Avtor: Aljoša Kandžič / Institut za korporativne varnostne študije

INTERVJU
Božidar Dajčman,
direktor Oddelka upravljanja fizične in informacijske varnosti, Nova KBM d.d.*

KORPORATIVNA VARNOST JE POMEMBEN DEJAVNIK ZA ZAGOTAVLJANJE USTREZNE ODPORNOSTI DELOVANJA ORGANIZACIJE

V današnjem zahtevnem varnostnem okolju je zagotavljanje odpornosti in s tem neprekinjenosti delovanja velikih poslovnih organizacij, nujna za poslovno učinkovitost. Korporativna varnost ima v tem okviru posebej izraženo vlogo in odgovornost.

Obvladovanje varnostnih tveganj je zelo pomembna nit vaše strokovne kariere. Katera področja so posebej zaznamovala vaš karierni razvoj?

V svet varnosti sem vstopil pred sedmimi leti, najprej na področje informacijske varnosti. Kljub temu, da sem imel takrat že veliko izkušenj z informacijsko tehnologijo, organizacijo in bančništvom, je bil začetek poln presenečenj. Kot bi odprl bomboniero Foresta Gumpa, kjer nikoli ne veš, kaj se skriva v ovitku. Tudi kasneje sem se največ časa ukvarjal s kibernetskimi tveganji, veliko pa tudi s tveganji fizične varnosti in neprekinjenega poslovanja. Ob začetku epidemije COVID-19 smo vsi največ pozornosti posvečali ukrepom za zdravje naših strank in zaposlenih.

g. Božidar Dajčman je prejemnik nagrade »Slovenian Grand Security Award« v kategoriji »Korporativno varnostni manager leta 2020«

Vsa ta področja se medsebojno prekrivajo v pojmih kot so »tveganje«, »varnostni ukrepi«, »incident«, »načrt odziva«, »odpornost«, »obrambne linije«. S temi pojmi se srečujem vsak dan, vendar vsakič malo drugače. Na žalost in na srečo moje delo še ne kaže znakov, da bi postajalo rutinsko.

V zadnjem obdobju ste zelo močno vpeti v upravljanje varnostnih tveganj v NKBM. Menite, da je ustrezno razumevanje sprememb kompleksnega varnostnega okolja lahko konkurenčna prednost podjetij?

Gotovo. Podjetje lahko tudi z omejenim proračunom uspešno zmanjša tveganja, če jih dobro razume. Pomembno je, da denar in energijo posvečamo pravim tveganjem, torej tistim z večjim produktom frekvence in učinka. To ni niti samoumevno niti lahko, saj so nekatera tveganja bolj vidna in razumljiva kot druga. Podjetje, ki pozna tveganja, bo sprejelo boljše odločitve o tem, katerim tveganjem se je treba izogniti, katerim je treba zmanjšati verjetnost ali učinek in katera si deli z zavarovalnico. Na koncu je treba določena tveganja tudi sprejeti. Prave odločitve prinašajo optimalno uporabo virov in obvladana tveganja, s tem pa prednost pred konkurenti.

*podjetje je korporacijski član Slovenskega združenja korporativne varnosti

Bančni sektor je zaradi regulativnih zahtev in varnostnih tveganj, ki se vedno bolj selijo v informacijsko okolje, zelo specifičen pri svojem delovanju. Kako kompleksni so v tem okviru koraki za obvladovanje tveganj, katerim je podvrženo delovanje vašega podjetja?

Bančno poslovanje je obvladovanje in sprejemanje tveganj. Vsakič, ko banka odobri kredit, prevzame tveganje, da denarja ne bo dobila nazaj.

Regulatorji skrbijo, da banka sprejme samo toliko tveganja, kolikor ga lahko z lastnim kapitalom prenese tudi v pesimističnih scenarijih. V prihodnosti se lahko zgodi, da bodo odločilna tudi varnostna tveganja.

