetij je na tem področju zelo dejavnih. V prihodnje bo izjemno pomembna implementacija evropske varnostne direktive NIS-2. Ta zadeva varovanje podatkov, kibernetsko varnost

Branko Slak: Kaj nas lahko najbolj skrbi?

1 **Kibernetski napadi –** vse pogostejši in bolj sofisticirani napadi, kot so izsiljevalski virusi (ransomware), phishing in vdori v sisteme, tudi z umetno inteligenco.

2 **Neenotnost varnostnih sistemov –** nepovezani fizični in informacijski varnostni sistemi otežujejo hiter in učinkovit odziv.

3 **Pomanjkanje investicij –** številna podjetja varnost še vedno vidijo kot strošek, in ne kot strateško naložbo, to pa upočasnjuje uvedbo sodobnih rešitev.

4 **Pomanjkanje ozaveščenosti –** zaposleni pogosto niso dovolj usposobljeni za prepoznavanje nevarnosti, kar predstavlja šibko točko v varnostni verigi.

... Tu bo morala država narediti velike in odločne korake ter ustanoviti skupino, ki bo te zadeve spremljala.

Kaj pa bo to pomenilo za podjetje?

Predvsem to, da bodo bdela nad varnostnimi problemi, o njih redno obveščala in jih tudi sanirala. Država pa mora vse to predpisati, vendar tega še ni storila. Vse bi morala urediti do oktobra, za zdaj pa nimam niti podatka, da bi bila ustanovljena skupina, ki bi to morala izpeljati.

Kako se bodo zaostrili standardi varovanja v prihodnosti?

Ukrepi bodo strožji na področju varovanja podatkov, kibernetske varnosti, informacijske varnosti ...

Bodo podjetja in pristojni kaznovani, če bodo denimo zamolčali varnostni incident?

Tako je. Morali bodo poročati o varnostnih incidentih, zbirati podatke, odreagirati v primeru incidentov in tako naprej. To bo v podjetja zagotovo prineslo višjo stopnjo varnostne kulture.

Poročanje bo bistveno bolj pod nadzorom sankcij, kar pomeni, da bo večji informativni pretok o varnostno pomembnih podatkih. Poleg tega bo morala biti varnostna zaščita pred tveganji v organizacijah bistveno bolj urejena. Nič več ne bo šlo po domače.

Kaj vas zdaj najbolj skrbi, ko gre za varnost podjetij v Sloveniji?

Napadi z uporabo umetne inteligence. Ti napadi so težje zaznavni in zahtevajo napredne obrambne mehanizme. Kibernetski napadi lahko naredijo izjemno škodo. Nekateri so jo že povzročili.

Spomnimo se primera v Holdingu slovenskih elektrarn. Ali na Univerzi v Mariboru, ki si po napadu ni opomogla pol leta. Vse to zaradi slabe zaščite podatkov, nezadostnih varnostnih protokolov, neenotnih varnostnih sistemov, pomanjkanja investicij v varnost in premajhne ozaveščenosti zaposlenih.

Malo za šalo, malo zares. Zakaj Evropska komisija državljane opozarja, naj naredijo 72-urne zaloge zaradi morebitnega napada, ne opozarja pa podjetij?

Ker se od podjetij pričakuje, da imajo načrt za ta namen. 72 ur je pričakovani časovni okvir, v katerem naj bi energetika, telekomunikacija, varnostne službe vzpostavile normalno delovanje. Do takrat bi morali državljani nekako funkcionirati sami, zato morajo biti na to pripravljeni.