INFORMACIJSKA IN RAČUNALNIŠKA PISMENOST

NENA OREL ŠANKO
Univerza v Mariboru, Fakulteta za logistiko, Celje, Slovenija
nena.orel@um.si

V današnjem času je varnost informacij in računalnikov izjemno pomembna iz več razlogov. Digitalizacija je omogočila ogromen pretok podatkov in informacij preko računalniških omrežij. Te informacije so pogosto občutljive narave, vključno s finančnimi podatki, osebnimi identifikacijami in poslovnimi skrivnostmi. Zato je nujno, da se informacije zaščitijo pred nepooblaščenim dostopom in zlorabo. V digitalnem svetu je veliko infrastrukture povezane z računalniškimi omrežji, to so šole, bolnišnice in prometni sistemi. Napadi na te sisteme lahko povzročijo resno finančno ali materialno škodo in ogrozijo življenja ljudi. Zato je pomembno zagotoviti, da so sistemi varni in odporni proti kibernetskim napadom. Kibernetski napadi so postali vse bolj pogosti, sofisticirani ter izkoriščajo ranljivosti v računalniških sistemih in omrežjih za krajo podatkov, vohunjenje ter povzročanje škode. Zato je nujno nenehno nadgrajevanje varnostnih ukrepov in seznanjenost ljudi. Torej, varnost informacij in računalnikov je ključnega pomena za zaščito zasebnosti, gospodarske stabilnosti in nacionalne varnosti v sodobnem digitalnem svetu.

DOI
https://doi.org/10.18690/um.fl.2.2025.3

ISBN
978-961-286-971-7

Ključne besede:
informacijska varnost,
računalniška varnost,
podatki,
informacije

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.fl.2.2025.3

ISBN
978-961-286-971-7

Keywords:
information security,
computer security,
data,
information

INFORMATION AND COMPUTER LITERACY

NENA OREL ŠANKO
University of Maribor, Faculty of Logistics, Celje, Slovenia
nena.orel@um.si

Today, information and computer security are extremely important for several reasons. Digitalisation has enabled a massive flow of data and information through computer networks, where information is often sensitive in nature, including financial data, personal identities, and business secrets. It is imperative to protect information from unauthorised access and misuse. In today's digital world, a lot of infrastructure is connected to computer networks, such as schools, hospitals, and transportation systems. Attacks on these systems can lead to significant financial or material damage and jeopardise people's lives. Hence, it is crucial to ensure systems' security and resiliency against cyber-attacks, which have become increasingly common, sophisticated, and exploit vulnerabilities to steal data, spy, and cause harm. Thus, constant upgrading of security measures and raising awareness among people are essential. Therefore, information and computer security are of paramount importance for safeguarding privacy, economic stability, and national security in the modern digital world.

University of Maribor Press

1 Uvod

Informacijska in računalniška varnost sta postali temeljna vprašanji v današnji digitalni dobi, kjer so podatki in informacije postali dragoceni viri, ki poganjajo tako zasebna kot poslovna okolja. S hitrim razvojem tehnologije in nenehnim povezovanjem preko interneta je varovanje podatkov postalo ključnega pomena, saj so se pojavile nove grožnje, ki ogrožajo tako posameznike kot organizacije. Varnostne kršitve, kot so: kraje identitete, hekerski napadi in izguba občutljivih informacij, predstavljajo resne posledice, ki lahko povzročijo nepopravljivo škodo tako na osebnem kot poslovnem nivoju. Zato je zaščita informacij in podatkov danes ključna naloga, ki varuje našo zasebnost, finančno stabilnost in poslovno konkurenčnost.

Na začetku pa je potrebno zavedanje, da sta obstoj in poslovanje vsake organizacije odvisna od virov informacijske tehnologije (v nadaljevanju: IT), brez katerih logistični procesi ter sistemi oskrbovalnih verig ne morejo (nemoteno) delovati (Jereb, 2017). Sem sodijo (Kajba et al., 2023): informacije, aplikacije (ali programska oprema), infrastruktura, neopredmetena sredstva in ljudje. IT viri so na voljo za implementacijo v različne IT procese (Jereb, 2017), razumemo pa jih lahko kot naložbe v te procese, kjer je pomembna tudi njihova primerna raven zaščite (Jereb et al., 2016). Trdimo lahko tudi, da so ti štirje IT viri temelj vsake tehnologije, kjer predstavljajo štiri soodvisne, soodločajoče ter enako pomembne komponente (Kabanda, 2019).

Za vsakega izmed IT virov pa je potrebno zagotavljati tudi IT zahteve, ki so že bile omenjene v poglavju Načrtovanje digitalizacije poslovanja. Glede na kontrolne cilje za informacijsko in sorodno tehnologijo (angl. Control Objectives for Information and related Technology) obstaja sedem poslovnih zahtev oziroma informacijskih kriterijev za IT vire (IT Governance Institute, 2007):

- uspešnost – se nanaša na informacije, pomembne za poslovni proces, ki so del tega poslovnega procesa ter njihovo pravočasno zagotovitev, pravilnost, skladnost in uporabnost,
- učinkovitost – se nanaša na zagotavljanje informacij z optimalno uporabo virov,

- zaupnost – se nanaša na varovanje občutljivih informacij pred razkritjem,
- celovitost – se nanaša na pravilnost in popolnost informacij, njihovo veljavnost v skladu s poslovno vrednostjo ter pričakovanji,
- razpoložljivost – se nanaša na informacije, ki morajo biti na razpolago, ko jih potrebujemo v poslovnih procesih, in varovanje potrebnih virov ter sorodnih zmogljivosti,
- skladnost – obravnava uskladitev z zakoni, predpisi in pogodbenimi dogovori (zunanja določena poslovna merila, notranje politike), ki veljajo za zadevni poslovni proces,
- zanesljivost – se nanaša na zagotavljanje ustreznih informacij za vodstvo, da lahko upravlja organizacijo in izvaja svoje odgovornosti iz naslova zaupnosti in vodenja.

