10. PODATKOVNA ETIKA IN INFORMACIJSKA VARNOST

Avtor: Dario Šebalj

V dobi digitalne preobrazbe sta etično ravnanje s podatki in njihova varnost postali glavni vprašanji za posameznike in organizacije. Ker se dnevno zbirajo in obdelujejo velike količine osebnih in občutljivih podatkov, je zelo pomembno zagotoviti odgovorno in varno upravljanje teh podatkov.

To poglavje obravnava načela etike ravnanja s podatki, poudarja moralne vidike in najboljše prakse ravnanja s podatki ter raziskuje različne grožnje informacijski varnosti. Z razumevanjem in obravnavanjem teh vprašanj lahko zaščitimo zasebnost, ohranimo zaupanje in spodbujamo varnejše digitalno okolje.

10.1. Pomen podatkovne etike

Podatkovna etika se nanaša na moralna načela in prakse, ki usmerjajo zbiranje, obdelavo, souporabo in uporabo podatkov, da bi zagotovili spoštovanje pravic posameznikov, družbeno blaginjo in zaupanje. Vključuje preglednost, odgovornost, poštenost in zasebnost ter zagotavlja, da so podatkovne prakse usklajene z etičnimi standardi in pravnimi okviri za preprečevanje škode in spodbujanje odgovornih inovacij (Cognizant, n.d.; Gov.uk, 2020; Knight, 2021; McKinsey, 2022; Cepelak, 2023)

V današnjem digitalnem okolju je etično ravnanje s podatki ključnega pomena za ohranjanje zaupanja in zagotavljanje konkurenčne prednosti. Članek McKinsey (2022) o etiki ravnanja s podatki poudarja pomen vključevanja etičnih vidikov v prakse ravnanja s podatki. Opozarja na tri pogoste napake: predpostavljanje, da je podatkovna etika nepomembna, zanašanje izključno na pravne ekipe in ekipe za skladnost pri nadzoru ter dajanje prednosti kratkoročnim finančnim dobičkom pred etičnimi praksami. Za reševanje teh vprašanj priporočajo več strategij. Prvič, podjetja bi morala določiti jasne, za podjetje specifične smernice za podatkovno etiko. Te smernice služijo kot osnova za etično upravljanje podatkov in pomagajo pri določanju standardov v celotni organizaciji. Drugič, oblikovanje različnih skupin za obravnavo vprašanj, povezanih s podatki, zagotavlja različne poglede in zmanjšuje tveganje pristranskega

odločanja. Tretjič, vključevanje višjega vodstva kot zagovornikov pobud za etično ravnanje s podatki je ključnega pomena za uveljavljanje teh praks v celotni organizaciji.

Slika 1015C podatkovne etike

Vir: Avtor, prirejeno po Atlan (2023).

Slika 10.1 prikazuje 5C podatkovne etike, ki jo je opisal Atlan (2023) in predstavlja bistvena načela za etično ravnanje s podatki:

- **Soglasje (Consent):** Pred zbiranjem podatkov posameznikov pridobite njihovo prostovoljno soglasje, ki je osveščeno, in zagotovite preglednost uporabe podatkov.
- **Zbirka (Collection):** Zbiranje podatkov: zbirajte le podatke, ki so potrebni za določene namene, in se izogibajte pretiranemu zbiranju podatkov.
- **Nadzor (Control):** Omogočite posameznikom, da dostopajo do svojih podatkov, jih pregledujejo in posodabljajo ter tako zagotavljajo nadzor nad njihovo uporabo.
- **Zaupnost (Confidentiality):** Zaščitite podatke pred nepooblaščenim dostopom in kršitvami z zanesljivimi varnostnimi ukrepi.
- **Skladnost s predpisi (Compliance):** Upoštevanje zakonskih in regulativnih zahtev ter izvajanje rednih revizij za zagotavljanje stalne skladnosti.

Podobno kot Atlanova načela tudi Cote (2021) opredeljuje pet ključnih načel podatkovne etike, ki jih morajo spoštovati poslovni strokovnjaki:

- **Lastništvo** poudarja, da posamezniki ohranijo lastništvo nad svojimi osebnimi podatki. Zbiranje osebnih podatkov brez izrecne privolitve je nezakonito in neetično. Podjetja morajo soglasje pridobiti z jasnimi sporazumi ali digitalnimi politikami zasebnosti, ki

zagotavljajo, da so uporabniki seznanjeni s praksami zbiranja podatkov in se z njimi strinjajo.

- **Preglednost** vključuje jasno obveščanje o načinu zbiranja, shranjevanja in uporabe podatkov. Podjetja morajo posameznike obvestiti o metodah in namenih zbiranja podatkov. Ta preglednost krepi zaupanje in uporabnikom omogoča, da se o svojih podatkih odločajo na podlagi informacij. Zavajajoče prakse ali prikrivanje informacij o uporabi podatkov so neetične in nezakonite.
- **Zasebnost** se osredotoča na odgovornost podjetij za zaščito zasebnosti osebnih podatkov. Osebni podatki ne smejo biti javno dostopni brez izrecnega dovoljenja posameznika, tudi če je ta privolil. Podjetja morajo izvajati zanesljive varnostne ukrepe za zaščito osebnih podatkov pred nepooblaščenim dostopom ali kršitvami.
- **Namen** se nanaša na etične motive za zbiranje in uporabo podatkov. Podatke je treba zbirati in uporabljati za namene, ki so koristni in ne škodljivi za posameznike ali družbo. Etične podatkovne prakse vključujejo uporabo podatkov za izboljšanje uporabniške izkušnje in izboljšanje storitev brez izkoriščanja ali povzročanja škode.
- **Rezultat** obravnava širše vplive uporabe podatkov na posameznike in družbo. Podjetja morajo oceniti morebitne posledice svojih podatkovnih praks in si prizadevati, da bi se izognila negativnim posledicam. To načelo poudarja potrebo po etičnem predvidevanju in odgovornosti pri sprejemanju odločitev na podlagi podatkov.

