INFORMACIJSKA VARNOST:
ETIČNO HEKANJE

Sara Tomše • Blaž Markelj

LEXPERA®
GV ZALOŽBA
Ljubljana 2020

Dr. Blaž Markelj (1982) je docent za področje varnostnih ved na Fakulteti za varnostne vede Univerze v Mariboru. Že vrsto let se izobraževalno in raziskovalno ukvarja z informacijsko varnostjo. Je avtor številnih mednarodnih in domačih znanstvenih in strokovnih člankov. Kot vabljeni predavatelj je predaval na številnih mednarodnih in domačih dogodkih. Njegova posebnost je združevanje raziskovalnega in aplikativnega področja, kar dokazuje tudi s številnimi dogodki s področja informacijske varnosti, ki jih je v zadnjih letih pomagal organizirati kot član ali vodja organizacijskega oziroma programskega odbora.

Sara Tomše (1994) je študirala na Fakulteti za varnostne vede Univerze v Mariboru in tam leta 2019 tudi magistrirala iz modula Informacijska varnost. Pri delu se je z informacijsko-komunikacijsko tehnologijo prvič srečala kot svetovalka za tehnična vprašanja v telekomunikacijskem podjetju. Pozneje se je zaposlila kot analitičarka kibernetske varnosti v operativnem centru za kibernetsko varnost, kjer dela še danes. Med študijem je veliko pozornosti namenila tematikam s področja informacijske varnosti, še posebej hekanju in penetracijskemu testiranju.

It's kind of interesting, because hacking is a skill that could be used for criminal purposes or legitimate purposes, and so even though in the past I was hacking for the curiosity, and the thrill, to get a bite of the forbidden fruit of knowledge, I'm now working in the security field as a public speaker.

Kevin Mitnick

Brainyquote.com, https://www.brainyquote.com/authors/kevin-mitnick-quotes

Kazalo vsebine

Kazalo tabel

Kazalo slik

Kratice in simboli

2G	second generation wireless telephone technology	druga generacija brezžične telefonije
4G	fourth generation of mobile telecommunications technology	četrta generacija mobilnih omrežij
5G	fifth generation mobile networks	peta generacija mobilnih omrežij
AP	access point	dostopna točka
ARP	address resolution protocol	protokol za preverbo naslovov

ASCII	American standard code for information interchange	ameriški standard za zapis znakov, brez šumnikov in preglasov
ATM	asynchronous transfer mode	protokol za prenos enako dolgih podatkovnih paketov
BLE	Bluetooth low energy	Bluetooth nizke energije
BYOD	bring your own device	prinesi svojo napravo
CD	compact disc	optični disk za zapis podatkov
CEH	certified ethical hacker	certificirani etični heker
CIA	confidentiality – integrity – availability	zaupnost – celovitost – dostopnost
CIRT	computer incident response team	ekipa za odziv na incidente
CPU	central processing unit	centralna procesna enota
CRC	cyclic redundancy check	ciklično preverjanje redundance
CSIRT	computer security incident response team	ekipa za odziv na varnostne incidente
C&C	command and control	poveljevanje in kontrola
DDoS	distributed denial of service	porazdeljena ohromitev storitve
DNS	domain name system	sistem domenskih imen
DoS	denial of service	ohromitev storitve
EBCDIC	extended binary-coded decimal interchange code	8-bitna koda za zapis številk, posebnih znakov in črk
ECE	EC-Council continuation education	nadaljnje izobraževanje, ki ga ponuja EC-Council
EDR	endpoint detection and response	odkrivanje in odziv na končni točki
FTAM	file transfer, access and management	prenos, dostop in upravljanje datotek

FTP	file transfer protocol	protokol za prenos datotek
GDPR	General Data Protection Regulation	Splošna uredba o varstvu podatkov
GIAC	Global Information Assurance Certification	Globalni certifikat informacijske varnosti
GNU	GNU's not Unix	odprtokodni operacijski sistem, podoben Unixu
GPEN	global penetration tester	globalni penetracijski tester
GPS	global positioning system	sistem določanja lokacije z geografsko širino in dolžino
HMAC	hash-based message authentication code	koda za preverjanje pristnosti sporočil na osnovi zgoščevanja
HTML	hypertext markup language	označevalni jezik za oblikovanje večpredstavnostnih dokumentov
HTTP	hypertext transfer protocol	protokol za izmenjavo hiperteksta na spletu
HTTPS	hypertext transfer protocol secure	protokol, ki omogoča varno spletno povezavo
IaaS	infrastructure as a service	infrastruktura kot storitev
ICMP	internet control message protocol	protokol internetnih kontrolnih sporočil
IEEE	Institute of Electrical and Electronics Engineers	svetovno združenje inženirjev elektronike in elektrotehnike
IMSI	international mobile subscriber identity	mednarodna identiteta mobilnega naročnika
IoT	internet of things	internet stvari
IP	internet protocol	internetni protokol
IPSec	internet protocol security	varnostni protokol za zaščito komunikacije