Slika 3.1: Trikotnik CIA
Vir: lasten

Informatika, z vidika varnosti, zahteva predvsem, da so informacije na voljo, celovite in zaupne v obsegu, ki je potreben za izvedbo ter podporo poslovnim procesom. V primeru logistike to pomeni zagotavljanje *razpoložljivosti*, *celovitosti* in *zaupnosti* informacij, da je mogoče zagotoviti prave izdelke ali storitve v pravilni količini in kakovosti, dostavljene na pravo mesto in ob pravem času. (Kajba & Jereb, 2021) Te tri zahteve (razpoložljivost, celovitost in zaupnost) pa predstavljajo tudi trikotnik

CIA (angl. The CIA Triad: Confidentiality, Integrity and Availability) (Slika 1), kjer (Kemmerer, 2003):

- zaupnost zagotavlja, da se občutljive informacije ne razkrijejo nepooblaščenim prejemnikom,
- celovitost zagotavlja, da so podatki in programi spremenjeni ali uničeni samo na določen ter pooblaščen način,
- razpoložljivost zagotavlja, da bodo IT viri uporabni, kadarkoli jih potrebuje pooblaščeni uporabnik.

2 Vrste varnosti in groženj, povezane z delovanjem IT

V poglavju Načrtovanje digitalizacije poslovanja je bila orisana splošna pomembnost informacijske in kibernetske varnosti z opisom ključnih elementov kibernetske varnosti ter proaktivnimi in celovitimi pristopi. V nadaljevanju sledi podroben opis vrst varnosti ter IT groženj.

2.1 Vrste varnosti, povezane z delovanjem IT

Potrebno je predstaviti vrste varnosti, povezane z delovanjem IT: informacijska varnost, IT varnost, kibernetska varnost, računalniška varnost in omrežna varnost.

Informacijska varnost (angl. Information Security, InfoSec) zajema orodja in postopke, ki jih organizacije uporabljajo za zaščito informacij ter preprečevanje nepooblaščenega dostopa do poslovnih ali osebnih informacij, vključno z nastavitvami pravilnika, ki nepooblaščenim ljudem preprečuje dostop do poslovnih ali osebnih podatkov. InfoSec je rastoče in razvijajoče se področje, ki zajema mnoge vidike; od preizkušanja, testiranja in revizije varnosti omrežja do infrastrukture. Ščiti občutljive podatke pred nepooblaščenimi dejavnostmi, vključno s pregledovanjem, spreminjanjem, snemanjem in kakršnokoli motnjo ali uničenjem. Glavni cilj je zagotoviti varnost in zasebnost kritičnih podatkov organizacij, kot so: podrobnosti o računih strank, finančnih podatkih ali intelektualni lastnini. Organizacije morajo dodeliti sredstva za zagotavljanje varnosti informacij in podatkov ter biti pripravljene na odkrivanje, odzivanje in proaktivno preprečevanje napadov, kot so: lažno predstavljanje, zlonamerna programska oprema, virusi, zlonamerni insajderji ter izsiljevalska programska oprema ('Information Security: The Ultimate Guide', n.d.).

IT varnost (angl. Information Technology Security, IT security) opisuje previdnostne ukrepe za zaščito računalnikov in omrežij pred nepooblaščenim dostopom. Postopki in procesi so zasnovani za preprečevanje kraje podatkov ali motenj v informacijskih sistemih. Visoka kakovost IT varnosti se osredotoča na varovanje celovitosti podatkov, ohranjanje zaupnosti informacij, shranjenih v omrežju, zagotavljanje dostopnosti podatkov in informacij pooblaščenemu osebju, preverjanje pristnosti uporabnikov, ki poskušajo dostopati do računalniških omrežij ter omogočanje varnega pošiljanja sporočil preko omrežij za uporabnike (The Upwork Team, 2021).

Medtem ko se tako IT varnost kot kibernetska varnost (angl. Cyber Security) osredotočata na zaščito podatkov o strankah, imata nekoliko drugačna pristopa. IT varnost se nanaša na širše razumevanje zaščite, raziskovanje korakov za zaščito poslovnih podatkov, vključno s fizičnimi podatki in informacijami v internih sistemih. Kibernetska varnost se bolj osredotoča na grožnje, s katerimi se organizacija lahko sreča preko interneta, ko se informacije in podatki prenašajo digitalno ali drugače uporabljajo na spletu (The Upwork Team, 2021). Kibernetska varnost zajema nabor orodij, politik, varnostnih konceptov, varnostnih ukrepov, smernic, pristopov k obvladovanju tveganj, dejanj, usposabljanja, najboljših praks, zagotovil ter tehnologij, ki se lahko uporabijo za zaščito kibernetskega okolja ter sredstev organizacije in uporabnikov (Von Solms & Van Niekerk, 2013).

Računalniška varnost se na splošno osredotoča na zaščito računalniških sistemov pred nepooblaščenim dostopom in uporabo. Strokovnjaki za računalniško varnost si prizadevajo vzpostaviti najboljše prakse računalniške varnosti, kar vključuje upravljanje računalniške varnosti in varnosti omrežja ter ustvarjanje kulture, osredotočene na varnost v organizaciji. Obstaja več različnih vrst računalniške varnosti, ki vplivajo na različne elemente fizične in digitalne infrastrukture organizacije. Posledično obstaja veliko različnih vrst varnosti, na katere se morajo osredotočiti strokovnjaki, vključno z (The Upwork Team, 2021; 'What Is Computer Security?', 2022):

- varnost aplikacij – opisuje korake, ki jih izvajajo razvijalci pri izdelavi aplikacije, da zagotovijo varnost uporabnikov in zmanjšajo ranljivosti v aplikaciji (pri tej vrsti varnosti je potrebno analizirati kodo aplikacije, da bi našli morebitne slabosti),

