
RIADENIE PRÍSTUPOVÝCH PRÁV ZÁKLADY

Autori: Ing. Ján Drahoš
doc. Ing. Dagmar Vidriková, PhD.
Prezentuje: Ing. Roderik Ploszek, PhD.

27.2.2026



PLÁN [OBNOVY]



OBSAH

- **Základné bezpečnostné princípy**
- **Ako systémy riadia prístup**
- **Ste prvou líniou obrany – vaše povinnosti a osvedčené postupy**
- **Poučenie z krízového vývoja**
- **Zhrnutie – Bezpečnosť je naša spoločná zodpovednosť**

ÚVOD - PREČO JE TO DÔLEŽITÉ?

Informácie sú najcennejšou komoditou

- V dnešnom digitálnom svete je ochrana informácií kľúčovou prioritou pre každú organizáciu.
- **Riadenie prístupových práv** je základný pilier informačnej a kybernetickej bezpečnosti.
- Nejde o byrokratickú záťaž, ale o systém, ktorý chráni:
 - Citlivé údaje firmy.
 - Vašu prácu a digitálnu identitu.

ANALÓGIA S FYZICKÝM SVETOM

Kľúče, zámky a bezpečnostné zóny

- Predstavte si firemné dáta ako budovu s mnohými miestnosťami.
- **Hlavný vchod (Základný prístup):** Každý zamestnanec má kľúč na vstup do spoločných priestorov.
- **Serverovňa (Privilegovaný prístup):** Kľúč majú len IT administrátori.
- **Trezor (Prísne tajný prístup):** Prístup má len pár ľudí z finančného oddelenia.

Kľúč nám dáva *prístupové právo vstúpiť do miestnosti*. Každý má prístup len tam, kam naozaj potrebuje.

Riadenie prístupových práv je systém, ktorý určuje, kto, kedy, odkiaľ a k akým informáciám či systémom môže pristupovať.

Fyzická analógia toho, čo nám dáva právo pristúpiť ku zdroju je **klúč**.

ČO JE RIADENIE PRÍSTUPU?

- **Riadenie prístupu (Access Control)** je bezpečnostný proces, ktorý definuje a vynucuje pravidlá o tom:

- **Kto** (zamestnanec, aplikácia) *subjekt*
- Môže pristupovať k **čomu** (súbor, databáza, systém) *objekt*
- A aké **operácie** môže vykonávať (čítať, zapisovať, mazať). *operácia*

Cieľom je zamedziť prístup neoprávneným osobám a povoliť ho len tým oprávneným za presne stanovených podmienok.

INFORMAČNÁ VS. KYBERNETICKÁ BEZPEČNOSŤ

Dva prepojené svety

- **Informačná bezpečnosť:** Širší pojem, ktorý chráni **všetky** typy informácií (digitálne aj fyzické) s cieľom zaistiť ich dôvernosť, integritu a dostupnosť.
- **Kybernetická bezpečnosť:** Podkategória informačnej bezpečnosti, ktorá sa sústreďuje **výhradne na ochranu počítačových systémov, sietí a dát** v online prostredí.
- Riadenie prístupu je kritickým nástrojom pre obe tieto disciplíny.

Riadenie prístupu je dôležitým nástrojom pre obe tieto disciplíny, pretože určuje a kontroluje prístup k chráneným aktívam.

KLÚČOVÉ POJMY: AUTENTIFIKÁCIA VS. AUTORIZÁCIA

Dva kroky k prístupu

1. Autentifikácia (Overenie identity):

- Proces, ktorým systém overuje, že ste to naozaj vy.
- Odpovedá na otázku: "**Kto ste?**"
- Je to ako ukázať preukaz totožnosti.

2. Autorizácia (Pridelenie oprávnení):

- Nasleduje po úspešnej autentifikácii.
 - Systém podľa bezpečnostnej politiky rozhodne, čo smiete robiť.
 - Odpovedá na otázku: "**Čo smiete robiť?**"
-

7

Na základe vašej identity (a priradenej roly či politiky) vám systém udelí konkrétne prístupové povolenia.

Je to ako keď vrátnik po overení preukazu odovzdá kľúč od šatne, ale nie od kancelárie riaditeľa.

METÓDY AUTENTIFIKÁCIE

Ako dokazujete svoju identitu?

Systémy používajú rôzne metódy na overenie vašej identity:

- **Niečo, čo viete:**
 - Heslo, PIN kód.
- **Niečo, čo máte:**
 - Bezpečnostný token, mobilný telefón, zamestnanecká karta.
- **Niečo, čo ste:**
 - Biometrické údaje (odtlačok prsta, sken tváre).

