Nitra, 2026

Základy kybernetickej bezpečnosti

Cyril Klimeš
Ján Skalka
Lívia Kelebercová
Ján Francisti
František Forgáč
Marek Hrabčák
Peter Švec

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Názov: Základy kybernetickej bezpečnosti
Autori: prof. Ing. Cyril Klimeš, CSc.
RNDr. Ján Skalka, PhD.
RNDr. Lívia Kelebercová, PhD.
Mgr. Ján Francisti, PhD.
Mgr. František Forgáč, PhD.
Mgr. Marek Hrabčák
PaedDr. Peter Švec, Ph.D.

Publikácia vznika v rámci projektu Nitrianske kompetenčné centrum pre kybernetickú bezpečnosť č. 17R05-04-V01-00003, financovaného z Plánu obnovy a odolnosti Slovenskej republiky.

Vydanie: prvé, 2026
ISBN:

Obsah

1 Základné pojmy v kybernetickej bezpečnosti

Kybernetická bezpečnosť patrí medzi základné oblasti modernej informačnej spoločnosti. V súčasnosti je väčšina komunikácie, spracovania údajov, poskytovania služieb aj riadenia procesov viazaná na digitálne technológie. Ľudia používajú počítače, mobilné telefóny, cloudové služby, internetové aplikácie a rôzne sieťové zariadenia prakticky nepretržite. S rastúcou mierou digitalizácie však rastie aj potreba chrániť tieto technológie, údaje a používateľov pred zneužitím, poškodením alebo neoprávneným prístupom.

Základným prostredím, v ktorom sa tieto činnosti odohrávajú, je **kyberpriestor**. Ide o komplexné digitálne prostredie tvorené počítačovými systémami, sieťami, aplikáciami, službami, používateľmi a dátami. Kyberpriestor zahŕňa internet, lokálne a rozľahlé siete, dátové centrá, cloudové platformy, mobilné zariadenia, priemyselné riadiace systémy aj zariadenia internetu vecí. Nie je teda obmedzený iba na webové stránky alebo internet v užšom zmysle slova, ale zahŕňa všetky technológie a vzťahy, ktoré umožňujú elektronickú komunikáciu a spracovanie informácií.

Kyberpriestor sa stal neoddeliteľnou súčasťou každodenného života. Umožňuje ľuďom komunikovať, pracovať, podnikať, študovať, nakupovať, využívať verejné služby a zdieľať informácie v reálnom čase bez ohľadu na geografickú vzdialenosť. Zároveň však vytvára priestor pre nové formy hrozieb, útokov a zneužitia. Práve preto je dôležité poznať základné pojmy kybernetickej bezpečnosti a rozumieť ich vzájomným súvislostiam.

1.1 Kyberpriestor a jeho význam

Kyberpriestor možno charakterizovať ako prostredie, v ktorom prebieha komunikácia, výmena dát, spracovanie informácií a interakcia medzi používateľmi a technickými systémami. Jeho základ tvorí prepojenie technológií, softvéru, sietí a ľudskej činnosti. Nejde teda iba o technický pojem, ale aj o spoločenský, ekonomický a bezpečnostný priestor.

Význam kyberpriestoru spočíva najmä v tom, že umožňuje rýchly prenos informácií, globálnu komunikáciu, vzdialený prístup k službám a efektívne spracovanie veľkého množstva dát. Bez kyberpriestoru by nebolo možné fungovanie elektronickej pošty, internetového bankovníctva, cloudových služieb, sociálnych sietí, videokonferencií, digitálnej štátnej správy ani moderných foriem podnikania.

Na druhej strane ide o prostredie, ktoré je dynamické, otvorené a zraniteľné. Jeho otvorenosť podporuje inovácie, slobodu prístupu k informáciám a medzinárodnú spoluprácu, no zároveň uľahčuje šírenie škodlivého obsahu, malvéru, dezinformácií a ďalších bezpečnostných rizík. Preto je dôležité chápať kyberpriestor nielen ako priestor príležitostí, ale aj ako priestor hrozieb.

1.2 Základné prvky kyberpriestoru

Kyberpriestor tvoria viaceré navzájom prepojené prvky. Medzi najdôležitejšie patria internet, siete, počítačové systémy, aplikácie a služby a samotní používatelia.

1.2.1 Internet

Internet predstavuje najrozsiahlejšiu globálnu sieť, ktorá prepája miliardy zariadení na celom svete. Umožňuje prenos informácií, komunikáciu medzi používateľmi a poskytovanie najrôznejších digitálnych služieb. Internet je základnou infraštruktúrou modernej digitálnej spoločnosti a jeho význam je technologický, ekonomický aj spoločenský.

Internet je často chápaný ako otvorená platforma. Otvorenosť internetu znamená, že používatelia môžu pristupovať k informáciám, využívať služby a vytvárať nový obsah bez zbytočných obmedzení. S tým úzko súvisí princíp sieťovej neutrality. Tento princíp vyjadruje požiadavku, aby poskytovatelia internetového pripojenia nepristupovali rozdielne k rôznym typom dát, neblokovali obsah, nespomaľovali konkrétne služby a neuprednostňovali vlastné alebo partnerské riešenia.

Otvorený internet podporuje slobodu prejavu, vzdelávanie, inovatívne podnikanie a globálnu výmenu poznatkov. Práve vďaka otvorenému charakteru internetu mohli vzniknúť mnohé dnes bežné služby, ako napríklad online encyklopédie, sociálne siete, vývojárske platformy či digitálne vzdelávacie portály. Súčasne však otvorenosť internetu prináša aj riziká, ako sú šírenie dezinformácií, kybernetické útoky, zneužívanie osobných údajov, nevhodný obsah pre deti alebo rastúca digitálna nerovnosť medzi skupinami obyvateľstva.

Kyberpriestor je vymedzený predovšetkým rozsahom internetu. Internet pritom chápeme ako otvorenú platformu. Princíp otvoreného internetu (anglicky open internet) je kľúčový pre slobodné, spravodlivé a inovatívne digitálne prostredie. Jeho dôležitosť spočíva v nasledujúcich aspektoch:

1. **Sloboda prístupu k informáciám –** otvorený internet zaručuje, že každý má rovnaký prístup k informáciám bez ohľadu na to, odkiaľ pochádza alebo aké má finančné možnosti. To podporuje vzdelávanie, informovanosť a demokratickú diskusiu.
2. **Sieťová neutralita –** zásada, že poskytovatelia internetového pripojenia nesmú uprednostňovať alebo blokovať určitý obsah, aplikácie či služby. To chráni menšie firmy a startupy pred diskrimináciou zo strany veľkých hráčov. Sieťová neutralita (*net neutrality*) je základný princíp, ktorý hovorí, že všetky dáta na internete by mali byť prenášané rovnako – bez ohľadu na ich obsah, pôvod alebo cieľ. Inými slovami, poskytovatelia internetového pripojenia nesmú:
    a. blokovať prístup k určitým webovým stránkam alebo službám,
    b. spomaľovať konkrétne typy prevádzky (napr. streamovanie videa),

   c. uprednostňovať vlastné služby alebo služby partnerov (napr. rýchlejší prístup k vlastnému videoportálu).
3. **Podpora inovací** - tvorený internet umožňuje komukoľvek vytvárať nové služby, aplikácie alebo platformy bez nutnosti žiadať o povolenie či platiť za prístup. To viedlo k rozvoju mnohých dnes bežných technológií (napr. YouTube, Wikipedia, GitHub).
4. **Globálne prepojenie –** otvorený internet spája ľudí naprieč kontinentmi, umožňuje medzinárodnú spoluprácu, kultúrnu výmenu a podporuje globálny obchod.
5. **Ochrana ľudských práv –** prístup k otvorenému internetu je často považovaný za súčasť slobody prejavu a práva na informácie. V niektorých krajinách je jeho obmedzenie spojené s cenzúrou a potláčaním opozície.

Vývoj otvoreného internetu je fascinujúcim príbehom technologického pokroku, spoločenských zmien a politických rozhodnutí. Otvorený internet nie je dostupný vo všetkých krajinách sveta. Prístup k internetu a jeho otvorenosť sa výrazne líšia podľa krajiny a závisia od politického režimu, infraštruktúry, ekonomickej situácie a legislatívy.

Aj keď je otvorený internet zásadný pre slobodu a inovácie, **nie je bez rizík.** Internet umožňuje:

1. Šírenie dezinformácií a manipulácie

- Otvára prístup komukoľvek publikovať obsah – vrátane nepravdivých alebo úmyselne zavádzajúcich informácií.
- Sociálne siete a algoritmy môžu tieto informácie šíriť veľmi rýchlo a cielene.

2. Kybernetické útoky a kriminalita

- Otvorený internet uľahčuje šírenie malvéru, phishingových útokov a iných foriem kyberkriminality.
- Útočníci môžu anonymne operovať naprieč štátmi a je ťažké ich vystopovať.

3. Nevhodný obsah pre deti a zraniteľné skupiny

- Bez dostatočnej regulácie je jednoduché naraziť na násilný, pornografický alebo inak škodlivý obsah.
- Rodičia a školy často nemajú dostatočné nástroje na ochranu detí.

4. Strata súkromia

- Mnoho služieb na otvorenom internete zbiera a analyzuje osobné údaje používateľov bez ich plného vedomia.
- Údaje môžu byť predávané tretím stranám alebo zneužité.

5. Digitálna priepasť

- Aj keď je internet otvorený, nie každý má k nemu rovnaký prístup (napr. kvôli cene, infraštruktúre alebo digitálnej gramotnosti).

- To môže prehlbovať sociálne nerovnosti.

Ako možno čeliť týmto rizikám?

- **Regulácia** (napr. GDPR v EÚ, zákony o kyberbezpečnosti).
- **Vzdelávanie** v oblasti mediálnej gramotnosti a bezpečného správania online.
- **Technologické riešenia** – rodičovské zámky, antivírusy, šifrovanie, anonymizačné nástroje.

1.2.2 Siete

Počítačové siete predstavujú základnú infraštruktúru kyberpriestoru. Ich úlohou je prepájať zariadenia, systémy a používateľov tak, aby medzi nimi mohla prebiehať komunikácia a výmena dát. Bez sietí by nebolo možné fungovanie internetu, cloudových služieb, elektronickej komunikácie ani vzdialenej spolupráce.

Siete zabezpečujú nielen samotné prepojenie zariadení, ale aj spoľahlivý a bezpečný prenos informácií. Umožňujú prenos súborov, prevádzku webových stránok, videokonferencie, streamovanie obsahu alebo vzdialený prístup k systémom. Zároveň sú nositeľom mnohých bezpečnostných opatrení, ako sú firewally, virtuálne privátne siete, sieťové segmentovanie, autentifikácia používateľov či detekcia bezpečnostných incidentov.

1.2.3 Počítačové systémy

Počítačové systémy tvoria výpočtovú a riadiacu vrstvu kyberpriestoru. Patria sem servery, pracovné stanice, notebooky, mobilné zariadenia, virtuálne servery, cloudové platformy aj špecializované riadiace zariadenia. Ich hlavnou úlohou je spracovávať, ukladať a poskytovať informácie a služby.

Počítačové systémy vykonávajú výpočty, zabezpečujú chod aplikácií, uchovávajú údaje, spravujú databázy a riadia procesy v reálnom čase. Súčasne zabezpečujú aj rôzne bezpečnostné funkcie, napríklad overovanie identity, správu prístupových práv, šifrovanie údajov alebo evidenciu udalostí. Bez počítačových systémov by siete a internet nemali obsah ani funkčný význam.

1.2.4 Aplikácie a služby

Aplikácie a služby predstavujú používateľskú vrstvu kyberpriestoru. Ide o to, čo používateľ priamo využíva pri práci, komunikácii, vzdelávaní alebo zábave. Patria sem webové stránky, mobilné aplikácie, cloudové kancelárske nástroje, e-mailové služby, komunikačné platformy, internetové obchody, podnikové informačné systémy a mnohé ďalšie riešenia.

Aplikácie a služby dávajú kyberpriestoru praktický význam. Umožňujú používateľom komunikovať, spolupracovať, vytvárať obsah, vykonávať obchodné operácie, pristupovať k dátam a využívať výpočtové zdroje bez potreby priamej práce s infraštruktúrou v pozadí. Zároveň sú častým cieľom útokov, pretože práve cez ne používateľ interaguje so systémom a odovzdáva svoje údaje.

1. Používateľské rozhranie kyberpriestoru

Aplikácie a služby sú tým, čo používatelia priamo využívajú:

- webové prehliadače, e-mailových klientov, kancelárske balíky,
- mobilné aplikácie, sociálne siete, streamovacie platformy,
- podnikové systémy (ERP, CRM, BI nástroje).

2. Poskytovanie digitálnych služieb

Zabezpečujú prístup ku:

- cloudovým úložiskám (napr. OneDrive, Google Drive),
- komunikačným nástrojom (Teams, Zoom, Slack),
- e-commerce (napr. e-shopy, platobné brány),
- e-governmentu (napr. dátové schránky, eRecepty).

3. Automatizácia a inteligencia

Mnohé aplikácie využívajú:

- umelú inteligenciu (napr. prekladače, chatboty, odporúčacie systémy),
- automatizáciu procesov (napr. robotická automatizácia RPA),
- analýzu dát (napr. Power BI, Tableau).

4. Zabezpečenie bezpečnosti a správy

Aplikácie a služby tiež:

- umožňujú správu identít a prístupov (napr. Microsoft Entra, Okta),
- poskytujú bezpečnostné nástroje (napr. antivírusy, firewally ako služba),
- zabezpečujú monitoring a audit (napr. SIEM systémy).

5. Prepájanie ľudí, organizácií a zariadení

Vďaka aplikáciám a službám:

- spolupracujú tímy naprieč kontinentmi,
- firmy poskytujú služby zákazníkom 24/7,
- zariadenia v IoT komunikujú a reagujú v reálnom čase.

1.2.5 Používatelia

Používatelia tvoria centrálny prvok kyberpriestoru. Sú jeho tvorcami, prevádzkovateľmi, správcami aj spotrebiteľmi. Bez používateľov by kyberpriestor nemal praktický význam, pretože práve oni dávajú technológiám účel a obsah.

Tu je prehľad hlavných úloh, ktoré používatelia v kyberpriestore plnia:

1. Spotrebitelia digitálnych služieb

Používatelia využívajú:

- aplikácie a webové stránky (napr. e-mail, sociálne siete, e-shopy),
- cloudové úložiská, streamovacie platformy, vzdelávacie portály,
- digitálnu komunikáciu (chaty, videohovory, fóra).

2. Tvorcovia obsahu

Používatelia vytvárajú:

- texty, obrázky, videa, hudbu,
- príspevky na sociálnych sieťach, blogy, komentáre,
- softvér, webové stránky, digitálne produkty.

3. Správcovia a operátori

Niektorí používatelia majú rolu:

- systémových administrátorov, sieťových technikov, bezpečnostných expertov,
- moderátorov komunít, editorov obsahu, správcov dát,
- vývojárov a analytikov, ktorí udržiavajú a rozvíjajú kyberpriestor.

4. Zodpovední aktéri bezpečnosti

Používatelia ovplyvňujú:

- kybernetickú hygienu (silné heslá, aktualizácie, opatrnosť),
- šírenie alebo zastavenie hrozieb (napr. phishing, malvér),
- dodržiavanie pravidiel a etických zásad v online prostredí.

5. Iniciátori inovácií a zmien

Používatelia:

- prinášajú nové nápady, potreby a spätnú väzbu,
- ovplyvňujú vývoj technológií a služieb,
- formujú trendy a kultúru v kyberpriestore.

6. Spoluúčastníci digitálnej spoločnosti

Používatelia sa podieľajú na:

- digitálnej ekonomike (nakupovanie, podnikanie, práca na diaľku),
- vzdelávaní a výskume,

- politickom a spoločenskom dianí (napr. online petície, diskusie, aktivizmus).

Používatelia pristupujú k digitálnym službám, komunikujú, vytvárajú obsah, spravujú systémy a podieľajú sa na fungovaní digitálnej spoločnosti. Zároveň však predstavujú aj významný bezpečnostný faktor. Ich správanie môže bezpečnosť posilniť, ale aj oslabiť. Slabé heslá, nepozornosť pri phishingu, inštalácia nedôveryhodného softvéru alebo nedodržiavanie bezpečnostných pravidiel patria medzi časté príčiny incidentov.

1.3 Základné pojmy kybernetickej bezpečnosti

Pri štúdiu kybernetickej bezpečnosti je nevyhnutné rozumieť základným pojmom, ktoré sa v tejto oblasti používajú.

1.3.1 Kybernetická hrozba

Kybernetická hrozba je potenciálna udalosť, okolnosť alebo činnosť, ktorá môže spôsobiť škodu informačnému systému, sieti alebo údajom. Hrozba ešte nemusí znamenať, že k incidentu naozaj dôjde, ale predstavuje možnosť vzniku negatívneho následku. Medzi príklady patria útoky hackerov, malvér, phishing, zneužitie slabého hesla alebo konanie nespokojného zamestnanca.

1.3.2 Zraniteľnosť

Zraniteľnosť je slabé miesto v systéme, softvéri, zariadení alebo procese, ktoré môže byť zneužité hrozbou alebo útočníkom. Môže ísť o technickú chybu, nesprávnu konfiguráciu, neaktuálny softvér, slabé heslo alebo nedostatočne nastavené prístupové práva. Zraniteľnosť sama osebe ešte nemusí viesť k incidentu, no vytvára podmienky, ktoré to umožňujú.

1.3.3 Kybernetický útok

Kybernetický útok je úmyselné konanie, ktorého cieľom je zneužiť zraniteľnosť systému. Útočník sa môže snažiť získať citlivé údaje, poškodiť systém, narušiť jeho funkčnosť alebo znemožniť poskytovanie služby. Kybernetické útoky môžu mať podobu phishingu, škodlivého softvéru, neoprávneného prístupu, zahltenia služby alebo manipulácie s údajmi.

1.3.4 Riziko

Riziko v kybernetickej bezpečnosti vyjadruje pravdepodobnosť, že konkrétna hrozba využije zraniteľnosť a spôsobí určitý dopad. Zjednodušene možno povedať, že riziko je výsledkom vzťahu medzi hrozbou, zraniteľnosťou a následkom. Čím vyššia je pravdepodobnosť zneužitia a čím väčší je možný dopad, tým vyššie je riziko.

1.3.5 Kybernetický incident

Kybernetický incident je udalosť, ktorá naruší alebo ohrozí bezpečnosť informačného systému, siete alebo údajov. Môže ísť o únik dát, infekciu malvérom, výpadok služby, neoprávnený prístup alebo inú udalosť, ktorá naruší dôvernosť, integritu alebo dostupnosť informácií.

1.4 Malware a jeho základné druhy

Malware, teda škodlivý softvér, je program alebo súbor vytvorený s cieľom poškodiť systém, zneužiť zariadenie, získať údaje alebo vykonať inú škodlivú činnosť bez vedomia používateľa. Malvér patrí medzi najvýznamnejšie hrozby v kybernetickom priestore a môže mať rôzne podoby.

- **Vírus** je typ malvéru, ktorý sa pripája k súborom a šíri sa ich prenášaním alebo spúšťaním.
- **Červ**, označovaný aj ako worm, sa na rozdiel od vírusu šíri samostatne po sieti bez potreby zásahu používateľa.
- **Trójsky kôň** sa tvári ako legitímny program, no v skutočnosti vykonáva škodlivú činnosť.
- **Ransomvér** zašifruje dáta alebo systém a požaduje výkupné za ich sprístupnenie.
- **Spyware** slúži na sledovanie používateľa, jeho činností a často aj na zhromažďovanie citlivých údajov.

Je dôležité uvedomiť si, že jednotlivé druhy malvéru sa v praxi často kombinujú. Jeden škodlivý program môže mať vlastnosti viacerých kategórií a jeho skutočný účel nemusí byť na prvý pohľad zrejmý.

1.5 Sociálne inžinierstvo a phishing

Kybernetická bezpečnosť nie je založená len na technických opatreniach. Útočníci často útočia na človeka, nie na technológiu. Práve na to slúži sociálne inžinierstvo, teda manipulácia ľudí s cieľom získať informácie, prístupy alebo prinútiť obeť vykonať určitú činnosť.

Útočník môže predstierať, že je pracovník IT oddelenia, nadriadený, kuriér, pracovník banky alebo iná dôveryhodná osoba. Cieľom je presvedčiť obeť, aby prezradila heslo, klikla na škodlivý odkaz, otvorila infikovanú prílohu alebo poskytla citlivé údaje.

Phishing je jednou z najrozšírenejších foriem sociálneho inžinierstva. Ide o podvodnú správu, e-mail, SMS alebo webovú stránku, ktorá sa tvári ako dôveryhodná. Cieľom phishingu je získať prihlasovacie údaje, údaje o platobných kartách, osobné informácie alebo prinútiť používateľa k inému nebezpečnému kroku. Charakteristickým znakom phishingu býva snaha vyvolať pocit naliehavosti, strachu alebo dôvery.

1.6 Autentifikácia, autorizácia a šifrovanie

Medzi základné mechanizmy ochrany v kybernetickej bezpečnosti patrí

- autentifikácia,
- autorizácia a
- šifrovanie.

Autentifikácia znamená overenie identity používateľa. Odpovedá na otázku, kto je daná osoba alebo systém. Môže byť realizovaná heslom, PIN kódom, biometrickým údajom alebo iným faktorom.
Autorizácia nadväzuje na autentifikáciu a určuje, čo môže overený používateľ robiť, ku ktorým údajom má prístup a aké operácie smie vykonávať.

Šifrovanie je proces, pri ktorom sa údaje premieňajú do nečitateľnej podoby tak, aby ich bez príslušného kľúča nebolo možné prečítať. Šifrovanie chráni údaje pri prenose aj pri ukladaní a patrí medzi základné nástroje ochrany dôvernosti.

1.7 Firewall, IDS a IPS

Firewall je bezpečnostný prvok, ktorý kontroluje sieťovú komunikáciu a rozhoduje, ktoré spojenia budú povolené a ktoré zablokované. Jeho úlohou je chrániť zariadenie alebo sieť pred nežiaducou alebo nebezpečnou komunikáciou.

IDS, teda Intrusion Detection System, je systém na detekciu narušenia. Sleduje dianie v sieti alebo v systéme a upozorňuje na možné útoky alebo anomálie.

IPS, teda Intrusion Prevention System, ide ešte ďalej, pretože nielen deteguje, ale dokáže aj aktívne blokovať škodlivú prevádzku alebo nebezpečné správanie.

Tieto technológie tvoria dôležitú súčasť obrany organizácie, pretože pomáhajú identifikovať útoky včas a obmedziť ich dopad.

1.8 Záloha a obnova dát

Záloha je kópia údajov vytvorená pre prípad ich straty, poškodenia alebo zneprístupnenia. Zálohy majú zásadný význam pri poruchách hardvéru, chybách používateľa, kybernetických útokoch alebo prírodných udalostiach. Bez funkčných záloh môže byť obnova dát nemožná alebo veľmi nákladná.

Zálohovanie je jedným zo základných opatrení kybernetickej hygieny. Nestačí však iba vytvárať kópie súborov. Zálohy musia byť pravidelné, bezpečne uložené a overené z hľadiska možnosti obnovy. V opačnom prípade nemusia byť pri incidente použiteľné.

1.9 Cloud a typy cloudových služieb

Cloud predstavuje spôsob poskytovania výpočtových zdrojov, aplikácií a úložiska prostredníctvom internetu. Dáta a služby sa v tomto prípade nenachádzajú priamo v zariadení používateľa, ale na vzdialených serveroch v dátových centrách. Cloud umožňuje flexibilitu, dostupnosť, škálovanie výkonu a jednoduchší prístup k službám.

Cloud môže poskytovať úložisko dát, virtuálne servery, aplikácie, databázy, výpočtový výkon aj bezpečnostné služby. Základné modely cloudových služieb sú tri.

- **Model IaaS**, teda Infrastructure as a Service, poskytuje infraštruktúru, ako sú virtuálne servery, siete a úložiská. Používateľ spravuje operačný systém a aplikácie.
- **Model PaaS**, teda Platform as a Service, poskytuje platformu na vývoj a prevádzku aplikácií, pričom používateľ sa sústreďuje najmä na samotnú aplikáciu.
- **Model SaaS**, teda Software as a Service, ponúka hotové aplikácie dostupné cez internet, ktoré používateľ iba využíva bez potreby starostlivosti o infraštruktúru.

Cloud je významný aj z hľadiska bezpečnosti, pretože prináša nové možnosti ochrany, ale aj nové riziká, napríklad nesprávne nastavenie prístupov, závislosť od poskytovateľa alebo únik údajov.

1.10 Riziká kyberpriestoru

Kyberpriestor prináša množstvo výhod, no zároveň aj široké spektrum rizík. Medzi najčastejšie patria kybernetické útoky, úniky dát, zneužitie osobných údajov, falošné webové stránky, šírenie škodlivého softvéru a narušenie dostupnosti služieb. Osobitnou hrozbou je aj využívanie internetu na šírenie propagandy, dezinformácií, extrémizmu alebo organizovanej trestnej činnosti.

Riziká kyberpriestoru majú technický, spoločenský aj ekonomický rozmer. Napríklad úspešný phishingový útok môže viesť k strate peňazí, úniku údajov, poškodeniu dôvery a prerušeniu prevádzky. Zneužitie osobných údajov môže mať dôsledky pre súkromie jednotlivca aj pre reputáciu organizácie.

Ochrana pred týmito rizikami si vyžaduje kombináciu technických opatrení, právnej regulácie, bezpečnostných procesov a vzdelávania používateľov. Bezpečnosť v kyberpriestore preto nemožno zabezpečiť jedným nástrojom, ale iba komplexným prístupom.

1.11 Informačná bezpečnosť a kybernetická bezpečnosť

Kybernetická bezpečnosť je súbor opatrení, procesov a technológií, ktorých cieľom je chrániť počítače, siete, systémy a údaje pred útokmi, poškodením alebo zneužitím v digitálnom prostredí. Zameriava sa teda predovšetkým na ochranu technických prostriedkov a digitálnych informácií.

Informačná bezpečnosť je širší pojem. Zahŕňa ochranu informácií vo všetkých formách, teda nielen digitálnych, ale aj papierových, ústnych alebo inak zaznamenaných. Kybernetická bezpečnosť je preto súčasťou informačnej bezpečnosti. Ak napríklad organizácia chráni elektronickú databázu, ide o kybernetickú bezpečnosť, no ak chráni aj listinné dokumenty v archíve, ide o širší rámec informačnej bezpečnosti.

1.12 Triáda bezpečnosti

Jedným zo základných teoretických modelov informačnej a kybernetickej bezpečnosti je tzv. **CIA triáda**. Tvoria ju tri základné princípy:

- **Confidentiality -** dôvernosť
- **Integrity –** integrita
- **Availability -** dostupnosť

Dôvernosť znamená, že k informáciám majú prístup iba oprávnené osoby. Chráni sa napríklad šifrovaním, autentifikáciou, riadením prístupových práv a fyzickým zabezpečením zariadení a dokumentov.

Integrita znamená, že informácie sú správne, úplné a neboli neoprávnene zmenené alebo poškodené. Integrita sa zabezpečuje napríklad kontrolnými súčtami, digitálnymi podpismi, verziovaním alebo evidenciou zmien.

Dostupnosť znamená, že informácie a služby sú k dispozícii vtedy, keď ich oprávnený používateľ potrebuje. Dostupnosť sa chráni pomocou záloh, redundancie, spoľahlivej infraštruktúry, ochrany proti výpadkom a opatrení proti útokom typu DDoS.

Tieto tri princípy tvoria základný rámec bezpečnosti a pomáhajú pri hodnotení, navrhovaní a správe ochranných opatrení.

1.13 Otázky a úlohy

1. Čo je kyberpriestor?
a) Fyzický priestor, v ktorom sú uložené servery
b) Izolovaná sieť vojenských systémov
c) Prostredie digitálnej komunikácie, zdieľania informácií a interakcie systémov
d) Súbor bezpečnostných nástrojov na ochranu internetu

2. Ktorý z nasledujúcich príkladov je kybernetická hrozba?
a) Silné heslo
b) Záloha dát
c) Phishingový útok
d) Aktualizovaný operačný systém

3. Čo označuje pojem „zraniteľnosť“ (vulnerability)?
a) Aktívny útok na systém
b) Slabé miesto v systéme, ktoré môže byť zneužité
c) Následok kybernetického incidentu
d) Bezpečnostné opatrenie

4. Z čoho sa skladá riziko v kybernetickej bezpečnosti?
a) Hrozba × incident × ochrana
b) Hrozba × zraniteľnosť × dopad
c) Útok × používateľ × sieť
d) Pravdepodobnosť × náklady × čas

5. Ktorý typ malvéru sa sám šíri po sieti bez zásahu používateľa?
a) Vírus
b) Trójsky kôň
c) Červ (worm)
d) Spyware

6. Aký je rozdiel medzi autentifikáciou a autorizáciou?
a) Autentifikácia určuje práva, autorizácia overuje identitu
b) Autentifikácia overuje identitu, autorizácia určuje práva
c) Oba pojmy majú rovnaký význam
d) Autorizácia sa používa len v cloude

7. Ktorá cloudová služba poskytuje hotové aplikácie dostupné cez internet?
a) IaaS
b) PaaS
c) SaaS
d) VPN

8. Čo znamená princíp sieťovej neutrality (net neutrality)?
a) Internet je dostupný len registrovaným používateľom
b) Dáta sú automaticky šifrované
c) Všetky dáta na internete sú prenášané rovnako – bez diskriminácie
d) Poskytovatelia internetu môžu uprednostňovať vlastné služby

9. Ktoré z nasledujúcich patrí medzi riziká otvoreného internetu?
a) Automatické zálohovanie dát
b) Zvýšený výpočtový výkon
c) Šírenie dezinformácií a kybernetických útokov
d) Lepšia dostupnosť vzdelávania

10. Ktorý princíp CIA triády zabezpečuje, že informácie a systémy sú dostupné vtedy, keď sú potrebné?
a) Confidentiality
b) Integrity
c) Availability
d) Authentication

2 Význam osobných údajov a citlivých informačných aktív

Ochrana osobných údajov je základným ľudským právom. Je dôležitým aspektom v súčasnej dobe digitálnej komunikácie a informačných technológií. Je zakotvené napríklad v Článku 8 Charty základných práv Európskej únie alebo Článku 19 Ústavy Slovenskej republiky.

Článok 8 Charty základných práv Európskej únie

- Každý má právo na ochranu osobných údajov, ktoré sa ho týkajú.
- Osobné údaje musia byť:
  - spracúvané spravodlivo,
  - na konkrétne a zákonné účely,
  - na základe súhlasu dotknutej osoby alebo iného zákonného dôvodu.
- Každý má právo:
  - na prístup k údajom, ktoré sa o ňom spracúvajú,
  - na ich opravu.
- Dodržiavanie týchto pravidiel kontroluje nezávislý orgán.

Článok 19 ods. 3 Ústavy Slovenskej republiky

„Každý má právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe.“ Ide o základné právo, ktoré platí pre každého – bez ohľadu na vek, občianstvo či postavenie. Toto ustanovenie chráni jednotlivca pred tým, aby jeho osobné údaje boli:

- neoprávnene zhromažďované,
- zverejňované bez súhlasu alebo zákonného dôvodu,
- zneužívané na iné než zákonné účely.

Článok 19 ods. 3 je kľúčový najmä pri:

- spracúvaní osobných údajov v informačných systémoch,
- ochrane dát v cloude,
- riešení únikov osobných údajov,
- ochrane pred profilovaním, sledovaním a zneužitím dát.

2.1 Význam osobných údajov

Osobné údaje hrajú v kybernetickej bezpečnosti zásadnú úlohu, pretože predstavujú cenný cieľ pre útočníkov a zároveň kľúčový prvok ochrany súkromia jednotlivcov. Útočníci často cielia na osobné údaje, pretože:

- **Môžu byť speňažené** (napr. na čiernom trhu).

- **Slúži na vydieranie** (napr. únik citlivých informácií).
- **Umožňujú krádež identity** (napr. zneužitie mena, rodného čísla, čísel dokladov).
- **Pomáhajú pri phishingu** (cielené útoky na základe znalosti obete).

V EÚ je ochrana osobných údajov upravená **nariadením GDPR**, ktoré ukladá organizáciám povinnosť chrániť dáta a oznamovať úniky. Porušenie týchto pravidiel môže viesť k **vysokým pokutám** a poškodeniu reputácie.

Identifikácia a klasifikácia osobných údajov je **prvým krokom** pri nastavovaní bezpečnostných opatrení. Pomáha určiť, **kde sú riziká najväčšie** a aké opatrenia treba zaviesť (napr. šifrovanie, prístupové práva). Používatelia a zákazníci očakávajú, že ich dáta budú chránené. Dôvera v organizácii je priamo spojená s tým, **ako zaobchádza s osobnými údajmi** .

Osobné údaje sú v kybernetickej bezpečnosti:

- **Cenným aktívom** , ktoré treba chrániť.
- **Zraniteľným bodom**, ktorý môže byť zneužitý.
- **Základom pre riadenie rizík** a dodržiavanie zákonov.

Osobné údaje patria do kategórie citlivého obsahu. Práca s citlivým obsahom vyžaduje pochopiť ako správne zaobchádzať s citlivými informáciami, vrátane ich šifrovania a bezpečného ukladania, aké sú základné návyky pri práci s informáciami, úskalia a riziká online komunikácie a čo sa chápe pod základnou bezpečnostnou hygienou.

2.2 Čo sú osobné údaje?

Osobné údaje sú akékoľvek údaje týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby. Rozlišujeme teda:

- **identifikovanú osobu** – jednoznačne vieme určiť, o koho ide, na základe určitého údaju
- **identifikovateľnú osobu** – osobu, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby;

2.3 Čo sú citlivé údaje?

Citlivé údaje sú informácie, ktoré vyžadujú osobitnú ochranu kvôli ich povahe a potenciálnemu vplyvu na jednotlivcov alebo organizácie, ak by boli zneužité.

Zakazuje sa spracúvanie osobných údajov, ktoré odhaľujú:

- rasový alebo etnický pôvod,
- politické názory,

- náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách,
- spracúvanie genetických údajov,
- biometrických údajov na individuálnu identifikáciu fyzickej osoby (odtlačky prstov, skeny dúhovky, rozpoznávanie tváre a ďalšie údaje používané na jedinečnú identifikáciu osoby)
- údajov týkajúcich sa zdravia (informácie o zdravotnom stave, lekárskych záznamoch a genetických údajoch)

Osobné údaje, ktoré môžu identifikovať jednotlivcov, ako sú meno, adresa, rodné číslo, telefónne číslo a e-mailová adresa, **finančné údaje** ako bankové účty, kreditné karty, finančné transakcie a ďalšie informácie týkajúce sa finančnej situácie, údaje o **sexuálnej orientácii a živote a duševnom vlastníctve,** ako patenty, obchodné tajomstvo, autorské práva a ďalšie informácie týkajúce sa duševného vlastníctva môže spôsobiť finančnú ujmu, poškodenie povesti alebo osobnú ujmu.

2.4 Online identifikátor

V online priestore sa stretávame aj s online identifikátormi. Sú nimi IP adresa, cookie alebo iné digitálne identifikátory. Pri každom prístupe k internetu oznamujeme aj svoju IP adresu. Je to technologický základ fungovania každej siete.

Podľa GDPR je osobný údaj každá informácia, ktorá umožňuje priame alebo nepriame určenie identity fyzickej osoby. Pri prístupe k internetu môžeme mať

- Dynamickú IP adresu: priradená dočasne poskytovateľom internetu
- Statickú IP adresu: pevne priradená konkrétnemu zariadeniu

V kombinácii s ďalšími informáciami (napr. protokoly o pripojení, prihlasovacie účty) môže umožniť identifikáciu konkrétnej osoby a teda sa považuje za osobný údaj.

Spracúvanie IP adries podlieha zásadám ochrany osobných údajov:

- účelové spracovanie
- minimalizácia dát
- bezpečnostné opatrenia (napr. anonymizácia, šifrovanie)

Webové stránky a služby musia oznamovať spracovanie IP adries (napr. cez cookies, logovanie prístupov). Pre analytiku a štatistiky sa často používajú anonymizované alebo pseudonymizované IP adresy. Únik IP adresy môže v kombinácii s ďalšími údajmi ohroziť súkromie používateľa.

Súbory cookies sú malými dátovými alebo textovými súbormi používanými servermi používateľom navštívených webových stránok za účelom zberu informácií, pričom sú ukladané priamo v zariadení používateľa. Jedná sa najmä o situácie ako:

- uchovávanie informácií o preferenciách používateľa vo vzťahu k navštevovanej webovej stránke (zvolený jazyk, veľkosť písma a pod.),
- overovanie totožnosti používateľa za účelom prihlásenia sa na konkrétnu stránku alebo na uskutočnenie obchodných transakcií online (bez potreby opätovného zadávania informácií),
- analýza efektívnosti a využívania konkrétnej webovej stránky (návštevnosť),
- analýza efektívnosti zobrazovaných reklám na stránke a realizácia cielenej online reklamy a marketingu založenej na predchádzajúcom správaní používateľa.

2.5 Spracúvanie osobných údajov

Prevádzkovateľ systému (firma, organizácia, webová služba) môže spracúvať osobné údaje iba, ak existuje aspoň jedna z týchto právnych základov:

- Súhlas dotknutej osoby
- Zákonný dôvod
- Oprávnený záujem

Súhlas dotknutej osoby

Osoba výslovne súhlasí so spracovaním svojich údajov. Súhlas musí byť

- Dobrovoľný
- konkrétny (na konkrétny účel)
- informovaný (osoba vie, čo sa deje s jej údajmi)
- jednoznačný (napr. potvrdením kliknutím alebo podpisom)

Príklad:

- Používateľ dáva súhlas na zasielanie newslettera
- Používateľ sa registruje na stránke a súhlasí s podmienkami ochrany osobných údajov

Zákonný dôvod

Spracovanie je povolené právnymi predpismi.

Typické prípady:

- mzdové listy zamestnancov
- účtovníctvo a daňové doklady
- zdravotnícka dokumentácia
- povinné evidencie podľa zákona

Príklad:

- Lekár spracúva zdravotné záznamy pacienta, pretože je to zákonná povinnosť

- Zamestnávateľ prihlasuje zamestnanca do sociálnej a zdravotnej poisťovne.

Oprávnený záujem

Prevádzkovateľ má legitímny dôvod spracovať údaje, ktorý neprevažuje práva a slobody dotknutej osoby. Používa sa hlavne v prípadoch, kde:

- sú údaje potrebné pre fungovanie služby
- sú nevyhnutné na ochranu majetku alebo prevádzky

Prevádzkovateľ musí zvážiť záujem osoby vs. svoj záujem (tzv. test rovnováhy alebo proporcionality), či množstvo a rozsah osobných údajov, ktoré sú spracúvané, nie je nadbytočné a či je primerané na dosiahnutie cieľa, ktorým sú oprávnené záujmy prenasledované.
Príklad:

- Web loguje IP adresy návštevníkov na zlepšenie bezpečnosti a prevencie útokov
- Firma zaznamenáva prístup zamestnancov do budovy kvôli bezpečnosti

Len jedna podmienka stačí na to, aby bolo spracovanie legálne

2.6 Čo zahŕňa ochrana citlivých údajov?

Ochrana citlivých údajov zahŕňa stratégie a procesy, ktoré zabezpečujú údaje proti poškodeniu, zneužitiu a strate. Tu sú hlavné aspekty ochrany citlivých údajov:

Šifrovanie: Prevádza dáta do formátu, ktorý je nečitateľný pre neoprávnené osoby. Iba tí, ktorí majú správny dešifrovací kľúč, môžu údaje prečítať.

Kontrola prístupu: Obmedzuje prístup k citlivým dátam iba na oprávnené osoby. To zahŕňa používanie silných hesiel, dvojfaktorovej autentizácie a správy prístupových práv.

Zálohovanie dát: Pravidelné zálohovanie dát zaisťuje, že v prípade straty alebo poškodenia dát je možné ich obnoviť z bezpečnej zálohy.

Monitorovanie a audit : Pravidelné sledovanie a auditovanie prístupov a aktivít v IT systémoch pomáha detekovať a reagovať na podozrivé aktivity.

Dodržiavanie predpisov: Zaisťuje, že firma dodržiava zákony a predpisy týkajúce sa ochrany údajov, ako je GDPR, čo minimalizuje riziko právnych problémov a sankcií.

Školenie zamestnancov: Pravidelné školenie zamestnancov o bezpečnostných postupoch a hrozbách pomáha predchádzať ľudským chybám, ktoré by mohli viesť k úniku dát.

Ochrana citlivých údajov je teda komplexný proces, ktorý zahŕňa technické opatrenia, správu prístupov a vzdelávanie zamestnancov, aby boli dáta chránené pred rôznymi hrozbami.

2.7 Základné návyky pri práci s informáciami

Základné návyky pri práci s informáciami sú kľúčové pre efektívne a bezpečné spracovanie údajov. Tu je niekoľko dôležitých zásad:

Overovanie zdrojov: Vždy overujte, či sú informácie z dôveryhodných a spoľahlivých zdrojov. To pomáha zaistiť, že pracujete s presnými a aktuálnymi dátami.

Organizácia informácií: Udržujte informácie dobre organizované. Používajte priečinky, štítky a ďalšie nástroje pre jednoduché vyhľadávanie a správu dát.

Zálohovanie dát: Pravidelne zálohujte dôležité dáta, aby ste predišli ich strate v prípade technických problémov alebo kybernetických útokov.

Dodržiavanie citačnej etiky: Pri používaní informácií od iných autorov vždy uvádzajte zdroje, aby ste sa vyhli plagiátorstvu a rešpektovali autorské práva.

Bezpečnostné opatrenia: Používajte silné heslá, šifrovanie a ďalšie bezpečnostné opatrenia na ochranu citlivých informácií pred neoprávneným prístupom.

Pravidelné aktualizácie: Udržujte softvér a systémy aktuálne, aby boli chránené proti najnovším bezpečnostným hrozbám.

Etické nakladanie s informáciami: Rešpektujte súkromie a dôvernosť informácií, najmä ak pracujete s osobnými alebo citlivými údajmi.

Dodržiavaním týchto zásad môžete zaistiť, že budete pracovať s informáciami efektívne a bezpečne.

2.8 Úskalia a riziká online komunikácie

Online komunikácia prináša mnoho výhod, ale aj niekoľko rizík a úskalia, na ktoré si treba dať pozor:

Kyberšikana: Útočníci môžu využívať internet a mobilné technológie na zosmiešňovanie, strápňovanie, ohrozovanie alebo zastrašovanie iných osôb.

Sexting: Zdieľanie intímnych fotografií alebo správ môže viesť k ich zneužitiu alebo šíreniu bez súhlasu, čo môže mať vážne osobné a právne dôsledky.

Kybergrooming: Páchatelia môžu nadväzovať kontakt s deťmi a mladistvými s cieľom získať ich dôveru a následne ich zneužiť.

Kyberstalking: Prenasledovanie a obťažovanie osôb prostredníctvom internetu, čo môže viesť k psychickému stresu a pocitu ohrozenia.

Únik osobných údajov: Pri neopatrnom zdieľaní informácií môže dôjsť k úniku citlivých dát, ktoré môžu byť zneužité k podvodom alebo krádeži identity

Falošné informácie a dezinformácie: Internet je plný neoverených a falošných informácií, ktoré môžu viesť k šíreniu dezinformácií a ovplyvňovaniu verejnej mienky.

Digitálna stopa: Každá aktivita na internete zanecháva digitálnu stopu, ktorú je možné sledovať a analyzovať, čo môže ohroziť súkromie užívateľov.

Závislosť na technológiách: Nadmerné používanie online komunikácie môže viesť k závislosti od technológií a negatívne ovplyvniť sociálne interakcie a duševné zdravie.

Je dôležité byť si týchto rizík vedomý a prijímať opatrenia na ich minimalizáciu, napríklad používaním silných hesiel, overovaním zdrojov informácií a dodržiavaním zásad bezpečného správania na internete.

2.9 Citlivé informačné aktíva

Citlivé informačné aktíva sú dáta, informácie alebo systémové zdroje, ktorých neoprávnené zverejnenie, zmena alebo strata môže vážne poškodiť organizáciu alebo jednotlivcov. Ide o hodnotné a chránené informácie, ktoré vyžadujú špeciálnu ochranu. Ich zneužitie môže spôsobiť finančné straty, poškodenie reputácie, porušenie zákonov (napr. GDPR) a ohrozenie bezpečnosti používateľov alebo zamestnancov. Príklady citlivých informačných aktív sú:

Osobné údaje a citlivé údaje

- mená, adresy, rodné čísla, e-maily
- zdravotné záznamy, biometrické údaje, politické názory, náboženstvo

Finančné informácie

- bankové účty, kreditné karty, daňové doklady, faktúry

Obchodné a strategické informácie

- obchodné tajomstvá, interné plány, marketingové stratégie
- cenníky, know-how, výskumné a vývojové projekty

Prístupové údaje a autentifikačné informácie

- heslá, PIN kódy, kľúče, tokeny
- certifikáty a kryptografické kľúče

Technické a infraštruktúrne dáta

- konfigurácie sietí, systémové nastavenia, zdrojový kód
- protokoly prístupov, logy serverov

2.10 Základná bezpečnostná hygiena

Základná bezpečnostná hygiena zahŕňa súbor návykov a postupov, ktoré pomáhajú chrániť vaše zariadenia a dáta pred kybernetickými hrozbami. Tu sú niektoré kľúčové prvky:

Používanie silných hesiel: Vytvárajte zložité heslá, ktoré obsahujú kombináciu písmen, čísel a špeciálnych znakov. Pravidelne ich meňte a nepoužívajte rovnaké heslá pre rôzne účty.

