



Digitálna
koalícia

DIGITÁLNA BUDÚCNOSŤ



Spolufinancovaný
Európskou úniou



PROGRAM
SLOVENSKO



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY



Kybernetická bezpečnosť

Dátum : 23.01.2025, Trnava

Agenda



1. Ciele seminára vo väzbe na RIS3 2021+
2. Špecifiká DT pre prioritnú oblasť *Kybernetická bezpečnosť*
 - a) existujúce ohrozenia, urgentnosť ich riešenia formou DT
 - b) hlavné zmeny vyvolané realizáciou DT



3. Šesť pilierov transformácie prioritnej oblasti
4. Digitálne a zelené zručnosti pre kľúčové povolania prioritnej



5. Zhrnutie cieľov seminára – odporúčenia ďalšieho postupu



Ciele seminára vo väzbe na RIS3 2021+





Cieľ seminára

- Pochopenie KB prostredia (Cybersecurity Landscape)
- Poskytnutie základných informácií ohľadom integrácie KB do iniciatív digitálnej transformácie
- Ukázanie prepojenia digitálnych zručností s KB

Časový rámec

13:00 – 13:50 – 1. časť seminára

13:50 – 14:00 – Coffee break

14:00 – 14:50 – 2. časť seminar

14:50 – 15:00 – Diskusia



Špecifiká digitálnej transformácie pre kybernetickú bezpečnosť

Existujúce ohrozenia, urgentnosť ich riešenia





Digitalizácia zasahuje už dnes každú oblasť života (a biznisu...)

Žiadna organizácia nie je “**osamelý ostrov**”

Kybernetický **incident** dokáže zabíjať

Nestabilná a nepredvídateľná **geopolitika**

Terorizmus

Dopady kybernetických incidentov na organizáciu

Priame finančné straty. Dôsledok nákladov na obnovu systémov a dát. Pokuty uložené regulačnými orgánmi.

Nepriame budúce straty. Dôsledok výpadku alebo zníženia produkcie.

Strata reputácie a dôvery.

Strata intelektuálneho vlastníctva.

Dopady na zamestnancov. Obavy o stabilitu pracovného miesta. Reputačné problémy. Obavy o plnenie záväzkov zo strany zamestnávateľa (platy).





Bez pochopenia základného konceptu kybernetickej bezpečnosti, nebude organizácia schopná nastavovať vhodné opatrenia a zlyhá.

Prístup ku kybernetickej bezpečnosti musí byť **top-down** – vedenie organizácií musí pochopiť, že zodpovednosť je neprenosná a vynucovať pravidlá sa musia „z hora“.

Iba vedenie dokáže **alokovať** potrebné zdroje.

Prístup **bottom-up** nefunguje.

Nová legislatíva v oblasti kybernetickej bezpečnosti

Od **Q1/2025** nový zákon o kybernetickej bezpečnosti

Transpozícia smernice NIS2

Zásadné **rozšírenie** počtu regulovaných subjektov

Prepracovaný **system sankcií**

do 10.000.000 EUR alebo 2% globálneho obratu

Nová legislatíva v oblasti kybernetickej bezpečnosti

9 druhov sankcií + „**rozkazné konanie**“ (do 10.000 EUR)

Povinné audity každé 2 roky (*5 rokov)

Trestno právna zodpovednosť pre štatutárov

Zákaz výkonu funkcie pre štatutárov



Špecifiká digitálnej transformácie pre kybernetickú bezpečnosť

Hlavné zmeny vyvolané realizáciou DT



Sedem hlavných zmien vyvolaných realizáciou DT

1. Rozšírenie digitálneho priestoru organizácie

Zvýšený počet digitálnych aktív, zavádzanie cloudových služieb, IoT zariadení a ďalších technológií zvyšuje počet zariadení a systémov, ktoré je potrebné chrániť.

