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

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 poglablja 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 kibernetske zaščite 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 kibernetski 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 kibernetskih 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 kibernetske 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 opažamo 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 posodabljanja, 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 kibernetska) 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 kibernetske varnosti (Del Conte, 2022). Motivacija za samozaščito končnih uporabnikov ima pomembno vlogo pri zagotavljanju kibernetske 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 kibernetske 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 dopolnjujemo 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.