ZODPOVEDNOSTNÉ VZŤAHY V KYBERNETICKEJ BEZPEČNOSTI

MODUL 4:
Zodpovednostné vzťahy osôb pre vybrané bezpečnostné role, Časť. I

JUDr. Michal Rampášek

CUSEC

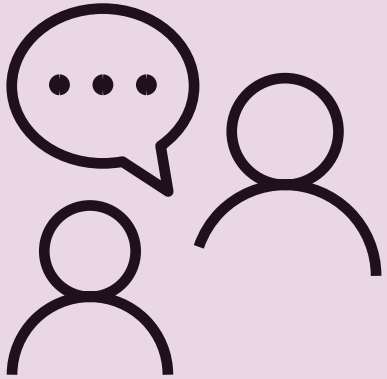
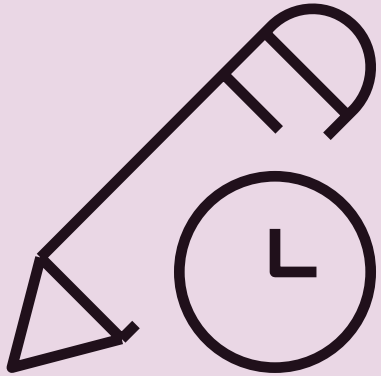
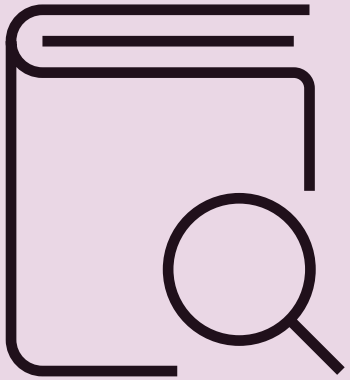
Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality

Financované Európskou úniou Next Generation EU prostredníctvom
Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17R05-04-V01-00002