Če zelo poenostavimo, sta koraka za obvladovanje tveganj samo dva: analiza tveganj in izvedba ukrepov za njihovo zmanjšanje. V resnici je precej bolj zapleteno. Različne vrste tveganj banka obravnava z različnimi koraki, vendar na koncu pridemo do skupne slike – profila tveganosti banke. Pri izračunu potrebnega kapitala banke so upoštevana vsa tveganja. Za operativna tveganja, kamor sodijo tudi varnostna, uporabljamo poseben okvir upravljanja. Ta opisuje korake, s katerimi zagotovimo, da tveganja ne presežejo sprejemljivih okvirov. Sprejemljivi okviri so tudi formalno opredeljeni v izjavi o nagnjenosti k prevzemanju tveganj.

Sistem obvladovanja tveganj v bankah je za zunanje opazovalce videti precej zapleten in ta videz ne vara. Ne glede na to, pa je osnovni gradnik logično razmišljanje z nekaj matematike.

Informacijska varnost je v vaši dejavnosti izrednega pomena. Še posebej so se ti izzivi izpostavili ob trajanju epidemije COVID-19, saj je pomembna večina zaposlenih svoje delo začela opravljati izven svojega rednega informacijskega delovnega okolja. Kako v vašem podjetju ocenjujete izvajanje potrebnih ukrepov na tem kompleksnem področju?

> Podjetje, ki pozna tveganja, bo sprejelo boljše odločitve o tem, katerim tveganjem se je treba izogniti, katerim je treba zmanjšati verjetnost ali učinek in katera si deli z zavarovalnico. Na koncu je treba določena tveganja tudi sprejeti. Prave odločitve prinašajo optimalno uporabo virov in obvladana tveganja, s tem pa prednost pred konkurenti.

Informacijska varnost je res še posebno poudarjena, saj banke razpolagajo z velikimi finančnimi sredstvi in je zato tudi potencialna korist za napadalca večja. Izpostavljeni so tudi komitenti, oz. njihova sredstva. Tveganja sledijo poslovanju: ker je večina poslovanja preseljena v digitalno okolje, je tam tudi večina tveganj.

COVID-19 je prinesel kup dodatnih izzivov. Na prvem mestu moramo poskrbeti za zdravje svojih strank in zaposlenih. Za tem pride na vrsto dodatna skrb za informacijsko varnost, ki

Vsaka tranzicija že zaradi svoje narave vedno prinaša dodatna tveganja. Pri vsaki spremembi je mogoče, da kakšen vidik zanemarimo ali naredimo napake. Poleg tega so spremembe vedno povezane z nekim prehodnim, začasnim obdobjem, ko je sistem bolj izpostavljen tveganjem. Ko je vmesno stanje mimo, pridejo do izraza prednosti.

je potrebna zaradi spremenjenega načina dela. Spremenila se je količina in vsebina dela na daljavo. Ne gre samo za to, da več ljudi dela od doma, ampak tudi omogočamo oddaljeno izvajanje nekaterih opravil, za katere je bila prej zahtevana fizična prisotnost. Kljub temu ne gre za neke nove rešitve, saj so bili tehnični pogoji za varno delo na daljavo na voljo že prej. Tehnika sama ne zadošča, deluje pa skupaj z drugimi ukrepi, od omejevanja pooblastil do ozaveščanja zaposlenih.

Premik se je zgodil tudi pri naših strankah. Kljub temu, da je bila večina poslovalnic odprta ves čas epidemije, so mnoge stranke na lastno ali našo pobudo prenesle poslovanje na digitalne kanale. Ti kanali so varni pred COVID-om, se pa tam stranke in banke srečujejo z drugačnimi virusi in drugimi tveganji.

Se v Republiki Sloveniji po vaše dovolj zavedamo pomembnosti področja kibernetske varnosti? So ukrepi, ki jih izvaja država na tem področju ustrezni ali pogrešate konkretnejše ukrepe?

Država ne more zagotoviti varnosti namesto posameznikov in podjetij, zato od nje ne smemo pričakovati preveč. Za zdaj smo lahko spremljali nekaj uspešnih in nekaj manj uspešnih zgodb. Med uspešne štejem dosedanje delovanje SI-CERT-a.

