INFORMAČNÁ A KYBERNETICKÁ BEZPEČNOSŤ

SLOVENSKÝ VODOHOSPODÁRSKY PODNIK, štátny podnik, 2022

SLOVENSKÝ
VODOHOSPODÁRSKY
PODNIK, štátny podnik

Prečo je potrebné riešiť bezpečnosť?

- Nie je to len o informačných technológiách a informačných systémoch
- Vedúcich pracovníkov sa informačná a kybernetická bezpečnosť týka
- Dôležité sú pravidlá, postupy, tréning a školenia
- Nejedná sa o jednorazovú činnosť je to proces

- Kľúčom sú ľudia – je to viac o práci s ľuďmi
  ako s počítačom

Zákonné požiadavky

- **zákon 69/2018 Z. z. o kybernetickej bezpečnosti**
- zákon 95/2019 Z. z. o informačných technológiách vo verejnej správe
- Interný predpis – Organizačná smernica 3/2020 INFORMAČNÁ A KYBERNETICKÁ BEZPEČNOSŤ

- pôsobnosť v oblasti kybernetickej bezpečnosti vykonáva **NÁRODNÝ BEZPEČNOSTNÝ ÚRAD**

- Národná jednotka CSIRT plní úlohu ústredného a kontrolného orgánu

- MŽP – ústredný orgán

- SVP, š.p. – prevádzkovateľ základnej služby: Voda a atmosféra/Vodné stavby

Informačná bezpečnosť – pojem

- Zachovanie **dôvernosti**, **integrity** a **dostupnosti** údajov

Dôvernosť – informácia je chránená pred prezradením neoprávneným osobám

Integrita – údaje sú chránené pred náhodnou alebo úmyselnou modifikáciou

Dostupnosť – dáta sú prístupné v okamihu ich potreby

Klasifikácia dokumentov

- V- Verejné dokumenty- nevyžaduje zvláštnu ochranu, oznamy na webovej stránke, povinne publikované informácie
- I – Interné dokumenty- prístupné pre všetkých zamestnancov, smernice, interné predpisy
- CH- Chránené dokumenty- obsahujú dôležité informácie o ochrane a bezpečnosti podniku a jeho aktív, musia sa definovať vymedzené skupiny osôb
- PCH- Prísne chránené dokumenty- obsahujú informácie osobitného určenia a významu, ktorých zverejnenie, strata, poškodenie môže spôsobiť incident. Určené jednotlivým vybraným používateľom

Zoznam oprávnených osôb

Klasifikačný stupeň	Označenie	Klasifikačné kritéria	Oprávnené osoby
I- Interné	Interné	Neoprávnený prístup k informáciám môže podniku spôsobiť menšie poškodenie alebo ťažkosti	Všetci zamestnanci a vybrané tretie strany
CH- Chránené	Chránené	Neoprávnený prístup k informáciám môže značne poškodiť podnik alebo môže poškodiť jeho povesť	Vedúci odboru/oddelenia a vybrané tretie strany
PCH- Prísne chránené	Prísne chránené	Neoprávnený prístup k informáciám môže spôsobiť katastrofálne (nenapraviteľné škody) na podnik alebo na jeho povesť	Odborný riaditeľ PR alebo riaditeľ OZ