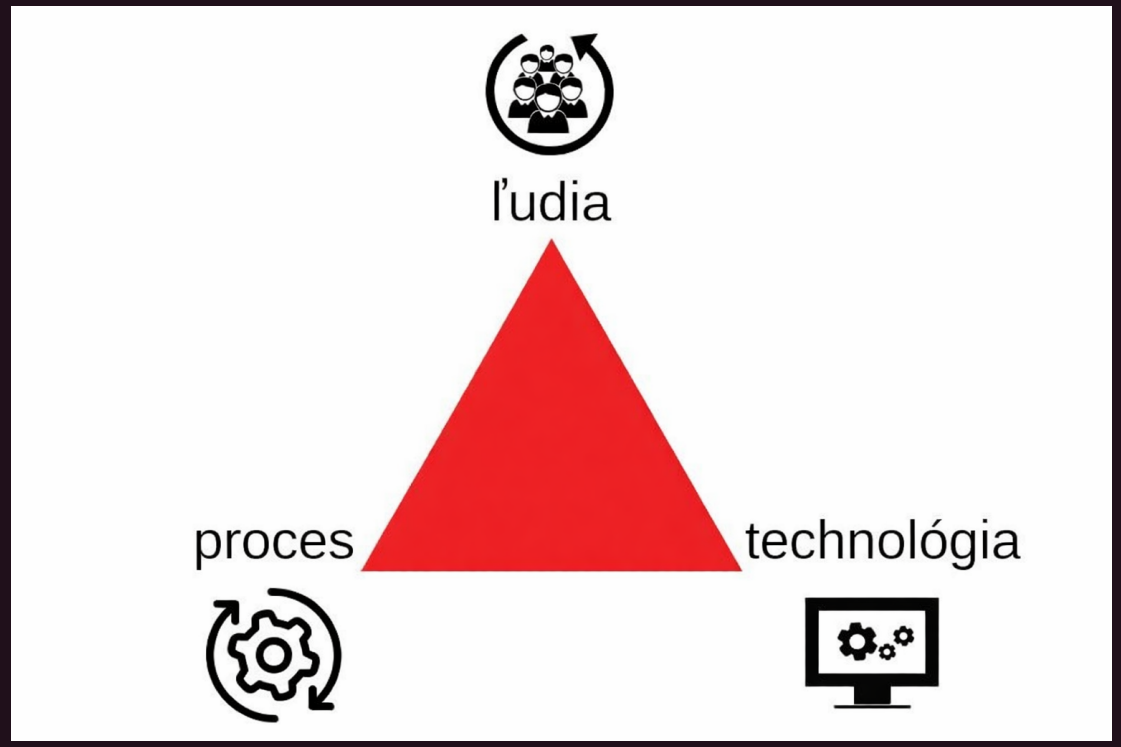
ÚVOD

- European Cybersecurity Skills Framework (ECSF)
- Vyhláška NBÚ č. 492/2022 Z. z.
- Prepojenie ECSF s požiadavkami ZoKB
- Bezpečnostné role a AI

ÚVOD

Zlatý trojuholník



ECSF = l'udia

Úlohy, role, a zodpovednosti v ZoKB

- Podľa § 20 ods. 4 písm. g) ZoKB bezpečnostné opatrenia musia zahŕňať aj **určenie a pridelenie úloh, rolí a zodpovednosti** podľa podmienok prevádzkovateľa základnej služby a **zabezpečenie primeraného vzdelávania a prešk**o**lovania pre všetky zavedené roly**

- Podľa § 20 ods. 4 písm. g) ZoKB bezpečnostné opatrenia musia zahŕňať aj **vzdelávanie a budovanie bezpečnostného povedomia** v oblasti kybernetickej bezpečnosti.

Európsky rámec zručností v oblasti kybernetickej bezpečnosti (ECSF)

- Praktický nástroj na **podporu identifikácie a formulovania úloh, kompetencií, zručností a vedomostí spojených s úlohami rolí** v oblasti kybernetickej bezpečnosti.
- ECSF poskytuje profily **12 typických pracovných pozícií** v oblasti kybernetickej bezpečnosti.
- Hlavným účelom ECSF je vytvoriť **spoločné porozumenie** medzi jednotlivcami, zamestnávateľmi a poskytovateľmi vzdelávacích programov v celej EÚ.

Európsky rámec zručností v oblasti kybernetickej bezpečnosti (ECSF)

- **Hlavným účelom ECSF je vytvoriť spoločné porozumenie medzi jednotlivcami, zamestnávateľmi a poskytovateľmi vzdelávacích programov v celej EÚ.**
- Pre každú rolu definuje:

1. Alternatívny názov / Alternative Title(s)
2. Výstupy / Deliverable(s)
3. Hlavné úlohy / Main task(s)
4. Kľúčové zručnosti / Key skill(s)
5. Kľúčové vedomosti / Key knowledge
6. Kompetencie / e-Competences

vedomosti –poznatky nadobudnuté v priebehu vzdelávania, učenia sa alebo získané skúsenosťou,

zručnosti – schopnosti jednotlivca uplatňovať vedomosti v praxi a využívať ich na plnenie úloh a riešenie problémov,

kompetencie – preukázané schopnosti jednotlivca použiť vedomosti, zručnosti a osobné, sociálne a/alebo metodologické schopnosti v pracovných alebo študijných situáciách a v odbornom a osobnom rozvoji,

STN EN 16234 Rámec e-kompetentnosti (e-CF)

European Cybersecurity Skills Framework (ECSF) - Introduction

Chief Information Security Officer (CISO)

Cyber Incident Responder

Cyber Legal, Policy and Compliance Officer

Cyber Threat Intelligence Specialist

Cybersecurity Architect

Cybersecurity Auditor

Cybersecurity Educator

Cybersecurity Implementer

Cybersecurity Researcher

Cybersecurity Risk Manager

Digital Forensics Investigator

Penetration Tester

Zdroj:ENISA

CHIEF INFORMATION SECURITY OFFICER (CISO)