Guzman in Dyer (2020) poudarjata, da etični izzivi pri podatkovnih praksah niso enostavni in pogosto nimajo jasnih rešitev. Navedla sta, da obstaja razhajanje med etičnimi pričakovanji na spletu in zunaj njega. Mnogi posamezniki zaznavajo obliko izjemnosti v spletnih prostorih, kjer se zdi, da tradicionalna etična pravila ne veljajo. Takšna miselnost lahko privede do upravičevanja dejanj na spletu, ki bi se brez povezave štela za neetična. Avtorji predlagajo etični pristop, ki povezuje obe področji, in poudarjajo, da morajo etična načela ostati dosledna ne glede na medij.

Članek o etiki podatkov, ki so ga objavili Basl in drugi (2021), obravnava zapleten proces prehoda od abstraktnih etičnih načel do konkretnih, izvedljivih obljub v kontekstu velikih količin podatkov in umetne inteligence. Ugotovili so, da je ta premik težaven in pomemben, da bi zagotovili, da etično ravnanje ne bo le teoretično, temveč tudi praktično in pomembno.

O'Reilly (2018) navaja, da sta Princetonski center za politiko informacijske tehnologije in Center za človekove vrednote pripravila štiri anonimne študije primerov, da bi spodbudila etični

diskurz. Ena od študij primera obravnava etične dileme, ki jih povzroča avtomatizirana zdravstvena aplikacija, zasnovana za pomoč bolnikom s sladkorno boleznijo odraslih z uporabo umetne inteligence. Poudarja potrebo po uravnoteženju tehnoloških koristi z etičnimi načeli, kot so avtonomija, pravičnost in odgovornost. Obravnava teh etičnih izzivov je ključna za odgovorno vključevanje umetne inteligence v zdravstveno varstvo, saj zagotavlja, da ta služi najboljšim interesom vseh bolnikov. Obravnavati je treba nekaj ključnih vprašanj:

- **Paternalizem:** Namen aplikacije je spodbujati zdravo vedenje bolnikov s tem, da jih spodbuja k boljšim odločitvam. To lahko sicer izboljša zdravstvene rezultate, vendar pa sproža etična vprašanja o avtonomiji in paternalizmu. Ali je etično, da aplikacija vpliva na vedenje bolnikov, ali pa bi morali biti bolniki popolnoma samostojni pri svojih zdravstvenih odločitvah?
- **Soglasje in preglednost:** Aplikacija za učinkovito delovanje zbira občutljive zdravstvene podatke. Ključnega pomena je zagotoviti informirano soglasje in preglednost glede zbiranja, uporabe in izmenjave podatkov. Pacienti morajo biti v celoti seznanjeni s tem, kateri podatki se zbirajo, kako se bodo uporabljali in kdo bo imel dostop do njih.
- **Zasebnost in varnost podatkov:** Ravnanje z občutljivimi zdravstvenimi podatki zahteva stroge ukrepe za zasebnost in varnost. Študija primera poudarja potrebo po zanesljivih protokolih za zaščito podatkov, da se podatki o bolnikih zavarujejo pred kršitvami in nepooblaščenim dostopom.
- **Odgovornost in odgovornost:** Določitev, kdo je odgovoren za odločitve in dejanja aplikacije, je še en ključni vidik. Če aplikacija poda napačno priporočilo, ki negativno vpliva na pacientovo zdravje, je določitev odgovorne osebe (razvijalci, ponudniki zdravstvenih storitev ali aplikacija sama) zapletena, vendar potrebna za odgovornost.

Sodobno upravljanje podatkov v osnovi temelji na podatkovni etiki, ki zagotavlja poštene, pregledne, odgovorne in zasebnost spoštujoče podatkovne prakse. Organizacije lahko z upoštevanjem etičnih standardov spodbujajo odgovorne inovacije, se izognejo pravnim pastem in povečajo zaupanje. Vključevanje močnih etičnih okvirov v prakse upravljanja podatkov ni le najboljša praksa, temveč tudi zahteva za trajnostno in odgovorno rast, saj podatki postajajo vse pomembnejši za delovanje in odločanje.

Drug pomemben vidik je informacijska varnost, saj sta etika podatkov in informacijska varnost neločljivo povezani. Zagotavljanje etičnega ravnanja s podatki je temelj za zanesljive ukrepe

informacijske varnosti. Zaščita podatkov pred nepooblaščenim dostopom, vdori in drugimi varnostnimi grožnjami ne le ohranja zasebnost in zaupnost, temveč tudi podpira etična načela, obravnavana v tem poglavju.