IPv4	internet protocol version 4	internetni protokol, ki uporablja 32-bitne naslove za naslavljanje naprav v omrežju
IPv6	internet protocol version 6	internetni protokol, ki uporablja 128-bitne naslove za naslavljanje naprav v omrežju
LLC	logical link control	nadzor logičnih povezav
LTE	long term evolution	standard nadgradnje omrežja, ki omogoča širokopasovni dostop do 300 Mbit/s
MAC	medium access control	nadzor dostopa do medijev
MDR	managed detection and response	upravljano zaznavanje in odziv
MSSP	managed security service provider	ponudnik upravljanja varnostnih storitev
model OSI	open systems interconnection model	model medsebojnega povezovanja odprtih sistemov
NBF	network basic input/output system frames	osnovni omrežni vhodno-izhodni okviri
NetBIOS	network basic input/output system	osnovni omrežni vhodno-izhodni sistem
NFC	near field communication	komunikacija kratkega dosega
OS	operating system	operacijski sistem
OSCP	the offensive security certified professional	strokovnjak za ofenzivno varnost
PAN	personal area network	osebno omrežje
PaaS	platform as a service	platforma kot storitev
PDCA	plan – do – check – act	načrt – izvedba – preverba – ukrepanje

PE	portable executable	prenosno izvršljiv
PPP	point-to-point protocol	protokol med vozliščema v omrežju
PPTP	point-to-point tunnelling protocol	protokol za vzpostavitev navideznega zasebnega omrežja
RAID	redundant array of independent disks	redundantno diskovno polje
RFID	radio frequency identification	radiofrekvenčna identifikacija
RTP	risk treatment plan	načrt obravnave tveganja
SaaS	software as a service	programska oprema kot storitev
SIEM	security information and event management	sistem za upravljanje varnostnih informacij in dogodkov
SLA	service level agreement	dogovor o ravni storitev
SMS	short message service	sistem za pošiljanje krajših besedilnih sporočil
SNMP	simple network management protocol	preprost protokol za upravljanje omrežja
SoA	statement of applicability	izjava o uporabnosti
SOAR	security orchestration, automation and response	varnostna orkestracija avtomatizacije in odziva
SQL	structured query language	strukturirani povpraševalni jezik za delo s podatkovnimi bazami
SSH	secure shell	varna lupina
SSL	secure socket layer	plast varnih vtičnic
STP	shielded twisted pair	oklopljena sukana parica
SYN	synchronization	sinhronizacija
TCP	transmission control protocol	komunikacijski protokol, ki zagotavlja prenos podatkovnih paketov brez napak

TLS	transport layer security	varnost prenosne ravni
UDP	user datagram protocol	nepovezavni protokol transportne ravni
USB	universal serial bus	vmesnik za povezavo različnih naprav z računalnikom
UTP	unshielded twisted pair	neoklopljena sukana parica
VPN	virtual private network	navidezno zasebno omrežje
WEP	wired equivalent privacy	zasebnost kot v žičnem omrežju
WMI	Windows management instrumentation	infrastruktura za upravljanje podatkov in operacij v operacijskih sistemih Windows
WPA	Wi-Fi protective access	zaščiteni brezžični dostop
WPAN	wireless personal area network	brezžično osebno omrežje