Prenos informácií

Komunikačný kanál	verejné	interné	chránené	prísne chránené
e-mail	Bez obmedzenia	Vo vnútornej mailovej komunikácií podniku bez obmedzenia. Pri posielaní mailov mimo podnik len v zašifrovanej podobe.	Len v zašifrovanej podobe	Len v zašifrovanej podobe
ftp	Bez obmedzenia	Vo vnútornej ftp komunikácií podniku bez obmedzenia. Pri posielaní súborov mimo podnik len v zašifrovanej podobe.	Len v zašifrovanej podobe	Len v zašifrovanej podobe
prostredníctvom internetu	Bez obmedzenia	Vo vnútornom Intranete podniku bez obmedzenia. Mimo podnik len cez zabezpečené https pripojenie.	Zakázané	Zakázané
telefón hovor	Bez obmedzenia	Bez obmedzenia	Bez obmedzenia	Zakázané
telefón SMS	Bez obmedzenia	Bez obmedzenia	Bez obmedzenia	Zakázané
prenosné média	Bez obmedzenia	V rámci podniku bez obmedzenia. Mimo len v zašifrovanej podobe.	Len v zašifrovanej podobe	Len v zašifrovanej podobe
diskusné fóra	Bez obmedzenia	Zakázané	Zakázané	Zakázané
sociálne siete	Bez obmedzenia	Zakázané	Zakázané	Zakázané
pošta	Bez obmedzenia	Bez obmedzenia	Doporučene	Do vlastných rúk

Bezpečnosť

Je založená na ochrane **aktív**

(aktíva – dáta podniku)

pred rôznymi **hrozbami**

(hrozby – krádež, únik údajov)

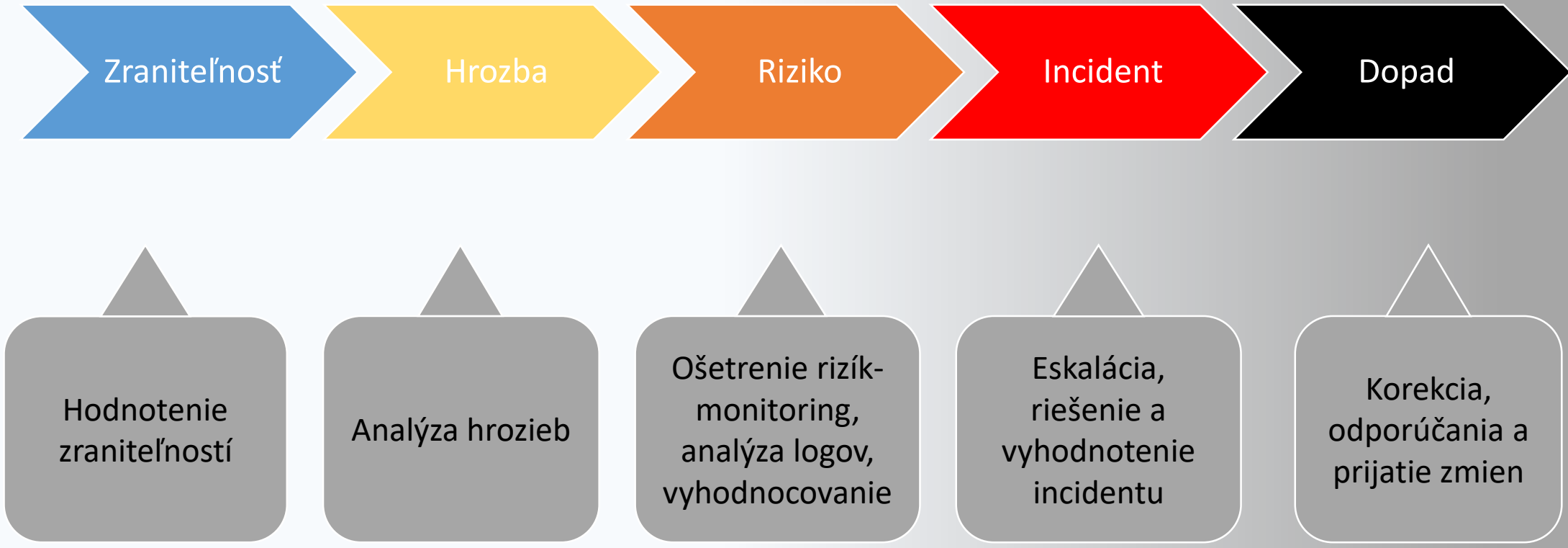
pri určitej **zraniteľnosti**

(zraniteľnosť – slabé miesto)

V prípade ak bude **hrozba** voči **aktívu** naplnená (zraniteľnosť zneužitá hrozbou) spôsobí **bezpečnostný incident**