10.2. Osnove informacijske varnosti

Informacijska varnost pomeni celovit sklop praks in načel, katerih cilj je varovanje informacij in informacijskih sistemov pred nepooblaščenim dostopom, uporabo, razkritjem, motnjami, spreminjanjem ali uničenjem. Z izvajanjem zaščitnih ukrepov, politik in tehnologij zagotavlja zaupnost, celovitost in razpoložljivost podatkov. Ti ukrepi vključujejo nadzor dostopa, šifriranje, obnovitev po nesreči ter skladnost z zakonskimi in regulativnimi standardi za zmanjšanje tveganj in zaščito pred morebitnimi grožnjami (Fruhlinger, 2020; CISCO, n.d., NIST, n.d.).

Informacijska varnost je zdaj bistvenega pomena za verodostojnost in celovitost organizacije v digitalni dobi. Njena pomembnost se kaže v vse večji odvisnosti od digitalnih podatkov in naraščanju kibernetskih groženj, ki ogrožajo občutljive podatke. Informacijska varnost predvsem varuje občutljive podatke pred nepooblaščenim dostopom, vdori in krajo. To vključuje osebne podatke, finančne podatke, intelektualno lastnino in zaupne poslovne komunikacije. Ker so kibernetski napadi vse bolj izpopolnjeni, se tveganje kršitev varnosti podatkov povečuje, kar lahko povzroči velike finančne izgube in škodo ugledu. V primeru kršitve Equifax leta 2017 so bili na primer izpostavljeni osebni podatki 147 milijonov ljudi, zaradi česar je bila sklenjena poravnava v višini do 425 milijonov dolarjev (Federal Trade Commission, 2022). Takšni incidenti opozarjajo na hude posledice neustreznih ukrepov za informacijsko varnost.

Poleg tega je varnost informacij ključnega pomena za ohranjanje zaupanja potrošnikov. V dobi, ko je zasebnost podatkov ključnega pomena, stranke vse bolj skrbi, kako se ravna z njihovimi podatki. Močna arhitektura informacijske varnosti zagotavlja, da so podatki potrošnikov varni, kar spodbuja zvestobo in zaupanje. Glede na raziskavo podjetja IBM **75 %** strank ne bi kupovalo pri podjetju, ki mu ne zaupajo, da varuje njihove podatke (PR Newswire, 2018). Zato je informacijska varnost tako tehnološka potreba kot strateška poslovna nujnost.

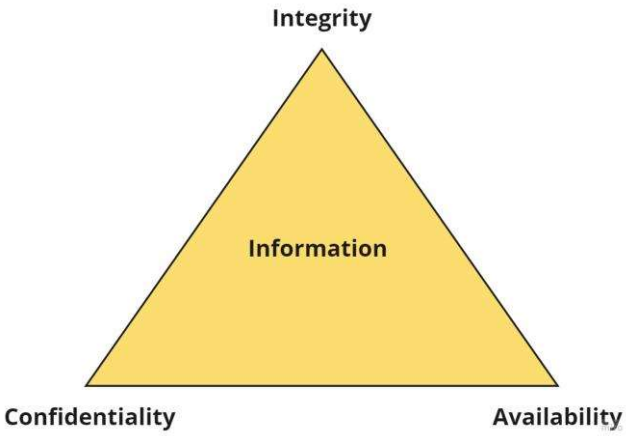
Informacijska varnost je prav tako ključnega pomena za ublažitev motenj v delovanju. Kibernetski napadi, kot je izsiljevalska programska oprema, lahko motijo delovanje podjetja, saj uporabnikom onemogočijo dostop do pomembnih sistemov , dokler ne plačajo odkupnine.

Napad z izsiljevalsko programsko opremo 2021 Colonial Pipeline, ki je povzročil pomanjkanje goriva na vzhodu Združenih držav, je primer motečega potenciala takšnih groženj (Kerner, 2022). Z izvajanjem strogih varnostnih ukrepov lahko organizacije zavarujejo neprekinjeno delovanje in odpornost proti takšnim motnjam.

Kim in Solomon (2018) pravita, da se informacije štejejo za varne, če izpolnjujejo tri glavna načela:

- **Zaupnost (Confidentiality):** do občutljivih informacij lahko dostopajo le pooblaščene osebe.
- **Integriteta (Integrity):** informacije lahko spreminjajo le osebe z dovoljenjem.
- **Razpoložljivost (Availability):** informacije in viri so dostopni pooblaščenim uporabnikom, kadar koli jih potrebujejo.

Ta načela se pogosto imenujejo triada CIA, kot je prikazano na sliki 10.2.



Slika 102CIA TRIADA

Vir: Avtor, prirejeno po Kim in Solomon (2018).

V informacijski varnosti so koncepti tveganja, grožnje in ranljivosti osrednjega pomena za razumevanje in upravljanje varnosti. **Tveganje** je verjetnost, da se bo sredstvu zgodilo nekaj slabega. Pri informacijski varnosti je tveganje verjetnost škodljivega dogodka, ki bo vplival na zaupnost, celovitost ali razpoložljivost informacij. Podjetje lahko na primer oceni tveganje kibernetskega napada na svoje omrežje tako, da upošteva verjetnost takega napada in morebitno škodo, ki bi jo lahko povzročil. Grožnja je vsako dejanje, ki lahko povzroči škodo informacijskim sistemom ali podatkom. **Grožnje** so lahko namerne, na primer kibernetski napadi hekerjev, ali nenamerne, na primer naravne nesreče ali človeške napake. **Ranljivost** se nanaša na slabosti ali vrzeli v obrambi sistema, ki jih lahko grožnje izkoristijo za povzročitev

škode. To so lahko pomanjkljivosti v programski in strojni opremi, organizacijskih procesih ali človeškem vedenju (Kim in Solomon, 2018).