Upravi za informacijsko varnost bomo morali dati nekaj časa, da bo lahko opravila svojo vlogo nacionalnega organa za informacijsko varnost in želim, da bi jim to dobro uspelo. Tudi druge akterje v nacionalnem sistemu kibernetske varnosti čaka še veliko dela. Nikakor si ne želim dveh stvari: slabega sodelovanja med različnimi deležniki v sistemu in pretirane regulacije. So pa področja, kjer je regulacija potrebna in vloga države nenadomestljiva. To zagotovo velja za zagotavljanje delovanja kritične infrastrukture in bistvenih storitev, pri čemer ni pomembno samo kdaj in kako pri nas uvedemo direktive in uredbe EU, kot npr. NIS/NIS2, GDPR, ECI/RCA, DORA.

Tako kot v podjetju, so tudi na nivoju države nekatera tveganja bolj vidna in razumljiva, druga manj. Zato moramo razumevanje tveganj nadgrajevati. Pri tem je ceneje, če se učimo na tujih in ne lastnih napakah. V začetku leta smo videli, kakšna je moč internetnih velikanov, ki lahko po lastni presoji enostavno odklopijo družbeno omrežje ali podjetje. Po potrebi bi lahko odklopili tudi celotne države in vsa podjetja, ki v njih delujejo. Za ilustracijo si lahko skušamo predstavljati, kakšne bi bile posledice, če nenadoma nehajo delovati vse rešitve Google v Sloveniji: iskalnik Google, brskalnik Chrome, telefoni z operacijskim sistemom Android, zemljevidi in navigacija, Gmail, Google Drive, Google Docs... In kakšne bi bile posledice, če bi državo v celoti odrezali od interneta? Ne vem, ali ima država pripravljene načrte odziva na takšne dogodke, bi si pa to želel.

V zadnjem obdobju ste izvedli zelo zahteven poslovni proces združevanja dveh pomembnih bančnih ustanov v Republiki Sloveniji. Posebej z varnostnega vidika je bil to verjetno pomemben izziv, ki je prinesel tudi veliko novih izkušenj in dobrih praks. Lahko z nami podelite nekaj najpomembnejših?

Združitev druge in tretje največje banke v Sloveniji je bil zelo zahteven projekt, ki je prinesel velike organizacijske, tehnološke, produktne, kadrovske, lokacijske in druge spremembe. Dodatna okoliščina je bila epidemija COVID-19 v času, ko so potekale ključne naloge na področju operativnega združevanja. Vsaka tranzicija že zaradi svoje narave vedno prinaša dodatna tveganja. Pri vsaki spremembi je mogoče, da kakšen vidik zanemarimo ali naredimo napake. Poleg tega so spremembe vedno povezane z nekim prehodnim, začasnim obdobjem, ko je sistem bolj izpostavljen tveganjem. Ko je vmesno stanje mimo, pridejo do izraza prednosti.

Na področju varnosti je bilo naše izhodiščno načelo preprosto: tam, kjer banki nista imeli enakih rešitev, se uporabi bolj varna možnost, oz. višji standard. Že pred operativno združitvijo smo uvedli enotno varnostno politiko in podrejene dokumente. Potem smo potrebovali še nekaj časa, da smo varnost poenotili tudi na operativni ravni. Pri fizični varnosti to pomeni tudi dodatne in posodobljene sisteme tehničnega varovanja, pri informacijski varnosti pa opustitev nekaterih orodij in uvedbo drugih v povečanem obsegu.

V Novi KBM smo pravočasno pričeli postavljati strukturo in ekipo za upravljanje varnosti v večji banki, zato smo bili na združitev dobro pripravljeni.

Kako pristopate k prepričevanju strateškega managementa, da za delovanje procesov korporativne varnosti nameni ustrezne organizacijske in finančne vire?