Najsilnejšou formou je **Viacfaktorová autentifikácia (MFA)**, ktorá kombinuje aspoň dve z týchto metód.

PREČO NA TOM ZÁLEŽÍ? (POHĽAD ORGANIZÁCIE)

Ochrana životne dôležitých aktív

- **Základná obranná línia:** Chráni zákaznicke dáta, finančné záznamy a duševné vlastníctvo.
- **Minimalizácia rizika:** Obmedzuje škody spôsobené externým útokom alebo interným zamestnancom.
- **Prevenia strát:** Predchádza obrovským finančným stratám a poškodeniu reputácie.
- **Súlad s legislatívou:** Pomáha plniť požiadavky ako GDPR alebo normy ISO/IEC 27001.

PREČO NA TOM ZÁLEŽÍ? (POHLÁD ZAMESTNANCA)

Nielen obmedzenie, ale aj ochrana

- **Zjednodušenie práce:** Zabezpečuje, že máte prístup ku všetkým systémom, ktoré potrebujete pre svoju prácu.
- **Ochrana pred chybami:** Znižuje riziko, že neúmyselne spôsobíte škodu (napr. vymazaním dôležitého súboru).
- **Osobná ochrana:** V prípade bezpečnostného incidentu vás správne nastavené práva chránia, pretože jasne definujú rozsah vašich oprávnení a zodpovednosti.

Keď zamestnanec vidí len tie systémy a súbory, ktoré sú pre neho relevantné, znižuje sa kognitívna záťaž a riziko náhodnej chyby.

ZÁKLADNÉ BEZPEČNOSTNÉ PRINCÍPY

Piliere efektívneho riadenia prístupu

- Princíp najmenších oprávnení (Principle of Least Privilege – PoLP)
- Vyvarovať sa „Privilege Creep“ (Nahromadenie oprávnení)
- Princíp oddelenia povinností (Separation of Duties – SoD)

Tieto princípy tvoria základ robustnej bezpečnostnej stratégie.

PRINCÍP NAJMENŠÍCH OPRAVNĚNÍ (POLP)

Zlaté pravidlo: „Ak to nepotrebuješ, nedostaneš to.“

- **Definícia:** Každý používateľ, program alebo proces by mal mať iba **minimálne oprávnenia nevyhnutné** na vykonanie svojich úloh. Nič viac, nič menej.
- **Prečo je to dôležité?**
 - **Minimalizácia rizika:** Ak útočník získa prístup k vášmu účtu, škody budú obmedzené len na tie systémy, ku ktorým máte prístup vy.
 - **Ochrana pred ľudskou chybou:** Znižuje pravdepodobnosť neúmyselného vymazania dát alebo zmeny konfigurácie.

12

Predstavte si upratovačku vo firemnej budove. Na to, aby mohla upratať kanceláriu, nepotrebuje kľúč od trezoru s finančnými dátami. Potrebuje len prístup do konkrétnych kancelárskych priestorov, a to len počas svojej pracovnej zmeny (miesto, čas). Prístup navyše je zbytočný a predstavuje riziko. V digitálnom svete to znamená, že marketingový špecialista nepotrebuje prístup do vývojárskeho prostredia a programátor nepotrebuje prístup k mzdovým údajom zamestnancov. Dôležitosť tohto princípu spočíva v znížení tzv. "blast radius" (dosah výbuchu) – teda rozsahu potenciálnych škôd v prípade bezpečnostného incidentu. Ak útočník získa prihlasovacie údaje zamestnanca, ktorý má len minimálne oprávnenia, jeho schopnosť spôsobiť škodu je výrazne obmedzená. Naopak, ak kompromituje účet s nadmernými, administrátorskými právami, následky môžu byť katastrofálne.

TICHÁ HROZBA: „PRIVILEGE CREEP“

Postupné hromadenie nepotrebných práv

- **Definícia:** Postupné a často nepovšimnuté hromadenie prístupových práv nad rámec toho, čo zamestnanec reálne potrebuje.
- **Ako vzniká?**
 - **Zmena pracovnej pozície:** Zamestnanec získa nové prístupy, ale staré mu nikto neodoberie.
 - **Dočasné projekty:** Dočasný prístup sa po skončení projektu neodoberie.
 - **Zastupovanie kolegu:** Dočasné práva sa stanú trvalými.
- Každé nepotrebné oprávnenie je otvorenou bezpečnostnou dierou.