Za učinkovito zaščito informacijskih sistemov morajo organizacije razumeti medsebojno delovanje tveganj, groženj in ranljivosti. Na primer, ranljivost v programski opremi (kot je varnostna pomanjkljivost) lahko izkoristi povzročitelj grožnje (kot je heker), kar privede do vdora v podatke, ki predstavlja tveganje za organizacijo. Z ugotavljanjem in zmanjševanjem ranljivosti lahko organizacije zmanjšajo tveganje, da bi grožnje povzročile veliko škodo.

10.2.1. Kršitve podatkov

V digitalni dobi so kršitve varnosti podatkov postale velika grožnja, ki je prizadela organizacije v različnih sektorjih. Te kršitve ogrožajo občutljive podatke, kar vodi do finančnih izgub, škode ugledu in pravnih posledic. Razumevanje obsega in vpliva kršitev varnosti podatkov je ključno za razvoj učinkovitih varnostnih strategij za zaščito pred takšnimi incidenti. Po podatkih podjetja Fortinet (n.d.) je **kršitev varnosti podatkov** "dogodek, zaradi katerega so zaupni, zasebni, zaščiteni ali občutljivi podatki izpostavljeni osebi, ki ni pooblaščena za dostop do njih". Te kršitve se lahko zgodijo na različne načine (Kaspersky, b.d.):

1. **Naključni insajder:** Zaposleni nenamerno dostopa do občutljivih informacij brez ustreznega dovoljenja. Na primer: uporabi računalnik sodelavca in si ogleda zaupne datoteke.
2. **Zlonamerni notranji uporabnik:** Posameznik s pooblaščenim dostopom namerno zlorabi podatke v škodljive namene. To lahko vključuje krajo ali uhajanje občutljivih informacij.
3. **Izgubljene ali ukradene naprave:** Nešifrirane in nezavarovane naprave, kot so prenosni računalniki ali zunanji diski z občutljivimi podatki, se izgubijo ali ukradejo, zaradi česar so podatki izpostavljeni nepooblaščenemu dostopu.
4. **Zlonamerni zunanji kriminalci:** Hekerji za vdor v sisteme uporabljajo različne metode, vključno z napadi z ribarjenjem, napadi z grobo silo in zlonamerno programsko opremo. Ti kibernetski kriminalci izkoriščajo ranljivosti v programski opremi, omrežjih in vedenju uporabnikov, da bi pridobili dostop do občutljivih podatkov.

Po podatkih družbe Kaspersky (n.d.) so pogoste metode, ki se uporabljajo pri kršitvah varnosti podatkov, **ribarjenje,** pri katerem se kibernetski kriminalci izdajajo za zaupanja vredne subjekte, da bi posameznike prepričali, da razkrijejo občutljive informacije. Druga metoda so **napadi z grobo silo**, pri katerih hekerji s pomočjo programske opreme večkrat ugibajo gesla

in izkoriščajo šibke ali večkrat uporabljene poverilnice za pridobitev nepooblaščenega dostopa do računov. Poleg tega se **zlonamerna programska oprema,** kot je vohunska programska oprema, uporablja za neopažen vdor v sisteme in krajo podatkov. Te metode bodo razložene v nadaljevanju poglavja.

Človeška napaka je vzrok za **95 %** vseh kršitev varnosti podatkov (Cybernews, 2022).

V 21. stoletju smo bili priča nekaterim najhujšim kršitvam varnosti podatkov, ki so opozorile na ranljivosti digitalnih sistemov in na nujno potrebo po zanesljivih varnostnih ukrepih. Po podatkih Hill in Swinhoe (2022) ter družbe ESET (n.d.) je nekaj najodmevnejših kršitev varnosti podatkov:

- **Yahoo (2013-2014):** Yahoo je doživel enega največjih vdorov v podatke v zgodovini, saj so bile leta 2013 ogrožene vse tri milijarde njegovih uporabniških računov. Ta kršitev je razkrila imena, e-poštne naslove, datume rojstva ter varnostna vprašanja in odgovore. Druga kršitev leta 2014 je prizadela 500 milijonov računov, kar je še dodatno opozorilo na varnostne ranljivosti podjetja.
- **Marriott International (2018):** Marriott je objavil kršitev, ki je prizadela približno 500 milijonov gostov. Hekerji so imeli dostop do podatkovne zbirke rezervacij gostov družbe Starwood, pri čemer so bili izpostavljeni osebni podatki, kot so imena, naslovi, telefonske številke, e-poštni naslovi in številke potnih listov. Ta kršitev je bila posledica nepooblaščenega dostopa iz leta 2014. Urad informacijskega pooblaščenca (ICO), britanski organ za nadzor podatkov, je leta 2020 korporaciji izrekel globo v višini 18,4 milijona funtov, ker ni zaščitila zasebnosti osebnih podatkov svojih strank.
- **Iskalnik prijateljev za odrasle (2016):** Pri kršitvi v storitvi Adult Friend Finder so bili razkriti osebni podatki 412 milijonov računov, vključno z imeni, e-poštnimi naslovi in gesli, od katerih so bili številni slabo šifrirani. Ta incident je sprožil veliko zaskrbljenost glede varnostnih praks spletnih platform, ki ravnajo z občutljivimi osebnimi podatki.
- **MySpace (2013):** V primeru kršitve varnosti podatkov MySpace leta 2013 je bilo izpostavljenih več kot 360 milijonov uporabniških računov. Podatki so vključevali imena, e-poštne naslove in gesla. Hekerji so te podatke pozneje prodali na temnem spletu, kar

je opozorilo na ranljivosti varnostnih sistemov platform družbenih medijev v tistem času.

