

INFORMACIJSKA VARNOST: ETIČNO HEKANJE 2.0

Na poti k zagotavljanju
večplastne zaščite

Sara Tomše • Sabina Zgaga Markelj
Blaž Markelj

LEXPERA®

GV
ZALOŽBA

Ljubljana 2023

It is fairly open secret that almost all systems can be hacked, somehow. It is a less spoken of secret that such hacking has actually gone quite mainstream.

Dan Kaminsky

Brainyquote.com, https://www.brainyquote.com/quotes/dan_kaminsky_610453

Kazalo vsebine

1	Uvod	23
2	Oprelitev informacijske varnosti	29
2.1	Referenčni model OSI	31
2.1.1	Fizična plast	32
2.1.2	Povezovalna plast	33
2.1.3	Omrežna plast	34
2.1.4	Transportna plast	34
2.1.5	Sejna plast	35
2.1.6	Predstavitvena plast	36
2.1.7	Aplikacijska plast	36
2.1.8	Primerjava modelov OSI in TCP/IP	37
2.2	Omrežni paketi	38
2.3	Omrežni protokoli	40
2.3.1	Protokoli fizične plasti	41
2.3.2	Protokoli povezovalne plasti	42
2.3.3	Protokoli omrežne plasti	43
2.3.4	Protokoli transportne plasti	45
2.3.5	Protokoli sejne plasti	46
2.3.6	Protokoli predstavitvene plasti	46
2.3.7	Protokoli aplikacijske plasti	47
2.4	Operacijski sistemi	50
2.4.1	Razvoj operacijskih sistemov	52
2.4.2	Microsoft Windows	54
2.4.3	MacOS	55
2.4.4	Android OS	55
2.4.5	Apple iOS	56
2.4.6	Linux OS	56

3	Zagotavljanje informacijske varnosti v sodobnih organizacijah	59
3.1	Model zagotavljanja informacijske varnosti CIA	63
3.1.1	Zaupnost	63
3.1.2	Celovitost	64
3.1.3	Dostopnost	65
3.1.4	Omejitve modela CIA	66
3.2	Obramba v globino	67
3.3	Model ničelnega zaupanja	71
3.4	Uporaba storitev v oblaku	73
3.5	Oddaljeno delo	76
3.6	Mobilna telefonija	80
3.6.1	Tveganja, povezana z mobilno telefonijo	81
3.6.2	Politika »prinesi svojo napravo«	83
3.6.3	Varnost pametnih ur	86
3.6.4	Omrežje 5G	90
3.7	Internet stvari	94
3.7.1	PAN	95
3.7.2	Zigbee	96
3.7.3	Z-Wave	98
3.7.4	Thread	98
3.7.5	Bluetooth	99
3.7.6	Wi-Fi	100
3.7.7	RFID	100
3.7.8	NFC	102
3.8	Upravljanje varnosti programskih vmesnikov	103
3.9	Tehnične rešitve za zagotavljanje kibernetске in informacijske varnosti v sodobnih organizacijah	108
3.9.1	Sistemi za zaznavanje in preprečevanje vdorov, požarne pregrade	108
3.9.2	Sistemi za zagotavljanje zaščite na končnih točkah (protivirusne zaščite, zaznavanje in odziv na končnih točkah, razširjeno zaznavanje in odziv na končnih točkah)	117

3.9.3	Sistemi za upravljanje varnostnih dogodkov in incidentov (SIEM, SOAR)	119
3.9.4	Večfaktorska avtentikacija	123
3.9.5	Sistemi za upravljanje privilegiranega dostopa (PAM)	124
3.9.6	Sistemi za beleženje revizijskih sledi	127
3.9.7	Sistemi za preprečevanje izgube in zaščito podatkov	129
3.9.8	Dobra praksa varnostnega kopiranja (piši enkrat, beri večkrat)	130
3.9.9	Upravljanje varnostnih incidentov	131
3.9.10	Upravljanje sprememb	133
3.9.11	Najem podizvajalcev za upravljanje kibernetske varnosti	134
4	Pravna ureditev področja informacijske varnosti	137
4.1	Pravo Evropske unije	137
4.1.1	Listina Evropske unije o temeljnih pravicah (Listina)	137
4.1.2	Direktiva 2013/40/EU Evropskega parlamenta in Sveta z dne 12. avgusta 2013 o napadih na informacijske sisteme in nadomestitvi Okvirnega sklepa Sveta 2005/222/PNZ	138
4.1.3	Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov)	139
4.1.4	Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2)	141

