INFORMACIJSKA VARNOST:
IZZIVI SODOBNE TEHNOLOGIJE

Urednik: Blaž Markelj

Maša Dreven • Bojan Dobovšek • Uroš Jelenc
Ida Majerle • Peter Makovšek • Blaž Markelj
Eneja Mervič • Gorazd Praprotnik
Gregor Skerl Beronja

LEXPERA®
GV ZALOŽBA
Ljubljana 2020

Predgovor

Knjiga *Informacijska varnost: Izzivi sodobne tehnologije* je druga v zbirki Informacijska varnost. Dotika se številnih problematičnih področij informacijske varnosti, s katerimi se kot družba srečujemo pri uporabi sodobne tehnologije. Nekatera so že del našega vsakdanjega življenja, večina v knjigi predstavljenih problemov pa je vezana na najnovejše pojave, povezane z informacijsko varnostjo. Ta področja so še dokaj neraziskana in ranljiva. Knjiga ponudi dober vpogled ter spodbudi nadaljnje raziskovanje in iskanje rešitev za kakovostnejše zagotavljanje varnosti informacij.

Prvo poglavje predstavi hibridne grožnje, ki so del našega vsakdanjega življenja, čeprav se morda tega niti ne zavedamo. Spremljajo nas že več stoletij, danes pa so posebno pomembne predvsem zaradi nove tehnologije, vezane na svetovni splet. Mednje uvrščamo uporabo konvencionalnega in nekonvencionalnega orožja ter kibernetičnih pristopov, za katere so značilni kreativnost, dvoumnost in kognitivni elementi vojne. Najpogosteje se sploh ne zavedamo, da smo tarča oziroma že žrtev hibridnega napada. Te grožnje so še resnejše zaradi tega, ker nikoli niso vezane le na lokalno raven, temveč so globalni problem. Za obrambo pred njimi je ključno tesno sodelovanje med posameznimi deležniki ter hitro izmenjevanje informacij in drugih potrebnih znanj.

Drugo in tretje poglavje obravnavata informacijsko varnost v zdravstvu. Drugo je usmerjeno na varstvo podatkov v aplikacijah m-zdravja. Ponudba teh pripomočkov, s katerimi lahko spremljamo svoje zdravje in splošno počutje, se je v zadnjih desetletjih močno razvila. Vzporedno z eksponentnim naraščanjem števila aplikacij se

krepi tudi obseg spremljanja in zbiranja občutljivih osebnih podatkov uporabnikov. Čeprav je pri ravnanju s tovrstnimi podatki zahtevana višja stopnja varnosti in zasebnosti, jih številne aplikacije prenašajo v nešifrirani obliki prek nezaščitenih omrežij, kar lahko privede do razkritja in zlorabe. Skrbi, povezane s tovrstnimi aplikacijami, vzbuja tudi premajhna transparentnost razvijalcev aplikacij m-zdravja glede uporabljenih varnostnih praks.

V tretjem poglavju je v ospredju informacijska varnost medicinskih pripomočkov. Uporabljamo širok nabor naprav, ki so zaradi možnosti povezovanja z različnimi brezžičnimi omrežji, programsko opremo, različnimi operacijskimi sistemi ipd. ranljive in dovzetne za različne varnostne grožnje. Njihova ranljivost je predvsem posledica vpeljave interneta stvari v medicino brez ustreznih varnostnih mehanizmov. Tudi pri medicinskih pripomočkih so lahko ogroženi osebni podatki uporabnikov, poleg tega pa še njihovo zdravje in življenje. Pri nekaterih pripomočkih je namreč mogoče spreminjanje nastavitev, kar lahko vpliva na uporabnikovo zdravje.

V četrtem poglavju je podrobneje predstavljeno varovanje podatkov pri uporabi zelo praktičnih pametnih merilnikov energije, ki zbirajo izredno natančne informacije o uporabnikovi porabi električne energije v kratkih časovnih intervalih. Vendar na podlagi teh informacij lahko prepoznamo naprave, ugotavljamo prisotnost ali odsotnost oseb, njihove navade ter dejavnosti, kar lahko močno poseže v uporabnikovo zasebnost. Raziskava je pokazala, da se uporabniki pametnih merilnikov energije tega zelo slabo zavedajo.

