10. PODATKOVNA ETIKA I INFORMACIJSKA SIGURNOST

Autor: Dario Šebalj

U eri digitalne transformacije, etičko postupanje i sigurnost podataka pojavili su se kao glavni problemi za pojedince i organizacije. Budući da se svakodnevno prikupljaju i obrađuju goleme količine osobnih i osjetljivih podataka, vrlo je važno osigurati da se tim podacima upravlja na odgovoran i siguran način.

Ovo poglavlje ispituje načela etike podataka, naglašavajući moralna razmatranja i najbolje prakse za rukovanje podacima te istražuje različite prijetnje informacijskoj sigurnosti. Razumijevanjem i rješavanjem ovih problema možemo zaštititi privatnost, održati povjerenje i poticati sigurnije digitalno okruženje.

10.1. Važnost podatkovne etike

Podatkovna etika odnosi se na moralna načela i prakse koji se uzimaju u obzir prilikom prikupljanja, obrade, dijeljenja i korištenja podataka kako bi se osiguralo poštivanje prava pojedinaca, društveno blagostanje i povjerenje. Ona obuhvaća transparentnost, odgovornost, pravednost i privatnost, osiguravajući da su prakse podataka usklađene s etičkim standardima i pravnim okvirima kako bi se spriječila šteta i promicale odgovorne inovacije (Cognizant, n.d.; Gov.uk, 2020; Knight, 2021; McKinsey, 2022; Cepelak , 2023).

U današnjem digitalnom okruženju etičko postupanje podacima ključno je za održavanje povjerenja i osiguranje konkurentske prednosti. McKinsey (2022) je objavio članak o etici podataka u kojem naglašava važnost integriranja etičkih razmatranja u prakse upravljanja podacima. Ističe tri uobičajene pogreške: pretpostavku da je etika podataka nevažna, oslanjanje isključivo na pravne timove i timove za usklađenost te davanje prioriteta kratkoročnim financijskim dobicima u odnosu na etičke prakse. Za rješavanje ovih problema preporučuju nekoliko strategija. Prvo, tvrtke bi trebale uspostaviti jasne, specifične smjernice za etiku podataka. Ove smjernice trebaju služiti kao temelj za etičko upravljanje podacima i pomagati u postavljanju standarda u cijeloj organizaciji. Drugo, formiranje različitih timova za rješavanje problema povezanih s podacima osigurava niz perspektiva i smanjuje rizik od

pristranog donošenja odluka. Treće, uključivanje višeg rukovodstva kao zagovornika inicijativa za etiku podataka ključno je za provođenje tih praksi u cijeloj organizaciji.

Slika 10.1 5C podatkovne etike

Izvor: Autor, prema Atlan (2023).

Slika 10.1 prikazuje 5C podatkovne etike, koju je opisao Atlan (2023), a koja predstavlja bitna načela za etičko rukovanje podacima:

- **Privola:** prije prikupljanja njihovih podataka pribavite informirani, dobrovoljni pristanak pojedinaca, čime se osigurava transparentnost upotrebe podataka.
- **Prikupljanje:** prikupljajte samo podatke koji su potrebni za točno određene svrhe, izbjegavajući prekomjerno prikupljanje podataka.
- **Kontrola:** dopustite pojedincima pristup, pregled i ažuriranje svojih podataka, osiguravajući da imaju kontrolu nad njihovim korištenjem.
- **Povjerljivost:** zaštitite podatke od neovlaštenog pristupa i proboja kroz snažne sigurnosne mjere.
- **Sukladnost:** pridržavajte se zakonskih i regulatornih zahtjeva, provodeći redovite revizije kako biste osigurali stalnu usklađenost.

Slično Atlanovim načelima, Cote (2021) identificira pet temeljnih načela etike podataka koja su ključna za poštivanje poslovnih stručnjaka:

- **Vlasništvo** naglašava da pojedinci zadržavaju vlasništvo nad svojim osobnim podacima. Protuzakonito je i neetično prikupljati osobne podatke bez izričitog pristanka.

Tvrtke moraju dobiti privolu kroz jasne ugovore ili politike digitalne privatnosti, osiguravajući da su korisnici upoznati s praksama prikupljanja podataka i da se slažu s njima.

- **Transparentnost** uključuje jasnu komunikaciju o tome kako će se podaci prikupljati, pohranjivati i koristiti. Poduzeća moraju informirati pojedince o metodama i svrsi prikupljanja podataka. Ova transparentnost gradi povjerenje i omogućuje korisnicima da donose informirane odluke o svojim podacima. Obmanjujuće prakse ili uskraćivanje informacija o korištenju podataka su i neetični i nezakoniti.
- **Privatnost** se fokusira na odgovornost poduzeća da zaštite privatnost osobnih podataka. Čak i uz privolu, osobni podaci ne bi trebali biti javno dostupni bez izričitog dopuštenja pojedinca. Tvrtke moraju primijeniti snažne sigurnosne mjere kako bi zaštitile osobne podatke od neovlaštenog pristupa ili kršenja.
- **Namjera** se odnosi na etičke motive koji stoje iza prikupljanja i korištenja podataka. Podatke treba prikupljati i koristiti u svrhe koje su korisne, a ne štetne za pojedince ili društvo. Etička praksa podataka uključuje korištenje podataka za poboljšanje korisničkog iskustva i poboljšanje usluga bez iskorištavanja ili nanošenja štete.
- **Ishod** razmatra šire utjecaje korištenja podataka na pojedince i društvo. Poduzeća moraju procijeniti moguće posljedice svojih postupaka s podacima i nastojati izbjeći negativne ishode. Ovo načelo naglašava potrebu za etičkim predviđanjem i odgovornošću u donošenju odluka na temelju podataka.