- **LinkedIn (2021):** Na temnem spletnem forumu so bili leta 2021 objavljeni osebni podatki 700 milijonov uporabnikov LinkedIna. Heker je s tehnikami strganja podatkov prek LinkedInovega vmesnika API pridobil e-poštne naslove, telefonske številke in druge osebne podatke. Čeprav ni šlo za tradicionalni vdor, je ta incident sprožil resno zaskrbljenost glede zasebnosti podatkov in morebitne zlorabe strganih podatkov za napade s socialnim inženiringom.
- **Equifax (2017):** Ta kršitev je razkrila osebne podatke skoraj 148 milijonov Američanov, 15,2 milijona Britancev in 19.000 Kanadčanov. Hekerji so izkoristili ranljivost v ogrodju spletnih aplikacij Apache Struts, ki je Equifax ni popravil. Ukradeni podatki so vključevali številke socialnega zavarovanja, rojstne datume in naslove, zaradi česar je družba Equifax utrpela za približno 1,7 milijarde dolarjev stroškov.
- **eBay (2014):** eBay je razkril kršitev, ki je prizadela 145 milijonov uporabnikov. Napad je izhajal iz kompromitiranih prijavnih podatkov zaposlenih, zaradi česar so bila razkrita imena, e-poštni naslovi, fizični naslovi, telefonske številke in šifrirana gesla. Ta kršitev je opozorila na ranljivosti pri nadzoru dostopa zaposlenih in na pomen močnih ukrepov avtentikacije.
- **Cilj (2013):** Vdor, ki je prizadel več kot 41 milijonov računov plačilnih kartic in kontaktne podatke več kot 60 milijonov strank. Kibernetski kriminalci so dostopali do podatkov strank, vključno z imeni, telefonskimi številkami, e-poštnimi naslovi, številkami kreditnih in debetnih kartic ter šifriranimi kodami PIN. Podjetje Target je imelo precejšnje pravne stroške in stroške poravnave, vključno s skupinsko tožbo v višini 10 milijonov USD in poravnavo v višini 18,5 milijona USD v več državah.

Te kršitve dokazujejo daljnosežne posledice kibernetskih napadov in ključno potrebo po močnih praksah kibernetske varnosti. Na podlagi teh odmevnih primerov lahko organizacije bolje zaščitijo svoje podatke, izboljšajo svoje varnostne protokole in zmanjšajo tveganje za prihodnje kršitve. Vdori v podatke so pogosto posledica številnih osnovnih groženj. Razumevanje teh groženj je ključnega pomena za oblikovanje uspešnih ukrepov za informacijsko varnost. Kibernetske grožnje se lahko pojavijo iz različnih virov, vključno z zlonamernimi notranjimi uporabniki, kibernetskimi kriminalci in celo akterji, ki jih sponzorira država. Poleg tega se lahko ranljivosti v sistemih in omrežjih izkoristijo za nepooblaščen dostop do občutljivih informacij.

10.2.2. Grožnje informacijske varnosti

Varnostna grožnja je zlonamerno dejanje, ki poskuša poškodovati ali ukrasti podatke, ogroziti sisteme organizacije ali ogroziti podjetje kot celoto (TechTarget, 2024). Obstaja veliko različnih informacijskih varnostnih groženj, ki resno ogrožajo razpoložljivost, celovitost in zaupnost podatkov.

Kim in Solomon (2018) ter Grubb (2021) pravita, da je **zlonamerna** programska oprema namenjena vdoru, poškodovanju ali onemogočanju računalnikov in omrežij. Pogoste vrste zlonamerne programske opreme vključujejo viruse, črve, trojanske konje, izsiljevalsko programsko opremo in vohunsko programsko opremo. **Virus** je vrsta zlonamerne programske opreme, ki se pritrdi na zakonit program ali datoteko in se ob izvajanju okužene programske opreme razširi na druge programe in datoteke. Virusi lahko poškodujejo ali izbrišejo podatke, motijo delovanje sistema in se razširijo na druge sisteme prek priponk elektronske pošte, omrežnih povezav ali izmenljivih medijev. V nasprotju z virusi so **črvi** samostojna zlonamerna programska oprema, ki se lahko samostojno razmnožuje in širi po omrežjih, ne da bi se ji bilo treba priključiti na gostiteljski program. Črvi za širjenje izkoriščajo ranljivosti v operacijskih sistemih ali aplikacijah, pri čemer pogosto povzročajo preobremenitev omrežja in preobremenitev sistemov, saj porabljajo pasovno širino in vire. **Trojanski konj** ali trojanski konj je zlonamerna programska oprema, prikrita kot zakonita programska oprema. Uporabniki so prevarani, da ga namestijo in verjamejo, da gre za neškodljiv ali uporaben program. **Ransomware** je vrsta zlonamerne programske opreme, ki zašifrira podatke žrtve in jih naredi nedostopne, dokler se napadalcu ne plača odkupnina. Napadi izsiljevalske programske opreme so lahko uničujoči, saj povzročijo veliko izgubo podatkov in motnje v delovanju, če odkupnina ni plačana ali če varnostne kopije niso na voljo. **Vohunska programska oprema** je zlonamerna programska oprema, namenjena zbiranju informacij o osebi ali organizaciji brez njene vednosti. Zbira lahko različne vrste podatkov, kot so pritiski tipk, navade brskanja in osebne informacije, ter jih posreduje tretji osebi.