Aktualizácia softvéru: Pravidelne aktualizujte operačné systémy, aplikácie a antivírusové programy, aby boli chránené proti najnovším hrozbám.

Šifrovanie dát: Používajte šifrovanie na ochranu citlivých dát, najmä pri ich prenose cez internet.

Bezpečné zálohovanie: Pravidelne zálohujte dôležité dáta na bezpečné miesto, aby ste ich mohli obnoviť v prípade straty alebo poškodenia.

Overovanie zdrojov: Pri práci s informáciami vždy overujte, či pochádzajú z dôveryhodných zdrojov.

Bezpečné používanie Wi-Fi: Používajte zabezpečené Wi-Fi siete a vyhýbajte sa pripájaniu k verejným nezabezpečeným sieťam

Školenie zamestnancov: Pravidelne školte zamestnancov o bezpečnostných hrozbách a správnych postupoch pri používaní IT systémov.

Dodržiavaním týchto zásad môžete výrazne znížiť riziko kybernetických útokov a chrániť citlivé informácie.

2.11 Anonymizácia a pseudonymizácia

Anonymizácia znamená, že údaje sú spracované tak, aby už nebolo možné identifikovať konkrétnu osobu, ani priamo, ani nepriamo. Osobu nie je možné identifikovať z údajov ani s doplnkovými informáciami. Údaje strácajú charakter osobných údajov, čo znamená, že GDPR sa na ne už nevzťahuje. Používa sa na štatistické, analytické alebo výskumné účely

Príklady

- Prepis mena „Ján Novák“ na „Osoba 1“ v súbore, kde nie je možné spätné spojenie s pôvodnou identitou
- Agregované štatistiky o veku a príjmoch bez menovania konkrétnych ľudí

Pseudonymizácia znamená, že údaje sú spracované tak, že sa identita osoby skrýva za identifikátor, ale je stále možné identitu obnoviť, ak existuje kľúč alebo doplnkové informácie. Údaje stále spadajú pod GDPR. Používa sa na bezpečnejšie spracovanie citlivých údajov

Príklady

- ID číslo alebo hash namiesto mena („Ján Novák“ → „Užívateľ #2457“)
- Kódovanie zdravotných záznamov s uloženým kľúčom, ktorý vie spätne určiť pacienta

2.12 Zodpovednosť prevádzkovateľa

Prevádzkovateľ je zodpovedný za dodržanie zásad ochrany údajov a musí to vedieť preukázať. S ohľadom na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb prevádzkovateľ prijme vhodné technické a organizačné opatrenia, aby zabezpečil a bol schopný preukázať, že spracúvanie sa vykonáva v súlade s týmto nariadením.

V prípade porušenia ochrany osobných údajov prevádzkovateľ bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti dozvedel, oznámi porušenie ochrany osobných údajov dozornému orgánu a v niektorých prípadoch aj dotknutej osobe.

Ktoré incidenty je potrebné oznámiť?

- Porušenie ochrany osobných údajov (personal data breach)
- Porušenie bezpečnosti

Kto musí oznamovať?

- Každý prevádzkovateľ a sprostredkovateľ

Komu je potrebné incident oznámiť?

- Úradu na ochranu osobných údajov, dotknutým osobám (niektoré prípady)

Do kedy je potrebné incident oznámiť?

- Bez zbytočného odkladu, resp. do 72 hodín

2.13 Otázky a úlohy

Situácia	Otázka
1	Firma posiela newsletter všetkým používateľom, ktorí výslovne súhlasili pri registrácii.
2	Web zaznamenáva IP adresy návštevníkov na analytiku a zlepšenie bezpečnosti, bez súhlasu, ale pre oprávnený záujem.
3	Zamestnávateľ bez súhlasu zverejní adresy a telefóny všetkých zamestnancov na internom webe.
4	Lekár spracúva zdravotné záznamy pacienta, pretože je to povinnosť podľa zákona.
5	Obchodná firma predáva databázu emailov a telefónnych čísel zákazníkov tretím stranám bez ich súhlasu.
6	Škola uverejní mená a fotografie žiakov na školskom webe s predchádzajúcim súhlasom rodičov.
7	Firma loguje prístup zamestnancov do budovy na účely bezpečnosti a ochrany majetku.
8	Webová stránka sleduje správanie používateľov a predáva tieto údaje marketingovej agentúre bez informovania používateľov.
9	Sociálna sieť umožňuje používateľom nastaviť, kto vidí ich profilové údaje.
10	Firma uchováva údaje o členoch odborovej organizácie a zverejňuje ich na internom fóre bez súhlasu.

Situácia	Zákonné / Nezákonné	Dôvod
1	ÁNO	Súhlas dotknutej osoby
2	ÁNO	Oprávnený záujem, ak neohrozí práva jednotlivca
3	NIE	Bez súhlasu alebo zákonného dôvodu
4	ÁNO	Zákonný dôvod (zdravotnícka povinnosť)
5	NIE	Bez súhlasu a neexistuje zákonný dôvod
6	ÁNO	Súhlas zákonného zástupcu
7	ÁNO	Oprávnený záujem (bezpečnosť majetku)

8	NIE	Bez súhlasu a informovania používateľov
9	ÁNO	Používateľ sám rozhoduje (súhlas)
10	NIE	Citlivé údaje, bez súhlasu, bez zákonného dôvodu

1. Ochrana osobných údajov je podľa práva EÚ a SR:
a) Základné ľudské právo
b) Dobrovoľné právo len pre občanov EÚ
c) Povinnosť len pre firmy
d) Technické odporúčanie

2. Čo sú osobné údaje podľa GDPR?
a) Údaje o identifikovanej alebo identifikovateľnej fyzickej osobe
b) Len údaje o zamestnancoch
c) Len údaje uložené v databázach
d) Iba citlivé zdravotné údaje

3. Prečo sú osobné údaje častým cieľom kybernetických útokov?
a) Môžu byť zneužité na krádež identity alebo vydieranie
b) Sú verejne dostupné
c) Nemajú žiadnu hodnotu
d) Slúžia len na technické účely

4. Ktoré údaje patria medzi citlivé osobné údaje?
a) Zdravotné a biometrické údaje
b) Meno a priezvisko
c) Názov webovej stránky
d) Názov firmy

5. Ktorý údaj je považovaný za online identifikátor?
a) IP adresa
b) Rodné číslo
c) Podpis osoby
d) Číslo pasu

6. Ktorý z nasledujúcich je právnym základom spracúvania osobných údajov?
a) Súhlas dotknutej osoby
b) Marketingový záujem bez obmedzení
c) Interné rozhodnutie firmy
d) Technická potreba systému

7. Ktoré opatrenie slúži priamo na ochranu citlivých údajov?

a) Šifrovanie dát

b) Zdieľanie hesiel

c) Vypnutie aktualizácií

d) Používanie verejnej Wi-Fi bez ochrany

8. Ktorý návyk patrí medzi základnú bezpečnostnú hygienu?

a) Používanie silných a jedinečných hesiel

b) Používanie jedného hesla všade

c) Ignorovanie aktualizácií

d) Zdieľanie účtov s inými osobami

9. Ktoré tvrdenie o anonymizácii je správne?

a) Údaje už nie je možné spätne priradiť ku konkrétnej osobe

b) Identitu možno obnoviť pomocou kľúča

c) Údaje stále podliehajú GDPR

d) Ide len o zmenu formátu dát

10. Do akej lehoty musí prevádzkovateľ oznámiť porušenie ochrany osobných údajov dozornému orgánu?

a) Najneskôr do 72 hodín

b) Do 24 hodín

c) Do 7 dní

d) Oznamovanie nie je povinné

3 Typy hrozieb, kybernetických útokov a podvodov

V tejto kapitole sa budeme venovať pochopeniu toho, čo sa považuje za bežný kybernetický útok, ako odhaliť potenciálny kybernetický útok a s tým súvisiace metódy podvodov na internete.

3.1 Metódy podvodov na internete

Kybernetické hrozby predstavujú akúkoľvek činnosť alebo softvér, ktorý môže poškodiť počítačové systémy, siete, dáta alebo ohroziť súkromie používateľov. Sú dynamické a neustále sa vyvíjajú, preto je dôležité ich poznať a vedieť sa proti nim chrániť. Existuje mnoho metód podvodov na internete, ktoré útočníci používajú na získanie citlivých informácií alebo finančných prostriedkov.

Jednou z najrozšírenejších hrozieb je škodlivý kód, nazývaný **malware**. Predstavuje softvér alebo súbor inštrukcií vytvorených s cieľom poškodiť počítač, infikovať sieť, získať neoprávnený prístup k dátam alebo sledovať činnosť používateľa bez jeho súhlasu. Škodlivý kód patrí medzi najčastejšie kybernetické hrozby a môže ohroziť osobné počítače, servery, mobilné zariadenia aj celú sieťovú infraštruktúru.

Jedným zo základných typov škodlivého kódu je **počítačový vírus**. Vírus sa šíri pripojením k iným súborom alebo programom a aktivuje sa až po ich spustení používateľom. Po aktivácii môže poškodzovať dáta, meniť systémové súbory alebo šíriť ďalšie formy malvéru. Na rozdiel od vírusu je **počítačový červ** schopný šírenia bez zásahu používateľa. Využíva zraniteľnosti v operačných systémoch a sieťach, čím sa dokáže veľmi rýchlo rozšíriť a spôsobiť výpadky služieb alebo zahltenie siete.

Trójsky kôň je malvér, ktorý sa vydáva za legitímny program alebo súbor, no po jeho spustení vykonáva škodlivé operácie. Trójske kone sa často používajú na inštaláciu ďalších škodlivých programov, napríklad spyware, keyloggerov alebo backdoorov. Na rozdiel od vírusov a červov sa trójske kone samé nešíria; na infikovanie systému je potrebný zásah používateľa, napríklad stiahnutie a otvorenie súboru.

Ransomware je špeciálny typ malvéru, ktorý šifruje súbory v infikovanom zariadení a požaduje výkupné za ich dešifrovanie. Moderný ransomware často kombinuje šifrovanie dát s hrozbou zverejnenia citlivých informácií, čo výrazne zvyšuje tlak na obeť. Tento typ útoku sa zameriava nielen na jednotlivcov, ale aj na organizácie, nemocnice, školy a podniky, pričom môže spôsobiť obrovské finančné a reputačné škody.

Spyware alebo špionážny softvér je navrhnutý na tajné sledovanie aktivít používateľa a získavanie citlivých informácií, ako sú prihlasovacie údaje, osobné dáta alebo návyky pri používaní internetu. Spyware často pracuje bez vedomia používateľa a predstavuje vážne riziko pre súkromie a ochranu osobných údajov.

Adware je softvér, ktorý zobrazuje nevyžiadané reklamy, mení nastavenia prehliadača alebo presmerováva používateľa na reklamné stránky. Aj keď adware nemusí byť priamo škodlivý, často umožňuje sledovanie používateľa a môže slúžiť ako vstupná brána pre vážnejší malvér. Infikované zariadenia môžu byť zneužité ako **boty**, ktoré útočník ovláda na diaľku. Takéto zariadenia sa často stávajú súčasťou **botnetu**, ktorý slúži na koordinované útoky, napríklad DDoS, rozosielanie spamu alebo šírenie malvéru.

Rootkit je mimoriadne nebezpečný typ škodlivého kódu, ktorý umožňuje útočníkovi získať a udržať si skrytý administrátorský prístup k systému. Rootkity dokážu skrývať svoju prítomnosť aj prítomnosť iného malvéru, čím výrazne sťažujú ich odhalenie a odstránenie.

Keylogger je nástroj na zaznamenávanie stlačení klávesnice, ktorý umožňuje útočníkovi získať heslá, prihlasovacie údaje, čísla kariet alebo súkromnú komunikáciu. Keyloggery môžu byť softvérové alebo hardvérové a často sa používajú pri krádeži identity.

Backdoor, alebo zadné vrátka, predstavuje skrytý prístup do systému, ktorý obchádza štandardné bezpečnostné mechanizmy. Útočník môže pomocou backdooru získať opakovaný prístup do systému aj po odstránení pôvodného malvéru. Backdoory sú často inštalované spolu s trójskymi koňmi alebo iným škodlivým softvérom a umožňujú ďalšie útoky.

Celkovo možno konštatovať, že rôzne typy škodlivého kódu sa často kombinujú. Jeden útok môže zahŕňať trójsky kôň, ktorý nainštaluje spyware, keylogger a backdoor, alebo ransomware, ktorý zároveň kradne dáta a šifruje súbory. Preto je dôležité nielen poznať jednotlivé typy malvéru, ale aj rozumieť ich vzájomnému pôsobeniu a rizikám, ktoré predstavujú pre bezpečnosť počítačových systémov a ochranu osobných údajov.

Napríklad útok ransomware WannaCry v roku 2017 zašifroval tisíce počítačov v nemocniciach a firmách po celom svete, čo spôsobilo obrovské finančné straty a dočasnú nedostupnosť kritických služieb. Podobný útok nastal v roku 2025 na spoločnosť Jaguar Land Rover. Firma bola nútená globálne odstaviť na viac ako jeden mesiac výrobu na celom svete. Finančné straty boli obrovské nielen pre firmu ale aj pre sieť subdodávateľov. Strata sa odhaduje na 2 miliardy eur. K útoku sa prihlásila skupina Scattered Lapsus$ Hunters. V roku 2025 sme na Slovensku boli tiež svedkom ransomware útoku na systémy „katastra“.

Ďalšou významnou hrozbou je **phishing**, teda podvodná komunikácia, často prostredníctvom e-mailov, SMS alebo falošných webových stránok, ktorá sa snaží používateľov oklamať a získať

citlivé údaje, ako sú prihlasovacie heslá, čísla platobných kariet alebo osobné údaje. Phishingové útoky môžu viesť ku krádeži identity alebo finančným stratám, pretože útočník tieto údaje následne zneužije. Typickým príkladom je e-mail od „banky“, ktorý vyzýva používateľa, aby potvrdil svoje prihlasovacie údaje na falošnej stránke, ktorá vyzerá úplne autenticky.

Spam, teda nevyžiadané správy, často súvisí s phishingom alebo šírením malvéru a zasahuje do súkromia používateľov. Spam môže byť vo forme e-mailov, SMS správ, chatov alebo reklamných bannerov a často obsahuje odkazy vedúce na podvodné weby. Aj keď sa môže zdať, že ide len o obťažujúce správy, spam je často prvým krokom pri vážnejších útokoch, ako je krádež identity alebo infikovanie zariadení malvérom.

Útoky na internetové služby a webové stránky predstavujú ďalší typ hrozieb. Klasickým príkladom **je Denial of Service (DoS)**, pri ktorom útočník posiela serveru obrovské množstvo požiadaviek, čím znemožní prístup legitímnym používateľom. Jeho rozšírenou formou je **Distributed Denial of Service (DDoS)**, kde útok prichádza z viacerých infikovaných zariadení, ktoré tvoria tzv. botnet. **Botnety** sú siete počítačov alebo zariadení infikovaných škodlivým softvérom, ktoré útočník ovláda na diaľku a môže ich použiť na DDoS útoky, šírenie spamu alebo malvéru, a dokonca na krádež osobných alebo finančných údajov. Takéto útoky môžu spôsobiť výpadky online služieb, stratu finančných prostriedkov a poškodenie reputácie organizácií.

Krádež identity je hrozba, pri ktorej útočník získava osobné údaje obete a zneužíva ich na podvody, neoprávnené transakcie alebo získanie finančného prospechu. Takéto útoky sú často spojené s phishingom alebo únikmi dát zo serverov. Dopady krádeže identity môžu byť veľmi vážne, vrátane finančných strát a poškodenia reputácie obete.

Okrem toho existujú aj ďalšie hrozby, ako napríklad **Man-in-the-Middle (MITM)**, pri ktorom útočník odpočúva alebo manipuluje komunikáciou medzi dvoma stranami, alebo **zero-day exploit**, využívajúci neznáme zraniteľnosti softvéru predtým, než je k dispozícii oprava. Ďalšími hrozbami sú **credential stuffing**, kde útočník automaticky skúša ukradnuté prihlasovacie údaje na viacerých stránkach, a hrozby z vnútra organizácie, tzv. **insider threats**, kde zamestnanci zneužijú prístup k citlivým údajom.

Kybernetické hrozby majú priamy dopad na citlivé údaje používateľov a organizácií, vrátane osobných, zdravotných alebo finančných informácií. Na ochranu pred nimi je potrebné kombinovať technické opatrenia, ako sú

- šifrovanie dát,
- firewally,
- antivírusy,
- zálohovanie a

- bezpečné autentifikačné metódy vrátane dvojfaktorového overenia

s organizačnými opatreniami, napríklad

- školeniami zamestnancov,
- zavedením bezpečnostných politík a
- kontrolou prístupov.

Pochopenie týchto hrozieb je kľúčové, pretože umožňuje používateľom identifikovať riziká, chrániť citlivé údaje a minimalizovať riziko zneužitia. Kybernetická bezpečnosť nie je len technická záležitosť – je to aj otázka zodpovedného správania sa používateľov a vedomého rozhodovania pri práci s digitálnymi systémami.

Prejdime si niektoré z najčastejších podvodov:

Phishing: Útočníci rozosielajú e-maily, ktoré vyzerajú ako od dôveryhodných inštitúcií (napr. bánk alebo úradov), a snažia sa získať citlivé údaje, ako sú heslá alebo čísla kreditných kariet.

Vishing: Telefónny podvod, pri ktorom sa útočníci vydávajú za pracovníkov banky alebo technickej podpory a snažia sa získať citlivé informácie telefonicky.

Smishing: Podobné phishingu, ale namiesto e-mailov sa používajú textové správy. Útočníci posielajú SMS správy s odkazmi na falošné webové stránky, ktoré sa snažia získať osobné údaje.

Falošné webové stránky: Útočníci vytvárajú webové stránky, ktoré vyzerajú ako legitímne, ale sú navrhnuté tak, aby kradli informácie alebo šírili škodlivý softvér.

Podvodné inzeráty: Falošné ponuky na predaj tovaru alebo služieb, ktoré v skutočnosti neexistujú. Kupujúci zaplatí, ale tovar nikdy nedostane.

Romantické podvody: Útočníci nadväzujú vzťahy s obeťami prostredníctvom online zoznamiek alebo sociálnych sietí a následne ich žiadajú o peniaze pod rôznymi zámienkami.

Ransomware: Škodlivý softvér, ktorý zašifruje dáta na počítači obete a požaduje výkupné za ich odblokovanie.

Podvodné investície: Ponuky investícií do neexistujúcich alebo podvodných projektov, ktoré sľubujú vysoké výnosy. Často sú to falošné burzy s akciami alebo krypto zmenárne.

Je dôležité byť obozretný a dodržiavať bezpečnostné opatrenia, aby sa minimalizovalo riziko, že sa stanete obeťou týchto podvodov.

3.2 Ako odhaliť potenciálny kybernetický útok?

Odhalenie potenciálneho kybernetického útoku je kľúčové pre ochranu vašich systémov a údajov. Tu je niekoľko krokov a nástrojov, ktoré vám môžu pomôcť:

Monitorovanie sieťovej prevádzky: Pravidelné sledovanie sieťovej prevádzky môže odhaliť nezvyčajné aktivity, ako sú neobvyklé prenosy dát alebo pripojenia z neznámych IP adries

Systémy detekcie a prevencie prienikov (IDS/IPS): Tieto systémy analyzujú sieťovú prevádzku a hľadajú známe vzory útokov. IDS (Intrusion Detection System) deteguje podozrivé aktivity, zatiaľ čo IPS (Intrusion Prevention System) môže aktívne blokovať útoky.

Bezpečnostné informácie a správa udalostí (SIEM): SIEM nástroje zhromažďujú a analyzujú logy z rôznych zdrojov v reálnom čase, čo umožňuje rýchlo identifikovať a reagovať na bezpečnostné incidenty.

Antivírusové a antimalvérové programy: Pravidelne aktualizované antivírusové a antimalvérové programy dokážu odhaliť a odstrániť škodlivý softvér, ktorý môže byť súčasťou kybernetického útoku.

Penetračné testovanie a etický hacking: Pravidelné testovanie vašich systémov odborníkmi na kybernetickú bezpečnosť môže odhaliť zraniteľnosti, ktoré by mohli byť zneužité útočníkmi

Školenie zamestnancov: Zamestnanci by mali byť pravidelne školení o aktuálnych hrozbách a správnych postupoch pri práci s IT systémami. Informovaní zamestnanci dokážu lepšie rozpoznať phishingové e-maily a iné pokusy o útok.

Zálohovanie dát: Pravidelné zálohovanie dôležitých dát zabezpečuje, že ich môžete obnoviť v prípade útoku, ako je napríklad ransomware.

Dodržiavaním týchto krokov môžete výrazne zvýšiť šance na včasné odhalenie a úspešné odvrátenie kybernetického útoku.

3.3 Prejavy malvéru

Väčšina kategórií malvéru navonok neprejavuje svoju činnosť. Výnimkou je napríklad zobrazená reklama pri **Advéri** alebo informačné okno o výkupnom za údaje pri Ransomvéri.

Výskyt malvéru na zariadení nám môžu potvrdiť nasledujúce symptómy:

- zvýšené využitie procesora,

- pomalá rýchlosť zariadenia alebo webového prehliadača, problémy s pripojením k počítačovej sieti,
- „mrznutie“ operačného systému alebo jeho náhodné reštartovanie,
- výskyt upravených alebo zmazaných súborov, výskyt podivných súborov, programov alebo ikon na ploche,
- spustenie, vypnutie, alebo zmena konfigurácie programov (malvér často zmení nastavenia, resp. vypne antivírusovú ochranu a firewall),
- ňnezvyčajné správanie zariadenia (napr. samočinné otváranie aplikácií),
- e-mailové správy sa posielajú automaticky a bez vedomia používateľa.

3.4 Spôsoby šírenia malvéru

Malvér sa do počítačových systémov a sietí nešíri náhodne, ale prostredníctvom konkrétnych techník, ktoré útočníci cielene využívajú. Cieľom týchto spôsobov šírenia je dostať škodlivý kód do zariadenia obete, často bez jej vedomia, a následne získať prístup k dátam, ovládnuť systém alebo šíriť útok ďalej. Pochopenie spôsobov šírenia malvéru je kľúčové pre jeho včasnú identifikáciu a prevenciu.

Jedným z najčastejších spôsobov šírenia malvéru je **e-mailová komunikácia**. Útočníci rozosielajú e-maily s infikovanými prílohami alebo odkazmi na škodlivé webové stránky. Tieto správy sú často súčasťou phishingových kampaní a snažia sa používateľa presvedčiť, aby otvoril prílohu alebo klikol na odkaz, napríklad pod zámienkou faktúry, upozornenia od banky alebo dôležitej správy od zamestnávateľa. Po otvorení prílohy sa malvér aktivuje a infikuje systém.

Ďalším rozšíreným spôsobom je **sťahovanie softvéru z nedôveryhodných zdrojov**. Nelegálne kópie programov, cracky, generátory licencií alebo softvér z neoficiálnych stránok často obsahujú trójske kone alebo iný škodlivý kód. Používateľ má pocit, že si inštaluje legitímny program, no v skutočnosti si do systému zavádza malvér.

Malvér sa často šíri aj prostredníctvom **infikovaných webových stránok**. Stačí navštíviť škodlivú alebo kompromitovanú stránku a v prípade neaktualizovaného prehliadača alebo operačného systému môže dôjsť k tzv. drive-by downloadu, pri ktorom sa malvér stiahne a spustí automaticky bez vedomia používateľa. Tento spôsob šírenia využíva zraniteľnosti v softvéri.

Významným spôsobom šírenia je aj **využívanie zraniteľností operačných systémov a aplikácií**. Červy a iné typy malvéru aktívne vyhľadávajú zariadenia s neaktualizovaným softvérom a následne ich infikujú bez potreby zásahu používateľa. Práve preto sú pravidelné aktualizácie a bezpečnostné záplaty mimoriadne dôležité.

Ďalším rizikovým spôsobom šírenia malvéru sú **vymeniteľné pamäťové médiá**, najmä USB kľúče alebo externé disky. Ak je takéto zariadenie infikované a pripojené k počítaču, malvér sa môže automaticky spustiť alebo sa do systému dostať pri otvorení súborov. Tento spôsob šírenia je obzvlášť nebezpečný v školách, firmách alebo verejných inštitúciách, kde sa zariadenia často zdieľajú.

Malvér sa môže šíriť aj prostredníctvom **sietí a zdieľaných zdrojov**. V podnikových alebo školských sieťach sa môže škodlivý kód šíriť z jedného infikovaného počítača na ďalšie zariadenia, najmä ak nie sú správne nastavené prístupové práva alebo bezpečnostné pravidlá. Tento spôsob je typický pre červy a botnety.

V posledných rokoch sa čoraz častejšie využíva aj **sociálne inžinierstvo**, teda manipulácia používateľov. Útočníci zneužívajú dôverčivosť, strach alebo zvedavosť obete a presvedčia ju, aby si sama nainštalovala škodlivý program, napríklad falošnú aktualizáciu, bezpečnostný nástroj alebo aplikáciu. Tento spôsob šírenia je veľmi účinný, pretože obchádza technické ochranné mechanizmy.

Špecifickým spôsobom šírenia malvéru je aj **kompromitácia legitímneho softvéru alebo aktualizácií**, pri ktorej útočníci vložia škodlivý kód priamo do inak dôveryhodného programu. Používateľ si tak stiahne oficiálnu aktualizáciu alebo aplikáciu, ktorá však obsahuje malvér. Tento typ útoku je známy ako útok na dodávateľský reťazec.

Na záver možno konštatovať, že malvér sa šíri kombináciou technických zraniteľností a ľudských chýb. Účinná ochrana preto vyžaduje nielen technické opatrenia, ako sú aktualizácie, antivírusy a firewally, ale aj zvyšovanie povedomia používateľov o bezpečnom správaní v digitálnom prostredí.

3.5 Modelové situácie – určovanie spôsobu infekcie malvérom

Situácia 1

Študent dostane e-mail s predmetom „Nezaplatená faktúra“. V správe je priložený súbor s názvom faktura.pdf.exe. Po jeho otvorení sa počítač začne správať pomaly a antivírus hlási podozrivú aktivitu.

Úloha: Urči spôsob, akým sa malvér dostal do systému.

Situácia 2

Používateľ si z neoficiálnej stránky stiahne platený grafický program zadarmo. Po inštalácii sa mu v prehliadači začnú zobrazovať nevyžiadané reklamy a zmení sa domovská stránka.

Úloha: Aký spôsob šírenia malvéru bol v tomto prípade použitý?

Situácia 3

Zamestnanec firmy navštívi webovú stránku, ktorá bola napadnutá útočníkom. Bez toho, aby niečo sťahoval alebo potvrdzoval, sa jeho počítač infikuje škodlivým kódom.

Úloha: Pomenuj spôsob infekcie.

Situácia 4

V škole sa medzi žiakmi používa jeden USB kľúč. Po jeho pripojení k počítaču sa na viacerých zariadeniach objavia rovnaké problémy a antivírus deteguje malvér.

Úloha: Urči spôsob šírenia malvéru.

Situácia 5

Používateľ odkladá aktualizácie operačného systému. Útočník následne zneužije známu bezpečnostnú chybu a do systému sa dostane škodlivý kód bez akéhokoľvek zásahu používateľa.

Úloha: Aký spôsob šírenia bol použitý?

Situácia 6

Zamestnanec dostane SMS správu s textom: „Váš balík čaká na doručenie. Sledujte zásielku tu:“ a klikne na priložený odkaz, ktorý ho presmeruje na podvodnú stránku.

Úloha: Urči spôsob infekcie.

Situácia 7

Používateľ si nainštaluje falošnú aktualizáciu prehrávača videa, ktorú mu ponúkne vyskakovacie okno na internete. Po inštalácii sa v systéme objaví neznámy softvér.

Úloha: Pomenuj spôsob šírenia malvéru.

Situácia 8

Počítač v podnikovej sieti sa infikuje a následne sa škodlivý kód začne šíriť na ďalšie počítače v rovnakej sieti.

Úloha: Aký spôsob šírenia malvéru sa tu uplatnil?

Situácia 9

Používateľ si nainštaluje oficiálnu aktualizáciu populárneho programu. Neskôr sa zistí, že aktualizačný server bol kompromitovaný a aktualizácia obsahovala škodlivý kód.

Úloha: Ako sa malvér dostal do systému?

Situácia 10

Používateľ je telefonicky presvedčený „technickou podporou“, aby si nainštaloval program na vzdialený prístup. Program však obsahuje škodlivý kód.

Úloha: Aký spôsob šírenia bol v tomto prípade použitý?

3.6 Cvičenia – Typy hrozieb, kybernetických útokov a podvodov

Úloha 1: Rozpoznaj podvodný e-mail (Phishing test)

Cieľ: Naučiť sa rozoznať phishingové znaky.

Zadanie: Prečítaj si nasledujúci e-mail a odpovedz na otázky:

Predmet: Potvrdenie platby – Slovenská sporiteľňa
Text:
Vážený klient,
Zaznamenali sme pokus o prihlásenie do vášho účtu z neznámeho zariadenia.
Pre potvrdenie vašej identity kliknite na odkaz TU:
Ak tak neurobíte do 24 hodín, váš účet bude zablokovaný.
S pozdravom,
Bezpečnostný tím Slovenskej sporiteľne

Otázky:
1. Ktoré znaky naznačujú, že ide o phishing?
2. Aký typ útoku to predstavuje?
3. Ako by ste mali reagovať?

Úloha 2: Kybernetický scenár – čo sa deje?

Cieľ: Určiť typ útoku podľa príznakov.

Scenáre:
1. Počítač sa spomalil, internet nefunguje, v sieti vidíš veľa odchádzajúcich dát.
2. Objaví sa správa: „Vaše súbory boli zašifrované. Zaplaťte 300 € v bitcoinoch.“
3. Z tvojho e-mailu boli odoslané správy, ktoré si neposielal.
4. Na sociálnej sieti ti píše priateľ a žiada o „rýchlu pôžičku“.

Úlohy:
- Urč o aký typ útoku ide.
- Popíš 2–3 kroky, ktoré by si mal urobiť.

Úloha 3: IDS/IPS v praxi

Cieľ: Pochopiť detekciu útokov.

Záznam zo systému:
[ALERT] 2025-10-22 13:45 - Multiple failed login attempts from 192.168.1.45
[NOTICE] 2025-10-22 13:47 - Unusual outbound traffic to IP 203.25.77.14
[ALERT] 2025-10-22 13:48 - Suspicious SQL query detected: SELECT * FROM users WHERE 'a'='a'

Otázky:
1. Aké útoky tu prebiehajú?
2. Ktorý záznam by mal IDS a ktorý IPS riešiť okamžite?
3. Ako by si reagoval ako správca siete?

Úloha 4: Spoj pojmy so správnym vysvetlením

Cieľ: Upevniť teoretické pojmy.

A. DDoS – _____
B. Ransomware – _____
C. Smishing – _____

D. Man-in-the-Middle – _____

1. Útok preťažením servera.
2. Škodlivý softvér, ktorý zašifruje dáta a žiada výkupné.
3. Podvodné SMS správy.
4. Odpočúvanie komunikácie medzi dvomi stranami.

Úloha 5: Kyberbezpečnostný checklist

Cieľ: Precvičiť preventívne opatrenia.

Zadanie: Vytvor vlastný „osobný bezpečnostný checklist“ – 10 pravidiel, ktoré dodržiavaš pri práci s počítačom alebo internetom.

Príklady: dvojfaktorové overenie, zálohovanie dát, neotváranie neznámych odkazov...

Úloha 6: Etický hacker (tímová aktivita)

Cieľ: Pochopiť princíp penetračného testovania.

Zadanie: Rozdeľte sa do dvoch tímov.
- Tím A: Navrhne scenár útoku (napr. phishingová kampaň).
- Tím B: Navrhne obranné opatrenia (IDS, SIEM, školenie...).
Potom diskutujte, ktorá stratégia bola účinnejšia.

Úloha 7: Mini test – rýchly prehľad

Odpovedz ÁNO / NIE:

1. DDoS útok preťažuje server? ____
2. Smishing sa vykonáva cez e-mail? ____
3. IDS automaticky blokuje útoky? ____
4. Ransomware šifruje dáta a žiada výkupné? ____
5. Zálohovanie dát pomáha po útoku? ____

Úloha 8: Test

1. Čo najlepšie vystihuje pojem „kybernetická hrozba“?
a) Akákoľvek činnosť alebo softvér, ktorý môže poškodiť systémy, siete, dáta alebo súkromie
b) Iba vírusy, ktoré sa šíria cez súbory

c) Len finančné podvody na internete
d) Len výpadky internetu spôsobené preťažením

2. Ktoré tvrdenie najlepšie opisuje počítačový vírus?
a) Šíri sa pripojením k súborom alebo programom a aktivuje sa po spustení používateľom
b) Šíri sa autonómne po sieti bez zásahu používateľa
c) Vždy šifruje súbory a žiada výkupné
d) Je to nástroj výhradne na zobrazovanie reklám

3. Čím sa počítačový červ (worm) líši od vírusu?
a) Na šírenie vždy potrebuje otvorenie prílohy používateľom
b) Šíri sa bez zásahu používateľa, často cez zraniteľnosti v OS a sieťach
c) Tvári sa ako legitímny program, no robí škodlivé operácie
d) Zaznamenáva stlačenia klávesnice

4. Ktoré tvrdenie najlepšie vystihuje trójskeho koňa?
a) Tvári sa ako legitímny program, no po spustení vykonáva škodlivé operácie
b) Šíri sa výhradne cez zraniteľnosti siete bez zásahu používateľa
c) Je určený len na zobrazovanie reklám bez ďalších rizík
d) Je to nástroj na blokovanie útokov v sieti

5. Čo je typické pre moderný ransomware?
a) Šifruje dáta a môže hroziť aj zverejnením citlivých informácií
b) Zaznamenáva klávesy a odosiela heslá útočníkovi
c) Presmerúva používateľa na reklamné stránky
d) Vytvára botnet na DDoS útoky bez šifrovania súborov

6. Prečo je rootkit mimoriadne nebezpečný?
a) Pretože zobrazuje veľké množstvo reklám
b) Umožňuje skrytý administrátorský prístup a skrýva prítomnosť malvéru
c) Je to forma podvodu cez SMS správy
d) Je to útok výhradne na dostupnosť webu

7. Ktoré tvrdenie o phishingu a spame je správne?
a) Phishing sa snaží získať citlivé údaje, spam sú nevyžiadané správy často s odkazmi na podvody
b) Spam vždy šifruje dáta a žiada výkupné
c) Phishing je vždy telefonát, spam je vždy e-mail
d) Phishing je bezpečnostný nástroj na odhalenie útokov

8. Čo je typické pre DDoS útok?

a) Jeden počítač pošle jednu požiadavku a server sa vypne

b) Útok prichádza z viacerých infikovaných zariadení (botnet) a zahlcuje službu

c) Útok je založený na krádeži hesiel cez klávesnicu

d) Ide o šifrovanie súborov a žiadosť o výkupné

9. Ktoré tvrdenie správne opisuje rozdiel medzi IDS a IPS?

a) IDS blokuje útoky, IPS ich len zaznamenáva

b) IDS deteguje podozrivé aktivity, IPS dokáže útoky aj aktívne blokovať

c) IDS aj IPS slúžia len na zálohovanie dát

d) IDS je typ malvéru, IPS je typ phishingu

10. Situácia: e-mail „Nezaplatená faktúra“, príloha faktura.pdf.exe – po otvorení sa zariadenie spomalí. Aký spôsob infekcie bol použitý?

a) E-mail s infikovanou prílohou (phishing/sociálne inžinierstvo)

b) Drive-by download po návšteve kompromitovanej webstránky bez kliknutia

c) Infekcia cez USB kľúč

d) Supply chain útok cez oficiálnu aktualizáciu softvéru

4 AAA – Autentifikácia (authentication), autorizácia (authorization), účtovanie / protokolovanie (accounting)

AAA je architektonický rámec na riadenie prístupu k počítačovým zdrojom, presadzovanie bezpečnostných politík a vykonávanie auditu, ktorý poskytuje základné informácie potrebné na účtovanie služieb a ďalšie procesy nevyhnutné na správu a zabezpečenie siete. Tento proces sa používa najmä na zabezpečenie toho, aby boli sieťové zdroje a softvérové aplikácie prístupné iba konkrétnym a oprávneným používateľom a je založený na nasledujúcich princípoch:

- **autentifikácia (authentication)** – slúži na identifikáciu používateľa a overenie pravosti jeho identity; ide o proces overenia, že osoba, ktorá sa prihlasuje, je skutočne tou, za ktorú sa vydáva,
- **autorizácia (authorization)** – zabezpečuje udelenie oprávnení na vykonávanie konkrétnych činností a riadi prístup používateľa k zdrojom,
- **accounting (účtovanie, protokolovanie)** – zabezpečuje zaznamenávanie a uchovávanie auditnej stopy o činnostiach používateľov.

AAA predstavuje rámec používaný na riadenie a monitorovanie prístupu v prostredí počítačových sietí.

Aký je postup pre AAA?

- **Prvý krok – Autentifikácia**
  Ide o spôsob identifikácie používateľa. Na základe autentifikačných údajov sa overuje, či je používateľ legitímny a či má oprávnenie na prístup do siete. Overenie prebieha porovnaním prihlasovacích údajov používateľa s údajmi uloženými v databáze poskytovateľa identity. Po úspešnej autentifikácii získa používateľ prístup k interným sieťovým zdrojom.

- **Druhý krok – Autorizácia**
  Aby mohol používateľ vykonávať konkrétne úlohy alebo zadávať príkazy v sieti, musí mu byť udelené príslušné oprávnenie. Autorizácia určuje rozsah prístupu do siete a definuje, aký typ služieb a zdrojov má autentifikovaný používateľ k dispozícii. Autorizácia predstavuje mechanizmus presadzovania bezpečnostných politík.

- **Tretí krok – Účtovanie / protokolovanie**
  V tejto fáze sa sleduje a zaznamenáva využívanie systémových prostriedkov používateľom, ako napríklad čas prihlásenia, množstvo odoslaných a prijatých dát či

čas odhlásenia. Účtovací proces zhromažďuje štatistiky relácie a informácie o využití zdrojov a používa sa na účely auditu, kontroly autorizácie, účtovania služieb a optimalizácie využívania zdrojov.

Výhodou rámca AAA je zvýšenie **škálovateľnosti siete**. Škálovateľnosť predstavuje schopnosť systému zvládať rastúce množstvo práce prostredníctvom pridávania ďalších zdrojov. To vedie k vyššej flexibilite a lepšej kontrole nad sieťou. Rámec AAA zároveň pomáha udržiavať štandardizované protokoly v počítačovej sieti. Príkladom takéhoto rámca je protokol **RADIUS**, ktorý umožňuje používať jedinečné prihlasovacie údaje pre každého používateľa. IT administrátori tak získavajú centrálny bod na overovanie používateľov a systémov.

Nevýhodou rámca AAA je skutočnosť, že konfigurácia a počiatočné nastavenie serverov môžu byť zložité a časovo náročné. Napríklad výber vhodného serverového softvéru **RADIUS** a správneho modelu implementácie pre konkrétnu organizáciu býva náročný. Údržba vlastného hardvéru môže byť taktiež komplikovaná a vyžaduje si značné časové aj personálne zdroje.

4.1 Autentifikácia

Autentifikácia predstavuje proces overovania identity používateľa, ktorého cieľom je zistiť, či osoba, ktorá sa pokúša získať prístup k systému, je skutočne tým, za koho sa vydáva. V oblasti informačnej bezpečnosti sa autentifikačné metódy delia podľa typu dôkazu, ktorým používateľ preukazuje svoju identitu. Najčastejšie rozlišujeme tri základné skupiny autentifikačných faktorov.

4.1.1 Autentifikačné metódy

1. Niečo, čo viem

Tento typ autentifikácie je založený na znalosti určitej informácie, ktorú by mal poznať iba oprávnený používateľ. Najbežnejším príkladom je heslo alebo osobný identifikačný kód (PIN). Medzi ďalšie príklady patria odpovede na bezpečnostné otázky alebo tajné frázy.

Výhodou tejto metódy je jej jednoduchosť a nízke náklady na implementáciu. Na druhej strane je však pomerne zraniteľná, pretože heslá môžu byť uhádnuté, odcudzené pomocou phishingu, zachytené škodlivým softvérom alebo prezradené samotným používateľom. Bezpečnosť tohto faktora výrazne závisí od kvality hesla, jeho dĺžky, zložitosti a pravidelnej zmeny.

2. Niečo, čo mám

Tento typ autentifikácie využíva fyzický alebo digitálny predmet, ktorý má používateľ k dispozícii. Môže ísť napríklad o USB bezpečnostný token, čipovú kartu, smart kartu, mobilný telefón alebo OTP kalkulačku generujúcu jednorazové heslá. V praxi sa často používa aj autentifikačná aplikácia v smartfóne, ktorá vytvára časovo obmedzené kódy.

Výhodou tejto metódy je vyššia úroveň bezpečnosti v porovnaní s klasickým heslom, keďže útočník musí fyzicky získať dané zariadenie. Nevýhodou je riziko straty alebo odcudzenia tokenu a tiež potreba jeho správy a distribúcie. V prípade mobilných zariadení môže byť problémom aj vybitá batéria alebo technická porucha.

3. Niečo, čo som
Autentifikácia založená na tom, „kým používateľ je“, využíva jedinečné biologické alebo behaviorálne vlastnosti človeka, teda biometrické údaje. Medzi najčastejšie používané biometrické metódy patrí snímanie odtlačku prsta, rozpoznávanie tváre (napr. Face ID), skenovanie očnej dúhovky, rozpoznávanie hlasu či analýza podpisu.

Hlavnou výhodou biometrickej autentifikácie je vysoká úroveň pohodlia a skutočnosť, že tieto vlastnosti nemožno jednoducho zabudnúť alebo stratiť. Na druhej strane však existujú obavy týkajúce sa ochrany súkromia a bezpečného ukladania biometrických údajov. Ak dôjde k úniku biometrických dát, nie je možné ich „zmeniť“ tak jednoducho ako heslo. Navyše, biometrické systémy môžu zlyhať v prípade zranenia, zmeny vzhľadu alebo technických obmedzení snímačov.

4.1.2 Viacfaktorová autentifikácia (MFA)

V praxi sa čoraz častejšie využíva **viacfaktorová autentifikácia** (Multi-Factor Authentication – MFA), ktorá kombinuje dva alebo viac rôznych autentifikačných faktorov. Jej cieľom je výrazne zvýšiť úroveň bezpečnosti tým, že samotné získanie jedného faktora (napríklad hesla) nestačí na neoprávnený prístup do systému.

Najčastejšie ide o kombináciu:

- **niečo, čo viem** (heslo alebo PIN),
- **niečo, čo mám** (mobilný telefón, bezpečnostný token),
- **niečo, čo som** (biometrické overenie).

Použitie viacerých faktorov výrazne znižuje riziko úspešného útoku, pretože útočník by musel prekonať viacero nezávislých bezpečnostných mechanizmov naraz.

Príklady viacfaktorovej autentifikácie:

- Zadanie hesla + jednorazový kód zaslaný SMS správou
- Heslo + potvrdenie prihlásenia v mobilnej aplikácii
- Heslo + odtlačok prsta alebo rozpoznanie tváre
- Čipová karta + PIN kód

4.1.3 Praktické príklady autentifikácie v reálnom živote

Bankovníctvo

V oblasti elektronického bankovníctva patrí viacfaktorová autentifikácia medzi štandardné bezpečnostné opatrenia. Pri prihlásení do internet bankingu používateľ zadáva svoje prihlasovacie meno a heslo, následne musí potvrdiť prístup jednorazovým kódom z SMS správy alebo prostredníctvom mobilnej aplikácie banky. Pri autorizácii finančných transakcií sa často využíva biometria, napríklad odtlačok prsta alebo rozpoznanie tváre v mobilnej aplikácii.

Tento prístup chráni finančné prostriedky klientov aj v prípade, že dôjde k úniku prihlasovacích údajov.

Školské systémy

V školskom prostredí sa autentifikácia využíva pri prístupe do elektronických žiackych knižiek, vzdelávacích platforiem, e-learningových systémov (napr. Moodle) alebo školských informačných systémov. Najčastejšie sa používa kombinácia používateľského mena a hesla. Vo vyššom vzdelávaní alebo pri prístupe učiteľov k citlivým údajom sa čoraz viac zavádza aj druhý faktor, napríklad overenie pomocou mobilnej aplikácie alebo školského preukazu s čipom.

Cieľom je chrániť osobné údaje žiakov, výsledky hodnotení a interné dokumenty školy.

Štátne systémy a verejná správa

V štátnych informačných systémoch je bezpečná autentifikácia kľúčová, keďže pracujú s citlivými osobnými údajmi občanov. Príkladom je prístup k elektronickým službám štátu, kde sa využíva **elektronický občiansky preukaz (eID)** spolu s bezpečnostným osobným kódom (BOK). V niektorých prípadoch je doplnená aj biometrická kontrola alebo overenie prostredníctvom mobilnej aplikácie.