Guzman i Dyer (2020) naglašavaju da etički izazovi vezani uz podatke nisu jednostavni i da im često nedostaju jasna rješenja. Naveli su da postoji razlika između etičkih očekivanja online i offline. Mnogi pojedinci percipiraju oblik iznimnosti u online prostorima, gdje se čini da se tradicionalna etička pravila ne primjenjuju. Ovakav način razmišljanja može dovesti do opravdanja online radnji koje bi se izvan mreže smatrale neetičnim. Autori predlažu etički pristup koji premošćuje oba područja, naglašavajući da etička načela trebaju ostati dosljedna bez obzira na medij.

Rad o etici podataka koji su objavili Basl et al. (2021) istražuje složeni proces prelaska s apstraktnih etičkih načela na konkretna, provediva obećanja u kontekstu velikih podataka i umjetne inteligencije (AI). Zaključili su da je teško, ali vrlo važno napraviti ovaj pomak kako bi se zajamčilo da etičko ponašanje nije samo teoretsko već i praktično i značajno.

Prema O'Reillyju (2018), Princetonov centar za politiku informacijske tehnologije i Centar za ljudske vrijednosti razvili su četiri anonimizirane studije slučaja kako bi potaknuli etički diskurs.

Jedna od studija slučaja istražuje etičke dileme koje postavlja automatizirana aplikacija za zdravstvenu skrb koja koristi AI, a dizajnirana je za pomoć pacijentima s dijabetesom u odrasloj dobi. Ističe potrebu za uravnoteženjem tehnoloških prednosti s etičkim načelima kao što su autonomija, pravednost i odgovornost. Rješavanje ovih etičkih izazova ključno je za odgovornu integraciju umjetne inteligencije u zdravstvu, osiguravajući da ona služi najboljim interesima svih pacijenata. Postoje neka ključna pitanja kojima se treba pozabaviti:

- **Paternalizam:** cilj aplikacije je potaknuti zdravije ponašanje među pacijentima potičući ih na bolje izbore. Iako to može poboljšati zdravstvene ishode, postavlja etička pitanja o autonomiji i paternalizmu. Je li etično da aplikacija utječe na ponašanje pacijenata ili bi pacijenti trebali imati potpunu autonomiju u donošenju zdravstvenih odluka?
- **Pristanak i transparentnost:** aplikacija prikuplja osjetljive zdravstvene podatke kako bi učinkovito funkcionirala. Osiguravanje informiranog pristanka i transparentnosti o prikupljanju, korištenju i dijeljenju podataka je ključno. Pacijenti moraju biti potpuno svjesni koji se podaci prikupljaju, kako će se koristiti i tko će im pristupiti.
- **Privatnost i sigurnost podataka:** rukovanje osjetljivim zdravstvenim podacima zahtijeva stroge mjere privatnosti i sigurnosti. Studija slučaja naglašava potrebu za robusnim protokolima za zaštitu podataka kako bi se podaci o pacijentu zaštitili od kršenja i neovlaštenog pristupa.
- **Odgovornost i odgovornost:** određivanje tko je odgovoran za odluke i radnje aplikacije još je jedan ključni aspekt. Ako aplikacija daje netočnu preporuku koja nepovoljno utječe na zdravlje pacijenta, identificiranje odgovorne strane (programeri, pružatelji zdravstvenih usluga ili sama aplikacija) je složeno, ali neophodno za odgovornost.

Suvremeno upravljanje podacima temelji se na etici podataka, koja jamči poštene, transparentne, odgovorne prakse podataka koje poštuju privatnost. Organizacije mogu poticati odgovorne inovacije, izbjeći pravne zamke i povećati povjerenje pridržavanjem etičkih standarda. Nije samo najbolja praksa, već i zahtjev za održiv i odgovoran rast uključiti jake etičke okvire u prakse upravljanja podacima jer podaci postaju sve bitniji za operacije i donošenje odluka.

Drugi važan aspekt je informacijska sigurnost jer su etika podataka i informacijska sigurnost suštinski povezane. Osiguravanje etičke prakse u vezi s podacima postavlja temelj za snažne mjere sigurnosti informacija. Zaštita podataka od neovlaštenog pristupa, proboja i drugih

sigurnosnih prijetnji ne samo da čuva privatnost i povjerljivost, već također podržava etička načela o kojima se govori u ovom poglavlju.

