10. ETIKA PODATAKA I INFORMACIONA 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 ogromne količine ličnih i osetljivih 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 pretnje informacione sigurnosti. Razumevanjem i rešavanjem ovih problema možemo zaštititi privatnost, održati poverenje i podsticati sigurnije digitalno okruženje.

10.1. Važnost etike podataka

Etika podataka odnosi se na moralna načela i prakse koji se uzimaju u obzir prilikom prikupljanja, obrade, deljenja i korišćenja podataka kako bi se osiguralo poštivanje prava pojedinaca, društveno blagostanje i poverenje. Ona obuhvata transparentnost, odgovornost, pravednost i privatnost, osiguravajući da su prakse podataka usklađene s etičkim standardima i pravnim okvirima kako bi se sprečila šteta i promovisale odgovorne inovacije (Cognizant, n.d.; Gov.uk, 2020; Knight, 2021; McKinsey, 2022; Cepelak , 2023).

U današnjem digitalnom okruženju etičko postupanje sa podacima ključno je za održavanje poverenja i osiguranje konkurentske prednosti. McKinsey (2022) je objavio članak o etici podataka u kojem naglašava važnost integrisanja etičkih razmatranja u prakse upravljanja podacima. Ističe tri uobičajene greške: pretpostavku da je etika podataka nevažna, oslanjanje isključivo na pravne timove i timove za usklađenost te davanje prioriteta kratkoročnim finansijskim dobitima u odnosu na etičke prakse. Za rešavanje ovih problema preporučuju nekoliko strategija. Prvo, kompanije bi trebale uspostaviti jasne, specifične smernice za etiku podataka. Ove smernice treba da služe kao temelj za etičko upravljanje podacima i da pomađu u postavljanju standarda u celoj organizaciji. Drugo, formiranje različitih timova za rešavanje problema povezanih s podacima osigurava niz perspektiva i smanjuje rizik od pristrasnog donošenja odluka. Treće, uključivanje višeg rukovodstva kao

zagovornika inicijativa za etiku podataka ključno je za sprovođenje tih praksi u celoj organizaciji.

Slika 10.1 5C etike podataka

Izvor: Autor, prema Atlan (2023).

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

- **Saglasnost:** pre prikupljanja njihovih podataka obezbedite informisanost i dobrovoljni pristanak pojedinaca, čime se osigurava transparentnost upotrebe podataka.
- **Prikupljanje:** prikupljajte samo podatke koji su potrebni za tačno određene svrhe, izbegavajući prekomerno prikupljanje podataka.
- **Kontrola:** dopustite pojedincima pristup, pregled i ažuriranje svojih podataka, osiguravajući da imaju kontrolu nad njihovim korišćenjem.
- **Poverljivost:** zaštitite podatke od neovlašćenog pristupa i proboja kroz snažne sigurnosne mere.
- **Usklađenost:** pridržavajte se zakonskih i regulatornih zahteva, sprovodeći redovne revizije kako biste osigurali stalnu usklađenost.

Slično Atlanovim načelima, Cote (2021) identifikuje pet baznih načela etike podataka koja su ključna za poštovanje poslovnih stručnjaka:

- **Vlasništvo** naglašava da pojedinci zadržavaju vlasništvo nad svojim ličnim podacima. Protivzakonito je i neetično prikupljati lične podatke bez izričitog pristanka. Kompanije moraju dobiti saglasnost 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, čuvati i koristiti. Preduzeća moraju informisati pojedince o metodama i svrsi prikupljanja podataka. Ova transparentnost gradi povjerenje i omogućava korisnicima da donose informisane odluke o svojim podacima. Obmanjujuće prakse ili uskraćivanje informacija o korišćenju podataka su i neetični i nezakoniti.
- **Privatnost** se fokusira na odgovornost preduzeća da zaštite privatnost ličnih podataka. Čak i uz saglasnost, lični podaci ne bi trebali biti javno dostupni bez izričitog dopuštenja pojedinca. Kompanije moraju primeniti snažne sigurnosne mere kako bi se zaštitili lični podaci od neovlašćenog pristupa ili kršenja.
- **Namera** se odnosi na etičke motive koji stoje iza prikupljanja i korišćenja podataka. Podatke treba prikupljati i koristiti u korisne svrhe, a ne štetne za pojedince ili društvo. Praksa etičnosti podataka uključuje korišćenje podataka za poboljšanje korisničkog iskustva i poboljšanje usluga bez iskorišćavanja ili nanošenja štete.
- **Ishod** razmatra šire uticaje korišćenja podataka na pojedince i društvo. Preduzeća moraju proceniti moguće posledice svojih postupaka s podacima i nastojati izbeći negativne ishode. Ovo načelo naglašava potrebu za etičkim predviđanjem i odgovornošću u donošenju odluka na osnovu podataka.