Takýto spôsob autentifikácie zabezpečuje vysokú úroveň dôveryhodnosti a právnu záväznosť elektronických úkonov.

4.1.4 Overenie heslom

Overenie heslom patrí medzi najrozšírenejšie a najpoužívanejšie formy autentifikácie používateľov v informačných systémoch. Napriek svojej jednoduchosti však prináša množstvo bezpečnostných a implementačných výziev. Pri návrhu autentifikačného mechanizmu je potrebné riešiť celý životný cyklus používateľského účtu – od jeho vzniku až po zrušenie.

Časté problémy pri implementácii autentifikácie

Jednou z prvých otázok je spôsob, akým sa používateľ dostane do aplikácie. Používateľský účet môže vzniknúť rôznymi spôsobmi – samostatnou registráciou používateľa, vytvorením účtu administrátorom alebo automatickým importom z existujúcej databázy (napríklad zo školského alebo firemného systému). Každý z týchto spôsobov má iné bezpečnostné požiadavky a riziká.

Ďalším dôležitým problémom je získanie hesla používateľa. Najčastejšie si používateľ zadáva heslo sám počas registrácie. Komplikovanejšia situácia nastáva v prípade, keď je účet vytvorený inou osobou alebo importovaný zo staršieho systému. V takom prípade je nevyhnutné zabezpečiť bezpečný spôsob, ako si používateľ nastaví vlastné heslo bez toho, aby bolo komukoľvek inému známe.

Mimoriadne dôležitou oblasťou je **bezpečné ukladanie používateľských hesiel**. Heslá nesmú byť ukladané v čitateľnej (plain-text) podobe. Správna implementácia využíva kryptografické hashovacie funkcie spolu so „soľou“ (salt), aby k heslu nemal prístup ani administrátor systému, ani útočník v prípade úniku databázy. Cieľom je, aby nebolo možné z pôvodných dát spätne získať heslo používateľa.

Salting (solenie hesiel)
Salting je bezpečnostná technika používaná pri ukladaní používateľských hesiel, ktorej cieľom je výrazne sťažiť ich zneužitie v prípade úniku databázy. Spočíva v tom, že k heslu sa pred jeho zahashovaním pridá **náhodná hodnota**, nazývaná *salt* (soľ).

Ak by sa heslá ukladali len ako obyčajné hashe, vzniká niekoľko vážnych rizík:

- Používatelia s rovnakým heslom by mali rovnaký hash.
- Útočník môže použiť **predpočítané tabuľky hashov** (tzv. *rainbow tables*) na rýchle získanie pôvodných hesiel.
- Slabé a často používané heslá (napr. „123456“, „heslo“) sú veľmi ľahko rozpoznateľné.

Salting tieto problémy účinne eliminuje.

Princíp saltingu:

1. Používateľ zadá heslo.
2. Systém vygeneruje **náhodný salt** (napr. reťazec znakov).
3. Salt sa pripojí k heslu (pred alebo za heslo).
4. Výsledný reťazec sa zahashuje kryptografickou hashovacou funkciou.
5. Do databázy sa uloží:
    - výsledný hash,
    - použitý salt (nie pôvodné heslo).

Pri ďalšom prihlásení systém:

- z databázy načíta uložený salt,

- pripojí ho k zadanému heslu,
- znovu vypočíta hash a porovná ho s uloženým hashom.

Príklad (zjednodušene)
Používateľské heslo:
mojeHeslo123
sha1 hash: *6b30a1e3ca05dfec59d6a0c06e0cd9b0b6a3ae66*

Vygenerovaný salt:
X9f!2Aq#

Spojenie hesla a saltu:
mojeHeslo123X9f!2Aq#

sha1 Hash výsledku :
9ad8ea4dd013f23bc79384827b2fcd7a2bac8006

Aj keby dvaja používatelia mali rovnaké heslo, vďaka rozdielnym saltom budú mať **odlišné hashe**.

Výhody saltingu

- Každý používateľ má jedinečný hash, aj pri rovnakom hesle.
- Rainbow tables sú prakticky nepoužiteľné.
- Útoky hrubou silou sú výrazne pomalšie a nákladnejšie.
- Únik databázy neznamená okamžitý kompromis všetkých hesiel.

Dôležité zásady

- Salt musí byť **náhodný a jedinečný pre každého používateľa**.
- Salt **nie je tajný** – môže byť uložený v databáze spolu s hashom.
- Salting **nenahrádza silné heslá**, ale výrazne zvyšuje ich ochranu.

Salting vs. „peppering“ (stručne)

- **Salt** – unikátna hodnota pre každého používateľa, uložená v databáze.
- **Pepper** – tajná hodnota spoločná pre celý systém, uložená mimo databázy (napr. v konfigurácii servera).

Používateľ musí mať možnosť meniť svoje prihlasovacie údaje, napríklad v prípade zmeny pracovnej e-mailovej adresy alebo podozrenia na kompromitáciu účtu. Rovnako je potrebné riešiť bezpečné odovzdávanie informácií medzi jednotlivými stránkami aplikácie po úspešnom prihlásení. Tento mechanizmus zabezpečuje, že používateľ sa nemusí prihlasovať na každej

stránke zvlášť, pričom jeho identita je overovaná pomocou relácií (sessions) alebo autentifikačných tokenov.

Dôležitou ochranou proti útokom hrubou silou (brute-force attack) je obmedzenie počtu neúspešných pokusov o prihlásenie. Systém môže napríklad povoliť maximálne šesť pokusov za hodinu alebo dočasne zablokovať účet po viacerých neúspešných pokusoch. Tým sa výrazne znižuje riziko prelomenia hesla systematickým skúšaním rôznych kombinácií.

Súčasťou autentifikačného procesu je aj možnosť odhlásenia používateľa. Odhlásenie môže nastať manuálne – kliknutím na tlačidlo „Odhlásiť sa“, alebo automaticky po určitej dobe nečinnosti. Tento mechanizmus je dôležitý najmä pri práci na zdieľaných alebo verejných zariadeniach.

V prípade bezpečnostného incidentu musí systém umožňovať vynútenie zmeny hesla alebo hromadné odhlásenie všetkých používateľov. Takýto krok sa využíva napríklad pri zistení úniku prihlasovacích údajov alebo inej bezpečnostnej chyby.

Moderné systémy musia zároveň umožňovať **zrušenie používateľského účtu**, a to najmä z dôvodu legislatívnych požiadaviek, ako je GDPR. Používateľ má právo na vymazanie svojich osobných údajov a systému musí byť tento proces technicky umožnený.
Neoddeliteľnou súčasťou autentifikácie je aj mechanizmus obnovy hesla v prípade, že ho používateľ zabudne. Tento proces musí byť navrhnutý tak, aby neohrozoval bezpečnosť účtu.

Príklad bezpečnej implementácie obnovy hesla
Používateľ zadá svoju e-mailovú adresu do formulára na obnovenie hesla. Systém mu nemôže vygenerovať nové heslo a poslať ho priamo e-mailom, pretože e-mailová komunikácia nie je šifrovaná a mohla by byť zachytená útočníkom.

Správnym riešením je vytvorenie jedinečnej URL adresy viazanej na konkrétneho používateľa a konkrétnu požiadavku. Táto adresa sa odošle používateľovi e-mailom a po jej otvorení sa zobrazí formulár, v ktorom si môže nastaviť nové heslo.

Platnosť takejto adresy musí byť časovo obmedzená (napríklad na 15 alebo 30 minút). Po uplynutí tejto doby alebo po úspešnej zmene hesla sa odkaz stáva neplatným, čím sa zabraňuje jeho zneužitiu neoprávnenou osobou.

4.1.5 Single Sign-On (SSO)

Single Sign-On (SSO) je autentifikačný mechanizmus, ktorý umožňuje používateľom prihlásiť sa do viacerých aplikácií a služieb pomocou jednej sady prihlasovacích údajov. Používateľ sa

autentifikuje len raz a následne získava prístup k rôznym systémom bez nutnosti opakovaného prihlasovania.

Typickým príkladom je prihlásenie do služby Office 365, po ktorom má používateľ automaticky prístup aj k ďalším integrovaným službám. V podnikových prostrediach sa SSO často realizuje prostredníctvom adresárových služieb, ako je Active Directory.

Výhody Single Sign-On
Hlavnou výhodou SSO je lepší prehľad o používateľských účtoch a ich oprávneniach. Správa identít je centralizovaná, čo zjednodušuje administráciu a znižuje riziko chýb.

SSO zároveň zvyšuje úroveň bezpečnosti, pretože používatelia si musia pamätať menej hesiel, a preto majú tendenciu používať silnejšie a jedinečné prihlasovacie údaje. V kombinácii s viacfaktorovou autentifikáciou poskytuje SSO vysokú úroveň ochrany.

Ďalšou výhodou je zníženie IT nákladov na správu identít a prístupov, keďže administrátori nemusia spravovať samostatné prihlasovacie údaje pre každú aplikáciu zvlášť.

Ako sa vysporiadať s implementáciou autentifikácie (časté problémy)
Implementácia autentifikácie používateľov nie je len otázkou vytvorenia prihlasovacieho formulára, ale zahŕňa celý rad technických, bezpečnostných a organizačných rozhodnutí. Každý systém, ktorý pracuje s identitou používateľa, musí riešiť niekoľko kľúčových problémov, aby bola autentifikácia bezpečná, používateľsky prívetivá a v súlade s legislatívnymi požiadavkami.

Jednou zo základných otázok je, **ako sa používateľ dostane do aplikácie**. Používateľský účet môže vzniknúť prostredníctvom samostatnej registrácie, ktorú iniciuje samotný používateľ, alebo môže byť vytvorený iným používateľom, napríklad administrátorom systému. V niektorých prípadoch sú účty automaticky importované z existujúcich databáz, napríklad zo školských alebo firemných informačných systémov. Každý z týchto spôsobov si vyžaduje odlišný prístup k overeniu identity a bezpečnému nastaveniu prihlasovacích údajov.

S tým úzko súvisí otázka, **ako získať heslo používateľa**. Najjednoduchším riešením je, keď si používateľ zvolí heslo sám počas registrácie. Problém nastáva v prípade, ak je účet vytvorený inou osobou alebo importovaný zo staršieho systému. V takýchto situáciách nie je bezpečné heslo generovať a posielať ho používateľovi. Správnym riešením je umožniť používateľovi, aby si heslo nastavil sám prostredníctvom zabezpečeného procesu.

Mimoriadne dôležitým aspektom je **bezpečné ukladanie používateľských hesiel**. Heslá nikdy nesmú byť ukladané v čitateľnej podobe. Namiesto toho sa používajú kryptografické hashovacie funkcie v kombinácii so saltingom, aby k heslu nemal prístup ani administrátor

servera, ani útočník v prípade úniku databázy. Cieľom je minimalizovať následky bezpečnostného incidentu.

Používateľ by mal mať **možnosť meniť svoje prihlasovacie údaje**, napríklad v prípade zmeny pracovnej e-mailovej adresy alebo pri podozrení na zneužitie účtu. Zmena údajov musí byť chránená opätovným overením identity, aby sa zabránilo neoprávneným zásahom.

Ďalším technickým problémom je **odovzdávanie informácií medzi stránkami aplikácie** po úspešnom prihlásení. Systém musí vedieť, že používateľ je autentifikovaný, aby sa nemusel prihlasovať na každej stránke zvlášť. Tento stav sa najčastejšie rieši pomocou relácií (sessions) alebo autentifikačných tokenov, ktoré bezpečne uchovávajú informáciu o identite používateľa.

Na ochranu proti útokom hrubou silou je potrebné implementovať **mechanizmus obmedzujúci počet neúspešných pokusov o prihlásenie**. Napríklad systém môže povoliť len šesť pokusov za hodinu alebo dočasne zablokovať účet po opakovaných neúspešných pokusoch. Takéto opatrenia výrazne sťažujú automatizované útoky založené na skúšaní veľkého množstva hesiel.

Súčasťou autentifikačného systému musí byť aj **odhlásenie používateľa**. To môže prebehnúť manuálne, kliknutím na tlačidlo „Odhlásiť sa“, alebo automaticky po určitom čase nečinnosti. Automatické odhlásenie je dôležité najmä v prostredí so zdieľanými alebo verejnými zariadeniami.

V prípade zistenia bezpečnostného problému musí mať systém možnosť **vynútiť zmenu hesla používateľov alebo hromadne odhlásiť všetkých používateľov**. Takýto krok sa využíva napríklad pri úniku dát alebo podozrení na kompromitáciu účtov.

Moderné informačné systémy musia zároveň umožňovať **zrušenie používateľského účtu**, a to najmä z dôvodu legislatívnych požiadaviek, ako je GDPR. Používateľ má právo na vymazanie svojich osobných údajov a systém musí tento proces podporovať.

Neoddeliteľnou súčasťou autentifikácie je aj **schopnosť používateľa zmeniť si heslo v prípade, že ho zabudol**. Tento proces musí byť navrhnutý tak, aby bol bezpečný a zároveň jednoduchý pre používateľa.

Príklad bezpečnej implementácie obnovy hesla
Používateľ zadá svoju e-mailovú adresu do formulára na obnovu hesla. Systém mu nemôže vygenerovať nové heslo a poslať ho priamo e-mailom, pretože e-mailová komunikácia nie je šifrovaná a mohla by byť zachytená neoprávnenou osobou.

Správnym riešením je vytvorenie **jedinečnej URL adresy**, ktorá je viazaná na konkrétneho používateľa a konkrétnu požiadavku na zmenu hesla. Tento odkaz sa odošle používateľovi e-mailom.

Po otvorení odkazu sa používateľovi zobrazí formulár, do ktorého si môže zadať nové heslo. Platnosť odkazu musí byť **časovo obmedzená** (napríklad na 15 alebo 30 minút) a po úspešnej zmene hesla alebo po uplynutí času sa odkaz stáva neplatným. Tým sa zabraňuje tomu, aby iná osoba mohla zmeniť heslo používateľa zneužitím získanej URL adresy.

4.1.6 Autentifikácia predmetom

Autentifikácia predmetom je spôsob overovania identity používateľa založený na princípe **„niečo, čo mám“**. V tomto prípade sa identita neoveruje na základe znalosti hesla ani biologických vlastností používateľa, ale pomocou fyzického alebo logického predmetu, ktorý má používateľ k dispozícii. Týmto predmetom je **token** – jedinečný objekt, ktorý nie je možné jednoducho skopírovať alebo napodobniť.

Tokeny sa v praxi používajú najmä v kombinácii s ďalšími autentifikačnými faktormi, čím vzniká viacfaktorová autentifikácia. Samotný token však už sám o sebe predstavuje výrazné zvýšenie bezpečnosti v porovnaní s autentifikáciou založenou len na hesle.

Token je fyzický alebo digitálny predmet, ktorý slúži na preukázanie identity používateľa. Je navrhnutý tak, aby jeho zneužitie bolo čo najnáročnejšie – buď vďaka fyzickým vlastnostiam, kryptografickej ochrane, alebo obmedzenej platnosti generovaných údajov. Token môže mať podobu karty, USB zariadenia, prívesku, mobilnej aplikácie alebo špecializovaného elektronického zariadenia.

V praxi rozlišujeme niekoľko základných typov tokenov.

4.1.7 Typy tokenov používaných v autentifikácii

Tokeny s pamäťou

Tokeny s pamäťou sú najjednoduchším typom autentifikačných predmetov. Obsahujú uloženú identifikačnú informáciu, ktorú systém pri použití tokenu overuje. Môžu mať podobu magnetických, elektronických alebo optických kariet. Ich fungovanie je často prirovnávané k mechanickému kľúču – ak má používateľ správny token, systém mu umožní prístup.

Typickým príkladom sú prístupové karty používané v budovách, školách alebo firmách. Nevýhodou týchto tokenov je, že v prípade ich straty alebo odcudzenia môže dôjsť k neoprávnenému prístupu, ak nie sú doplnené o ďalší bezpečnostný faktor.

Tokeny s heslom

Tokeny s heslom vyžadujú pri svojom použití súčasné zadanie hesla alebo PIN kódu. Ide teda o kombináciu dvoch autentifikačných faktorov – **niečo, čo mám** (token) a **niečo, čo viem** (heslo). Tento prístup výrazne zvyšuje bezpečnosť, pretože samotné vlastníctvo tokenu nestačí na získanie prístupu.

Príkladom sú platobné karty, pri ktorých je na vykonanie transakcie potrebné zadať PIN kód. Podobný princíp sa používa aj pri čipových kartách alebo USB bezpečnostných kľúčoch chránených heslom.

Logické tokeny

Logické tokeny sú zariadenia alebo softvérové riešenia, ktoré dokážu **aktívne spracovávať podnety** a generovať autentifikačné údaje. Najčastejšie ide o generovanie jednorazových hesiel (OTP – One-Time Password) alebo cyklických sekvencií kľúčov, ktoré sú platné len obmedzený čas alebo pre jedno použitie.

Tieto tokeny môžu byť implementované ako samostatné hardvérové zariadenia (napríklad OTP kalkulačky) alebo ako mobilné aplikácie. Ich výhodou je, že aj v prípade zachytenia vygenerovaného kódu je jeho zneužitie veľmi obmedzené časom.

Inteligentné tokeny

Inteligentné tokeny predstavujú najpokročilejšiu formu autentifikácie predmetom. Disponujú vlastným procesorom a často aj vstupným zariadením, ktoré umožňuje komunikáciu s používateľom. Podporujú kryptografické operácie, dokážu generovať náhodné čísla a bezpečne uchovávať kryptografické kľúče.

Medzi inteligentné tokeny patria napríklad smart karty, USB bezpečnostné kľúče alebo hardvérové bezpečnostné moduly. Používajú sa v prostrediach s vysokými bezpečnostnými nárokmi, ako sú štátne systémy, bankovníctvo alebo podnikové informačné systémy. Ich výhodou je vysoká úroveň ochrany, nevýhodou sú vyššie náklady a potreba špeciálneho hardvéru.

Autentifikácia predmetom predstavuje dôležitú súčasť moderných bezpečnostných systémov. V kombinácii s heslom alebo biometrickými údajmi tvorí základ viacfaktorovej autentifikácie, ktorá výrazne znižuje riziko neoprávneného prístupu k citlivým systémom a údajom.

4.1.8 Reálne príklady autentifikácie predmetom

Autentifikácia predmetom sa v súčasnosti využíva v mnohých oblastiach každodenného života – od komunikácie so štátom, cez bankovníctvo až po prístup k online službám. Nasledujúce príklady ilustrujú praktické použitie rôznych typov tokenov.

Elektronický občiansky preukaz (eID)

Elektronický občiansky preukaz je príkladom **inteligentného tokenu**, ktorý obsahuje čip schopný vykonávať kryptografické operácie. Slúži na bezpečné overenie identity občana pri komunikácii s elektronickými službami štátu. Používateľ sa autentifikuje pomocou fyzickej karty (eID) v kombinácii s osobným bezpečnostným kódom (BOK), čím sa dosahuje viacfaktorová autentifikácia.

eID umožňuje nielen prihlásenie do štátnych portálov, ale aj elektronické podpisovanie dokumentov s právnou záväznosťou. Bezpečnosť je zabezpečená tým, že kryptografické kľúče sú uložené priamo v čipe karty a nikdy neopúšťajú token.

Bankové tokeny

Bankové tokeny sú bežným príkladom autentifikácie predmetom v oblasti finančných služieb. Môžu mať podobu samostatného hardvérového zariadenia, mobilnej aplikácie alebo kombinácie s platobnou kartou. Ich hlavnou úlohou je generovať **jednorazové heslá (OTP)**, ktoré používateľ zadáva pri prihlásení do internet bankingu alebo pri potvrdzovaní transakcií.

Staršie riešenia využívali fyzické tokeny vo forme malých kalkulačiek, zatiaľ čo moderné banky čoraz častejšie používajú mobilné aplikácie. Výhodou bankových tokenov je vysoká úroveň bezpečnosti, keďže vygenerovaný kód je platný len krátky čas alebo len pre jednu konkrétnu operáciu.

Google Authenticator

Google Authenticator je príkladom **logického tokenu** realizovaného ako mobilná aplikácia. Slúži na generovanie časovo obmedzených jednorazových kódov (TOTP – Time-based One-Time Password), ktoré sa používajú ako druhý faktor pri prihlasovaní do online služieb.

Aplikácia funguje offline a generuje nové kódy v pravidelných časových intervaloch, zvyčajne každých 30 sekúnd. Google Authenticator sa často používa pri ochrane e-mailových účtov, cloudových služieb, sociálnych sietí alebo vývojárskych platforiem. Jeho výhodou je jednoduchá implementácia a vysoká dostupnosť, keďže väčšina používateľov vlastní smartfón.

Ďalšie príklady z praxe

Medzi ďalšie často používané autentifikačné predmety patria:

- **USB bezpečnostné kľúče** (napr. FIDO2, U2F), ktoré sa pripájajú priamo k zariadeniu a slúžia na rýchle a bezpečné prihlásenie,
- **Prístupové karty** používané v školách, firmách a verejných budovách,
- **Mobilné autentifikačné aplikácie** bánk a štátnych inštitúcií, ktoré kombinujú token s biometrickým overením.

Autentifikácia predmetom je dnes bežnou súčasťou digitálneho života. V kombinácii s heslom alebo biometriou predstavuje účinný spôsob ochrany používateľských účtov a citlivých údajov.

4.1.9 Biometrická autentifikácia

Biometrická autentifikácia je proces automatizovaného overovania identity osoby na základe jej **jedinečných biologických alebo behaviorálnych vlastností**. Na rozdiel od hesiel alebo autentifikačných predmetov je biometria úzko spätá s konkrétnym jednotlivcom a nie je možné ju jednoducho preniesť, ukradnúť ani zabudnúť. Práve táto vlastnosť robí biometrickú autentifikáciu veľmi atraktívnou z hľadiska bezpečnosti aj používateľského komfortu.

Biometrické charakteristiky sú spravidla počas života relatívne stabilné a vykazujú dostatočnú mieru jedinečnosti medzi jednotlivými osobami. Moderné biometrické systémy pracujú s digitalizovanými vzormi, ktoré sú porovnávané s údajmi uloženými v databázach alebo bezpečných úložiskách. Overenie identity prebieha rýchlo a automatizovane, často bez aktívnej spoluúčasti používateľa.

Výhody biometrickej autentifikácie

Medzi hlavné výhody biometrickej autentifikácie patrí **vysoký stupeň spoľahlivosti**. Overené a kvalitne implementované biometrické technológie je veľmi ťažké oklamať, najmä ak využívajú kombináciu viacerých kontrolných mechanizmov, ako je detekcia živosti (liveness detection).

Ďalšou výhodou sú **nulové alebo minimálne prevádzkové náklady**, keďže nie je potrebné distribuovať fyzické tokeny ani riešiť zabudnuté heslá. Po zavedení systému nevzniká dodatočná režijná záťaž spojená s procesom autentifikácie.

Biometrická autentifikácia je zároveň **rýchla**, keďže overenie identity prebieha prakticky okamžite, často v priebehu zlomkov sekundy. To zvyšuje komfort používateľov a plynulosť práce so systémom.

Z hľadiska používateľskej skúsenosti je biometria veľmi **praktická** – používateľ si nemusí pamätať heslá ani nosiť žiadne autentifikačné predmety. Autentifikácia prebieha prirodzene a nenápadne.

Výsledok biometrického overenia je **jednoznačný a okamžitý**, čo zjednodušuje rozhodovanie systému o povolení alebo zamietnutí prístupu. Vďaka priamemu dátovému prepojeniu s databázami a informačnými systémami je biometria zároveň veľmi **efektívna**.

V neposlednom rade je biometrická autentifikácia považovaná za **cenovo priaznivú**, pretože ponúka výhodný pomer medzi cenou a úrovňou bezpečnosti. Moderné zariadenia, ako sú snímače odtlačkov prstov či kamery, sú dnes bežnou súčasťou spotrebnej elektroniky a nevyžadujú dodatočné investície.

Používané biometrické vlastnosti

Biometrické systémy využívajú široké spektrum biologických a behaviorálnych charakteristík. Medzi najčastejšie používané patria:

- **Odtlačok prsta**, ktorý vychádza zo štruktúry papilárnych línií a ich charakteristických detailov. Ide o jednu z najrozšírenejších biometrických metód, používanú napríklad v mobilných zariadeniach a prístupových systémoch.
- **Dynamika podpisu**, pri ktorej sa nesleduje len samotný tvar podpisu, ale aj rýchlosť písania, tlak pera a časové intervaly medzi jednotlivými ťahmi.
- **Geometria tváre**, založená na meraní vzdialeností medzi charakteristickými bodmi tváre, ako sú oči, nos, ústa alebo tvar čeľuste. Táto metóda je známa napríklad z technológie Face ID.
- **Dúhovka oka**, ktorá využíva jedinečný obrazový vzor dúhovky. Poskytuje veľmi vysokú úroveň presnosti a používa sa najmä v systémoch s vysokými bezpečnostnými nárokmi.
- **Sietnica oka**, kde sa analyzuje štruktúra ciev na očnom pozadí. Ide o mimoriadne presnú, no menej rozšírenú metódu z dôvodu vyšších technických nárokov.
- **Geometria ruky**, ktorá pracuje s rozmermi dlane a prstov. Táto metóda sa často používa v dochádzkových systémoch.
- **Štruktúra žíl na zápästí alebo dlani**, založená na jedinečnej žilovej kresbe, ktorá je skrytá pod povrchom kože a ťažko napodobniteľná.
- **Tvar ucha**, ktorý sa vyznačuje stabilnou geometriou počas života a môže slúžiť ako doplnkový biometrický znak.
- **Hlas**, pri ktorom sa analyzuje výška, tón, rytmus a zafarbenie hlasu. Používa sa najmä v telefónnych autentifikačných systémoch.
- **DNA**, ktorá poskytuje najvyššiu mieru jednoznačnosti, avšak z dôvodu časovej a finančnej náročnosti sa v bežných autentifikačných systémoch prakticky nepoužíva.
- **Pach**, založený na chemickom zložení telesného pachu, ktorý je pre každého človeka jedinečný, no zatiaľ má skôr experimentálne využitie.

- **Písanie na klávesnici**, ktoré patrí medzi behaviorálne biometrické metódy a analyzuje rytmus, rýchlosť a dynamiku úderov pri písaní.

Nevýhody a riziká biometrickej autentifikácie

Napriek mnohým výhodám biometrickej autentifikácie existujú aj **významné nevýhody a riziká**, ktoré je potrebné zohľadniť pri jej návrhu a nasadení. Biometria nie je univerzálnym riešením a v niektorých situáciách môže predstavovať bezpečnostné, technické alebo etické problémy.

Jedným z najvážnejších rizík je **nezvratnosť biometrických údajov**. Na rozdiel od hesla alebo tokenu nie je možné biometrické znaky jednoducho zmeniť. Ak dôjde k úniku biometrických dát, používateľ nemá možnosť „nastaviť nové“ odtlačky prstov alebo inú fyziologickú vlastnosť. Takýto únik má preto dlhodobé a potenciálne trvalé následky.

Biometrické systémy môžu trpieť **chybovosťou pri rozpoznávaní**. V praxi sa stretávame s dvoma typmi chýb – falošným zamietnutím oprávneného používateľa (False Rejection Rate – FRR) a falošným prijatím neoprávnenej osoby (False Acceptance Rate – FAR). Kvalita systému spočíva v správnom vyvážení týchto dvoch parametrov, čo však môže byť náročné najmä v prostredí s veľkým počtom používateľov.

Ďalším problémom je **citlivosť biometrických systémov na vonkajšie podmienky**. Zranenie prsta, znečistenie snímača, zmena osvetlenia, hluk v prostredí alebo zmeny vzhľadu používateľa (napr. brada, okuliare, rúško) môžu negatívne ovplyvniť úspešnosť autentifikácie. To môže viesť k zníženiu komfortu alebo nutnosti opakovaného overovania.

Biometrická autentifikácia prináša aj **riziká pre súkromie a ochranu osobných údajov**. Biometrické údaje sú považované za citlivé osobné údaje a ich spracovanie podlieha prísnym legislatívnym požiadavkám, napríklad podľa GDPR. Nesprávne uchovávanie alebo spracovanie týchto údajov môže viesť k právnym dôsledkom pre prevádzkovateľa systému.

Z technického hľadiska je potrebné počítať s tým, že biometrické systémy môžu byť cieľom **sofistikovaných útokov**, ako je falšovanie biometrických vzorov (napr. umelé odtlačky prstov, fotografie alebo masky tváre). Aj keď moderné systémy používajú mechanizmy detekcie živosti, žiadne riešenie nie je úplne odolné voči pokročilým útokom.

Ďalším rizikom je **závislosť od technológie a hardvéru**. Porucha snímača, výpadok systému alebo nekompatibilita zariadení môžu znemožniť prístup používateľov k systému. Preto je nevyhnutné mať vždy k dispozícii záložný spôsob autentifikácie.

V neposlednom rade treba spomenúť aj **etické a spoločenské otázky**. Niektorí používatelia môžu vnímať biometrickú autentifikáciu ako zásah do súkromia alebo formu neprimeraného

sledovania. Tieto obavy môžu viesť k odmietaniu technológie, najmä ak nie je dostatočne vysvetlený jej účel a spôsob ochrany údajov.

4.2 Autorizácia

Autorizácia je proces, ktorý nasleduje po úspešnej autentifikácii používateľa a určuje, **k akým zdrojom, službám alebo funkciám má používateľ povolený prístup**. Kým autentifikácia odpovedá na otázku *„Kto si?“*, autorizácia odpovedá na otázku *„Čo smieš robiť?“*.

V praxi môže byť používateľ úspešne autentifikovaný, ale jeho oprávnenia môžu byť obmedzené – napríklad len na čítanie údajov, bez možnosti ich úpravy. Autorizácia je preto kľúčovým bezpečnostným mechanizmom v každom informačnom systéme.

4.2.1 Spôsoby autorizácie

HTTP autorizácia

Jednoduchým a historicky jedným z najstarších spôsobov autorizácie je **HTTP autorizácia**. V tomto prípade používateľ zadáva svoje používateľské meno a heslo priamo prostredníctvom HTTP hlavičiek. Server tieto údaje použije na overenie identity a zároveň na rozhodnutie o povolení alebo zamietnutí prístupu k chránenému zdroju.

Dôležitou vlastnosťou HTTP autorizácie je, že:

- nevyužíva cookies,
- nepoužíva identifikátory relácií,
- nepracuje s klasickými prihlasovacími stránkami.

Každá požiadavka obsahuje autentifikačné údaje, čo zvyšuje nároky na zabezpečenie prenosu. Z tohto dôvodu sa HTTP autorizácia používa výhradne v kombinácii s HTTPS. V moderných webových aplikáciách je tento spôsob považovaný za zastaraný a využíva sa najmä v jednoduchých alebo interných systémoch.

API autorizácia

V moderných aplikáciách, najmä v prostredí mikroslužieb a webových API, sa často používa **API autorizácia**. Pri registrácii alebo vytvorení aplikácie sa používateľovi (alebo aplikácii) vygeneruje **API kľúč**, ktorý slúži ako identifikátor.

API kľúč je zvyčajne spárovaný so **skrytým tokenom** (identifikačným tokenom), ktorý nie je priamo viditeľný používateľovi. Táto dvojica sa používa pri každej požiadavke na prístup k systémovým zdrojom alebo službám.

API autorizácia umožňuje:

- presne sledovať a obmedzovať prístup k rozhraniam,
- prideľovať rôzne úrovne oprávnení,
- monitorovať využívanie API a detegovať zneužitie.

Nevýhodou je, že kompromitovaný API kľúč môže viesť k neoprávnenému prístupu, preto je nevyhnutné jeho bezpečné uchovávanie a možnosť jeho zneplatnenia.

OAuth 2.0

OAuth 2.0 je moderný a široko používaný štandard, ktorý umožňuje bezpečnú autorizáciu bez potreby zdieľania prihlasovacích údajov. Je navrhnutý predovšetkým pre API a distribuované systémy, kde jedna služba potrebuje pristupovať k zdrojom inej služby v mene používateľa.

Typickým príkladom je prihlásenie do aplikácie pomocou účtu Google alebo Facebook. Používateľ zadáva svoje prihlasovacie údaje iba u poskytovateľa identity, zatiaľ čo samotná aplikácia získava len **obmedzený prístupový token**.

OAuth 2.0 umožňuje:

- presne definovať rozsah oprávnení (scope),
- časovo obmedziť platnosť prístupov,
- bezpečne delegovať prístup tretím stranám.

Vďaka týmto vlastnostiam patrí OAuth 2.0 medzi **najbezpečnejšie a najpoužívanejšie metódy autorizácie a autentifikácie** v moderných informačných systémoch.

Autorizácia pomocou JWT (JSON Web Token)

JSON Web Token (JWT) je otvorený štandard určený na bezpečný prenos informácií medzi dvoma stranami. JWT sa často používa na **autorizáciu v bezstavových (stateless) aplikáciách**, kde server neuchováva informácie o reláciách používateľov.

JWT obsahuje:

- identitu používateľa,
- jeho oprávnenia,
- ďalšie metadata (napr. čas platnosti).

Token je kryptograficky podpísaný pomocou **súkromného a verejného kľúča** alebo zdieľaného tajomstva, čo zabezpečuje integritu a dôveryhodnosť prenášaných údajov. Server môže overiť

platnosť tokenu bez nutnosti komunikácie s databázou, čo zvyšuje výkon a škálovateľnosť systému.

JWT sa bežne používa v kombinácii s OAuth 2.0 alebo ako samostatný mechanizmus autorizácie v REST API a mobilných aplikáciách.

4.2.2 Praktický príklad toku autorizácie

Na lepšie pochopenie rozdielu medzi autentifikáciou a autorizáciou si ukážeme praktický príklad toku autorizácie v modernej webovej aplikácii. Príklad je založený na bežne používaných technológiách OAuth 2.0 a JWT.

Scenár

Používateľ sa chce prihlásiť do webovej aplikácie a získať prístup k chráneným údajom (napr. k svojmu profilu alebo dokumentom).

Krok 1 – Prihlásenie používateľa (autentifikácia)

Používateľ zadá svoje prihlasovacie údaje (napr. e-mail a heslo) do prihlasovacieho formulára aplikácie alebo sa prihlási prostredníctvom externého poskytovateľa identity (napr. Google).

Systém overí identitu používateľa. Tento krok predstavuje **autentifikáciu** – systém zistí, kto je používateľ.

Krok 2 – Vydanie autorizačného tokenu

Po úspešnej autentifikácii server vygeneruje **autorizačný token** (napr. JWT). Token obsahuje informácie o:

- identite používateľa,
- jeho roli alebo oprávneniach,
- čase platnosti tokenu.

Token je kryptograficky podpísaný, aby nebolo možné jeho údaje dodatočne meniť.

Krok 3 – Uloženie tokenu na strane klienta

Autorizačný token je odoslaný klientovi (prehliadaču alebo mobilnej aplikácii). Klient si token uloží, napríklad do pamäte aplikácie alebo bezpečného úložiska.

Od tohto momentu už používateľ nemusí zadávať prihlasovacie údaje pri každej akcii.

Krok 4 – Prístup k chráneným zdrojom (autorizácia)

Pri každej požiadavke na chránený zdroj (napr. načítanie profilu) klient priloží token k požiadavke, najčastejšie v HTTP hlavičke.

Server:

1. overí platnosť tokenu (podpis, čas platnosti),
2. zistí, aké oprávnenia používateľ má,
3. rozhodne, či je požadovaná operácia povolená.

Tento krok predstavuje **autorizáciu** – systém rozhoduje, čo môže používateľ vykonať.

Krok 5 – Povolenie alebo zamietnutie prístupu

Ak má používateľ potrebné oprávnenia, server vráti požadované údaje. Ak oprávnenia nemá (napr. bežný používateľ sa pokúša o administrátorskú akciu), server prístup zamietne.

Krok 6 – Vypršanie platnosti tokenu

Autorizačný token má obmedzenú platnosť. Po jej uplynutí musí používateľ:

- získať nový token (napr. pomocou obnovovacieho tokenu),
- alebo sa znovu prihlásiť.

Tým sa znižuje riziko zneužitia tokenu v prípade jeho úniku.

4.3 Protokolovanie (Accounting)

Accounting predstavuje proces zaznamenávania a uchovávania informácií o činnostiach používateľov a systémov po ich autentifikácii a autorizácii. Jeho cieľom je vytvoriť **prehľadný a auditovateľný záznam o tom, kto, kedy, kde a akým spôsobom používal systémové prostriedky**.

Zatiaľ čo autentifikácia a autorizácia rozhodujú o prístupe, accounting zabezpečuje **zodpovednosť (accountability)** používateľov a administrátorov za ich činnosť v systéme.

V rámci accountingových záznamov sa typicky protokolujú údaje ako:

- identita používateľa alebo systému,

- čas začiatku a ukončenia relácie,
- typ vykonanej operácie (napr. prihlásenie, zmena hesla, vytvorenie účtu),
- použité oprávnenia alebo rola,
- zdroj prístupu (IP adresa, zariadenie),
- výsledok operácie (úspech, zlyhanie).

Tieto údaje sú ukladané do logov, ktoré slúžia na analýzu, audit a forenzné vyšetrovanie.

Vzťah medzi Accountingom a protokolovaním
Protokolovanie je **technický nástroj**, zatiaľ čo accounting je **bezpečnostný koncept**. Inými slovami:

- **protokolovanie** = ako sa údaje zaznamenávajú,
- **accounting** = prečo sa údaje zaznamenávajú.

Accounting využíva protokolovanie na to, aby:

- umožnil spätnú kontrolu činností,
- odhalil porušenie bezpečnostných politík,
- poskytol dôkazy pri bezpečnostných incidentoch,
- splnil legislatívne a auditné požiadavky.

Praktický príklad Accounting v praxi
Pri prihlasovaní používateľov do domény môže systém:

- **autentifikovať** používateľa (overiť meno a heslo),
- **autorizovať** jeho prístup (prideliť rolu používateľa alebo administrátora),
- **zaznamenať** udalosť do logu (accounting).

Príklad accountingového záznamu:

- používateľ *admin01* sa prihlásil,
- čas: 08:42,
- zariadenie: pracovná stanica,
- operácia: prihlásenie s administrátorskými právami,
- výsledok: úspešné.

Takýto záznam umožňuje spätne overiť, kto vykonal konkrétnu činnosť, a je nevyhnutný napríklad pri vyšetrovaní bezpečnostného incidentu.

Význam Accounting pre bezpečnosť
Accounting má zásadný význam najmä:

- v podnikových a štátnych systémoch,
- pri práci s citlivými údajmi,
- pri správe privilegovaných účtov,

- v prostredí s legislatívnymi požiadavkami (napr. GDPR, ISO/IEC 27001).

Bez accountingových záznamov nie je možné preukázať zodpovednosť používateľov ani spätne analyzovať bezpečnostné incidenty.

4.3.1 Príklad 1: Accounting v RADIUS

Scenár
Používateľ sa pripája do podnikovej siete prostredníctvom VPN alebo Wi-Fi. Overenie prebieha cez RADIUS server.

1. **Začiatok relácie (Accounting-Start)**
   Po úspešnej autentifikácii používateľa pošle sieťové zariadenie (napr. VPN koncentrátor alebo Wi-Fi controller) na RADIUS server accounting správu typu *Start*.
   Táto správa obsahuje informácie ako:
   - používateľské meno,
   - IP adresa klienta,
   - čas začiatku relácie,
   - typ služby (VPN, Wi-Fi),
   - identifikátor relácie.
2. **Priebežné záznamy (Accounting-Interim-Update)**
   Počas aktívnej relácie môže zariadenie periodicky odosielať priebežné aktualizácie.
   Tie obsahujú:
   - dĺžku trvania relácie,
   - množstvo prenesených dát,
   - stav spojenia.
3. **Ukončenie relácie (Accounting-Stop)**
   Po odhlásení používateľa alebo prerušení spojenia odošle zariadenie správu typu *Stop*.
   Tá obsahuje:
   - čas ukončenia relácie,
   - celkovú dobu pripojenia,
   - prenesené dáta,
   - dôvod ukončenia (odhlásenie, timeout, chyba).

Význam RADIUS accounting-u
- sledovanie využívania siete,
- odhaľovanie podozrivých aktivít,
- podklady pre fakturáciu alebo reporting,
- audit prístupov do siete.

4.3.2 Príklad 2: Accounting v TACACS+

Scenár

Administrátor sa prihlasuje na sieťové zariadenie (napr. router alebo switch) pomocou SSH. Autentifikácia a autorizácia prebieha cez TACACS+ server.

1. **Prihlásenie administrátora**
   Po úspešnom prihlásení odošle zariadenie na TACACS+ server záznam o začiatku relácie.
   Záznam obsahuje:
   - meno administrátora,
   - zariadenie, na ktoré sa prihlásil,
   - čas prihlásenia,
   - typ prístupu (SSH, konzola).
2. **Zaznamenávanie príkazov (Command Accounting)**
   Jednou z hlavných výhod TACACS+ je možnosť **zaznamenávať každý vykonaný príkaz**.
   Príklady zaznamenaných operácií:
   - zmena konfigurácie rozhrania,
   - vytvorenie VLAN,
   - reštart zariadenia,
   - zmena hesla.
3. **Ukončenie relácie**
   Po odhlásení administrátora sa zaznamená koniec relácie vrátane:
   - dĺžky prihlásenia,
   - počtu vykonaných príkazov,
   - prípadných chýb.

Význam TACACS+ accounting-u

- presná auditná stopa administrátorských zásahov,
- spätná dohľadateľnosť zmien konfigurácie,
- zvýšená zodpovednosť administrátorov,
- splnenie bezpečnostných a auditných požiadaviek.

4.3.3 Porovnanie RADIUS vs TACACS+ z pohľadu accounting-u

- **RADIUS**
  - zameraný na prístup používateľov do siete,
  - zaznamenáva relácie a prenos dát,
  - vhodný pre Wi-Fi, VPN, dial-up.
- **TACACS+**
  - zameraný na správu sieťových zariadení,
  - zaznamenáva jednotlivé príkazy,
  - ideálny pre administrátorské prístupy.

4.4 Otázky

1. Čo v modeli AAA znamená autentifikácia (Authentication)?
a) Určenie, aké zdroje môže používateľ používať
b) Zaznamenávanie činností používateľa do logov
c) Overenie identity používateľa
d) Šifrovanie komunikácie medzi klientom a serverom

2. Ktorá veta najlepšie vystihuje autorizáciu (Authorization)?
a) „Kto si?“
b) „Čo smieš robiť?“
c) „Ako dlho si bol prihlásený?“
d) „Kde je uložené heslo?“

3. Čo je hlavným cieľom accounting-u v AAA?
a) Vytvoriť nové používateľské účty
b) Uchovávať auditnú stopu o činnostiach používateľov
c) Overiť, či má používateľ silné heslo
d) Zabezpečiť šifrovanie databázy

4. Aký je typický správny postup krokov v AAA?
a) Autorizácia → Autentifikácia → Accounting
b) Accounting → Autentifikácia → Autorizácia
c) Autentifikácia → Autorizácia → Accounting
d) Autentifikácia → Accounting → Autorizácia

5. Ktorý príklad patrí medzi „niečo, čo viem“?
a) USB token
b) Odtlačok prsta
c) PIN kód
d) Smart karta

6. Ktorá kombinácia je príkladom viacfaktorovej autentifikácie (MFA)?
a) Heslo + bezpečnostná otázka
b) Heslo + jednorazový kód z mobilnej aplikácie
c) Odtlačok prsta + rozpoznanie tváre
d) Používateľské meno + e-mailová adresa

7. Ktorý výrok o saltingu je správny?
a) Salt musí byť tajný a nikdy nesmie byť uložený v databáze
b) Salt je unikátna náhodná hodnota pridaná k heslu pred hashovaním

c) Salt nahrádza potrebu silných hesiel
d) Salt sa používa na šifrovanie hesla symetrickým kľúčom

8. Čo je typickým príkladom toho, čo sa zaznamenáva v accounting-u?
a) Dĺžka hesla používateľa pri registrácii
b) Čas prihlásenia a odhlásenia používateľa
c) Obsah súkromných správ používateľa
d) Kompletné heslo používateľa v čitateľnom tvare

9. Čím sa vyznačuje TACACS+ accounting v porovnaní s RADIUS accounting?
a) TACACS+ sa používa hlavne na Wi-Fi pripojenia používateľov
b) TACACS+ dokáže zaznamenávať aj jednotlivé príkazy administrátora
c) TACACS+ neumožňuje audit a logovanie
d) TACACS+ je určený len na šifrovanie prenosu dát

10. Ktoré tvrdenie o RADIUS accounting-u je najpresnejšie?
a) Zaznamenáva relácie používateľov (start, interim update, stop) pri VPN/Wi-Fi prístupe
b) Slúži výhradne na biometrickú autentifikáciu
c) Ukladá heslá používateľov v čitateľnej podobe
d) Používa sa len na vytváranie používateľských účtov v databáze

5 Metódy overovania digitálnej identity

Overovanie digitálnej identity je proces, ktorým sa potvrdzuje, že používateľ, ktorý sa prihlasuje alebo pristupuje k určitej digitálnej službe, je skutočne tou osobou, za ktorú sa vydáva. Tento proces tvorí **základný pilier kybernetickej bezpečnosti**, pretože chráni informačné systémy pred neoprávneným prístupom, zneužitím údajov a rôznymi formami digitálnych podvodov.