Bezpečnostný incident – je akákoľvek udalosť, ktorá ma z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky negatívny vplyv na **aktíva** a spôsobí **ujmu**

Bezpečnostný incident



Bezpečnostný incident

Neautorizované prihlásenie do informačného systému:

- Po prekonaní fyzických prekážok, môže dôjsť k neautorizovanému vstupu do informačného systému
- Únik prihlasovacích údajov (prezradenie, útok z vonku)

Opatrenia minimálne:

- Zmena zneužitého prihlasovacieho mena a hesla
- Používajte silné heslo; čím dlhšie, tým lepšie
- Heslá s nikým nezdieľajte
- Dodržiavajte prijatú politiku hesiel
- **Vždy nahlásiť incident nadriadenému**

Hrozby

1
- Získať citlivé osobné informácie
- (adresa, dátum narodenia, rodné číslo, údaje o platobnej karte)

2
- Získať prihlasovacie údaje
- Do informačných systémov obete

3
- Nainštalovať podvodné aplikácie
- Do počítača, tabletu, mobilného zariadenia

4
- Spustiť škodlivý kód
- Z prílohy, alebo návštevou falošnej stránky

Typy útokov

- PHISHING – vylákať cez email, alebo webovú stránku
  osobné údaje, heslá alebo údaje o platobnej karte

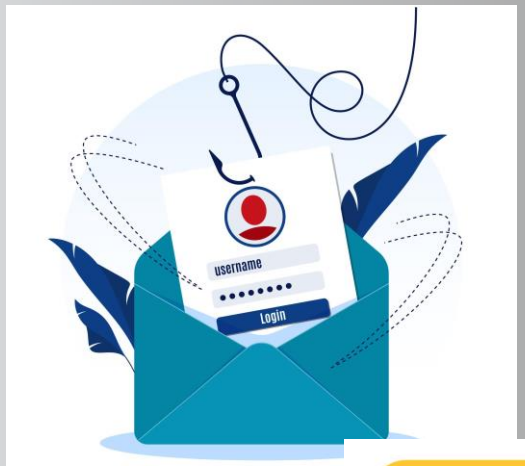
- SMISHING – podvodné SMS, klikni a zaplať
- VISHING – podvodné telefonáty z banky, podpora Microsoft a účelom získania údajov, hesiel

Časté chyby

- Slabé heslá
- Rovnaké heslo vo viacerých účtoch
- Používanie služobných prostriedkov na súkromné účely

Ako sa k Vám hrozba dostane

- phishingové emaily
- nebezpečné webové stránky
- reklamy vo webových stránkach
- upload / download dokumentov
- nezabezpečená sieť
- fyzický prístup – USB kľúč