RIEŠENIE PRE „PRIVILEGE CREEP“

Pravidelná revízia prístupových práv

- „**Privilege Creep**“ je prirodzeným nepriateľom princípu najmenších oprávnení.
- Tento stav opätovne otvára bezpečnostné medzery a robí organizáciu zraniteľnou.
- **Riešenie:**
 - Zavedenie prísnych procesov pri akejkoľvek zmene roly.
 - **Pravidelná revízia prístupových práv (access rights review)**, počas ktorej manažéri overujú, či sú existujúce prístupy stále oprávnené a potrebné.

PRINCÍP ODDELENIA POVINNOSTÍ (SOD)

Systém vzájomnej kontroly a rovnováhy

- **Definícia:** Žiadna kritická alebo citlivá úloha by nemala byť plne v rukách jedinej osoby. Proces musí byť rozdelený medzi viacero ľudí.
- **Príklad (Úhrada faktúry):**
 1. **Iniciácia:** Jeden zamestnanec zaeviduje faktúru.
 2. **Autorizácia:** Nadriadený ju schváli.
 3. **Vykonanie:** Iný zamestnanec vykoná platbu.
- Tento princíp znemožňuje, aby jednotlivec mohol vykonať a zároveň zakryť podvodnú transakciu.

V IT svete to môže znamenať, že programátor, ktorý napíše kód, ho nemôže sám nasadiť do produkčného prostredia bez kontroly a schválenia inou osobou.

ARCHITEKTÚRA DÔVERY: MODEL Y RIADENIA PRÍSTUPU

Ako systémy rozhodujú o prístupe?

Existuje niekoľko základných modelov, ktoré definujú logiku udeľovania prístupu:

- **Discretionary Access Control (DAC):** Vlastník zdroja sám udeľuje práva (napr. práva na súbor vo Windows).
- **Mandatory Access Control (MAC):** Prístup riadi centrálny systém na základe bezpečnostných značiek (napr. „Prísne tajné“). Pochádza z prostredia armády, dnes sa používa v OS Android.
- **Role-Based Access Control (RBAC):** Najrozšírenejší model v podnikoch. Práva sú viazané na roly.
- **Attribute-Based Access Control (ABAC):** Najmodernejší model. Rozhoduje v reálnom čase na základe atribútov (používateľ, zdroj, prostredie).

MODEL RBAC – DIGITÁLNY „KABÁT“

Riadenie prístupu na základe rolí

- Prístupové práva sa neprideľujú priamo používateľom, ale sú viazané na definované **roly** (napr. „účtovník“, „manažér“, „predajca“).
- Používatelia získavajú práva na základe rolí, ktoré im boli pridelené.
- **Výhody:** Prehľadnosť, škálovateľnosť, zjednodušené audity. Pri zmene pozície stačí zmeniť rolu.
- **Nevýhody:**
 - Relatívna neflexibilita.
 - Riziko "**explózie rolí**" (**role explosion**), kedy sa spravujú stovky rolí a stráca sa prehľadnosť.

17

Neflexibilita: ak zamestnanci potrebujú časté výnimky alebo majú veľmi špecifické potreby, ktoré nezapadajú do žiadnej roly, administrátori sú nútení vytvárať stále nové a nové roly.

MODEL ABAC – DYNAMICKÉ ROZHODOVANIE

Riadenie prístupu na základe atribútov

- Namiesto statických rolí používa flexibilné politiky, ktoré v reálnom čase vyhodnocujú **kontext** žiadosti.
- **Príklad:** Lekár má prístup k záznamom pacienta, **len ak** je jeho ošetrojúcim lekárom, **počas** svojej služby a prihlasuje sa **z** nemocničnej siete.
- **Výhody:** Extrémne jemnozrnná a kontextovo citlivá kontrola. Ideálny pre zložité a dynamické prostredia (cloud, IoT).
- **Nevýhody:** Zložitejšie počiatočné nastavenie politík.