Metódy overovania digitálnej identity vychádzajú z rovnakých princípov, ktoré sú známe z oblasti autentifikácie. Na základe spôsobu fungovania ich možno rozdeliť do troch základných kategórií – **overovanie na základe vedomostí, vlastníctva a biometrických vlastností**. V praxi sa tieto metódy často kombinujú, aby sa dosiahla vyššia úroveň bezpečnosti.

5.1 Overovanie na základe vedomostí (niečo, čo viete)

Overovanie na základe vedomostí je založené na informáciách, ktoré pozná výlučne používateľ. Najčastejším a zároveň najrozšírenejším príkladom je **heslo** alebo **PIN kód**. Ide o jednoduchý a lacný spôsob overovania identity, ktorý je však zároveň náchylný na zneužitie, ak nie je správne implementovaný.

Bezpečnosť tejto metódy závisí najmä od:

- dĺžky hesla,
- jeho zložitosti,
- jedinečnosti (nepoužívania rovnakého hesla na viacerých službách).

Ako doplnkové overenie identity sa niekedy používajú aj **bezpečnostné otázky**. Ich praktická hodnota je však obmedzená, keďže odpovede na ne možno často získať z verejne dostupných zdrojov, ako sú sociálne siete alebo osobné profily. Z tohto dôvodu sa dnes považujú skôr za slabý autentifikačný prvok.

5.2 Overovanie na základe vlastníctva (niečo, čo máte)

Druhou významnou kategóriou je overovanie identity prostredníctvom predmetu alebo zariadenia, ktoré používateľ vlastní. Najčastejším príkladom je **mobilný telefón**, ktorý slúži na prijímanie jednorazových SMS kódov alebo na používanie autentifikačných aplikácií, ako je napríklad **Google Authenticator**.

V podnikových, bankových a štátnych systémoch sa často používajú aj:

- **hardvérové tokeny**,
- **čipové karty**,

- **USB bezpečnostné kľúče**, ktoré generujú jednorazové kódy alebo uchovávajú kryptografické certifikáty.

Zaujímavým príkladom z praxe je **banková identita (BankID)**, ktorá sa v niektorých krajinách využíva na bezpečné elektronické prihlasovanie do online služieb. Používateľ sa identifikuje prostredníctvom svojej banky, ktorá už jeho identitu overila, čím sa zvyšuje dôveryhodnosť celého procesu.

5.3 Biometrické overovanie (niečo, čím ste)

Biometrické overovanie identity využíva **jedinečné fyzické alebo behaviorálne vlastnosti človeka**. Medzi najčastejšie používané biometrické metódy patria:

- rozpoznávanie odtlačku prsta,
- rozpoznávanie tváre,
- skenovanie dúhovky oka,
- hlasová biometria.

Hlavnou výhodou biometrie je **rýchlosť a pohodlie**, keďže používateľ si nemusí pamätať žiadne heslá ani nosiť autentifikačné predmety. Overenie identity prebieha takmer okamžite a prirodzene.

Na druhej strane však biometrické údaje predstavujú **citlivé osobné údaje**. Ak dôjde k ich úniku, nie je možné ich jednoducho zmeniť, ako je to v prípade hesla. Z tohto dôvodu sa biometrické overovanie zriedkavo používa samostatne a často sa kombinuje s inými metódami.

5.4 Viacfaktorová autentifikácia (MFA / 2FA)

Viacfaktorová autentifikácia spája viacero rôznych metód overovania digitálnej identity. Najčastejšie ide o kombináciu:

- niečo, čo používateľ vie (heslo),
- niečo, čo používateľ má (mobilný telefón alebo token).

Takýto prístup výrazne zvyšuje úroveň bezpečnosti, pretože útočník by musel získať prístup k viacerým nezávislým faktorom súčasne. MFA sa dnes bežne používa pri prihlasovaní do e-mailových účtov, bankovníctva, firemných systémov, cloudových služieb či sociálnych sietí.

5.5 Digitálne certifikáty a elektronické podpisy

V prostredí online komunikácie zohrávajú dôležitú úlohu aj **digitálne certifikáty a elektronické podpisy**. Tieto technológie slúžia nielen na overenie identity používateľa, ale aj na zabezpečenie **integrity a dôveryhodnosti prenášaných údajov**.
Digitálne certifikáty vydávajú **certifikačné autority**, ktoré garantujú, že verejný kľúč patrí konkrétnej osobe alebo organizácii. Elektronický podpis má v mnohých prípadoch rovnakú právnu váhu ako vlastnoručný podpis, čo umožňuje bezpečnú elektronickú komunikáciu a uzatváranie zmlúv.

5.6 Elektronická identita (eID)

Elektronická identita predstavuje moderný spôsob bezpečného prihlasovania k online službám verejnej správy. Umožňuje občanom preukazovať svoju totožnosť v digitálnom priestore bez nutnosti osobnej návštevy úradov.

Pomocou systémov eID sa používatelia môžu:

- prihlasovať na portály verejnej správy,
- elektronicky podpisovať dokumenty,
- vybavovať úradné záležitosti online.

Elektronická identita zohráva kľúčovú úlohu v digitalizácii verejnej správy a zvyšovaní dostupnosti elektronických služieb.

5.7 Správa hesiel a odporúčania pre ich bezpečné používanie

Bezpečné narábanie s heslami je neoddeliteľnou súčasťou digitálnej identity. Odporúča sa používať **správcov hesiel**, ktorí bezpečne uchovávajú prihlasovacie údaje a umožňujú generovať silné a jedinečné heslá pre každú službu.

Základné odporúčania zahŕňajú:

- používanie dlhého a silného hlavného hesla,
- neopakovanie hesiel na viacerých službách,
- aktiváciu viacfaktorového overenia všade, kde je to možné,
- pravidelnú kontrolu bezpečnosti účtov.

Moderní správcovia hesiel využívajú silné šifrovanie a poskytujú vysokú úroveň ochrany. Ich používanie je jedným z najefektívnejších spôsobov, ako si udržať digitálnu identitu bezpečnú a pod kontrolou.

5.8 Otázky

1. Čo je hlavným cieľom overovania digitálnej identity?
a) Zvýšiť rýchlosť internetu
b) Potvrdiť, že osoba je tou, za ktorú sa vydáva
c) Získať anonymitu na internete
d) Umožniť voľný prístup ku všetkým systémom

2. Ktorý príklad patrí medzi „niečo, čo viete“?
a) Odtlačok prsta
b) Heslo alebo PIN
c) USB bezpečnostný kľúč
d) Čipová karta

3. Ktorý príklad je overovanie na základe vlastníctva?
a) Bezpečnostná otázka
b) Rozpoznávanie tváre
c) Mobilný telefón s autentifikačnou aplikáciou
d) Podpis na papieri

4. Ktorá možnosť NIE JE biometrickým overením?
a) Rozpoznávanie hlasu
b) Skenovanie dúhovky oka
c) Bezpečnostné otázky
d) Rozpoznávanie tváre

5. Čo znamená viacfaktorová autentifikácia (MFA)?
a) Použitie jedného silného hesla
b) Kombinácia viacerých nezávislých faktorov
c) Prihlasovanie bez hesla
d) Zdieľanie účtu viacerými osobami

6. Aká je hlavná výhoda biometrického overovania?
a) Rýchlosť a pohodlie používateľa
b) Možnosť zmeniť údaje po úniku
c) Nulové bezpečnostné riziká
d) Anonymita používateľa

7. Aké je hlavné riziko biometrických údajov?
a) Nie je možné ich zmeniť po úniku
b) Sú príliš krátke

c) Sú vždy nepresné
d) Nedajú sa technicky spracovať

8. Akú úlohu majú digitálne certifikáty?
a) Overujú identitu a dôveryhodnosť komunikácie
b) Slúžia ako antivírus
c) Zvyšujú rýchlosť siete
d) Umožňujú anonymné prihlásenie

9. Na čo slúži elektronická identita (eID)?
a) Na zdieľanie hesiel
b) Na bezpečný prístup k službám verejnej správy
c) Na sledovanie používateľov
d) Na anonymné hlasovanie

10. Prečo je odporúčané používať správcu hesiel?
a) Umožňuje používať silné a jedinečné heslá
b) Znižuje potrebu zabezpečenia účtov
c) Nahrádza viacfaktorovú autentifikáciu
d) Umožňuje používať jedno heslo všade

6 Princípy bezpečného používania hesiel

Heslá patria medzi najzákladnejšie, no zároveň najčastejšie zneužívané prvky kybernetickej bezpečnosti. Napriek rozvoju moderných autentifikačných metód sa heslá stále používajú v prevažnej väčšine informačných systémov. Ich bezpečné používanie je preto kľúčové pre ochranu digitálnej identity používateľov, osobných údajov aj citlivých systémových zdrojov.

Bezpečné používanie hesiel zahŕňa **správnu tvorbu silných hesiel, ich bezpečnú správu, pravidelnú údržbu a pochopenie rizík spojených s ich prelomením**. Nesprávne zvolené alebo opakovane používané heslá patria medzi najčastejšie príčiny bezpečnostných incidentov.

6.1 Tvorba hesiel

Vytváranie silných hesiel je základným predpokladom ochrany digitálnej identity. Silné heslo by malo byť dostatočne dlhé, zložité a jedinečné, aby odolalo bežným útokom.

6.1.1 Zásady pre tvorbu silných hesiel

Dĺžka hesla

Heslo by malo mať minimálne **12 znakov**, ideálne však viac. Dlhšie heslá sú výrazne odolnejšie voči útokom hrubou silou a slovníkovým útokom, a to aj v prípade, že obsahujú bežné slová.

Kombinácia znakov

Odporúča sa používať kombináciu:

- veľkých a malých písmen,
- číslic,
- špeciálnych znakov (napr. @, #, $, !).

Takáto kombinácia výrazne zvyšuje počet možných variantov hesla a tým aj jeho odolnosť.

Vyhýbanie sa bežným slovám

Nepoužívajte jednoduché a často používané heslá, ako napríklad „password“, „123456“, „qwerty“ alebo ich obmeny. Tieto heslá sú súčasťou slovníkov používaných útočníkmi.

Osobné údaje

Heslá by nemali obsahovať osobné informácie, ako sú:

- meno alebo priezvisko,
- dátum narodenia,
- meno domáceho miláčika,
- rodné číslo.

Tieto údaje sú často verejne dostupné alebo ľahko zistiteľné.

Unikátnosť hesiel
Pre každý účet by sa malo používať **iné heslo**. Ak dôjde k úniku jedného hesla, ostatné účty zostanú chránené.

Používanie správcu hesiel
Správca hesiel dokáže generovať a bezpečne ukladať silné a jedinečné heslá, čím výrazne znižuje riziko chýb zo strany používateľa.

6.2 Význam dĺžky hesla z pohľadu kombinatoriky

Pri hodnotení sily hesla zohráva **dĺžka hesla často dôležitejšiu úlohu než jeho zložitosť**. Z pohľadu kombinatoriky totiž počet možných kombinácií rastie **exponenciálne** s každým ďalším znakom hesla. To znamená, že aj malé predĺženie hesla môže dramaticky zvýšiť jeho odolnosť voči útokom hrubou silou.

Počet možných hesiel závisí od:

- počtu povolených znakov (abeceda hesla),
- dĺžky hesla.

Matematicky možno počet kombinácií vyjadriť ako:
počet kombinácií = počet znakov^dĺžka hesla

6.2.1 Jednoduché dlhé vs. krátke zložité heslo

Krátke heslo so zložitými znakmi môže pôsobiť bezpečne, no v skutočnosti môže mať **menej kombinácií** než dlhé heslo z jednoduchších znakov.

Príklad:

- heslo s dĺžkou **8 znakov** z množiny **94 znakov** (malé a veľké písmená, čísla, špeciálne znaky)
  → $94^8 \approx 6{,}1 \times 10^{15}$ kombinácií
- heslo s dĺžkou **16 znakov** len z malých písmen (26 znakov)
  → $26^{16} \approx 4{,}3 \times 10^{22}$ kombinácií

Aj keď druhé heslo používa výrazne menší počet rôznych znakov, vďaka svojej dĺžke má **niekoľkonásobne viac možných kombinácií** a je teda omnoho odolnejšie voči automatizovaným útokom.

6.2.2 Praktický dôsledok

Z praktického hľadiska to znamená, že:

- **dlhé heslá sú spravidla bezpečnejšie než krátke, aj keď sú jednoduchšie**,
- dlhé heslá sa zároveň **ľahšie pamätajú**, ak majú podobu vety alebo frázy,
- útočníkovi sa výrazne predlžuje čas potrebný na ich prelomenie.

Preto sa v moderných bezpečnostných odporúčaniach čoraz častejšie uprednostňujú **heslové frázy (passphrases)** namiesto krátkych zložitých hesiel.

6.2.3 Príklad porovnania

- Krátke zložité heslo: **X7@Q!9a$**
- Dlhé jednoduché heslo (heslová fráza): **mamradcokoladuakavu**

Druhé heslo je:

- dlhšie,
- ľahšie zapamätateľné,
- kombinatoricky výrazne silnejšie.

Odporúčanie

Za optimálne sa dnes považujú heslá alebo heslové frázy s dĺžkou:

- **minimálne 12 znakov**,
- ideálne **16 znakov a viac**.

V kombinácii so správcom hesiel a viacfaktorovou autentifikáciou predstavujú dlhé heslá jednu z najefektívnejších foriem ochrany digitálnej identity.

Príklad silného hesla

Efektívnym spôsobom tvorby hesla je použitie **zapamätateľnej vety**, ktorú používateľ skráti alebo upraví.

Príklad:

„Mám rád pizzu so syrom 4× týždenne!“ → heslo: **MrPsS4xt**

Takéto heslo je pre používateľa ľahko zapamätateľné, no pre útočníka veľmi ťažko uhádnuteľné.

6.2.4 Porovnanie sily hesiel (kombinatorický pohľad)

Typ hesla	Príklad	Dĺžka	Použité znaky	Počet kombinácií (≈)	Relatívna bezpečnosť

Krátke jednoduché	`heslo123`	8	malé písmená + čísla (36)	$36^8 \approx 2{,}8 \times 10^{12}$	❌ veľmi nízka
Krátke zložité	`X7@Q!9a$`	8	všetky znaky (94)	$94^8 \approx 6{,}1 \times 10^{15}$	⚠️ nízka
Stredne dlhé jednoduché	`mamradpizzu`	11	malé písmená (26)	$26^{11} \approx 3{,}7 \times 10^{15}$	⚠️ stredná
Dlhé jednoduché (fráza)	`mamradcokoladuakavu`	19	malé písmená (26)	$26^{19} \approx 2{,}0 \times 10^{27}$	✅ vysoká
Dlhé kombinované	`MamRadCoko!2025`	15	kombinované (62)	$62^{15} \approx 7{,}7 \times 10^{26}$	✅ veľmi vysoká

6.3 Správa hesiel

Správna správa hesiel je rovnako dôležitá ako ich samotná tvorba. Používateľ môže mať desiatky až stovky účtov, preto je manuálne zapamätanie silných a jedinečných hesiel prakticky nemožné.

Používanie správcu hesiel

Správca hesiel je aplikácia, ktorá bezpečne uchováva prihlasovacie údaje a umožňuje ich jednoduché používanie. Medzi známe správcovské nástroje patria napríklad LastPass, 1Password alebo Bitwarden. Okrem ukladania hesiel poskytujú aj funkcie na ich generovanie a kontrolu bezpečnosti.

Hlavné heslo

Prístup k správcovi hesiel je chránený **hlavným heslom**, ktoré musí byť:

- dlhé,
- jedinečné,
- nepoužívané nikde inde.

Toto heslo predstavuje „kľúč ku všetkým ostatným heslám“ a musí byť obzvlášť dobre chránené.

6.3.1 Google ako správca hesiel

Google poskytuje vlastného **správcu hesiel**, ktorý je integrovaný priamo do prehliadača **Google Chrome** a do **Google účtu** používateľa. Tento správca hesiel umožňuje bezpečné ukladanie, automatické vypĺňanie a správu prihlasovacích údajov naprieč zariadeniami.

Pri prihlásení na webovú stránku môže Chrome používateľa vyzvať na uloženie hesla. Uložené heslá sú následne:

- automaticky vypĺňané pri ďalšom prihlásení,

- synchronizované medzi zariadeniami (počítač, mobil, tablet),
- chránené zabezpečením Google účtu.

Google správca hesiel podporuje aj **kontrolu bezpečnosti hesiel**. Dokáže upozorniť na:

- slabé heslá,
- opakovane používané heslá,
- heslá, ktoré sa objavili v známych únikoch dát.

Bezpečnosť uložených hesiel závisí najmä od **hlavného zabezpečenia Google účtu**, preto je nevyhnutné používať silné hlavné heslo a zapnutú viacfaktorovú autentifikáciu.

6.3.2 Prihlasovacie kľúče (Passkeys)

Prihlasovacie kľúče (Passkeys) predstavujú modernú alternatívu ku klasickým heslám. Ide o autentifikačný mechanizmus založený na **kryptografii verejného a súkromného kľúča**, ktorý výrazne zvyšuje bezpečnosť a zároveň zjednodušuje prihlasovanie.

Pri použití passkey:

- používateľ **nezadáva heslo**,
- autentifikácia prebieha pomocou zariadenia (telefón, počítač),
- identita sa potvrdzuje biometricky (Face ID, Touch ID) alebo PIN kódom zariadenia.

Súkromný kľúč nikdy neopustí zariadenie používateľa, čím sa eliminuje riziko jeho odcudzenia.

Prihlasovacie kľúče v iPhone (Apple)
V ekosystéme Apple sú passkeys integrované do systému **iOS, iPadOS a macOS** a spravované prostredníctvom **iCloud Keychain (Kľúčenka iCloud)**.

Pri vytvorení passkey:

- systém vygeneruje kryptografický pár kľúčov,
- verejný kľúč sa uloží na server služby,
- súkromný kľúč zostáva bezpečne uložený v zariadení.

Pri prihlásení sa používateľ overí:

- pomocou **Face ID**, **Touch ID** alebo
- kódom zariadenia.

Výhodou je, že passkeys sa **automaticky synchronizujú medzi Apple zariadeniami** používateľa cez iCloud, pričom zostávajú šifrované end-to-end.

Prihlasovacie kľúče v Google Chrome

Google Chrome podporuje prihlasovacie kľúče v kombinácii s **Google účtom** a **Google správcom hesiel**. Používateľ si môže vytvoriť passkey pre podporované webové služby a následne sa prihlasovať bez zadávania hesla.

Chrome umožňuje:

- používať passkeys uložené v Google účte,
- prihlasovať sa pomocou mobilného telefónu ako bezpečnostného zariadenia,
- kombinovať passkeys s biometrickým overením alebo PIN kódom zariadenia.

Prihlasovacie kľúče v Chrome fungujú naprieč platformami, čo znamená, že používateľ môže potvrdiť prihlásenie napríklad na počítači pomocou mobilného telefónu.

Výhody prihlasovacích kľúčov

Používanie passkeys prináša viacero zásadných výhod:

- odolnosť voči phishingu – neexistuje heslo, ktoré by bolo možné vylákať,
- vyššia bezpečnosť – využitie silnej kryptografie,
- pohodlie – rýchle prihlásenie bez zapamätania hesiel,
- eliminácia opakovania hesiel.

Z týchto dôvodov sú prihlasovacie kľúče považované za **budúcnosť autentifikácie** a postupne ich zavádzajú veľké technologické spoločnosti aj štátne systémy.

6.4 Dvojfaktorová autentifikácia (2FA)

Aktivácia 2FA pre správcu hesiel aj jednotlivé účty výrazne znižuje riziko ich kompromitácie. Druhý faktor môže byť napríklad mobilná aplikácia alebo hardvérový token.

6.5 Otázky

1. Prečo sú heslá stále dôležité aj pri moderných autentifikačných metódach?
a) Lebo nahrádzajú šifrovanie
b) Lebo sa používajú vo väčšine informačných systémov
c) Lebo zvyšujú rýchlosť internetu
d) Lebo automaticky bránia phishingu

2. Aká je odporúčaná minimálna dĺžka hesla podľa kapitoly?
a) 6 znakov
b) 8 znakov
c) 12 znakov
d) 20 znakov vždy povinne

3. Prečo je z pohľadu kombinatoriky často lepšie dlhé jednoduché heslo než krátke zložité?

a) Lebo špeciálne znaky sa dajú vypnúť
b) Lebo počet kombinácií rastie exponenciálne s dĺžkou hesla
c) Lebo brute force nefunguje na dlhé heslá
d) Lebo dlhé heslá sa nedajú hashovať

4. Ktorý príklad je nevhodný, lebo obsahuje osobné údaje?
a) MamRadCoko!2025
b) Peter1990
c) MrPsS4xt
d) X7@Q!9a$

5. Prečo je problém používať rovnaké heslo na viacerých službách?
a) Znižuje to rýchlosť prihlasovania
b) Jedno uniknuté heslo môže ohroziť viac účtov
c) Heslo sa potom nedá zmeniť
d) Správca hesiel to automaticky zakáže

6. Ktorá možnosť najlepšie vystihuje úlohu správcu hesiel?
a) Ukladá heslá v čitateľnej forme pre rýchlosť
b) Pomáha generovať a uchovávať silné jedinečné heslá
c) Nahrádza 2FA vo všetkých prípadoch
d) Slúži iba na kontrolu vírusov

7. Čo je „hlavné heslo“ v správcovi hesiel?
a) Heslo, ktoré môže byť rovnaké ako e-mailové heslo
b) Heslo ku všetkým uloženým heslám, musí byť silné a jedinečné
c) Dočasný SMS kód
d) PIN kód na odomknutie telefónu

8. Čo dokáže Google správca hesiel (v Chrome/Google účte) okrem ukladania?
a) Automaticky mení heslá na všetkých weboch bez súhlasu
b) Upozorní na slabé/opakované/uniknuté heslá
c) Vypne potrebu silného hesla
d) Zaručí anonymitu používateľa

9. Ktoré tvrdenie o Passkeys je správne?
a) Passkeys sú to isté ako SMS kódy
b) Passkeys sú založené na verejnom/súkromnom kľúči a používateľ nezadáva heslo
c) Passkeys vyžadujú vždy bezpečnostnú otázku
d) Passkeys znižujú bezpečnosť oproti heslám

10. Prečo je vhodné mať zapnuté 2FA aj pre správcu hesiel?
a) Lebo nahrádza potrebu silného hlavného hesla
b) Lebo znižuje riziko kompromitácie aj pri úniku hesla
c) Lebo zrýchľuje prihlásenie
d) Lebo umožní zdieľať účet s kolegami

7 Význam škodlivého kódu a riziká používania IKT

7.1 Škodlivý kód

Škodlivý kód, často označovaný aj pojmom **malvér**, má zásadný význam v oblasti kybernetickej bezpečnosti, pretože predstavuje jeden z najčastejších a zároveň najnebezpečnejších nástrojov, ktoré útočníci používajú na narušenie informačných systémov. Prostredníctvom škodlivého kódu môžu útočníci kradnúť citlivé údaje, meniť alebo ničiť informácie, získavať neoprávnený prístup k systémom alebo úplne paralyzovať prevádzku organizácií.

Za škodlivý kód sa považuje **akýkoľvek softvér alebo časť kódu, ktorá je vytvorená s úmyslom poškodiť, narušiť alebo zneužiť počítačový systém, sieť alebo údaje používateľa**. Malvér môže pôsobiť nenápadne a dlhodobo, alebo naopak okamžite spôsobiť viditeľné škody. Medzi najznámejšie a najčastejšie typy škodlivého kódu patria vírusy, červy, trójske kone, ransomvér, spyware, rootkity a keyloggery.

Medzi najznámejšie a najčastejšie typy škodlivého kódu patria **vírusy, červy, trójske kone, ransomvér, spyware, rootkity a keyloggery**, pričom každý z týchto typov má špecifické vlastnosti, spôsoby šírenia a dopady na bezpečnosť informačných systémov.

Počítačové vírusy sú formou škodlivého kódu, ktorá sa pripája k iným súborom alebo programom a aktivuje sa až po ich spustení používateľom. Ich šírenie je teda závislé od ľudskej činnosti, napríklad otvorenia infikovanej prílohy e-mailu alebo spustenia napadnutého programu. Vírusy môžu poškodzovať alebo mazať súbory, meniť systémové nastavenia a v niektorých prípadoch slúžia ako nosiče ďalšieho škodlivého kódu.

Počítačové červy sa na rozdiel od vírusov dokážu šíriť samostatne, bez zásahu používateľa. Využívajú zraniteľnosti v operačných systémoch a sieťach a môžu sa veľmi rýchlo rozšíriť na veľké množstvo zariadení. Červy často spôsobujú preťaženie sietí, spomalenie systémov alebo výpadky služieb, čím ohrozujú najmä dostupnosť informačných systémov.

Trójske kone sú škodlivé programy, ktoré sa tvária ako legitímny alebo užitočný softvér. Po ich spustení však vykonávajú škodlivé činnosti, napríklad inštalujú ďalší malvér, vytvárajú skryté prístupy do systému alebo zbierajú citlivé údaje. Trójske kone sa samy nešíria, ale spoliehajú sa na to, že ich používateľ dobrovoľne nainštaluje alebo spustí.

Ransomvér predstavuje mimoriadne nebezpečný typ škodlivého kódu, ktorého cieľom je zašifrovať údaje obete a následne požadovať výkupné za ich obnovenie. Moderné formy ransomvéru často kombinujú šifrovanie dát s ich krádežou a hrozbou zverejnenia, čo výrazne

zvyšuje tlak na obete. Ransomvérové útoky môžu úplne paralyzovať činnosť organizácií a spôsobiť rozsiahle finančné aj reputačné škody.

Spyware, teda špionážny softvér, je navrhnutý na skryté sledovanie činnosti používateľa. Zbiera informácie o jeho správaní, navštívených stránkach, prihlasovacích údajoch alebo iných citlivých dátach a odosiela ich útočníkovi. Spyware vážne ohrozuje súkromie používateľov a často je súčasťou širších útokov zameraných na krádež identity.

Rootkity patria medzi najnebezpečnejšie formy škodlivého kódu, pretože umožňujú útočníkovi získať a dlhodobo udržať skrytý administrátorský prístup k systému. Ich hlavnou vlastnosťou je schopnosť skrývať svoju prítomnosť aj prítomnosť iného malvéru, čím výrazne sťažujú detekciu a odstránenie infekcie. Rootkity sa často používajú pri cielených a dlhodobých útokoch.

Keyloggery sú nástroje určené na zaznamenávanie stlačení klávesnice. Pomocou nich môže útočník získať heslá, prihlasovacie údaje, čísla platobných kariet alebo obsah súkromnej komunikácie. Keyloggery môžu byť implementované ako softvér alebo hardvérové zariadenia a sú častým prostriedkom pri krádeži identity a finančných podvodoch.
Spoločne tieto typy škodlivého kódu predstavujú vážnu hrozbu pre dôvernosť, integritu a dostupnosť informačných systémov, a preto ich poznanie tvorí základ porozumenia kybernetickej bezpečnosti.

Škodlivý kód priamo ohrozuje tzv. **triádu kybernetickej bezpečnosti (CIA – Confidentiality, Integrity, Availability)**. V oblasti dôvernosti môže malvér neoprávnene získavať osobné, finančné alebo firemné údaje a odosielať ich útočníkovi. Z hľadiska integrity môže meniť, poškodzovať alebo mazať údaje bez vedomia používateľa, čo môže viesť k nesprávnym rozhodnutiam alebo finančným stratám. Dostupnosť systémov je ohrozená najmä v prípadoch, keď malvér zablokuje prístup k dátam alebo službám, napríklad prostredníctvom ransomvéru alebo útokov na sieťovú infraštruktúru.

Malvér často nepredstavuje izolovanú hrozbu, ale slúži ako **nosič alebo nástroj ďalších kybernetických útokov**.

Infikované zariadenia môžu byť po napadnutí škodlivým kódom **prevzaté pod kontrolu útočníka a zapojené do tzv. botnetov**, teda sietí infikovaných počítačov, serverov alebo iných zariadení, ktoré sú ovládané na diaľku bez vedomia ich majiteľov. Každé takéto zariadenie sa v botnete správa ako „bot“ a vykonáva príkazy útočníka, často bez akýchkoľvek viditeľných prejavov pre používateľa.

Botnety sa veľmi často využívajú na **masové útoky typu Distributed Denial of Service (DDoS)**. Pri týchto útokoch tisíce alebo dokonca milióny infikovaných zariadení súčasne zasielajú veľké

množstvo požiadaviek na cieľový server alebo službu. Výsledkom je zahltenie systému, jeho spomalenie alebo úplná nedostupnosť pre legitímnych používateľov. Takéto útoky môžu ochromiť webové stránky, online služby, bankové systémy alebo kritickú infraštruktúru.

Ďalším častým spôsobom využitia botnetov je **rozosielanie spamu**, teda nevyžiadanej elektronickej pošty alebo správ. Infikované zariadenia slúžia ako zdroj obrovského množstva e-mailov, ktoré môžu obsahovať reklamy, phishingové odkazy alebo škodlivé prílohy. Vďaka rozptýleniu spamu medzi veľké množstvo zariadení je pre bezpečnostné systémy náročnejšie takúto aktivitu odhaliť a zablokovať.

Botnety sa zároveň používajú aj na **ďalšie šírenie škodlivého kódu**. Infikované zariadenia môžu aktívne vyhľadávať nové obete, zneužívať zraniteľnosti v systémoch alebo rozosielať odkazy a prílohy obsahujúce malvér. Týmto spôsobom sa botnet neustále rozširuje a zvyšuje svoju útočnú kapacitu.

Z hľadiska kybernetickej bezpečnosti predstavujú botnety mimoriadne nebezpečnú hrozbu, pretože umožňujú útočníkom vykonávať rozsiahle a koordinované útoky s minimálnymi nákladmi. Používatelia si často ani neuvedomujú, že ich zariadenie je súčasťou botnetu, no zároveň sa nevedomky podieľajú na kybernetickej kriminalite a ohrozovaní iných systémov.

Dôsledky napadnutia škodlivým kódom môžu byť pre jednotlivcov aj organizácie veľmi vážne. Medzi najčastejšie dopady patria finančné straty spôsobené výkupným, výpadkami služieb alebo pokutami, poškodenie dobrého mena a dôvery zákazníkov, ako aj právne dôsledky, napríklad v prípade porušenia ochrany osobných údajov podľa GDPR. V extrémnych prípadoch môže útok viesť k dlhodobému prerušeniu činnosti organizácie.

Z tohto dôvodu je **detekcia a prevencia škodlivého kódu základnou súčasťou bezpečnostnej stratégie** každého informačného systému. Medzi kľúčové ochranné opatrenia patria antivírusové a antimalvérové riešenia, firewally, behaviorálna analýza správania aplikácií, pravidelné aktualizácie softvéru a operačných systémov, ako aj systematické zálohovanie dát. Účinná ochrana však nie je len technickou otázkou, ale zahŕňa aj vzdelávanie používateľov a dodržiavanie bezpečnostných politík.

Škodlivý kód tak tvorí jadro mnohých kybernetických hrozieb a jeho pochopenie je nevyhnutné pre ochranu údajov, zabezpečenie prevádzkovej kontinuity a splnenie zákonných požiadaviek v oblasti kybernetickej a informačnej bezpečnosti.

7.2 Ransomware

Ransomvér je špecifický a mimoriadne nebezpečný typ škodlivého kódu, ktorého cieľom je **zašifrovať údaje obete a následne požadovať výkupné za ich obnovenie**. V posledných rokoch

sa ransomvér stal jednou z najväčších hrozieb pre organizácie, školy, nemocnice aj verejné inštitúcie, keďže útoky často vedú k úplnej nedostupnosti kritických systémov.

Moderný ransomvér často nepracuje iba so šifrovaním dát, ale kombinuje tento útok s **krádežou a hrozbou zverejnenia citlivých informácií**, čím zvyšuje tlak na obeť. Zaplatenie výkupného však nezaručuje obnovenie dát a zároveň podporuje ďalšiu trestnú činnosť.

Účinná obrana proti ransomvéru si vyžaduje **komplexný prístup**, ktorý spája technické, organizačné aj personálne opatrenia. Keďže ransomvérové útoky sú často cielené a využívajú kombináciu technických zraniteľností a ľudských chýb, samotné jedno ochranné opatrenie nestačí. Bezpečnosť musí byť budovaná ako viacvrstvový systém, v ktorom jednotlivé prvky navzájom spolupracujú a dopĺňajú sa.

Základným pilierom ochrany proti ransomvéru je **pravidelné a bezpečné zálohovanie dát**. Zálohy umožňujú obnoviť údaje a systémy do funkčného stavu aj v prípade, že dôjde k ich zašifrovaniu škodlivým kódom. Mimoriadne dôležité je, aby boli zálohy uložené **mimo hlavného systému**, napríklad na externých médiách alebo v cloudovom úložisku, ktoré nie je trvalo pripojené k napadnutému zariadeniu. Rovnako významná je podpora **verziovania záloh**, vďaka ktorej je možné vrátiť sa k staršej, neinfikovanej verzii dát a eliminovať riziko obnovy už poškodených súborov. Pravidelné testovanie obnovy zo záloh je nevyhnutné na overenie ich funkčnosti v reálnej krízovej situácii.

Ďalším kľúčovým prvkom obrany je **používanie aktuálneho antivírusového a antimalvérového softvéru**. Takéto nástroje dokážu identifikovať známe hrozby na základe signatúr, ale čoraz častejšie využívajú aj behaviorálnu analýzu, ktorá sleduje podozrivé správanie aplikácií, napríklad hromadné šifrovanie súborov. Nevyhnutnou súčasťou účinnej ochrany je **aktívna ochrana v reálnom čase**, ktorá dokáže útok zastaviť ešte predtým, než dôjde k väčším škodám. Rovnako dôležité je pravidelné aktualizovanie databáz hrozieb, aby bezpečnostný softvér dokázal reagovať aj na najnovšie formy ransomvéru.

Spoločne tieto opatrenia vytvárajú základnú obrannú líniu proti ransomvérovým útokom. Ak sú správne nastavené a doplnené o ďalšie organizačné a personálne opatrenia, výrazne znižujú pravdepodobnosť úspešného útoku a minimalizujú jeho následky na dostupnosť dát a kontinuitu prevádzky.

Významnú úlohu zohráva aj **opatrnosť používateľov**, najmä pri otváraní e-mailových príloh a kliknutí na odkazy. Ransomvér sa často šíri prostredníctvom phishingových správ, ktoré sa tvária ako legitímna komunikácia. Pravidelné aktualizácie operačných systémov a aplikácií sú nevyhnutné, pretože útočníci často zneužívajú známe, no neopravované zraniteľnosti.

Dôležitou súčasťou ochrany je aj **obmedzenie prístupových práv**, využívanie princípu najmenších oprávnení a oddelenie administrátorských účtov od bežných používateľských účtov. Firewall, sieťová segmentácia a monitorovanie prevádzky môžu zabrániť šíreniu ransomvéru v rámci siete. Organizácie by mali mať zavedené mechanizmy na sledovanie neobvyklého správania, ako je hromadné šifrovanie súborov, a používať nástroje na centralizovanú analýzu logov.

Zásadným pravidlom pri ransomvérovom útoku je **neplatiť výkupné**, ale postupovať podľa pripraveného incident response plánu, izolovať napadnuté systémy a obnoviť dáta zo záloh.

7.3 Riziká používania IKT zariadení

Používanie zariadení informačných a komunikačných technológií (IKT), ako sú počítače, smartfóny, tablety, servery či sieťové prvky, je dnes neoddeliteľnou súčasťou každodenného života aj fungovania organizácií. IKT zariadenia umožňujú rýchlu komunikáciu, prístup k informáciám, automatizáciu procesov a efektívne riadenie činností. Zároveň však prinášajú aj **viaceré riziká**, ktoré môžu mať negatívny dopad na bezpečnosť, súkromie, psychickú pohodu používateľov aj na chod organizácií.

Tieto riziká sa dotýkajú nielen technickej oblasti, ale aj ľudského správania, organizačných procesov a právnej zodpovednosti. Ich pochopenie je preto základom bezpečného a zodpovedného používania IKT zariadení.

7.3.1 Bezpečnostné riziká

Medzi najvýznamnejšie riziká používania IKT zariadení patria **bezpečnostné riziká**, ktoré súvisia s ochranou systémov, sietí a údajov. Jedným z najčastejších problémov je výskyt **malvéru a počítačových vírusov**, ktoré môžu poškodiť zariadenie, spomaliť jeho činnosť, zničiť alebo zašifrovať dáta a v niektorých prípadoch umožniť útočníkovi úplnú kontrolu nad systémom. Škodlivý softvér sa často šíri prostredníctvom e-mailových príloh, infikovaných webových stránok alebo nelegálneho softvéru.

Významným bezpečnostným rizikom je aj **phishing a sociálne inžinierstvo**, pri ktorých útočníci cielene manipulujú používateľov, aby od nich získali citlivé informácie, ako sú prihlasovacie údaje, osobné údaje alebo čísla platobných kariet. Tieto útoky sú obzvlášť nebezpečné, pretože nevyužívajú technické zraniteľnosti, ale dôverčivosť a nepozornosť používateľov.

Ďalším rizikom je **neoprávnený prístup k systémom**, ku ktorému môže dôjsť v dôsledku slabých alebo opakovane používaných hesiel, nezabezpečených Wi-Fi sietí alebo chýb v konfigurácii systémov. Takýto prístup môže viesť k úniku citlivých údajov, ich zneužitiu alebo poškodeniu.

7.3.2 Riziká súkromia

Používanie IKT zariadení je úzko späté aj s rizikami v oblasti **ochrany súkromia**. Moderné aplikácie, sociálne siete a webové služby často zhromažďujú veľké množstvo osobných údajov o používateľoch, nie vždy s ich plným vedomím alebo porozumením. Ide napríklad o údaje o polohe, správaní na internete, kontaktoch alebo preferenciách.

Tieto údaje môžu byť následne **zneužité na cielenú reklamu**, sledovanie správania používateľov alebo dokonca na podvody a krádež identity. V prípade úniku osobných údajov z databáz môže dôjsť k vážnemu narušeniu súkromia jednotlivcov, čo má často dlhodobé následky.

7.3.3 Psychologické a sociálne riziká

Používanie IKT zariadení má dopad aj na **psychologickú a sociálnu oblasť**. Nadmerné používanie digitálnych technológií môže viesť k **závislosti od technológií**, ktorá sa prejavuje úzkosťou, stresom, poruchami spánku alebo zníženou schopnosťou sústredenia. Tento problém sa často týka najmä detí a mladistvých.

Významným spoločenským problémom je aj **kyberšikana**, ktorá prebieha prostredníctvom sociálnych sietí, správ alebo online platforiem. Kyberšikana môže mať vážne psychické následky na obete a je ťažšie ju kontrolovať než tradičné formy šikany.

Dlhodobé nahrádzanie osobných kontaktov digitálnou komunikáciou môže viesť k **sociálnej izolácii**, oslabeniu medziľudských vzťahov a zhoršeniu komunikačných schopností.

7.3.4 Riziká pre organizácie

Z pohľadu organizácií predstavujú IKT zariadenia aj **významné prevádzkové a ekonomické riziká**. Jedným z najvážnejších problémov je **strata dát**, ku ktorej môže dôjsť v dôsledku hardvérového zlyhania, ľudskej chyby alebo kybernetického útoku, napríklad ransomvéru.

Ďalším rizikom je **narušenie prevádzky**, keď výpadok informačných systémov môže ochromiť činnosť organizácie, spôsobiť finančné straty a poškodiť dôveru zákazníkov. Organizácie zároveň čelia riziku **nedodržania legislatívnych požiadaviek**, najmä v oblasti ochrany osobných údajov. Nedostatočné zabezpečenie IKT zariadení môže viesť k porušeniu právnych predpisov a vysokým sankciám.

7.3.5 Technické riziká

Technické riziká súvisia najmä so stavom a správou IKT infraštruktúry. **Zastaralý softvér** a operačné systémy často obsahujú bezpečnostné zraniteľnosti, ktoré môžu útočníci zneužiť. Problémy môžu vzniknúť aj pri **nekompatibilite systémov**, čo sťažuje ich integráciu a správu. Ďalším rizikom je **závislosť od technológií**, keď výpadok IKT infraštruktúry môže paralyzovať celú organizáciu. Bez správne nastavených záložných mechanizmov a plánov obnovy môže mať takýto výpadok vážne následky.

7.3.6 Zásady ochrany IKT zariadení

Na minimalizáciu rizík je nevyhnutné zaviesť **systematické ochranné opatrenia**. Základom je pravidelná aktualizácia softvéru, používanie antivírusovej a antimalvérovej ochrany, silné heslá a správna správa prístupov. Nevyhnutnou súčasťou ochrany je aj pravidelné zálohovanie dát a zabezpečenie bezpečného pripojenia k sieti.

Rovnako dôležitá je **fyzická bezpečnosť zariadení**, ako aj vzdelávanie používateľov v oblasti kybernetickej bezpečnosti. Monitorovanie systémov, logovanie udalostí a pravidelné audity pomáhajú včas odhaliť hrozby a reagovať na ne.

7.3.7 Kybernetické hrozby ohrozujúce IKT zariadenia

IKT zariadenia sú vystavené širokému spektru kybernetických hrozieb, medzi ktoré patria phishing, malware, ransomware, sociálne inžinierstvo, útoky na heslá, DDoS útoky, zero-day útoky, Man-in-the-Middle útoky, úniky dát a botnety. Tieto hrozby môžu mať vážne technické, finančné aj právne dôsledky a ich dopad neustále narastá s rastúcou digitalizáciou spoločnosti.

7.4 Otázky

1. **Prečo má škodlivý kód (malvér) zásadný význam v kybernetickej bezpečnosti?**
   a) Lebo zvyšuje výkon počítača a šetrí energiu
   b) Lebo je to najčastejší a najnebezpečnejší nástroj na narušenie systémov a krádež údajov
   c) Lebo slúži iba na zobrazovanie reklám
   d) Lebo nahrádza potrebu aktualizácií systému

2. **Ktorá definícia najlepšie vystihuje škodlivý kód?**
   a) Softvér, ktorý vždy chráni systém pred útokmi
   b) Softvér alebo časť kódu vytvorená s úmyslom poškodiť, narušiť alebo zneužiť systém/sieť/údaje
   c) Program určený iba na zálohovanie dát
   d) Nástroj na zlepšenie kvality internetového pripojenia

3. **Ktorý typ malvéru sa pripája k súborom/programom a aktivuje sa po spustení používateľom?**
   a) Počítačový červ
   b) Rootkit
   c) Počítačový vírus
   d) DDoS

4. **Ktorý typ malvéru sa dokáže šíriť samostatne bez zásahu používateľa a využíva zraniteľnosti?**
   a) Počítačový červ
   b) Trójsky kôň
   c) Spyware
   d) Keylogger

5. **Ktoré tvrdenie najlepšie opisuje trójskeho koňa?**
   a) Šíri sa autonómne po sieti a zahlcuje ju
   b) Tvári sa ako legitímny softvér, ale po spustení vykonáva škodlivé činnosti
   c) Vždy šifruje súbory a pýta výkupné
   d) Zobrazuje len reklamy bez ďalšieho rizika

6. **Čo je typické pre moderné ransomvérové útoky podľa textu?**
   a) Len zobrazenie reklám a presmerovanie prehliadača
   b) Len krádež hesiel cez zaznamenávanie klávesnice
   c) Šifrovanie dát + často aj krádež dát a hrozba zverejnenia
   d) Výhradne preťaženie siete bez zásahu do súborov

7. **Ktorý typ malvéru je určený na skryté sledovanie činnosti používateľa a zbieranie údajov?**
   a) Spyware
   b) Vírus
   c) DDoS
   d) Firewall

8. **Prečo sú rootkity považované za veľmi nebezpečné?**
   a) Pretože iba spomaľujú internet
   b) Pretože umožňujú skrytý administrátorský prístup a skrývajú prítomnosť malvéru
   c) Pretože sa nedajú šíriť a nepredstavujú riziko
   d) Pretože len odstraňujú vírusy zo systému

9. **Čo robí keylogger?**
   a) Blokuje neautorizované pripojenia do siete
   b) Zaznamenáva stlačenia klávesnice a získava heslá či citlivé údaje
   c) Šifruje súbory a žiada výkupné
   d) Zabezpečuje automatické aktualizácie systému

10. **Aké je zásadné pravidlo pri ransomvérovom útoku podľa textu?**
    a) Okamžite zaplatiť výkupné, aby sa dáta určite obnovili

b) Výkupné neplatiť a postupovať podľa incident response plánu, izolovať systémy a obnoviť zo záloh
c) Vypnúť firewall a antivírus, aby sa systém „nezasekol“
d) Ignorovať útok, lebo ransomvér sa vždy sám odstráni

11. **Ktoré tvrdenie najlepšie vystihuje riziká používania IKT zariadení?**
a) Riziká sú len technické a netýkajú sa ľudí
b) Riziká sa týkajú techniky, správania používateľov, organizácie aj právnej zodpovednosti
c) Riziká sa týkajú iba starých počítačov
d) Riziká vznikajú len pri používaní internetu v práci

12. **Ktorá situácia patrí medzi bezpečnostné riziká používania IKT?**
a) Zálohovanie dát do cloudu
b) Výskyt malvéru a vírusov, ktoré môžu poškodiť alebo zašifrovať dáta
c) Používanie silných hesiel
d) Zapnuté aktualizácie operačného systému

13. **Čo je typické pre phishing a sociálne inžinierstvo?**
a) Využíva technické zraniteľnosti jadra OS
b) Využíva dôverčivosť a nepozornosť používateľa na získanie citlivých informácií
c) Je to typ malvéru šíriaci sa cez USB
d) Je to bezpečnostný nástroj na detekciu útokov

14. **Ktorý faktor často vedie k neoprávnenému prístupu do systémov?**
a) Silné a jedinečné heslá
b) Slabé alebo opakovane používané heslá a nezabezpečené Wi-Fi siete
c) Pravidelné audity a logovanie
d) Šifrovanie komunikácie

15. **Ktorá situácia patrí medzi riziká súkromia?**
a) Aplikácie zbierajú údaje o polohe, správaní a preferenciách používateľov
b) Pravidelné zálohovanie dát
c) Aktualizácia operačného systému
d) Segmentácia siete

16. **Ktorý jav je psychologické/sociálne riziko používania IKT?**
a) SIEM analýza logov
b) Závislosť od technológií, stres, poruchy spánku a znížená schopnosť sústredenia
c) Šifrovanie disku
d) Antivírusová ochrana v reálnom čase

17. **Čo je kyberšikana?**
a) Technická chyba v softvéri
b) Zosmiešňovanie, obťažovanie alebo zastrašovanie cez online platformy
c) Typ ransomvéru
d) Metóda aktualizácie operačného systému

18. **Ktoré tvrdenie najlepšie opisuje riziká pre organizácie?**
    a) Organizácie nemajú riziká, iba jednotlivci
    b) Riziká zahŕňajú stratu dát, narušenie prevádzky, finančné straty a pokuty za nedodržanie legislatívy
    c) Jediným rizikom je pomalý internet
    d) Riziká sa týkajú iba IT oddelenia, nie celej organizácie

19. **Čo je typické technické riziko v IKT infraštruktúre?**
    a) Zastaralý softvér so zraniteľnosťami a problémy s kompatibilitou systémov
    b) Silné heslá
    c) Pravidelné aktualizácie
    d) Monitorovanie a audit

20. **Ktoré opatrenia patria medzi zásady ochrany IKT zariadení podľa textu?**
    a) Vypnutie aktualizácií a používanie jedného hesla
    b) Aktualizácie, antivírus/antimalvér, silné heslá, správa prístupov, zálohovanie a bezpečné pripojenie
    c) Zdieľanie účtov medzi používateľmi
    d) Používanie nelegálneho softvéru, lebo je „overený“ komunitou

8 Základné zraniteľnosti smartfónov

Smartfóny sa stali neoddeliteľnou súčasťou každodenného života. Používame ich na komunikáciu, prácu, bankovníctvo, navigáciu, nákupy aj prístup k školským či firemným systémom. Z pohľadu kybernetickej bezpečnosti však smartfón nie je len „telefón“, ale plnohodnotný počítač so stálym pripojením na internet, s množstvom senzorov a s vysokou koncentráciou osobných údajov. V praxi to znamená, že kompromitovaný smartfón môže útočníkovi poskytnúť oveľa viac než kompromitovaný počítač v internetovej kaviarni – často totiž obsahuje identitu používateľa v podobe uložených účtov, tokenov, autentifikačných aplikácií a biometrických údajov.