4.2	Pravo Sveta Evrope	146
4.2.1	Konvencija o varstvu človekovih pravic in temeljnih svoboščin (EKČP)	147
4.2.2	Konvencija o kibernetiski kriminaliteti (Budimpeška konvencija)	147
4.3	Slovenska ureditev	148
4.3.1	Ustava Republike Slovenije	148
4.3.2	Zakon o informacijski varnosti	151
4.3.3	Zakon o elektronskih komunikacijah (ZEKom-2)	152
4.3.4	Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP)	154
4.3.5	Zakon o elektronskem poslovanju na trgu (ZEPT)	154
4.3.6	Zakon o elektronski identifikaciji in storitvah zaupanja (ZEISZ)	156
4.3.7	Zakon o varstvu osebnih podatkov (ZVOP-2)	157
4.3.8	Zakon o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD)	158
4.3.9	Zakon o zaščiti prijaviteljev (ZPri)	159
4.3.10	Kazenski zakonik (KZ-1)	160
4.3.11	Nacionalni načrt odzivanja na kibernetiske incidente	163
4.4	Standardizacija informacijske varnosti	164
4.4.1	Družina standardov ISO/IEC 27000 za upravljanje informacijske varnosti	164
4.4.2	Standard ISO 22301 za upravljanje neprekinjenega poslovanja	165
4.4.3	Standardi ISA-99/IEC 62443 za varnost industrijskih nadzornih sistemov	166
5	Upravljanje tveganj v informacijski varnosti	169
5.1	Upravljanje ranljivosti v kibernetiskem okolju	170
5.2	Upravljanje tveganj in etično hekanje	172

6	Hekanje	177
6.1	Razvoj hekanja	179
6.2	Vrste hekerjev	180
6.3	Najpogostejši napadi na informacijske sisteme	182
7	Etično hekanje	185
7.1	Faze hekanja	189
7.1.1	Izvidništvo	190
7.1.2	Skeniranje	191
7.1.3	Pridobivanje dostopa v sistem	191
7.1.4	Ohranjanje dostopa v sistem	192
7.1.5	Zabrisovanje sledi	192
7.1.6	Poročanje	193
7.2	Penetracijsko testiranje	193
7.3	Socialni inženiring	198
7.3.1	Najpogostejši napadi s socialnim inženiringom ..	199
7.3.2	Vloga končnih uporabnikov pri prepoznavi socialnega inženiringa	200
7.3.3	Vloga organizacij pri obrambi pred napadi socialnega inženiringa	203
7.3.4	Izobraževanje in testiranje zaposlenih o napadih socialnega inženiringa	207
7.3.5	Obramba pred kampanjami spletnega ribarjenja	209
7.3.6	Analiza neželenih e-poštnih sporočil	214
7.3.7	Preiskovanje kampanj spletnega ribarjenja	226
7.4	Vaje z rdečo ekipo	229
7.4.1	Življenjski cikel napada	231
7.4.2	Penetracijsko testiranje in vaje z rdečo ekipo ...	234
7.4.3	Faze napada z rdečo ekipo	235
7.5	Obratni inženiring	236
7.6	Orodja za etično hekanje	239
7.6.1	Kali Linux	239

7.6.2	Ettercap	240
7.6.3	Metasploit	240
7.6.4	Acunetix	240
7.6.5	WireShark.....	241
7.6.6	Nessus	241
7.6.7	Burp Suite.....	241
7.6.8	Invicti.....	242
7.6.9	Aircrack-ng.....	242
7.6.10	Maltego	243
7.7	Pomen etičnega hekanja storitev v oblaku.....	243
7.8	Etično hekanje kot metoda zagotavljanja informacijske varnosti kritične infrastrukture	245
8	Vloga izobraževanja etičnih hekerjev	249
8.1	Primeri dobrih praks učenja etičnega hekanja.....	250
8.1.1	Sledenje aktualnim tehničnim problemom s področja varnosti spletnih aplikacij – OWASP Top 10.....	252
8.1.2	Uporaba aplikacij za učenje etičnega hekanja ...	253
8.2	Certificiranje etičnih hekerjev.....	254
8.2.1	Certificirani etični heker	255
8.2.2	Globalni certifikat za penetracijsko testiranje ...	256
8.2.3	Strokovnjak za ofenzivno varnost	256
9	Izzivi informacijske in kibernetike varnosti v prihodnosti ...	259
	Literatura in pravni viri	263
	Stvarno kazalo.....	299
	O avtorjih	303
	Recenziji	305