V petem poglavju je obravnavana informacijska varnost koncepta interneta igrač. Danes v pametne naprave, ki postajajo del digitalnega sveta, razvijajo celo igrače. Internet igrač je del interneta stvari ter omogoča še večjo raznolikost igre in aktivnosti kot pametne igrače, hkrati pa staršem in skrbnikom omogoča, da otroke spremljajo in z njimi pri tem tudi komunicirajo. Toda ob uporabi te pridobitve se pretakajo ogromne količine osebnih podatkov, zato je pomembno, da

se zavedamo ranljivosti takega sistema. Ker so vpleteni otroci, je to še toliko bolj nujno, saj so ti precej lažje tarča kibernetskih napadov kot odrasli.

Šesto poglavje se ukvarja s preprečevanjem zlorab internetnega in elektronskega bančnega poslovanja, ki temelji na prepoznavanju vzorcev uporabnikovih značilnosti. Kibernetski kriminal poleg materialne in poslovne škode dolgoročno tudi upočasnjuje razvoj internetnega in elektronskega bančnega poslovanja, lahko ga celo popolnoma ustavi. Zato se pri uporabi kibernetskega poslovanja poleg klasičnih metod varovanja, ki temeljijo na preverjanju pristnosti uporabnikov, vse bolj uporabljajo metode zaznavanja in preprečevanja sumljivih transakcij s spremljanjem, analiziranjem in prepoznavanjem vzorcev uporabnikovih značilnosti.

Zadnje, sedmo poglavje nam podrobneje predstavi stičišče standardov ISO/IEC 270xx in Splošne uredbe o varstvu podatkov. Osebni podatki so ena izmed vrst informacij, zato praksa pri zagotavljanju varstva osebnih podatkov sledi splošnim načelom varovanja informacij in obvladovanja informacijskovarnostnih tveganj. Kljub temu pa je pri varstvu osebnih podatkov treba upoštevati še druge posebnosti. V nadaljevanju sta predstavljena tudi družina standardov 270xx in kontekst, kamor je Informacijski pooblaščenec uvrstil ta standard. Prikazana so glavna stičišča uredbe in standarda, pojasnjeno je tudi, na katerih področjih varstva osebnih podatkov si organizacije lahko dodatno pomagajo pri implementiranju organizacijskih in tehnoloških ukrepov v skladu s standardom.

Knjiga tako z vsemi vsebinskimi sklopi predstavi ključne izzive pri uporabi sodobnih tehnologij in zagotavljanju informacijske varnosti.

doc. dr. Blaž Markelj
Fakulteta za varnostne vede, Univerza v Mariboru

Kazalo

Kazalo slik

Recenziji

Knjiga *Informacijska varnost: Izzivi sodobne tehnologije* je sestavljena iz sedmih poglavij, ki so vsako zase in skupaj znanstveno zaokrožena celota o izbrani problematiki informacijske varnosti. Nastala je v soavtorstvu in ponuja dobro premišljeno sintezo znanstvenih prispevkov, ki so strnjeni v sedem poglavij.

Navdušenje zbuja zadostna in potrebna celovitost, saj so poglavja napisana sistemsko in sistematično. Avtorji v izbrani problematiki in opredeljenih problemih iščejo součinkovanje in soodvisnost, vendar ob tem ostajajo na realnih tleh. V tej celovitosti so termin varnost iz polja nedotakljivega prenesli v dotakljivo, saj povsem nevsiljivo opomnijo na ključni pomen informacijske varnosti na ravni posameznika in družbe. Pri tem se ne izogibajo nesporni in zahtevni dvojnosti sodobne tehnologije. Pomen varnosti podatkov, ki je nujna za varovanje zasebnosti, je osrednje sporočilo znanstvene monografije. Toda avtorji to dominanco predstavijo povsem nevtralno, kar omogoča znanstvene, strokovne in celo laične interpretacije ter nadaljnje družbeno odgovorne in kreativne razprave.

Znanstvena monografija ponuja dragocena izhodišča za strokovno, študentsko in znanstveno javnost pri prepoznavi nespornih prednosti in pasti uporabe sodobne tehnologije ter, kar je najpomembnejše: opiše, kako upravljati, obvladovati in reševati klinične zaplete, s katerimi se tako posameznik kot družba srečujemo pri uporabi sodobne tehnologije in varovanju neprecenljive posameznikove in družbene zasebnosti. Izjemno pomembna dodana vrednost knjige je tudi prispevek k splošnemu zavedanju o pomenu varnosti pri uporabi sodobne tehnologije.

red. prof. ddr. Teodora Ivanuša

Ljubljana, 24. marca 2020

Informacijska varnost: Izzivi sodobne tehnologije je znanstvena monografija, ki jo sestavlja sedem poglavij. Vsako poglavje je sklenjena celota, hkrati pa pomemben del mozaika knjige. Monografija se začne s poglavjem o hibridnih grožnjah, ki bralcu na inovativen način oriše širšo sliko groženj v kibernetskem in realnem svetu. Nadaljnja poglavja obravnavajo specifične tematike informacijske varnosti, s katerimi se srečujemo vsak dan, vendar se pri tem premalo zavedamo problematičnih vidikov sodobne tehnologije. Avtorji to problematiko opišejo na zanimiv način in jo podkrepijo s statističnimi podatki.