V smartfónoch sa nachádza veľké množstvo citlivých informácií – fotografie, kontakty, správy, údaje o polohe, prístupy do e-mailu, sociálnych sietí a často aj do bankových aplikácií. Útok na smartfón môže spôsobiť finančné škody, únik osobných údajov, krádež identity alebo zneužitie zariadenia na ďalšie útoky (napr. rozosielanie spamu, podvody cez kontakty, šírenie škodlivých odkazov). Zároveň ide o zariadenie, ktoré používateľ nosí neustále pri sebe, čím sa zvyšuje riziko jeho straty, krádeže alebo neúmyselného zdieľania údajov v nevhodnom prostredí.

Poznanie najčastejších zraniteľností preto umožňuje používateľom znižovať riziko a prijímať vhodné bezpečnostné opatrenia. Zraniteľnosť pritom nemusí znamenať iba „chybu v systéme“. Veľmi často je zraniteľnosťou nesprávny návyk používateľa (napr. kliknutie na podvodný odkaz) alebo nevhodné nastavenie (napr. priveľa oprávnení aplikáciám).

8.1 Najčastejšie zraniteľnosti smartfónov

8.1.1 Zastaralý alebo nezabezpečený operačný systém

Jednou z najčastejších zraniteľností smartfónov je používanie zastaraného operačného systému alebo dlhodobo neaktualizovaného firmvéru. Staršie verzie Androidu alebo iOS môžu obsahovať známe bezpečnostné chyby, ktoré sú verejne zdokumentované a útočníci ich v praxi aktívne zneužívajú. Je dôležité pochopiť, že v momente, keď je zraniteľnosť odhalená a zverejnená, vznikajú dve skupiny ľudí: vývojári, ktorí pripravujú opravu, a útočníci, ktorí sa snažia chybu zneužiť čo najrýchlejšie, kým ju používatelia neopravili aktualizáciou.

Ak výrobca alebo operátor prestane poskytovať bezpečnostné aktualizácie, zariadenie sa stáva zraniteľné aj bez toho, aby používateľ urobil chybu. Problém je výrazný najmä pri lacnejších zariadeniach, ktoré dostávajú aktualizácie kratšie obdobie. Zároveň platí, že aj keď aktualizácia existuje, používateľ ju často odkladá – napríklad kvôli obavám, že sa zariadenie spomalí alebo že aktualizácia „niečo pokazí“. Z bezpečnostného hľadiska však odkladanie znamená ponechanie otvorených dverí útočníkovi.

Aktualizácie pritom nie sú len o nových funkciách – v prvom rade opravujú kritické chyby. Z tohto dôvodu je pravidelné aktualizovanie systému a aplikácií jedným zo základných krokov ochrany. V praxi je vhodné skontrolovať nielen „verziu systému“, ale aj dátum poslednej bezpečnostnej záplaty (security patch level). Ak je patch starý mnoho mesiacov, ide o zvýšené riziko.

Typický scenár z praxe: používateľ má starší telefón bez aktualizácií a pripojí sa do verejnej Wi-Fi siete. Útočník využije zraniteľnosť v systéme alebo prehliadači a získa prístup k zariadeniu alebo aspoň k dátam, ktoré zariadenie prenáša.

8.1.2 Aplikácie z nedôveryhodných zdrojov

Ďalším častým rizikom je inštalácia aplikácií mimo oficiálnych obchodov, ako sú Google Play alebo App Store. Aplikácie stiahnuté z neznámych webov (napr. APK súbory) môžu obsahovať škodlivý kód, ktorý kradne údaje, sleduje používateľa alebo umožní útočníkovi vzdialený prístup k zariadeniu. Útočníci často zneužívajú aj to, že používateľ chce získať platený obsah zadarmo (pirátstvo), alebo si nainštaluje „užitočnú“ aplikáciu, ktorá v skutočnosti slúži na zber údajov.

Riziko však existuje aj v oficiálnych obchodoch, kde sa občas objavia škodlivé alebo klamlivé aplikácie. V takom prípade aplikácia zvyčajne nepôsobí ako „vírus“, ale skôr ako bežná aplikácia, ktorá žiada neprimerané oprávnenia alebo zobrazuje agresívnu reklamu. Používateľ si často neuvedomí, že skutočnou cenou za „zadarmo“ je jeho súkromie alebo bezpečnosť.
Preto je dôležité všímať si hodnotenia, recenzie, počet stiahnutí, identitu vývojára a najmä oprávnenia, ktoré aplikácia vyžaduje. Dôležité je aj rozlišovať medzi „užitočným oprávnením“ (napr. aplikácia na kameru potrebuje kameru) a „podozrivým oprávnením“ (napr. baterka potrebuje kontakty, SMS a mikrofón).

Typický scenár z praxe: falošná aplikácia „kuriérske sledovanie“ alebo „zľavový kupón“ si vyžiada prístup k SMS správam a následne zachytí jednorazové overovacie kódy (OTP), ktoré sú používané pri prihlasovaní do banky.

8.1.3 Slabé zabezpečenie zariadenia

Mnoho používateľov zanedbáva základné bezpečnostné nastavenia. Smartfón bez zámku obrazovky alebo so slabým PIN kódom je veľmi ľahko zneužiteľný pri strate, krádeži alebo aj krátkodobom odložení bez dozoru. Útočník nemusí zariadenie „hacknúť“ – stačí mu fyzický prístup. Ak je telefón odomknutý, môže okamžite získať prístup k e-mailom, dokumentom, fotografiám či bankovým aplikáciám.

Rizikom je aj to, keď používateľ povolí odomykanie jednoduchým vzorom alebo používa rovnaký PIN ako na iné služby. Opakovanie PIN-u alebo hesla znamená, že únik jednej informácie môže otvoriť viacero účtov. Rovnako nebezpečné je automatické pripájanie k neznámym Wi-Fi sieťam alebo ponechanie zapnutých zdieľacích funkcií bez kontroly.
Silný zámok obrazovky, šifrovanie a správne nastavenie bezpečnosti sú pritom dostupné aj bežnému používateľovi. Moderné systémy navyše umožňujú automatické uzamknutie po krátkom čase, skrytie obsahu notifikácií na uzamknutej obrazovke a ochranu citlivých aplikácií biometrickým zámkom.

Typický scenár z praxe: používateľ nechá telefón na stole v reštaurácii, niekto ho vezme, otvorí e-mail a cez „zabudnuté heslo“ získa prístup k ďalším účtom.

8.1.4 Zraniteľnosti v bezdrôtovej komunikácii

Smartfóny používajú viacero bezdrôtových technológií, ktoré zvyšujú komfort, ale zároveň rozširujú útočný priestor. Pri Wi-Fi pripojení je rizikom najmä používanie verejných sietí, kde môže útočník vykonávať útok typu man-in-the-middle, teda zachytávať alebo meniť prenášané údaje. Aj keď dnes veľa služieb používa šifrovanie, stále existujú situácie, keď môže byť používateľ oklamaný (napr. falošná Wi-Fi sieť so zhodným názvom).

Bluetooth môže byť zneužitý pri zle zabezpečenom párovaní alebo pri starších zraniteľnostiach, ktoré umožňovali neautorizovaný prístup či šírenie malvéru. Rizikom je aj „viditeľnosť“ zariadenia a automatické prijímanie požiadaviek. NFC technológia, používaná pri platbách alebo párovaní, môže byť zneužitá pri podvodných tagoch (napr. nalepený QR/NFC štítok, ktorý presmeruje na škodlivú stránku).

Prevenciou je vypínať nepotrebné bezdrôtové funkcie, nepárovať sa s neznámymi zariadeniami a vyhýbať sa nezabezpečeným sieťam. V praxi to znamená aj kontrolu uložených Wi-Fi sietí a vypnutie automatického pripájania.

8.1.5 Prístupové práva (oprávnenia) aplikácií

Zraniteľnosťou smartfónov často nie je len technická chyba, ale aj zle nastavené oprávnenia aplikácií. Aplikácie môžu vyžadovať prístup k mikrofónu, fotoaparátu, polohe, kontaktom alebo súborom, aj keď ich na svoju funkciu nepotrebujú. Používateľ tieto oprávnenia často potvrdí automaticky, bez premyslenia, pričom si neuvedomuje dôsledky.

Takéto správanie môže viesť k sledovaniu polohy, odpočúvaniu, zberu kontaktov alebo k odosielaniu údajov tretím stranám. Problematické je aj to, že niektoré aplikácie zhromažďujú údaje „na pozadí“ a používateľ nemá okamžitú spätnú väzbu. Preto je vhodné pravidelne kontrolovať oprávnenia v nastaveniach systému, využívať režim „povoliť len pri používaní aplikácie“ a odoberať prístup tam, kde nie je opodstatnený.

Príklad: aplikácia na úpravu fotiek potrebuje prístup k fotkám – to je logické. Ak však vyžaduje mikrofón, SMS alebo kontakty, je to dôvod na otázku „prečo?“.

8.1.6 Sociálne inžinierstvo a phishing

Jednou z najčastejších metód útoku na smartfóny je manipulácia používateľa. Útočníci posielajú falošné SMS správy, e-maily alebo notifikácie, ktoré sa tvária ako správa od banky, kuriéra, školy či štátneho úradu. Cieľom býva vylákanie prihlasovacích údajov alebo presmerovanie na podvodnú stránku, kde používateľ zadá svoje údaje. Mobilné prostredie navyše spôsobuje, že používateľ často nevidí celú webovú adresu a ľahšie si nevšimne podvod. Phishing sa čoraz viac kombinuje aj s QR kódmi. Používateľ naskenuje kód (napr. „zaplaťte parkovné“) a otvorí škodlivý odkaz bez toho, aby si všimol podozrivú doménu. V niektorých prípadoch sa útočníci vydávajú aj za technickú podporu a snažia sa presvedčiť používateľa, aby nainštaloval „pomocnú“ aplikáciu na vzdialený prístup.

Najlepšou obranou je overovanie zdroja správy, neklikať na neznáme odkazy a využívať oficiálne aplikácie alebo weby. Základná zásada znie: ak správa vytvára tlak (čas, strach, výhra), treba spomaliť a overiť informáciu.

8.1.7 Zálohovanie a cloud

Cloudové služby zvyšujú komfort, no prinášajú aj riziká. Ak používateľ nemá účet zabezpečený silným heslom a dvojfaktorovým overením, útočník môže získať prístup k zálohám, fotografiám, kontaktom či dokumentom. Útočník často nepotrebuje priamo napadnúť telefón – stačí mu prelomiť konto používateľa v cloude.

Zraniteľnosťou je aj automatická synchronizácia medzi zariadeniami. Tá môže viesť k nechcenému zdieľaniu údajov (napr. v rodinnom účte), alebo k tomu, že škodlivé zmeny sa prenesú aj do záloh. Bezpečná prax zahŕňa šifrovanie, 2FA, kontrolu nastavení zdieľania a pravidelné vytváranie záloh aj mimo cloudu (offline). Výhodou offline záloh je, že ich neohrozí kompromitácia online účtu.

8.2 Ako zabezpečiť smartfón

Ochrana smartfónu je najúčinnejšia vtedy, keď je postavená na kombinácii technických nastavení a správnych používateľských návykov. Kľúčové je, aby bezpečnosť bola „zapnutá“ už od prvého dňa používania zariadenia a aby používateľ rozumel základným princípom ochrany. Bezpečnosť v praxi znamená znížiť pravdepodobnosť útoku a zároveň znížiť dopad, ak útok nastane.

8.2.1 Zabezpečenie zariadenia prihlasovaním

Zámok obrazovky je prvá obranná línia. Ideálne je používať dlhší PIN alebo heslo a v prípade biometrie mať vždy nastavený aj bezpečný záložný PIN. Okrem samotného zámku je vhodné nastaviť krátky čas automatického uzamknutia a obmedziť zobrazenie citlivých notifikácií na uzamknutej obrazovke (napr. neukazovať obsah SMS a e-mailov).

8.2.2 Aktualizácia systému a aplikácií

Bezpečnostné záplaty riešia konkrétne chyby, ktoré útočníci môžu zneužívať. Pravidelné aktualizácie sú prakticky najlacnejšou a najefektívnejšou formou ochrany. Bezpečnostný prínos je najvyšší vtedy, ak sú aktualizácie automatické a používateľ ich dlhodobo neodkladá.

8.2.3 Inštalácia aplikácií len z oficiálnych obchodov

Aplikácie z neznámych zdrojov sú častým nosičom škodlivého kódu. Aj pri aplikáciách z oficiálnych obchodov je vhodné kontrolovať reputáciu vývojára, počet stiahnutí, recenzie a najmä oprávnenia. Pri pochybnostiach je bezpečnejšie aplikáciu neinštalovať alebo hľadať alternatívu.

8.2.4 Kontrola oprávnení aplikácií

Používateľ by mal pravidelne kontrolovať, ktoré aplikácie majú prístup ku kamere, mikrofónu, polohe, SMS alebo kontaktom. Vhodné je využívať nastavenie „povoliť len pri používaní“ a odobrať prístup aplikáciám, ktoré ho nepotrebujú. Ide o dôležitý nástroj ochrany súkromia aj prevencie zneužitia.

8.2.5 Ochrana pri pripojení na internet

Pri verejných Wi-Fi sieťach sa odporúča používať VPN a vyhýbať sa citlivým činnostiam, ako je bankovníctvo alebo prístup do školských/firemých systémov, ak nie je pripojenie dôveryhodné. Bluetooth a NFC je vhodné vypnúť, keď nie sú potrebné, a nepárovať sa s neznámymi zariadeniami.

8.2.6 Zálohovanie a šifrovanie dát

Šifrovanie chráni údaje v prípade krádeže zariadenia. Zálohy by mali byť chránené silným heslom a ideálne aj 2FA, pričom používateľ by mal vedieť, čo presne sa do cloudu synchronizuje. Pre citlivé dáta je vhodné kombinovať cloudovú a offline zálohu.

8.2.7 Ochrana pred podvodmi

Pri správach a odkazoch platí zásada: ak správa vyvoláva tlak (strach, časová tieseň, výhra), je pravdepodobne podozrivá. Používateľ by mal overovať adresy stránok, nepodliehať nátlaku a v prípade pochybností kontaktovať organizáciu cez oficiálny kanál (nie cez číslo alebo odkaz zo správy).

8.2.8 Lokalizácia pri strate alebo krádeži

Aktivované „Nájsť moje zariadenie“ alebo „Find My iPhone“ umožňuje telefón lokalizovať, uzamknúť alebo vymazať. V praxi ide o jeden z najdôležitejších krokov ochrany osobných údajov pri krádeži, pretože aj keď sa telefón nevráti, dáta nemusia skončiť u útočníka.

8.2.9 Bezpečnostné signály možnej infekcie

Používateľ by mal vnímať nezvyčajné správanie telefónu: rýchle vybíjanie batérie, prehrievanie, zvýšenú spotrebu dát, samovoľné reštarty, neznáme aplikácie alebo vyskakovacie reklamy. Tieto prejavy nemusia vždy znamenať malvér, ale sú dôvodom na kontrolu zariadenia, sken bezpečnostným nástrojom a revíziu nainštalovaných aplikácií.

8.3 Príklady zabezpečenia smartfónov

8.3.1 Príklad 1: Použitý mobil od známeho (Android)

Pri použitom zariadení je kľúčové odstrániť riziko, že v ňom zostali staré účty alebo škodlivé nastavenia. Odporúča sa vykonať továrenské nastavenie, prihlásiť sa vlastným účtom, nastaviť zámok obrazovky, zapnúť šifrovanie a aktualizovať systém. Následne je vhodné skontrolovať

oprávnenia, zapnúť Play Protect, zakázať inštaláciu z neznámych zdrojov a aktivovať „Nájsť moje zariadenie“. Pri verejných sieťach sa odporúča VPN a vypnuté Bluetooth/NFC, ak nie sú potrebné.

8.3.2 Príklad 2: Zálohovanie dát v Android telefóne

Zálohovanie sa dá realizovať cez Google One alebo výrobcu (napr. Samsung), pričom je dôležité mať účet chránený silným heslom a 2FA. Praktické je tiež pravidelne uložiť kópiu fotografií a dokumentov aj offline (napr. na PC alebo externý disk). Pri pokročilých nástrojoch na zálohovanie treba dbať na to, aby boli dôveryhodné a aby zálohy neboli prístupné bez ochrany.

8.4 Kontrola zabezpečenia smartfónu (Android a iPhone)

Používanie smartfónu bez správneho nastavenia bezpečnosti predstavuje významné riziko pre ochranu osobných údajov, financií aj súkromia používateľa. Tento návod slúži ako praktická príručka, ktorá krok za krokom vysvetľuje, ako skontrolovať a nastaviť bezpečnostné prvky v mobilných zariadeniach so systémom **Android** a **iOS (iPhone)**.

8.4.1 Kontrola zabezpečenia zariadenia v systéme Android

Zámok obrazovky a autentifikácia
Zámok obrazovky predstavuje **základnú obrannú líniu** smartfónu. Bez neho má každý, kto získa zariadenie do rúk, okamžitý prístup k e-mailom, fotografiám, aplikáciám aj uloženým heslám.

Postup kontroly:

1. Otvor **Nastavenia**
2. Vyber **Zabezpečenie** alebo **Zabezpečenie a súkromie**
3. Klikni na **Zámok obrazovky**

Odporúčané nastavenia:

- PIN kód s minimálne **6 číslicami**
- Heslo (alfanumerické)
- Biometria (odtlačok prsta / rozpoznanie tváre) **v kombinácii s PIN-om**

Nevhodné sú jednoduché kombinácie ako *1234*, *0000* alebo jednoduché vzory.

Aktualizácie operačného systému
Bezpečnostné aktualizácie opravujú **konkrétne zraniteľnosti**, ktoré sú často verejne známe a zneužívané.

Postup:

1. **Nastavenia**
2. **O telefóne**
3. **Aktualizácie systému**

Skontroluj:
- verziu Androidu,
- dátum bezpečnostnej záplaty.

Ak zariadenie nedostalo aktualizáciu dlhšie než niekoľko mesiacov, ide o **zvýšené riziko**.

Kontrola oprávnení aplikácií
Aplikácie môžu získať prístup k citlivým funkciám, ktoré výrazne zasahujú do súkromia.

Postup:
1. **Nastavenia**
2. **Súkromie**
3. **Správca oprávnení**

Skontroluj samostatne:
- Kamera
- Mikrofón
- Poloha
- Kontakty
- Súbory

Ak napríklad kalkulačka žiada prístup ku kontaktom, ide o **varovný signál**.

Google Play Protect
Google Play Protect slúži ako základná ochrana pred škodlivými aplikáciami.

Postup:
1. Otvor **Google Play**
2. Klikni na profil → **Play Protect**
3. Over, či je zapnutý a kedy prebehla posledná kontrola

Inštalácia aplikácií z neznámych zdrojov
Inštalácia APK súborov z internetu patrí medzi **najčastejšie príčiny infekcie malvérom**.

Postup:
1. **Nastavenia**
2. **Zabezpečenie**
3. **Inštalácia neznámych aplikácií**

Ideálne nastavenie: **zakázané pre všetky aplikácie**

Funkcia „Nájsť moje zariadenie“
Táto funkcia je kľúčová pri strate alebo krádeži zariadenia.

Postup:
1. **Nastavenia**
2. **Zabezpečenie**
3. **Nájsť moje zariadenie**

Umožňuje:

- lokalizáciu zariadenia,
- vzdialené uzamknutie,
- vymazanie dát.

Bezdrôtové rozhrania (Wi-Fi, Bluetooth, NFC)
Odporúčania:

- vypínať Bluetooth a NFC, ak sa nepoužívajú,
- odstraňovať uložené neznáme Wi-Fi siete,
- nepripájať sa automaticky na otvorené siete.

8.4.2 Kontrola zabezpečenia zariadenia v systéme iOS (iPhone)

Zabezpečenie – Face ID / Touch ID
Postup:

1. **Nastavenia**
2. **Face ID a kód** / **Touch ID a kód**

Odporúčania:

- nepoužívať 4-miestny kód,
- nastaviť alfanumerický kód,
- aktivovať Face ID / Touch ID.

Aktualizácie iOS
Apple pravidelne vydáva bezpečnostné aktualizácie.

Postup:

1. **Nastavenia**
2. **Všeobecné**
3. **Aktualizácia softvéru**

Aktualizácie by mali byť zapnuté **automaticky**.

Oprávnenia aplikácií v iOS
Postup:

1. **Nastavenia**
2. **Súkromie a bezpečnosť**

Kontroluj:

- Poloha (Nikdy / Pri používaní),
- Kamera,
- Mikrofón,
- Fotky (vybrané položky).

Sledovanie aplikácií (Tracking)
Postup:

1. **Nastavenia**
2. **Súkromie a bezpečnosť**
3. **Sledovanie**

Odporúča sa **zakázať sledovanie**.

Funkcia „Nájsť iPhone“
Postup:

1. **Nastavenia**
2. **[tvoje meno]**
3. **Nájsť**
4. Zapnúť **Nájsť iPhone**

Zabezpečenie Apple ID
Apple ID je kľúč ku všetkým dátam.
Postup:

1. **Nastavenia**
2. **[tvoje meno]**
3. **Heslo a zabezpečenie**
4. Zapnúť **dvojfaktorové overovanie (2FA)**

8.5 Otázky

1. Prečo je smartfón z pohľadu kybernetickej bezpečnosti považovaný za plnohodnotný počítač?
a) Pretože má väčší displej ako počítač
b) Pretože slúži len na telefonovanie
c) Pretože má trvalé pripojenie na internet a obsahuje veľké množstvo citlivých údajov
d) Pretože sa používa iba doma

2. Prečo je zastaraný operačný systém smartfónu vážnym bezpečnostným rizikom?
a) Spôsobuje rýchlejšie vybíjanie batérie
b) Obsahuje známe zraniteľnosti, ktoré môžu útočníci zneužiť
c) Znižuje kvalitu fotografií
d) Neumožňuje inštaláciu aplikácií

3. Aké je hlavné riziko inštalácie aplikácií z neznámych zdrojov?
a) Aplikácie spotrebujú viac pamäte
b) Môžu obsahovať škodlivý kód alebo kradnúť údaje
c) Nezobrazujú reklamu
d) Nevyžadujú žiadne oprávnenia

4. Prečo je smartfón bez zámku obrazovky nebezpečný?
a) Skracuje životnosť zariadenia
b) Spôsobuje prehrievanie
c) Každý s fyzickým prístupom môže okamžite získať prístup k dátam
d) Neumožňuje používať aplikácie

5. Ktorá situácia predstavuje typický príklad zneužitia oprávnení aplikácie?
a) Fotoaparát potrebuje prístup ku kamere
b) Navigácia potrebuje prístup k polohe
c) Aplikácia baterky žiada prístup ku kontaktom a SMS
d) Hudobná aplikácia prehráva hudbu

6. Aké je hlavné riziko používania verejných Wi-Fi sietí?
a) Vyššia spotreba dát
b) Slabší signál
c) Útok typu man-in-the-middle a odpočúvanie komunikácie
d) Vyššia cena pripojenia

7. Prečo sú prístupové práva aplikácií považované za častú zraniteľnosť?
a) Sú automaticky zakázané
b) Sú viditeľné len pre vývojárov
c) Používatelia ich často povoľujú bez premyslenia
d) Nemajú vplyv na súkromie

8. Čo je hlavným cieľom phishingu na smartfónoch?
a) Spomaliť zariadenie
b) Zobraziť reklamu
c) Vylákať prihlasovacie alebo osobné údaje používateľa
d) Aktualizovať operačný systém

9. Prečo je zabezpečenie cloudového účtu kľúčové pre bezpečnosť smartfónu?
a) Cloud slúži len na zálohovanie aplikácií
b) Útočník môže získať dáta aj bez fyzického prístupu k telefónu
c) Cloud zvyšuje výkon telefónu
d) Cloud neobsahuje citlivé údaje

10. Ktorý príznak môže naznačovať možnú infekciu smartfónu?
a) Jasný displej
b) Rýchle vybíjanie batérie a zvýšená spotreba dát
c) Aktualizácia systému
d) Príchod SMS správy

9 Princípy vzdialeného prístupu a bezpečnostné zásady pri práci na diaľku

9.1 Všeobecné princípy

Práca na diaľku (remote work) predstavuje v súčasnosti štandardný model fungovania organizácií, vzdelávacích inštitúcií aj verejnej správy. Používatelia pristupujú k informačným systémom z rôznych lokalít, často mimo bezpečne kontrolovaného prostredia organizácie. Tento model prináša výrazné výhody z hľadiska flexibility a dostupnosti, avšak súčasne zásadne mení bezpečnostný model organizácie.

Kým v tradičnom prostredí boli systémy chránené perimetrom (firewall, interná sieť), pri práci na diaľku sa tento perimetr rozpadá. Zariadenia, siete aj samotní používatelia sa nachádzajú mimo centrálnej kontroly, čo vytvára nové útokové vektory. Útočníci môžu cieliť priamo na koncové zariadenia, zneužívať nezabezpečené pripojenia alebo manipulovať používateľov prostredníctvom sociálneho inžinierstva.

Z tohto dôvodu sa bezpečnosť vzdialeného prístupu musí opierať o viacvrstvový prístup, ktorý zahŕňa technické opatrenia, procesné pravidlá aj bezpečnostné povedomie používateľov. Cieľom je minimalizovať riziko neoprávneného prístupu, úniku dát, kompromitácie účtov a narušenia dostupnosti služieb.

9.2 Základné princípy vzdialeného prístupu

Základom bezpečného vzdialeného prístupu je spoľahlivé overenie identity používateľa. Autentizácia už dávno neznamená len zadanie hesla. Moderné systémy využívajú viacfaktorové overovanie (MFA), ktoré kombinuje viacero nezávislých faktorov – napríklad znalosť (heslo), vlastníctvo (mobilné zariadenie alebo bezpečnostný kľúč) a biometrické údaje. Tento prístup výrazne znižuje riziko zneužitia účtu, aj keď dôjde k úniku hesla.

Rovnako dôležitým prvkom je zabezpečenie komunikácie. Dáta prenášané cez internet sú vystavené riziku odpočúvania alebo manipulácie, najmä v prípade verejných alebo nedôveryhodných sietí. Z tohto dôvodu sa využíva šifrovanie prostredníctvom protokolov ako TLS (pri webových službách) alebo technológií virtuálnych privátnych sietí (VPN), ktoré vytvárajú zabezpečený komunikačný tunel medzi používateľom a cieľovým systémom.

Ďalším kľúčovým princípom je riadenie prístupových práv. Používateľ by mal mať prístup len k tým systémom a údajom, ktoré nevyhnutne potrebuje na výkon svojej práce. Tento princíp, označovaný ako „least privilege“, minimalizuje dopady bezpečnostného incidentu a znižuje riziko interných chýb alebo zneužitia oprávnení.

Bezpečný vzdialený prístup si vyžaduje aj dôsledný audit a monitoring. Každá aktivita používateľa by mala byť zaznamenaná a analyzovaná. Moderné systémy dokážu identifikovať anomálie, ako napríklad prihlásenie z neobvyklej geografickej lokality, prístup v netypickom čase alebo neštandardné správanie používateľa. Takéto mechanizmy umožňujú včasnú detekciu incidentov a rýchlu reakciu.

Významným aspektom je aj oddelenie pracovného a súkromného prostredia. Používanie jedného zariadenia na viacero účelov zvyšuje riziko infekcie malvérom alebo úniku dát. Ideálnym riešením je využívanie spravovaných zariadení, prípadne virtualizovaných pracovných prostredí, kde sú pracovné dáta izolované od súkromného používania.

9.3 Bezpečnostné zásady pri práci na diaľku

Pri práci na diaľku zohráva zásadnú úlohu samotný používateľ. Aj keď sú implementované technické bezpečnostné opatrenia, nesprávne správanie môže viesť k ich obchádzaniu alebo úplnému zlyhaniu ochrany.

Základom je používanie silných a unikátnych hesiel. Heslá by mali byť dostatočne dlhé a komplexné, pričom ich opakované používanie na viacerých službách predstavuje významné riziko. V kombinácii s viacfaktorovým overovaním poskytujú účinnú ochranu proti útokom typu credential stuffing alebo phishing.

Pri pripájaní k firemným systémom je nevyhnutné využívať zabezpečené pripojenie. VPN zabezpečuje dôvernosť komunikácie a znižuje riziko odpočúvania, avšak sama o sebe nezaručuje úplnú bezpečnosť. Používateľ musí byť stále obozretný a vyhýbať sa podozrivým aktivitám.

Zariadenie, z ktorého sa používateľ pripája, predstavuje kritický prvok bezpečnosti. Neaktualizovaný operačný systém alebo aplikácie môžu obsahovať zraniteľnosti, ktoré útočníci aktívne zneužívajú. Pravidelné aktualizácie, používanie bezpečnostného softvéru a správna konfigurácia systému sú preto nevyhnutné.

Ochrana dát zahŕňa ich šifrovanie, kontrolu prístupu a pravidelné zálohovanie. Zálohy predstavujú poslednú líniu obrany, napríklad pri ransomvérovom útoku. Bez funkčných záloh môže byť obnova dát nemožná alebo finančne náročná.

Pri komunikácii je potrebné počítať s tým, že útočníci často využívajú sociálne inžinierstvo. Phishingové správy môžu byť veľmi presvedčivé a často napodobňujú legitímne služby. Používateľ by mal vždy overovať zdroj informácií a vyhýbať sa impulzívnym reakciám.

Vzdelávanie používateľov je preto neoddeliteľnou súčasťou bezpečnostnej stratégie. Informovaný používateľ dokáže identifikovať hrozby a správne reagovať, čím výrazne znižuje pravdepodobnosť úspešného útoku.

9.4 Webové stránky a bezpečnosť

Webové aplikácie predstavujú základnú platformu pre vzdialený prístup k službám. Používateľ prostredníctvom webového prehliadača pristupuje k e-mailom, informačným systémom, cloudovým službám alebo databázam.

Bezpečnosť webových stránok je preto kľúčová. Z technického hľadiska zahŕňa šifrovanie komunikácie, ochranu proti škodlivému kódu, validáciu vstupov a správu identít. Z pohľadu používateľa je však rovnako dôležité vedieť rozpoznať dôveryhodný web.

9.4.1 Bezpečný web

Bezpečný web zabezpečuje dôvernosť, integritu a autenticitu komunikácie. Používanie protokolu HTTPS je základným predpokladom, no samo o sebe nestačí. Útočníci dnes bežne využívajú platné certifikáty aj na phishingových stránkach.

Používateľ by mal hodnotiť web komplexne – podľa domény, reputácie, obsahu a správania stránky. Dôležitým indikátorom je napríklad vek domény alebo jej história. Nové domény sú častejšie využívané pri podvodných aktivitách.

Na overenie webových stránok možno použiť nástroje ako URLScan.io alebo VirusTotal, ktoré umožňujú analyzovať stránku bez jej priameho otvorenia.

9.4.2 Bezpečné používanie webových stránok

Bezpečné používanie webu si vyžaduje kritické myslenie a obozretnosť. Používateľ by mal kontrolovať adresu stránky, vyhýbať sa podozrivým odkazom a nevkladať citlivé údaje na nedôveryhodné stránky. Pri práci na verejných sieťach je vhodné používať dodatočné zabezpečenie, napríklad VPN.

9.4.3 Falošné webové stránky

Falošné webové stránky predstavujú jednu z najčastejších foriem útoku. Útočníci sa snažia napodobniť legitímne služby a prinútiť používateľa zadať prihlasovacie údaje alebo iné citlivé informácie.

Tieto stránky často využívajú podobné názvy domén, vizuálne identické rozhranie a psychologický tlak. Používateľ by mal byť schopný identifikovať nezrovnalosti a v prípade pochybností stránku opustiť.

9.5 Práca s e-mailami

E-mail zostáva jedným z najvýznamnejších komunikačných kanálov, no zároveň je hlavným cieľom útočníkov. Prostredníctvom e-mailu sa šíria phishingové kampane, škodlivé prílohy aj odkazy na podvodné stránky.

Rozpoznanie podvodného e-mailu si vyžaduje pozornosť k detailom, ako sú adresa odosielateľa, jazyk správy, obsah odkazu alebo charakter prílohy. Používateľ by mal byť obzvlášť opatrný pri správach, ktoré vyvolávajú naliehavosť alebo vyžadujú okamžitú reakciu.

9.5.1 E-mailové filtre a ochrana pred spamom

Moderné e-mailové systémy využívajú pokročilé filtre, ktoré analyzujú obsah správ, reputáciu odosielateľov a technické parametre komunikácie. Tieto filtre dokážu identifikovať väčšinu nevyžiadaných alebo škodlivých správ, no nie sú neomylné.

Používateľ by mal preto kombinovať automatickú ochranu s vlastným posúdením rizika. V prípade pochybností je vždy bezpečnejšie správu ignorovať alebo overiť jej pravosť.

9.6 Moderné prístupy a technológie vzdialeného prístupu

9.6.1 Zero Trust model

Tradičný bezpečnostný model bol dlhodobo založený na princípe dôvery voči internému prostrediu. Ak sa používateľ nachádzal „vo vnútri siete“, bol považovaný za dôveryhodného. Tento prístup však v podmienkach vzdialenej práce a cloudových služieb prestáva byť účinný. Útočníci dnes často získajú prístup do siete prostredníctvom kompromitovaných účtov alebo zariadení, pričom následne sa pohybujú v systéme bez väčších obmedzení.

Z tohto dôvodu vznikol moderný bezpečnostný koncept známy ako Zero Trust (nulová dôvera). Jeho základná myšlienka spočíva v tom, že žiadny používateľ ani zariadenie nie sú automaticky považované za dôveryhodné – bez ohľadu na to, či sa nachádzajú v internej alebo externej sieti.

Zero Trust model je založený na niekoľkých kľúčových princípoch. Každý prístup musí byť explicitne overený, pričom sa zohľadňuje identita používateľa, stav zariadenia, lokalita, čas a správanie. Prístup k zdrojom je poskytovaný len v minimálnom rozsahu a len na nevyhnutný čas. Dôležitou súčasťou je aj neustále monitorovanie a vyhodnocovanie rizika počas celej relácie.

V praxi to znamená, že aj po úspešnom prihlásení môže systém dodatočne vyžadovať overenie alebo obmedziť prístup, ak zistí podozrivú aktivitu. Tento model výrazne znižuje riziko laterálneho pohybu útočníka v sieti a zvyšuje celkovú odolnosť infraštruktúry.

9.6.2 RDP (Remote Desktop Protocol)

Jednou z najčastejšie používaných technológií vzdialeného prístupu je RDP (Remote Desktop Protocol). Tento protokol umožňuje používateľovi ovládať vzdialený počítač tak, akoby sedel priamo pri ňom. RDP sa využíva najmä v prostredí operačných systémov Windows na správu serverov alebo prístup k pracovným staniciam.

Z bezpečnostného hľadiska však RDP predstavuje významné riziko, ak nie je správne zabezpečený. Otvorené RDP služby sú častým cieľom útokov typu brute force, pri ktorých útočníci skúšajú rôzne kombinácie prihlasovacích údajov. Po úspešnom prihlásení môžu získať plnú kontrolu nad systémom.

Bezpečné používanie RDP vyžaduje:

- použitie silnej autentizácie a MFA,

- obmedzenie prístupu (napr. cez VPN),
- zmenu predvolených portov,
- monitorovanie prístupov a pokusov o prihlásenie.

9.6.3 SSH (Secure Shell)

SSH (Secure Shell) je protokol určený na bezpečný vzdialený prístup k systémom, najmä v prostredí Linux a Unix. Na rozdiel od RDP poskytuje prístup prostredníctvom príkazového riadku, čo je vhodné najmä pre administrátorov.

SSH využíva silné šifrovanie a autentizáciu pomocou kľúčov, čo ho robí výrazne bezpečnejším než tradičné prihlasovanie heslom. Pri správnej konfigurácii je SSH jedným z najbezpečnejších spôsobov vzdialeného prístupu.

Riziká vznikajú najmä v prípade:

- používania slabých hesiel,
- povoleného prihlásenia ako root,
- nesprávnej konfigurácie firewallu.

Odporúčanou praxou je používanie autentizácie pomocou verejného a súkromného kľúča a obmedzenie prístupu len na dôveryhodné IP adresy.

9.6.4 VDI (Virtual Desktop Infrastructure)

VDI (Virtual Desktop Infrastructure) predstavuje moderný prístup k práci na diaľku, pri ktorom používateľ nepristupuje priamo k fyzickému zariadeniu, ale k virtuálnemu desktopu, ktorý beží v dátovom centre alebo cloude.

Používateľ pracuje s virtuálnym prostredím, pričom všetky dáta a aplikácie zostávajú na serveri. Na lokálne zariadenie sa prenáša len obraz a vstupy (klávesnica, myš).

Výhody VDI:

- vyššia bezpečnosť dát (dáta neopúšťajú server),
- centralizovaná správa,
- jednoduchšia kontrola prístupov,
- zníženie rizika úniku dát.

VDI je často využívané v prostrediach s vysokými bezpečnostnými požiadavkami, ako sú banky, zdravotníctvo alebo verejná správa.

9.6.5 SASE (Secure Access Service Edge)

SASE (Secure Access Service Edge) predstavuje moderný architektonický model, ktorý kombinuje sieťové a bezpečnostné služby do jednotnej cloudovej platformy. Ide o reakciu na potrebu zabezpečiť prístup k aplikáciám bez ohľadu na to, kde sa používateľ nachádza.

SASE integruje funkcie ako:

- VPN,
- firewall ako služba (FWaaS),
- bezpečnostné brány (Secure Web Gateway),
- kontrolu prístupu (ZTNA – Zero Trust Network Access).

Cieľom SASE je poskytnúť bezpečný a konzistentný prístup k aplikáciám a dátam bez ohľadu na lokalitu používateľa. Namiesto toho, aby sa používateľ pripájal do internej siete, pripája sa priamo k aplikácii cez bezpečnostne kontrolovaný cloudový bod.

Tento model je úzko prepojený s princípmi Zero Trust a predstavuje budúcnosť bezpečného vzdialeného prístupu.

9.7 Test

1. Čo je hlavnou zmenou bezpečnostného modelu pri práci na diaľku?
a) Zvýšenie výkonu serverov
b) Rozpad perimetra siete a presun mimo kontrolovaného prostredia
c) Zníženie potreby autentizácie
d) Používanie iba lokálnych zariadení

2. Čo znamená viacfaktorové overovanie (MFA)?
a) Používanie viacerých hesiel naraz
b) Overenie identity pomocou jedného silného hesla
c) Kombináciu viacerých nezávislých faktorov (napr. heslo, zariadenie, biometria)
d) Overenie identity iba pomocou biometrie

3. Aký je cieľ princípu „least privilege“?
a) Poskytnúť používateľovi maximálne oprávnenia
b) Zjednodušiť prístup do všetkých systémov
c) Obmedziť používateľa len na nevyhnutné prístupy
d) Zrušiť autentizáciu používateľa

4. Prečo samotné HTTPS nestačí na zabezpečenie webovej stránky?
a) Pretože nešifruje komunikáciu
b) Pretože HTTPS funguje len na interných sieťach
c) Pretože aj phishingové stránky môžu mať platný certifikát
d) Pretože HTTPS neumožňuje prihlásenie

5. Aká je základná myšlienka modelu Zero Trust?
a) Dôvera vo všetkých používateľov v internej sieti
b) Automatické povolenie prístupu po prihlásení
c) Nikto nie je automaticky dôveryhodný, každý prístup musí byť overený
d) Zrušenie autentizácie v interných systémoch

10Obsah pojmu digitálne súkromie

10.1 Digitálne súkromie

Pojem **digitálne súkromie** označuje právo jednotlivca rozhodovať o tom, aké informácie o jeho osobe sú v digitálnom prostredí zhromažďované, ukladané, spracúvané, zdieľané a ďalej využívané. V podmienkach súčasnej informačnej spoločnosti ide o jednu zo základných podmienok ochrany ľudskej dôstojnosti, osobnej slobody a informačnej sebaurčenosti. Digitálne súkromie je úzko prepojené s ochranou osobných údajov, bezpečnosťou informačných systémov, právom na súkromie a s ochranou pred neoprávneným sledovaním. Význam digitálneho súkromia neustále rastie, pretože veľká časť komunikácie, práce, vzdelávania, nakupovania aj spoločenského života sa presúva do online prostredia. Jednotlivec pri každodennom používaní digitálnych technológií zanecháva množstvo údajov, ktoré môžu byť analyzované, spájané a vyhodnocované. Tieto údaje môžu byť využité na personalizáciu služieb, marketing, profilovanie používateľov, ale aj na manipuláciu, diskrimináciu, podvod alebo krádež identity.

Digitálne súkromie preto nemožno chápať len ako „utajenie informácií“, ale skôr ako **možnosť mať kontrolu nad vlastnými dátami a nad tým, kto, kedy, akým spôsobom a na aký účel ich používa**. Ak používateľ túto kontrolu stráca, stráca zároveň aj schopnosť účinne chrániť svoju digitálnu identitu a rozhodovať o svojej prítomnosti v online priestore.

Digitálne súkromie zahŕňa viacero kategórií údajov. Prvou skupinou sú **osobné údaje**, teda informácie, ktoré umožňujú priamo alebo nepriamo identifikovať konkrétnu osobu. Patria sem meno, adresa, telefónne číslo, e-mailová adresa, dátum narodenia, rodné číslo, číslo občianskeho preukazu, bankové údaje či iné identifikátory. Niektoré z týchto údajov majú osobitne citlivý charakter, pretože ich zneužitie môže viesť k finančným stratám, vydieraniu alebo k závažnému zásahu do súkromia.

Druhou oblasťou sú **digitálne stopy**, ktoré človek zanecháva pri používaní internetu a digitálnych služieb. Ide napríklad o históriu prehliadania, vyhľadávacie dotazy, kliknutia na odkazy, geolokačné údaje, metadáta z fotografií alebo aktivitu na sociálnych sieťach. Tieto údaje síce na prvý pohľad nemusia pôsobiť citlivo, no pri dlhodobom zhromažďovaní a analytickom spracovaní dokážu poskytnúť veľmi presný obraz o živote, návykoch a záujmoch používateľa.