1 Uvod

Podjetjem in državam na spletu pretijo vztrajni in nadarjeni sovražniki. Če želimo obvladovati zlonamerne napade, moramo razumeti njihovo delovanje in poznati postopke, prek katerih lahko uspešno zamejimo ali celo preprečimo škodljivo in uničevalno vedenje. Izdelava dobrega načrta obrambe ni enkraten postopek, ampak se moramo nenehno izpopolnjevati, prilagajati in iskati nove rešitve. Za to potrebujemo znanja z veliko različnih področij, da jih lahko povežemo v celoto. Zagotavljanje informacijske varnosti sestoji iz poznavanja tehničnih podrobnosti (omrežne infrastrukture, naprednega znanja računalništva, sistemske administracije in penetracijskih testiranj, tako imenovanega etičnega hekanja), poznavanja zakonodajnih okvirov, ki vključujejo področno zakonodajo in industrijske certifikate, ter poznavanja standardov in človeške psihologije (zlasti pri napadih s tehniko socialnega inženiringa). Dober etični heker ima širok spekter naštetih znanj (Baloch, 2015). Pri zagotavljanju informacijske varnosti je ključno, da so vsi deležniki zmožni prepoznave kibernetskih[1] groženj. Tudi če se v organizacijah uporabljajo primerni tehnični ukrepi za zagotovitev informacijske varnosti, so šibka točka še vedno uporabniki (Mihelič in Vrhovec, 2017). Podjetja morajo sama poskrbeti za lastno zaščito. Pri tem morajo stalno nadgrajevati varnost informacijsko-komunikacijske tehnologije, podatkovnih baz ter podatkov, informacijske in fizične infrastrukture, sočasno pa morajo skrbeti za odpravo varnostnih ranljivosti (Bernik, Hribar in Ivanuša, 2012). Sledenje kibernetskim storilcem je izredno težko, saj je odstranjevanje sledi v kibernetskem prostoru veliko lažje kot

[1] Kibernetski prostor zajema podatke, računalnike in ljudi, ki so povezani tako, da delujejo drug na drugega (iSlovar, 2019).

v resničnem življenju. Čeprav je kibernetski prostor virtualen, se posledice napadov čutijo v resničnem svetu. Tako bi lahko na primer manjši napad na banko onemogočil delovanje celotnega gospodarstva, škoda pa ima lahko čezmejne posledice (Svete, 2012).

Etično hekanje[2] je širši pojem, ki vključuje vse metode hekanja in kibernetskega napadanja. Cilj etičnega hekanja je identificirati ranljivosti in jih odpraviti, preden bi jih lahko izkoristili storilci kaznivih dejanj. Dejanja etičnih hekerjev lahko primerjamo s početjem osebe, ki vdre v svoj avtomobil, ker je notri pozabila ključe (Omoyiola, 2018). Da lahko etični heker deluje legalno, potrebuje dovoljenje lastnika informacijskega sistema za vdor vanj (Roy, 2019). Najpogostejša vrsta etičnega hekanja je penetracijsko testiranje, ki vključuje identifikacijo varnostnih ranljivosti in tveganj. Pri tovrstnem testiranju tester posnema kibernetskega kriminalca (InfoSec, n. d.). Ob vse pogostejših primerih razkritja osebnih in korporativnih podatkov se po svetu povečuje tudi število etičnih hekerjev (Abel, 2018).

Brenan (2018) ugotavlja, da so uporabniki v Združenih državah Amerike bolj zaskrbljeni, da bi postali žrtve spletne kriminalitete kot pa žrtve nasilnih zločinov (vključno s terorizmom, umori in spolnim nasiljem). Leta 2019 se je po svetu zgodilo več odmevnejših kibernetskih napadov. Kljub poudarjanju pomembnosti izobraževanja uporabnikov še vedno prevladujejo napadi spletnega ribarjenja. Najobsežnejši napadi leta 2019 so bili na sisteme Citrix, na banko Capital One, spletno družbeno omrežje Facebook in zavarovalniško podjetje First American (Flesch, 2019). Leta 2019 so bila napadena večja mesta, vlade, podjetja, bolnišnice in šole po vsem svetu. Januarja 2019 je bil opažen napad z dvema različnima zlonamernima programskima opremama Vidar in Grandcrab, marca pa je bila zaznana izsiljevalska programska oprema LockerGoga, ki je okužila enega največjih svetovnih proizvajalcev aluminija, Norsk Hydro. Škoda je

[2] Hekanje v splošnem pomeni nepooblaščen vdor v računalnik ali omrežje (Techopedia, 2019). Pojem je podrobneje opisan v 6. poglavju.