POROVNANIE RBAC VS. ABAC

Vlastnosť	Riadenie prístupu na základe rolí (RBAC)	Riadenie prístupu na základe atribútov (ABAC)
Základ rozhodovania	Statická rola používateľa (pracovná pozícia)	Dynamické atribúty (používateľ, zdroj, prostredie, akcia)
Granularita	Hrubozrná (na úrovni rolí)	Jemnozrná (na úrovni jednotlivých atribútov)
Flexibilita	Nízka (zmeny vyžadujú úpravu roly)	Vysoká (dynamicky sa prispôsobuje kontextu)
Zložitosť správy	Jednoduchšia na začiatku, riziko „explózie rolí“	Zložitejšia na úvodné nastavenie politik
Ideálne pre	Stabilné organizácie s jasne definovanými rolami	Zložité, dynamické organizácie, cloudové prostredia

STE PRVOU LÍNIOU OBRANY

Vaše povinnosti a osvedčené postupy

- Technológie a politiky tvoria dôležitý rámec, no **najdôležitejším a zároveň najzraniteľnejším prvkom je človek.**
- Každý zamestnanec svojím každodenným správaním priamo ovplyvňuje bezpečnosť celej organizácie.

Kľúčové oblasti zodpovednosti:

1. Správa hesiel a prihlasovacích údajov
2. Pochopenie životného cyklu prístupu
3. Rozpoznávanie a nahlásenie hrozieb

SPRÁVA HESIEL – ZÁKLADNÝ KAMEŇ BEZPEČNOSTI

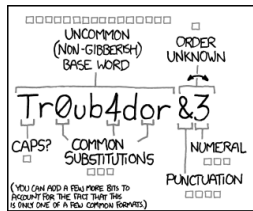
Ochrana vašich digitálnych kľúčov

- **Tvorba silných hesiel:** Dĺžka je dôležitejšia ako zložitosť. Používajte **heslové frázy** (napr. MojaPrvaCestaDoPrahyBolaV2005!). Minimálna dĺžka 12-14 znakov.
- **Nebezpečenstvo recyklácie hesiel:** Používanie rovnakého hesla pre viacero služieb je extrémne rizikové.
- **Nebezpečenstvo zdieľania údajov:** Vaše heslo je ako zubná kefka – **nepožičiavajte ho!** Zdieľanie ruší princíp zodpovednosti.

21

Ak dôjde k úniku dát z jednej, čo i len menej dôležitej služby, útočníci automaticky skúšajú ukradnuté prihlasovacie údaje použiť na prístup k všetkým ostatným dôležitým účtom.

Ak sa pod zdieľaným účtom vykoná škodlivá aktivita, je nemožné zistiť, kto bol skutočným páchatelom.



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

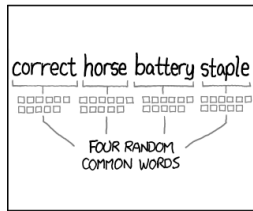
(PSYCHOLOGICAL: PEOPLE DON'T KNOW HOW MANY BITS SERVICE TECHS CRACKS A STRONG PASSWORD IN MINUTES, BUT IT'S NOT WHAT THE ANSWER USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOLOGY...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 530 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT?

DIFFICULTY TO REMEMBER: **YOU'VE ALREADY MEMORIZED IT**

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Zdroj: <https://xkcd.com/936/>

NÁSTROJE PRE SPRÁVU HESIEL

Ako si to všetko zapamätať?

- **Správcovia hesiel (Password Managers):**
 - Dnes už nevyhnutný nástroj.
 - Bezpečne ukladajú všetky vaše heslá v zašifrovanom trezore.
 - Generujú extrémne silné, náhodné heslá pre každú službu.
 - Vy si musíte pamätať len jedno hlavné heslo.
- **Viacfaktorová autentifikácia (MFA):**
 - Najúčinnější obrana proti zneužitiu ukradnutých hesiel.
 - Aj keby útočník získal vaše heslo, bez druhého faktora sa do účtu nedostane.
 - **Všade, kde je to možné, by malo byť MFA povinne zapnuté.**

MFA: Vyžaduje kombináciu niečoho, čo viete (heslo), niečoho, čo máte (telefón), alebo niečoho, čím ste (biometria).

ŽIVOTNÝ CYKLUS PRÍSTUPU

Od nástupu po odchod

- **Onboarding (Nástup):** Na základe vašej roly a v súlade s PoLP sú vám pridelené potrebné prístupy.
- **Zmena pozície:** Vyžaduje okamžitú revíziu prístupov. Nepotrebné práva musia byť odobraté a nové pridané. Je to vaša zodpovednosť a zodpovednosť vášho nadriadeného iniciovať tento proces.
- **Offboarding (Odchod):** Najneskôr v posledný deň musia byť **všetky vaše prístupy deaktivované**. Je to kritický bezpečnostný krok.