Tretia skupina zahŕňa **správanie a preferencie používateľa**. Prevádzkovatelia digitálnych služieb analyzujú spôsob používania aplikácií, nákupné správanie, reakcie na reklamu, preferovaný obsah, dĺžku návštevy stránok alebo čas, v ktorom je používateľ online. Na základe týchto údajov dochádza k algoritmickému profilovaniu, ktoré sa používa napríklad pri cielenej reklame, odporúčacích systémoch alebo pri automatizovanom rozhodovaní.

Významnú kategóriu tvoria aj **technické údaje**, ako sú IP adresa, typ zariadenia, operačný systém, verzia prehliadača, cookies, identifikátory zariadenia alebo sledovacie skripty. Hoci sa tieto údaje môžu javiť ako čisto technické, v kombinácii s ďalšími informáciami môžu umožniť identifikáciu osoby alebo jej zariadenia a slúžiť na sledovanie jej správania v online prostredí.

Ochrana digitálneho súkromia si vyžaduje nielen technické nástroje, ale aj uvedomelé správanie používateľa. Dôležitým krokom je používanie silných a jedinečných hesiel, ideálne v kombinácii s dvojfaktorovým overením. Rovnako podstatné je obmedzovanie zdieľania osobných údajov, pravidelná kontrola oprávnení aplikácií a rozšírení, používanie prehliadačov orientovaných na súkromie a blokovanie sledovacích prvkov. Používateľ by mal pravidelne preverovať nastavenia súkromia na sociálnych sieťach a pri citlivej komunikácii využívať šifrované komunikačné kanály.

V súčasnosti existuje viacero nástrojov, ktoré môžu ochranu súkromia podporiť. Patria sem správcovia hesiel, služby VPN, anti-tracking nástroje, bezpečné prehliadače či aplikácie na ochranu zariadení. Ich význam spočíva v tom, že pomáhajú používateľovi udržať kontrolu nad jeho digitálnou stopou a znižujú riziko neoprávneného sledovania alebo zneužitia údajov. Samotné technické nástroje však nie sú postačujúce, ak používateľ nerozumie základným princípom ochrany súkromia a nekoná obozretne.

S pojmom digitálne súkromie úzko súvisí **digitálna identita**, teda súbor údajov a charakteristík, na základe ktorých je človek rozpoznateľný v online priestore. Digitálne súkromie a digitálna identita spolu tvoria základ bezpečného fungovania jednotlivca v digitálnom svete. Kým digitálna identita opisuje, kto je človek v online prostredí, digitálne súkromie určuje, do akej miery má kontrolu nad tým, ako je táto identita vytváraná, zobrazovaná a využívaná.

10.2 Čo je to digitálna identita

Digitálna identita predstavuje súbor údajov, atribútov, záznamov a digitálnych prejavov, ktoré sú spojené s konkrétnou osobou v online prostredí. Ide o digitálny obraz jednotlivca, ktorý vzniká na základe informácií, ktoré o sebe vedome poskytuje, ale aj na základe údajov, ktoré o ňom zhromažďujú rôzne služby, platformy a technológie.

Digitálna identita zahŕňa klasické identifikačné údaje, ako sú meno, adresa, dátum narodenia, telefónne číslo alebo e-mailová adresa. Okrem toho však zahŕňa aj prihlasovacie údaje, finančné informácie, nákupnú históriu, sociálne interakcie, históriu prehliadania, pracovné profily, obsah publikovaný na sociálnych sieťach a multimediálne záznamy, napríklad fotografie a videá.

V širšom zmysle digitálna identita nepredstavuje len súhrn údajov, ale aj spôsob, akým je jednotlivec vnímaný a hodnotený digitálnymi systémami. Algoritmy sociálnych sietí, reklamných systémov, e-shopov či vyhľadávačov vytvárajú o používateľovi profil, ktorý môže ovplyvniť, aký obsah sa mu zobrazí, aké reklamy dostane alebo ako bude posudzovaný pri určitých rozhodovacích procesoch.

Digitálna identita môže byť vytváraná vedome, napríklad pri registrácii na webovej stránke, publikovaní príspevkov alebo dopĺňaní profilových údajov. Zároveň však vzniká aj pasívne, bez priameho zásahu používateľa, napríklad zhromažďovaním technických údajov, cookies, metadát alebo údajov o správaní. Z tohto dôvodu má používateľ len obmedzenú možnosť úplne kontrolovať, aká digitálna identita o ňom vzniká.

Ochrana digitálnej identity je preto kľúčová. Ak útočník získa prístup k dôležitým prvkom digitálnej identity, môže ich využiť na prevzatie účtov, podvodné konanie, finančné zneužitie, poškodenie reputácie alebo vydieranie. Digitálna identita sa tak stáva nielen technickým, ale aj právnym, sociálnym a bezpečnostným problémom.

10.3 Digitálna stopa na internete

S digitálnou identitou úzko súvisí pojem **digitálna stopa**, ktorý označuje všetky údaje a záznamy, ktoré človek zanecháva pri používaní internetu a digitálnych technológií. Digitálna stopa vzniká pri návšteve webových stránok, používaní sociálnych sietí, komunikácii cez e-mail alebo chat, pri online nákupoch, používaní mobilných aplikácií aj pri pohybe v priestore so zapnutou lokalizáciou.

Rozlišujeme **aktívnu digitálnu stopu**, teda údaje, ktoré používateľ zverejňuje vedome, napríklad príspevky, komentáre, fotografie, e-maily alebo profilové informácie, a **pasívnu digitálnu stopu**, ktorá vzniká bez jeho priameho vedomia. Do pasívnej digitálnej stopy patria napríklad IP adresy, cookies, údaje o polohe, čas pripojenia, technické informácie o zariadení alebo história prehliadania.

Digitálnu stopu možno ďalej rozdeliť na vlastnú stopu, ktorú zanecháva samotný používateľ, stopu vytvorenú inými osobami, ktoré o ňom zverejňujú informácie, a negatívnu digitálnu stopu, teda nepravdivé, škodlivé alebo kompromitujúce informácie. Práve negatívna digitálna stopa môže mať výrazné dôsledky na osobný a profesijný život človeka.

Je dôležité zdôrazniť, že digitálna stopa môže byť dlhodobá a v mnohých prípadoch ťažko odstrániteľná. Informácie, ktoré sa raz objavia na internete, môžu byť kopírované, archivované alebo zdieľané ďalšími subjektmi. Preto platí, že ochrana digitálnej stopy nie je len otázkou technických nástrojov, ale aj zodpovedného správania pri zverejňovaní informácií.

V odbornom kontexte sa často hovorí, že úplná anonymita na internete je v bežných podmienkach prakticky nedosiahnuteľná. Aj pri použití nástrojov na ochranu súkromia totiž používateľ zanecháva určité technické alebo behaviorálne znaky, ktoré možno analyzovať. Z tohto dôvodu je vhodnejšie hovoriť nie o absolútnej anonymite, ale o **minimalizácii digitálnej stopy a znižovaní identifikovateľnosti**.

10.4 Ako chrániť digitálnu identitu

Ochrana digitálnej identity predstavuje súbor technických, organizačných a behaviorálnych opatrení, ktorých cieľom je zabrániť zneužitiu osobných údajov, prihlasovacích údajov a online profilov používateľa. Vzhľadom na to, že digitálna identita zahŕňa množstvo rôznorodých informácií, jej ochrana musí byť systematická a dlhodobá.

Základným opatrením je používanie silných a jedinečných hesiel. Každý účet by mal mať vlastné heslo, aby kompromitácia jednej služby neviedla k ohrozeniu ďalších účtov. Vhodným riešením je využívanie správcu hesiel, ktorý umožňuje bezpečné uchovávanie a generovanie hesiel.

Významným bezpečnostným prvkom je dvojfaktorová autentizácia. Táto metóda zvyšuje bezpečnosť tým, že na prístup k účtu nestačí len znalosť hesla, ale je potrebný aj ďalší overovací prvok. Tým sa podstatne znižuje pravdepodobnosť neoprávneného prístupu.

Dôležitá je aj pravidelná aktualizácia operačného systému, aplikácií a bezpečnostného softvéru. Mnohé útoky sú úspešné práve preto, že používateľ pracuje so zastaraným softvérom obsahujúcim známe zraniteľnosti.

Pri ochrane digitálnej identity zohráva zásadnú úlohu aj obozretnosť voči phishingu. Útočníci sa často snažia získať citlivé údaje prostredníctvom falošných e-mailov, správ alebo webových stránok. Používateľ by mal byť opatrný pri otváraní neznámych príloh, pri klikaní na odkazy a pri zadávaní prihlasovacích údajov.

Významnou oblasťou je aj ochrana súkromia na sociálnych sieťach. Používateľ by mal pravidelne kontrolovať, aké informácie o sebe zverejňuje, kto má k nim prístup a do akej miery môžu byť tieto informácie zneužité. Často práve verejne zdieľané údaje slúžia útočníkom ako zdroj informácií pre sociálne inžinierstvo alebo obnovu hesla.

Chrániť digitálnu identitu je dôležité nielen z dôvodu ochrany majetku, ale aj z dôvodu ochrany osobnej povesti, profesijného postavenia a psychickej bezpečnosti jednotlivca.

10.5 Krádež digitálnej identity

Krádež digitálnej identity je proces, pri ktorom útočník získa citlivé informácie o osobe a následne ich použije na neoprávnený prístup k účtom, finančným prostriedkom alebo službám, prípadne na vydávanie sa za obeť. Ide o jednu z najvýznamnejších foriem kybernetickej kriminality, pretože môže mať závažné finančné, právne aj osobné dôsledky.

Jednou z najbežnejších metód je phishing. Útočník zašle obeti správu, ktorá vyzerá ako komunikácia od banky, sociálnej siete alebo inej dôveryhodnej inštitúcie. Správa obsahuje odkaz na falošnú stránku, kde obeť zadá svoje prihlasovacie údaje. Tie sú následne zneužité.

Ďalšou častou metódou je použitie malvéru, napríklad keyloggera alebo spyware. Takýto škodlivý softvér môže zaznamenávať stlačenia kláves, prihlasovacie údaje, obsah obrazovky alebo ďalšie citlivé informácie. Útočník tak získa prístup k účtom bez toho, aby si to obeť všimla.

Rizikovou metódou je aj vishing, teda telefonický podvod, pri ktorom sa útočník vydáva za zamestnanca banky, úradu alebo technickej podpory a presvedčí obeť, aby mu poskytla citlivé údaje. Veľmi účinné býva aj sociálne inžinierstvo, pri ktorom útočník využíva informácie z verejných profilov a vytvára dôveryhodný príbeh.

Krádež identity môže prebiehať aj využitím verejne dostupných informácií. Ak používateľ zverejní svoje meno, dátum narodenia, adresu, kontakty alebo odpovede na bezpečnostné otázky, môže tým nevedomky vytvoriť podmienky na zneužitie svojich účtov.

Príkladom z praxe je situácia, keď útočník využije verejne dostupné informácie zo sociálnych sietí na obnovenie hesla do e-mailového účtu. Po prevzatí e-mailu môže následne resetovať heslá do ďalších služieb, čím postupne preberie kontrolu nad celou digitálnou identitou obete. Ochrana pred krádežou digitálnej identity si preto vyžaduje kombináciu technických opatrení, obozretnosti a minimálneho zdieľania citlivých údajov.

10.6 Právny rámec pre ochranu osobných údajov

Ochrana digitálneho súkromia a digitálnej identity je úzko spojená s právnym rámcom ochrany osobných údajov. V prostredí Európskej únie predstavuje základný právny nástroj **Všeobecné nariadenie o ochrane osobných údajov (GDPR)**, ktoré stanovuje pravidlá spracúvania osobných údajov a posilňuje práva jednotlivcov.

GDPR poskytuje subjektom údajov viacero významných práv. Patria sem právo na prístup k osobným údajom, právo na opravu nepresných údajov, právo na výmaz, právo na obmedzenie spracúvania, právo na prenosnosť údajov a právo namietať proti určitým formám spracúvania. Tieto práva posilňujú postavenie jednotlivca vo vzťahu k organizáciám, ktoré jeho údaje spracúvajú.

Významným princípom je aj požiadavka na súhlas. Spracúvanie osobných údajov musí byť založené na právnom základe, pričom v mnohých prípadoch sa vyžaduje slobodný, konkrétny, informovaný a jednoznačný súhlas dotknutej osoby. Organizácie zároveň musia používateľa transparentne informovať o tom, aké údaje zbierajú, na aký účel a ako dlho ich budú uchovávať.

GDPR kladie dôraz aj na bezpečnosť údajov. Organizácie sú povinné zavádzať primerané technické a organizačné opatrenia, ako sú šifrovanie, pseudonymizácia, riadenie prístupov a pravidelné testovanie bezpečnosti. Tieto opatrenia majú chrániť osobné údaje pred stratou, zneužitím, neoprávneným prístupom alebo zničením.

V prípade porušenia ochrany osobných údajov existuje povinnosť oznámenia incidentu dozornému orgánu, v Slovenskej republike Úradu na ochranu osobných údajov, spravidla do 72 hodín od zistenia incidentu. Ak incident predstavuje vysoké riziko pre práva a slobody osôb, je potrebné informovať aj samotné dotknuté osoby.

Niektoré organizácie sú povinné ustanoviť poverenca na ochranu osobných údajov (DPO), ktorý dohliada na súlad spracúvania s GDPR, poskytuje poradenstvo a slúži ako kontaktná osoba medzi organizáciou, dotknutými osobami a dozorným orgánom.

GDPR teda vytvára robustný právny rámec, ktorý podporuje ochranu digitálneho súkromia a digitálnej identity. Nejde však len o právnu formalitu, ale o praktický nástroj ochrany jednotlivca v digitálnom prostredí.

10.7 Test

1. Čo vyjadruje pojem digitálne súkromie?
a) Utajenie všetkých informácií o používateľovi

b) Právo jednotlivca kontrolovať svoje údaje v digitálnom prostredí
c) Používanie anonymných účtov na internete
d) Zákaz zdieľania údajov na sociálnych sieťach

2. Ktoré z nasledujúcich údajov patria medzi digitálne stopy?
a) Rodné číslo a číslo občianskeho preukazu
b) Heslo k e-mailu
c) História prehliadania a geolokačné údaje
d) Len meno a priezvisko

3. Čo je digitálna identita?
a) Iba prihlasovacie meno a heslo
b) Súbor údajov a prejavov, ktoré reprezentujú osobu v online prostredí
c) Výlučne profil na sociálnej sieti
d) IP adresa používateľa

4. Aký je rozdiel medzi aktívnou a pasívnou digitálnou stopou?
a) Aktívna stopa vzniká bez vedomia používateľa
b) Pasívna stopa vzniká len na sociálnych sieťach
c) Aktívna stopa je vedome zverejnená, pasívna vzniká bez priameho vedomia
d) Medzi nimi nie je žiadny rozdiel

5. Ktorá z nasledujúcich možností je typickou metódou krádeže digitálnej identity?
a) Aktualizácia softvéru
b) Šifrovanie komunikácie
c) Phishing
d) Používanie VPN

11 Význam pojmov: digitálny podpis, elektronický podpis, kvalifikovaný elektronický podpis a časová pečiatka

Porozumenie pojmom ako **digitálny opis (metadáta)**, **elektronický podpis**, **kvalifikovaný elektronický podpis** a **časová pečiatka** je dôležité najmä v kontexte digitálnej bezpečnosti, právnej istoty a efektívnej elektronickej komunikácie. V súčasnom digitálnom prostredí sa čoraz viac právnych, obchodných aj administratívnych úkonov vykonáva elektronicky. Aby bolo možné takýmto úkonom dôverovať, je potrebné zabezpečiť, aby bolo zrejmé, kto dokument vytvoril alebo podpísal, či bol dokument po podpísaní zmenený a kedy presne vznikol alebo bol autorizovaný.

Tieto pojmy sa uplatňujú najmä pri práci s elektronickými dokumentmi, zmluvami, faktúrami, úradnými podaniami, elektronickou komunikáciou s orgánmi verejnej moci, ale aj pri archivácii a dokazovaní právnych skutočností. Ich význam teda nespočíva len v technickom spracovaní dokumentov, ale aj v ochrane dôveryhodnosti, integrity a právnej použiteľnosti elektronických záznamov.

Digitálny opis alebo metadáta pomáhajú dokument identifikovať, triediť, spravovať a archivovať. Elektronický podpis umožňuje potvrdiť identitu podpisujúcej osoby a zabezpečiť integritu dokumentu. Kvalifikovaný elektronický podpis predstavuje najvyššiu úroveň dôveryhodnosti elektronického podpisu a má právne účinky porovnateľné s vlastnoručným podpisom. Časová pečiatka dopĺňa tieto mechanizmy tým, že poskytuje dôkaz o existencii dokumentu v konkrétnom okamihu.

Význam týchto nástrojov sa prejavuje vo viacerých oblastiach. Pri práci s dokumentmi umožňujú bezpečné podpisovanie zmlúv, potvrdenie prevzatia dokumentu alebo jeho dlhodobú archiváciu. Pri komunikácii s úradmi sú základom elektronických podaní a úradne uznávaných úkonov. Z hľadiska právnej istoty slúžia ako dôkazné prostriedky v prípade sporov. V oblasti kybernetickej bezpečnosti chránia dokumenty pred neoprávnenou manipuláciou, podvrhnutím alebo popretím autorstva.

11.1 Digitálny opis (metadáta)

Digitálny opis, často označovaný aj ako **metadáta**, predstavuje súbor informácií o digitálnom dokumente alebo súbore, ktoré nepredstavujú jeho vlastný obsah, ale ho opisujú. Metadáta majú veľký význam pri identifikácii, správe, triedení, vyhľadávaní a archivácii elektronických dokumentov. Bez nich by bola práca s veľkým množstvom súborov neprehľadná a menej efektívna.

Medzi typické metadáta patrí názov dokumentu, meno autora, dátum vytvorenia, dátum poslednej úpravy, formát súboru, veľkosť, jazyk dokumentu alebo kľúčové slová. V závislosti od typu súboru môžu metadáta obsahovať aj ďalšie údaje, napríklad pri fotografiách informácie o zariadení, ktorým boli zhotovené, alebo pri dokumentoch údaje o verzii softvéru, v ktorom boli vytvorené.

Z praktického hľadiska majú metadáta viacero funkcií. Umožňujú používateľovi rýchlo vyhľadať požadovaný dokument, triediť súbory podľa času, autora alebo typu a uľahčujú ich evidenciu v informačných systémoch. V archívnom a úradnom prostredí sú dôležité aj z hľadiska dlhodobého uchovávania dokumentov, pretože pomáhajú zachovať informácie o pôvode a histórii dokumentu.

Metadáta však môžu predstavovať aj bezpečnostné a súkromné riziko. Používateľ si často neuvedomuje, že dokument alebo fotografia môžu obsahovať skryté informácie, ako sú meno autora, názov organizácie, interné poznámky alebo geolokačné údaje. Pri zdieľaní súborov je preto vhodné zvážiť, či neobsahujú metadáta, ktoré by mohli prezradiť viac, než je žiaduce.

11.2 Elektronický podpis

Elektronický podpis je údaj v elektronickej podobe, ktorý je pripojený k iným elektronickým údajom alebo je s nimi logicky spojený a ktorý podpisujúca osoba používa na podpisovanie. Jeho hlavnou funkciou je potvrdiť vôľu osoby viazať sa obsahom dokumentu a zároveň umožniť určitú mieru identifikácie podpisujúceho.

Je dôležité zdôrazniť, že pojem elektronický podpis je širší než pojem digitálny podpis. Elektronickým podpisom môže byť viacero foriem potvrdenia súhlasu alebo autorizácie v digitálnom prostredí. V najjednoduchšej podobe môže ísť napríklad o naskenovaný vlastnoručný podpis vložený do dokumentu, kliknutie na tlačidlo „Súhlasím“, uvedenie mena na konci e-mailu alebo potvrdenie akcie prostredníctvom autentifikovaného používateľského účtu.

Takéto jednoduché formy elektronického podpisu však neposkytujú rovnakú úroveň bezpečnosti a právnej istoty. Preto sa v praxi rozlišujú viaceré úrovne elektronického podpisu. Vyššiu úroveň predstavuje **pokročilý elektronický podpis**, ktorý je jednoznačne spojený s podpisujúcou osobou, umožňuje jej identifikáciu a je vytvorený spôsobom, ktorý zabezpečuje, že každá následná zmena dokumentu je rozpoznateľná.
Z technického hľadiska sa elektronické podpisovanie často opiera o kryptografické mechanizmy. Podpisujúca osoba vytvorí podpis pomocou súkromného kľúča a príjemca alebo overovateľ môže jeho pravosť overiť pomocou zodpovedajúceho verejného kľúča. Takto sa dosahuje nielen potvrdenie identity, ale aj ochrana integrity dokumentu.

Elektronický podpis má význam najmä v digitálnej komunikácii, pri uzatváraní zmlúv, schvaľovaní dokumentov a elektronickom vybavovaní administratívnych úkonov. Jeho použitie urýchľuje procesy, znižuje potrebu fyzickej prítomnosti a podporuje elektronizáciu služieb. Zároveň však platí, že právna sila elektronického podpisu závisí od jeho typu, od spôsobu jeho vytvorenia a od konkrétneho právneho kontextu.

11.3 Kvalifikovaný elektronický podpis (QES)

Kvalifikovaný elektronický podpis predstavuje najvyššiu úroveň elektronického podpisu podľa európskej legislatívy, najmä nariadenia **eIDAS**. Ide o osobitný typ elektronického podpisu,

ktorý spĺňa prísne technické a právne požiadavky a je uznávaný ako ekvivalent vlastnoručného podpisu.

Aby bolo možné hovoriť o kvalifikovanom elektronickom podpise, musia byť splnené viaceré podmienky. Podpis musí byť vytvorený pomocou **kvalifikovaného certifikátu**, ktorý vydáva dôveryhodný poskytovateľ dôveryhodných služieb. Zároveň musí byť vytvorený pomocou **kvalifikovaného zariadenia na vytváranie podpisu**, napríklad čipovej karty, bezpečnostného tokenu alebo certifikovanej aplikácie. Takýto podpis je úzko viazaný na konkrétnu podpisujúcu osobu a umožňuje jednoznačne zistiť, či dokument po podpísaní nebol zmenený.

Najväčší význam kvalifikovaného elektronického podpisu spočíva v jeho právnej sile. V právnom prostredí členských štátov Európskej únie má rovnaký právny účinok ako vlastnoručný podpis, pokiaľ právny predpis neustanovuje inak. To znamená, že dokument podpísaný kvalifikovaným elektronickým podpisom môže byť použitý pri právnych úkonoch, v úradnom styku, v obchodných vzťahoch a v mnohých prípadoch aj v súdnom konaní.

Používanie QES je výhodné najmä pri elektronickom podpisovaní zmlúv, úradných podaní, komunikácii so štátnou správou, pri interných procesoch organizácií a tam, kde je potrebná vysoká miera dôveryhodnosti a preukázateľnosti. Výhodou je aj možnosť rýchlej elektronickej komunikácie bez potreby osobnej návštevy úradu alebo fyzického podpisu papierového dokumentu.

Na druhej strane má kvalifikovaný elektronický podpis aj určité obmedzenia. Jeho používanie si vyžaduje technické vybavenie, správu certifikátu a určitú mieru digitálnej gramotnosti. Získanie kvalifikovaného certifikátu môže byť spoplatnené a v niektorých prípadoch je potrebné osobné overenie totožnosti. Z tohto dôvodu nie je QES vždy vhodný na jednoduché a neformálne úkony, kde postačuje nižšia úroveň elektronickej autorizácie.

Z pohľadu výhod možno zdôrazniť najmä vysokú právnu istotu, dôveryhodnosť, silnú ochranu integrity dokumentu a široké uznávanie v rámci Európskej únie. Nevýhodou sú najmä vyššie technické a administratívne nároky, potreba kvalifikovaného certifikátu a v niektorých prípadoch aj dodatočné finančné náklady.

11.4 Časová pečiatka

Časová pečiatka je dôveryhodný elektronický dôkaz o tom, že konkrétny dokument alebo digitálny údaj existoval v určitom čase. Jej význam spočíva v tom, že umožňuje preukázať okamih existencie dokumentu a zároveň podporuje dôkaz o jeho integrite. Časová pečiatka sa využíva najmä tam, kde je potrebné spoľahlivo doložiť, že dokument bol vytvorený, podpísaný alebo predložený v konkrétnom časovom okamihu.

Z technického hľadiska časová pečiatka obsahuje dátum a čas, odtlačok dokumentu vo forme kryptografického hashu a elektronický podpis autority, ktorá časovú pečiatku vydala. Túto úlohu vykonáva dôveryhodná časová autorita, označovaná ako TSA (Time Stamping Authority). Keďže časová pečiatka neobsahuje celý dokument, ale len jeho kryptografický odtlačok, je možné neskôr overiť, či dokument zodpovedá stavu, ktorý existoval v čase pečiatkovania.

Časová pečiatka má významný dôkazný efekt. Ak je dokument opatriť časovou pečiatkou, možno preukázať, že v určitom čase už existoval v konkrétnej podobe. To je dôležité napríklad pri zmluvách, podaniach, archivácii, autorskoprávnej ochrane, dokazovaní splnenia lehôt alebo v sporových situáciách. Časová pečiatka zároveň zvyšuje dôveryhodnosť elektronických dokumentov, pretože komplikuje možnosť spätného falšovania času alebo obsahu.

V kombinácii s elektronickým alebo kvalifikovaným elektronickým podpisom vytvára časová pečiatka silný nástroj na zabezpečenie autenticity, integrity a preukázateľnosti elektronických dokumentov. Kým podpis potvrdzuje, kto dokument podpísal, časová pečiatka potvrdzuje, kedy dokument existoval v danej podobe.

11.5 Mandátny certifikát

Mandátny certifikát je špecifický typ kvalifikovaného certifikátu, ktorý sa používa v situáciách, keď fyzická osoba koná **v mene právnickej osoby alebo organizácie**. Na rozdiel od bežného kvalifikovaného certifikátu, ktorý identifikuje konkrétnu fyzickú osobu, mandátny certifikát obsahuje aj informáciu o tom, **v akej funkcii alebo na základe akého oprávnenia osoba koná**.

To znamená, že podpis vytvorený pomocou mandátneho certifikátu nevyjadruje len osobnú vôľu podpisujúceho, ale zároveň potvrdzuje, že daná osoba koná napríklad ako štatutár, zamestnanec, splnomocnený zástupca alebo iná oprávnená osoba organizácie.

Mandátny certifikát je dôležitý najmä v praxi verejnej správy, podnikovej sféry a právnych úkonov, kde je potrebné preukázať nielen identitu osoby, ale aj jej oprávnenie konať v mene iného subjektu. Využíva sa napríklad pri elektronických podaniach za firmu, podpisovaní zmlúv v mene organizácie alebo komunikácii so štátnymi inštitúciami.

Z hľadiska právnej istoty mandátny certifikát zvyšuje dôveryhodnosť elektronických úkonov, pretože umožňuje jednoznačne preukázať, že podpis bol vykonaný oprávnenou osobou v rámci jej kompetencií.

11.6 Elektronická pečať

Elektronická pečať je nástroj podobný elektronickému podpisu, avšak na rozdiel od podpisu nie je viazaná na fyzickú osobu, ale na **právnickú osobu** (napr. firmu, úrad alebo organizáciu). Slúži na potvrdenie, že dokument pochádza od konkrétnej organizácie a že jeho obsah nebol po vytvorení zmenený.

Elektronická pečať teda nevyjadruje osobnú vôľu konkrétneho človeka, ale **autenticitu a integritu dokumentu ako výstupu organizácie**. Jej použitie je vhodné najmä v prípadoch, keď dokument generuje informačný systém automaticky alebo keď nie je potrebné, aby dokument podpisovala konkrétna osoba.

Podobne ako pri elektronickom podpise existuje aj **kvalifikovaná elektronická pečať**, ktorá je založená na kvalifikovanom certifikáte a poskytuje vyššiu úroveň dôveryhodnosti. Takáto pečať je uznávaná v rámci Európskej únie podľa nariadenia eIDAS.

Elektronická pečať sa využíva napríklad pri:

- vydávaní výpisov z registrov,
- generovaní faktúr a potvrdení,
- automatizovanej komunikácii úradov,
- archivácii dokumentov.

Jej hlavnou výhodou je možnosť automatizácie a zníženie potreby manuálneho podpisovania dokumentov, pričom sa zachováva vysoká úroveň dôveryhodnosti.

11.7 Autorizačná doložka

Autorizačná doložka je špecifický prvok používaný pri elektronických dokumentoch, najmä v prostredí verejnej správy. Ide o informáciu, ktorá je pripojená k dokumentu a obsahuje údaje o tom, **kto dokument autorizoval (podpísal), akým spôsobom a kedy**.

Autorizačná doložka spravidla obsahuje:

- identifikáciu podpisujúcej osoby,
- údaj o použitom type podpisu (napr. kvalifikovaný elektronický podpis),
- dátum a čas autorizácie,
- prípadne informácie o certifikáte alebo autorite.

Jej účelom je zvýšiť transparentnosť a preukázateľnosť elektronického úkonu. Umožňuje jednoducho overiť, že dokument bol riadne autorizovaný a že spĺňa požiadavky na právnu platnosť.

Autorizačná doložka sa často využíva pri:

- úradných rozhodnutiach,
- elektronických podaniach,
- dokumentoch vydávaných verejnou správou.

Z praktického hľadiska predstavuje „viditeľnú vrstvu“ informácií o podpise, ktorá dopĺňa technické údaje obsiahnuté v samotnom elektronickom podpise.

11.8 Zaručená konverzia

Zaručená konverzia je proces, pri ktorom dochádza k **prevedeniu dokumentu z listinnej (papierovej) formy do elektronickej formy alebo naopak**, pričom sa zachováva jeho právna hodnota. Výsledkom zaručenej konverzie je dokument, ktorý má rovnaké právne účinky ako pôvodný dokument.

Tento proces je presne regulovaný právnymi predpismi a môže ho vykonávať len oprávnený subjekt, napríklad orgán verejnej moci, notár alebo iná autorizovaná osoba. Súčasťou zaručenej konverzie je vytvorenie doložky, ktorá obsahuje informácie o priebehu konverzie, použitých technológiách a identifikácii osoby alebo systému, ktorý konverziu vykonal.

Zaručená konverzia sa využíva najmä v situáciách, keď je potrebné:

- digitalizovať papierové dokumenty pre elektronické podanie,
- vytvoriť listinný ekvivalent elektronického dokumentu,
- zabezpečiť právnu použiteľnosť dokumentu v inom prostredí.

Na rozdiel od bežného skenovania dokumentov zaručená konverzia poskytuje právnu istotu, že obsah dokumentu je verne zachovaný a že nedošlo k jeho zmene. Preto má zásadný význam pri komunikácii s úradmi, v právnej praxi a pri archivácii dokumentov.

11.9 Zhrnutie

Digitálny opis, elektronický podpis, kvalifikovaný elektronický podpis a časová pečiatka predstavujú základné nástroje dôveryhodnej práce s elektronickými dokumentmi. Každý z týchto prvkov plní osobitnú funkciu, no ich spoločným cieľom je posilniť bezpečnosť, dôveryhodnosť a právnu použiteľnosť digitálnych záznamov.

Metadáta pomáhajú dokument opísať, spravovať a archivovať. Elektronický podpis umožňuje potvrdiť vôľu podpisujúcej osoby a v pokročilých formách chráni aj integritu dokumentu. Kvalifikovaný elektronický podpis má osobitné právne postavenie a je uznávaný ako ekvivalent vlastnoručného podpisu. Časová pečiatka poskytuje dôkaz o existencii dokumentu v konkrétnom čase a dopĺňa systém elektronickej dôveryhodnosti.

V modernej digitálnej spoločnosti je porozumenie týmto pojmom nevyhnutné nielen pre právnikov, úradníkov a pracovníkov verejnej správy, ale aj pre bežných používateľov, ktorí pracujú s elektronickými dokumentmi, uzatvárajú zmluvy online alebo komunikujú s inštitúciami elektronickou formou.

Z praktického hľadiska sa tieto prvky často používajú spoločne. Elektronický dokument môže obsahovať metadáta, byť podpísaný kvalifikovaným elektronickým podpisom a zároveň opatriť časovou pečiatkou. Takýto dokument je potom nielen technicky spracovateľný, ale aj právne dôveryhodný a dlhodobo overiteľný.

V oblasti kybernetickej bezpečnosti a právnej praxe majú tieto mechanizmy veľký význam. Pomáhajú chrániť dokumenty pred manipuláciou, znižujú možnosť falšovania, umožňujú preukazovať autorstvo a podporujú dôveru v elektronickú komunikáciu. Bez nich by elektronické dokumenty nemali rovnakú dôkaznú a právnu hodnotu ako tradičné listinné dokumenty.

11.10Test

1. Čo je hlavnou funkciou metadát (digitálneho opisu) pri elektronickom dokumente?
a) Nahradiť obsah dokumentu
b) Opísať, identifikovať a uľahčiť správu dokumentu
c) Zašifrovať dokument
d) Potvrdiť právnu platnosť dokumentu podpisom

2. Ktoré tvrdenie najlepšie vystihuje elektronický podpis?
a) Je to vždy ekvivalent vlastnoručného podpisu

b) Je to údaj v elektronickej podobe používaný na podpisovanie elektronických údajov
c) Je to výlučne naskenovaný vlastnoručný podpis
d) Môže ho vytvoriť len orgán verejnej moci

3. Čím sa kvalifikovaný elektronický podpis (QES) odlišuje od bežného elektronického podpisu?
a) Nemá žiadnu právnu silu
b) Môže byť použitý len pri e-mailoch
c) Spĺňa prísne technické a právne požiadavky a je uznávaný ako ekvivalent vlastnoručného podpisu
d) Nepotrebuje certifikát ani špeciálne zariadenie

4. Aký je hlavný význam časovej pečiatky?
a) Potvrdzuje, kto dokument podpísal
b) Umožňuje dokument vytlačiť
c) Dokazuje, že dokument existoval v konkrétnom čase
d) Šifruje obsah dokumentu

5. Na čo slúži elektronická pečať?
a) Na potvrdenie identity fyzickej osoby pri podpise
b) Na potvrdenie, že dokument pochádza od konkrétnej organizácie a nebol zmenený
c) Na prevod papierového dokumentu do PDF
d) Na zobrazenie metadát dokumentu

12 Základné zásady bezpečnosti, ochrany osobných údajov a etikety pri telekonferenciách a online rokovaniach a stretnutiach

12.1 Úvod do problematiky online komunikácie

Telekonferencie a online stretnutia sa stali neoddeliteľnou súčasťou pracovného, vzdelávacieho aj spoločenského života. Moderné komunikačné platformy umožňujú rýchlu a efektívnu výmenu informácií bez ohľadu na geografickú vzdialenosť, čím zvyšujú flexibilitu organizácií a dostupnosť komunikácie. Tento spôsob komunikácie však prináša aj nové bezpečnostné a etické výzvy.

Na rozdiel od tradičných stretnutí v kontrolovanom fyzickom prostredí prebiehajú online rokovania prostredníctvom digitálnych systémov, ktoré sú vystavené rôznym typom kybernetických hrozieb. Okrem technických rizík je potrebné zohľadniť aj ochranu osobných údajov a dodržiavanie pravidiel profesionálnej komunikácie, ktoré ovplyvňujú priebeh a výsledok stretnutia.

Bezpečné a efektívne využívanie telekonferenčných nástrojov si preto vyžaduje kombináciu technických opatrení, správnych používateľských návykov a dodržiavania etických zásad komunikácie.

12.2 Bezpečnostné zásady pri telekonferenciách

Z pohľadu kybernetickej bezpečnosti je kľúčové zabezpečiť, aby sa k online stretnutiu dostali len oprávnené osoby a aby komunikácia nebola odpočúvaná alebo manipulovaná. Výber vhodnej platformy zohráva v tomto procese zásadnú úlohu. Organizácie by mali používať overené nástroje, ktoré poskytujú šifrovanie komunikácie, správu identít používateľov a kontrolu prístupu.

Jedným z najčastejších bezpečnostných problémov je neoprávnený prístup na stretnutie, známy napríklad ako „zoombombing“. K nemu dochádza v prípade, že sú odkazy na stretnutia zverejnené verejne alebo nie sú dostatočne chránené. Preto je nevyhnutné používať mechanizmy ako heslá, čakárne (waiting room), pozvánky pre konkrétnych používateľov alebo autentifikáciu účastníkov.

Dôležitým prvkom bezpečnosti je aj ochrana prihlasovacích údajov. Používateľ by nemal zdieľať svoje prihlasovacie údaje ani odkazy na stretnutia s neoverenými osobami. V prípade firemných účtov je vhodné využívať viacfaktorové overovanie, ktoré znižuje riziko kompromitácie účtu.

Aktualizácia softvéru predstavuje ďalší kľúčový aspekt. Telekonferenčné aplikácie sú často cieľom útokov, pretože obsahujú funkcie ako zdieľanie obrazovky, prenos súborov alebo

komunikáciu v reálnom čase. Vývojári pravidelne vydávajú aktualizácie, ktoré opravujú zraniteľnosti, a preto je dôležité ich inštalovať bez odkladu.

Pri práci na diaľku, najmä z verejných alebo nezabezpečených sietí, je vhodné používať virtuálnu privátnu sieť (VPN), ktorá zabezpečuje šifrovaný prenos dát a znižuje riziko odpočúvania komunikácie. Okrem toho je potrebné dbať na fyzickú bezpečnosť zariadenia. Používateľ by mal pri odchode od pracovného miesta uzamknúť obrazovku, aby zabránil neoprávnenému prístupu k prebiehajúcemu stretnutiu alebo zdieľanému obsahu.

12.3 Ochrana osobných údajov pri online stretnutiach

Telekonferencie často zahŕňajú spracúvanie osobných údajov, či už ide o obraz, hlas, meno účastníka alebo obsah komunikácie. Z tohto dôvodu je potrebné dodržiavať zásady ochrany osobných údajov v súlade s legislatívou, najmä nariadením GDPR.
J
edným z najdôležitejších aspektov je nahrávanie stretnutí. Ak je stretnutie zaznamenávané, účastníci musia byť o tejto skutočnosti informovaní a v mnohých prípadoch je potrebné získať ich súhlas. Nahrávky by mali byť uchovávané len po nevyhnutnú dobu a zabezpečené proti neoprávnenému prístupu.

Pri online komunikácii je tiež potrebné minimalizovať množstvo zdieľaných údajov. Používateľ by mal zvážiť, či je zdieľanie konkrétnych informácií nevyhnutné, najmä ak ide o citlivé údaje. V pracovnom prostredí je vhodné riadiť sa princípom minimalizácie údajov, teda spracúvať len tie údaje, ktoré sú nevyhnutné na daný účel.

Významnú úlohu zohráva aj prostredie, v ktorom sa používateľ nachádza. Kamera môže zachytiť osobné alebo citlivé predmety, dokumenty alebo informácie v pozadí. Preto sa odporúča používať funkcie ako rozmazanie pozadia alebo virtuálne pozadie, ktoré znižujú riziko neúmyselného úniku informácií.

Pri zdieľaní obrazovky je potrebné venovať zvýšenú pozornosť tomu, aký obsah je viditeľný. Otvorené e-maily, dokumenty alebo pracovné plochy môžu obsahovať citlivé informácie, ktoré by nemali byť zdieľané s ostatnými účastníkmi. Vhodným riešením je zdieľanie konkrétneho okna aplikácie namiesto celej obrazovky.

12.4 Etiketa (netiketa) pri online rokovaniach

Okrem technických a právnych aspektov zohráva významnú úlohu aj správanie účastníkov, ktoré ovplyvňuje kvalitu komunikácie a celkový priebeh stretnutia. Etiketa online komunikácie, označovaná aj ako netiketa, predstavuje súbor pravidiel, ktoré podporujú profesionálne a efektívne vystupovanie v digitálnom prostredí.

Dochvíľnosť je základným prejavom profesionality. Pripojenie sa na stretnutie s predstihom umožňuje vyriešiť technické problémy a zabezpečiť plynulý začiatok rokovania. Rovnako dôležitá je pripravenosť účastníka, ktorá zahŕňa znalosť programu stretnutia a pripravenosť diskutovať o príslušných témach.

Používanie kamery môže prispieť k lepšej komunikácii, pretože umožňuje vnímať neverbálne prejavy, ako sú mimika a gestá. V niektorých situáciách však môže byť jej používanie nevhodné alebo technicky obmedzené, preto je potrebné zohľadniť kontext stretnutia.

Dôležitým pravidlom je stlmenie mikrofónu v čase, keď účastník nehovorí. Tým sa predchádza rušivým zvukom, ktoré môžu znižovať kvalitu komunikácie. Pri vystupovaní je vhodné hovoriť jasne, stručne a rešpektovať ostatných účastníkov, napríklad tým, že sa neprerušujú a dávajú si navzájom priestor na vyjadrenie.

Online komunikácia by mala zachovávať profesionálny charakter aj z hľadiska vystupovania a vzhľadu. Aj keď účastník pracuje z domáceho prostredia, mal by dodržiavať primeraný dress code a správať sa tak, ako keby bol prítomný na fyzickom stretnutí.

12.5 Typické riziká a hrozby pri online stretnutiach

Online stretnutia sú vystavené viacerým typom hrozieb. Medzi najčastejšie patrí neoprávnený prístup na stretnutie, odpočúvanie komunikácie, phishingové útoky prostredníctvom falošných pozvánok alebo zneužitie zdieľaného obsahu.

Rizikom je aj ľudský faktor. Neopatrné zdieľanie obrazovky, zverejnenie citlivých údajov alebo slabé zabezpečenie účtu môžu viesť k úniku informácií. Útočníci často využívajú práve tieto slabiny, pretože sú jednoduchšie než technické útoky na samotnú platformu.

Zvláštnu pozornosť je potrebné venovať aj nahrávkam stretnutí. Ak sa dostanú do nesprávnych rúk, môžu obsahovať citlivé informácie, ktoré môžu byť zneužité.

12.6 Praktické odporúčania

Pre bezpečné a efektívne online stretnutia je vhodné dodržiavať niekoľko zásad. Organizátor by mal zabezpečiť ochranu prístupu k stretnutiu, informovať účastníkov o prípadnom nahrávaní a kontrolovať priebeh komunikácie. Účastník by mal používať zabezpečené zariadenie, aktualizovaný softvér a pristupovať k stretnutiu z dôveryhodnej siete.

Dôležité je aj uvedomenie si, že online stretnutie je súčasťou pracovného alebo oficiálneho prostredia. Správanie účastníkov by tomu malo zodpovedať, a to nielen z hľadiska profesionality, ale aj bezpečnosti a ochrany údajov.

12.7 Test

1. Čo je hlavnou výhodou telekonferencií a online stretnutí?
a) Eliminácia potreby internetu
b) Možnosť komunikácie bez ohľadu na geografickú vzdialenosť
c) Úplná bezpečnosť komunikácie
d) Nahradenie všetkých foriem komunikácie

2. Čo je „zoombombing“?
a) Technická chyba aplikácie
b) Neoprávnený prístup na online stretnutie
c) Spomalenie internetového pripojenia
d) Nahrávanie stretnutia bez zvuku

3. Ktoré opatrenie pomáha chrániť osobné údaje pri online stretnutiach?
a) Zdieľanie celej obrazovky vždy
b) Používanie verejných Wi-Fi bez ochrany
c) Používanie rozmazania alebo virtuálneho pozadia
d) Vypnutie všetkých bezpečnostných nastavení

4. Ktoré pravidlo patrí medzi zásady netikety pri online rokovaniach?
a) Neustále zapnutý mikrofón
b) Ignorovanie ostatných účastníkov
c) Stlmenie mikrofónu, keď účastník nehovorí
d) Neskoré pripojenie na stretnutie

5. Ktoré riziko patrí medzi typické hrozby pri online stretnutiach?
a) Zvýšenie kvality zvuku
b) Automatické šifrovanie všetkých dát
c) Phishing prostredníctvom falošných pozvánok
d) Zníženie počtu účastníkov

13 Bezpečnostné riziká a riziká ochrany súkromia pri používaní sociálnych sietí

13.1 Úvod do problematiky sociálnych sietí a bezpečnosti

Sociálne siete predstavujú jeden z najvýznamnejších fenoménov digitálnej spoločnosti. Platformy ako Facebook, Instagram, TikTok, LinkedIn alebo X (Twitter) umožňujú používateľom komunikovať, zdieľať obsah a vytvárať sociálne väzby v globálnom prostredí. Okrem osobnej komunikácie zohrávajú významnú úlohu aj v oblasti marketingu, politiky, vzdelávania či budovania profesijných kontaktov.

S rastúcim významom sociálnych sietí však narastá aj množstvo bezpečnostných hrozieb a rizík pre ochranu súkromia. Sociálne siete fungujú na princípe zhromažďovania a analýzy veľkého množstva údajov o používateľoch, čo z nich robí atraktívny cieľ pre útočníkov. Zároveň samotní používatelia často vedome alebo nevedome zverejňujú informácie, ktoré môžu byť zneužité.

Bezpečné používanie sociálnych sietí preto vyžaduje nielen technické zabezpečenie účtov, ale aj kritické myslenie, uvedomelé správanie a znalosť rizík.