Zmena hraníc siete spôsobí, že tradičné perimetrické bezpečnostné modely sú menej efektívne v prostredí hybridných a cloudových infraštruktúr.



Sedem hlavných zmien vyvolaných realizáciou DT

2. Technologické závislosti

Kritická infraštruktúra organizácie. Digitálna transformácia spôsobí, že činnosti organizácie sú čoraz viac závislé od dostupnosti IT systémov a dát.

Výpadky v dôsledku kybernetických útokov, môžu spôsobiť vážne narušenie prevádzky.

Sedem hlavných zmien vyvolaných realizáciou DT

3. Nové riziká a zraniteľnosti

Komplexita systémov, spôsobená integráciou rôznych technológií a služieb, prináša nové hrozby a zvyšuje riziko ich zneužitia.

Prepájanie rôznych typov infraštruktúr a prostredí (IT, OT, IoT) prináša nové vektory útokov, čím zvyšuje riziko vzniku kybernetických incidentov a komplikuje ochranu pred nimi.

Používanie **neautorizovaných**, alebo nedostatočne otestovaných nástrojov a aplikácií.



Sedem hlavných zmien vyvolaných realizáciou DT

4. Zmena pracovného prostredia

Práca na diaľku a používanie vlastných zariadení (**BYOD**) si vyžadujú nové prístupy k autentifikácii a ochrane dát.

Mobilita zamestnancov vyvoláva zvýšenú potrebu ochrany prístupu k systémom mimo firemnej siete.



Sedem hlavných zmien vyvolaných realizáciou DT

5. Zvýšený tlak na súlad s reguláciami

Nové regulačné požiadavky – zákon o kybernetickej bezpečnosti (NIS2) kladie na množstvo organizácií vysoké požiadavky na ochranu dát a infraštruktúry.

Audit a posúdenie súladu (compliance) ako nové regulačné požiadavky, vyvolané digitálnou transformáciou, budú vyžadovať zavedenie nových politík, procesov a monitorovacích nástrojov.



Sedem hlavných zmien vyvolaných realizáciou DT

6. Využitie AI a automatizácie

Pri zavádzaní AI riešení je potrebné integrovať bezpečnostné opatrenia na ochranu pred manipuláciou modelov a dát, ktoré tieto aplikácie využívajú.

AI môže podporiť odolnosť organizácie simuláciou bezpečnostných incidentov a optimalizáciou reakčných procesov v rámci prevádzkových a obchodných činností.

Automatizácia procesov vyžaduje dôkladnú správu prístupov a zabezpečenie komunikačných kanálov medzi systémami, aby sa minimalizovalo riziko kybernetických útokov.

Sedem hlavných zmien vyvolaných realizáciou DT

7. Nové spôsoby ochrany a riadenia rizík

Zero-trust – „nikomu never“ – prístup založený na nulovej dôvere v užívateľov, zariadenia, aplikácie a dáta, až dovedy, pokiaľ sa nepreukáže ich dôveryhodnosť.

Riadenie rizík organizácie ako neoddeliteľná súčasť strategického plánovania a operatívneho rozhodovania, zaisťujúca identifikáciu, hodnotenie a zmierňovanie potenciálnych hrozieb pre zabezpečenie kontinuity a stability činností.



Hlavné zmeny sú zamerané na budovanie kybernetickej odolnosti (resillience)



Schopnosť **odolať** a rýchlo sa **zotaviť** z kybernetických útokov

Schopnosť **odolať** kybernetickým hrozbám

Schopnosť **prispôbiť** sa neustále sa meniacemu prostrediu

Neustále sa **vzdelávať** v oblasti KB



Šesť pilierov transformácie DT z pohľadu kybernetickej bezpečnosti



Budovanie kybernetickej odolnosti (resillience)

Ľudia. Systematické vzdelávania šírenie povedomia o KB.

Organizácia. Aktívna podpora vedenia. Bezpečnostné politiky.
Kultúra bezpečnosti.