10.2. Temelji informacijske sigurnosti

Informacijska sigurnost odnosi se na sveobuhvatan skup praksi i načela usmjerenih na zaštitu informacija i informacijskih sustava od neovlaštenog pristupa, korištenja, otkrivanja, ometanja, modifikacije ili uništenja. Osigurava povjerljivost, cjelovitost i dostupnost podataka kroz implementaciju zaštitnih mjera, politika i tehnologija. Ove mjere uključuju kontrolu pristupa, enkripciju, oporavak od katastrofe i usklađenost sa pravnim i regulatornim standardima za ublažavanje rizika i zaštitu od potencijalnih prijetnji (Fruhlinger, 2020; CISCO, n.d., NIST, n.d.).

Informacijska sigurnost je ključna za vjerodostojnost i integritet organizacije u digitalnoj eri. Njezina je važnost naglašena rastućom ovisnošću o digitalnim podacima i porastom kibernetičkih prijetnji koje ugrožavaju osjetljive podatke. Prije svega, informacijska sigurnost štiti osjetljive podatke od neovlaštenog pristupa, provale i krađe. To uključuje osobne podatke, financijske podatke, intelektualno vlasništvo i povjerljive poslovne komunikacije. Kako kibernetički napadi postaju sve sofisticiraniji, rizik od povrede podataka raste, što može dovesti do ozbiljnih financijskih gubitaka i reputacijske štete. Na primjer, curenje podataka Equifaxa 2017. razotkrilo je osobne podatke 147 milijuna ljudi, što je rezultiralo nagodbom do 425 milijuna dolara (Federal Trade Commission, 2022). Takvi incidenti naglašavaju strašne posljedice neadekvatnih mjera sigurnosti informacija.

Nadalje, sigurnost informacija ključna je za zadržavanje povjerenja potrošača. U doba kada je privatnost podataka ključna, korisnici postaju sve zabrinutiji o tome kako se postupa s njihovim podacima. Snažna informacijska sigurnosna arhitektura osigurava da su podaci potrošača sigurni, što potiče lojalnost i povjerenje. Prema anketi IBM-a, 75% kupaca ne bi kupilo proizvode od tvrtke kojoj ne vjeruju da će sačuvati njihove podatke (PR Newswire, 2018). Stoga je informacijska sigurnost i tehnološka potreba i strateški imperativ poslovanja.

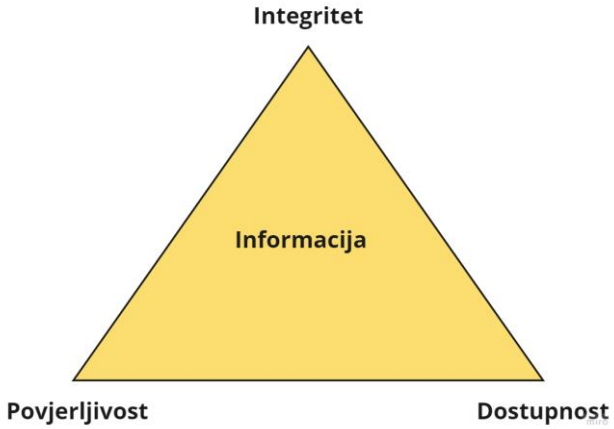
Informacijska sigurnost također je ključna za ublažavanje operativnih smetnji. Kibernetički napadi, kao što je *ransomware*, mogu poremetiti korporativne operacije sprječavajući korisnike da pristupe osnovnim sustavima dok se ne plati otkupnina. *Ransomware* napad na Colonial Pipeline iz 2021. godine, koji je doveo do nestašice goriva u istočnom dijelu SAD-a, primjer je

razornog potencijala takvih prijetnji (Kerner, 2022). Primjenom jakih sigurnosnih mjera organizacije mogu zaštititi svoj operativni kontinuitet i otpornost na takve poremećaje.

Prema Kimu i Solomonu (2018), informacije se smatraju sigurnima ako zadovoljavaju tri glavna načela:

- **Povjerljivost** (eng. *Confidentiality*): osjetljivim informacijama pristupaju samo ovlaštene osobe
- **Integritet** (eng. *Integrity*): podatke mogu mijenjati samo oni koji imaju dopuštenje
- **Dostupnost** (eng. *Availability*): informacije i resursi dostupni su ovlaštenim korisnicima kad god je to potrebno.

Ta se načela često nazivaju CIA trokut, kao što je prikazano na slici 10.2.



Slika 10.2 CIA trokut

Izvor: Autor, prema Kim i Solomon (2018).

U informacijskoj sigurnosti, koncepti rizika, prijetnje i ranjivosti ključni su za razumijevanje i upravljanje sigurnošću. **Rizik** je vjerojatnost da će se nešto loše dogoditi imovini. U informacijskoj sigurnosti rizik je vjerojatnost štetnog događaja koji utječe na povjerljivost, integriteta ili dostupnost informacija. Na primjer, tvrtka može procijeniti rizik kibernetičkog napada na svoju mrežu uzimajući u obzir i vjerojatnost takvog napada i potencijalnu štetu koju bi mogao prouzročiti. **Prijetnja** je svaka radnja koja može uzrokovati štetu informacijskim sustavima ili podacima. Prijetnje mogu biti namjerne, poput kibernetičkog napada hakera, ili nenamjerne, poput prirodnih katastrofa ili ljudske pogreške. **Ranjivost** se odnosi na slabosti ili praznine u obrani sustava koje prijetnje mogu iskoristiti za nanošenje štete. To mogu biti nedostaci u softveru, hardveru, organizacijskim procesima ili ljudskom ponašanju (Kim i Solomon, 2018).