Delo v središče postavlja pomen varnosti za posameznika in družbo pri uporabi kibernetskega prostora in danes dostopnih sodobnih tehnologij. Že s prvim poglavjem, ki poda širši opis današnjih hibridnih groženj, se avtorji dotaknejo tematike, ki je del posameznikovega vsakdanjika. V nadaljevanju pa nato podrobneje predstavijo pomen varovanja posameznikove zasebnosti in podatkov ter težave, povezane s tem.

Knjiga je izredno pomembno gradivo za posameznika in družbo, namenjena pa je tako za splošno kot specifično rabo.

izr. prof. dr. Janez Mekinc

Ljubljana, 29. marca 2020

Mnenja o knjigi

Knjiga je pomemben prispevek k ozaveščanju splošne in strokovne javnosti o izzivih za našo varnost in zasebnost, ki jih prinašajo nekatere sodobne tehnologije. V vsakdanjem življenju smo namreč z njimi vse bolj povezani, v internet stvari se vključujejo naše naprave, pripomočki, celo igrače, s čimer se povečuje tudi količina zbranih podatkov o nas. Podatki pa so moč, zato bo zavedanje, kdaj in komu jo dajemo ter kaj to pomeni za nas, za ohranitev zasebnosti v sodobni družbi ključno.

mag. Andrej Tomšič, *namestnik Informacijske pooblaščenke*

Informacijska varnost in zmanjšanje tveganj na tem področju postajata v vse bolj digitalizirani družbi čedalje pomembnejša. Z vpeljavo tehnologije 5G bomo v gospodarstvu in družbi začeli uporabljati internet stvari, ki omogoča neposredno komunikacijo in integracijo podatkov med fizičnim in virtualnim svetom ter izredno velike podatkovne zbirke. Poleg izjemnih priložnosti pa prinaša tudi široko paleto novih tveganj na področju kibernetske varnosti. Eden pomembnejših varnostnih vidikov je nedvomno zagotavljanje zaupnosti, integritete in dostopnosti podatkov – osebnih podatkov posameznikov, občutljivih poslovnih podatkov gospodarskih subjektov in podatkov, povezanih z nacionalno varnostjo – kar zahteva vpeljavo in zagotavljanje vrhunskih varnostnih mehanizmov in rešitev. Knjiga ponuja odličen vpogled v opisano problematiko zagotavljanja informacijske varnosti in je tehtno gradivo tako za strokovno kot tudi za laično javnost, saj ta z informiranim delovanjem lahko pomembno pripomore k omejevanju kibernetskih tveganj.

Lovro Peterlin, *managing direktor A1 Slovenija*

V podjetjih se premalo zavedajo, da so zaposleni lahko ključna šibka točka pri neustrezno pripravljenem načrtu o kibernetski varnosti. Kljub visokim denarnim vložkom, namenjenim varnostni infrastrukturi, namreč informacijski sistem podjetja lahko ogrozi že en sam napačen klik. Zato je izredno pomembno stalno izpopolnjevanje zaposlenih na področju informacijske varnosti; v našem podjetju za to dosledno skrbimo. Knjiga po mojem mnenju lahko pomembno izboljša splošno ozaveščenost slovenske javnosti o pomenu varnosti v kibernetskem prostoru in pri uporabi sodobnih informacijskih tehnologij.