1 Uvod

Živimo v obdobju, v katerem se organizacije srečujejo s posebnim fenomenom pri zagotavljanju varovanja informacij. Digitalni odtis organizacij se zelo hitro širi, centraliziran nadzor nad kibernetsko varnostjo pa je zastarel. Večina organizacij je v zadnjih letih uvedla hibridni model dela, posledično so se poslovni procesi digitalizirali. Varovanje podatkov v oblaku je pridobilo nove razsežnosti (Moore, 2022). Kibernetski napadi so vedno bolj izpopolnjeni. Napadalci se sistematično usmerjajo predvsem na notranje uporabnike organizacije (Vrhovec in Mihelič, 2021). Izpopolnili so izsiljevalsko programsko opremo (Moore, 2022), ki je v svetu tako razširjena, da mediji poročajo le še o največjih napadih (Filipkowski, 2023). Razvili so sofisticirane napade na dobavno verigo z izkoriščanjem vgrajenih ranljivosti programske in strojne opreme. Problem dodatno pogloblja pomanjkanje kadrov s področja informacijske in kibernetske varnosti (Moore, 2022). Pomanjkanje varnostnih strokovnjakov deloma nadomeščamo z avtomatizacijo varnostnih procesov (Scarfone, 2022). Avtomatizacija, ki se dosega z uporabo podatkovne analitike velikih količin podatkov, strojnim učenjem in sistemi umetne inteligence, prinaša nove izzive pri zagotavljanju skladnosti s človekovimi pravicami in spoštovanju načel pravne države (Završnik, 2020). Zaradi hitrega tehnološkega razvoja in potrebe po nenehnem komuniciranju je zaščita komunikacijske zasebnosti v vseh vidikih našega življenja postala zelo pomembna (Zgaga, 2015).

Kibernetska kriminaliteta je postala gospodarska dejavnost. Naročniki lahko pri izvedbi kibernetskih napadov uporabljajo znanja več tisoč drugih hekerjev, ki ponujajo svoja znanja v zameno za primerno plačilo. Spletne tržnice na temnem spletu še vedno uspešno deluje-

jo, kljub temu da so organi pregona v zadnjih letih uspešno ukinili kar nekaj velikih tržnic. Zlonamerna programska oprema dobiva nove razsežnosti, saj napadi s pridom izkoriščajo avtomatizacijo. Hekerji že dolgo niso več posamezniki, ki preizkušajo svoje poznavanje omrežij in kodiranja. Pri delovanju zlonamerne programske opreme so dejavnosti avtomatizirane, virtualna programska oprema omogoča več tisoč napadov na dan. Zlonamerna programska oprema vsebuje polimorfne značilnosti (Filipkowski, 2023), kar pomeni, da se programska koda nenehno spreminja in zakriva svojo prepoznavo pred tradicionalnimi protivirusnimi zaščitami, ki delujejo na podlagi prepoznave s pomočjo podpisov. Proizvajalci orodij za zagotavljanje kibernetike razvijajo nova orodja, ki delujejo na podlagi algoritmov strojnega učenja in analize obnašanja programske opreme (Shimony in Tsarfati, 2023; Lord, 2020).