13.2 Charakteristika komunikácie na sociálnych sieťach

Komunikácia na sociálnych sieťach sa výrazne odlišuje od tradičných foriem komunikácie, a to najmä svojou dynamikou, rozsahom a formou. Informácie sa šíria v reálnom čase a často bez akejkoľvek kontroly alebo overenia. Táto okamžitosť podporuje spontánne reakcie, ktoré však môžu viesť k neuváženému zdieľaniu citlivých informácií.

Významným znakom je verejnosť komunikácie. Aj keď používateľ nastaví určitý stupeň súkromia, obsah môže byť jednoducho skopírovaný, zdieľaný alebo uložený inými osobami. Strata kontroly nad zverejneným obsahom je preto jedným z kľúčových rizík.

Sociálne siete podporujú interaktivitu, čo znamená, že komunikácia je obojsmerná a často verejná. Komentáre, reakcie a zdieľania môžu zásadne ovplyvniť šírenie obsahu a jeho interpretáciu.

Ďalším dôležitým aspektom je tzv. **kurátorovanie identity**. Používatelia si vedome vytvárajú svoj online obraz, pričom prezentujú vybrané aspekty svojho života. Tento jav môže viesť k skresleniu reality a zároveň poskytuje útočníkom cenné informácie využiteľné pri sociálnom inžinierstve.

13.3 Výhody sociálnych sietí

Sociálne siete prinášajú množstvo benefitov, ktoré prispievajú k ich širokému využívaniu. Umožňujú rýchlu a efektívnu komunikáciu bez geografických obmedzení a poskytujú platformu na zdieľanie informácií v reálnom čase.

Z hľadiska spoločenského života podporujú vytváranie komunít a prepojenie ľudí s podobnými záujmami. V profesionálnom prostredí slúžia ako nástroj na networking, budovanie osobnej značky a kariérny rast.

V oblasti marketingu predstavujú silný nástroj na oslovenie cieľového publika, analýzu správania zákazníkov a personalizáciu obsahu. Ich interaktivita umožňuje okamžitú spätnú väzbu a zapojenie používateľov do diskusie.

13.4 Riziká a nevýhody sociálnych sietí

Napriek mnohým výhodám predstavujú sociálne siete aj významné riziká. Jedným z najzávažnejších je strata súkromia. Používatelia často zverejňujú osobné informácie, ktoré môžu byť zneužité na profilovanie, krádež identity alebo cielené útoky.

Ďalším problémom je šírenie dezinformácií. Algoritmy sociálnych sietí uprednostňujú obsah, ktorý vyvoláva emócie a interakciu, čo môže viesť k rýchlemu šíreniu nepravdivých alebo manipulatívnych informácií.

Významným rizikom je aj kyberšikana, ktorá sa prejavuje urážkami, vyhrážkami alebo verejným zosmiešňovaním. Tento typ správania môže mať vážne psychologické dôsledky.

Sociálne siete tiež podporujú vznik závislosti a nadmerného používania, čo negatívne ovplyvňuje koncentráciu, produktivitu a duševné zdravie. Navyše vytvárajú ilúziu ideálneho života, ktorá môže viesť k pocitom nedostatočnosti alebo frustrácie.

13.5 Typické bezpečnostné hrozby na sociálnych sieťach

Sociálne siete sú častým cieľom rôznych typov kybernetických útokov. Medzi najčastejšie patrí phishing, pri ktorom útočník využíva falošné správy alebo odkazy na získanie prihlasovacích údajov.

Ďalšou hrozbou je **prevzatie účtu (account takeover)**, ku ktorému dochádza v prípade slabého hesla alebo úniku prihlasovacích údajov. Útočník následne môže vystupovať v mene obete a šíriť podvody alebo škodlivý obsah.

Rozšírené je aj sociálne inžinierstvo, pri ktorom útočník manipuluje používateľa, aby mu dobrovoľne poskytol citlivé informácie. Využíva pritom verejne dostupné údaje zo sociálnych sietí.

Modernou hrozbou je aj **profilovanie a sledovanie používateľov**, ktoré umožňuje vytvárať detailné profily správania a preferencií. Tieto údaje môžu byť využité na cielenú reklamu, ale aj na manipuláciu alebo diskrimináciu.

13.6 Podvody na sociálnych sieťach

Sociálne siete sú prostredím, kde sa vyskytuje široké spektrum podvodov. Falošné účty podpory sa snažia získať prihlasovacie údaje tým, že sa vydávajú za oficiálne profily.

Pri kompromitácii účtu útočník kontaktuje priateľov obete a žiada finančnú pomoc pod zámienkou núdzovej situácie. Tento typ útoku je účinný, pretože využíva dôveru medzi používateľmi.

Milostné podvody sú založené na dlhodobom budovaní dôvery, po ktorom nasleduje žiadosť o peniaze. Podvodníci často používajú ukradnuté fotografie a falošné identity.

Časté sú aj investičné podvody a falošné súťaže, ktoré sľubujú vysoké zisky alebo výhry výmenou za poplatok alebo osobné údaje.

13.7 Ochrana súkromia a bezpečné správanie

Základom ochrany na sociálnych sieťach je uvedomelé správanie používateľa. Každá zverejnená informácia by mala byť zvážená z pohľadu jej možného zneužitia. Platí zásada minimalizácie údajov – zverejňovať len nevyhnutné informácie.

Dôležité je správne nastavenie súkromia účtu, ktoré obmedzuje prístup k obsahu len na dôveryhodné osoby. Používateľ by mal pravidelne kontrolovať tieto nastavenia, keďže platformy ich často menia.

Z technického hľadiska je nevyhnutné používať silné a jedinečné heslá a aktivovať dvojfaktorové overenie. Tým sa výrazne znižuje riziko neoprávneného prístupu.

Používateľ by mal byť opatrný pri komunikácii s neznámymi osobami a pri klikaní na odkazy. Každý podozrivý účet alebo obsah je vhodné nahlásiť, čím sa prispieva k bezpečnosti celej komunity.

13.8 Digitálna stopa a jej dôsledky

Používanie sociálnych sietí zanecháva digitálnu stopu, ktorá môže byť dlhodobo dostupná a analyzovateľná. Táto stopa zahŕňa nielen príspevky, ale aj interakcie, polohu, metadáta a správanie používateľa.

Digitálna stopa môže ovplyvniť napríklad:

- pracovné príležitosti,
- reputáciu jednotlivca,
- právne postavenie.

Preto je dôležité uvedomiť si, že obsah zverejnený online môže mať dlhodobé následky a nemusí byť možné ho úplne odstrániť.

13.9 Test

1. Prečo sú sociálne siete atraktívnym cieľom pre útočníkov?
a) Pretože neobsahujú žiadne údaje
b) Pretože zhromažďujú veľké množstvo údajov o používateľoch
c) Pretože sú vždy anonymné
d) Pretože neumožňujú komunikáciu

2. Aká je typická vlastnosť komunikácie na sociálnych sieťach?
a) Informácie sa šíria pomaly a kontrolovane
b) Komunikácia je vždy súkromná
c) Informácie sa šíria rýchlo a často bez overenia
d) Obsah nie je možné zdieľať

3. Ktoré z nasledujúcich patrí medzi riziká sociálnych sietí?
a) Zlepšenie komunikácie
b) Kyberšikana
c) Networking
d) Rýchla výmena informácií

4. Čo znamená phishing na sociálnych sieťach?
a) Zdieľanie fotografií
b) Vytváranie skupín
c) Pokus získať citlivé údaje pomocou falošných správ alebo odkazov
d) Automatické aktualizácie aplikácie

5. Aké je základné pravidlo ochrany súkromia na sociálnych sieťach?
a) Zverejňovať čo najviac informácií
b) Ignorovať nastavenia súkromia
c) Zverejňovať len nevyhnutné informácie
d) Prijímať všetky žiadosti o priateľstvo

14 Poznatky v oblasti kybernetickej bezpečnosti v kontexte trestného práva Slovenskej republiky

Kybernetická bezpečnosť patrí medzi kľúčové oblasti súčasnej bezpečnostnej politiky štátu. Rozvoj informačných a komunikačných technológií priniesol zásadné zmeny v spôsobe fungovania spoločnosti, ekonomiky aj verejnej správy. Digitalizácia však zároveň vytvorila nové možnosti páchania trestnej činnosti, ktorá sa presúva do kybernetického priestoru.

Kybernetický priestor má niekoľko špecifických vlastností, ktoré ho odlišujú od tradičného fyzického prostredia. Ide najmä o jeho globálny charakter, vysokú mieru anonymity, rýchlosť šírenia informácií a technologickú komplexnosť. Tieto faktory výrazne ovplyvňujú aj spôsob páchania trestnej činnosti a možnosti jej odhaľovania.

Trestné právo Slovenskej republiky reaguje na tieto výzvy postupným rozširovaním právnej úpravy a jej prispôsobovaním medzinárodným štandardom. Zároveň však platí, že právna regulácia často zaostáva za dynamikou technologického vývoja, čo vytvára priestor pre nové formy kriminality.

14.1 Kyberkriminalita v trestnom práve Slovenskej republiky

Kyberkriminalita predstavuje súhrn trestných činov, ktoré sú páchané prostredníctvom informačných a komunikačných technológií alebo sú na tieto technológie zamerané. V praxi možno rozlíšiť dve základné kategórie:

- trestné činy, pri ktorých je počítačový systém cieľom útoku (napr. hacking),
- trestné činy, pri ktorých je počítačový systém nástrojom (napr. online podvody).

Základnú právnu úpravu obsahuje zákon č. 300/2005 Z. z. (Trestný zákon). Medzi najvýznamnejšie ustanovenia patria:

- **§ 247 – Neoprávnený prístup do počítačového systému**
  Ide o konanie, pri ktorom páchateľ bez oprávnenia prenikne do informačného systému. Typickým príkladom je prelomenie hesla alebo zneužitie bezpečnostnej zraniteľnosti.
- **§ 247a – Neoprávnený zásah do počítačového systému**
  Zahŕňa napríklad zmazanie dát, zmenu údajov alebo narušenie prevádzky systému.
- **§ 247b – Neoprávnené získanie alebo držanie prístupových údajov**
  Týka sa napríklad získania hesiel prostredníctvom phishingu alebo ich ďalšieho predaja.
- **§ 247c – Poškodenie a zneužitie záznamu na nosiči informácií**
  Ide o manipuláciu s dátami, ich zničenie alebo zneužitie.

Je dôležité zdôrazniť, že kybernetická kriminalita sa často neobmedzuje len na tieto ustanovenia. V praxi sa uplatňujú aj ďalšie skutkové podstaty, najmä:

- podvod (napr. falošné e-shopy),
- vydieranie (ransomvér),
- porušovanie autorských práv,
- neoprávnené nakladanie s osobnými údajmi.

V aplikačnej praxi sa čoraz častejšie stretávame s prípadmi:

- kompromitácie e-mailových účtov a následného finančného podvodu (BEC – Business Email Compromise),
- útokov na bankové účty prostredníctvom škodlivého softvéru,
- zneužívania digitálnych identít,
- neoprávneného získavania a predaja dát na dark webe.

Osobitnú kategóriu predstavujú trestné činy spojené s kryptomenami, kde dochádza k legalizácii príjmov z trestnej činnosti alebo k podvodným investičným schémam. Tieto prípady kladú vysoké nároky na odborné znalosti vyšetrovateľov a znalcov.

Z pohľadu trestnoprávnej kvalifikácie je často problematické správne subsumovať konkrétne konanie pod jednotlivé skutkové podstaty, najmä v prípadoch technologicky komplexných útokov.

14.2 Typické formy kyberkriminality

V súčasnosti možno identifikovať viacero typických foriem kybernetickej kriminality, ktoré sa vyskytujú aj v podmienkach Slovenskej republiky:

Phishing a sociálne inžinierstvo
Ide o techniky, pri ktorých útočník manipuluje obeť s cieľom získať citlivé údaje (napr. heslá, čísla kariet). Využíva pritom psychologické prvky, ako sú dôvera alebo strach.

Ransomvér
Škodlivý softvér, ktorý zašifruje dáta a požaduje výkupné za ich obnovenie. Tento typ útoku predstavuje vážnu hrozbu najmä pre verejné inštitúcie.

DDoS útoky
Útoky zamerané na zahltenie servera a znemožnenie jeho fungovania. Často sú využívané aj ako forma vydierania.

Neoprávnené prieniky (hacking)
Zahŕňajú získanie neoprávneného prístupu do systémov s cieľom krádeže dát alebo ich zneužitia.

Kybernetické podvody
Patria sem napríklad falošné investičné platformy, podvodné e-shopy alebo tzv. „romance scam“.

Tieto formy kriminality sa neustále vyvíjajú a často kombinujú viacero techník.

14.3 Zákon o kybernetickej bezpečnosti a prevencia

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti predstavuje základný nástroj prevencie kybernetických incidentov. Jeho cieľom je zabezpečiť ochranu informačných systémov a minimalizovať riziká.

Zákon zavádza povinnosti najmä pre:

- prevádzkovateľov základných služieb,
- poskytovateľov digitálnych služieb.

Tieto subjekty sú povinné:

- analyzovať riziká,
- zavádzať bezpečnostné opatrenia,
- hlásiť incidenty,
- viesť bezpečnostnú dokumentáciu.

Pre pochopenie významu zákona je dôležité uvedomiť si, že ide o preventívny nástroj, ktorý dopĺňa represívnu funkciu trestného práva.

14.4 Dokazovanie v kybernetickej kriminalite

Jednou z najzložitejších oblastí je dokazovanie. Digitálne dôkazy majú špecifický charakter a vyžadujú osobitný prístup.

Medzi hlavné problémy patrí:

- rýchla zmena alebo zánik dôkazov,
- potreba odborných znalostí,
- medzinárodný charakter dát.

V praxi sa využívajú metódy digitálnej forenznej analýzy, ktoré umožňujú rekonštruovať priebeh incidentu. Dôležitá je aj spolupráca so znalcami.

Pre študenta je kľúčové pochopiť, že dôkazná situácia v kybernetických prípadoch býva často nepriamo založená na technických stopách (logy, IP adresy, metadata).

14.5 Výzvy pre aplikačnú prax

Kybernetická kriminalita prináša viacero výziev:

- **Identifikácia páchateľa** – anonymita a využívanie zahraničných infraštruktúr,
- **Jurisdikcia** – útok môže byť realizovaný z iného štátu,
- **Odbornosť** – potreba špecializovaných znalostí,
- **Rýchlosť vývoja** – nové typy útokov vznikajú veľmi rýchlo.

Tieto faktory spôsobujú, že boj proti kyberkriminalite je náročnejší ako pri tradičných formách kriminality.

14.6 Medzinárodný kontext

Kybernetická kriminalita má globálny charakter, preto je nevyhnutná medzinárodná spolupráca. Kľúčovým dokumentom je Dohovor o kyberkriminalite (Budapešť, 2001).

Na úrovni Európskej únie zohrávajú významnú úlohu:

- smernica NIS2,
- akt o kybernetickej bezpečnosti (Cybersecurity Act),
- akt o digitálnych službách (DSA),
- činnosť agentúr ako ENISA a Europol (EC3).

Tieto nástroje umožňujú koordináciu a efektívnejší boj proti kybernetickej kriminalite.

14.7 Budúce trendy

Vývoj kybernetickej kriminality je úzko spätý s technologickým pokrokom. V súčasnosti možno identifikovať viacero trendov:

- využívanie umelej inteligencie na generovanie phishingových kampaní,
- deepfake technológie využívané na podvody a dezinformácie,
- útoky na IoT zariadenia a smart infraštruktúru,
- automatizácia útokov prostredníctvom botnetov,
- rozmach „crime-as-a-service“ modelov.

Tieto trendy naznačujú, že kybernetická kriminalita bude čoraz sofistikovanejšia a dostupnejšia širšiemu okruhu páchateľov.

14.8 Test

1. Čo je kyberkriminalita podľa trestného práva SR?
a) Len fyzické útoky na zariadenia
b) Trestné činy páchané prostredníctvom alebo proti ICT systémom
c) Iba nelegálne sťahovanie filmov
d) Používanie internetu bez povolenia

2. Ktorý paragraf rieši neoprávnený prístup do počítačového systému?
a) § 247
b) § 300
c) § 404
d) § 123

3. Čo je ransomware?
a) Program na ochranu dát
b) Škodlivý softvér, ktorý šifruje dáta a požaduje výkupné
c) Nástroj na zálohovanie
d) Antivírusový program

4. Aký je hlavný cieľ zákona o kybernetickej bezpečnosti (69/2018 Z. z.)?
a) Trestať hackerov
b) Regulovať internet
c) Predchádzať incidentom a zvyšovať bezpečnosť systémov
d) Zakázať sociálne siete

5. Prečo je dokazovanie kybernetickej kriminality náročné?

a) Pretože neexistujú dôkazy
b) Pretože dôkazy sú vždy verejné
c) Kvôli rýchlej zmene dát, potrebe odbornosti a medzinárodnému charakteru
d) Pretože zákony to neumožňujú

15 Bezpečné používanie IT systémov a sietí

Bezpečné používanie informačných technológií a počítačových sietí patrí medzi základné predpoklady spoľahlivého fungovania každej organizácie. V súčasnosti je väčšina pracovných činností priamo závislá od informačných systémov, sieťovej komunikácie, cloudových služieb a digitálne uchovávaných údajov. Firemné prostredie preto čelí širokému spektru kybernetických hrozieb, medzi ktoré patria útoky škodlivým softvérom, phishing, zneužitie používateľských účtov, neoprávnený prístup do systémov, úniky údajov či znefunkčnenie prevádzky.

Bezpečnosť IT systémov nemožno chápať iba ako technický problém, ktorý rieši správca siete alebo oddelenie informačných technológií. Ide o komplexnú oblasť, v ktorej zohrávajú významnú úlohu technické opatrenia, organizačné pravidlá aj správanie samotných používateľov. Aj technologicky dobre zabezpečený systém môže byť oslabený nepozornosťou používateľa, slabým heslom, ignorovaním aktualizácií alebo neuváženým pripojením do nezabezpečenej siete.

Cieľom bezpečného používania IT systémov a sietí je chrániť dôvernosť, integritu a dostupnosť údajov. Dôvernosť znamená, že k údajom majú prístup iba oprávnené osoby. Integrita znamená, že údaje nie sú neoprávnene zmenené alebo poškodené. Dostupnosť znamená, že systémy a informácie sú k dispozícii vtedy, keď ich oprávnený používateľ potrebuje. Práve tieto tri princípy tvoria základ modernej informačnej bezpečnosti.
V podmienkach organizácie sa bezpečné používanie IT systémov prejavuje v mnohých každodenných činnostiach: pri prihlasovaní sa do systémov, práci s heslami, prenose súborov, používaní e-mailu, práci mimo pracoviska, pripájaní sa do Wi-Fi sietí alebo pri rozhodovaní o tom, kto má prístup ku konkrétnym údajom. Zamestnanec tak nie je iba používateľom technológií, ale zároveň aj aktívnym prvkom bezpečnostného systému organizácie.

15.1 Používanie silných hesiel

Heslo predstavuje najčastejší spôsob overenia identity používateľa v informačných systémoch. Napriek rozvoju viacfaktorového overovania zostávajú heslá jedným zo základných ochranných prvkov. Ich význam je preto mimoriadne vysoký, keďže slabé alebo opakovane používané heslo môže útočníkovi umožniť prístup k účtu, firemným údajom aj interným systémom.

Bezpečné heslo by malo byť dostatočne dlhé a ťažko uhádnuteľné. V minulosti sa kládol dôraz najmä na kombinovanie veľkých a malých písmen, číslic a špeciálnych znakov. V súčasnosti sa však čoraz viac zdôrazňuje najmä dĺžka hesla a jeho jedinečnosť. Praktickým riešením je používanie heslových fráz, teda dlhších kombinácií slov alebo viet, ktoré si používateľ dokáže zapamätať, no pre útočníka sú ťažko predvídateľné.

Pri tvorbe hesiel je potrebné vyhýbať sa osobným údajom, ako sú meno, dátum narodenia, názov firmy alebo mená rodinných príslušníkov. Takéto informácie možno často zistiť z verejne dostupných zdrojov alebo zo sociálnych sietí. Rovnako nevhodné sú jednoduché kombinácie znakov, napríklad „123456“, „qwerty“ alebo „heslo2025“.

Dôležitou zásadou je jedinečnosť hesiel. Používanie rovnakého hesla na viacerých účtoch výrazne zvyšuje riziko. Ak dôjde k úniku jedného hesla, útočník môže získať prístup aj k ďalším službám používateľa. V firemnom prostredí môže takáto chyba viesť k ohrozeniu viacerých systémov naraz.

Vhodným riešením je použitie správcu hesiel. Ide o aplikáciu, ktorá umožňuje bezpečne ukladať, generovať a organizovať silné heslá. Používateľ si potom musí pamätať len jedno hlavné heslo, pričom ostatné prístupové údaje spravuje systém. Správca hesiel zároveň znižuje potrebu zapisovania hesiel na papier alebo ich uchovávania v nezašifrovaných súboroch.

Pri práci s heslami treba myslieť aj na ich ochranu v bežnej prevádzke. Heslá sa nesmú zdieľať medzi kolegami, posielať nezabezpečeným e-mailom ani zapisovať na viditeľné miesta. V organizáciách by malo byť samozrejmosťou aj používanie viacfaktorového overovania, teda kombinácie hesla s ďalším prvkom, napríklad mobilnou aplikáciou, SMS kódom alebo hardvérovým tokenom. Takéto riešenie podstatne zvyšuje úroveň ochrany účtov.

15.2 Aktualizácie softvéru

Jedným zo základných predpokladov bezpečnej prevádzky zariadení a systémov je pravidelná aktualizácia softvéru. Operačné systémy, kancelárske aplikácie, webové prehliadače, antivírusové riešenia, sieťové zariadenia aj mobilné aplikácie môžu obsahovať bezpečnostné chyby, ktoré sú výrobcami priebežne opravované. Ak používateľ alebo organizácia tieto opravy neaplikuje, ponecháva svoje systémy zraniteľné.

Aktualizácie majú v bezpečnosti zásadný význam, pretože odstraňujú známe zraniteľnosti, ktoré môžu útočníci využiť na neoprávnený prístup, spustenie škodlivého kódu alebo získanie citlivých informácií. Veľká časť úspešných útokov v praxi nevyužíva zložité nové techniky, ale práve staré a už dávno známe chyby v neaktualizovaných systémoch.

Okrem bezpečnosti prinášajú aktualizácie aj zlepšenie stability, výkonu a kompatibility. Novšie verzie softvéru často opravujú chyby, zlepšujú správu pamäte, reagujú na zmeny v hardvéri a prinášajú podporu nových štandardov. Z pohľadu organizácie je preto aktualizácia nielen bezpečnostným, ale aj prevádzkovým opatrením.

Osobitnú pozornosť treba venovať aktualizáciám antivírusových a bezpečnostných programov. Tieto riešenia fungujú efektívne iba vtedy, ak majú k dispozícii aktuálne databázy hrozieb a pravidlá detekcie. Keďže nové formy malvéru vznikajú neustále, zastaraný antivírus nedokáže zabezpečiť dostatočnú ochranu.

V praxi sa odporúča zaviesť centralizovanú správu aktualizácií, najmä vo väčších organizáciách. Tá umožňuje kontrolovať, ktoré zariadenia sú aktuálne, plánovať nasadzovanie opráv a minimalizovať riziko, že niektoré stanice zostanú bez aktualizácií. Súčasťou bezpečnostnej politiky by mala byť aj jasne definovaná zodpovednosť za aktualizácie jednotlivých systémov.

15.3 Šifrovanie dát

Šifrovanie patrí medzi najdôležitejšie nástroje ochrany údajov. Jeho podstatou je transformácia údajov do takej podoby, aby boli bez príslušného kľúča nečitateľné. Aj keby sa k nim neoprávnená osoba dostala, bez možnosti dešifrovania ich nedokáže využiť.

Význam šifrovania je mimoriadny najmä pri práci s citlivými údajmi, ako sú osobné údaje, finančné informácie, obchodné tajomstvá, zdravotná dokumentácia či interné firemné dokumenty. Šifrovanie chráni údaje nielen pri ich ukladaní, ale aj pri prenose cez sieť.

Pri prenose údajov cez internet je dôležité používať zabezpečené komunikačné protokoly, napríklad HTTPS, TLS alebo VPN. Tieto technológie chránia dáta pred odpočúvaním a zásahom počas komunikácie. V prípade elektronickej pošty možno zvýšiť ochranu využitím šifrovania obsahu správ alebo aspoň zasielaním heslom chránených a šifrovaných príloh.

Šifrovanie uložených dát je dôležité napríklad na notebookoch, externých diskoch, USB kľúčoch alebo mobilných zariadeniach. Ak dôjde k strate alebo odcudzeniu zariadenia, šifrovanie môže zabrániť tomu, aby sa útočník dostal k jeho obsahu. V firemnom prostredí je preto vhodné využívať full disk encryption, teda úplné šifrovanie disku.

Treba rozlišovať medzi šifrovaním súboru, šifrovaním celého zariadenia a šifrovaním komunikácie. Každý z týchto prístupov chráni inú časť pracovného procesu. Efektívna bezpečnostná prax preto kombinuje viacero foriem šifrovania podľa charakteru spracúvaných údajov.

15.4 Používanie VPN

Virtuálna privátna sieť, označovaná skratkou VPN, slúži na vytvorenie chráneného komunikačného kanála medzi zariadením používateľa a firemnou sieťou alebo vzdialenou službou. Z pohľadu bezpečnosti je VPN dôležitá najmä pri práci mimo kancelárie, počas služobných ciest alebo pri pripájaní sa cez verejné Wi-Fi siete.

Hlavnou výhodou VPN je šifrovanie komunikácie. Ak sa používateľ pripája k firemnému systému cez nezabezpečenú alebo verejnú sieť, bez použitia VPN môže byť komunikácia vystavená riziku odpočúvania, manipulácie alebo presmerovania. VPN tieto riziká výrazne obmedzuje, pretože vytvára šifrovaný tunel, cez ktorý sa údaje prenášajú.

VPN však nemožno chápať ako univerzálne riešenie všetkých bezpečnostných problémov. Poskytuje ochranu prenosu, no neochráni používateľa pred phishingom, slabými heslami alebo škodlivým softvérom v zariadení. Preto musí byť jej používanie súčasťou širšieho súboru bezpečnostných opatrení.

Vo firemnom prostredí je dôležité, aby VPN riešenie bolo správne nakonfigurované, využívalo silné šifrovacie mechanizmy a bolo doplnené o spoľahlivé overovanie identity používateľa. Vhodné je aj viacfaktorové overovanie. Organizácie by mali zároveň evidovať, kto a kedy pristupuje cez VPN, a monitorovať neobvyklé prístupy alebo pokusy o zneužitie.

15.5 Bezpečnostné školenie zamestnancov

Ľudský faktor patrí medzi najvýznamnejšie prvky informačnej bezpečnosti. Veľká časť úspešných incidentov vzniká nie v dôsledku zlyhania technológie, ale v dôsledku chyby používateľa. Práve preto je bezpečnostné školenie zamestnancov nevyhnutnou súčasťou ochrany organizácie.

Cieľom školení je zvýšiť povedomie o hrozbách, vysvetliť zásady bezpečného správania a naučiť zamestnancov správne reagovať v rizikových situáciách. Zamestnanci by mali vedieť rozpoznať phishingový e-mail, podozrivú prílohu, falošnú prihlasovaciu stránku, neštandardnú požiadavku na platbu alebo neobvyklé správanie zariadenia.

Bezpečnostné školenie by nemalo byť jednorazovou aktivitou. Hrozby sa vyvíjajú a menia, preto je potrebné vzdelávanie pravidelne opakovať a aktualizovať. Účinné sú krátke tematické školenia, praktické ukážky, simulované phishingové kampane a priebežné pripomínanie bezpečnostných pravidiel.

Dôležité je, aby bezpečnostná kultúra v organizácii nebola založená na strachu alebo hľadaní vinníka, ale na podpore zodpovedného správania. Zamestnanec musí mať istotu, že ak nahlási podozrivý incident alebo prizná chybu, organizácia bude reagovať konštruktívne a zameria sa na riešenie problému.

15.6 Obmedzenie prístupu

Nie každý zamestnanec potrebuje mať prístup ku všetkým údajom a systémom. Jednou zo základných zásad informačnej bezpečnosti je princíp minimálnych oprávnení. To znamená, že používateľ má mať iba taký prístup, aký nevyhnutne potrebuje na výkon svojej práce.

Tento princíp znižuje riziko úniku údajov, obmedzuje možnosti zneužitia prístupu a minimalizuje dopad prípadného kompromitovania účtu. Ak napríklad zamestnanec z oddelenia marketingu nepotrebuje prístup k účtovníctvu alebo personálnym údajom, nemal by ho mať pridelený.

Riadenie prístupových práv by malo vychádzať z pracovných rolí a zodpovedností. V praxi sa využíva model role-based access control, pri ktorom sa oprávnenia prideľujú podľa funkcie používateľa v organizácii. Takéto riešenie je prehľadnejšie, bezpečnejšie a jednoduchšie na správu.

Osobitne dôležité je správne nastavovanie prístupov pri nástupe nového zamestnanca, zmene pracovnej pozície a ukončení pracovného pomeru. V mnohých organizáciách vznikajú problémy práve tým, že bývalým zamestnancom zostávajú aktívne účty alebo nadbytočné oprávnenia. Pravidelné revízie prístupových práv sú preto nevyhnutné.

15.7 Monitorovanie a audit

Monitorovanie a audit patria medzi základné nástroje kontroly bezpečnosti IT prostredia. Ich cieľom je sledovať, kto, kedy a akým spôsobom pristupoval k systémom, údajom alebo

sieťovým zdrojom. Takéto informácie majú zásadný význam pri odhaľovaní incidentov, vyšetrovaní podozrivých aktivít aj pri overovaní súladu s internými pravidlami a právnymi požiadavkami.

Monitorovanie umožňuje včas zachytiť neobvyklé správanie, napríklad opakované neúspešné prihlasovania, prístupy mimo bežného pracovného času, presuny veľkého objemu dát alebo pokusy o prístup k neštandardným systémom. Audit zase poskytuje systematické vyhodnotenie toho, či organizácia dodržiava definované bezpečnostné pravidlá a či sú prijaté opatrenia účinné.

Z pohľadu prevádzky je dôležité zaznamenávať udalosti v logoch a zabezpečiť ich ochranu pred neoprávnenou manipuláciou. Logy majú význam nielen pri reakcii na incident, ale aj pri spätnej analýze udalostí. Ak organizácia nedisponuje spoľahlivými záznamami, jej schopnosť identifikovať príčinu incidentu je výrazne oslabená.

Treba však dbať aj na primeranosť monitorovania. Organizácia musí rešpektovať právne predpisy, ochranu osobných údajov a princíp transparentnosti voči zamestnancom. Monitorovanie preto musí mať jasne definovaný účel, rozsah a pravidlá používania získaných údajov.

15.8 Bezpečné Wi-Fi siete

Bezdrôtové siete sú dnes bežnou súčasťou firemnej infraštruktúry, no zároveň predstavujú špecifické bezpečnostné riziko. Na rozdiel od káblovej siete sa signál šíri priestorom a môže byť zachytený aj mimo priestorov organizácie. Preto je nevyhnutné venovať zabezpečeniu Wi-Fi siete osobitnú pozornosť.

Prvým krokom je zmena predvolených prihlasovacích údajov na sieťových zariadeniach. Výrobné mená a heslá bývajú verejne známe a ich ponechanie výrazne zvyšuje riziko kompromitovania zariadenia. Rovnako dôležité je pravidelne aktualizovať firmvér prístupových bodov a routerov.

Z hľadiska šifrovania sa odporúča používať moderné štandardy, prednostne WPA3, prípadne bezpečne nastavené WPA2 tam, kde novší štandard nie je dostupný. Používanie zastaraných a slabých mechanizmov predstavuje významné riziko. Heslo do Wi-Fi siete by malo byť dostatočne silné a nemalo by sa nekontrolovane zdieľať.

Vo firemnom prostredí je vhodné oddeliť internú sieť od siete pre návštevníkov. Hosťovská sieť by nemala umožniť prístup k interným serverom, pracovným staniciam ani tlačiarňam. Segmentácia siete je dôležitým opatrením, ktoré znižuje riziko laterálneho pohybu útočníka v prípade kompromitácie jedného segmentu.

Ďalším opatrením môže byť obmedzenie administrácie zariadení iba z interných adries, deaktivácia nepotrebných služieb, používanie sieťového firewallu a sledovanie pripojených zariadení. Filtrovanie MAC adries môže predstavovať doplnkové opatrenie, no nemožno ho považovať za samostatne postačujúcu ochranu, keďže MAC adresu možno relatívne ľahko napodobniť.

15.9 Praktické odporúčania pre používateľov

Bezpečné používanie IT systémov a sietí je v každodennej praxi postavené na zodpovednom správaní používateľa. Medzi základné odporúčania patrí neprihlasovať sa do firemných systémov z nedôveryhodných zariadení, neotvárať neznáme prílohy, overovať si neštandardné požiadavky, zamykať pracovnú stanicu pri odchode od pracoviska a nepoužívať neautorizovaný softvér.

Používateľ by mal byť obozretný aj pri práci s cloudovými úložiskami, externými médiami a mobilnými zariadeniami. Každý prenos dát mimo schválených systémov organizácie zvyšuje riziko straty kontroly nad údajmi. Rovnako dôležité je nahlasovať bezpečnostné incidenty bez zbytočného odkladu, aj keď sa používateľ domnieva, že chyba je zanedbateľná. Rýchla reakcia totiž často rozhoduje o rozsahu škôd.

Z pedagogického hľadiska je potrebné zdôrazniť, že bezpečnosť v IT nie je stav, ktorý sa dosiahne jednorazovo. Ide o nepretržitý proces, ktorý si vyžaduje pravidelné vyhodnocovanie rizík, aktualizáciu opatrení a adaptáciu na nové hrozby.

15.10 Bezpečné používanie IT systémov a sietí – cvičenia

Úloha 1: Silné heslo – alebo nie?
Cieľ: Naučiť sa rozpoznávať silné a slabé heslá.
Zadanie: Posúď, ktoré z nasledujúcich hesiel sú bezpečné, a stručne vysvetli prečo:

1. 123456
2. Peter2024
3. $M0jeSiln3Heslo!
4. qwerty
5. H3slov@Fr@ze2025

Otázky:

1. Ktoré heslá by si označil ako silné?
2. Aké vlastnosti má bezpečné heslo?
3. Prečo nie je vhodné používať meno alebo rok narodenia v hesle?
4. Aký význam má jedinečnosť hesla pre každý účet?

Úloha 2: Scenár – aktualizácie v praxi
Cieľ: Pochopiť význam pravidelných aktualizácií.
Scenár:
Na firemnom notebooku sa ti už niekoľko dní zobrazuje upozornenie, že je dostupná nová verzia operačného systému. Kolega tvrdí, že aktualizácie netreba riešiť, pretože iba spomaľujú počítač.
Otázky:

1. Ako by si v tejto situácii postupoval?
2. Aké bezpečnostné riziká vznikajú pri odkladaní aktualizácií?
3. Prečo sú dôležité aj aktualizácie antivírusových programov?
4. Aký je rozdiel medzi funkčnou aktualizáciou a bezpečnostnou opravou?

Úloha 3: Šifrovanie – tajomstvo v dátach

Cieľ: Pochopiť význam šifrovania pri ochrane údajov.
Zadanie:
Predstav si, že potrebuješ kolegovi zaslať súbor obsahujúci mzdové údaje zamestnancov.
Otázky:

1. Aký spôsob odoslania by bol najbezpečnejší?
2. Ako môžeš zabezpečiť, aby obsah súboru nebol čitateľný pre neoprávnenú osobu?
3. Aký je rozdiel medzi šifrovaním súboru a šifrovaním e-mailovej komunikácie?
4. Prečo je dôležité chrániť aj zariadenie, na ktorom sú súbory uložené?

Úloha 4: VPN – bezpečné pripojenie
Cieľ: Pochopiť význam VPN pri práci mimo firemnej siete.
Scenár:
Pracuješ z kaviarne a potrebuješ sa pripojiť do interného informačného systému organizácie. K dispozícii je iba verejná otvorená Wi-Fi sieť.
Otázky:

1. Aké riziká sú spojené s používaním verejnej Wi-Fi siete?
2. Ako VPN znižuje tieto riziká?
3. Chráni VPN používateľa pred všetkými hrozbami? Vysvetli.
4. V ktorých situáciách je používanie VPN obzvlášť dôležité?

Úloha 5: Firemná Wi-Fi – nastav to správne
Cieľ: Precvičiť správne zásady zabezpečenia bezdrôtovej siete.
Zadanie:
Rozhodni, ktoré z nasledujúcich opatrení patria k bezpečnej správe Wi-Fi siete:
A. Ponechať predvolené heslo routera.
B. Použiť šifrovanie WPA3.
C. Pravidelne aktualizovať firmvér.
D. Zdieľať heslo s každým návštevníkom.
E. Oddeliť sieť pre hostí od internej siete.
Otázky:

1. Ktoré opatrenia sú správne a prečo?
2. Prečo je nebezpečné ponechať predvolené prihlasovacie údaje?
3. Aký význam má oddelenie hosťovskej siete od internej siete?

Úloha 6: Kto má prístup?
Cieľ: Pochopiť význam obmedzenia prístupových práv.
Scenár:
Nový zamestnanec má po nástupe prístup do všetkých firemných priečinkov vrátane účtovníctva, personálnej agendy a vedenia spoločnosti, hoci tieto údaje nepotrebuje na výkon svojej práce.
Otázky:

1. Prečo je takto nastavený prístup problematický?
2. Aká zásada informačnej bezpečnosti je v tomto prípade porušená?
3. Ako by mali byť správne nastavené prístupové práva?
4. Prečo je potrebné pravidelne kontrolovať a auditovať pridelené oprávnenia?

Úloha 7: Phishingový e-mail

Cieľ: Rozvíjať schopnosť rozpoznať podvodnú správu.
Zadanie:
Predstav si, že ti príde e-mail s predmetom „Okamžité overenie účtu“, v ktorom sa od teba žiada kliknúť na odkaz a zadať prihlasovacie údaje.
Otázky:

1. Ktoré znaky môžu naznačovať, že ide o phishing?
2. Aký by mal byť správny postup používateľa?
3. Prečo je nebezpečné reagovať pod časovým tlakom?
4. Komu by si mal takýto e-mail nahlásiť?

Úloha 8: Monitorovanie a audit
Cieľ: Pochopiť význam logovania a kontroly aktivít.
Scenár:
Správca IT zistí, že sa jeden používateľský účet prihlasoval v noci z dvoch rôznych miest v krátkom časovom odstupe.
Otázky:

1. Prečo ide o podozrivú udalosť?
2. Ako môže monitoring pomôcť pri odhalení incidentu?
3. Aký význam majú logy pri vyšetrovaní bezpečnostných udalostí?
4. Prečo nestačí mať logy uložené, ale treba ich aj pravidelne vyhodnocovať?

15.11Test

1. Aké tri princípy tvoria základ modernej informačnej bezpečnosti?
a) Rýchlosť, dostupnosť, zisk
b) Dôvernosť, integrita, dostupnosť
c) Heslo, Wi-Fi, cloud
d) Šifrovanie, e-mail, firewall

2. Ktoré tvrdenie o bezpečných heslách je správne?
a) Najlepšie je používať rovnaké heslo na viacerých účtoch
b) Heslo by malo obsahovať osobné údaje, aby sa ľahšie pamätalo
c) Heslo by malo byť dlhé a jedinečné pre každý účet
d) Heslá je vhodné zapisovať na papier pri monitore

3. Prečo sú aktualizácie softvéru dôležité?
a) Len kvôli zmene vzhľadu aplikácie
b) Odstraňujú známe zraniteľnosti a zvyšujú bezpečnosť
c) Spomaľujú útoky len na Wi-Fi
d) Nahrádzajú potrebu antivírusu aj hesiel

4. Aký je hlavný prínos VPN pri práci mimo kancelárie?
a) Zrýchľuje počítač
b) Automaticky chráni pred phishingom
c) Vytvára šifrovaný komunikačný kanál
d) Nahrádza aktualizácie softvéru

5. Čo znamená princíp minimálnych oprávnení?
a) Každý zamestnanec má prístup ku všetkým údajom
b) Používateľ má len taký prístup, aký nevyhnutne potrebuje
c) Prístupové práva sa nepridelujú podľa pracovnej roly
d) Bývalým zamestnancom zostávajú účty aktívne

16Zaobchádzanie s flash diskami a externými médiami

Externé pamäťové médiá, ako sú USB kľúče, externé pevné disky, pamäťové karty či prenosné SSD, patria medzi bežné nástroje na prenos a uchovávanie dát. Ich používanie je jednoduché, rýchle a praktické, no z pohľadu kybernetickej bezpečnosti predstavujú významné riziko. Prostredníctvom externých médií môže dôjsť k strate údajov, ich neoprávnenému sprístupneniu, poškodeniu alebo zavedeniu škodlivého softvéru do informačného systému.

Používatelia často vnímajú flash disky a ďalšie externé médiá ako technicky nenáročné zariadenia, ktoré nevyžadujú osobitnú pozornosť. V skutočnosti však práve tieto médiá predstavujú častý zdroj bezpečnostných incidentov. Môžu byť stratené, odcudzené, nesprávne zlikvidované alebo použité v nebezpečnom zariadení. V organizáciách je preto nevyhnutné stanoviť jasné pravidlá ich používania a zabezpečenia.

Bezpečné zaobchádzanie s externými médiami zahŕňa ochranu údajov pred technickým zlyhaním, fyzickým poškodením aj neoprávneným prístupom. Dôležitá je nielen ochrana samotného zariadenia, ale aj správne postupy pri prenose súborov, zálohovaní, šifrovaní a likvidácii dát. V praxi totiž nestačí sústrediť sa len na vytvorenie kópie súborov. Rovnako dôležité je zabezpečiť, aby sa tieto dáta nedostali do nepovolaných rúk.

16.1 Riziká spojené s používaním externých médií

Externé médiá prinášajú viaceré bezpečnostné riziká. Prvým je riziko fyzickej straty alebo krádeže. USB kľúče a prenosné disky sú malé, ľahko prenosné a často sa používajú mimo priestorov organizácie. Ich strata môže mať vážne následky, najmä ak obsahujú citlivé dokumenty, osobné údaje alebo obchodné informácie.

Druhým rizikom je zavlečenie škodlivého softvéru. Externé médiá môžu byť nositeľom vírusov, ransomvéru alebo iného škodlivého kódu. Ak používateľ pripojí neznámy alebo nedôveryhodný USB kľúč k pracovnému počítaču, môže nevedome ohroziť celý informačný systém organizácie. Z tohto dôvodu by sa nemali používať náhodne nájdené zariadenia ani médiá neznámeho pôvodu.

Tretím významným rizikom je neoprávnené kopírovanie alebo odnášanie dát. Externé médium môže byť zneužité na úmyselné aj neúmyselné vynesenie citlivých údajov mimo organizácie. V mnohých prípadoch nejde o sofistikovaný útok, ale o nedostatočnú disciplínu používateľa, ktorý si bez súhlasu skopíruje dokumenty na súkromný USB disk.

Rizikom je aj technické poškodenie zariadenia. Externé disky sú citlivé na nárazy, vlhkosť, prach, extrémne teploty alebo nesprávne odpojenie. Poškodenie média môže viesť k strate dát alebo k ich čiastočnej nečitateľnosti. Osobitne citlivé sú mechanické pevné disky, ktoré obsahujú pohyblivé časti.

16.2 Pravidlá bezpečného používania externých médií

Bezpečné používanie externých médií si vyžaduje dodržiavanie niekoľkých základných zásad. V prvom rade je potrebné používať iba dôveryhodné a schválené zariadenia. V organizáciách

by malo byť jasne určené, ktoré typy médií možno pripájať k firemným počítačom a za akých podmienok.

Pri práci s externými médiami je vhodné zabezpečiť pravidelné zálohovanie dôležitých údajov. Externý disk síce môže slúžiť ako úložisko, no sám osebe nie je zárukou bezpečnosti. Ak dôjde k jeho poškodeniu alebo strate, bez ďalšej zálohy môžu byť údaje nenávratne stratené. Preto by používateľ nemal považovať jediný externý disk za definitívne a postačujúce úložisko.

Dôležité je aj šifrovanie dát uložených na prenosných médiách. Ak sa zariadenie stratí alebo je odcudzené, šifrovanie výrazne znižuje riziko zneužitia dát. V operačných systémoch sú na tento účel dostupné rôzne nástroje, napríklad BitLocker vo Windows alebo FileVault v prostredí macOS. Šifrovanie je obzvlášť dôležité pri médiách, ktoré sa používajú na prenos osobných údajov, finančných dokumentov alebo internej firemnej agendy.

Používateľ by mal dbať aj na správne odpojovanie zariadenia. Funkcia bezpečného odstránenia hardvéru nie je len formálnym úkonom, ale slúži na korektné ukončenie zápisu a minimalizáciu rizika poškodenia súborového systému. Náhle odpojenie média počas prenosu dát môže viesť k poškodeniu súborov aj samotného úložiska.

Súčasťou bezpečného používania je aj ochrana pred fyzickým poškodením. Externé médiá by mali byť chránené pred pádom, otrasmi, vlhkosťou a nadmerným teplom. Pri prenášaní je vhodné používať ochranné puzdrá a pri skladovaní voliť bezpečné a suché miesto. V organizáciách je potrebné zabrániť tomu, aby boli externé médiá voľne ponechané na stole, v spoločných priestoroch alebo v neuzamknutých zásuvkách.