Infraštruktúra. Segmentácia sietí. Používanie vhodných technológií.

Aplikácie. Bezpečnostné testovanie. Aktualizácie. Prístup Zero-Trust.

Dáta. Klasifikácia. Šifrovanie. Zálohovanie. Kontrola prístupu.

Procesy. Automatizácia bezpečnostných procesov. Štandardizované postupy. Testovanie a aktualizácie bezpečnostných plánov.



Dopady KB na šesť pilierov DT

1. Ľudia

Školenia a zvyšovanie povedomia zamestnancov sú kľúčové, pretože predstavujú prvú líniu obrany. Investícia do ich vzdelávania im umožní rozpoznať podozrivé správanie a znižuje riziko ich nebezpečného konania.

Bezpečnostné zásady a povinnosti by mali byť jasne a konkrétne zakotvené v pracovných zmluvách a interných predpisoch organizácie.



2. Organizácia

Budovanie kultúry kybernetickej bezpečnosti znamená integráciu bezpečnostného povedomia a zodpovednosti do každodenných činností všetkých zamestnancov.

Manažment musí zabezpečiť jasné definovanie úloh a zodpovedností, aby všetky oddelenia rozumeli svojej úlohe pri ochrane dát a systémov.

Manažment musí vytvárať podmienky pre kybernetickú bezpečnosť, vrátane jasnej podpory a alokácie potrebných zdrojov na ochranu dát, systémov a procesov.



3. Procesy

Automatizácia bezpečnostných procesov umožňuje monitorovanie a detekciu hrozieb v reálnom čase, čím zaisťuje rýchlu reakciu na podozrivé aktivity.

Zavedenie štandardizovaných postupov, ako je metodika ISO 27001 pre riadenie informačnej bezpečnosti, umožňuje organizáciám efektívne nastaviť a udržiavať systematické procesy na ochranu dát.

Pravidelné testovanie a aktualizácia plánov, ako je napr. Disaster Recovery Plan (DRP), spolu so simuláciami kybernetických útokov, overujú pripravenosť organizácie na zvládanie incidentov.



4. Infraštruktúra

Segmentácia siete, ktorá spočíva v logickom oddelení jednotlivých častí siete na základe ich kategorizácie, výrazne znižuje efektivitu rôznych typov útokov.

Nasadenie bezpečnostných riešení, ako sú EDR (Endpoint Detection and Response), SIEM (Security Information and Event Management) alebo XDR (Extended Detection and Response), umožňuje efektívnu detekciu, reakciu a izoláciu kybernetických hrozieb.

Pravidelné penetračné testy a skenovanie zraniteľností pomôžu s identifikáciou slabých miest v infraštruktúre, ktoré by mohli byť zneužitú útočníkmi.

5. Aplikácie

Bezpečnostné testovanie aplikácií, vrátane pravidelného penetračného testovania a hodnotenia zraniteľností, umožňuje identifikovať a odstrániť slabé miesta v softvéri.

Pravidelné aktualizácie a bezpečnostné záplaty aplikácií sú nevyhnutné na ochranu pred najnovšími kybernetickými hrozbami.



6. Dáta

Klasifikácia všetkých dát a šifrovanie citlivých dát pomáhajú minimalizovať riziko ich zneužitia v prípade kybernetického útoku.

Pravidelné zálohovanie dát, vrátane ich ukladania na oddelené a offsite úložiská, zaisťuje možnosť obnovy dát po útoku (jediné funkčné opatrenie proti ransomware).

Kontrola prístupu prostredníctvom prísnych pravidiel, ako je princíp minimálnych oprávnení, zaisťuje, že k citlivým dátam majú prístup iba autorizované osoby



Digitálne a zelené zručnosti pre klúčové povolania vo vzťahu ku kybernetickej bezpečnosti



Vyhláška 492/2022 o znalostných štandardoch

Požiadavky na „digitálne zručnosti“ pre oblasť kybernetickej bezpečnosti definuje vyhláška 492/2022 o znalostných štandardoch.

