Sodobni časi in kibernetska varnost

Andrej Guštin, maj 2020

Povzetek:
Zadnja situacija s COVID-19 je pokazala, da je mogoče celoten ustroj družbe prestaviti v spletni prostor. Vse deluje, ni nam potrebno hoditi v službo ali na predavanja in iz domačega naslonjača lahko upravljam vse, kar v sodobnem času potrebujem. Ampak vsa ta lahkotnost in udobnost ima svojo ceno. Ta se kaže v povečanju tveganj, da morebiti naše početje spremlja še kdo in si morda pri tem kakorkoli že pomaga.
Ključne besede: Cyber Security
Vloga: varnost, upravljanje tveganj, kibernetska varnost, zlorabe

Odprem naslovnico enega od slovenskih spletnih časopisov in udarna novica se glasi »Hekerji napadli Easyjet in pobrali podatke devetih milijonov oseb«. Ker sem pred časom – lahko bi rekli še v normalnih razmerah turističnega udejstvovanja navadnih državljanov – potoval z njimi tudi sam, se lahko upravičeno sprašujem, ali so med temi ukradenimi podatki tudi moji? So sedaj naprodaj somalskim hekerjem za ustvarjanje lažnih profilov in lajkov na FB in LN, ali se lahko znajdejo v kakšnem sodobnem programu za analizo zemljanov in pripravah na naslednjo pomoč pri volitvah (pustimo kje in kdaj, dovolj je, da vemo, da v resnici je to mogoče).

Zadnja situacija s COVID-19 je pokazala, da je mogoče celoten ustroj družbe prestaviti v spletni prostor in da lahko živimo s socialno distanco praktično preko svojih avatarjev. Vse deluje, ni nam potrebno hoditi v službo ali na predavanja in iz domačega naslonjača lahko upravljam vse, kar v sodobnem času potrebujem (naročam hrano, plačujem položnice, izvajam predavanja in delavnice, spremljam delo na projektih in tu pa tam pogledam kak film, ki je že dolgo na čakalni listi). Ampak vsa ta lahkotnost in udobnost ima svojo ceno. Ta se kaže v povečanju tveganj, da morebiti naše početje spremlja še kdo in si morda pri tem kakorkoli že pomaga. Se vam je morda zgodilo – v zadnjem času zelo popularnem ZOOM ali JITSI programu – da je sredi vašega sestanka nekdo »uletel« za trenutek, morda povedal kak stavek v tujem jeziku, potem pa zapustil srečanje? To je samo vrh ledene gore, možnih napak ali zlorab, ki se lahko pripetijo pri uporabi sodobnih digitalnih platform, če ne skrbimo za varnost. Kibernetska varnost[1] (ang. Cyber Security) je pojem, ki opredeljuje sklop metodologij in tehnologij, s katerimi se lahko zaščitimo (preventivno in kurativno) v sodobnem času. Pesem »Ker sovražnik ne spi« - zasedbe Martin Krpan[2] je tako rekoč vizionarska za čase korona krize – trend naraščajoče zlorabe v trenutnih razmerah, ki eksponentno rastejo[3] (samo v aprilu je bilo 30% povečanje) in povzročajo ogromno globalno gospodarsko škodo. Vloga kibernetske varnosti še nikoli ni bila tako pomembna, kot je sedaj v teh časih – tako v vlogi posameznika, kot seveda gospodarskih družb, kjer moramo neprestano uravnotežiti nemoteno poslovanje in notranjo učinkovitost, kot na drugi strani spreminjajoče se nevarnosti in tveganja v digitalnem prostoru (več o tem [4]).

[1] https://sl.wikipedia.org/wiki/Glosar_kibernetske_varnosti
[2] https://www.youtube.com/watch?v=gW3NvJA4UCs
[3] https://ikt.finance.si/8961727/BODITE-PREVIDNI-Kibernetski-napadi-povezani-s-korono-se-se-kar-mnozijo
[4] https://www.mckinsey.com/business-functions/risk/our-insights/cybersecuritys-dual-mission-during-the-coronavirus-crisis

Kaj je področje kibernetske varnosti

Kibernetska varnost je v splošnem smislu opredeljena, kot sklop med seboj povezanih elementov in aktivnosti, ki imajo skupen cilj v zagotavljanju visoke ravni varnosti vseh informacijskih in komunikacijskih rešitev v podjetju (in tudi širše), ki so bistvenega pomena za nemoteno in pravilno delovanje samega podjetja v vseh varnostnih razmerah in zagotavljajo bistvene storitve podjetja na področju njegovih ključnih dejavnosti.

Kibernetska varnost je tako sklop aktivnosti in drugih ukrepov, tehničnih in ne-tehničnih, katerih namen je zaščititi računalnike, računalniška omrežja, strojno in programsko opremo ter informacije, ki jih le-ta vsebuje in obravnava, kar vključuje programsko opremo in podatke, kot tudi druge elemente kibernetskega prostora, pred vsemi grožnjami, vključno z grožnjami nacionalni varnosti.