Druga vrsta grožnje je **lažno ribarjenje**. Kosinski (2024) pojasnjuje, da phishing napadi vključujejo goljufiva e-poštna sporočila, besedila, klice ali spletna mesta, katerih namen je prevarati posameznike, da razkrijejo osebne podatke ali prenesejo zlonamerno programsko opremo. Ti napadi izkoriščajo človeške napake in zaupanje, zato so zelo učinkoviti. V boju proti ribarjenju morajo organizacije uporabljati napredna orodja za odkrivanje groženj in zagotoviti temeljito usposabljanje zaposlenih za učinkovito prepoznavanje in odzivanje na te prevare.

Glavni vzrok za kršitve varnosti podatkov je ribarjenje, ki predstavlja 16 % kršitev in organizacije v povprečju stane **4,76 milijona dolarjev** na kršitev (Kosinski, 2024).

Obstajajo štiri glavne vrste ribarjenja (Forbes, 2024):

- **Goljufanje po e-pošti**: uporaba e-pošte za krajo občutljivih podatkov. Napadalci lahko ciljajo na veliko občinstvo tako, da prevzamejo identiteto uglednih organizacij.
- **Izsiljevanje (Spear phishing):** pošiljanje posameznih e-poštnih sporočil, besedilnih sporočil ali telefonskih klicev z namenom pridobitve dostopa do računalniških sistemov ali občutljivih informacij. Pri uporabi te tehnike napadalci običajno uporabijo podatke iz odprtih podatkovnih zbirk, družabnih medijev ali preteklih kršitev, da okrepijo svojo legitimnost.
- **Kitolov**: osredotoča se na visoko rangirano ali vodilno osebje, vključno s finančniki in izvršnimi direktorji. Napadalci oblikujejo zelo prepričljiva in zelo prilagojena sporočila, da bi od podjetja pridobili občutljive podatke in informacije.
- **Vishing:** telefoniranje ali puščanje glasovne pošte pod pretvezo zanesljivega vira. Cilj je pridobiti bančne račune, izkoristiti osebne podatke in ukrasti denar.

Notranje grožnje so varnostna tveganja, ki izvirajo iz organizacije. To so lahko zaposleni, izvajalci ali poslovni partnerji, ki imajo dostop do sistemov in podatkov organizacije. Te grožnje so lahko še posebej nevarne, ker imajo notranji uporabniki pogosto zakonit dostop do občutljivih informacij in sistemov, zaradi česar je njihove zlonamerne dejavnosti težje odkriti (TechTarget, 2024).

Druga vrsta nevarnosti so napadi DDoS (**Distributed Denial-of-Service**). Njihov cilj je prekiniti normalen promet ciljnega strežnika, storitve ali omrežja tako, da ga preplavijo s poplavo internetnega prometa. To se doseže z uporabo več ogroženih računalniških sistemov kot virov napadalnega prometa. Ko te naprave, ki so pogosto razporejene po vsem svetu, hkrati pošljejo številne zahteve ciljnemu strežniku, porabijo njegovo razpoložljivo pasovno širino in vire, kar povzroči izpad storitev in prepreči dostop do storitve zakonitim uporabnikom (TechTarget, 2024).

Spletne varnostne grožnje so tesno povezane z dejanji hekerjev, ki izkoriščajo ranljivosti v sistemih za različne zlonamerne namene. Po besedah Grubba (2021) se hekerji pogosto razvrščajo glede na njihove namene in metode. Dve osnovni kategoriji sta hekerji belega

klobuka in hekerji črnega klobuka. **White hat hekerji**, znani tudi kot etični hekerji, uporabljajo svoje spretnosti v obrambne namene. Prizadevajo si za zaščito organizacij pred kibernetskimi grožnjami tako, da prepoznajo in odpravijo varnostne ranljivosti, preden jih zlonamerni hekerji lahko izkoristijo. Nasprotno pa **hekerji črnega klobuka** izvajajo nezakonite dejavnosti z zlonamernimi nameni. Varnostne ranljivosti izkoriščajo za osebno korist, kar lahko vključuje krajo podatkov, širjenje zlonamerne programske opreme ali povzročanje motenj.

Ena od ključnih obrambnih ukrepov pred grožnjami informacijski varnosti je uporaba močnih gesel. Močna gesla, ki morajo biti kompleksna in edinstvena za vsak račun, bistveno zmanjšajo tveganje nepooblaščenega dostopa

V preglednici 10.1 je prikazan čas, ki ga heker potrebuje, da z grobo silo pridobi geslo, v skladu z raziskavo, ki jo je izvedla družba Hive Systems (2024).