Guzman i Dyer (2020) naglašavaju da etički izazovi vezani uz podatke nisu jednostavni i da im često nedostaju jasna rešenja. Naveli su da postoji razlika između etičkih očekivanja online i offline. Mnogi pojedinci u online prostorima percipiraju izuzetnost, gde se čini da se tradicionalna etička pravila ne primjenjuju. Ovakav način razmišljanja može dovesti do opravdanja online aktivnosti koje bi se izvan mreže smatrale neetičnim. Autori predlažu etički pristup koji premošćuje oba područja, naglašavajući da etička načela trebaju ostati dosledna 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, izvršiva obećanja u kontekstu velikih podataka i veštačke inteligencije (AI). Zaključili su da je teško, ali vrlo važno napraviti ovaj pomak kako bi se garantovalo da etičko ponašanje nije samo teoretsko već i praktično i značajno.

Prema O'Reillyju (2018), Princetonov centar za politiku informacionih tehnologija i Centar za ljudske vrednosti razvili su četiri anonimne studije slučaja kako bi ohrabrili etički diskurs. Jedna od studija slučaja istražuje etičke dileme koje postavlja automatizovana aplikacija za zdravstvenu zaštitu koja koristi AI, a dizajnirana je za pomoć pacijentima s dijabetesom u

odraslom dobu. Ističe potrebu za uravnoteženjem tehnoloških prednosti s etičkim načelima kao što su autonomija, pravednost i odgovornost. Rešavanje ovih etičkih izazova ključno je za odgovornu integraciju veštačke inteligencije u zdravstvu, osiguravajući da ona služi najboljim interesima svih pacijenata. Postoje neka ključna pitanja kojima se treba pozabaviti:

- **Paternalizam:** cilj aplikacije je podstaknuti zdravije ponašanje među pacijentima podstičući ih na bolje izbore. Iako to može poboljšati zdravstvene ishode, postavlja etička pitanja o autonomiji i paternalizmu. Da li je etično da aplikacija utiče na ponašanje pacijenata ili bi pacijenti trebali imati potpunu autonomiju u donošenju zdravstvenih odluka?
- **Pristanak i transparentnost:** aplikacija prikuplja osetljive zdravstvene podatke kako bi učinkovito funkcionisala. Osiguravanje informisanog pristanka i transparentnosti o prikupljanju, korišćenju i deljenju podataka je ključno. Pacijenti moraju biti potpuno svesni koji se podaci prikupljaju, kako će se koristiti i ko će im pristupati.
- **Privatnost i sigurnost podataka:** rukovanje osetljivim zdravstvenim podacima zahteva stroge mere privatnosti i sigurnosti. Studija slučaja naglašava potrebu za robusnim protokolima za zaštitu podataka kako bi se podaci o pacijentu zaštitili od kršenja i neovlašćenog pristupa.
- **Odgovornost i odgovornost:** određivanje ko je odgovoran za odluke i aktivnosti aplikacije još je jedan ključni aspekt. Ako aplikacija daje netačnu preporuku koja nepovoljno utiče na zdravlje pacijenta, identifikovanje odgovorne strane (programeri, davaoci zdravstvenih usluga ili sama aplikacija) je složeno, ali neophodno za odgovornost.

Savremeno upravljanje podacima bazira se na etici podataka, koja garantuje poštene, transparentne i odgovorne prakse podataka koje poštuju privatnost. Organizacije mogu podsticati odgovorne inovacije, izbeći pravne zamke i povećati poverenje pridržavanjem etičkih standarda. Nije samo najbolja praksa, već i zahtev 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 informaciona sigurnost jer su etika podataka i informaciona sigurnost suštinski povezane. Osiguravanje etičke prakse u vezi s podacima postavlja temelj za snažne mere sigurnosti informacija. Zaštita podataka od neovlašćenog pristupa, proboja i drugih sigurnosnih pretnji ne samo da čuva privatnost i poverljivost, već takođe podržava etička načela o kojima se govori u ovom poglavlju.