Uprava Nove KBM se zaveda varnostnih tveganj in je pripravljena sorazmerno s tem tudi dodeljevati vire. Kljub temu ni tako preprosto. Predlogi morajo biti utemeljeni z jasnim vplivom na tveganja. Še posebno morajo biti argumenti močni, kadar gre za izdatke zunaj načrtovanih okvirov. Velja tudi pregovor »daleč od oči, daleč od srca«, zato skušamo izkoristiti vsako priložnost, da so varnostna vprašanja obravnavana na najvišjih nivojih upravljanja. Pomembno je, da je oddelek organizacijsko podrejen neposredno upravi.

Na koncu odloča medsebojno zaupanje, ki smo ga pri dosedanjem delu z upravo že vzpostavili.

Verjetno redno spremljate stanje na področju korporativne varnosti v slovenskem okolju. Kako bi ocenili zavedanje strateškega managementa v slovenskih podjetjih o pomenu korporativne varnosti in učinkovitega obvladovanja tveganj?

Nekaj informacij o stanju korporativne varnosti v okolju dobim od kolegov iz drugih podjetij, nekaj pa lahko sklepam glede na varnostne dogodke, za katere izvem.

V najslabšem primeru se zavedanje dvigne šele ob večjih incidentih. Zunaj finančnega sektorja ni mnogo organizacij, kjer je strateški management jasno ugotovil in opredelil kolikšna tveganja lahko organizacija prenese in kolikšna so pripravljeni sprejeti, kar velja tudi za varnostna tveganja.

Po drugi strani tudi na dnevih korporativne varnosti srečujemo predstavnike podjetij, kjer je obvladovanje tveganj in še posebno korporativna varnost na visokem nivoju. To ne bi bilo mogoče brez podpore strateškega managementa.

Je vlaganje v izobraževanje kadrovskih potencialov v organizacij lahko tista potrebna kvaliteta, ki tudi na področju varnostnega zavedanja, loči uspešna podjetja od povprečnih?

Po mojih izkušnjah lahko najhitreje in najceneje zmanjšamo varnostna tveganja ravno z izbiro in oblikovanjem pravih kadrov. Še posebno na področju kibernetske varnosti poznam več primerov, ko so organizacije investirale velike zneske v tehnične rešitve, zmanjkalo pa je denarja ali volje za vzpostavitev ekipe, ki bi te rešitve izkoristila. Prodajalci varnostnih rešitev poznajo nešteto takih zgrešenih projektov (ni pa nujno, da o njih govorijo potencialnim kupcem).

Varnostna ozaveščenost ni le vprašanje informiranosti, ampak gre za del organizacijske kulture. Na žalost je včasih lažje zamenjati zaposlene, kot spremeniti njihov način razmišljanja in obnašanja. To še najbolj velja za nas managerje, saj je organizacijsko kulturo treba graditi od zgoraj navzdol.

Vaše podjetje je tudi eden od pomembnih korporativnih članov Slovenskega združenja korporativne varnosti. Menite, da so take oblike združevanja strokovnjakov s področja korporativne varnosti potrebna in lahko prinesejo v naš prostor dodatno kvaliteto?

Skupaj s sodelavci v Novi KBM smo naredili že veliko, nikoli pa ne bo zmanjkalo izzivov na področju varnosti. Za pravi odziv na te izzive ni dovolj en človek. Imamo izredno ekipo, s katero je pravi užitek delati.

Združevanje je potrebno, da lahko kot vsebinsko močna skupina prispevamo pri oblikovanju okvirjev varnosti v državi. Potrebno je tudi zaradi prenosa znanj in izkušenj. Sam sem se na srečanjih s kolegi že veliko naučil, vendar to ni edini razlog, da se udeležujem dogodkov združenja. Pridem predvsem zato, ker je zanimivo in prijetno.

Kaj vam pomeni prejeta nagrada Slovenian Grand Security Award v kategoriji »korporativno varnostni manager leta«?

Počaščen sem. To je elitna nagrada za področje korporativne varnosti. Kdor pozna dosedanje nagrajence, ve da je tako. Lepo je biti v taki družbi.

Skupaj s sodelavci v Novi KBM smo naredili že veliko, nikoli pa ne bo zmanjkalo izzivov na področju varnosti. Za pravi odziv na te izzive ni dovolj en človek. Imamo izredno ekipo, s katero je pravi užitek delati. ■