16.3 Aktualizácia, kontrola a údržba médií

Hoci sa pri externých médiách kladie dôraz najmä na ochranu dát, dôležitá je aj ich technická údržba. Používateľ by mal priebežne kontrolovať funkčnosť zariadenia a v prípade potreby aktualizovať príslušné ovládače alebo firmvér, ak to výrobca podporuje. Tieto aktualizácie môžu odstrániť technické chyby a zlepšiť spoľahlivosť zariadenia.

Pri podozrení na poškodenie alebo chyby v súborovom systéme je vhodné vykonať kontrolu a opravu média pomocou systémových nástrojov. V prostredí Windows možno využiť napríklad nástroj chkdsk, v iných systémoch zasa obdobné diagnostické utility. Takéto riešenia môžu pomôcť odhaliť logické chyby, poškodené sektory alebo nekonzistenciu súborového systému. Treba však zdôrazniť, že technická kontrola média nenahrádza zálohovanie. Ak sa objavia prvé príznaky poruchy, ako sú pomalý prístup, chybové hlásenia alebo výpadky spojenia, prioritou má byť okamžité zálohovanie dát a až následne diagnostika zariadenia.

16.4 Ochrana dát pri prenose a zdieľaní

Prenos údajov prostredníctvom externých médií musí byť vždy zvážený z hľadiska bezpečnosti a nevyhnutnosti. V prostredí organizácií by sa citlivé súbory nemali prenášať na súkromných USB kľúčoch bez súhlasu a bez primeranej ochrany. Ak je prenos potrebný, údaje by mali byť šifrované a prístup k nim by mal byť obmedzený len na oprávnené osoby.

Dôležitým princípom je aj evidencia prenosných médií, najmä v prípadoch, keď obsahujú dôležité alebo citlivé informácie. Organizácia by mala vedieť, kto médium používa, aké dáta obsahuje a kde sa nachádza. Takýto prístup znižuje riziko straty kontroly nad dátami a zvyšuje zodpovednosť používateľov.

Pri pripájaní externých médií je vhodné využívať antivírusovú kontrolu. Mnohé škodlivé programy sa v minulosti šírili práve cez USB zariadenia, pričom používateľ si často neuvedomoval, že médium bolo infikované na inom počítači. Automatická kontrola pri pripojení preto predstavuje dôležitú preventívnu vrstvu ochrany.

16.5 Bezpečné vymazanie dát

Osobitnou otázkou pri práci s externými médiami je bezpečné odstránenie dát. Bežné vymazanie súboru alebo formátovanie disku spravidla neznamená, že dáta boli skutočne nenávratne zničené. V mnohých prípadoch je ich možné obnoviť pomocou špecializovaného softvéru. Ak preto ide o citlivé alebo dôverné informácie, je potrebné použiť metódy bezpečného mazania.

Pri mechanických pevných diskoch sa tradične využíva viacnásobné prepísanie dát vhodným nástrojom. Takýto prístup sťažuje alebo znemožňuje ich obnovu. Pri SSD diskoch je však situácia odlišná, keďže používajú inú technológiu zápisu. V ich prípade sa odporúča využiť funkcie zabudované vo firmvéri zariadenia, napríklad ATA Secure Erase alebo nástroje dodávané výrobcom.

Ďalším možným prístupom je šifrovanie disku a následné vymazanie. Ak boli údaje predtým zašifrované a dôjde k bezpečnému odstráneniu kľúča alebo k vymazaniu zariadenia, aj prípadne obnovené dáta zostanú nečitateľné. Tento prístup je praktický najmä v organizáciách, ktoré používajú plošné šifrovanie zariadení.

V niektorých prípadoch, najmä pri vyradení nefunkčného alebo vysoko citlivého média, je vhodné aj fyzické zničenie zariadenia. Ide o krajnú, ale veľmi účinnú metódu. Fyzická likvidácia sa využíva najmä tam, kde je potrebná maximálna istota, že údaje nebudú nikdy obnovené.

Pred každým bezpečným vymazaním musí používateľ alebo správca systému overiť, že všetky dôležité dáta boli zálohované. Proces bezpečného mazania je nevratný a chyba pri ňom môže viesť k definitívnej strate údajov.

16.6 Organizačné pravidlá a používateľská disciplína

Bezpečné používanie externých médií nie je iba technickou otázkou. Rovnako dôležité sú interné pravidlá organizácie a disciplína používateľov. Organizácia by mala mať určené, či zamestnanci smú používať súkromné USB zariadenia, aké dáta možno prenášať mimo internej siete, kto schvaľuje použitie externých médií a akým spôsobom sa evidujú.

Z pedagogického hľadiska je potrebné zdôrazniť, že externé médium je síce užitočný nástroj, no zároveň aj potenciálny bezpečnostný incident v malom formáte. Preto je potrebné

pristupovať k nemu s rovnakou zodpovednosťou ako k iným informačným aktívam organizácie.

16.7 Zhrnutie kapitoly

Flash disky, externé disky a ďalšie prenosné médiá predstavujú praktický prostriedok na prenos a uchovávanie dát, no zároveň aj významné bezpečnostné riziko. Ich bezpečné používanie si vyžaduje kombináciu technických opatrení, ako sú šifrovanie, antivírusová kontrola a bezpečné mazanie, spolu s organizačnými pravidlami, evidenciou a zodpovedným správaním používateľov.

Kľúčovými zásadami sú používanie dôveryhodných zariadení, pravidelné zálohovanie, ochrana pred fyzickým poškodením, správne odpojovanie, kontrola zariadení a bezpečné vymazanie údajov pred vyradením média. Len tak možno minimalizovať riziko straty dát, ich zneužitia alebo zavlečenia škodlivého softvéru do informačného systému.

16.8 Test

1. Aké je jedno z hlavných rizík používania externých médií?
a) Zrýchlenie prenosu dát
b) Zavlečenie škodlivého softvéru
c) Automatické šifrovanie súborov
d) Zníženie kapacity siete

2. Prečo je dôležité šifrovanie dát na externých médiách?
a) Aby sa zrýchlil prenos dát
b) Aby boli údaje čitateľné pre každého
c) Aby sa pri strate alebo krádeži znížilo riziko zneužitia dát
d) Aby nebolo potrebné zálohovanie

3. Čo je správny postup pri odpojovaní USB zariadenia?
a) Vytiahnuť ho kedykoľvek bez kontroly
b) Použiť bezpečné odstránenie hardvéru
c) Reštartovať počítač
d) Najprv vypnúť monitor

4. Čo platí o bežnom vymazaní súborov z externého média?
a) Dáta sú vždy nenávratne zničené
b) Formátovanie automaticky znemožní obnovu dát
c) Dáta možno v mnohých prípadoch ešte obnoviť
d) Vymazanie súboru znamená fyzické zničenie média

5. Ktoré pravidlo je správne pri používaní externých médií v organizácii?
a) Používať akýkoľvek nájdený USB kľúč
b) Prenášať citlivé údaje na súkromných médiách bez ochrany
c) Používať len dôveryhodné a schválené zariadenia
d) Nechať externé disky voľne položené v spoločných priestoroch

17 Zálohovanie dát

Zálohovanie dát patrí medzi základné piliere informačnej a kybernetickej bezpečnosti. Predstavuje proces vytvárania kópií údajov s cieľom zabezpečiť ich obnovu v prípade straty, poškodenia, zneprístupnenia alebo napadnutia. V digitálnom prostredí, kde sú organizácie aj jednotlivci závislí od dostupnosti informácií, predstavuje záloha jeden z najúčinnejších spôsobov ochrany pred dôsledkami technických porúch, ľudských chýb a kybernetických útokov.

Význam zálohovania spočíva v tom, že chráni nielen samotné dáta, ale aj kontinuitu činností, ktoré sú na nich závislé. Bez možnosti obnovy údajov môže aj pomerne malý incident prerásť do vážneho prevádzkového alebo ekonomického problému. Strata účtovných dokumentov, databáz, projektových súborov, zmlúv či osobných údajov môže mať ďalekosiahle dôsledky pre jednotlivca aj organizáciu.

Je dôležité rozlišovať medzi ukladaním dát a ich zálohovaním. To, že sa súbor nachádza na pevnom disku, v cloudovom úložisku alebo na sieťovom disku, ešte automaticky neznamená, že je bezpečne zálohovaný. Skutočná záloha musí byť oddelenou a použiteľnou kópiou, ktorá umožní obnovu údajov po incidente.

17.1 Prečo zálohovať dáta

Zálohovanie údajov slúži ako ochranný mechanizmus proti rôznym typom incidentov. Medzi najčastejšie patria poruchy hardvéru, zlyhanie úložiska, poškodenie súborového systému, omyl používateľa, vymazanie súborov, krádež zariadenia, požiar, zaplavenie či iná fyzická udalosť. V každom z týchto prípadov môže záloha rozhodnúť o tom, či bude možné dáta obnoviť.

Mimoriadne významnú úlohu zohrávajú zálohy pri obrane proti ransomvéru. Tento typ škodlivého softvéru zašifruje alebo zneprístupní údaje a následne požaduje výkupné za ich obnovenie. Organizácia, ktorá má k dispozícii kvalitné a oddelené zálohy, môže po incidente obnoviť dáta bez toho, aby musela komunikovať s útočníkmi alebo platiť výkupné.

Pre organizácie má zálohovanie strategický význam aj z pohľadu kontinuity prevádzky. Ak dôjde k zlyhaniu servera, databázy alebo úložiska, záloha umožní návrat k funkčnému stavu a minimalizáciu výpadku služieb. Zálohovanie preto úzko súvisí s plánovaním obnovy po havárii a so širšou koncepciou prevádzkovej odolnosti.

Zálohovanie však nie je dôležité iba vo firemnom prostredí. Aj bežný používateľ môže prísť o fotografie, dokumenty, kontakty alebo osobné záznamy. Záloha je preto dôležitá pre každého, kto pracuje s digitálnymi údajmi a nechce riskovať ich nenahraditeľnú stratu.

17.2 Spôsoby realizácie záloh

Existuje viacero spôsobov realizácie záloh a každý z nich má svoje výhody, obmedzenia a vhodné oblasti použitia. Pri výbere metódy je potrebné zohľadniť objem dát, požadovaný čas obnovy, dostupný priestor, finančné možnosti aj dôležitosť chránených informácií.

17.2.1 Úplná záloha

Úplná záloha predstavuje najjednoduchší a najprehľadnejší typ zálohovania. Pri jej vytvorení sa kopírujú všetky vybrané dáta bez ohľadu na to, či sa od poslednej zálohy zmenili. Výhodou tejto metódy je vysoká spoľahlivosť a jednoduchá obnova, pretože všetko potrebné sa nachádza v jednej záložnej sade.

Nevýhodou úplnej zálohy je vyššia časová aj priestorová náročnosť. Pri veľkom objeme dát môže byť jej pravidelné vykonávanie neefektívne. V praxi sa preto často kombinuje s inými metódami.

17.2.2 Inkrementálna záloha

Inkrementálna záloha ukladá iba tie dáta, ktoré sa zmenili od poslednej vykonanej zálohy, bez ohľadu na to, či išlo o úplnú alebo inkrementálnu zálohu. Táto metóda je úspornejšia z hľadiska času aj úložného priestoru, keďže sa zálohujú len nové alebo upravené súbory.

Nevýhodou je náročnejšia obnova. Na úplné obnovenie stavu je potrebné mať k dispozícii poslednú úplnú zálohu a všetky nasledujúce inkrementálne zálohy. Ak niektorá z nich chýba alebo je poškodená, proces obnovy môže byť neúplný alebo nemožný.

17.2.3 Rozdielová záloha

Rozdielová záloha kopíruje všetky zmeny, ktoré vznikli od poslednej úplnej zálohy. Ide o kompromis medzi úplnou a inkrementálnou metódou. Je rýchlejšia ako opakované vytváranie úplnej zálohy, no zároveň jednoduchšia na obnovu než inkrementálna záloha, pretože na obnovu stačí posledná úplná a posledná rozdielová záloha.

Nevýhodou je, že s pribúdajúcim časom od poslednej úplnej zálohy rastie aj objem rozdielovej zálohy. Preto sa aj táto metóda zvyčajne kombinuje s pravidelnými úplnými zálohami.

17.2.4 Zrkadlová záloha

Zrkadlová záloha vytvára presnú kópiu dát na inom úložisku, často takmer v reálnom čase. Jej výhodou je rýchla dostupnosť a možnosť okamžitého použitia záložných dát. V niektorých prípadoch umožňuje takmer plynulé pokračovanie prevádzky aj pri zlyhaní primárneho úložiska.

Na druhej strane je táto metóda náročná na kapacitu aj financie. Navyše treba myslieť na to, že ak dôjde k nechcenej zmene, poškodeniu alebo zašifrovaniu dát na primárnom úložisku, táto zmena sa môže preniesť aj do zrkadlovej kópie. Zrkadlenie preto nemožno považovať za plnohodnotnú náhradu zálohovania s históriou verzií.

17.2.5 Cloudové zálohovanie

Cloudové zálohovanie predstavuje moderný a rozšírený spôsob ochrany dát. Údaje sa ukladajú na vzdialené servery poskytovateľa služby a používateľ má k nim prístup cez internet. Výhodou

je pohodlnosť, automatizácia, geografická oddelenosť úložiska a možnosť obnovy aj v prípade fyzickej straty zariadenia.

Nevýhodou je závislosť od internetového pripojenia, dôvera voči poskytovateľovi služby a možné náklady na úložný priestor alebo prenos dát. Pri citlivých údajoch treba zároveň dbať na šifrovanie, právny režim spracúvania údajov a umiestnenie dátových centier.

17.2.6 Externé disky a NAS

Zálohovanie na externé disky alebo sieťové úložiská NAS je medzi používateľmi aj organizáciami veľmi rozšírené. Výhodou je relatívne nízka cena, rýchly prístup k dátam a plná kontrola nad fyzickým úložiskom. Takéto riešenie je vhodné najmä pre lokálne zálohy väčšieho objemu dát.

Nevýhodou je riziko fyzického poškodenia, odcudzenia alebo zasiahnutia rovnakou udalosťou ako primárne dáta, napríklad požiarom či prepätím. Ak sa zálohy uchovávajú v tom istom priestore a na tom istom type úložiska, ich ochranná hodnota sa znižuje.

17.2.7 Synchronizácia dát

Synchronizácia znamená udržiavanie rovnakého obsahu medzi viacerými zariadeniami alebo úložiskami. Hoci môže na prvý pohľad pripomínať zálohu, nejde o to isté. Synchronizované súbory sa priebežne aktualizujú, a preto sa chyba, vymazanie alebo zašifrovanie môže preniesť aj na ďalšie zariadenia.

Synchronizácia je užitočná na zabezpečenie dostupnosti a aktuálnosti dát, no sama osebe nepredstavuje plnohodnotnú zálohu, pokiaľ neobsahuje verziovanie a možnosť návratu k starším stavom.

17.2.8 Odporúčaná stratégia: pravidlo 3-2-1

Jednou z najznámejších a najúčinnejších zásad zálohovania je pravidlo 3-2-1. Toto pravidlo odporúča mať najmenej tri kópie dát: originál a dve zálohy. Tieto kópie by mali byť uložené na dvoch rôznych typoch médií a aspoň jedna z nich by mala byť uchovávaná mimo hlavného pracoviska alebo domácnosti.

Zmyslom tejto stratégie je znížiť pravdepodobnosť, že všetky kópie budú poškodené alebo zničené tou istou udalosťou. Ak sú všetky dáta aj zálohy uložené na jednom mieste, jedna havária môže spôsobiť úplnú stratu informácií. Geograficky oddelená kópia preto výrazne zvyšuje odolnosť.

V modernej praxi sa pravidlo 3-2-1 často dopĺňa aj o požiadavku, aby aspoň jedna kópia bola odpojená alebo nemenná, teda chránená pred zásahom ransomvéru alebo neoprávneným prepísaním.

17.3 Kvalita zálohovania a testovanie obnovy

Samotné vytvorenie zálohy ešte neznamená, že organizácia je pripravená na incident. Rovnako dôležité je overiť, či je záloha použiteľná a či z nej možno dáta skutočne obnoviť. V praxi sa totiž často ukáže, že zálohy sú neúplné, poškodené, zastarané alebo nevhodne uložené.

Preto je nevyhnutné zálohy pravidelne testovať. Test obnovy by mal preveriť nielen technickú funkčnosť záložných súborov, ale aj čas potrebný na obnovu a schopnosť organizácie vrátiť systém do prevádzky. Tento aspekt je dôležitý najmä v prostredí, kde je dostupnosť služieb časovo kritická.

Pri plánovaní zálohovania sa často používajú pojmy RPO a RTO. RPO vyjadruje, o aké množstvo dát si organizácia môže dovoliť prísť, teda aký starý môže byť posledný zálohovaný stav. RTO zas označuje maximálny čas, za ktorý musí byť služba alebo systém obnovený. Tieto ukazovatele pomáhajú nastaviť vhodnú frekvenciu záloh a zvoliť primerané technické riešenie.

17.4 Organizačné zásady zálohovania

Efektívne zálohovanie si vyžaduje nielen technické nástroje, ale aj jasne určené pravidlá. Organizácia by mala vedieť, ktoré dáta sa zálohujú, ako často, kde sú zálohy uložené, kto za ne zodpovedá a ako sa vykonáva obnova. Bez týchto pravidiel môže byť aj technicky kvalitný systém zálohovania v praxi neúčinný.

Osobitnú pozornosť treba venovať ochrane samotných záloh. Záloha často obsahuje rovnaké alebo ešte citlivejšie údaje ako produkčný systém, a preto musí byť primerane chránená. Znamená to používanie šifrovania, riadenia prístupu, fyzického zabezpečenia aj monitorovania prístupu k záložným úložiskám.

Je vhodné zdôrazniť, že zálohovanie nie je jednorazová činnosť, ale priebežný proces. Potreby organizácie sa menia, objem dát rastie a menia sa aj hrozby. Zálohovacia stratégia preto musí byť pravidelne vyhodnocovaná a aktualizovaná.

17.5 Praktické úlohy

Úloha 1: Strata USB kľúča
Zamestnanec stratil USB kľúč, na ktorom mal uložené osobné údaje klientov.
Otázky:

1. Aké riziká z tejto situácie vyplývajú?
2. Ako mohlo šifrovanie znížiť následky incidentu?
3. Aké pravidlá by mala mať organizácia pri používaní prenosných médií?

Úloha 2: Bezpečné vyradenie externého disku
Firma chce vyradiť starý externý disk, na ktorom boli dlhodobo uložené interné dokumenty.
Otázky:

1. Prečo nestačí disk iba bežne naformátovať?
2. Ktoré metódy bezpečného vymazania prichádzajú do úvahy?
3. Kedy je vhodné pristúpiť k fyzickému zničeniu média?

Úloha 3: Návrh zálohovacej stratégie
Navrhni jednoduchú zálohovaciu stratégiu pre malú firmu s desiatimi zamestnancami.
Otázky:

1. Aké dáta by mali byť zálohované prioritne?
2. Ktoré metódy zálohovania by bolo vhodné kombinovať?
3. Ako by sa dalo uplatniť pravidlo 3-2-1 v praxi?
4. Ako často by bolo vhodné testovať obnovu dát?

17.6 Test

1. Čo je hlavným cieľom zálohovania dát?
a) Zvýšiť rýchlosť internetu
b) Vytvoriť kópie údajov pre ich obnovu po incidente
c) Nahradiť antivírusový program
d) Znížiť počet súborov v systéme

2. Ktoré tvrdenie o inkrementálnej zálohe je správne?
a) Ukladá vždy všetky dáta
b) Ukladá len zmeny od poslednej vykonanej zálohy
c) Je to presná kópia dát v reálnom čase
d) Nepotrebuje úplnú zálohu na obnovu

3. Prečo synchronizácia dát sama osebe nie je plnohodnotnou zálohou?
a) Pretože nefunguje cez internet
b) Pretože nezaberá žiadne miesto
c) Pretože chyba alebo vymazanie sa môže preniesť aj na ďalšie zariadenia
d) Pretože sa používa len vo veľkých firmách

4. Čo odporúča pravidlo 3-2-1 pri zálohovaní?
a) Mať tri heslá k jednému účtu
b) Mať tri kópie dát, na dvoch rôznych médiách, pričom jedna je mimo hlavného miesta
c) Zálohovať len raz za mesiac
d) Uchovávať všetky zálohy na jednom serveri

5. Prečo je dôležité testovanie obnovy zo záloh?
a) Aby sa znížila kapacita úložiska
b) Aby sa overilo, či sú zálohy skutočne použiteľné
c) Aby sa odstránili pôvodné dáta
d) Aby nebolo potrebné šifrovanie záloh

18Základy fyzickej bezpečnosti

Fyzická bezpečnosť predstavuje neoddeliteľnú súčasť celkového systému ochrany informácií, technológií a majetku organizácie. V prostredí kybernetickej bezpečnosti sa často kladie dôraz najmä na softvérové zraniteľnosti, sieťové útoky alebo ochranu dát v digitálnej forme, no rovnako dôležitá je aj ochrana fyzických priestorov, zariadení a technickej infraštruktúry. Ak útočník získa fyzický prístup k zariadeniam, serverom, pracovným staniciam alebo dokumentom, môže obísť mnohé logické a technické ochranné opatrenia.

Fyzická bezpečnosť zahŕňa súbor organizačných, technických a režimových opatrení, ktorých cieľom je zabrániť neoprávnenému vstupu do chránených priestorov, poškodeniu zariadení, odcudzeniu majetku a zneužitiu informačných aktív. V praxi sa týka nielen serverovní a dátových centier, ale aj kancelárií, archívov, skladov, vstupných priestorov, recepcií a pracovných stanovíšť zamestnancov.

Z pedagogického hľadiska je potrebné zdôrazniť, že fyzická bezpečnosť nie je oddelená od kybernetickej bezpečnosti, ale ju dopĺňa. Odcudzený notebook, ponechaný odomknutý počítač, voľne prístupná serverovňa alebo stratená prístupová karta môžu mať rovnaké následky ako úspešný kybernetický útok. Bez primeraného fyzického zabezpečenia teda nemožno hovoriť o skutočne účinnej ochrane informačných systémov.

18.1 Význam fyzickej bezpečnosti

Úlohou fyzickej bezpečnosti je chrániť osoby, priestory, technológie a informácie pred hrozbami, ktoré majú materiálny alebo priestorový charakter. Môže ísť o neoprávnený vstup, krádež zariadenia, vandalizmus, sabotáže, manipuláciu so zariadeniami, poškodenie techniky alebo neoprávnené získanie dokumentov a nosičov dát.

V informačnej bezpečnosti má fyzická ochrana veľký význam najmä preto, že mnoho digitálnych prostriedkov je stále viazaných na konkrétne fyzické zariadenia. Server, router, záložné úložisko, pracovná stanica či prenosné médium sú hmotné objekty, ktoré možno odcudziť, poškodiť alebo zneužiť. Fyzický útok môže preto viesť k strate dostupnosti služieb, úniku citlivých údajov aj k narušeniu dôvernosti a integrity informácií.

Význam fyzickej bezpečnosti rastie aj v súvislosti s ochranou kritickej infraštruktúry, inteligentných budov, priemyselných riadiacich systémov a zariadení internetu vecí. Ak je útočník schopný získať fyzický prístup k technologickému prostrediu, môže spôsobiť nielen informačný, ale aj prevádzkový alebo bezpečnostný incident s dosahom na reálny chod organizácie.

18.2 Kontrola prístupu do priestorov

Jedným zo základných pilierov fyzickej bezpečnosti je kontrola prístupu. Jej cieľom je zabezpečiť, aby do chránených priestorov vstupovali iba oprávnené osoby a len v rozsahu potrebnom na výkon ich činností. Kontrola prístupu sa môže realizovať mechanickými aj elektronickými prostriedkami.

V tradičnom prostredí sa používajú kľúče a mechanické zámky. Hoci ide o jednoduché a osvedčené riešenie, jeho nevýhodou je náročnejšia evidencia a kontrola. V modernejších systémoch sa využívajú elektronické prístupové karty, čipy, PIN kódy alebo biometrické prvky, napríklad odtlačky prstov či rozpoznávanie tváre. Výhodou elektronických systémov je možnosť presne definovať oprávnenia, časovo obmedziť vstup a viesť evidenciu pohybu osôb.

Pri nastavovaní prístupových oprávnení je dôležité uplatňovať princíp minimálnej nevyhnutnosti. Nie každý zamestnanec potrebuje mať prístup do všetkých priestorov. Napríklad vstup do serverovne, archívu alebo miestnosti s bezpečnostnou technikou by mal byť obmedzený len na úzky okruh osôb. Takéto opatrenie znižuje riziko náhodného aj úmyselného narušenia bezpečnosti.

Zvláštnu pozornosť treba venovať návštevám, externým dodávateľom a servisným pracovníkom. Tieto osoby by sa nemali pohybovať v chránených priestoroch bez sprievodu alebo evidencie. Organizácia by mala mať stanovené pravidlá registrácie návštev, vydávania dočasných vstupných oprávnení a kontroly ich pohybu v objekte.

18.3 Mechanické a technické bariéry

Fyzickú bezpečnosť významne podporujú mechanické a technické bariéry, ktorých úlohou je sťažiť neoprávnený vstup alebo predĺžiť čas potrebný na prekonanie ochrany. Patria sem bezpečnostné dvere, spevnené zárubne, uzamykateľné skrine, mreže, bezpečnostné fólie na oknách alebo ochranné skrine pre technické zariadenia.

Tieto opatrenia majú veľký význam najmä v priestoroch, kde sa nachádzajú servery, sieťové prvky, záložné zdroje, záznamové zariadenia, dokumentácia alebo nosiče dát. Mechanické bariéry často nepôsobia len ako ochrana pred vniknutím, ale aj ako preventívny psychologický faktor. Potenciálny narušiteľ môže od útoku upustiť, ak zistí, že prekonanie ochrany bude časovo alebo technicky náročné.

Pri návrhu takýchto opatrení treba myslieť aj na prevádzkovú stránku. Bezpečnostné prvky nesmú neprimerane komplikovať prácu oprávneným osobám, no zároveň musia poskytovať dostatočnú úroveň ochrany. Vhodné riešenie preto vychádza z posúdenia rizík a významu chráneného priestoru.

18.4 Kamerové systémy a monitorovanie

Významným nástrojom fyzickej bezpečnosti sú kamerové systémy. Umožňujú monitorovať vybrané priestory, zaznamenávať pohyb osôb a spätne analyzovať incidenty. Kamerový systém môže pôsobiť preventívne, pretože samotná prítomnosť kamerového dohľadu často znižuje pravdepodobnosť nežiadúceho správania.

Kamery sa zvyčajne umiestňujú na vstupoch do budovy, na chodbách, v priestoroch recepcie, pri serverovniach, na parkoviskách alebo v okolí objektu. Ich využitie však musí byť primerané a v súlade s právnymi predpismi, najmä s pravidlami ochrany osobných údajov. Monitorovanie nemôže byť svojvoľné a organizácia musí mať jasne určený účel, rozsah a spôsob spracúvania záznamov.

Z bezpečnostného hľadiska je dôležité nielen samotné snímanie priestoru, ale aj ochrana záznamov. Ak by útočník získal prístup k záznamovému zariadeniu alebo mohol záznamy vymazať, účinnosť systému by sa výrazne znížila. Záznamové zariadenia preto musia byť fyzicky aj logicky zabezpečené.

18.5 Alarmové systémy a detekcia narušenia

Alarmové systémy dopĺňajú kontrolu prístupu a monitorovanie tým, že upozorňujú na neoprávnený vstup, pokus o vniknutie alebo iné neštandardné situácie. Môžu byť založené na pohybových snímačoch, magnetických kontaktoch na dverách a oknách, detektoroch rozbitia skla alebo ďalších prvkoch.

Ich význam spočíva najmä v rýchlej reakcii. Ak dôjde k narušeniu priestoru mimo pracovného času alebo v neobsadenej časti budovy, alarmový systém môže automaticky spustiť poplach, odoslať oznámenie zodpovedným osobám alebo kontaktovať bezpečnostnú službu. Tým sa skracuje čas medzi incidentom a zásahom.

Alarmové systémy sú obzvlášť dôležité v priestoroch s technickou infraštruktúrou, archívmi, cenným majetkom alebo citlivými dokumentmi. Ich účinnosť však závisí od správneho nastavenia, údržby a pravidelného testovania. Zanedbaný alebo chybne nakonfigurovaný systém môže spôsobovať falošné poplachy alebo naopak zlyhať v kritickej situácii.

18.6 Osvetlenie a bezpečnosť okolia objektu

Dôležitou súčasťou fyzickej bezpečnosti je aj ochrana bezprostredného okolia budovy. Dostatočné osvetlenie vstupných priestorov, prístupových ciest, parkovísk, nakladacích zón a technických dvorov zvyšuje prehľadnosť prostredia a sťažuje neoprávnený pohyb osôb v blízkosti objektu.

Zanedbané alebo tmavé priestory vytvárajú vhodné podmienky na skryté pozorovanie objektu, neoprávnené manipulácie či prípravu na vniknutie. Osvetlenie preto plní nielen praktickú, ale aj preventívnu funkciu. V kombinácii s kamerovým systémom zvyšuje pravdepodobnosť včasného odhalenia podozrivej činnosti.

Fyzická bezpečnosť okolia zahŕňa aj úpravu areálu, oplotenie, kontrolu vedľajších vstupov, zabezpečenie technických šácht, pivničných a strešných priestorov a elimináciu miest, kde by sa mohli neoprávnene zdržiavať osoby bez povšimnutia.

18.7 Správa kľúčov a prístupových kariet

Kľúče, prístupové karty a iné autentifikačné prostriedky predstavujú samostatnú bezpečnostnú oblasť. Ak sa s nimi nakladá nedôsledne, môžu sa stať slabým miestom celého systému. Organizácia by preto mala viesť presnú evidenciu o tom, komu bol vydaný kľúč alebo karta, do akých priestorov umožňuje vstup a kedy bol vrátený.

Pri strate kľúča alebo karty je nevyhnutné okamžite reagovať. V prípade elektronických systémov treba prístup bezodkladne zablokovať. Pri mechanických kľúčoch môže byť v závažných prípadoch potrebná výmena vložky alebo prekonfigurovanie systému uzamknutia. Osobitne dôležité je zabezpečiť, aby boli všetky prístupové prostriedky vrátené pri skončení pracovného pomeru alebo pri zmene pracovného zaradenia.

Z pedagogického hľadiska je vhodné študentom vysvetliť, že prístupová karta alebo kľúč je rovnako citlivý prostriedok ako heslo do informačného systému. Nemožno ho požičiavať, nechávať bez dozoru ani uchovávať nedbalým spôsobom.

18.8 Bezpečnostné školenia a bezpečnostná kultúra

Technické opatrenia samy osebe nestačia, ak ich používatelia nerešpektujú. Aj vo fyzickej bezpečnosti zohráva zásadnú úlohu bezpečnostné povedomie zamestnancov. Pravidelné školenia by mali zamestnancov oboznámiť so zásadami vstupu do chránených priestorov, pravidlami pre návštevy, používaním prístupových kariet, uzamykaním kancelárií, ochranou dokumentov a postupmi pri bezpečnostnom incidente.

Bezpečnostná kultúra sa prejavuje v každodenných návykoch. Patrí sem napríklad zatváranie dverí, nenechávanie cudzích osôb vstupovať „na kartu niekoho iného“, neukladanie citlivých dokumentov na voľne prístupné miesta, zamykanie skriniek a stolov či oznamovanie podozrivého pohybu v objekte.

Práve ľudská nedôslednosť býva častou príčinou fyzických incidentov. Organizácia preto musí vytvárať prostredie, v ktorom zamestnanci vnímajú bezpečnostné pravidlá ako prirodzenú súčasť pracovného procesu, nie ako zbytočnú administratívnu záťaž.

18.9 Monitorovanie, kontrola a audit fyzických opatrení

Tak ako v oblasti informačnej bezpečnosti, aj pri fyzickej ochrane je potrebné pravidelne preverovať účinnosť prijatých opatrení. Organizácia by mala vykonávať kontroly funkčnosti prístupových systémov, alarmov, kamerových systémov, zámkov a ďalších bezpečnostných prvkov. Súčasťou tejto činnosti sú aj interné audity, prehliadky objektov a preverovanie dodržiavania stanovených postupov.

Audit fyzickej bezpečnosti môže odhaliť slabé miesta, ktoré si organizácia v bežnej prevádzke neuvedomuje. Môže ísť o neuzamknuté priestory, nefunkčné kamery, zdieľané prístupové karty, nedostatočne chránené dokumenty alebo nedôslednú evidenciu návštev. Pravidelné preverovanie preto zvyšuje odolnosť organizácie a umožňuje včas prijať nápravné opatrenia.

18.10Test

1. Prečo je fyzická bezpečnosť dôležitá aj v kontexte kybernetickej bezpečnosti?
a) Pretože nahrádza antivírus
b) Pretože fyzický prístup môže obísť logické a technické ochranné opatrenia

c) Pretože sa týka len recepcie
d) Pretože slúži iba na ochranu majetku bez súvisu s IT

2. Čo je cieľom kontroly prístupu do priestorov?
a) Umožniť vstup každému zamestnancovi všade
b) Zabrániť evidencii pohybu osôb
c) Zabezpečiť, aby do chránených priestorov vstupovali len oprávnené osoby
d) Nahradiť kamerový systém

3. Aký význam majú kamerové systémy?
a) Len estetickú funkciu
b) Umožňujú monitorovať priestory a spätne analyzovať incidenty
c) Nahrádzajú všetky ostatné bezpečnostné opatrenia
d) Slúžia len na meranie osvetlenia

4. Čo je dôležité pri správe kľúčov a prístupových kariet?
a) Požičiavať ich kolegom podľa potreby
b) Neevidovať ich, aby bola správa jednoduchšia
c) Viesť presnú evidenciu a pri strate okamžite reagovať
d) Uchovávať ich voľne na stole

5. Čo patrí medzi prejavy bezpečnostnej kultúry vo fyzickej bezpečnosti?
a) Nechať dvere otvorené pre pohodlie
b) Púšťať cudzie osoby do objektu bez kontroly
c) Zamykať kancelárie a oznamovať podozrivý pohyb
d) Zdieľať prístupové karty medzi zamestnancami

19 Smery kybernetickej bezpečnosti v budúcnosti

Kybernetická bezpečnosť patrí medzi najdynamickejšie sa rozvíjajúce oblasti súčasnej spoločnosti. Rozvoj digitálnych technológií, rastúca miera prepojenia systémov, automatizácia procesov a masové využívanie dát zásadne menia charakter bezpečnostných hrozieb aj spôsob ochrany pred nimi. Budúcnosť kybernetickej bezpečnosti preto nemožno chápať len ako pokračovanie súčasných prístupov, ale ako oblasť, v ktorej sa budú meniť technológie, metódy obrany aj samotné chápanie rizika.

Vývoj v tejto oblasti je ovplyvnený viacerými faktormi. Na jednej strane ide o technologický pokrok, ako je umelá inteligencia, internet vecí, cloud computing alebo kvantové počítanie. Na druhej strane ide o meniace sa správanie útočníkov, ktorí stále častejšie využívajú automatizáciu, personalizované kampane, sociálne inžinierstvo a sofistikované techniky obchádzania ochrany. Organizácie preto musia prechádzať od prevažne reaktívnej ochrany k inteligentnejšiemu, prediktívnemu a adaptívnemu modelu bezpečnosti.

Je dôležité vnímať budúce smerovanie kybernetickej bezpečnosti nielen ako technickú otázku, ale aj ako problém strategického riadenia, legislatívy, etiky a vzdelávania. Budúca bezpečnosť nebude závisieť len od technických nástrojov, ale aj od pripravenosti ľudí, procesov a organizácií reagovať na meniace sa prostredie.

19.1 Umelá inteligencia a strojové učenie

Umelá inteligencia a strojové učenie sa stávajú jedným z najvýznamnejších nástrojov modernej kybernetickej bezpečnosti. Ich význam spočíva v schopnosti analyzovať veľké množstvo údajov v reálnom čase, vyhľadávať anomálie a identifikovať vzorce správania, ktoré by pri tradičných metódach zostali nepovšimnuté.

V oblasti obrany možno umelú inteligenciu využiť pri detekcii útokov, triedení bezpečnostných udalostí, analýze logov, automatizácii reakcií na incidenty a vyhodnocovaní rizika. Bezpečnostné tímy tak môžu pracovať efektívnejšie a sústrediť sa na zložitejšie prípady, kým rutinné úlohy spracúva automatizovaný systém.

Strojové učenie môže byť užitočné aj pri predikcii hrozieb. Na základe historických údajov a priebežného učenia vie systém lepšie odhadovať, ktoré typy správania môžu naznačovať blížiaci sa incident. Významné je to najmä pri odhaľovaní anomálií v sieťovej prevádzke, podozrivých prístupov do systémov či neobvyklého správania používateľov.

Zároveň však platí, že umelá inteligencia môže byť zneužitá aj útočníkmi. Môže slúžiť na automatizované generovanie phishingových správ, vytváranie presvedčivých podvodných správ, adaptívne škodlivé kódy alebo deepfake obsah. Budúcnosť kybernetickej bezpečnosti preto nebude spočívať len v používaní AI na obranu, ale aj v obrane proti útokom podporovaným AI.

19.2 Internet vecí

Internet vecí označuje prepojenie rôznych fyzických zariadení do siete, v ktorej medzi sebou komunikujú, zbierajú údaje a reagujú na podnety. Do tejto kategórie patria priemyselné snímače, inteligentné kamery, domáce spotrebiče, zdravotnícke zariadenia, vozidlá, meracie systémy aj prvky inteligentných budov.

Rast počtu IoT zariadení prináša nové možnosti, ale zároveň vytvára veľké množstvo nových vstupných bodov pre útočníkov. Mnohé z týchto zariadení majú obmedzený výpočtový výkon, slabé bezpečnostné mechanizmy, predvolené heslá alebo nedostatočnú podporu aktualizácií. To z nich robí zraniteľný prvok celej infraštruktúry.

Budúcnosť kybernetickej bezpečnosti bude preto výrazne ovplyvnená schopnosťou chrániť IoT prostredie. Kľúčové bude meniť predvolené nastavenia zariadení, zabezpečovať pravidelné aktualizácie, používať šifrovanie, segmentovať siete a monitorovať komunikáciu zariadení. V priemyselnom a kritickom prostredí bude ochrana IoT obzvlášť významná, pretože útok na jedno zariadenie môže mať dosah na celý technologický proces.

19.3 Kvantové počítanie

Kvantové počítanie predstavuje technologický smer, ktorý môže v budúcnosti zásadne zmeniť oblasť kryptografie a bezpečnosti. Na rozdiel od klasických počítačov, ktoré pracujú s bitmi nadobúdajúcimi hodnoty 0 alebo 1, kvantové počítače využívajú qubity, ktoré môžu existovať vo viacerých stavoch súčasne. Táto vlastnosť, označovaná ako superpozícia, spolu s ďalšími javmi, napríklad kvantovým previazanim, umožňuje vykonávať určité typy výpočtov výrazne rýchlejšie než pri tradičných technológiách.

Z pohľadu kybernetickej bezpečnosti je význam kvantového počítania spojený najmä s možnosťou prelomiť niektoré dnes používané kryptografické algoritmy. V budúcnosti by mohli byť ohrozené najmä asymetrické šifrovacie mechanizmy, na ktorých sú založené mnohé dnešné bezpečnostné riešenia, napríklad digitálne podpisy, certifikáty a bezpečná výmena kľúčov.

Preto sa už v súčasnosti rozvíja oblasť postkvantovej kryptografie, ktorej cieľom je vytvoriť také algoritmy, ktoré budú odolné aj voči útokom kvantových počítačov. Budúcnosť bezpečnosti preto nebude spočívať len v reakcii na existujúce hrozby, ale aj v príprave na technologické zmeny, ktoré ešte len prídu.

19.4 Model nulovej dôvery

Model zabezpečenia s nulovou dôverou, označovaný ako Zero Trust, predstavuje významný posun v chápaní bezpečnosti informačných systémov. Tradičné prístupy vychádzali z predstavy, že všetko vo vnútri firemnej siete je relatívne dôveryhodné a riziko prichádza najmä zvonku. V súčasnosti však takýto model prestáva postačovať.

Práca na diaľku, používanie cloudových služieb, mobilných zariadení a hybridných infraštruktúr spôsobujú, že pevne definovaný bezpečnostný perimeter sa oslabuje. Zero Trust

preto vychádza z princípu, že žiadny používateľ, zariadenie ani služba nesmú byť automaticky považované za dôveryhodné. Každý prístup musí byť priebežne overovaný, vyhodnocovaný a povoľovaný len v nevyhnutnom rozsahu.

Význam tohto modelu spočíva v obmedzení laterálneho pohybu útočníka, v dôslednejšom riadení prístupových práv a v lepšej ochrane pred internými aj externými hrozbami. V budúcnosti bude Zero Trust pravdepodobne jedným z kľúčových princípov moderného bezpečnostného dizajnu.

19.5 Cloudová bezpečnosť

Cloudové služby sa stali bežnou súčasťou digitálneho prostredia. Organizácie ukladajú do cloudu dáta, prevádzkujú aplikácie, využívajú cloudové identity a presúvajú doň stále väčšiu časť svojich procesov. S tým rastie aj význam cloudovej bezpečnosti.

Bezpečnosť v cloude zahŕňa ochranu dát, správnu konfiguráciu služieb, riadenie prístupov, monitorovanie aktivít, šifrovanie a dodržiavanie regulačných požiadaviek. Jedným z častých problémov nie je slabosť samotného cloudového prostredia, ale nesprávne nastavenie zo strany používateľa alebo organizácie. Chybne nastavené úložisko, príliš široké prístupové práva alebo neexistujúci dohľad nad účtami môžu viesť k vážnym incidentom.

Budúcnosť cloudovej bezpečnosti bude úzko súvisieť s modelom zdieľanej zodpovednosti. Poskytovateľ cloudovej služby zabezpečuje určitú časť infraštruktúry, no organizácia zodpovedá za správne nastavenie svojich služieb, ochranu účtov, správu identít a bezpečné používanie dát. Práve pochopenie tejto delen ej zodpovednosti bude pre budúcnosť kľúčové.

19.6 Behaviorálna biometria

Behaviorálna biometria predstavuje moderný spôsob overovania identity a detekcie podozrivého správania na základe charakteristických vzorcov správania používateľa. Nepracuje iba s tým, čo používateľ vie alebo vlastní, ale aj s tým, ako sa správa. Môže ísť napríklad o spôsob písania na klávesnici, pohyb myši, rytmus práce s dotykovou obrazovkou alebo spôsob držania zariadenia.

Výhodou behaviorálnej biometrie je, že umožňuje priebežné a relatívne nenápadné overovanie identity. Ak sa správanie používateľa výrazne odlišuje od bežného profilu, systém môže vyhodnotiť situáciu ako rizikovú a vyžiadať si ďalšie overenie. Takýto prístup môže pomôcť pri odhaľovaní krádeže účtu, neoprávneného používania zariadenia alebo podvodného konania.

Budúcnosť tejto technológie súvisí s rastúcou potrebou kontinuálnej autentifikácie. Nestačí overiť používateľa len pri prihlásení. V dynamickom digitálnom prostredí bude čoraz dôležitejšie overovať aj to, či používateľ počas práce zostáva tou osobou, za ktorú sa vydáva.

19.7 Prediktívna bezpečnosť

Prediktívna bezpečnosť predstavuje prístup, ktorého cieľom je predvídať a zmierňovať hrozby ešte predtým, ako dôjde k samotnému útoku alebo incidentu. Vychádza z analýzy historických údajov, správania systémov, trendov v útokoch a identifikácie znakov, ktoré môžu naznačovať budúce riziko.

Tento prístup sa opiera o pokročilú analytiku, umelú inteligenciu, strojové učenie a koreláciu veľkého množstva dát z rôznych zdrojov. Prediktívna bezpečnosť sa snaží presunúť organizáciu z reaktívnej pozície do stavu, v ktorom dokáže prijať preventívne opatrenia skôr, ako nastane škoda.

Jej prínos spočíva v rýchlejšej reakcii, znížení nákladov na incidenty a lepšom zameraní obranných kapacít. Zároveň však treba počítať s tým, že predikcia nikdy nie je absolútna. Ide o pravdepodobnostný prístup, ktorý musí byť kombinovaný s ľudským odborným úsudkom, kvalitnými procesmi a priebežným overovaním výstupov.

19.8 Budúce výzvy a širší kontext

Budúcnosť kybernetickej bezpečnosti nebude ovplyvnená len samotnými technológiami, ale aj právnym, spoločenským a etickým rámcom. Rast využívania umelej inteligencie vyvoláva otázky zodpovednosti za rozhodnutia automatizovaných systémov. Rozvoj biometrických a behaviorálnych metód zase otvára diskusiu o ochrane súkromia a proporcionalite zásahov do práv jednotlivca.

Významnú úlohu bude zohrávať aj nedostatok odborníkov, potreba bezpečnostného vzdelávania a nutnosť medzinárodnej spolupráce. Kybernetické hrozby sú globálne a často prekračujú hranice štátov, sektorov aj technických platforiem. Budúca bezpečnosť preto bude závisieť nielen od technologickej vyspelosti, ale aj od úrovne spolupráce medzi štátom, súkromným sektorom, akademickou obcou a používateľmi.