HROZBA "MŔTVÝCH DUŠÍ"

Časovaná bomba v systémech

- **Definícia:** Neaktívne účty bývalých zamestnancov, ktoré zostávajú v systémech.
- **Riziko:** Sú obľúbeným cieľom útočníkov, pretože ich nikto aktívne nepoužíva a ich kompromitácia môže zostať dlho nepovšimnutá.
- **Ochrana:** Jedinou ochranou je dôsledný a nepriestrelný proces offboardingu.

ROZPOZNÁVANIE A NAHLASOVANIE HROZIEB

Vaše oči a uši

- **Phishing a sociálne inžinierstvo:** Budte extrémne opatrní pri e-mailoch, SMS alebo telefonátoch, ktoré žiadajú citlivé údaje alebo vytvárajú pocit naliehavosti.
- **Prečo je nahlasovanie kriticky dôležité?**
 - Ste kľúčovou súčasťou systému včasného varovania.
 - Je lepšie nahlásiť desať falošných poplachov ako umožniť jeden reálny útok.
 - Včasné nahlásenie môže ochrániť desiatky ďalších kolegov.
- Zistite, aký je oficiálny proces nahlasovania vo vašej firme a neváhajte ho použiť.

26

Útočníci sú majstri v manipulácii a často vytvárajú pocit naliehavosti alebo strachu.

Každá organizácia by mala mať jasne definovaný a jednoduchý proces nahlasovania bezpečnostných incidentov – kontakt na IT helpdesk alebo priamo na manažéra kybernetickej bezpečnosti. Zistite, aký je tento proces vo vašej firme a neváhajte ho použiť.

POUČENIE Z KRÍZOVÉHO VÝVOJA

Keď sa riadenie prístupu zanedbá

- Najväčšie a najdrahšie bezpečnostné incidenty často nezačali sofistikovaným „hackom“, ale triviálnym zlyhaním v základnej hygiene riadenia prístupu.
- Typická stratégia útočníkov sa nazýva **eskalácia privilégii (privilege escalation)**.

ESKALÁCIA PRIVILÉGIÍ: Z MALEJ TRHLINY KATASTROFA

Ako útočníci postupujú

- 1. Počiatočný prienik:** Útočník získava prístup k účtu bežného zamestnanca s nízkymi oprávneniami (napr. cez phishing).
- 2. Prieskum a pohyb:** Po vstupe do siete útočník potichu skúma prostredie a hľadá ďalšie zraniteľnosti.
- 3. Získanie vyšších práv:** Cieľom je postupne získať prístup k účtom s vyššími oprávneniami a nakoniec získať plnú kontrolu nad sieťou.

Správne riadenie prístupu (PoLP) robí tento proces pre útočníka oveľa zložitejším.

PRÍPADOVÁ ŠTÚDIA 1: ÚTOK NA SONY PICTURES (2014)

Zlyhanie základnej ochrany

- **Scenár:** Útočníci rozposlali cieľené phishingové e-maily zamestnancom. Niekoľko z nich zadalo svoje prihlasovacie údaje na falošnú stránku.
- **Zneužitie:** S ukradnutými údajmi sa útočníci dostali do siete. Zistili, že mnohí zamestnanci používajú **rovnaké heslá** pre viacero systémov.
- **Následky:** Postupná eskalácia privilégii, krádež a zverejnenie obrovského množstva citlivých dát (e-maily, platy, osobné údaje, nevydané filmy).
- **Poučenie:** Útok bol umožnený kombináciou phishingu a recyklácie hesiel.

29

Vydávali sa za spoločnosť Apple a žiadali overenie Apple ID.

Unikli filmy [Annie](#), [Mr. Turner](#), [Still Alice](#) and [To Write Love on Her Arms](#).

Problémy: nedostatočné školenie zamestnancov v rozpoznávaní phishingu, recyklácia hesiel a pravdepodobne nedostatočná segmentácia siete.

PRÍPADOVÁ ŠTÚDIA 2: ÚTOK NA COLONIAL PIPELINE (2021)

Ochromenie kritickej infraštruktúry

- **Scenár:** Útočníci získali prístup do firemnej VPN siete pomocou jediného kompromitovaného hesla, ktoré našli na dark webe. Zamestnanec toto heslo recykloval.
- **Kľúčové zlyhanie:** Tento VPN účet **nebol chránený viacfaktorovou autentifikáciou (MFA)**.
- **Následky:** Nasadenie ransomvéru, preventívne odstavenie najväčšieho palivového potrubia v USA, nedostatok paliva na východnom pobreží a zaplatenie miliónového výkupného.
- **Poučenie:** Mrzivá ukážka dôsledkov recyklácie hesiel a absencie MFA.