- informacijska varnost,
- varnost omrežja – ščiti digitalno infrastrukturo organizacije in preprečuje varnostne incidente v računalniških omrežjih, tako da lahko uporabniki nemoteno delajo,
- internetna varnost – ščiti brskalnike in informacije v aplikacijah, ki uporabljajo internet. Požarni zidovi in podobne vrste zaščite, ki samo pooblaščenim uporabnikom zagotavljajo dostop do zaščitenih območij, veljajo za internetne varnostne storitve,
- varnost v oblaku – zagotavlja, da uporabniki, ki se povezujejo preko aplikacij v oblaku, ostanejo zaščiteni ter uporablja sisteme, kot je poenoteno upravljanje groženj (UTM) v oblaku, da ohranja varne povezave v oblaku,
- operativna varnost – opisuje prakse in analize, ki se uporabljajo pri rutinskih dejanjih za iskanje potencialnih ranljivosti, ki jih lahko hekerji izkoristijo. Cilj je videti redne akcije z vidika slabega akterja in ugotoviti, kje lahko izkoristijo prednost,
- varnost končne točke – s številom naprav, ki se uporabljajo v organizaciji (mobilni telefoni, tablice, prenosniki in računalniki), se varnost končnih točk osredotoča na zaščito teh sistemskih končnih točk in vključuje zaščito naprav pred okužbo z zlonamerno programsko opremo.

Vsaka od teh vrst računalniške varnosti vključuje več komponent, zaradi česar jih je mogoče obravnavati kot lastna specializirana področja. ('What Is Computer Security?', 2022) Prej omenjeni trikotnik CIA velja za industrijski standard računalniške varnosti že od razvoja glavnega centralnega procesorskega kompleksa[1] (Whitman & Mattord, 2011).

Razumevanje razlike med IT varnostjo in varnostjo omrežja (angl. Network Security) se osredotoča na razumevanje različne uporabe podatkov. IT varnost se osredotoča na vse podatke, s katerimi upravlja organizacija, medtem ko se varnost omrežja osredotoča na omrežne sisteme in njihovo zaščito pred vdori ter napadi na podatke. Ponudniki varnostnih storitev pogosto ščitijo infrastrukturo, ki organizacijam omogoča elektronsko sodelovanje. (The Upwork Team, 2021)

[1] Glavni centralni procesorski kompleks (angl. mainframe) - v svojem bistvu so »mainfram-i« visoko zmogljivi računalniki z veliko količino pomnilnika in podatkovnimi procesorji, ki obdelujejo milijarde preprostih izračunov ter transakcij v realnem času (IBM, n.d.).

2.2 Vrste IT groženj

Preden nadaljujemo z vrstami vdorov, je potrebno omeniti vrste groženj IT varnosti (The Upwork Team, 2021):

- kibernetski kriminal – vključuje usmerjanje ali uporabo računalnikov ali računalniških sistemov za storitve kaznivih dejanj (kraja identitete ali izsiljevanje) za določeno vrsto finančne nagrade,
- kibernetski napadi – obsežni digitalni napadi, ki lahko onesposobijo celoten računalniški sistem ali več računalniških sistemov (napadi lahko uporabljajo zlonamerno programsko opremo ali izsiljevalsko programsko opremo), da dosežejo cilj pridobivanja informacij o milijonih uporabnikov ali izvedejo napad z zavrnitvijo storitve (DoS),
- kibernetski terorizem – uporablja orodja ter metode kibernetskega kriminala in napadov, s čimer poskuša ciljati na kritično infrastrukturo držav ali drugače škodovati državam in povzročiti strah z nepooblaščenim dostopom do komunikacijske infrastrukture.

3 Zlonamerna programska oprema

Pogost izraz za zlonamerno programsko opremo je tudi zlonamerna koda ali »malware«. Vsako leto je poslovanje preplavljeno z napadi zlonamerne programske opreme, ki jih povzročajo vedno večje komunikacijske zmogljivosti računalnikov in telefonov. Značilnost vseh oblik zlonamerne programske opreme je, da je njihov obstoj nezaželen, neznan ali sovražen do napadenega uporabnika, ki prejme te programe. Še pred dvajsetimi leti se je zlonamerna koda širila izključno z disketami, ki so jih uporabniki prenašali iz računalnika v računalnik. S povečanjem komunikacijskih zmožnosti se je povečala tudi razširjenost zlonamerne kode. Danes se škodljivci radi širijo preko datotek, e-pošte, sistemov za takojšnje sporočanje in spletnih mest. (Šepec, 2018)

Zlonamerna programska oprema izkorišča varnostne pomanjkljivosti v operacijskih sistemih in aplikacijah za širjenje okužb. Uspešen prodor zlonamernih kod je posledica neustreznosti tradicionalnih obrambnih orodij, katerih način delovanja je predvsem reaktiven. Protivirusni in protivohunski programi so najuspešnejši v boju

proti znanim napadom. Ko se na spletu pojavi nova vrsta zlonamerne programske opreme, se lahko neovirano širi, dokler proizvajalci protivirusnih programov ne analizirajo napada in ustvarijo primernega »cepiva«. Pravilno konfigurirani požarni zidovi bi lahko odigrali bistveno vlogo v tem boju, vendar večina uporabnikov sploh ne ve, kaj je požarni zid.

3.1 Vrste zlonamerne programske opreme

Škodljive kode (angl. malicious software ali malware) se pojavljajo kot pomožno ali glavno sredstvo izvršitve pri številnih kaznivih dejanjih kibernetskega kriminala in so opredeljene kot škodljivi programi, posebej prirejeni za napade (škodenju) na informacijske sisteme, omrežja ali podatke. (Šepec, 2018) V današnji informacijski dobi, v kateri je možnost profiliranja posameznikov nekaj povsem običajnega in so posegi v informacijsko zasebnost posameznikov dosegli najvišjo raven v zgodovini, so vohunski programi vse prej kot nedolžni skupki kod. Škodljive kode, ki prevladujejo pri kaznivih dejanjih, preko katerih se vršijo različni načini, imajo za posledice različna motenja, poškodovanje in resno oviranje informacijskih sistemov ter e-podatkov. Značilno za vse oblike programov malware je, da je njihov obstoj nezaželen, nepoznan ali sovražen napadenemu uporabniku, ki te programe prejme (Šepec, 2018).