Preglednica 101Čas, ki ga heker potrebuje, da v letu 2024 z grobo silo pridobi geslo

Število znakov	Samo številke	Male črke	Velike in male črke	Številke, velike in male črke	Številke, velike in male črke, simboli
4	Takoj	Takoj	3 sekunde	6 sekund	9 sekund
5	Takoj	4 sekunde	2 minuti	6 minut	10 minut
6	Takoj	2 minuti	2 uri	6 ur	12 ur
7	4 sekunde	50 minut	4 dni	2 tedna	1 mesec
8	37 sekund	22 ur	8 mesecev	3 leta	7 let
9	6 min	3 tedne	33 let	161 let	479 let
10	1 ura	2 leti	1k let	9k let	33 tisoč let
11	10 ur	44 let	89k let	618k let	2 milijona let
12	4 dni	1k let	4 milijone let	38 milijonov let	164 milijonov let
13	1 mesec	29k let	241 milijonov let	2 milijardi let	11 milijard let
14	1 leto	766k let	12 milijard let	147 milijard let	805 milijard let
15	12 let	19 milijonov let	652 milijard let	9tn let	56tn let
16	119 let	517 milijonov let	33tn let	566tn let	3qd let
17	1k let	13 milijard let	1qd let	35qd let	276qd let
18	11k let	350 milijard let	91qd let	2qn let	19qn let

Vir: Avtor, prilagojeno po Hive Systems (2014).

Razumevanje različnih vrst groženj informacijski varnosti, kot so phishing napadi, zlonamerna programska oprema in napadi DDoS, kaže na ključno potrebo po zanesljivih ukrepih kibernetske varnosti. Te grožnje pomenijo veliko tveganje za osebne podatke, finančne informacije in organizacijsko celovitost. Zaradi tega je nujno sprejeti celovite varnostne strategije. V naslednjem podpoglavju so predstavljeni predlogi za vzdrževanje močne internetne varnosti, vključno s praktičnimi nasveti, ki jih lahko ljudje in institucije uporabijo za zaščito svojih digitalnih virov.

10.2.3. Priporočila za informacijsko varnost

Veliko število varnostnih tveganj, kot sta ribarjenje in zlonamerna programska oprema, je mogoče močno zmanjšati, če jih razumete in izvajate v praksi. Obstaja več najpomembnejših priporočil za zagotavljanje informacijske varnosti (Rubenking & Duffy, 2023; NSW Government, n.d.; Kaspersky, n.d.b):

- **Uporabljajte močna gesla**: za vsak račun ustvarite zapletena gesla, ki vsebujejo črke, številke in simbole. Izogibajte se uporabi podatkov, ki jih je mogoče zlahka uganiti, kot so rojstni dnevi. Za varno shranjevanje in upravljanje gesel uporabite upravitelja gesel.
- Če je mogoče, **omogočite večfaktorsko preverjanje pristnosti (MFA):** dodajte dodatno raven varnosti tako, da za dostop do računov zahtevate dva ali več načinov preverjanja, na primer geslo in enkratno kodo, poslano na vaš telefon.
- **Posodabljajte programsko opremo:** redno posodabljajte operacijske sisteme, brskalnike in aplikacije, da popravite varnostne ranljivosti. Če je mogoče, omogočite samodejne posodobitve, da boste vedno zaščiteni pred najnovejšimi grožnjami.
- **Bodite pozorni na goljufije**: ne klikajte na povezave in ne prenašajte priponk iz neznanih ali sumljivih e-poštnih sporočil. Preverite podatke pošiljatelja in poiščite znake ribarjenja, kot so na primer pravopisne napake ali nujne zahteve po osebnih podatkih.
- **Uporaba varnih povezav**: zagotovite varnost svoje internetne povezave z uporabo virtualnih zasebnih omrežij (VPN) in se izogibajte javnim omrežjem Wi-Fi za občutljive dejavnosti, kot je spletno bančništvo. Preverite, ali je v naslovu URL zapisano "https://", kar pomeni, da gre za varno povezavo.
- **Redno varnostno kopiranje podatkov:** redno varnostno kopirajte podatke na zunanje diske ali v storitve shranjevanja v oblaku. Ta praksa zagotavlja, da lahko

obnovite podatke v primeru okvare strojne opreme, kraje ali napada z izsiljevalsko programsko opremo.

- **Namestite protivirusno programsko opremo:** uporabite ugledno varnostno programsko opremo za odkrivanje, preprečevanje in odstranjevanje zlonamerne programske opreme. Protivirusno programsko opremo posodabljajte in redno preverjajte, ali je vaš sistem čist.
- **Redno nadzorujte račune**: pogosto preverjajte svoje finančne in spletne račune za morebitne nepooblaščene dejavnosti. Nastavite opozorila za nenavadne transakcije in o vsakem sumljivem ravnanju takoj obvestite ponudnika storitev.

Z razumevanjem etičnih posledic ravnanja s podatki in prepoznavanjem obstoječih varnostnih groženj lahko posamezniki in organizacije razvijejo učinkovite strategije za zaščito občutljivih podatkov. Te prakse skupaj zagotavljajo celovitost, zaupnost in razpoložljivost podatkov, od vzpostavitve etičnih smernic in uporabe močnih, edinstvenih gesel do izvajanja naprednih varnostnih ukrepov in obveščanja o morebitnih grožnjah. Z dajanjem prednosti etiki ravnanja s podatki in zanesljivim varnostnim protokolom lahko ustvarimo varnejše in bolj zaupanja vredno digitalno okolje.