Kibernetsko varnost definiramo tudi kot stopnjo zaščite, ki jo aktivnosti in ukrepi lahko zagotovijo na področju delovanja in poslovanja podjetja. Nenazadnje je kibernetska varnost tudi neprekinjen proces, ki združuje področja profesionalnih naporov, vključno z raziskavami in razvojem na področju implementiranja in izboljševanja ukrepov ter dvigovanja kakovosti le-teh, z namenom neprestanega dvigovanja stopnje zaščite, kot tudi neprestanega sledenja in odzivanja na razvoj in napredek potencialnih groženj in zlonamernih aktivnosti.

Temeljna naloga kibernetske varnosti

Kibernetska varnost je zelo širok pojem, z velikim številom zelo aktualnih izzivov (več o tem[5]). Njena temeljna naloga je, okrepiti in sistemsko urediti področje zagotavljanja kibernetske varnosti v podjetju glede na sam evolucijski razvoj podjetja, njegove aktivnosti in področja delovanja ter zrelost internega okolja procesov in IKT infrastrukture. Zagotoviti mora varnost zaposlenih, vodstva, partnerjev in deležnikov v ekosistemih v kibernetskem prostoru, pri čemer kot varnost mislimo na (vsaj sledeče) dimenzije:

- Varnost medsebojnega komuniciranja v notranjih in zunanjih omrežjih med vsemi deležniki.
- Upravljanje z dostopi do občutljivih (npr. osebnih) in tajnih podatkov ter virov, s katerimi delamo, razpolagamo, jih hranimo ali upravljamo.
- Preprečevanje prejemanja, branja, shranjevanja ali posredovanja škodljive programske opreme, ki nam jo lahko zlonamerno nastavijo kot sprožilec nadaljnjih nevarnih korakov zlorab.
- Zagotoviti preprečevanje varnostnih incidentov (odtekanje podatkov, nepooblaščeni dostopi in vstopi v omrežja in naprave) v izvajanju vsakodnevnih procesov.
- Zagotoviti kibernetsko varnost na področju splošne varnosti in zatiranje gospodarskega kibernetskega kriminala (vdorov, virusov, kraj, onesposodobitev ipd);
- Zagotavljanje varnega delovanja in razpoložljivosti ključnih informacijsko-komunikacijskih sistemov podjetja ob velikih naravnih in drugih nesrečah, ki lahko prizadenejo ožje ali širše področje (geografsko, procesno, organizacijsko, telekomunikacijsko).
- Neprestano usposabljati vse deležnike ter dvigovati osveščenost in kulturo upravljanja kibernetskih tveganj (»nam se to ne more zgoditi«) na vseh stičnih točkah med ljudmi in tehnologijo.
- Upravljanje z elementi ukrepanja v primeru incidentov, zlorab ali drugih dogodkov, ki nastanejo v primeru napada ter čim hitrejša povrnitev v prvotno stanje s čim manj izgubami.
- Priprava politik upravljanja in delovanja ter internih organizacijskih pravil, s katerimi preventivno postavljamo okvirje za pravilno izvajanje vseh procesov v podjetju.

[5] http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7707

Seveda je teorija lažja od prakse. Pri varnostnem pregledu procesov v podjetju ugotavljamo številne kritične točke, ki so lahko ponekod že sistemske narave in zaradi zgodovine vgrajene v vse pore poslovanja – in se jih vodstva družb niti ne zavedajo. Naj omenimo samo najpogostejše:

- Slabo upravljanje tveganj, nepripravljenost na različne možne scenarije v stilu »nam se to ne more zgoditi«.
- Ne-posodabljanje programske opreme oziroma ne vzdrževanje strojne opreme, kar lahko pripelje do varnostnih dogodkov (npr. Odpovedi delovanja) ali incidentov (npr. vdorov).
- Nedefinirano ali slabo definirano zaznavanje in ukrepanje v primeru kibernetskih napadov.
- Slaba ali sploh ne izvedena usposabljanja zaposlenih, partnerjev in drugih deležnikov v ekosistemih.
- Puščanje nezaščitenih delov celotnega procesa ali informacijskega okolja (npr. prenosa, vstopa, kopiranja, delovnega terminala ipd.).
- Slabo izvajanje testnih vaj in usposabljanj, kar prinese napake v času odzivanja, ko se tveganja udejanjijo in pride do kibernetske grožnje.
- Slabo izmenjevanje informacij med internimi deležniki, pa tudi med različnimi eksternimi deležniki, tako o samih grožnjah, tveganjih, kot tudi postopkih zaznavanja in odzivanja.
- Neopredeljenost bistvene infrastrukture, rešitev in kritičnih procesov za primer odpovedi delovanja in vzpostavitve načrta neprekinjenega poslovanja.
- Vključitev kibernetske varnosti pod področje IT-ja, njegovo upravljanje in proračun, namesto neodvisne vzpostavitve funkcije upravljanja s kibernetsko varnostjo nadrejeno področju IT kot takem.