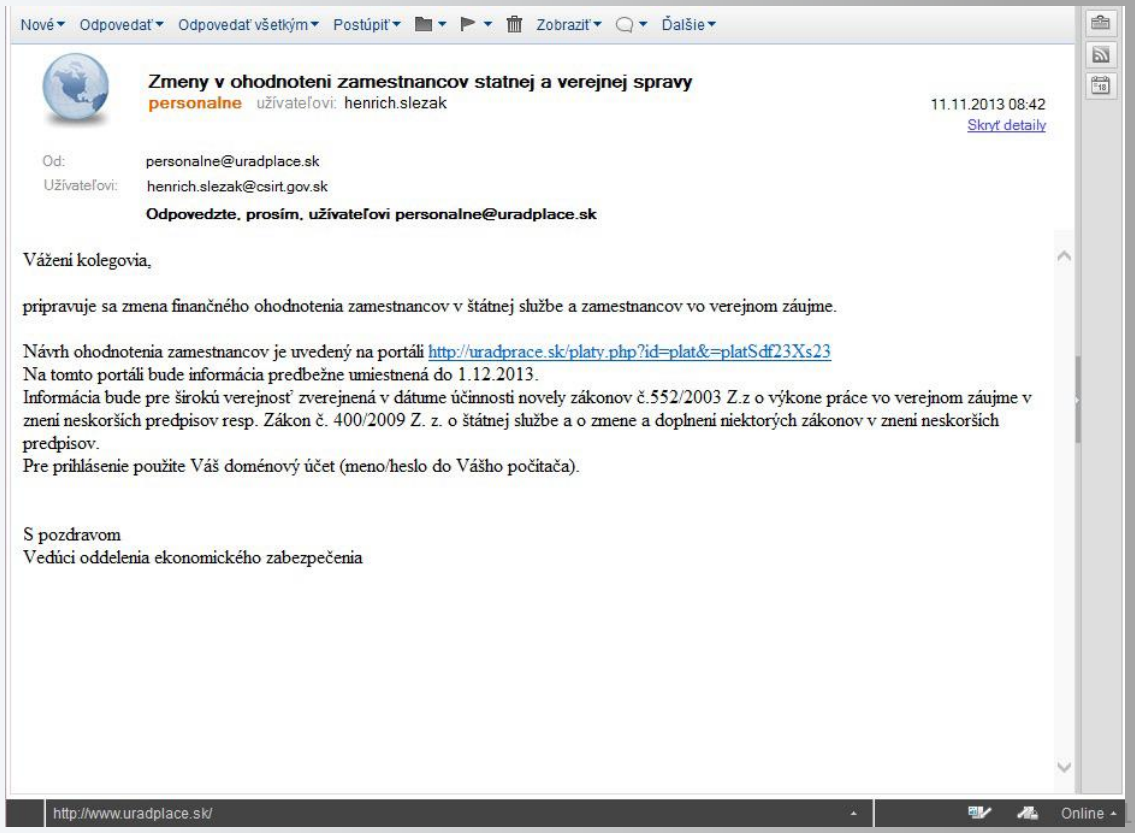


Ako rozpoznať škodlivú aktivitu

- Email, SMS alebo podvodný telefonát z banky- podvodníci sa snažia vyvolať strach, text je väčšinou urgencia, alebo fantastická novinka (rýchlo klikni)

- Ak je email podozrivý overím jeho pravosť telefónom, alebo na webe

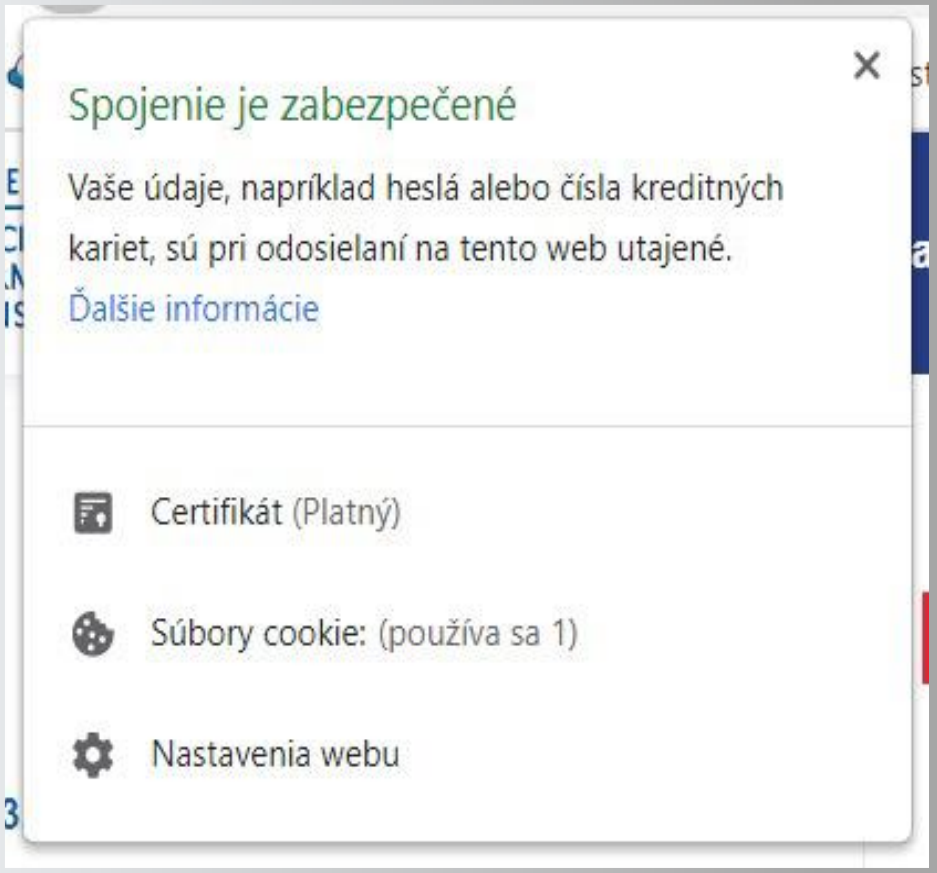
- **Na prílohy, alebo webové odkazy <u>neklikám!</u>** (považuje sa za bezpečnostný incident)