LITERATURA

1. Atlan (2023). Data Ethics Unveiled: Principles & Frameworks Explored [available at: https://atlan.com/data-ethics-101/, access May 17, 2024]
2. Basl, J., Sandler, R. & Tiell, S. (2021). Getting from commitment to content in AI and data ethics: Justice and explainability. Atlantic Council [available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/specifying-normative-content/, access May 17, 2024]
3. Cepelak, C. (2023). What is Data Ethics? Datacamp [available at: https://www.datacamp.com/blog/introduction-to-data-ethics, access May 14, 2024]
4. CISCO (n.d.). What Is Information Security? [available at: https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html, access May 20, 2024]

5. Cognizant (n.d.). Data ethics [available at: https://www.cognizant.com/us/en/glossary/data-ethics, access May 14, 2024]

6. Cote (2021). 5 Princples of Data Ethics for Business. Harvard Business School Online [available at: https://online.hbs.edu/blog/post/data-ethics, access May 17, 2024]

7. Cybernews (2022). World Economic Forum finds that 95% of cybersecurity incidents occur due to human error [available at: https://cybernews.com/editorial/world-economic-forum-finds-that-95-of-cybersecurity-incidents-occur-due-to-human-error/, access May 21, 2024]

8. ESET (n.d.). 5 scary data breaches that shook the world [available at: https://www.eset.com/in/about/newsroom/corporate-blog/corporate-blog/eset-5-scary-data-breaches-that-shook-the-world/, access May 21, 2024]

9. Federal Trade Commission (2022). Equifax Data Breach Settlement [available at: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement, access May 20, 2024]

10. Forbes (2024). Cybersecurity Stats: Facts And Figures You Should Know [available at: https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/, access May 24, 2024]

11. Fortinet (n.d.). What Is A Data Breach? [available at: https://www.fortinet.com/resources/cyberglossary/data-breach, access May 21, 2024]

12. Fruhlinger, J. (2020). What is information security? Definition, principles, and jobs. CSO [available at: https://www.csoonline.com/article/568841/what-is-information-security-definition-principles-and-jobs.html, access May 20, 2024]

13. Gov.uk (2020). Data Ethics Framework: glossary and methodology [available at: https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-glossary-and-methodology, access May 14, 2024]

14. Grubb, S. (2021). How Cybersecurity Really Works: A Hands-on Guide for Total Beginners. No starch press.

15. Guzman, L. & Dyer, S. (2020). Ten questions we're asking about ethics, data, and open source research. Amnesty International [available at:

https://citizenevidence.org/2020/11/10/ethics-data-open-source/, access May 17, 2024]

16. Hill, M. & Swinhoe, D. (2022). The 15 biggest data breaches of the 21st century. CSO Online [available at: https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html, access May 21, 2024]

17. Hive Systems (2024). Are Your Passwords in the Green? [available at: https://www.hivesystems.com/blog/are-your-passwords-in-the-green?utm_source=tabletext, access May 24, 2024]

18. Kaspersky (n.d.a). How Data Breaches Happen & How to Prevent Data Leaks [available at: https://www.kaspersky.com/resource-center/definitions/data-breach, access May 21, 2024]

19. Kaspersky (n.d.b). Top 15 internet safety rules and what not to do online [available at: https://www.kaspersky.com/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online, access May 25, 2024]

20. Kerner, S. M. (2022). Colonial Pipeline hack explained: Everything you need to know. TechTarget [available at: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know, access May 20, 2024]

21. Kim, D. & Solomon, M. G. (2018). Fundamentals of Information Systems Security, 3rd Edition. Jones & Bartlett Learning.

22. Knight, M. (2021). What Is Data Ethics?. Dataversity [available at: https://www.dataversity.net/what-are-data-ethics/, access May 14, 2024]

23. Kosinski, M. (2024). What is a phishing attack? IBM [available at: https://www.ibm.com/topics/phishing, access May 24, 2024]

24. McKinsey (2022). Data ethics: What it means and what it takes [available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/data-ethics-what-it-means-and-what-it-takes, access May 14, 2024]

25. National Institute of Standards and Technology (NIST) (n.d.). Information security [available at: https://csrc.nist.gov/glossary/term/information_security, access May 20, 2024]

26. NSW Government (n.d.). 10 Tips for Cyber Security [available at: https://www.digital.nsw.gov.au/sites/default/files/2022-09/top-10-cyber-security-tips.pdf, access May 25, 2024]

27. O'Reilly (2018). Case studies in data ethics [available at: https://www.oreilly.com/content/case-studies-in-data-ethics/, access May 17, 2024]

28. PR Newswire (2018). New Survey Finds Deep Consumer Anxiety over Data Privacy and Security [available at: https://www.prnewswire.com/news-releases/new-survey-finds-deep-consumer-anxiety-over-data-privacy-and-security-300630067.html, access May 20, 2024]

29. Rubenking, N. J. & Duffy, J. (2023). 12 Simple Things You Can Do to Be More Secure Online. PC mag [available at: https://www.pcmag.com/how-to/12-simple-things-you-can-do-to-be-more-secure-online, access May 25, 2024]

30. TechTarget (2024). Top 10 types of information security threats for IT teams [available at: https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams, access May 24, 2024]