Uporaba umetne inteligence v programski opremi je postala stalnica. Z umetno inteligenco lahko izboljšamo uporabniško izkušnjo, nove funkcionalnosti se razvijajo hitreje, varnost in zasebnost se izboljšujeta z uvedbo novih varnostnih mehanizmov, ki delujejo na podlagi analitike vzorcev obnašanja uporabnikov in druge programske opreme (Pandey, 2022). Razvili so se veliki jezikovni modeli (*large language models* – LLMs), ki so ena najhitreje rastočih aplikacij do zdaj. Pri velikih jezikovnih modelih gre za algoritem, ki je bil izpopolnjen na veliki količini besedilnih podatkov, običajno pridobljenih z interneta. Zajema spletne strani, znanstvene raziskave, knjige in objave na spletnih socialnih medijih. Z analizo razmerja med različnimi besedami ustvarijo verjetnostni model. Nekatera orodja LLM delujejo tako, da imamo občutek, da se pogovarjamo s pravo osebo na drugi strani zaslona. Kljub dovršenosti prinaša uporaba orodij LLM nekatera tveganja, saj lahko predlagajo napačna dejstva, včasih so lahko pristranska in lahkoverna, za delovanje potrebujejo ogromen obseg začetnih podatkov in virov, njihova uporaba pa mnogokrat ni zgolj legitimna (David in Paul, 2023). V začetku leta 2023 je bilo ugotovljeno, da lahko kibernetiki napadalci uporabljajo orodja LLM

za ustvarjanje zlonamerne programske opreme v različnih programskih jezikih (Rees, 2023). Pojavljajo se tudi primeri, ko se uporabljajo orodja LLM za »izboljšanje« programske kode že aktivne zlonamerne programske opreme. To pomeni nova tveganja, saj se bo zaradi širitve kroga razvijalcev zlonamerne programske opreme izboljšala stroškovna učinkovitost napadalcev, grožnje pa bodo še bolj sofisticirane (Zacharakos, 2023).

Uporaba »zlonamerne programske opreme kot storitve« (*Malware-as-a-service*) narašča. To je vrsta storitve, ki vsakomur, neodvisno od tehničnega znanja in izkušenj, omogoča izvedbo kibernetških napadov z dostopom do vnaprej pripravljene zlonamerne programske opreme. Koncept zlonamerne programske opreme kot storitve je podoben legitimnemu konceptu, ko stranke plačujejo za dostop do programske opreme prek interneta. Obstajajo naročniški modeli in modeli enkratnega plačila za uporabo. Takšen koncept je pri razvoju kibernetške kriminalitete ključen, saj omogoča izvedbo napadov naročnikom, ki sami nimajo dovolj tehničnega znanja. Zlonamerna programska oprema, ki se prodaja naročnikom, je pogosto zasnovana tako, da se izogne odkrivanju s tradicionalnimi varnostnimi ukrepi (Prakash, 2023). S takšnim poslovnim modelom se pogosto ponujajo storitve izsiljevalske programske opreme. To je vrsta zlonamerne programske opreme, ki šifrira žrtvine datoteke in mape. Po izvedbi šifriranja ponujajo napadalci ključ v zameno za plačilo odkupnine (Goodchild, 2023). Drugi tip zlonamerne programske opreme, ki se pogosto pojavlja kot storitev, so kradljivci podatkov. Ti delujejo tako, da po okužbi končne naprave zbirajo podatke in jih pošiljajo napadalcu. V večini primerov so tarča podatki iz brskalnika (poverilnice in piškotki). Najpogosteje se okužimo z odpiranjem priponk, ki jih prejmemo po spletni pošti (Conrad, 2022). Poleg omenjenih napadov lahko zakupimo tudi kampanje lažnih e-poštnih sporočil (phishing), napade porazdeljene ohromitve storitev (DDoS), bančno trojansko opremo, računalniške črve, oglaševalsko programsko opremo (adware), OSINT-analize potencialnih žrtev in ciljno usmerjene napade (Mladenovska, 2023).

V zadnjem času lahko pogosto opazamo napade na dobavno verigo, pri čemer so tarča razvijalci in dobavitelji programske opreme. Napadalci skušajo dostopati do izvorne kode, postopkov izdelave programske opreme ali mehanizmov posodobljanja, kamor vrinejo zlonamerno kodo, ki se širi s prenosi in rednimi posodobitvami legitimne programske opreme. Takšne napade izvršujejo z izkoriščanjem nezavarovanih omrežnih protokolov, nezaščitene strežniške infrastrukture in slabe prakse programiranja. Ker je programska oprema izdelana s strani zaupanja vrednih prodajalcev, so aplikacije in njihove posodobitve podpisane in certificirane. Pri napadih na dobavno verigo se prodajalci ne zavedajo, da je njihova oprema okužena z zlonamerno kodo (Microsoft, 2023).

