
ÚVOD DO INFORMAČNEJ BEZPEČNOSTI



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



KOMPETENČNÉ
CENTRUM
KYBERNETICKEJ
BEZPEČNOSTI

STU

SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE

ÚVOD DO INFORMAČNEJ BEZPEČNOSTI

Autori: Ing. Ján Drahoš a doc. Ing. Dagmar Vidriková , PhD.

Prezentuje: Matúš Jókay



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



KOMPETENČNÉ
CENTRUM
KYBERNETICKEJ
BEZPEČNOSTI

STU

SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE

OBSAH

- 1.Úvod do informačnej bezpečnosti
- 2.Informačný a komunikačný systém
- 3.Právna úprava informačnej bezpečnosti
- 4.Kľúčové oblasti a zodpovednosti
- 5.Ohrozenia v oblasti informačnej bezpečnosti
- 6.Moderné stratégie a princípy obrany
- 7.Zásady bezpečného správania**
- 8.Hlásenie bezpečnostných incidentov
- 9.Na čo by si mali zamestnanci dávať pozor**
- 10.Aktuálne trendy a výzvy pre rok 2025

PREČO JE INFORMAČNÁ BEZPEČNOSŤ DÔLEŽITÁ?

- V súčasnosti takmer každá organizácia spracúva informácie s využitím informačných a komunikačných technológií (IKT).
- Informácie sú všade – v e-mailoch, mobiloch, na USB kľúčoch, v zdravotných kartách aj v hlavách ľudí.
- Mnohé z týchto informácií majú veľkú hodnotu a môžu byť zneužitú.
- Preto do popredia vystupuje kľúčová úloha informačnej bezpečnosti.

HISTORICKÝ KONTEXT A MODERNÁ ÉRA

- Ochrana informácií je súčasťou ľudských činností od počiatku (napr. ukryvanie papyrusov v staroveku).
- V minulosti sa šifrovali vojenské rozkazy a bankové spisy sa zamykali do trezorov.
- S nástupom počítačov a internetu sa informácie presunuli z papiera do digitálneho priestoru.
- Dnešné hrozby sú globálne; útočník môže byť tisíce kilometrov ďaleko a prelomiť slabé heslo v priebehu sekúnd.

CIEĽ INFORMAČNEJ BEZPEČNOSTI: TRIÁDA CIA

- Cieľom informačnej bezpečnosti je zabezpečiť, aby sa s informáciami zaobchádzalo správne.
- Tento cieľ je definovaný tromi základnými piliermi, známymi ako

Triáda CIA:

- **C** – Dôvernosť (Confidentiality): Informácie sú prístupné len oprávneným osobám.
- **I** – Integrita (Integrity): Informácie sú presné, úplné a neboli neoprávnene zmenené.
- **A** – Dostupnosť (Availability): Informácie sú k dispozícii vtedy, keď ich potrebujeme.

TRIÁDA CIA V PRAXI

- Dôvernosť (Confidentiality)**

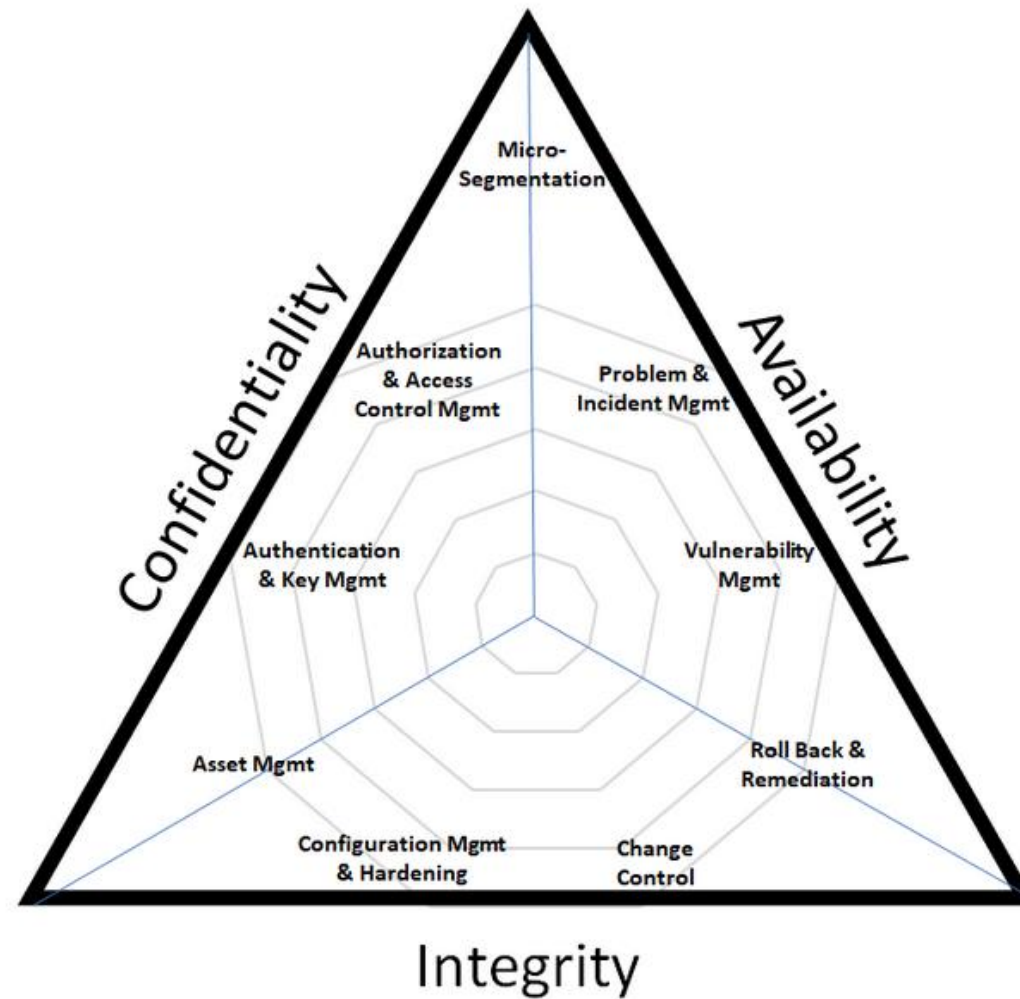
- Význam:** Informácie sú prístupné len oprávneným osobám.
- Príklad:** Len personalista má prístup k mzdovým údajom zamestnancov.

- Integrita (Integrity)**

- Význam:** Informácie sú presné a neboli neoprávnene zmenené.
- Príklad:** Faktúra odoslaná e-mailom nebola počas prenosu upravená.

- Dostupnosť (Availability)**

- Význam:** Informácie a systémy sú funkčné a prístupné, keď ich potrebujeme.
 - Príklad:** E-shop funguje aj počas najväčšej nákupnej špičky.
-



Zdroj: <https://www.cimcor.com/blog/what-integrity-means-in-the-cia-triad>

ZDIEĽANÁ ZODPOVEDNOSŤ

- Bezpečnosť už dávno nie je vnímaná ako výlučná kompetencia IT oddelenia.
- Za bezpečnosť informácií zodpovedá **každý**, kto s nimi prichádza do kontaktu – od riaditeľa až po zamestnanca na recepcii.
- Technológie môžu pomôcť, ale najslabším článkom je často človek.
- Informačná bezpečnosť nie je len o technike, ale hlavne o zodpovednosti, vedomostiach a zdravom rozume.

ZÁKLADNÉ POJMY A DEFINÍCIE

KLÚČOVÉ POJMY I.

- **Informácia:** Údaj, ktorý má pre niekoho význam a hodnotu. Môže mať formu textu, obrazu, zvuku alebo kódu.
-
- **Informačné aktívum:** Čokoľvek, čo má pre organizáciu hodnotu z hľadiska informácií (napr. databáza klientov, e-mailový účet, dokumentácia).

ZÁKLADNÉ POJMY A DEFINÍCIE

KLÚČOVÉ POJMY II.

• **Informačná bezpečnosť**: Ochrana informácií pred stratou, zneužitím, poškodením alebo neoprávneným prístupom, a to vo všetkých formách – digitálnej, papierovej aj ústnej.

Kybernetická bezpečnosť: Ochrana výlučne digitálnych informácií.

ZÁKLADNÉ POJMY A DEFINÍCIE

KLÚČOVÉ POJMY III.

- **Hrozba (Threat):** Potenciálny zdroj škody alebo narušenia bezpečnosti (napr. kyberútok, prírodná katastrofa, chyba človeka).
- **Zraniteľnosť (Vulnerability):** Slabé miesto v systéme alebo procese, ktoré môže byť zneužitá hrozbou (napr. nezabezpečená Wi-Fi, slabé heslo, neaktualizovaný softvér).
- **Incident (Incident):** Bezpečnostná udalosť, ktorá narušila (alebo mohla narušiť) informačnú bezpečnosť. Príklad: odoslanie e-mailu s citlivými údajmi nesprávnemu príjemcovi.

ČO JE RIZIKO?

- **Riziko (Risk):** Je to pravdepodobnosť, že daná hrozba zneužije konkrétnu zraniteľnosť a spôsobí škodu (dopad).

- Vzorec:

$$\text{Riziko} = \text{Hrozba} \times \text{Zraniteľnosť} \times \text{Dopad}$$

- Cieľom riadenia rizík je znížiť riziko na akceptovateľnú mieru prostredníctvom bezpečnostných opatrení.

PRÁVNÝ A NORMATÍVNY RÁMEC

PREHĽAD LEGISLATÍVY EÚ A SR

- Ochrana IKT systémov je kľúčová, preto sú zaradené medzi sektory **kritickej infraštruktúry**.
- Bezpečnosť je upravená širokým spektrom právnych predpisov, interných noriem a medzinárodných zmlúv.
- **Dôležitá poznámka:** Nie každý musí poznať všetky zákony naspamäť, ale každý zamestnanec má zodpovednosť chrániť informácie, ktoré spracúva.

KLÚČOVÉ ZÁKONY A NARIADENIA

- **Ochrana osobných údajov:**

- Nariadenie EÚ 2016/679 (**GDPR**)
- Zákon č. 18/2018 Z. z. o ochrane osobných údajov

- **Kybernetická bezpečnosť:**

- Implementácia smernice **NIS2** do národnej legislatívy (Zákon o kybernetickej bezpečnosti).

KLÚČOVÉ ZÁKONY A NARIADENIA

- **Ochrana utajovaných a iných skutočností:**

- Zákon č. 215/2004 Z. z. (utajované skutočnosti)
- Obchodný zákonník (obchodné tajomstvo), Zákon o bankách (bankové tajomstvo)

- **Trestnoprávna zodpovednosť:**

- Trestný zákon č. 300/2005 Z. z. (počítačová kriminalita)

IT vo verejnej správe

- Zákon 95/2019 Z. z. o informačných technológiách vo verejnej správe

TECHNICKÉ NORMY – RODINA ISO/IEC 27000

- Tieto medzinárodné normy poskytujú rámec a osvedčené postupy pre riadenie informačnej bezpečnosti.
- ISO/IEC 27001:2022**: Špecifikuje požiadavky na zavedenie, prevádzku a zlepšovanie **Systemu manažérstva informačnej bezpečnosti (ISMS)**. Je to certifikačná norma.
- ISO/IEC 27002:2022**: Poskytuje referenčný súbor všeobecných bezpečnostných opatrení a návod na ich implementáciu.
- ISO/IEC 27005:2022**: Poskytuje usmernenie k procesu **riadenia rizík** informačnej bezpečnosti.

SMERNICA NIS2: NOVÁ ÉRA ZODPOVEDNOSTI

- **Rozšírený rozsah:** Povinnosti sa týkajú tisícok ďalších firiem a organizácií v sektoroch ako potravinárstvo, výroba, poštové služby či odpadové hospodárstvo.
- **Zodpovednosť manažmentu:** Vedenie spoločnosti (konatelia, predstavenstvo) je priamo a osobne zodpovedné za zavedenie a dodržiavanie bezpečnostných opatrení.
- **Povinnosť hlásiť incidenty:** Závažné incidenty musia byť nahlásené príslušnému úradu (napr. SK-CERT) do **24 hodín** od ich zistenia.

KLÍČOVÉ OBLASTI A ZODPOVEDNOSTI

TRI PILIERE BEZPEČNOSTI

- Účinná informačná bezpečnosť stojí na troch pilieroch:
 - **Ľudia:** Najdôležitejší, no často najslabší článok.
 - **Procesy:** Pravidlá, politiky a postupy, ktorými sa organizácia riadi.
 - **Technológie:** Nástroje, ktoré používame na ochranu a presadzovanie pravidiel.
- Až súhra všetkých troch zložiek zaručuje skutočne efektívnu ochranu.

PILIER 1: ĽUDIA

- Ľudia sú prvou a poslednou líniou obrany. Viac ako 80 % kyberútokov je zameraných práve na človeka cez sociálne inžinierstvo.

- Kľúčové aktivity:**

- Bezpečnostné školenia (Security Awareness):** Pravidelný a nepretržitý proces pre všetkých zamestnancov.

- Simulované phishingové kampane:** Najefektívnejší spôsob overenia a tréningu odolnosti zamestnancov.

- Budovanie bezpečnostnej kultúry:** Vytvorenie prostredia, kde bezpečnosť je spoločná zodpovednosť a zamestnanci sa neboja nahlásiť chybu.

PILIER 2: PROCESY

- Procesy sú chrbticou bezpečnostnej stratégie; definujú, **ako** má organizácia pristupovať k bezpečnosti.
- **Kľúčové aktivity:**
 - **Riadenie rizík (Risk Management):** Cyklický proces identifikácie aktív, hrozieb, analýzy a ošetrenia rizík.
 - **Bezpečnostné politiky a smernice:** Oficiálne dokumenty definujúce pravidlá (napr. politika hesiel, politika práce z domu).
 - **Riadenie bezpečnostných incidentov:** Presný plán, čo robiť, keď nastane incident – kto je zodpovedný, ako incident izolovať, odstrániť a ako komunikovať.

PILIER 3: TECHNOLOGIE

- Technológie sú nástroje, ktoré automatizujú obranu, poskytujú prehľad a vynucujú pravidlá definované v procesoch.
- Kľúčové technológie:**
 - Riadenie prístupu (IAM):** Zabezpečuje, že každý má prístup len k tomu, čo nevyhnutne potrebuje.
 - Viacfaktorová autentifikácia (MFA):** Povinný štandard pre overenie identity.
 - Ochrana siete a koncových bodov:** Firewally novej generácie (NGFW) a systémy EDR (nástupca antivírusu).
 - Monitoring a detekcia (SIEM):** Zber a analýza bezpečnostných záznamov (logov) na odhalenie útokov.

DIALEKTIKA TRIÁDY V PRAXI

- **PROCES** (Bezpečnostná politika) stanoví pravidlo: "Heslo musí mať minimálne 12 znakov."
- **TECHNOLÓGIA** (Systém správy účtov) toto pravidlo technicky vynúti a nedovolí používateľovi zvoliť si kratšie heslo.
- **ČLOVEK** (Zamestnanec, ktorý prešiel školením) chápe, prečo je to dôležité, a preto si zvolí vhodné heslo vyhovujúce bezpečnostnej politike.

HROZBY A STRATÉGIE OBRANY

PREHĽAD OHROZENÍ (1/2)

- Úmyselné hrozby**

- Kybernetické útoky (Phishing, Ransomware, DDoS)
- Sociálne inžinierstvo
- Sabotáž a vnútorné hrozby
-

- Neúmyselné hrozby**

- Chyby používateľov (odoslanie zlého e-mailu, slabé heslo)
- Nesprávna konfigurácia systémov

HROZBY A STRATÉGIE OBRANY

PREHLÁD OHROZENÍ (2/2)

- Technické a systémové hrozby**

- Výpadky technológií (zlyhanie hardvéru)
- Zlyhanie siete alebo internetového pripojenia
-

- Fyzické a prírodné hrozby**

- Požiar, povodeň
- Krádež alebo strata zariadenia (notebook, mobil)

MODERNÉ STRATÉGIE OBRANY: ÚVOD

- Tradičná obrana založená na budovaní jednej veľkej steny (firewall) už nestačí.
- Moderný prístup je viacvrstvový.
- **Kľúčové moderné princípy:**
 - Hĺbková obrana (Defense in Depth)
 - Princíp nulovej dôvery (Zero Trust)
 - Povinná viacfaktorová autentifikácia (MFA)
 - Kybernetická hygiena

STRATÉGIA 1: HĽBKOVÁ OBRANA (DEFENSE IN DEPTH)

- Myšlienka:** Nikdy sa nespoliehajte na jedno bezpečnostné opatrenie. Vytvorte viacero na sebe nezávislých vrstiev ochrany.
- Analógia:** Zabezpečenie stredovekého hradu. Ak útočník prekonal jednu prekážku, narazil na ďalšiu.
- Príklady vrstiev v IT:** Fyzická ochrana -> Perimeter siete (Firewall) -> Vnútoraná sieť (Segmentácia) -> Koncové body (EDR) -> Aplikácie -> Dáta (Šifrovanie) -> Ľudia (Školenia).

STRATÉGIA 2:

PRINCÍP MINIMÁLNYCH OPRÁVNENÍ (POLP)

- Pravidlo:** Každý používateľ, aplikácia alebo systém by mal mať len tie najnutnejšie oprávnenia, ktoré nevyhnutne potrebuje na vykonanie svojej úlohy. Nič viac.

- Analógia:** Hotelový personál. Chyžná má kartu, ktorá otvára len izby na jej poschodí, nie trezor riaditeľa.

- Praktická implementácia:**

- Bežní používatelia nikdy nesmú mať administrátorské práva na svojich počítačoch.

- Administrátori by mali používať samostatný, privilegovaný účet len vtedy, keď je to nevyhnutné.

STRATÉGIA 3: NULOVÁ DÔVERA (ZERO TRUST)

- **Nová paradigma:** Starý model "dôveruj, ale preveruj" je mŕtvy.
- **Heslo:** "Nikdy nedôveruj, vždy overuj" (Never trust, always verify).
- **Predpoklad:** Útočník je už v sieti. Dôvera nie je nikdy automatická.
- Každá jedna požiadavka na prístup k dátam alebo aplikácii musí byť overená, bez ohľadu na to, odkiaľ prichádza (z kancelárie alebo z domu).

STRATÉGIA 4: KYBERNETICKÁ HYGIENA

- Toto nie je stratégia, ale súbor základných, opakovaných činností, ktoré tvoria základ pre všetko ostatné.
 - **Analógia:** Osobná hygiena. Môžete mať najlepších lekárov, ale ak si pravidelne neumývate ruky, budete neustále chorí.
 - **Základné návyky:**
 - **Pravidelné aktualizácie a záplaty (Patch Management):** Okamžité aplikovanie bezpečnostných aktualizácií.
 - **Silné heslá:** Vynucovanie používania dlhých a unikátnych hesiel.
 - **Zálohovanie:** Pravidelné a testované zálohy kritických dát.
-

ZHRNUTIE STRATÉGIÍ

- **Híbková obrana** vytvára vrstvy.
- **Princíp minimálnych oprávnení** znižuje dopad, ak jedna vrstva zlyhá.
- **Zero Trust** mení filozofiu a overuje každý pohyb medzi vrstvami aj vnútri nich.
- **Kybernetická hygiena** je tmel, ktorý to všetko drží pohromade.

PRAKTICKÉ ZÁSADY PRE ZAMESTNANCOV ZÁSADY BEZPEČNÉHO SPRÁVANIA: PREHLÁD

- Bezpečnosť je kombináciou technických, organizačných a personálnych opatrení.
- Každý zamestnanec by mal dodržiavať tieto základné pravidlá:
 - Používanie silných a jedinečných hesiel, ideálne s dvojfaktorovou autentifikáciou (2FA).
 - Zamykanie obrazovky pri odchode od počítača.
 - Neotváranie príloh z neznámych e-mailov.
 - Neinštalovanie neschváleného softvéru.
 - Správne ukladanie a zálohovanie dokumentov.
 - Neposkytovanie informácií cez telefón bez overenia.

PRAVIDLO #1: BEZPEČNÉ HESLÁ A 2FA

•Zlé praktiky:

- Používanie rovnakého hesla pre viacero služieb.
- Vytváranie jednoduchých hesiel ako "firma2025" alebo "123456".
- Zdieľanie hesiel s kolegami alebo ich zapisovanie na papierik pod klávesnicu.

•Dobré praktiky:

- Používanie dlhých hesiel (minimálne 12 znakov) s kombináciou písmen, čísel a symbolov.
- Používanie správcu hesiel na generovanie a ukladanie unikátnych hesiel.
- Aktivácia dvojfaktorovej autentifikácie (2FA) všade, kde je to možné.

PRAVIDLO #2:

POZOR NA PHISHING

- Nikdy neklikajte na podozrivé odkazy a neotvárajte neznáme prílohy.
- **Ako rozpoznať phishingový e-mail:**
 - Dôkladne skontrolujte e-mailovú adresu odosielateľa – často sa len podobá na originál.
 - Všímajte si gramatické chyby a nezvyčajný štýl písania.
 - Buďte opatrní pri e-mailoch, ktoré vytvárajú nátlak a žiadajú okamžitú akciu ("potvrďte ihneď", "vaše konto bude zablokované").
- V prípade akejkoľvek pochybnosti kontaktujte IT oddelenie.

PRAVIDLO #3: FYZICKÁ BEZPEČNOSŤ NA PRACOVISKU

- **Zamykajte počítač** vždy, keď sa vzdáľujete od stola, aj na krátku chvíľu. (Klávesová skratka **Win + L**).
- Dodržiavajte **politiku čistého stola** – nenechávajte dôverné dokumenty voľne položené na stole.
- Nenechávajte prenosné zariadenia (notebook, mobil) a USB kľúče bez dozoru.

PRAVIDLO #4: OPATRNOŠŤ PRI KOMUNIKÁCI

- Nerozprávajte o citlivých firemných alebo osobných informáciách na verejných miestach (napr. vo výtahu, kaviarni, vlaku).
- Pozor na **Vishing** (voice phishing) – útok cez telefón.
- Ak vás niekto telefonicky žiada o citlivé údaje alebo prístupy,
- **vždy si overte jeho totožnosť**. Môžete napríklad zavolať späť na známe interné číslo.

HLÁSENIE BEZPEČNOSTNÝCH INCIDENTOV

- **Čo je incident?** Akákoľvek udalosť, ktorá môže ohroziť bezpečnosť informácií. Napríklad podozrivý e-mail, strata USB kľúča, alebo neobvyklé správanie systému.
- **Prečo hlásiť?** Včasné hlásenie je kľúčové na rýchlu reakciu a minimalizáciu škôd. Každý incident môže byť začiatkom väčšieho útoku.
- **Kultúra bez obviňovania:** Cieľom nie je hľadať vinníkov, ale chrániť organizáciu. Je lepšie nahlásiť planý poplach, ako nenahlásiť skutočný problém.

DÔSLEDKY NARUŠENIA BEZPEČNOSTI

- **Finančné škody:** Priame straty, náklady na obnovu, pokuty.
- **Poškodenie reputácie:** Strata dôvery zákazníkov a partnerov.
- **Právne dôsledky:** Porušenie zákonov a regulácií (napr. GDPR) môže viesť k vysokým pokutám.
- **Ohrozenie zdravia alebo života:** Najmä v kritických sektoroch ako zdravotníctvo alebo energetika.

AKTUÁLNE TRENDY A VÝZVY PRE ROK 2025

TRENDY 2026: ÚVOD

- V roku 2026 už trendy nie sú teóriou, ale každodennou realitou.
- Bezpečnostní profesionáli dnes bojujú nielen s technológiami, ale aj s ekonomikou, legislatívou a ľudskou psychológiou.
- Kľúčové témy:**
 - Umelá inteligencia (AI): Dvojsečná zbraň
 - Bezpečnosť cloudu
 - Regulácie (Compliance), najmä NIS2
 - Bezpečnosť internetu vecí (IoT)

TREND 1:

UMELÁ INTELIGENCIA (AI) – DVOJSEČNÁ ZBRAŇ

- **AI ako obranca (Príležitosť):**

- Pomáha preťaženým bezpečnostným tímom analyzovať obrovské množstvo dát.
- Automatizuje detekciu anomálií a umožňuje okamžitú reakciu (napr. izolovanie napadnutého PC).

- **AI ako zbraň útočníka (Výzva):**

- **Hyperrealistický Phishing:** AI generuje dokonalé podvodné e-maily bez gramatických chýb.
- **Deepfake Vishing:** AI dokáže v reálnom čase klonovať hlas riaditeľa a telefonicky nariadiť urgentnú platbu.
- **Polymorfný malvér:** AI vytvára škodlivé kódy, ktoré neustále menia svoju podobu, aby sa vyhli detekcii.

TREND 2: BEZPEČNOSŤ CLOUDU

- Výzvou už nie je *či* prejsť do cloudu, ale *ako* to urobiť bezpečne.
- **Model zdieľanej zodpovednosti:**
 - **Poskytovateľ** (napr. Microsoft, AWS) zodpovedá za bezpečnosť **CLOUDU** (fyzické datacentrá, hardvér, siete).
 - **Zákazník** (firma) zodpovedá za bezpečnosť **V CLOUDE** (správna konfigurácia, riadenie prístupov, šifrovanie dát).
- **Najčastejšia hrozba: Nesprávna konfigurácia** zo strany zákazníka. Ide o najčastejšiu príčinu úspešných útokov na cloudové prostredia.

TREND 3: REGULÁCIE A SÚLAD (NIS2)

- Bezpečnosť už nie je len odporúčaním, ale **tvrdou právnou požiadavkou** s hrozbou vysokých pokút.
- V roku 2025 boli firmy v plnej **implementačnej fáze smernice NIS2.**
- Kontrolné orgány začali vykonávať prvé audity a udeľovať sankcie.

TREND 4: BEZPEČNOSŤ OT A IOT

- Stiera sa hranica medzi digitálnym (IT) a fyzickým (OT - Operačné technológie) svetom.
 - Konvergencia IT/OT:** Výrobné linky, roboty a senzory sú prepojené s firemnými sieťami, čím sú vystavené hrozbám z internetu.
 - Špecifické riziká OT:**
 - Útok môže mať
 - fyzické následky:** zastavenie výroby, poškodenie strojov, ekologická havária alebo ohrozenie životov.
 - Mnoho OT systémov je zastaraných (bežia napr. na Windows XP) a nemôžu byť aktualizované.
-

VÝZVY PRE SLOVENSKO

- **Nedostatok expertov:** Akútny nedostatok certifikovaných cloudových a OT bezpečnostných špecialistov, analytikov a dátových vedcov.
- **Vysoké náklady:** Pre menšie a stredné podniky predstavujú náklady na dosiahnutie súladu s NIS2 a na nákup pokročilých technológií významnú finančnú záťaž.
- **Zmena myslenia:** Tradičné firmy často zápasia so zmenou firemnej kultúry, ktorá je pre modernú bezpečnosť nevyhnutná.

ZÁVER

KLÚČOVÉ POSOLSTVÁ NA ZAPAMÄTANIE

- Informačná bezpečnosť je **zodpovednosťou každého** zamestnanca, nielen IT oddelenia.
- Človek je kľúčový – môže byť najslabším článkom, ale pri správnom prístupe aj **najlepšou líniou obrany**.
- Základom všetkého je dôsledné dodržiavanie **kybernetickej hygieny** (silné heslá, aktualizácie, opatrnosť).
- Nikdy sa nebojte **nahlásiť podozrivú udalosť**. Včasná reakcia je najlepšia ochrana.

ĎAKUJEM ZA POZORNOST