10.2. Temelji informacione sigurnosti

Informaciona sigurnost odnosi se na sveobuhvatan skup praksi i načela usmerenih na zaštitu informacija i informacionih sistema od neovlašćenog pristupa, korišćenja, otkrivanja, ometanja, modifikacije ili uništenja. Osigurava poverljivost, celovitost i dostupnost podataka kroz implementaciju zaštitnih mera, politika i tehnologija. Ove mere uključuju kontrolu pristupa, enkripciju, oporavak od katastrofe i usklađenost sa pravnim i regulatornim standardima za ublažavanje rizika i zaštitu od potencijalnih pretnji (Fruhlinger, 2020; CISCO, n.d., NIST, n.d.).

Informaciona sigurnost je ključna za verodostojnost i integritet organizacije u digitalnoj eri. Njena važnost je naglašena rastućom zavisnošću od digitalnih podataka i porastom kibernetičkih pretnji koje ugrožavaju osetljive podatke. Pre svega, informaciona sigurnost štiti osetljive podatke od neovlašćenog pristupa, provale i krađe. To uključuje lične podatke, finansijske podatke, intelektualno vlasništvo i poverljive poslovne komunikacije. Kako kibernetički napadi postaju sve sofisticiraniji, rizik od povrede podataka raste, što može dovesti do ozbiljnih finansijskih gubitaka i reputacijske štete. Na primer, curenje podataka Equifaxa 2017. razotkrilo je lične podatke 147 miliona ljudi, što je rezultovalo nagodbom do 425 miliona dolara (Federal Trade Commission, 2022). Takvi incidenti naglašavaju strašne posledice neadekvatnih mera sigurnosti informacija.

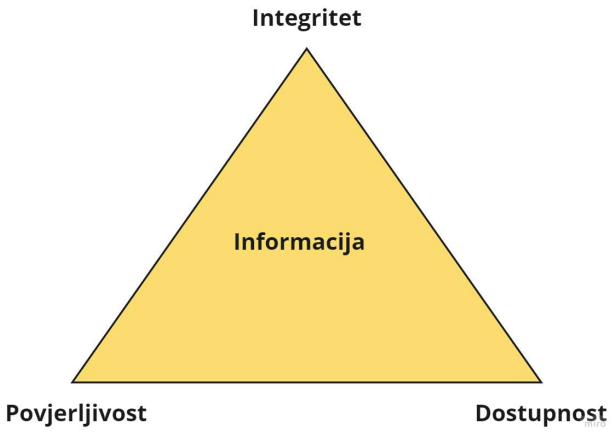
Nadalje, sigurnost informacija ključna je za zadržavanje poverenja potrošača. U doba kada je privatnost podataka ključna, korisnici postaju sve zabrinutiji o tome kako se postupa s njihovim podacima. Snažna informaciono sigurnosna arhitektura osigurava da su podaci potrošača sigurni, što podstiče lojalnost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

Informaciona sigurnost takođe je ključna za ublažavanje operativnih smetnji. Kibernetički napadi, kao što je *ransomware*, mogu poremetiti korporativne operacije sprečavajući korisnike da pristupe osnovnim sistemima dok se ne plati otkupnina. *Ransomware* napad na Colonial Pipeline iz 2021. godine, koji je doveo do nestašice goriva u istočnom delu SAD-a, primer je razornog potencijala takvih pretnji (Kerner, 2022). Primenom jakih sigurnosnih mera 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:

- **Poverljivost** (eng. *Confidentiality*): osetljivim informacijama pristupaju samo ovlašćene osobe;
- **Integritet** (eng. *Integrity*): podatke mogu menjati samo oni koji imaju dopuštenje;
- **Dostupnost** (eng. *Availability*): informacije i resursi dostupni su ovlašćenim korisnicima kad god je to potrebno.