Kategórie používateľov:

- laik
- odborný zamestnanec
- manažér
- IT manažér
- informatik
- zamestnanec v kybernetickej bezpečnosti
- manažér kybernetickej bezpečnosti
- audítor a výskumník kybernetickej bezpečnosti



Digitálne zručnosti vo vzťahu ku kybernetickej bezpečnosti

Odborný zamestnanec - používateľ, ktorý pri výkone povolania využíva sieť alebo informačný systém (úroveň B1.1)

- porozumieť vybraným základným pojmom kybernetickej bezpečnosti
- porozumieť svojej úlohe a zodpovednosti v systéme kybernetickej bezpečnosti
- chápať význam informačných aktív s ktorými zamestnanec pracuje
- porozumieť potrebe ochrany informácií a informačných aktív
- osvojiť si základné pravidlá bezpečnej práce s IKT
- rozpoznať incident a vedieť naň správne reagovať
- porozumieť bezpečnostným politikám a používaniu bezpečnostných mechanizmov v pracovných procesoch



Digitálne zručnosti vo vzťahu ku kybernetickej bezpečnosti

Informatik - zamestnanec zodpovedný za poskytovanie IT služieb, návrh, implementáciu, obstaranie, prevádzku, údržbu a osudzovanie IKT (úroveň B2.2)

- doplniť vlastné odborné znalosti špecificky pre oblasť kybernetickej bezpečnosti
- porozumieť podstate bezpečnostných požiadaviek na IKT a IT služby
- porozumieť zraniteľnostiam, hrozbám a rizikám spojeným s používanými IKT a IT službami
- nadobudnúť schopnosť navrhovať, implementovať, udržiavať a prevádzkovať mechanizmy na naplnenie bezpečnostných požiadaviek na IKT a IT služby
- nadobudnúť zručnosť kvalifikovane komunikovať a spolupracovať so špecialistami kybernetickej bezpečnosti, formulovať problémy, posudzovať a implementovať navrhované opatrenia.



Digitálne zručnosti vo vzťahu ku kybernetickej bezpečnosti

Manažér kybernetickej bezpečnosti - riadiaci zamestnanec špecializovaný na oblasť bezpečnosti informácií a riadenia rizík kybernetickej bezpečnosti, vlastníci bezpečnostných procesov (úroveň C1)

- vytvoriť rámec riadenia kybernetickej bezpečnosti v organizácii
- riadiť procesy súvisiace s informačnou a kybernetickou bezpečnosťou v organizácii
- formulovať návrhy a odporúčania na obstaranie, implementáciu, prevádzku a vyhodnocovanie bezpečnostných mechanizmov a riešení a navrhovať a manažovať procesy riadenia rizík v informačnej a kybernetickej bezpečnosti
- navrhovať, implementovať, udržiavať a prevádzkovať bezpečnostné mechanizmy a riešenia
- znalosti o právnych a etických požiadavkách na zaručenie bezpečnosti informačných aktív,
- navrhovať a prezentovať bezpečnostné stratégie, bezpečnostné politiky a bezpečnostnú architektúru
- znalosti o technikách a metódach vyhodnocovania efektívnosti bezpečnostných mechanizmov a riešení a schopnosť uplatňovať ich v procesoch organizácie



Digitálne zručnosti vo vzťahu ku kybernetickej bezpečnosti

Audítor a výskumník kybernetickej bezpečnosti - odborný zamestnanec špecializovaný na oblasť výskumu alebo posudzovania kybernetickej bezpečnosti, analýzy rizík, testovania a vyhodnocovania efektivity bezpečnostných opatrení, posudzovania zhody a súladu (úroveň C1)

- nadobudnúť schopnosti v rozsahu podľa predchádzajúcich cieľov platných pre všetky ostatné kategórie
- vykonať audit kybernetickej bezpečnosti a posúdiť efektívnosť prijatých bezpečnostných opatrení



Zhrnutie prínosov a rizík DT v oblasti KB – návrh ďalšieho postupu



1. Zlepšenie kybernetickej ochrany

Využitie moderných technológií, ako je automatizované monitorovanie a umelá inteligencia, umožňuje rýchlu detekciu a reakciu na incidenty, čím sa znižuje riziko finančných strát a poškodenia reputácie.