Recenziji

Informacijska varnost je brez dvoma eno od področij, ki danes vse bolj zaposlujejo varnostne strokovnjake na ravni podjetij, držav in tudi širše mednarodne skupnosti. Že precej časa smo namreč v tako imenovanem informacijskem obdobju, ko informacije in nadzor nad njimi pomenijo enega glavnih virov družbene moči. Monografija *Informacijska varnost: etično hekanje* slovenski znanstveni in strokovni javnosti s celovitim in sistemskim pristopom ponudi vpogled v informacijsko varnost skozi perspektivo etičnega hekanja. Kompleksnega izziva se avtorja lotita pogumno in celovito. Temeljita analiza informacijske varnosti na več področjih – tako v smislu programske in logične plasti kot strojne opreme in telekomunikacij – uspešno utre pot nadaljnji analizi. Glavna teza je usmerjena v preučevanje različnih vidikov etičnega hekanja, med drugim tehničnih možnosti, taktike in prispevka na polju informacijske varnosti. Informacijsko tehnologijo namreč že od vsega začetka močno zaznamuje nekonvencionalno razmišljanje tehničnih *freakov*, ki so pozneje dobili naziv hekerji. V prvi fazi razvoja informacijsko-komunikacijske tehnologije so bili predvsem inovatorji in vizionarji, pozneje so postali *trouble makerji*, na koncu pa celo kriminalci, ki so jih kazensko preganjali organi pregona. Zato je pomembno, da sta avtorja analizirala tudi pravne vidike informacijske varnosti v Sloveniji. Potem ko je iskanje napak in ranljivosti informacijske tehnologije (tako imenovanih *exploitov*) v veliki večini (zahodnih) držav postalo kriminalizirano, se je postavilo temeljno vprašanje: kako tehnologijo sploh preverjati zunaj »laboratorijev« (zaprtih raziskovalnih sistemov)? In tu nastopi etično hekanje, ki ponudi legalen in legitimen način varnostnega preverjanja informacijske tehnologije. Dinamični razvoj tehnologije in naša vse večja odvisnost od nje pred etične hekerje vsekakor

postavljata veliko odgovornost, da bodo s svojim znanjem in vpogledom v »srce« tehnologije njenim najrazličnejšim uporabnikom in tudi laični javnosti ponudili strokovno oporo, ki bo ključna za zaupanje v tehnologijo ter njen nadaljnji in vse bolj samostojni prodor v vse pore našega življenja. Knjigo bodo zato z zanimanjem prebirali tako študenti kot znanstvena in strokovna javnost pa tudi tisti, ki bodo z etičnim hekanjem optimizirali svoje poslovne procese in modele.

izr. prof. dr. Uroš Svete
Fakulteta za družbene vede Univerze v Ljubljani

Ljubljana, marec 2020

* * *

Monografija celovito in na sodoben hibridni način zaobjame problematiko kibernetskih napadov s fokusom na preventivnem delovanju, z identifikacijo ranljivosti tako sistemov kot tudi posameznika. Prav zaznavanje in odpravljanje informacijskih ogrožanj je eden ključnih elementov uspešnega delovanja institucij v družbi. Zato avtorja v knjigi pojasnita, kakšna znanja in sposobnosti mora imeti oseba, ki jo označita za etičnega hekerja, da se zoperstavi tem ogrožanjem in opozori na napake. Pri tem v mozaik varnosti v sodobnem kibernetskem prostoru dodata zelo pomemben kamenček hekanja.

Avtorja s poglobljeno analizo dosedanjih virov presežeta klasične okvire varnostnega mišljenja ter tem znanstvenim dognanjem dodata novo, svojstveno dimenzijo, ki bralca sili k razmišljanju o procesih kibernetske varnosti in globalizacije. Analitično zasnovano delo predstavi temeljna izhodišča za opredelitev pojma informacijska varnost, kar omogoča podlago za izpeljavo definicije etičnega hekanja. To bo v pomoč podjetjem, državnim institucijam in predvsem javnosti, da se bodo podrobneje seznanili s problematiko kibernetske kriminalitete in se zavedeli resnosti problema, ki ga pomeni za sodobno družbo.

Avtorja s kritično distanco opredeljujeta informacijsko varnost in pojav hekanja tudi v njegovi deviantni obliki. Knjiga je prav tako uporabna v praksi, saj po analizi stanja in napak na tem področju poda informacije, na podlagi katerih se bodo lahko načrtovali ukrepi za informacijsko varnost družbe v prihodnje.

Z vsem navedenim avtorja v knjigi vzpostavita kategorialni aparat, ki dejansko prispeva k hitremu razumevanju pojava hekanja. V besedilu se kažeta kritično razmišljanje in argumentiranje, kar prispeva h kakovosti dela s postavitvijo temeljnih pojmov. Avtorja s poglobljeno analizo teorije in prakse presežeta klasične okvire mišljenja in z znanstvenim pristopom dodata nov celovit pristop; ta zajema tudi pojav socialnega inženiringa, ki je na področju informacijske varnosti večkrat zanemarjen. Dodana vrednost dela je tudi poglavje o vlogi izobraževanja etičnih hekerjev. Pri posameznih temah so pojavi jasno in določno dodatno razmejeni z vizualnim gradivom, kar je tudi trend sodobnih monografij v svetu.