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



Slika 10.2 CIA trougao

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

U informacionoj sigurnosti, koncepti rizika, pretnje i ranjivost ključni su za razumievanje i upravljanje sigurnošću. **Rizik** je verovatnost da će se nešto loše dogoditi imovini. U informacionoj sigurnosti rizik je verovatnost štetnog događaja koji utiče na poverljivost, integritet ili dostupnost informacija. Na primer, kompanija može proceniti rizik kibernetičkog napada na svoju mrežu uzimajući u obzir i verovatnost takvog napada i potencijalnu štetu koju bi mogao prouzrokovati. **Pretnja** je svaka radnja koja može prouzrokovati štetu informacionim sistemima ili podacima. Pretnje mogu biti namerne, poput kibernetičkog napada hakera, ili nenamerne, poput prirodnih katastrofa ili ljudske greške. **Ranjivost** se odnosi na slabosti ili praznine u obrani sistema koje pretnje mogu iskoristiti za nanošenje štete. To mogu biti nedostaci u softveru, hardveru, organizacionim procesima ili ljudskom ponašanju (Kim i Solomon, 2018).

Za učinkovitu zaštitu informacionih sistema, organizacije moraju razumeti kako rizici, pretnje i ranjivost međusobno deluju. Na primer, ranjivost u softveru (kao što je sigurnosni propust) može iskoristiti pretnja (kao što je haker), što dovodi do povrede podataka, što predstavlja rizik za organizaciju. Prepoznavanjem i ublažavanjem ranjivosti, organizacije mogu smanjiti rizik od pretnji koje uzrokuju značajnu štetu.

10.2.1. Curenja podataka

Curenja podataka postale su značajna pretnja u digitalnom dobu, utičući na organizacije u raznim sektorima. Ova kršenja ugrožavaju osetljive informacije, što dovodi do finansijskih gubitaka, štete po ugled i pravnih posledica. Razumevanje veličine i uticaja curenja podataka ključno je za razvoj učinkovitih sigurnosnih strategija za zaštitu od takvih incidenata. Prema Fortinetu (n.d.), curenje podataka "je događaj koji rezultira izlaganjem poverljivih, privatnih, zaštićenih ili osetljivih informacija osobi koja nije ovlašćena da im pristupi". Ta se kršenja mogu dogoditi na različite načine (Kaspersky, n.d.a):

- **Slučajni insajder:** zaposleni nenamerno pristupa osetljivim informacijama bez odgovarajućeg ovlašćenja. Na primer, korišćenje računara kolege i pregledanje poverljivih datoteka.
- **Zlonamerni insajder:** pojedinac s ovlašćenim pristupom namerno zloupotrebljava podatke u štetne svrhe. To može uključivati krađu ili curenje osetljivih informacija.
- **Izgubljeni ili ukradeni uređaji:** nešifrirani i nezaštićeni uređaji poput prenosnih računara ili spoljnih diskova koji sadrže osetljive podatke izgubljeni su ili ukradeni, čineći informacije ranjivima na neovlašćeno pristupanje.
- **Zlonamerni spoljni kriminalci:** hakeri koriste različite metode za probijanje sistema, uključujući napade krađe identiteta, napade brutalnom silom i *malware*. Ovi kibernetički kriminalci iskorišćavaju ranjivosti u softveru, mrežama i ponašanju korisnika kako bi dobili pristup osetljivim podacima.

Prema Kasperskom (n.d.a), uobičajene metode koje se koriste u povredama podataka uključuju ***phishing***, gde se kibernetički kriminalci lažno predstavljaju kao određeni subjekti kako bi prevarili pojedince da otkriju osetljive informacije. Druga metoda su **napadi brutalnom silom** (eng. *brute force attacks*)**,** gde hakeri koriste softver za višestruko pogađanje lozinki, iskorišćavajući slabe ili ponovno korišćene akreditiva kako bi dobili neovlašćeni pristup računima. Osim toga, **zlonamerni softver**, poput špijunskog softvera, koristi se za infiltraciju u sisteme i neotkrivenu krađu podataka. Ove metode biće objašnjene kasnije u poglavlju.