Ko kibernetski kriminalci načrtujejo napad na računalniška omrežja in sisteme, imajo na voljo različna orodja. Obstaja več načinov zlonamernih napadov, na katere morajo biti organizacije pozorne, ko razvijajo svoje strategije kibernetske varnosti in varnosti IT. Nekatere izmed vrst zlonamerne programske opreme bodo predstavljene v nadaljevanju; virusi, črvi, trojanski konj, vohunska programska oprema, oglaševalska programska oprema, izsiljevalska programska oprema in (distribuirana) zavrnitev storitve.

3.1.1 Virusi

Beseda VIRUS pomeni »Vitalni informacijski vir pod obleganjem« (angl. »Vital Information Resource under Siege«) (Maity & Dey, 2021). Vse vrste zlonamerne programske opreme se pogosto obravnavajo kot virusi, vendar so virusi le ena izmed oblik zlonamerne programske opreme, niso pa vse vrste virusi. Virus je računalniški

program, ki je bil sprva napisan za zabavo, danes pa povzroča predvsem neprecenljivo škodo informacijskim sistemom.

Izraz virus se v računalniškem žargonu uporablja po zgledu samopodvajajočih se bioloških virusov – virus je program ali koda, ki se samodejno razširi na druge datoteke, s katerimi pride v stik in izvaja zlonamerna opravila, kot je prikaz preprostih sporočilnih oken ali uničenje podatkov. Virus lahko opišemo kot program, ki okuži različne medije in spremeni delovanje računalnika ali omrežja (Šepec, 2018). Ali kot samorazmnoževalni program, ki lahko "okuži" druge programe tako, da spremeni njih ali njihovo okolje tako, da klic "okuženega" programa pomeni klic morda razvite ter v večini primerov funkcionalno podobne kopije virusa (Horton & Seberry, 1997).

Da se virusi aktivirajo in razširijo, je potrebna pomoč uporabnika, kar se zgodi ob klikanju na določeno datoteko, zagonu določenega programa ali klikanju na povezavo. Ko je okužena datoteka odprta, se virus razširi in lahko okuži druge programe, zagonski sektor trdega diska, njegovo particijo ali dokument. Ko je enkrat aktiviran, se prične širiti tudi na druge datoteke ali preko drugih komunikacijskih kanalov. Računalniški sistem se lahko okuži celo, če okuženega programa ne zaženemo, saj se nekateri virusi širijo že med kopiranjem. Virusi ne morejo okužiti računalnika, če gledamo le spletne strani – okužba se zgodi le, če dovolimo izvajanje spletnih programov. Dobro je vedeti, da virusi niso prisotni le v ukradenih ali razpokanih programih; zaradi nepazljivosti se lahko pojavijo tudi v legalnih programih. Zaradi programskih napak se nekateri virusi širijo tudi preko elektronske pošte brez prilog. (Šepec, 2018)

Virusi se na okuženem računalniku običajno nastanijo v posameznih izvršljivih programih, kar poveča velikost programa. Vsebina zaslona okuženega računalnika se nenadoma začne spreminjati, posamezni deli zaslona se lahko premikajo, pojavijo pa se tudi različne slike ali napisi, kot na primer: "Vaš računalnik je zdaj okužen." Okuženi računalnik lahko zahteva različna gesla in šifre ali kako drugače spremeni tipične ukaze, poslane preko tipkovnice ali miške. Prav tako je delovanje računalnika upočasnjeno (to ne pomeni, da je vsak počasen računalnik tudi okužen z virusom). Večina virusov je zasnovanih za uničenje računalnika ali podatkov. (Šepec, 2018)

Vsak virus ima sledeče komponente (Šepec, 2018):

- okužba: programski del, ki omogoča širjenje virusa,
- koristni tovor (angl. Payload): predstavlja glavno aktivnost virusa in je zasnovan za izvajanje posebnih funkcij, kot so brisanje, spreminjanje ter konfiguracija podatkov in namestitev programske opreme za oddaljeni dostop,
- prožilna funkcija: definira čas ali dogodek in izvede podporno komponento programa.

3.1.2 Črvi

Virusi se razlikujejo od črvov (angl. worms), saj njihov zagon zahteva aktivnost prejemnika v obliki izvajanja programa; uporabnik mora sam izvesti datoteko virusa (odpreti priponko v elektronski pošti, klikniti z miško na izvršljivo datoteko). Črvi izkoriščajo pomanjkljivosti v operacijskih sistemih (na primer: Windows in Linux) ter ne zahtevajo nobene aktivnosti s strani žrtve. (Šepec, 2018)

Tako je črv neodvisen program, ki lahko širi svoje kopije ali svoje dele na druge računalnike, običajno preko omrežnih povezav, te kopije pa so popolnoma funkcionalni neodvisni programi, ki se lahko bodisi širijo naprej in/ali komunicirajo z nadrejenim črvom (na primer za poročanje o rezultatih nekega izračuna) (Horton & Seberry, 1997). Pogosto napadejo pomembne sisteme in spletne strani. V primeru črvov je najopaznejša posledica povečan promet v omrežju.

Podobno kot virusi so tudi črvi samorepliciraječi programi, ki se največkrat nenadzorovano širijo po računalniškem sistemu, internetu in drugih omrežjih (Šepec, 2018). Vendar so v primerjavi z virusi nekoliko bolj inteligentni, saj so sposobni samodejno najti primerne tarče za okužbo, širijo pa se brez pomoči uporabnika, saj uporabljajo napake v operacijskih sistemih in programih (Bhargava et al., 2022). Običajno so zelo uspešni pri širjenju, saj računalniški uporabniki ne nameščajo potrebnih varnostnih sistemov. Podobno kot virusi, črvi nosijo "tovor" (payload), ki jim omogoča nadzor nad okuženim računalnikom, brisanje datotek ali krajo osebnih informacij in podatkov. Leta 2004 je črv po imenu Blaster v samo petih urah okužil več kot 100.000 računalnikov. Drug črv, imenovan Mydoom, je

morda najhujši zlonamerni program v zgodovini, saj je leta 2004 povzročil več kot 38 milijard dolarjev škode (Paulo, 2022).