Sistemska in analitična zasnova dela predstavlja temeljna izhodišča za spoznanja o hekerstvu na Slovenskem. Tako bo monografija v pomoč podjetjem, državnim institucijam, predvsem pa posameznikom in tudi študentom, da se podrobneje seznanijo s problematiko informacijske varnosti s poudarkom na etičnem hekanju. Uporabnost dela je tudi v tem, da glede na analizo dosedanjega stanja in napak poda definicije, na podlagi katerih se bodo lahko načrtovali ukrepi za spremembe v prihodnje. Pri tem z analizo in določitvijo pojmov pionirsko postavlja temeljno terminologijo za nadaljnje iskanje odgovorov na zastavljena, v prihodnost usmerjena vprašanja.

red. prof. dr. Bojan Dobovšek
Fakulteta za varnostne vede Univerze v Mariboru

Ljubljana, februar 2020

Mnenja o knjigi

Varstva osebnih podatkov ni brez zagotavljanja njihove varnosti, ta pa vključuje tudi redno preverjanje in posodabljanje tehničnih in organizacijskih ukrepov za zagotavljanje varnosti. Etično hekanje zato lahko pripomore, da se organizacije ustrezno pripravijo na tveganja, povezana z informacijsko varnostjo. Potekati pa mora v zakonsko dopustnih okvirih.

***Mojca Prelesnik**, Informacijska pooblaščenka RS*

Etično hekanje v zadnjem času postaja eden najučinkovitejših mehanizmov za doseganje visoke stopnje informacijske varnosti in s tem večje učinkovitosti podjetja. Etični hekerji so zato upravičeno vse pogosteje izpostavljeni kot junaki, ki delajo svet boljši. V Sloveniji imamo že več podjetij in posameznikov, ki se uspešno ukvarjajo s to dejavnostjo. Zelo me veseli, da smo s knjigo Informacijska varnost: Etično hekanje na tem področju dobili tudi nov strokovni prispevek v slovenskem jeziku.

***Lovro Peterlin**, managing direktor, A1 Slovenija*

Kibernetska varnost je sestavni del digitalne preobrazbe, saj si industrijskega interneta stvari danes brez nje ne moremo predstavljati. Odgovornost za kibernetsko varnost pa je treba prevzeti tudi zunaj meja lastne organizacije, zato smo v Siemensu z Listino zaupanja spodbudili vodilna podjetja k zavezanosti k enotnim standardom na področju kibernetske varnosti. Prepričana sem, da bo tudi knjiga, ki je pred vami, pomemben delček v mozaiku varnejšega digitalnega sveta.

***Medeja Lončar**, direktorica, Siemens Slovenija*

Z vidika informacijske varnosti je to strokovno delo svojevrsten mejnik in pomeni precejšen napredek v slovenskem prostoru. Avtorja bralcu s celovitim pristopom tako z vidika zakonodaje kakor metod in veščin etičnega preverjanja ponudita širši vpogled v izzive kibernetske varnosti, vse do ravni etičnega hekanja. Prepletanje analitičnega in praktičnega pristopa v monografiji je tako odlična odskočna deska za vse bodoče etične hekerje, varnostne inženirje, upravljavce informacijskih sistemov in druge, ki dnevno zagotavljajo varnost ter preverjajo skladnost in ranljivost informacijskih sistemov.

***Matjaž Katarinčič**, vodja področja kibernetske varnosti, Smart Com, d. o. o.*

Kriza zaradi epidemije koronavirusne bolezni nas je še dodatno ozavestila, da je v času, ko je delovanje javnih služb, podjetij in posameznika zelo odvisno od informacijske tehnologije, pomen informacijske varnosti ključen. Knjiga poudarja vlogo etičnega hekanja kot metode varovanja kritične infrastrukture, zato ima veliko vrednost.

***Vida Dolenc Pogačnik**, direktorica operative in vodja mednarodnega sodelovanja, koordinatorka Ready4D Future, AmCham Slovenija*

V času, ko se poslovanje vse bolj seli na internet, nujno potrebujemo vsa znanja o informacijski varnosti, zato menim, da bi morala ta knjiga spadati med obvezno branje vsakega podjetnika. Priporočam!

***Bernard Primožič**, direktor, Priber, d. o. o.*

Knjiga celovito in praktično opisuje pomen informacijske varnosti in načine napadov na informacijske sisteme. Avtorja preprosto pojasnita osnovne koncepte informacijske varnosti in obvladovanja tveganj. Zato je knjiga odličen pripomoček za vse, ki se srečujemo z napadi na informacijske sisteme, in obvezno branje za tiste, ki jih moramo preprečevati.

***mag. Miha Ozimek**, specialist za informacijsko varnost, CISA, CISM, ISO/IEC 27001, PCI DSS QSA, ASV*