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

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

- **Yahoo (2013.-2014.):** Yahoo je doživeo jedno od najvećih curenja podataka u istoriji, sa svih tri milijarde njegovih korisničkih računa kompromitovanih u 2013. Ovo curenje otkrilo je imena, adrese e-pošte, datume rođenja te sigurnosna pitanja i odgovore. Još jedno curenje u 2014. uticalo je na 500 miliona računa, dodatno naglašavajući sigurnosne propuste kompanije.
- **Marriott International (2018.):** Marriott je objavio curenje podataka koje je uticalo na približno 500 miliona gostiju. Hakeri su pristupili Starwood bazi podataka rezervacija gostiju, otkrivajući lične podatke poput imena, adresa, telefonskih brojeva, e-mail adresa i brojeva pasoša. Ovo curenje bilo je rezultat neovlašćenog pristupa koji datira iz 2014. Kancelarija poverenika za informacije (ICO), regulatorno telo za podatke u Ujedinjenom Kraljevstvu, u konačnici je 2020. kaznila korporaciju s 18,4 miliona funti jer nije zaštitila privatnost ličnih podataka svojih klijenata.
- **Adult Friend Finder (2016.):** curenje Adult Friend Finder razotkrilo je lične podatke 412 miliona računa, uključujući imena, adrese e-pošte i lozinke, od kojih su mnoge bile loše šifrirane. Ovaj incident je izazvao značajnu zabrinutost oko sigurnosnih praksi online platformi koje postupaju s osetljivim ličnim podacima.
- **MySpace (2013.):** curenje podataka MySpacea, koje se dogodilo 2013., rezultiralo je izlaganjem više od 360 miliona korisničkih računa. Podaci su uključivali imena, adrese e-pošte i lozinke. Hakeri su kasnije prodali te informacije na dark webu, što je istaklo ranjivost sigurnosnih sistema platformi društvenih medija tokom tog vremena.
- **LinkedIn (2021.):** 2021. godine, lični podaci 700 miliona 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 lične podatke. Iako ne spada u tradicionalno hakovanje, ovaj je incident izazvao ozbiljnu zabrinutost u vezi s privatnošću podataka i mogućom zloupotrebom podataka za napade društvenog inženjeringa.
- **Equifax (2017.):** ovo curenje razotkrilo je lične podatke gotovo 148 miliona Amerikanaca, 15,2 miliona Britanaca i 19.000 Kanađana. Hakeri su iskoristili ranjivost u sklopu web aplikacije Apache Struts koju Equifax nije uspeo zakrpiti. Ukradeni podaci uključivali su brojeve socijalnog osiguranja, datume rođenja i adrese, što je dovelo do procenjenih 1,7 milijardi dolara troškova za Equifax.

- **eBay (2014.):** eBay je otkrio curenje koje je uticalo na 145 miliona korisnika. Napad je potekao od kompromitovanih akreditiva za prijavu zaposlenih, što je dovelo do otkrivanja imena, adresa e-pošte, fizičkih adresa, telefonskih brojeva i šifriranih lozinki. Ovo kršenje ukazalo je na ranjivost u pristupnim kontrolama zaposlenih i važnost snažnih mera provere autentičnosti.
- **Target (2013.):** curenje podataka koje je uticalo na više od 41 miliona računa vezanih za bankarske kartica i kontakt podatke više od 60 miliona klijenata. Cyber kriminalci 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 grupnu tužbu od 10 miliona dolara i nagodbu u više država od 18,5 miliona dolara.

Ova curenja podataka pokazuju dalekosežne posledice 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 pretnji u pozadini. Razumevanje ovih pretnji ključno je za izgradnju uspešnih mera informacione sigurnosti. Kibernetičke prijetnje mogu proizaći iz raznih izvora, uključujući zlonamerne insajdere, kibernetičke kriminalce pa čak i aktere koje sponzoriše država. Osim toga, ranjivosti u sistemima i mrežama mogu se iskoristiti kako bi se neovlašćeno pristupilo osetljivim informacijama.

10.2.2. Pretnje informacionoj sigurnosti

Sigurnosna pretnja je zlonamerna radnja koja pokušava oštetiti ili ukrasti podatke, ugroziti sisteme organizacije ili ugroziti kompaniju u celini (TechTarget, 2024). Mnogo je različitih pretnji informacionoj sigurnosti koje ozbiljno ugrožavaju dostupnost, celovitost i poverljivost podataka.