3.1.3 Trojanski konj

Trojanski konj nima možnosti samorepliciranja. Značilnost trojanskih konjev je, da pogosto vsebujejo neko nedolžno funkcijo (na primer prikaz ure in vremena na namizju računalniškega sistema) (Šepec, 2018), predstavljajoč majhen in škodljiv del nekega prvotnega, splošno uporabnega programa. Trojanski konj je za razliko od računalniškega virusa (ki se prilepi na drug program s katerokoli od številnih metod) samostojen program in ima lahko uporabniške funkcije za uporabnika. (Horton & Seberry, 1997)

Trojanski konj se lahko zlahka predstavi kot navidezno nedolžna datoteka, prenesena s spleta kot Word ali PDF dokument, priložen elektronski pošti (Bhargava et al., 2022). Ko je ta generični program nameščen, se z njim namesti tudi trojanski konj, kar omogoča napadalcu prevzem nad računalnikom. Čeprav se ta vrsta zlonamerne programske opreme ne razmnožuje, lahko izvaja številne škodljive dejavnosti. Za primarnim programom se skrivajo t. i. "zasilna vrata" (angl. trap door), ki omogočajo avtorju trojanskega konja, da izvede določeno funkcijo (dostop do informacijskega sistema uporabnika, pridobivanje datotek iz sistema ali namestitev škodljivih kod v sistem). Delujejo podobno kot virusi, saj zahtevajo neko predhodno aktivnost žrtve v obliki zagona izvršljive datoteke, obiska spletne strani ali odpiranja navidezno nedolžne datoteke, ki vsebuje kodo trojanskega konja. Glavni namen trojanskih konjev je ustvarjanje in kraja identitet v povezavi z dosego finančnega dobička. (Šepec, 2018)

3.1.4 Vohunska, oglaševalska in izsiljevalska programska oprema

Vohunski programi (angl. spyware) in oglasi (angl. adware) predstavljajo veliko nadlogo v računalniškem svetu. Obe sta vrsti zlonamerne programske opreme in se razlikujeta od virusov in črvov v tem, da se ne moreta širiti z enega računalniškega sistema na drugega.

Vohunski program je splošen izraz za različne vrste zlonamerne programske opreme, ki na določen način nadzira delovanje informacijskih sistemov ter zbira osebne podatke (Šepec, 2018). Je sklop kode, ki je nameščen v računalniškem sistemu in deluje kot vohun, se osredotoča na dejavnosti lastnika sistema ter zbira vse informacije, do katerih dostopa neavtorizirano (Maity & Dey, 2021). Vohunska programska oprema se namesti na računalnik med brskanjem po internetu, za okužbo računalnika pa izkorišča varnostne pomanjkljivosti v spletnem brskalniku. Zasede lahko različne oblike, od brezplačnih programov, zaslonov za zaščito zaslona, do različnih orodnih vrstic, pa vse do programov za deljenje datotek. Eden od priljubljenih trikov kriminalcev je preusmerjanje vašega brskalnika na neželene spletne strani, kar napadalcem omogoča izvrševanje dodatnih kaznivih dejanj. Namen vohunske programske opreme ni uničevanje, poškodovanje ali motenje podatkov in sistemov, temveč zbiranje različnih informacij o uporabniku (njegovih navadah in vedenju, pomnjenje in beleženje gesel ter drugih zaupnih informacij) preko spletnih mest, družbenih omrežij in spletnih trgovin, o čemer nato poroča nazaj na osrednji vir bodisi za zakonite bodisi nezakonite namene. (Šepec, 2018)

Oglaševalska programska oprema (angl. adware) zbira podatke o uporabnikih in njihovih spletnih navadah, svoje ugotovitve pa pošilja različnim agencijam, ki uporabnike zasipajo z oglasi in neželeno pošto. Adware lahko nenehno prikazuje pojavna okna, kar znatno upočasni delovanje računalnika. (Šepec, 2018)

Izsiljevalska programska oprema (angl. ransomware) ima sama po sebi razumljiv pomen – programi držijo ključne informacije za "talce", da bi prejeli odkupnino. Posledice lahko vključujejo izgubo podatkov ali neavtorizirano distribucijo podatkov v javnost, kar vpliva na prihodnje poslovanje organizacije (Šepec, 2018), njen ugled ali ugled osebe. Dandanes večina izsiljevalske programske opreme nastane kot posledica računalniškega črva, ki se lahko širi iz enega sistema v naslednjega in po omrežjih brez ukrepanja uporabnika (Bhargava et al., 2022). Izsiljevalska programska oprema lahko cilja na vse industrijske sektorje, kjer so nekateri bolj ranljivi od drugih. Na primer leta 2021 je izsiljevalska programska oprema najbolj prizadela (Fedor, 2022) pravne, proizvodne, finančne in kadrovske storitve (Cyberreason, 2022).

3.1.5 Zavrnitev storitve

Napad z zavrnitvijo storitve (angl. Denial of Service, v nadaljevanju DoS) je vrsta kibernetskega napada, pri katerem kriminalci naredijo določeno omrežje nedostopno uporabnikom in vstopijo v računalniški sistem, da zbirajo osebne podatke. Napad izvira iz enega samega sistema ali omrežja. Gre za poskus napadalcev, da preprečijo zakonitemu uporabniku storitve uporabo te storitve. Napad DoS se lahko izvede preko (Šepec, 2018):

- onemogočanja omrežnih preusmerjevalnikov, ki omogočajo dostop do interneta napadenega informacijskega sistema. Brezžične dostopne točke se reprogramirajo, da ne zagotavljajo več brezžične internetne povezave do napadenih IT sistemov,
- pošiljanja množice e-poštnih sporočil (angl. mail bombing), kar preobremeni strežnik za elektronsko pošto,
- programov, ki se nenehno razmnožujejo ali drugih vrst virusnih kod, ki napadajo informacijski sistem.