Za učinkovitu zaštitu informacijskih sustava, organizacije moraju razumjeti kako rizici, prijetnje i ranjivosti međusobno djeluju. Na primjer, ranjivost u softveru (kao što je sigurnosni propust) može iskoristiti prijetnja (kao što je haker), što dovodi do povrede podataka, što predstavlja rizik za organizaciju. Prepoznavanjem i ublažavanjem ranjivosti, organizacije mogu smanjiti rizik od prijetnji koje uzrokuju značajnu štetu.

10.2.1. Curenja podataka

Curenja podataka postale su značajna prijetnja u digitalnom dobu, utječući na organizacije u raznim sektorima. Ova kršenja ugrožavaju osjetljive informacije, što dovodi do financijskih gubitaka, štete po ugled i pravnih posljedica. Razumijevanje veličine i utjecaja curenja podataka ključno je za razvoj učinkovitih sigurnosnih strategija za zaštitu od takvih incidenata. Prema Fortinetu (n.d.), curenje podataka podataka "je događaj koji rezultira izlaganjem povjerljivih, privatnih, zaštićenih ili osjetljivih informacija osobi koja nije ovlaštena da im pristupi". Ta se kršenja mogu dogoditi na različite načine (Kaspersky, n.d.a):

- **Slučajni insajder:** zaposlenik nenamjerno pristupa osjetljivim informacijama bez odgovarajućeg ovlaštenja. Na primjer, korištenje računala kolege i pregledavanje povjerljivih datoteka.
- **Zlonamjerni insajder:** pojedinac s ovlaštenim pristupom namjerno zlorabi podatke u štetne svrhe. To može uključivati krađu ili curenje osjetljivih informacija.
- **Izgubljeni ili ukradeni uređaji:** nešifrirani i nezaštićeni uređaji poput prijenosnih računala ili vanjskih diskova koji sadrže osjetljive podatke izgubljeni su ili ukradeni, čineći informacije ranjivima na neovlašteno pristupanje.
- **Zlonamjerni vanjski kriminalci:** hakeri koriste različite metode za probijanje sustava, uključujući napade krađe identiteta, napade brutalnom silom i *malware*. Ovi kibernetički kriminalci iskorištavaju ranjivosti u softveru, mrežama i ponašanju korisnika kako bi dobili pristup osjetljivim podacima.

Prema Kasperskom (n.d.a), uobičajene metode koje se koriste u povredama podataka uključuju ***phishing***, gdje se kibernetički kriminalci lažno predstavljaju kao određeni subjekti kako bi prevarili pojedince da otkriju osjetljive informacije. Druga metoda su **napadi brutalnom silom** (eng. *brute force attacks*)**,** gdje hakeri koriste softver za opetovano pogađanje lozinki, iskorištavajući slabe ili ponovno korištene vjerodajnice kako bi dobili neovlašteni pristup računima. Osim toga, **zlonamjerni softver**, poput špijunskog softvera,

koristi se za infiltraciju u sustave i neotkrivenu krađu podataka. Ove metode bit će objašnjene kasnije u poglavlju.

Ljudske pogreške uzrok su **95%** svih curenja podataka(Cybernews, 2022).

U 21. stoljeću dogodile su se neka od najvećih curenja podataka, čime se naglašava ranjivost digitalnih sustava i kritična potreba za snažnim sigurnosnim mjerama. Prema Hillu i Swinhoeu (2022) i ESET-u (n.d.), neka od najznačajnijih curenja podataka:

- **Yahoo (2013.-2014.):** Yahoo je doživio jedno od najvećih curenja podataka u povijesti, sa svih tri milijarde njegovih korisničkih računa kompromitiranih u 2013. Ovo curenje otkrilo je imena, adrese e-pošte, datume rođenja te sigurnosna pitanja i odgovore. Još jedno curenje u 2014. utjecalo je na 500 milijuna računa, dodatno naglašavajući sigurnosne propuste tvrtke.
- **Marriott International (2018.):** Marriott je objavio curenje podataka koje je utjecalo na približno 500 milijuna gostiju. Hakeri su pristupili Starwood bazi podataka rezervacija gostiju, otkrivajući osobne podatke poput imena, adresa, telefonskih brojeva, e-mail adresa i brojeva putovnica. Ovo curenje bilo je rezultat neovlaštenog pristupa koji datira iz 2014. Ured povjerenika za informacije (ICO), regulatorno tijelo za podatke u Ujedinjenom Kraljevstvu, u konačnici je 2020. kaznio korporaciju s 18,4 milijuna funti jer nije zaštitila privatnost osobnih podataka svojih klijenata.
- **Adult Friend Finder (2016.):** curenje Adult Friend Finder razotkrilo je osobne podatke 412 milijuna računa, uključujući imena, adrese e-pošte i lozinke, od kojih su mnoge bile loše šifrirane. Ovaj je incident izazvao značajnu zabrinutost oko sigurnosnih praksi online platformi koje postupaju s osjetljivim osobnim podacima.
- **MySpace (2013.):** curenje podataka MySpacea, koja se dogodilo 2013., rezultiralo je izlaganjem više od 360 milijuna korisničkih računa. Podaci su uključivali imena, adrese e-pošte i lozinke. Hakeri su kasnije prodali te informacije na dark webu, što je istaknulo ranjivosti u sigurnosnim sustavima platformi društvenih medija tijekom tog vremena.
- **LinkedIn (2021.):** 2021. godine, osobni podaci 700 milijuna korisnika LinkedIna objavljeni su na forumu na dark webu. Haker je koristio tehnike skidanja podataka putem LinkedIn API-ja kako bi dobio adrese e-pošte, telefonske brojeve i druge osobne podatke. Iako ne spada u tradicionalno hakiranje, ovaj je incident izazvao ozbiljnu