Mateja Gramc Debeljak, *direktorica PHD Slovenija*

Sodobna orodja in tehnologije interneta stvari so postali nepogrešljiv del našega vsakdanjega življenja, s tem pa se povečuje tudi naša odvisnost od sodobnih tehnologij in informacijskih storitev. Na ravni posameznika in družbe se zelo dobro zavedamo prednosti, ki nam jih prinašajo, premalo pa tveganj za informacijsko varnost, ki jim z uporabo teh tehnologij na široko odpiramo vrata domov, ustanov, podjetij. To kažejo primeri varnostnih incidentov in pojavov na področju informacijske varnosti, o kakršnih lahko slišimo vsak dan. Zato je knjiga Informacijska varnost: Izzivi sodobne tehnologije pomemben pripomoček za ozaveščanje o nujnosti informacijske varnosti tako na ravni posameznikov kot tudi na ravni delovanja različnih družbenih sistemov. K zmanjševanju prepada med razvojem, razširjenostjo in uporabnostjo sodobnih orodij in tehnologij interneta stvari na eni strani ter izzivi informacijske varnosti na drugi lahko ključno prispeva tudi znanstvena in strokovna javnost – tako da obravnava dileme in izzive na tem področju ter skuša poiskati ustrezne rešitve zanje. Menim, da bo v tem pogledu knjiga izpolnila bralčeva pričakovanja.

Andrej Maslo, *direktor področja Korporativna varnost in nadzor, Pošta Slovenije, d. o. o.*

Informacijska varnost je že v zadnjem desetletju eden največjih izzivov v digitalnem svetu, v prihodnosti pa bo še toliko bolj pomembna za vse segmente – od držav in podjetij do posameznikov. Zavedanja glede informacijske varnosti je na splošno premalo, zato knjigo toplo priporočam vsem, saj ponuja veliko odgovorov na ključne izzive glede informacijske varnosti. Najpomembnejši vidik, da bi čim bolj zmanjšali tveganja, pa so ozaveščeni posamezniki – le tako bomo vsi bolj varni pred kibernetskimi napadi, zlorabo osebnih podatkov in drugimi tveganji.

Zdravka Zalar, *direktorica SmartIS, d. o. o.*

Tehnološki razvoj je vse hitrejši. Brez informacijsko-komunikacijskih tehnologij si sodobnega načina življenja ne moremo več predstavljati. Zahteva po čim hitrejšem prilagajanju je vse večja, s številnimi izzivi pa se srečujemo prvič in prepogosto smo nanje popolnoma nepripravljeni. Tehnologija nam seveda močno olajša življenje, vendar nas lahko tudi ogrozi, zato je pri njeni uporabi potrebna previdnost. Knjiga zelo razumljivo prikaže tako pozitivne kot negativne strani uporabe sodobnih tehnologij.

mag. Ajša Vodnik, *generalna direktorica AmCham Slovenija in podpredsednica AmChams in Europe*

Veseli me, da smo dobili knjigo v slovenskem jeziku z uglednimi domačimi avtorji. Kot vemo, se informacijska varnost začne pri posamezniku. S kibernetskimi grožnjami se srečujemo tudi v Sloveniji, absolutne varnosti pa seveda ni mogoče zagotoviti. Tarča oziroma že žrtev hibridnega napada se tega ponavadi niti ne zave takoj. Knjiga nam bo pomagala, da bomo bolje razumeli pomen varnosti pri uporabi sodobnih tehnologij tako za posameznika kot za družbo.

dr. Michele Leonardi, *izvršni direktor IBM Slovenija, d. o. o.*

Informacijska varnost je tematika, s katero nikoli ne moremo biti preveč seznanjeni. Incidenti nas znova in znova opozarjajo, kje so naše pomanjkljivosti in na katerem področju nekdo ni naredil dovolj. Spekter področij oziroma potencialnih groženj je zelo obširen. Čeprav se o tem morda ne sliši veliko, številna slovenska poslovna okolja kljub vlaganjem v informacijsko tehnologijo vsak dan prizadenejo hudi informacijski pretresi in grožnje z »lockdownom«. Mogoči so nepredstavljivi scenariji, primerljivi s presenečenjem svetovnih razsežnosti, kar zdaj doživljamo ob pandemiji koronavirusne bolezni. Knjiga bralcu omogoči poglobljen vpogled v problematiko in ponudi številne odgovore za varnejši in lepši jutri nas vseh.

Klemen Zupan, *direktor ZupO.si, d. o. o.*

Že bežen pogled v ne tako oddaljeno zgodovino na področju informacijsko-komunikacijskih tehnologij, recimo na prehod v 21. stoletje, nam razkrije izredno intenziven razvoj tega področja. Pripadniki mlajše generacije se niti ne spomnijo več, da smo za dostop do interneta uporabljali klicne modeme s hitrostjo 56 kbit/s. Danes se nam zdijo normalne hitrosti nekaj 10 ali 100 Mbit/s, optična omrežja, ki vodijo do naših domov in podjetij, pa so običajna tehnološka rešitev. A kakšno povezavo ima to s tehnologijami na področju informacijske varnosti? Veliko, saj je vsesplošna povezljivost in dostopnost prinesla veliko novih vprašanj in izzivov, povezanih prav z informacijsko varnostjo.