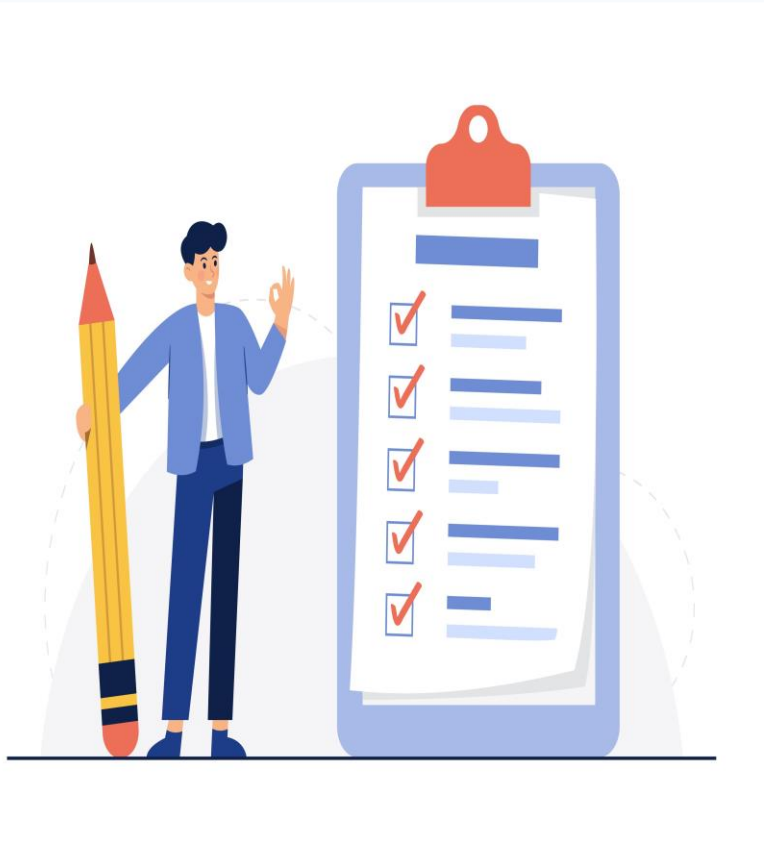
Bezpečné prehliadanie webu

- HTTPS
- poskytuje záruku, že stránka ku ktorej sa pripájate, je legitímna

- všetky údaje posielané medzi touto stránkou sú šifrované, teda nikto ich "po ceste" nemôže odpočúvať



Odporúčania na záver



- Vyhodnocujte podozrivé emailové správy
- Aktualizujte operačný systém a aplikácie
- Používajte silné heslá a bezpečne ich ukladajte
- Používajte antivírusový program
- Šifrujte údaje pri ich ukladaní a prenose
- Používajte bezpečnostné nastavenia webových prehliadačov
- Identifikujte a hláste bezpečnostné incidenty