zabrinutost u vezi s privatnošću podataka i mogućom zlouporabom podataka za napade društvenog inženjeringa.

- **Equifax (2017.):** ovo curenje razotkrilo je osobne podatke gotovo 148 milijuna Amerikanaca, 15,2 milijuna Britanaca i 19.000 Kanađana. Hakeri su iskoristili ranjivost u sklopu web aplikacije Apache Struts koju Equifax nije uspio zakrpati. Ukradeni podaci uključivali su brojeve socijalnog osiguranja, datume rođenja i adrese, što je dovelo do procijenjenih 1,7 milijardi dolara troškova za Equifax.
- **eBay (2014.):** eBay je otkrio curenje koje je utjecalo na 145 milijuna korisnika. Napad je potekao od kompromitiranih vjerodajnica za prijavu zaposlenika, što je dovelo do otkrivanja imena, adresa e-pošte, fizičkih adresa, telefonskih brojeva i šifriranih zaporki. Ovo kršenje ukazalo je na ranjivosti u pristupnim kontrolama zaposlenika i važnost snažnih mjera provjere autentičnosti.
- **Target (2013.):** curenje podataka koje je utjecalo na više od 41 milijun računa vezanih uz bankovne kartica i kontakt podatke više od 60 milijuna klijenata. Cyberkriminalci pristupili su korisničkim podacima, uključujući imena, telefonske brojeve, adrese e-pošte, brojeve kreditnih i debitnih kartica i šifrirane PIN-ove. Target se suočio sa znatnim pravnim troškovima i troškovima nagodbe, uključujući skupnu tužbu od 10 milijuna dolara i nagodbu u više država od 18,5 milijuna dolara.

Ova curenja podataka pokazuju dalekosežne posljedice kibernetičkih napada i kritičnu potrebu za snažnim praksama kibernetičke sigurnosti. Učeći iz ovih slučajeva visokog profila, organizacije mogu bolje zaštititi svoje podatke, poboljšati svoje sigurnosne protokole i minimizirati rizik od budućih provala. Povrede podataka često su rezultat niza prijetnji u pozadini. Razumijevanje ovih prijetnji ključno je za izgradnju uspješnih mjera informacijske sigurnosti. Kibernetičke prijetnje mogu proizaći iz raznih izvora, uključujući zlonamjerne insajdere, kibernetičke kriminalce pa čak i aktere koje sponzorira država. Osim toga, ranjivosti u sustavima i mrežama mogu se iskoristiti kako bi se neovlašteno pristupilo osjetljivim informacijama.

10.2.2. Prijetnje informacijskoj sigurnosti

Sigurnosna prijetnja zlonamjerna je radnja koja pokušava oštetiti ili ukrasti podatke, ugroziti sustave organizacije ili ugroziti tvrtku u cjelini (TechTarget, 2024). Mnogo je različitih prijetnji informacijskoj sigurnosti koje ozbiljno ugrožavaju dostupnost, cjelovitost i povjerljivost podataka.

Prema Kimu i Solomonu (2018) i Grubbu (2021), **malware** (maliciozni softver) dizajniran je za infiltraciju, oštećenje ili onesposobljavanje računala i mreža. Uobičajene vrste zlonamjernog softvera uključuju viruse, crve, trojance, ransomware i spyware. **Virus** je vrsta zlonamjernog softvera koji se pričvršćuje na legitiman program ili datoteku i širi se na druge programe i datoteke kada se zaraženi softver pokrene. Virusi mogu oštetiti ili izbrisati podatke, poremetiti rad sustava i proširiti se na druge sustave putem privitaka e-pošte, mrežnih veza ili prijenosnih medija. Za razliku od virusa, **crvi** su samostalni zlonamjerni softver koji se može samostalno umnožavati i širiti mrežama bez potrebe za spajanjem na glavni program. Crvi iskorištavaju ranjivosti u operativnim sustavima ili aplikacijama za širenje, često uzrokujući zagušenje mreže i preopterećenje sustava trošenjem propusnosti i resursa. **Trojanac** ili trojanski konj zlonamjerni je softver prerušen u legitimni softver. Korisnici ga instaliraju, vjerujući da je bezopasan ili koristan program. **Ransomware** je vrsta zlonamjernog softvera koji šifrira podatke žrtve, čineći ih nedostupnima dok se napadaču ne plati otkupnina. Ransomware napadi mogu biti razorni, dovesti do značajnog gubitka podataka i operativnih poremećaja ako se ne plati otkupnina ili ako nisu dostupne sigurnosne kopije. **Spyware** je zlonamjerni softver dizajniran za prikupljanje informacija o osobi ili organizaciji bez njihovog znanja. Može prikupljati različite vrste podataka, kao što su informacije o pritisnutim tipkama, navike pregledavanja i osobne informacije, te prenositi te podatke trećoj strani.