- Information Security Officer (ISO), Information Security Manager, Head of Information Security, IT/ICT Security Officer
- Riadi stratégiu kybernetickej bezpečnosti organizácie a jej implementáciu s cieľom zabezpečiť, aby digitálne systémy, služby a aktíva boli primerane zabezpečené a chránené.
- Definuje, udržiava a komunikuje víziu, stratégiu, politiky a postupy v oblasti kybernetickej bezpečnosti. Riadi implementáciu politiky kybernetickej bezpečnosti v celej organizácii. Zabezpečuje výmenu informácií s externými orgánmi a profesijnými organizáciami.
- Výstupy: Stratégia kybernetickej bezpečnosti, politika kybernetickej bezpečnosti
- Hlavné úlohy: Dohliadať na uplatňovanie a zlepšovanie systému riadenia informačnej bezpečnosti (ISMS), zabezpečiť, aby vrcholový manažment schválil riziká kybernetickej bezpečnosti organizácie, vypracovať plány kybernetickej bezpečnosti, hlásiť incidenty, riziká a zistenia v oblasti kybernetickej bezpečnosti vrcholovému manažmentu, rokovať s vrcholovým manažmentom o rozpočte na kybernetickú bezpečnosť.

CYBER INCIDENT RESPONDER

- Cyber Incident Handler, Cyber Crisis Expert, Incident Response Engineer, Security Operations Center (SOC) Analyst
- Monitorovať stav kybernetickej bezpečnosti organizácie, riešiť incidenty počas kybernetických útokov a zabezpečiť nepretržité fungovanie systémov IKT.
- Monitoruje a hodnotí stav kybernetickej bezpečnosti systémov. Analyzuje, hodnotí a zmierňuje dopad incidentov kybernetickej bezpečnosti. Identifikuje príčiny kybernetických incidentov a zločinných aktérov. V súlade s plánom organizácie na riešenie incidentov obnovuje funkčnosť systémov a procesov do prevádzkového stavu, zbiera dôkazy a dokumentuje prijaté opatrenia.
- Výstupy: Plán reakcie na incidenty, správa o kybernetickom incidente
- Hlavné úlohy: Vypracovať, implementovať a hodnotiť postupy súvisiace s riešením incidentov, identifikovať, analyzovať, zmierňovať a komunikovať incidenty kybernetickej bezpečnosti, hodnotiť a riadiť technické zraniteľnosti, hodnotiť odolnosť kontrol kybernetickej bezpečnosti a zmierňovacích opatrení prijatých po incidente kybernetickej bezpečnosti alebo porušení ochrany údajov, prijať a vyvinúť techniky testovania riešenia incidentov, zaviesť postupy analýzy výsledkov incidentov a podávania správ o riešení incidentov, dokumentovať analýzu výsledkov incidentov a opatrenia pri riešení incidentov.

CYBER LEGAL, POLICY & COMPLIANCE OFFICER

- Data Protection Officer (DPO), Privacy Protection Officer, Cyber Law Consultant, Cyber Legal Advisor
- Riadi dodržiavanie noriem, právnych a regulačných rámcov týkajúcich sa kybernetickej bezpečnosti na základe stratégie organizácie a právnych požiadaviek.
- Dohliada na dodržiavanie právnych a regulačných rámcov a politík týkajúcich sa kybernetickej bezpečnosti a údajov v súlade so stratégiou organizácie a právnymi požiadavkami a zabezpečuje ich dodržiavanie. Prispieva k činnostiam organizácie súvisiacim s ochranou údajov. Poskytuje právne poradenstvo pri vývoji procesov riadenia kybernetickej bezpečnosti organizácie a odporúčaných nápravných stratégií/riešení na zabezpečenie dodržiavania predpisov.
- Výstupy: Príručka o súlade, správa o súlade
- Hlavné úlohy: Zabezpečovať súlad s normami, zákonmi a predpismi v oblasti ochrany osobných údajov a poskytovať právne poradenstvo a usmernenia v tejto oblasti, identifikovať a dokumentovať nedostatky v súlade, vykonávať posúdenia vplyvu na súkromie a vypracovávať, udržiavať, komunikovať a školenia v oblasti politík a postupov v oblasti ochrany súkromia, presadzovať a obhajovať program organizácie v oblasti ochrany osobných údajov a súkromia, spolupracovať a zdieľať informácie s orgánmi a profesijnými skupinami.