2. Zvýšená efektívita procesov

Automatizácia bezpečnostných kontrol a štandardizácia procesov zvyšujú efektívnosť, eliminujú manuálne chyby a urýchľujú reakciu na kybernetické hrozby.



3. Zvýšená bezpečnosť dát

Šifrovanie, zálohovanie a zlepšená správa prístupu spoločne minimalizujú riziko úniku, straty či neoprávneného prístupu k citlivým dátam.

4. Posilnenie kultúry kybernetickej bezpečnosti

Školenia zamestnancov a proaktívny prístup k bezpečnosti posilňujú povedomie o hrozbách, bezpečnostné návyky a dôveru klientov i partnerov.



1. Komplexnosť a náklady na implementáciu

Digitálna transformácia môže byť finančne a časovo náročná, pričom nesprávna implementácia môže vytvoriť nové riziká a ohroziť bezpečnosť organizácie. KB je neoddeliteľnou súčasťou všetkých procesov DT.



2. Technologická závislosť

Vyššia automatizácia zvyšuje závislosť od technológií, čo môže viesť k problémom pri technických zlyhaniach alebo útokoch a zároveň zvyšuje nároky na pravidelnú údržbu a prevádzkové náklady.

3. Odolnosť voči zmenám u zamestnancov

Odolnosť voči zmenám u zamestnancov môže spôsobiť ťažkosti s adaptáciou na nové technológie a procesy, čo dočasne znižuje produktivitu a oslabuje dodržiavanie bezpečnostných politík.




4. Riziko neúmyselných chýb

Nesprávne nastavenia, nezabezpečené konfigurácie a nedostatočné testovanie môžu vytvoriť bezpečnostné diery a vystaviť organizáciu neočakávaným hrozbám.



Odporúčania ďalšieho postupu – projekt Digitálna budúcnosť



V rámci plánovaných konferencií ktoré sú súčasťou projektu **získať informácie o možnostiach financovania** interných projektov/častí projektov z Plánu obnovy a Štrukturálnych fondov (PSK).

V rámci prebiehajúceho projektu **požiadať o vykonanie auditu digitálnych zručností** prostredníctvom služby Meranie digitálnej zrelosti ľudského kapitálu – dostupnosť v roku 2025



Odporúčania ďalšieho postupu – vaša organizácia

“Identifikujte sa“, nečakajte na štát, nemusí sa to vyplatiť.

Zistite ako na tom ste. Objednajte si u skúsenej konzultačnej firmy rozdielovú analýzu (GAP) na identifikovanie rozdielov (realita vs. regulačné požiadavky / odporúčania normy).

Identifikujte riziká. Objednajte si u skúsenej konzultačnej firmy analýzu rizík, aby ste boli schopní začať kybernetickú bezpečnosť systematicky riadiť.

Vytvorte si roadmapu na implementáciu opatrení z rozdielovej a rizikovej analýzy.

Ak sa vás regulácie netýkajú, začnite riadiť kybernetickú bezpečnosť **dobrovoľne**, vyplatí sa to. **Kybernetickú bezpečnosť vnímajte ako investíciu, nie náklad.**



HODNOTENIE SEMINÁRA





ĎAKUJEM ZA POZORNOST





Digitálna
koalícia

DIGITÁLNA BUDÚCNOSŤ



Spolufinancovaný
Európskou úniou



PROGRAM
SLOVENSKO



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY