
KLASIFIKÁCIA AKTÍV A KATEGORIZÁCIA SIETÍ A INFORMAČNÝCH SYSTÉMOV



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



KOMPETENČNÉ
CENTRUM
KYBERNETICKEJ
BEZPEČNOSTI

STU

SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE

OBSAH

1. **Úvod do problematiky:** Čo sú informačné aktíva a prečo ich chrániť.
 2. **Základné pojmy:** Kto je kto v procese ochrany.
 3. **Vlastník vs. Správca:** Rozdelenie zodpovedností.
 4. **Klasifikácia informačných aktív:** Ako určiť citlivosť informácií.
 5. **Kategorizácia sietí a IS:** Ako určiť kritickosť systémov.
 6. **Zásady ochrany:** Kľúčové princípy bezpečnosti.
 7. **Povinnosti zamestnanca:** Prečo je ochrana aktív súčasťou práce.
 8. **Záver a príklady z praxe.**
-

ÚVOD: ČO SÚ INFORMAČNÉ AKTÍVA?

- Informačné aktíva sú všetky informácie a prostriedky, ktoré majú pre organizáciu hodnotu a je potrebné ich chrániť.
 - Zahŕňajú dáta, dokumenty, systémy, ale aj znalosti, ktoré používame pri práci.
 - Jednoducho povedané:
„Informačné aktívum je čokoľvek, čo obsahuje informácie dôležité pre našu firmu a bez čoho by sme nemohli pracovať efektívne alebo bezpečne.“
-

PRÍKLADY INFORMAČNÝCH AKTÍV

- Osobné údaje klientov alebo zamestnancov (meno, adresa, rodné číslo).
- Zmluvy a interné dokumenty.
- E-mailová komunikácia.
- IT systémy (účtovný softvér, CRM).
- Prístupové heslá a kódy.
- Know-how, postupy a obchodné tajomstvá.
- Zálohy dát a archívy.

PREČO SÚ INFORMAČNÉ AKTÍVA DÔLEŽITÉ?

Ich strata, poškodenie alebo zneužitie môže spôsobiť:

- **Finančnú škodu.**
- **Poškodenie dobrej povesti firmy.**
- **Porušenie zákonov** (napr. GDPR).
- **Zastavenie alebo narušenie prevádzky.**

„Predstavte si, že informačné aktíva sú ako vaše osobné veci doma – napríklad peňaženka, mobil, alebo kľúče od bytu. Majú pre vás hodnotu, a preto si ich chránite.“

POVINNOSŤ CHRÁNIŤ AKTÍVA: SPOLOČNÁ ZODPOVEDNOSŤ

- Nestačí sa spoliehať, že „IT oddelenie sa o to postará“. Bez každého zamestnanca by nefungoval ani najlepší bezpečnostný systém.
- Najčastejším dôvodom únikov informácií nie je technická chyba, ale **ľudské zlyhanie**.
 - Zdieľanie hesiel.
 - Kliknutie na podvodný e-mail.
 - Nezabezpečený USB kľúč.

„Chrániť informačné aktíva nie je len IT téma. Je to súčasť mojej každodennej práce, pretože informácie sú hodnotné a ich strata môže poškodiť firmu aj mňa.“

DÔSLEDKY CHÝB A ZANEDBANIA OCHRANY

Strata alebo únik informácií môže viesť k:

- **Vysokým pokutám** (napr. za porušenie GDPR).
- **Poškodeniu povesti firmy**, keď sa únik dostane do médií.
- **Právnym sporom** alebo strate dôvery partnerov.

Všetky tieto následky môžu mať dopad aj na zamestnanca – reputačný, pracovný alebo právny.

ZÁKLADNÉ POJMY: AKTÍVUM A SYSTÉM

- **Aktívum:** Všetko, čo má pre organizáciu definovateľnú hodnotu a jeho náhrada nie je možná bez značných zdrojov (finančných, časových, ľudských). Zahŕňa aj nehmotné veci ako reputácia a dobré meno.
- **Informačné aktívum (IA):** Špecifický typ aktíva, ktorý zahŕňa informácie, dáta, softvér, hardvér a služby.
- **Informačný systém (IS):** Funkčný celok, ktorý zabezpečuje spracúvanie a ochranu údajov prostredníctvom technických a programových prostriedkov.

ZÁKLADNÉ POJMY: KLÚČOVÉ ROLY

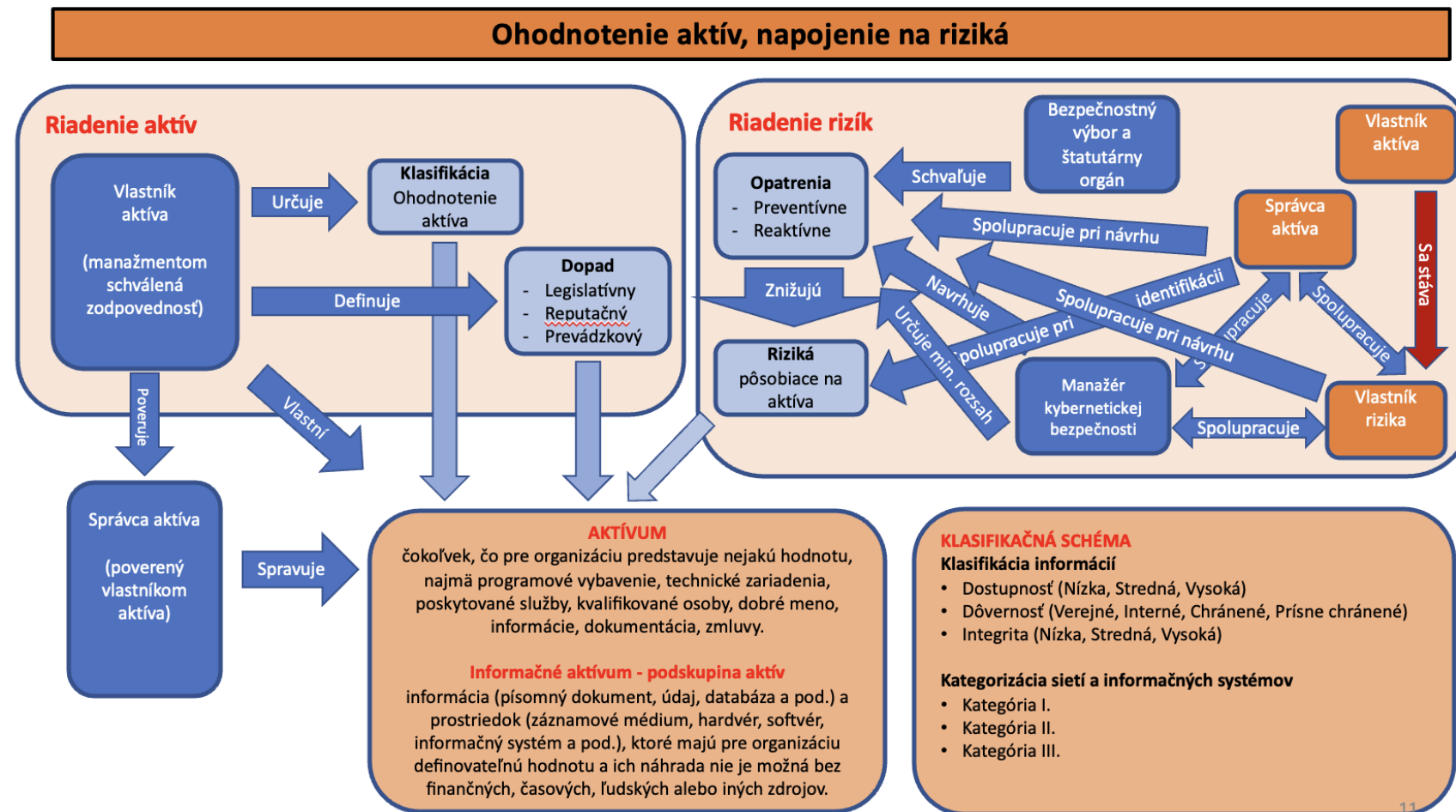
- **Vlastník informačného aktíva:** Osoba alebo útvar zodpovedný za adekvátnu ochranu zvereného aktíva počas jeho celého životného cyklu.
- **Správca informačného aktíva:** Subjekt (často IT), ktorý pre vlastníka technicky zabezpečuje zhromažďovanie, uchovávanie alebo spracovávanie informácií.
- **Manažér kybernetickej bezpečnosti (MKB):** Zodpovedá za riadenie a koordináciu kybernetickej a informačnej bezpečnosti v organizácii.

	Vlastník aktíva	Správca aktíva
Zodpovedá za	Obsah, význam, využitie a bezpečnosť aktíva.	Technickú správu, prevádzku a funkčnosť aktíva.
Kto to býva?	Obchodná alebo odborná rola (napr. vedúci oddelenia).	Zvyčajne IT alebo technická rola.
Úlohy	Určuje prístupové práva Rozhoduje o uchovaní/vyradení.	Implementuje technické opatrenia Zabezpečuje zálohovanie a monitoring.
Príklad	Vedúci personálneho oddelenia je vlastníkom údajov o zamestnancoch.	IT administrátor spravuje systém, v ktorom sú tieto údaje uložené.

VLASTNÍK VS. SPRÁVCA: KTO ZA ČO ZODPOVEDÁ?

VLASTNÍK VS. SPRÁVCA: PŘÍKLAD Z PRAXE

- **Aktívum:** Databáza zákazníkov.
- **Vlastník (Vedúci obchodu):**
 - Rozhoduje, aké údaje sa zbierajú.
 - Určuje, kto ich môže vidieť.
 - Definuje, ako dlho sa uchovávajú.
- **Správca (IT administrátor):**
 - Zabezpečuje, že databáza technicky funguje.
 - Stará sa o jej zálohovanie.
 - Implementuje ochranu prístupu (heslá, šifrovanie).



SCHEMATICKÉ ZNÁZORNENIE ROLÍ

URČENIE VLASTNÍKA AKTÍVA

- Vlastníka určuje štatutárny orgán organizácie alebo bezpečnostný výbor.
- **Kľúčová otázka:** Ktorý útvar alebo proces bude najviac ohrozený nedostupnosťou, stratou alebo zneužitím daného aktíva?
- Typicky je vlastníkom vedúci zamestnanec príslušného organizačného útvaru.
- V prípade sporov rozhoduje najbližší spoločný nadriadený.

PROCES PRIRADENIA VLASTNÍKA

Celý proces koordinuje **Manažér kybernetickej bezpečnosti (MKB)**.

- 1. Identifikácia aktív:** Vedúci oddelení pomáhajú identifikovať aktíva vo svojich útvaroch. IT oddelenie pomáha s technickými aktívami.
 - 2. Návrh vlastníka:** MKB vyzve útvary na určenie príslušnosti aktíva k procesom.
 - 3. Zaradenie do Katalógu aktív:** MKB zaeviduje aktívum a priradí mu dočasného vlastníka.
 - 4. Schválenie:** Bezpečnostný výbor formálne schváli priradenie vlastníka.
 - 5. Finalizácia:** MKB zmení status vlastníka z "dočasný" na "schválený".
-

ČO JE KLASIFIKÁCIA INFORMAČNÝCH AKTÍV?

- Je to proces, ktorý určuje, akú **hodnotu, citlivosť a mieru ochrany** má konkrétna informácia.
- Na základe klasifikácie sa rozhoduje:
 - Kto k informácii smie mať prístup.
 - Ako sa má chrániť (napr. šifrovanie, heslo).
 - Ako sa smie prenášať, zdieľať alebo zničiť.

„Cieľom nie je komplikovať prácu, ale chrániť to najcennejšie – dáta, dôveru a povesť organizácie.“

PROCES KLASIFIKÁCIE INFORMAČNÝCH AKTÍV

Ako prebieha proces
klasifikácie informačných aktív

Identifikácia
informačných aktív



Posúdenie hodnoty
a citlivosti aktíva



Zaradenie aktíva
do klasifikačnej úrovne



Určenie
ochranných opatrení



Priebežná kontrola
a preklasifikácia

KRITÉRIÁ PRE KLASIFIKÁCIU

Klasifikácia sa vykonáva z pohľadu narušenia troch základných pilierov bezpečnosti:

1. **Dôvernost'**: Ochrana pred neoprávneným prístupom. Môže byť informácia voľne sprístupnená?
2. **Dostupnost'**: Potreba dostupnosti informácie, keď ju oprávnený používateľ požaduje.
3. **Integrita**: Požiadavka na presnosť a správnosť poskytovanej informácie.

A ďalších kritérií ako hodnota, časová citlivosť či požiadavky legislatívy.

KLASIFIKAČNÉ STUPNE (Z POHĽADU DÔVERNOSTI)

Sú definované štyri základné stupne:

- **VEREJNÉ:** Určené pre verejnosť („môže čítať každý“).
- **INTERNÉ:** Prístupné pre všetkých zamestnancov v rámci organizácie („len vo firme“).
- **CHRÁNENÉ:** Prístupné len pre určené skupiny oprávnených osôb („len tí, čo to naozaj potrebujú“).
- **PRÍSNE CHRÁNENÉ:** Prístupné len pre vopred schválených jednotlivcov („len vybraní zamestnanci so špeciálnym prístupom“).

STUPEŇ „VEREJNÉ“

- **Definícia:** Aktíva určené pre verejnosť, získateľné z verejných zdrojov alebo pripravené na tento účel.
- **Príklady:** Informácie z médií, povinne publikované informácie, marketingové materiály.
- **Poznámka:** Verejnou sa môže stať aj interná informácia, ak o tom rozhodne jej vlastník (napr. zverejnením v tlačovej správe).

STUPEŇ „INTERNÉ“

- **Definícia:** Aktíva prístupné všetkým používateľom v rámci organizácie bez ohľadu na ich rolu.
- **Dopad zneužitia:** Neautorizovaný prístup by mohol spôsobiť vážny negatívny dopad (finančná strata, poškodenie mena).
- **Zdieľanie:** Sprístupnenie tretím stranám vyžaduje schválenie vlastníka informácie.
- **Príklady:** Pracovné postupy, interné smernice, zápisy z porád.

STUPEŇ „CHRÁNENÉ“

- **Definícia:** Aktíva prístupné len určeným skupinám oprávnených osôb.
- **Princíp prístupu:** Uplatňuje sa zásada „potreby viedieť“ (need-to-know) a „najnižších privilégií“.
- **Ochrana:** Vyžaduje špeciálne technické a organizačné opatrenia.
- **Príklady:** Osobné údaje zamestnancov a zákazníkov, zmluvy, finančné reporty.

STUPEŇ „PRÍSNE CHRÁNENÉ“

- **Definícia:** Aktíva prístupné len konkrétnym, vopred schváleným jednotlivcom.
 - **Dopad zneužitia:** Neautorizované odhalenie môže mať s vysokou pravdepodobnosťou kritický negatívny vplyv.
 - **Prístup:** Prísne riadený podľa zásad „need-to-know“ a „najnižších privilégii“.
 - **Príklady:** Strategické plány, obchodné tajomstvá, výsledky kľúčového výskumu a vývoja.
-

SÚHRN KLASIFIKÁCIE S PRÍKLADMI

Úroveň klasifikácie	Príklad informácie	Opatrenia a prístup
Verejné	Tlačové správy, webová stránka	Prístupné každému
Interné	Interné procesy, pracovné postupy	Prístup len pre zamestnancov
Chránené	Osobné údaje, zmluvy, zákaznícke dáta	Prístup len pre oprávnené osoby, šifrovanie, ochrana heslom
Prísne chránené	Obchodné tajomstvá, strategické plány	Prísna kontrola prístupu, dvojfaktorové overenie, špeciálny režim

ČO JE KATEGORIZÁCIA SIETÍ A IS?

- Je to proces, ktorým sa určuje, **ako dôležitý alebo kritický** je konkrétny systém alebo sieť.
- Vykonáva sa na základe predchádzajúcej klasifikácie informácií, ktoré daný systém spracúva.
- **Odpovedá na otázku:** „Čo by sa stalo, keby tento systém prestal fungovať alebo by boli údaje zneužitú?“

PREČO KATEGORIZOVAŤ SIETE A IS?

- 1. Určenie úrovne ochrany:** Nie každý systém potrebuje rovnakú ochranu. Kategorizácia pomáha nastaviť primerané bezpečnostné opatrenia.
- 2. Optimalizácia nákladov a rizík:** Umožňuje chrániť viac to, čo je hodnotnejšie, a efektívne plánovať investície do bezpečnosti.
- 3. Súlad s legislatívou:** Zákon o kybernetickej bezpečnosti (č. 69/2018 Z. z.) vyžaduje, aby prevádzkovatelia základných služieb vykonali kategorizáciu svojich systémov.

KATEGORIZAČNÉ TRIEDY SIETÍ A IS

Siete a informačné systémy sa zaraďujú do troch kategórií:

- **Kategória I:** Systémy, ktorých ohrozenie nemá žiadny alebo len minimálny negatívny dopad.
- **Kategória II:** Systémy, ktorých ohrozenie môže spôsobiť kybernetický bezpečnostný incident I. stupňa a narušiť činnosť organizácie.
- **Kategória III:** Kľúčové systémy, ktorých ohrozenie môže spôsobiť kybernetický bezpečnostný incident II. a III. stupňa, a teda vážne ohroziť poskytovanie základnej služby alebo bezpečnosť štátu.

KATEGÓRIA I

Zahŕňa systémy, ktoré:

- Spracúvajú informácie klasifikované ako **verejné** (prípadne interné).
- Majú nízke požiadavky na dostupnosť a integritu.
- Ich ohrozenie nemá žiadny negatívny dopad na poskytovanú základnú službu.
- Nie je pri nich potrebné vykonávať kontrolnú činnosť alebo sledovať zodpovednosť používateľov.

KATEGÓRIA II

Zahŕňa systémy, ktoré:

- Spracúvajú informácie klasifikované ako **interné alebo chránené**.
- Majú stredné alebo vysoké požiadavky na dostupnosť a integritu.
- Ich ohrozenie môže spôsobiť citeľný dopad na kontinuitu služieb.
- Je pri nich potrebné identifikovať zodpovednosť za kritické aktivity (napr. administrátorov).
- Často ide o agendové informačné systémy alebo špecializované portály.

KATEGÓRIA III

Zahŕňa systémy, ktoré:

- Spracúvajú informácie klasifikované ako **prísne chránené**.
- Majú vysoké požiadavky na dostupnosť a integritu.
- Ich výpadok alebo poškodenie priamo znemožní poskytovanie základnej služby.
- Sú nevyhnutné pre obranu a bezpečnosť štátu alebo obsahujú utajované skutočnosti.
- Je pri nich potrebné auditovať aktivity všetkých používateľov.

PROCES KATEGORIZÁCIE SIETÍ A IS

- Proces je veľmi podobný klasifikácii aktív a vedie ho vlastník siete/IS v spolupráci s MKB a IT.
- **Kroky zahŕňajú:**
 1. Identifikácia siete alebo IS.
 2. Určenie prístupov a procesov.
 3. Určenie kategórie na základe klasifikácie spracúvaných dát a dopadov.
 4. Oznámenie výsledku MKB pre aktualizáciu Katalógu aktív.
- Kategorizácia sa prehodnocuje minimálne raz ročne alebo pri každej zásadnej zmene.

KLÚČOVÉ ZÁSADY OCHRANY AKTÍV (1/2)

- 1. Dôvernost' (Confidentiality):** Zabezpečiť, aby sa k informáciám dostali iba oprávnené osoby.
- 2. Integrita (Integrity):** Zachovanie správnosti, úplnosti a nezmenenosti údajov.
- 3. Dostupnosť (Availability):** Informácie a systémy musia byť dostupné vtedy, keď ich používateľ potrebuje.
- 4. Zodpovednosť a vlastníctvo:** Každé aktívum musí mať určeného vlastníka, ktorý zaň zodpovedá.

KLÍČOVÉ ZÁSADY OCHRANY AKTÍV (2/2)

- 5. Kontrola prístupu (Need-to-know):** Každý má mať prístup len k tomu, čo naozaj potrebuje pre svoju prácu.
- 6. Auditovateľnosť:** Musí byť možné spätne overiť, kto, kedy a ako s informáciou narábal.
- 7. Ochrana počas celého životného cyklu:** Od vzniku aktíva až po jeho bezpečné zničenie.
- 8. Zvyšovanie povedomia:** Každý zamestnanec je súčasťou bezpečnostného reťazca a musí byť školený.
- 9. Súlad s legislatívou:** Ochrana musí byť v súlade so zákonmi (GDPR, ZoKB) a normami.

POVINNOSŤ ZAMESTNANCA CHRÁNIŤ AKTÍVA

Táto povinnosť vyplýva z viacerých zdrojov:

- **Z pracovnej zmluvy a Zákonníka práce** (povinnosť riadne hospodáriť so zverenými prostriedkami a zachovávať mlčanlivosť).
- **Z vnútorných predpisov organizácie** (bezpečnostná politika, smernice).
- **Z legislatívy** (GDPR, Trestný zákon, Zákon o kybernetickej bezpečnosti).
- **Z logiky dôvery a lojality** voči zamestnávateľovi.
- „Chrániť informačné aktíva nie je voľba – je to mojou pracovnou, právnou a morálnou povinnosťou.“

ZÁVER: PREČO BY MAL KAŽDÝ POZNAŤ TIETO PRAVIDLÁ?

Pretože zamestnanci:

- denne pracujú s citlivými informáciami a systémami,
- znalosť pravidiel im pomáha konať správne a bezpečne,
- znižuje sa tak riziko ľudských chýb a bezpečnostných incidentov,
- umožňuje im to zodpovedne pristupovať k svojej úlohe v organizácii.

PRÍKLAD Z PRAXE č. 1: ÚNIK CITLIVÝCH DÁT

- **Situácia:** Zamestnanec HR oddelenia poslal pracovné zmluvy (klasifikované ako „Chránené“) bežným, nešifrovaným e-mailom externej firme na tlač.
- **Problém:** Zamestnanec ignoroval klasifikáciu. E-mail bol zachytený pri phishingovom útoku.
- **Následky:**
 - Únik osobných údajov a porušenie GDPR.
 - Povinnosť hlásenia incidentu úradu.
 - Strata dôvery zamestnancov a disciplinárne konanie.
- **Poučenie:** Zamestnanec mal vedieť, že ide o chránené údaje a použiť zabezpečený kanál na prenos.

PRÍKLAD Z PRAXE Č. 2: VÝPADOK KRITICKÉHO SYSTÉMU

- **Situácia:** Interný systém na evidenciu objednávok nebol nikdy oficiálne kategorizovaný. IT ho považovalo za „bežný systém“.
 - **Problém:** Systém zlyhal. Keďže nebol označený ako kritický, jeho obnova nemala prioritu.
 - **Následky:**
 - Zastavenie výroby na 2 dni.
 - Finančná strata v desiatkach tisíc eur.
 - Poškodenie vzťahov s obchodnými partnermi.
 - **Poučenie:** Správna kategorizácia by vopred určila jeho kritickosť, priradila mu vyššiu prioritu obnovy a predišla by takýmto vysokým stratám.
-

BEZPEČNÁ VÝMENA INFORMÁCIÍ (TLP)

- Na podporu bezpečnej výmeny informácií (napr. s jednotkou CSIRT) sa používa

Traffic Light Protocol (TLP).

- Ide o metódu klasifikácie informácií pomocou farebných označení, ktorá uľahčuje ich zdieľanie a určuje pravidlá ďalšej distribúcie.
- Je to najpoužívanejší spôsob klasifikácie neutajovaných informácií v bezpečnostnej komunite.

ZÁVEREČNÉ ZHRNUTIE

- Každé informačné aktívum musí mať **vlastníka**.
- Všetky aktíva musia byť **klasifikované** podľa ich citlivosti.
- Všetky systémy a siete musia byť **kategorizované** podľa ich kritickosti.
- Ochrana informácií je **zákonná a pracovná povinnosť** každého zamestnanca.
- Neznalosť pravidiel **neospravedlňuje** a môže viesť k vážnym následkom pre organizáciu aj jednotlivca.

ĎAKUJEM ZA POZORNOST

- Otázky a odpověde