Prema Kimu i Solomonu (2018) i Grubbu (2021), **malware** (maliciozni softver) je dizajniran za infiltraciju, oštećenje ili onesposobljavanje računara i mreža. Uobičajene vrste zlonamernog softvera uključuju viruse, crve, trojance, ransomware i spyware. **Virus** je vrsta zlonamernog 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 sistema i proširiti se na druge sisteme putem priloga e-pošte, mrežnih veza ili prenosnih medija. Za razliku od virusa, **crvi** su samostalni zlonamerni softver koji se može samostalno umnožavati i širiti mrežama bez potrebe za spajanjem na glavni

program. Crvi iskorišćavaju ranjivosti u operativnim sistemima ili aplikacijama za širenje, često izazivajući zagušenje mreže i preopterećenje sistema trošenjem propusnosti i resursa. **Trojanac** ili trojanski konj je zlonamerni softver prerušen u legitimni softver. Korisnici ga instaliraju, verujući da je bezopasan ili koristan program. **Ransomware** je vrsta zlonamernog 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 zlonamerni 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 lične informacije, i 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 lične podatke ili preuzmu zlonamerni softver. Ovi napadi iskorišćavaju ljudske greške i poverenje, što ih čini vrlo učinkovitim. Kako bi se borile protiv krađe identiteta, organizacije moraju koristiti napredne alate za otkrivanje pretnji i osigurati snažnu obuku zaposlenih kako bi uspešno prepoznali te prevare i odgovorili na njih.

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

Četiri su osnovne vrste phishinga (Forbes, 2024):

- **E-mail phishing:** korišćenje e-pošte za krađu osjetljivih informacija. Napadači mogu ciljati veliku publiku predstavljajući se kao renomirane organizacije.
- **Spear phishing:** slanje individualizovanih e-poruka, SMS-ova ili telefonskih poziva s namerom pristupa računarskim sistemima ili osetljivim informacijama. Kada koriste ovu tehniku, napadači obično koriste podatke iz otvorenih baza podataka, društvenih medija ili ranijih curenja, kako bi pojačali svoju legitimnost.
- **Whaling:** fokusiran je na visoko rangirano ili više osoblje, uključujući referente za finansije i izvršne direktore. Napadači šalju vrlo uverljive, dobro prilagođene poruke kako bi dobili osetljive podatke i informacije od preduzeća.
- **Vishing:** telefoniranje ili ostavljanje govorne pošte pod maskom pouzdanog izvora. Cilj je doći do bankarskih računa, iskoristiti lične podatke i ukrasti novac.

Insajderske pretnje su sigurnosni rizici koji nastaju unutar organizacije. To mogu biti zaposleni, izvođači ili poslovni partneri koji imaju pristup sistemima i podacima organizacije. Ove pretnje mogu biti posebno opasne jer insajderi često imaju legitiman pristup osetljivim informacijama i sistemima, što otežava otkrivanje njihovih zlonamernih aktivnosti (TechTarget, 2024).

Druga vrsta pretnje su napadi **distribuiranog uskraćivanja usluge** (eng. Distributed Denial-of-Service - DDoS). Cilj im je poremetiti normalan promet ciljanog servera, usluge ili mreže preplavljajući ih internetskim prometom. To se postiže korišćenjem više kompromitovanih računarskih sistema kao izvora napada generisanjem prometa. Kada ti uređaji, često distribuirani globalno, istovremeno šalju brojne zahteve meti, troše njegovu dostupnu propusnost i resurse, što dovodi do prekida usluge i sprečava legitimne korisnike da pristupe usluzi (TechTarget, 2024).

Internetske sigurnosne pretnje usko su povezane s delovanjem hakera, koji iskorišćavaju ranjivosti u sistemima u razne zlonamerne svrhe. Prema Grubbu (2021), hakeri se često kategorizuju na osnovu njihovih namera i metoda. Dve osnovne kategorije su *white hat* hakeri i *black hat* hakeri. **White hat hakeri**, takođe poznati kao etički hakeri, koriste svoje veštine u odbrambene svrhe. Rade na zaštiti organizacija od kibernetičkih pretnji identifikovanjem i popravljanjem sigurnosnie ranjivosti pre nego što ih zlonamerni hakeri iskoriste. **Black hat hakeri**, nasuprot tome, učestvuju u ilegalnim aktivnostima sa zlom namerom. Iskorišćavaju sigurnosne propuste za ličnu korist, što može uključivati krađu podataka, širenje zlonamernog softvera ili izazivanje poremećaja.