Druga vrsta prijetnje je **phishing**. Kosinski (2024) objašnjava da phishing napadi uključuju lažnu e-poštu, SMS-ove, pozive ili web-stranice osmišljene kako bi prevarili pojedince da otkriju osobne podatke ili preuzmu zlonamjerni softver. Ovi napadi iskorištavaju ljudsku pogrešku i povjerenje, što ih čini vrlo učinkovitima. Kako bi se borile protiv krađe identiteta, organizacije moraju koristiti napredne alate za otkrivanje prijetnji i osigurati snažnu obuku zaposlenika kako bi učinkovito prepoznali te prijevare i odgovorili na njih.

Phishing je vodeći uzrok curenja podataka, s udjelom od 16% i košta organizacije u prosjeku 4,76 milijuna dolara po štetnom događaju (Kosinski, 2024).

Četiri su osnovne vrste phishinga (Forbes, 2024):

- **E-mail phishing:** korištenje e-pošte za krađu osjetljivih informacija. Napadači mogu ciljati veliku publiku predstavljajući se kao renomirane organizacije.

- **Spear phishing:** slanje individualiziranih e-poruka, SMS-ova ili telefonskih poziva s namjerom pristupa računalnim sustavima ili osjetljivim informacijama. Kada koriste ovu tehniku, napadači obično koriste podatke iz otvorenih baza podataka, društvenih medija ili ranijih curenja, kako bi pojačali svoju legitimnost.
- **Whaling:** usredotočen je na visoko rangirano ili više osoblje, uključujući referente za financije i izvršne direktore. Napadači šalju vrlo uvjerljive, visoko prilagođene poruke kako bi dobili osjetljive podatke i informacije od poduzeća.
- **Vishing:** telefoniranje ili ostavljanje govorne pošte pod krinkom pouzdanog izvora. Cilj je doći do bankovnih računa, iskoristiti osobne podatke i ukrasti novac.

Insajderske prijetnje su sigurnosni rizici koji potječu unutar organizacije. To mogu biti zaposlenici, izvođači ili poslovni partneri koji imaju pristup sustavima i podacima organizacije. Ove prijetnje mogu biti osobito opasne jer insajderi često imaju legitiman pristup osjetljivim informacijama i sustavima, što otežava otkrivanje njihovih zlonamjernih aktivnosti (TechTarget, 2024).

Druga vrsta prijetnje su napadi **distribuiranog uskraćivanja usluge** (eng. Distributed Denial-of-Service - DDoS). Cilj im je poremetiti normalan promet ciljanog poslužitelja, usluge ili mreže preplavljujući ih internetskim prometom. To se postiže korištenjem više kompromitiranih računalnih sustava kao izvora prometa napada. Kada ti uređaji, često distribuirani globalno, istovremeno šalju brojne zahtjeve meti, troše njegovu dostupnu propusnost i resurse, što dovodi do prekida usluge i sprječava legitimne korisnike da pristupe usluzi (TechTarget, 2024).

Internetske sigurnosne prijetnje usko su povezane s djelovanjem hakera, koji iskorištavaju ranjivosti u sustavima u razne zlonamjerne svrhe. Prema Grubbu (2021), hakeri se često kategoriziraju na temelju njihovih namjera i metoda. Dvije osnovne kategorije su *white hat* hakeri i *black hat* hakeri. **White hat hakeri**, također poznati kao etički hakeri, koriste svoje vještine u obrambene svrhe. Rade na zaštiti organizacija od kibernetičkih prijetnji identificiranjem i popravljanjem sigurnosnih ranjivosti prije nego što ih zlonamjerni hakeri iskoriste. **Black hat hakeri**, nasuprot tome, sudjeluju u ilegalnim aktivnostima sa zlom namjerom. Iskorištavaju sigurnosne propuste za osobnu korist, što može uključivati krađu podataka, širenje zlonamjernog softvera ili izazivanje poremećaja.

Jedna ključna obrana od prijetnji informacijskoj sigurnosti je korištenje jakih lozinki. Jake lozinke, koje bi trebale biti složene i jedinstvene za svaki račun, značajno smanjuju rizik od neovlaštenog pristupa.

Tablica 10.1 pokazuje vrijeme koje je potrebno hakeru da dođe do lozinke, prema istraživanju koje je proveo Hive Systems (2024).

Tablica 10.1 Vrijeme potrebno hakeru da dođe do lozinke u 2024. godini

Broj znakova	Samo brojevi	Mala slova	Velika i mala slova	Brojevi, velika i mala slova	Brojevi, velika i mala slova, simboli
4	Odmah	Odmah	3 sec	6 sec	9 sec
5	Odmah	4 sec	2 min	6 min	10 min
6	Odmah	2 min	2 sata	6 sati	12 sati
7	4 sec	50 min	4 days	2 tjedna	1 mjesec
8	37 sec	22 sata	8 mjeseci	3 god	7 god
9	6 min	3 tjedna	33 god	161 god	479 god
10	1 sat	2 god	1.000 god	9.000 god	33.000 god
11	10 sati	44 god	89.000 god	618.000 god	2 mil. god
12	4 dana	1.000 god	4 mil god	38 mil god	164 mil. god
13	1 mjesec	29.000 god	241 mil god	2mlrd god	11mlrd god
14	1 god	766.000 god	12mlrd god	147mlrd god	805mlrd god
15	12 god	19 mil god	652 mlrd god	9tn god	56tn god
16	119 god	517 mil god	33tn god	566tn god	3qd god
17	1.000 god	13 mlrd god	1qd god	35qd god	276qd god
18	11.000 god	350 mlrd god	91qd god	2qn god	19qn god

Izvor: Autor, prema Hive Systems (2014).

Razumijevanje različitih vrsta prijetnji informacijskoj sigurnosti, kao što su phishing napadi, zlonamjerni softver i DDoS napadi, naglašava kritičnu potrebu za snažnim mjerama kibernetičke sigurnosti. Ove prijetnje predstavljaju značajne rizike za osobne podatke, financijske informacije i organizacijski integritet. Zbog toga postaje neophodno usvojiti sveobuhvatne sigurnosne strategije. Sljedeće potpoglavlje predstavlja prijedloge za održavanje jake internetske sigurnosti, uključujući praktične savjete koje ljudi i institucije mogu koristiti za zaštitu svojih digitalnih izvora.

10.2.3. Smjernice za informacijsku sigurnost

Velik broj sigurnosnih rizika, poput krađe identiteta i zlonamjernog softvera, mogu se uvelike minimizirati njihovim razumijevanjem i primjenom u praksi. Postoji nekoliko najvažnijih preporuka za osiguranje informacijske sigurnosti (Rubenking i Duffy, 2023; NSW Government, n.d.; Kaspersky, n.d.b):

- **Koristite jake lozinke:** koristite složene lozinke kombinirajući slova, brojke i simbole za svaki korisnički račun. Izbjegavajte korištenje informacija koje je lako pogoditi poput rođendana. Koristite upravitelj zaporki za sigurno pohranjivanje i upravljanje zaporkama.
- Ako je moguće, **omogućite multifaktorsku autentikaciju** (MFA): dodajte dodatni sloj sigurnosti zahtijevajući dvije ili više metoda verifikacije za pristup vašim računima, poput lozinke i jednokratnog koda poslanog na vaš telefon.
- **Održavajte softver ažuriranim:** redovito ažurirajte svoje operativne sustave, preglednike i aplikacije kako biste zakrpali sigurnosne propuste. Omogućite automatsko ažuriranje kad god je to moguće kako biste bili sigurni da ste uvijek zaštićeni od najnovijih prijetnji.
- **Budite svjesni phishing prijevara:** nemojte klikati na poveznice ili preuzimati privitke iz nepoznatih ili sumnjivih poruka e-pošte. Provjerite podatke pošiljatelja i potražite znakove krađe identiteta, kao što su pravopisne pogreške ili hitni zahtjevi za osobnim podacima.
- **Koristite sigurne veze:** osigurajte da je vaša internetska veza sigurna korištenjem virtualnih privatnih mreža (VPN) i izbjegavajte javni Wi-Fi za osjetljive aktivnosti poput internetskog bankarstva. U URL adresu uvijek tražite "https://" , što ukazuje na sigurnu vezu.
- **Redovito sigurnosno kopirajte podatke:** redovito sigurnosno kopirajte svoje podatke na vanjske diskove ili usluge pohrane u oblaku. Ova praksa osigurava da možete vratiti svoje podatke u slučaju kvara hardvera, krađe ili napada ransomwarea.
- **Instalirajte antivirusni softver:** koristite renomirani sigurnosni softver za otkrivanje, sprječavanje i uklanjanje zlonamjernog softvera. Redovno ažurirajte antivirusni softver i redovito skenirajte kako biste bili sigurni da je vaš sustav čist.
- **Redovito nadzirite račune:** često provjeravajte svoje financijske račune kako biste na vrijeme uočili bilo kakve neovlaštene aktivnosti. Postavite upozorenja za neobične transakcije i odmah prijavite bilo kakvo sumnjivo ponašanje svom pružatelju usluga.

Razumijevanjem etičkih implikacija rukovanja podacima i prepoznavanjem sigurnosnih prijetnji koje postoje, pojedinci i organizacije mogu razviti učinkovite strategije za zaštitu osjetljivih informacija. Od uspostavljanja etičkih smjernica i korištenja jakih, jedinstvenih zaporki do implementacije naprednih sigurnosnih mjera i informiranja o potencijalnim prijetnjama, ove prakse zajedno osiguravaju integritet, povjerljivost i dostupnost podataka. Davanjem prioriteta

etici podataka i robusnim sigurnosnim protokolima može se stvoriti sigurnije i pouzdanije digitalno okruženje.