PRÍPADOVÁ ŠTÚDIA 3: HROZBY ZVNÚTRA (INSIDER THREATS)

Hrozba nemusí prísť zvonku

Nie všetky hrozby sú externé. Zamestnanci predstavujú obrovské riziko, pretože už majú legitímny prístup.

• Typy insiderov:

- **Zlomyseľní (Malicious):** Úmyselne kradnú dáta pre zisk, pomstu alebo konkurenčnú výhodu.
- **Nedbanliví (Negligent):** Spôsobujú škodu neúmyselne (kliknutie na phishing, odoslanie dát na zlú adresu).

PRÍKLADY INTERNÝCH HROZIEB

- **Tesla (2023):** Dvaja bývalí zamestnanci zneužili svoj prístup a poskytli médiám osobné údaje viac ako 75 000 kolegov.
- **Cash App Investing (2021):** Bývalý zamestnanec po odchode stiahol reporty s osobnými a finančnými údajmi viac ako 8 miliónov zákazníkov.

Poučenie: Ochrana vyžaduje striktný PoLP, SoD, monitorovanie a hlavne nepriestrelný proces offboardingu.

ZHRNUTIE: BEZPEČNOSŤ JE SPOLOČNÁ ZODPOVEDNOSŤ

Rekapitulácia kľúčových bodov

- Riadenie prístupových práv nie je len starosťou IT oddelenia.
- Je to systém, ktorý zabezpečuje, aby **správni ľudia mali správne kľúče (prístupy) v správnom čase.**
- Ochrana prístupov chráni priamo vás, vašu prácu a vašu zodpovednosť.
- Zlaté pravidlo: „**Ak to nepotrebuješ, nedostaneš to.**“ Toto nie je prejav nedôvery, ale najúčinnější spôsob minimalizácie rizika.

VAŠICH 5 KLÍČOVÝCH POVINNOSTÍ (1/3)

Čo sa od vás očakáva?

1. Vaše heslo je ako zubná kefka: Nikomu ho nepožičiavajte.
 - Nikdy a nikomu nezdievajte svoje heslo – ani kolegovi, ani nadriadenému.
 - Používajte silné a unikátne heslá.
 - Ak je k dispozícii MFA/2FA, **vždy ju používajte**. Je to ako druhý bezpečnostný zámok.
2. Jeden účet = Jedna osoba
 - Nikdy nepracujte pod účtom kolegu. Stráca sa tak evidencia, kto danú zmenu v systéme vykonal.

VAŠICH 5 KLÍČOVÝCH POVINNOSTÍ (2/3)

Čo sa od vás očakáva?

3. Zamykajte svoje „digitálne dvere“

- Vždy si zamykajte počítač, keď od neho odchádzate.
- Klávesová skratka: **Win + L** (Windows, Linux), **Ctrl + Cmd + Q** (Mac).
- Je to rovnaké, ako keď zamykáte dvere od kancelárie.

4. Buďte ostražití a hláste podozrenia

- Okamžite hláste akúkoľvek podozrivú aktivitu.
- Podozrivé je: e-mail žiadajúci heslo, nečakaná výzva na prihlásenie, alebo ak máte prístup niekam, kam by ste nemali.

VAŠICH 5 KLÍČOVÝCH POVINNOSTÍ (3/3)

Čo sa od vás očakáva?

5. Uvedomujte si svoje prístupy

- Ak meníte pracovnú pozíciu, očakávajte, že sa vaše prístupy zmenia. Staré a nepotrebné vám budú odobraté.
- Ak máte pocit, že máte prístup k dátam, ktoré pre svoju prácu nepotrebujete, **proaktívne na to upozornite.**

ZÁVER

Nevyhnutosť pre digitálny ekosystém

- Riadenie prístupových práv je kritickým pilierom informačnej a kybernetickej bezpečnosti.
- Je to nepretržitý proces, ktorý si vyžaduje kombináciu:
 - Správne nastavených technológií.
 - Jasne definovaných firemných politík.
 - Bezpečnostného povedomia a zodpovednosti **každého zamestnanca**.
- V dnešnom svete je dôsledné riadenie prístupov absolútnou nevyhnutnosťou pre prežitie a úspech organizácie.

ĎAKUJEM ZA POZORNOST

- Otázky a odpovědi