Ključna odbrana od pretnji informacione sigurnosti je korišćenje jakih lozinki. Jake lozinke, koje bi trebale biti složene i jedinstvene za svaki račun, značajno smanjuju rizik od neovlašćenog pristupa.

Tabela 10.1 pokazuje vreme koje je potrebno hakeru da dođe do lozinke, prema istraživanju koje je sproveo Hive Systems (2024).

Tabela 10.1 Vreme 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).

Razumevanje različitih vrsta pretnji informacionoj sigurnosti, kao što su phishing napadi, zlonamerni softver i DDoS napadi, naglašava kritičnu potrebu za snažnim merama kibernetičke sigurnosti. Ove pretnje predstavljaju značajne rizike za lične podatke, finansijske informacije i organizacioni integritet. Zbog toga postaje neophodno usvojiti sveobuhvatne sigurnosne strategije. Sledeće potpoglavlje predstavlja predloge za održavanje jake internetske sigurnosti, uključujući praktične savete koje ljudi i institucije mogu koristiti za zaštitu svojih digitalnih izvora.

10.2.3. Smernice za informacionu sigurnost

Velik broj sigurnosnih rizika, poput krađe identiteta i zlonamernog softvera, mogu se u velikoj meri minimizirati njihovim razumevanjem i primenom u praksi. Postoji nekoliko najvažnijih preporuka za osiguranje informacione sigurnosti (Rubenking i Duffy, 2023; NSW Government, n.d.; Kaspersky, n.d.b):

- **Koristite jake lozinke:** koristite složene lozinke kombinujući slova, brojeve i simbole za svaki korisnički račun. Izbegavajte korišćenje informacija koje je lako pogoditi poput rođendana. Koristite menadžer lozinki za sigurno čuvanje i upravljanje lozinkama.
- Ako je moguće, **omogućite multifaktorsku autentikaciju** (MFA): dodajte dodatni sloj sigurnosti zahtevajući dve ili više metoda verifikacije za pristup vašim računima, poput lozinke i jednokratnog koda poslatog na vaš telefon.
- **Održavajte softver ažuriranim:** redovno ažurirajte svoje operativne sisteme, pretraživače i aplikacije kako biste popravili sigurnosne propuste. Omogućite automatsko ažuriranje kad god je to moguće kako biste bili sigurni da ste uvek zaštićeni od najnovijih pretnji.
- **Budite svesni phishing prevara:** nemojte kliktati na linkove ili preuzimati priloge iz nepoznatih ili sumnjivih poruka e-pošte. Proverite podatke pošiljaoca i potražite

znakove krađe identiteta, kao što su pravopisne greške ili hitni zahtevi za ličnim podacima.

- **Koristite sigurne veze:** osigurajte da je vaša internetska veza sigurna korišćenjem virtuelnih privatnih mreža (VPN) i izbegavajte javni Wi-Fi za osetljive aktivnosti poput internetskog bankarstva. U URL adresu uvek tražite "https://" , što ukazuje na sigurnu vezu.
- **Redovno sigurnosno kopirajte podatke:** redovno sigurnosno kopirajte svoje podatke na spoljne diskove ili usluge memorisanja 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, sprečavanje i uklanjanje zlonamernog softvera. Redovno ažurirajte antivirusni softver i redovno skenirajte kako biste bili sigurni da je vaš sistem čist.
- **Redovno nadzirite račune:** često proveravajte svoje finansijske račune kako biste na vreme uočili bilo kakve neovlašćene aktivnosti. Postavite upozorenja za neobične transakcije i odmah prijavite bilo kakvo sumnjivo ponašanje svom provajderu usluga.

Razumevanjem etičkih implikacija rukovanja podacima i prepoznavanjem sigurnosnih pretnji koje postoje, pojedinci i organizacije mogu razviti učinkovite strategije za zaštitu osetljivih informacija. Od uspostavljanja etičkih smernica i korišćenja jakih, jedinstvenih lozinki do implementacije naprednih sigurnosnih mera i informisanja o potencijalnim pretnjama, ove prakse zajedno osiguravaju integritet, poverljivost 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]