Tradicionalno se je kibernetska varnost zagotavlja z varovanjem posameznih računalnikov in omrežij, ki so bili umeščeni za požarno pregrado. Z razvojem aplikacij in migracijo v uporabo oblačnih storitev so se spremenile tudi grožnje. Pomembno grožnjo v svetu pomenijo programski vmesniki (*application programming interface* – API), ki določajo vrsto interakcij med aplikacijami in raven varnosti, ki je potrebna za interakcijo. Uporaba programskih vmesnikov narašča, posledično narašča tudi število povezanih kršitev. Če programski vmesniki niso jasno zabeleženi in zavarovani, predstavljajo ogromno površino za izvedbo napadov. Napadalci lahko z izkoriščanjem ranljivosti programskih vmesnikov pridobijo nepooblaščen dostop do osebnih podatkov strank, poslovnih skrivnosti in drugih občutljivih podatkov, ki jih lahko prodajajo na temnem spletu ali za nerazkritje zahtevajo odkupnino (McCormick, 2023). Zaradi neustrezne zaščite programskih vmesnikov smo lahko v zadnjem času opazili napade na večja podjetja, kot so Paypal, T-Mobile, Amazon Web Services (AWS), Automobile Giants, Azure, Yahoo, LinkedIn, Facebook in še nekatera druga (Isbitski, 2021; Ilany, 2022; Tripwire, 2022).

Pri zagotavljanju kibernetske varnosti ostaja človeški dejavnik še vedno stalnica. Še vedno se srečujemo z napačno konfiguracijo

omrežja in prehitrimi »kliki« na zlonamerne povezave. Ljudje bodo v tehnologiji vedno prisotni, ne glede na to, ali jo bodo razvijali, konfigurirali ali uporabljali. Zato bodo vedno prisotne napake. Izvedba izobraževanj, usposabljanj, izmenjava informacij in ozaveščenost so ključni za zmanjševanje verjetnosti, da bo človeška napaka usodna in bo pustila resne posledice (Filipkowski, 2023). Tudi na drugih področjih, povezanih z varnostjo, Furman, Meško in Sotlar (2012) ugotavljajo, da je v Evropski uniji razvoj v zadnjih dvajsetih letih šel v smer izmenjave informacij in medsebojnega sodelovanja. Informacijska (in kibernetika) varnost temeljita na treh ključnih stebrih: tehnologija, procesi in ljudje. Pri ljudeh je ključno, da poleg gradnje strokovnih kompetenc zagotavljamo stalna izobraževanja in programe ozaveščanja s področja kibernetike varnosti (Del Conte, 2022). Motivacija za samozaščito končnih uporabnikov ima pomembno vlogo pri zagotavljanju kibernetike varnosti v organizacijah (Vrhovec in Mihelič, 2021).

Socialni inženiring je še vedno ena najpomembnejših vstopnih točk napadalcev v informacijski sistem organizacij (SI-CERT, 2022). Lastnost socialnega inženiringa je manipulacija s človeškimi čustvi, kot sta radovednost in strah (Bolland, n. d.). V literaturi je mogoče najti različne metode učenja in ozaveščanja uporabnikov o pomenu socialnega inženiringa za zagotavljanje kibernetike in informacijske varnosti. Vrhovec, Bernik in Markelj (2023) ugotavljajo, da je učinkovito, če v gradivo za ozaveščanje vključujemo komponento strahu, saj obstaja večja možnost, da bodo uporabniki sami iskali več podatkov o napadih socialnega inženiringa.

Pred vami je nova knjiga *Informacijska varnost: Etično hekanje 2.0*, ki obravnava izzive s področja zagotavljanja informacijske varnosti. Etično hekanje se še naprej izkazuje kot izredno učinkovita metoda pri zagotavljanju večplastne zaščite v organizacijah. V novi knjigi vpeljujemo nekatere pomembne tehnične in organizacijske okvire, ki temeljijo na najnovejših grožnjah in razvoju tehnologije.

Predstavljamo izzive in možnosti zagotavljanja informacijske varnosti v organizacijah z uporabo najsodobnejših metod in dobrih praks. Tehnične in organizacijske rešitve dopolnujemo s poglavjem, namenjenim pravni ureditvi informacijske varnosti, ki je pomemben temelj vsem preostalim ukrepom – vse skupaj z namenom, da bralce popeljemo skozi dobre prakse pri zagotavljanju večplastne zaščite, pri čemer je etično hekanje zgolj ena, a zelo pomembna plast.