Danes se digitalizacija širi z neverjetno hitrostjo, vse bolj se uveljavljajo tehnologije umetne inteligence in avtomatizacije v IKT-sistemih, ki presegajo človeške omejitve pri obdelavi masovnih podatkov. Kaj bi se zgodilo, če bi kibernetski napad na elektroenergetski sistem povzročil mrk in za nekaj dni pretrgal dobavo električne energije, kot je to apokaliptično, a realno opisal Marc Elsberg v knjigi Blackout?

Pred takimi in podobnimi izzivi smo vsi tisti, ki se vsak dan ukvarjamo s tehnološkimi rešitvami in njihovim razvojem. Kako zagotoviti

primerne rešitve, ki bodo omogočile uspešno in učinkovito varovanje informacijskih sistemov, podatkov, procesov, tovarn, infrastrukture, ne nazadnje tudi zdravja in človeških življenj? Napadalci, hekerji s temne strani interneta, imajo danes na voljo več orodij in možnosti za izvajanje kibernetskih napadov kot kadarkoli doslej. Po robu se jim lahko postavimo le z uporabo številnih naprednih tehnoloških rešitev. Potrebujemo dobro izurjeno armado strokovnjakov s področja kibernetske varnosti in IKT, ki so primerno organizirani proti delovanju kibernetskih nepridipravov.
Knjiga je pomemben prispevek h krepitvi zavedanja in posredovanju znanj tako za strokovno kot za laično javnost, saj pri zagotavljanju kibernetske varnosti sodelujemo vsi, ki sodobna informacijska sredstva uporabljamo pri svojih vsakodnevnih aktivnostih in delu.

Peter Ceferin, *tehnični direktor (CTO) Smart Com, d. o. o.*

Knjiga obravnava konkretne in aktualne teme s področja informacijske varnosti ter opozori na zanimive izzive, s katerimi se bomo morali spoprijeti v bližnji prihodnosti.

Gorazd Božič, *vodja SI-CERT*

Kibernetski napadi v zadnjem desetletju niso več le neke vrste igra nadobudnih mladih hekerjev, temveč so prevzeli vlogo vodilnega orožja v mednarodnem vojskovanju. Vključujejo različne strategije in taktike, namenjene vplivanju na procese odločanja, kar pripomore k uresničevanju strateških ciljev, kot so obsežne informacijske kampanje, novačenje radikalcev ali vplivanje na oblikovanje politike. Z njimi ne želijo povzročati materialne škode, temveč dosegati politične in sociološke cilje. Knjiga je odlično izhodišče za učinkovito seznanitev in prepoznavanje današnjih kibernetskih groženj ter ponuja usmeritve, kako se z njimi spoprijeti in jih obvladovati.

Janez Križan, *strokovnjak za informacijsko varnost, CISM*

Knjiga zelo dobro zapolnjuje vrzel med splošnimi zapisi s področja informacijske in kibernetske varnosti na eni strani ter visokospecializirano »hekersko« literaturo na drugi. Ob tem osvetljuje več področij, na katerih se internetne tehnologije šele uveljavljajo, s tem pa ustvarjajo tako koristi kot tudi nova tveganja. Širšemu bralstvu na razumljiv in strokoven način podaja zelo aktualne teme, s katerimi se bomo v prihodnje pogosto srečevali.

Metod Platiše, *Telekom Slovenije, d. d.*

Pogled v zgodovino civilizacije kaže, da je razvoj na vseh področjih potekal inkrementalno, postopoma, dovoljen je bil čas, da se človek navadi in osvoji nekaj novega. V dobi informacijske tehnologije takšni intervali ne obstajajo več. Osrednja značilnost pri razvoju tehnologije je konstanta eksponentne rasti, ki nas postavlja pred vprašanje, v kolikšni meri bomo sposobni odgovoriti na izzive tehnologije, navsezadnje tudi v smislu naših bioloških omejitev. V takšnem okolju bi informacijska varnost morala spadati med temeljne človeške vrednote, a tega še vedno ni čutiti. Zato izid knjige pozdravljamo, saj vsekakor prispeva k našemu skupnemu cilju – vse večji ozaveščenosti slovenske družbe o teh vprašanjih.

Marko Milotič, *direktor, Unistar PRO*