REFERENCE

1. Atlan (2023). Data Ethics Unveiled: Principles & Frameworks Explored [dostupno na: https://atlan.com/data-ethics-101/, pristupljeno 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 [dostupno na: https://www.atlanticcouncil.org/in-depth-research-reports/report/specifying-normative-content/, pristupljeno May 17, 2024]
3. Cepelak, C. (2023). What is Data Ethics? Datacamp [dostupno na: https://www.datacamp.com/blog/introduction-to-data-ethics, pristupljeno May 14, 2024]
4. CISCO (n.d.). What Is Information Security? [dostupno na: https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html, pristupljeno May 20, 2024]
5. Cognizant (n.d.). Data ethics [dostupno na: https://www.cognizant.com/us/en/glossary/data-ethics, pristupljeno May 14, 2024]
6. Cote (2021). 5 Princples of Data Ethics for Business. Harvard Business School Online [dostupno na: https://online.hbs.edu/blog/post/data-ethics, pristupljeno May 17, 2024]
7. Cybernews (2022). World Economic Forum finds that 95% of cybersecurity incidents occur due to human error [dostupno na: https://cybernews.com/editorial/world-economic-forum-finds-that-95-of-cybersecurity-incidents-occur-due-to-human-error/, pristupljeno May 21, 2024]
8. ESET (n.d.). 5 scary data breaches that shook the world [dostupno na: https://www.eset.com/in/about/newsroom/corporate-blog/corporate-blog/eset-5-scary-data-breaches-that-shook-the-world/, pristupljeno May 21, 2024]
9. Federal Trade Commission (2022). Equifax Data Breach Settlement [dostupno na: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement, pristupljeno May 20, 2024]

10. Forbes (2024). Cybersecurity Stats: Facts And Figures You Should Know [dostupno na: https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/, pristupljeno May 24, 2024]
11. Fortinet (n.d.). What Is A Data Breach? [dostupno na: https://www.fortinet.com/resources/cyberglossary/data-breach, pristupljeno May 21, 2024]
12. Fruhlinger, J. (2020). What is information security? Definition, principles, and jobs. CSO [dostupno na: https://www.csoonline.com/article/568841/what-is-information-security-definition-principles-and-jobs.html, pristupljeno May 20, 2024]
13. Gov.uk (2020). Data Ethics Framework: glossary and methodology [dostupno na: https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-glossary-and-methodology, pristupljeno 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 [dostupno na: https://citizenevidence.org/2020/11/10/ethics-data-open-source/, pristupljeno May 17, 2024]
16. Hill, M. & Swinhoe, D. (2022). The 15 biggest data breaches of the 21st century. CSO Online [dostupno na: https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html, pristupljeno May 21, 2024]
17. Hive Systems (2024). Are Your Passwords in the Green? [dostupno na: https://www.hivesystems.com/blog/are-your-passwords-in-the-green?utm_source=tabletext, pristupljeno May 24, 2024]
18. Kaspersky (n.d.a). How Data Breaches Happen & How to Prevent Data Leaks [dostupno na: https://www.kaspersky.com/resource-center/definitions/data-breach, pristupljeno May 21, 2024]
19. Kaspersky (n.d.b). Top 15 internet safety rules and what not to do online [dostupno na: https://www.kaspersky.com/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online, pristupljeno May 25, 2024]
20. Kerner, S. M. (2022). Colonial Pipeline hack explained: Everything you need to know. TechTarget [dostupno na: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know, pristupljeno 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 [dostupno na: https://www.dataversity.net/what-are-data-ethics/, pristupljeno May 14, 2024]
23. Kosinski, M. (2024). What is a phishing attack? IBM [dostupno na: https://www.ibm.com/topics/phishing, pristupljeno May 24, 2024]
24. McKinsey (2022). Data ethics: What it means and what it takes [dostupno na: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/data-ethics-what-it-means-and-what-it-takes, pristupljeno May 14, 2024]
25. National Institute of Standards and Technology (NIST) (n.d.). Information security [dostupno na: https://csrc.nist.gov/glossary/term/information_security, pristupljeno May 20, 2024]
26. NSW Government (n.d.). 10 Tips for Cyber Security [dostupno na: https://www.digital.nsw.gov.au/sites/default/files/2022-09/top-10-cyber-security-tips.pdf, pristupljeno May 25, 2024]
27. O'Reilly (2018). Case studies in data ethics [dostupno na: https://www.oreilly.com/content/case-studies-in-data-ethics/, pristupljeno May 17, 2024]
28. PR Newswire (2018). New Survey Finds Deep Consumer Anxiety over Data Privacy and Security [dostupno na: https://www.prnewswire.com/news-releases/new-survey-finds-deep-consumer-anxiety-over-data-privacy-and-security-300630067.html, pristupljeno May 20, 2024]
29. Rubenking, N. J. & Duffy, J. (2023). 12 Simple Things You Can Do to Be More Secure Online. PC mag [dostupno na: https://www.pcmag.com/how-to/12-simple-things-you-can-do-to-be-more-secure-online, pristupljeno May 25, 2024]
30. TechTarget (2024). Top 10 types of information security threats for IT teams [dostupno na: https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams, pristupljeno May 24, 2024]