Kaj storiti – kako narediti prvi in najpreprostejši korak naprej

Težko je rešiti vse težave v eni potezi. Če bi moral izbrati eno samo potezo, s katero bi naredili največ koristi za vse deležnike, na področju njihove zaščite in upravljanja, potem bi se odločil za uporabo samodejne, z elementi umetne inteligence podprto, nevidno, natančno in tehnološko napredno rešitev, ki bi »pod radarjem« skrbela za preventivno in kurativno zaščito podjetja, njegovih procesov in deležnikov v njih, skozi različne načine njihove interakcije. Ker ljudi ne moremo spremeniti čez noč, na drugi strani pa so lahko vložki v tehnološke (strojne) zaščite dragi, je optimalna rešitev »hobotnica« načinu zagotavljanja varnosti. Integrira proaktivno spremljanje in nadzor informacijske tehnologije v organizaciji, preprečuje in odkriva napade ter celovito usklajuje odziv v primeru napada. Takšna rešitev izvaja napredno zaščito na končnih točkah, spremlja omrežni promet, proaktivno upravlja ranljivosti in pomaga notranjim odgovornim skrbeti za optimalni kibernetsko varnost.

S pomočjo sodobnih tehnologij (več o tem[6]) rešitev, nenehno – samodejno - analizira aktivnosti v notranjem zaščitenem okolju, kot so npr.: aktivnost uporabnikov, obnašanje procesov ter omrežni promet, obnašanje naprav in povezanih komunikacijskih sredstev ipd, ter na osnovi spremljave vzorcev obnašanja zagotavlja ciljano zaščito pred nevarnostmi z visoko natančnostjo, skupaj z avtomatiziranimi postopki obvladovanja vseh glavnih vektorjev napadov. V primeru resnejših napadov pa samodejno aktivira varnostno operativni center (SOC), delujoč 24/7, ki s svojimi varnostnimi strokovnjaki dopolnjuje varnostno ekipo v podjetju ter zagotavlja odziv na napad, iskanje groženj in obvladovanje tveganj. Ena takih rešitev je danes – v praksi preverjen - Cynet (več o tem[7]).

[6] https://www.creaplus.si/sl/cynet
[7] https://www.cynet.com/

Dodatno so področje kibernetske varnosti okrepili tudi z metodami IIBA poslovne analize (več o tem[8]), s katerimi si lahko pomagamo pri postavitvi konceptov varnosti v podjetjih, identifikacijah tveganj v poslovnih procesih, pripravi kontrolnih funkcij za upravljanje s tveganji ter pripravo predlogov za uvedbo rešitev. Pri pripravi vsebine sta združila moči mednarodni organizaciji IIBA in IEEE, ki sta pripravili tudi strokovno podlago in gradivo z potrebnimi znanji, vključno s certifikacijo (več o tem[9]).

Sklep – bo jutri bolje in varneje?

Ja, kako naj napišemo? Kot je rekel nekoč en predsednik vlade, nam ostane le napor, kri, solze in znoj - »*I have nothing to offer but blood, toil, tears and sweat*.«. Enako bo na področju kibernetske varnosti in zagotavljanja nemotenega življenja posameznikov in družb. Z napredkom tehnologij, se lov mačke in miši nadaljuje. V naslednjih 5 letih se bo fokus napadov in branjenja zagotovo usmeril v pametne naprave, stroje in senzorje (IoT 4.0 in kibernetska varnost), ki bo vedno bolj zlepil fizični in digitalni svet med napravami in ljudmi. S tem se bo število končnih točk, ki so najbolj ranljive za potencialne napade drastično povečalo in priča bomo obsegu, ki ga za sedaj niti ne poznamo in ne zmoremo dojeti. Po nekaterih ocenah bo leta 2025 medsebojno povezanih več kot 75 milijard naprav. Tega obsega človek kljub največjim naporom in znanjem ne more več spremljati samostojno. S tem pa se odpira nov element kibernetske varnosti in to je uporaba umetne inteligence za spremljanje, preprečevanje groženj ter napadov in saniranje škode po le teh. Nad stroj s strojem, nad pametne stroje s še bolj pametnimi stroji ☺. A žal je res tako.

Avtor članka: Andrej Guštin

---

[8] https://www.iiba.org/standards-and-resources/cybersecurity-analysis/
[9] https://www.iiba.org/certification/iiba-certifications/specialized-business-analysis-certifications/certificate-in-cybersecurity-analysis/