Napad z distribuirano zavrnitvijo storitve (angl. Distributed Denial of Service, v nadaljevanju DDoS) je koordiniran preko več informacijskih sistemov, pri čemer vsak pošilja del podatkov za izvedbo napada hkrati iz več točk napada. Gre za distribuirano onemogočanje delovanja storitve informacijskega sistema. Napadalec lahko napade več podrejenih sistemov (sužnjev - angl. slaves), ki jih nadzira preko nadzornih sistemov (vodij - angl. masters). Napadi se pogosto izvajajo na bistveno večji ravni z več podrejenimi sistemi. (Šepec, 2018)

4 Ukrepi za zaščito pred IT grožnjami

Rek »bolje preventiva kot kurativa« velja tudi, kadar govorimo o informacijski in računalniški varnosti. V današnjem, visoko digitaliziranem in povezanem svetu, tako na posameznike kot podjetja na vsakem koraku prežijo najrazličnejše nevarnosti, zaradi česar je pomembno, da poznamo ukrepe, kako se zaščititi pred IT grožnjami ter zlonamernimi programskimi opremami. Različne strategije in metode v prvi vrsti sledijo postopku preprečevanja, odkrivanja ali zaznavanja ter odzivanja (Kemmerer, 2003) na IT grožnje. Pri tem se kibernetska varnost ukvarja predvsem z varovanjem

IT virov (informacije, aplikacije ali programska oprema, infrastruktura, neopredmetena sredstva in ljudje) pred nepooblaščenim razkritjem, spreminjanjem ali uničenjem. Na ta način se zagotovijo IT zahteve CIA trikotnika (razpoložljivost, celovitost in zaupnost).

Informacijska in računalniška varnost sta ključni temi, ki ju je potrebno obravnavati in implementirati v kateremkoli podjetju, da se zagotovi zaščito notranjih sredstev ter intelektualne lastnine (McFadzean et al., 2011). Večina podjetij (kot tudi posameznikov) posluje preko spleta, saj le-ta omogoča povezovanje in komunikacijo v realnem času (Chen et al., 2010). Obstajajo različni načini, kako se lahko podjetje zaščiti pred IT grožnjami ter napadi. V določenih primerih je potreben tudi finančni vložek, ki je odvisen od samega načina in ravni zaščite. V prvi vrsti je potrebno poučiti in izobraziti ljudi o primernem obnašanju v kibernetskem prostoru, saj so v večini primerov ravno ljudje odgovorni, da se napad sploh zgodi (odpiranje neprimernih strani, klikanje na spletne povezave ali priponke). V podpoglavjih je zajetih nekaj ukrepov, kako lahko podjetje zaščiti svoje IT vire s pomočjo zaposlenih pred IT grožnjami ter napadi. Enake ukrepe je mogoče uporabiti tudi v primeru fizičnega posameznika za varovanje osebnih naprav.

4.1 Ustvarjanje gesel

Za vsak uporabniški račun ter tudi nekatere aplikacije je potrebno ustvariti geslo. Veliko ljudi si določi zanje enostavno geslo, ki po navadi zajema kraj bivanja ali rojstni kraj, datume rojstnih dni, imena otrok ali ljubljenčkov in podobno. Prav tako se v geslih pogosto uporabijo besede iz slovarja. To nikakor ni primerna vsebina gesel, saj so lahko ugotovljiva in tudi dokaj kratka. Kadar napadalci poskušajo dostopati do računov, se poslužujejo napadov s surovo silo (angl. brute-force attack), kjer s pomočjo programske opreme "pregledajo" slovarje in uporabijo veliko število različnih gesel z upanjem, da bo eno izmed njih pravilno. (Kaspersky, 2023b)

Vsakoletno se podaljšuje tudi priporočljiva dolžina gesel, pri čemer se minimalno zahteva vsaj osem znakov. Daljša gesla so vedno boljša od kratkih – več, kot je znakov, dlje bo trajalo "razbijanje" gesla ali njegovo ugotavljanje. En dodaten znak (črka, številka ali simbol) lahko podaljša čas za razbijanje gesla za mesece ali celo leta. Zato je vedno bolje ustvariti daljša gesla, kot so minimalno zahtevana. Priporočljiva je uporaba gesel z vsaj 12 znaki. Pri tem je potrebno kombinirati velike in male črke,

številke ter simbole. Seveda moramo biti pozorni tudi na vrstni red, saj se vse pogosteje dogaja, da so gesla sestavljena iz (v tem zaporedju): ene velike črke, nabora malih črk, nabora števil in enega ali dveh simbolov. Zato je zelo pomembna uporaba »soljenja in popranja« gesel (The Upwork Team, 2021), kjer gre za naključno uporabo mešanice velikih in malih črk, številk ter simbolov, kar močno poveča stopnjo težavnosti in podaljša čas, ki je potreben za razbijanje gesla.

Zaradi preobremenjenosti smo ljudje nagnjeni k lenobi in enostavnosti, kadar ustvarjamo spletne račune, zaradi česar velikokrat uporabimo eno geslo za več računov, kar sploh ni priporočljivo. Kadar uporabljamo eno geslo za več računov ali naprav, lahko napadalci ob nepooblaščenem dostopu ali vdoru dostopajo do vseh teh računov in podatkov v njih. Če pa imamo za vsak račun in napravo drugačno geslo, je ogrožen samo en račun, drugi pa ne. Tako so naši podatki bolj varni in zaščiteni pred IT grožnjami ter napadi.

4.2 Zaščita računalniškega omrežja

Varovanje IT infrastrukture ter aplikacij ali programske opreme, posledično tudi informacij in ljudi v podjetju, je možno doseči na različne načine. Tabela 3.1 predstavlja nabor preventivnih ukrepov, katerih se lahko podjetje posluži za zaščito omenjenih IT virov ter njihov opis.

Tabela 3.1: Preventivni ukrepi za zaščito pred IT grožnjami

Ukrep	Opis
Namestitev varnostnih IT okvirjev	Varnostni IT okvirji opisujejo dokumentirane in medsebojno razumljive politike, ki narekujejo upravljanje z občutljivimi informacijami v podjetju.
Ustvaritev belega seznama (angl. whitelist) aplikacij	Na podlagi seznama dovoljenih aplikacij lahko podjetje zaposlenim določi, katere aplikacije se smejo nameščati in/ali izvajati na službenih napravah.
Uporaba protivirusne programske opreme	Omogoča vzdrževanje "čistih" računalnikov in operacijskih sistemov na podlagi rednega preverjanja, zaznavanja, preprečevanja in odstranjevanja različne zlonamerne programske opreme.
Požarni zid (angl. firewalls)	Požarni zid določa pravila, ki urejajo promet podatkov ter nadzira vstop in izstop podatkov ter drugih naprav v in iz računalnika.
Uporaba sistema za zaznavanje vdorov v omrežje (NIDS)	Sistem za zaznavanje vdorov v omrežje (angl. network intrusion detection systems, v nadaljevanju NIDS) deluje podobno kot protivirusna programska oprema ter požarni zid; spremlja promet, ki poteka v in iz

Ukrep	Opis
	različnih naprav, povezanih v omrežje ter preverja izvajanje zlonamernih dejavnosti ali nepooblaščene dostope ter o tem obvesti lastnika omrežja.
Izvedba večstopenjske avtentikacije	Varnost informacij in podatkov se lahko zagotovi na podlagi večstopenjske avtentikacije, ki se zahteva za dostop do občutljivih informacij. V tem primeru lahko gre za kombinacijo vnosa različnih gesel, ki se jih prejme preko različnih naprav (telefon in računalnik) ali računov (e-pošta, telefonska številka).
Uporaba kriptiranja	Z asimetričnim kriptiranjem se zaščiti občutljive informacije, ki se prenašajo iz ene naprave v drugo bodisi preko spleta bodisi drugih naprav. Dokument ali datoteko s pomočjo javnega ključa kriptiramo (ustvarimo tajnopis), na drugi strani pa jo dekriptiramo z zasebnim ključem (spremenimo nazaj v čistopis).
Uporaba navidezno zasebnega omrežja (VPN)	Navidezno zasebno omrežje (angl. virtual private network, v nadaljevanju VPN) predstavlja način oblikovanja zasebnega mesta na spletu, ki uporabnikom pomaga ustvariti varno povezavo ter šifrira podatke, poslane preko omrežja. VPN je velikokrat vključen v protivirusno programsko opremo.
Uporaba „medenih loncev“ (angl. honeypots)	»Medeni lonci« predstavljajo umetno ustvarjeno tarčo, ki zajema nekoristne informacije. Medtem, ko napadalci nevede poskušajo dostopati do medenih loncev, so pomembne informacije in datoteke v računalniku zaščitene.
Izvedba ocene ranljivosti in penetracijskega testa	Izvedba ocene ranljivosti vključuje iskanje potencialnih težav v omrežju ali sistemu, ki bi lahko omogočile nepooblaščen zunanji dostop. Ranljivosti se odkrijejo, določi se njihova resnost in prednost razreševanja. Slednje se stori preko poskusa dostopa do omrežja ali sistema od zunaj, pri čemer lahko pomagajo etični hekerji.

Vir: (Chen et al., 2010; The Upwork Team, 2021; Vacca, 2013)

5 Sklep

Leta 2020 je bilo v povprečju odkritih 360.000 novih zlonamernih datotek (Kaspersky, 2023a), vsako leto pa postajajo njihovi avtorji bolj inovativni. Pojavljajo se nove vrste zlonamernih kod, ki lahko izkoriščajo varnostne pomanjkljivosti v operacijskih sistemih, programih za protivirusno zaščito in požarnih zidovih. Najpogostejše škodljive kode, ki prevladujejo v kriminalnih dejanjih, v katerih se izvajajo različne metode, so motnje, poškodbe in hudo oviranje informacijskih sistemov ter elektronskih podatkov (Šepec, 2018).

Internet je postal najpogostejše mesto za širjenje virusov. Zlonamerna programska oprema se lahko skriva v vsem, kar je preneseno s spletnih strani, brez ustreznega varnostnega sistema pa lahko povzroči veliko škodo. Zaradi hitre rasti pogostosti elektronske pošte so priloge postale najpogostejši razlog za širjenje računalniških virusov. Pomembno je omeniti, da obstaja veliko različnih vrst zlonamerne

programske opreme, ki se skoraj vsak dan izboljšujejo, množijo in se pojavljajo v novih oblikah ali variacijah.

Zato mora informacijska in računalniška varnost podjetij vključevati tudi zaščito pred socialnim inženiringom, kot so različne oblike phishinga (tudi smishing in vishing), saj napadalci pogosto ciljajo na človeški dejavnik kot najšibkejši člen v varnostni verigi. Phishing napadi, kjer se napadalci predstavljajo kot zaupanja vredni subjekti, da bi pridobili občutljive podatke ali dostop do sistemov, so še posebej nevarni v logistiki zaradi kompleksnih in razvejanih oskrbovalnih verig. Zaposleni lahko prejmejo lažna e-poštna sporočila, ki jih pozivajo k razkritju gesel, številk kreditnih kartic ali drugih zaupnih informacij podjetja, kar lahko vodi do resnih varnostnih incidentov in motenj v poslovanju. Zato je ključno, da podjetja izvajajo redna izobraževanja in ozaveščanja zaposlenih o prepoznavanju phishing poskusov ter uvajajo varnostne ukrepe, ki zmanjšujejo tveganje za tovrstne napade.

V kontekstu digitalizacije logistike imata informacijska in računalniška varnost ključno vlogo pri zagotavljanju nemotenega in varnega delovanja logističnih procesov. Digitalizacija prinaša številne prednosti, kot so povečana učinkovitost, boljša sledljivost pošiljk in optimizacija zalog, obenem pa izpostavlja podjetja IT grožnjam in napadom. Kibernetski napadi, kot so: vdor v sisteme, kraja podatkov ali napadi z izsiljevalsko programsko opremo, lahko povzročijo resne motnje v oskrbovalnih verigah, kar vodi do zamud, finančnih izgub in splošne škode za ugled podjetij. Zato je nujno, da podjetja vlagajo v informacijsko in računalniško varnost skozi primerne rešitve ter ukrepe, predstavljene znotraj tega poglavja.

Informacijska varnost v logistiki se poleg zgoraj napisanega nanaša tudi na zaščito zaupnih podatkov, kot so: informacije o strankah, transakcijah, dobaviteljih ter poslovnih partnerjih in drugih. Učinkovito upravljanje podatkov je bistveno za vzdrževanje zaupanja med poslovnimi partnerji in končnimi uporabniki. Skladnost z zakonodajo in standardi varovanja podatkov, kot sta GDPR in ISO 27001, je pomemben vidik informacijske varnosti, ki zagotavlja, da podjetja delujejo v skladu z zakonskimi zahtevami in najboljšimi praksami. Varnostne politike in postopki, ki vključujejo redne varnostne preglede in ocene tveganja, so nujne za preprečevanje varnostnih incidentov in zmanjševanje tveganj pri digitalizaciji logistike.

Literatura

Bhargava, P., Choudhary, R., & Gupta, A. (2022, May). A Review Study on Computer Virus. *World Journal of Research and Review (WJRR)*, *14*(5), 39–44.

Chen, R.-S., Chung, Y.-M., & Tsai, C.-H. (2010). A study of the performance evaluation of a network intrusion detection system. *Asian Journal on Quality*, *11*(1), 28–38. https://doi.org/10.1108/15982681011051804

Cyberreason. (2022). *Ransomware: The True Cost to Business—A Global Study on Ransomware Business Impact*. https://www.cybereason.com/hubfs/dam/collateral/reports/Ransomware-The-True-Cost-to-Business-2022.pdf

Fedor, O. (2022, November 3). *93 Must-Know Ransomware Statistics [2023]*. Antivirus Guide. https://www.antivirusguide.com/cybersecurity/ransomware-statistics/?gclid=Cj0KCQjwi46iBhDyARIsAE3nVrYtrwBey_1ErcYLO6UBJVk3as7CfdxsGKVcHVkKJfM_Mcyvk92IlH0aAr3WEALw_wcB

Horton, J., & Seberry, J. (1997). *Computer Viruses—An Introduction. 19, 1*, 122–131. https://documents.uow.edu.au/~jennie/WEBPDF/1997_09.pdf

IBM. (n.d.). *What is a mainframe?* IBM. Retrieved 4 October 2023, from https://www.ibm.com/topics/mainframe

Information Security: The Ultimate Guide. (n.d.). *Imperva*. Retrieved 3 October 2023, from https://www.imperva.com/learn/data-security/information-security-infosec/

IT Governance Institute. (2007). *COBIT 4.1: Framework, control objectives, management guidelines, maturity models*. IT Governance Institute.

Jereb, B. (2017). Mastering logistics investment management. *Transformations in Business and Economics*, *16*, 100–120.

Jereb, B., Cvahte Ojsteršek, T., & Rosi, B. (2016). *Governance of Investments in Logistics* (pp. 236–247). https://doi.org/10.4018/978-1-5225-0001-8.ch011

Kabanda, G. (2019). *Trends in Information Technology Management*.

Kajba, M., & Jereb, B. (2021). *Three Crucial Years of IT Trends in Logistics*. 187–198. https://www.elibrary.ru/item.asp?id=46600879&pff=1

Kajba, M., Jereb, B., & Obrecht, M. (2023). Considering IT Trends for Modelling Investments in Supply Chains by Prioritising Digital Twins. *Processes*, *11*(1), Article 1. https://doi.org/10.3390/pr11010262

Kaspersky. (2023a, May 18). *The number of new malicious files detected every day increases by 5.2% to 360,000 in 2020*. Www.Kaspersky.Com. https://www.kaspersky.com/about/press-releases/2020_the-number-of-new-malicious-files-detected-every-day-increases-by-52-to-360000-in-2020

Kaspersky. (2023b, June 30). *Brute Force Attack: Definition and Examples*. Www.Kaspersky.Com. https://www.kaspersky.com/resource-center/definitions/brute-force-attack

Kemmerer, R. A. (2003). Cybersecurity. *25th International Conference on Software Engineering, 2003. Proceedings.*, 705–715. https://doi.org/10.1109/ICSE.2003.1201257

Maity, S., & Dey, D. (2021). Computer Virus Attacks. *La Pensée*, *51*(3), 585–594. https://doi.org/10.6084/m9.figshare.19258763.v1

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2011). Information Assurance and Corporate Strategy: A Delphi Study of Choices, Challenges, and Developments for the Future. *Information Systems Management*, *28*(2), 102–129. https://doi.org/10.1080/10580530.2011.562127

Paulo. (2022, December 21). *Top 10 most dangerous computer viruses of all time*. Dynamic Solutions Group. https://www.dsolutionsgroup.com/top-10-most-dangerous-malware-of-all-time/

Šepec, M. (2018). Kibernetski kriminal: Kazniva dejanja in kazenskopravna analiza. In *Univerzitetna založba Univerze v Mariboru*. Univerzitetna založba Univerze v Mariboru. https://press.um.si/index.php/ump/catalog/book/335

The Upwork Team. (2021, June 8). *What Is IT Security? Examples and Best Practices for 2024*. https://www.upwork.com/resources/it-security

Vacca, J. R. (2013). *Cyber Security and IT Infrastructure Protection*. Syngress.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

What Is Computer Security? (And Why It's Important). (2022, August 23). *Berkeley Boot Camps*. https://bootcamp.berkeley.edu/blog/what-is-computer-security/

Whitman, M. E., & Mattord, H. J. (2011). *Principles of Information Security* (4th edition). http://almuhammadi.com/sultan/sec_books/Whitman.pdf