CYBER THREAT INTELLIGENCE SPECIALIST

- Zbieranie, spracovávanie a analýza údajov a informácií s cieľom vypracovať použiteľné spravodajské správy a ich šírenie medzi zainteresované strany.
- Riadenie životného cyklu spravodajských informácií o kybernetických hrozbách, vrátane zberu informácií o kybernetických hrozbách, analýzy a vypracovania použiteľných spravodajských informácií a ich šírenia medzi zainteresované strany v oblasti bezpečnosti a komunitu CTI na taktickej, operačnej a strategickej úrovni. Identifikuje a monitoruje taktiky, techniky a postupy (TTP) používané aktérmi kybernetických hrozieb a ich trendy, sleduje aktivity aktérov hrozieb a pozoruje, ako môžu udalosti mimo kybernetického priestoru ovplyvňovať kybernetické akcie.
- Výstupy: Príručka o spravodajských informáciách o kybernetických hrozbách, správa o kybernetických hrozbách
- Hlavné úlohy: Implementácia zberu informácií o hrozbách, analýza a tvorba využiteľných informácií a ich šírenie medzi zainteresované strany v oblasti bezpečnosti, identifikácia a hodnotenie aktérov kybernetických hrozieb, ktorí sa zameriavajú na organizáciu, identifikácia, monitorovanie a hodnotenie taktík, techník a postupov (TTP) používaných aktérmi kybernetických hrozieb prostredníctvom analýzy otvorených a proprietárnych údajov, informácií a spravodajských informácií, tvorba využiteľných správ na základe údajov o hrozbách, vypracovanie a poradenstvo v oblasti plánov zmierňovania na taktickej, operačnej a strategickej úrovni.

CYBERSECURITY ARCHITECT

- Cybersecurity Solutions Architect, Cybersecurity Designer
- Plánuje a navrhuje riešenia v oblasti bezpečnosti podľa návrhu (infraštruktúry, systémy, aktíva, softvér, hardvér a služby) a kontroly kybernetickej bezpečnosti.
- Navrhuje riešenia založené na princípoch bezpečnosti a ochrany súkromia. Vytvára a neustále vylepšuje architektonické modely a vyvíja príslušnú architektonickú dokumentáciu a špecifikácie. Koordinuje bezpečný vývoj, integráciu a údržbu komponentov kybernetickej bezpečnosti v súlade s normami a ďalšími súvisiacimi požiadavkami.
- Výstupy: Diagram architektúry kybernetickej bezpečnosti, Správa o požiadavkách kybernetickej bezpečnosti
- Hlavné úlohy: Rozvíjať architektúru kybernetickej bezpečnosti organizácie s cieľom riešiť otázky bezpečnosti a ochrany súkromia, vypracovávať architektonickú dokumentáciu a špecifikácie, prezentovať zainteresovaným stranám návrh high-level bezpečnostnej architektúry, vytvárať bezpečné prostredie počas životného cyklu vývoja systémov, služieb a produktov, koordinovať vývoj, integráciu a údržbu komponentov kybernetickej bezpečnosti s cieľom zabezpečiť špecifikácie kybernetickej bezpečnosti, analyzovať a hodnotiť kybernetickú bezpečnosť architektúry organizácie, zabezpečovať bezpečnosť architektúr riešení prostredníctvom bezpečnostných preskúmaní a certifikácie.

CYBERSECURITY AUDITOR

- Information Security Auditor (IT or Legal Auditor), Governance Risk Compliance (GRC) Auditor, Cybersecurity Audit Manager
- Vykonávať audity kybernetickej bezpečnosti. Zabezpečovať súlad so zákonnými, regulačnými a politickými, bezpečnostnými požiadavkami, normami a osvedčenými postupmi.
- Vykonávať nezávislé posúdenia s cieľom posúdiť účinnosť procesov a kontrolných mechanizmov a celkový súlad s právnymi a regulačnými rámcami organizácie. Vyhodnocovať, testovať a overovať produkty (systémy, hardvér, softvér a služby), funkcie a politiky súvisiace s kybernetickou bezpečnosťou, ktoré zabezpečujú súlad s normami a predpismi.
- Výstupy: Plán auditu kybernetickej bezpečnosti, Správa o audite kybernetickej bezpečnosti
- Hlavné úlohy: Vypracovať politiku, postupy, normy a usmernenia organizácie v oblasti auditu, Stanoviť metodiky a postupy používané pri audite systémov, Stanoviť cieľové prostredie a riadiť audítorské činnosti, Definovať rozsah auditu, ciele a kritériá, podľa ktorých sa bude audit vykonávať, Vypracovať plán auditu opisujúci rámce, normy, metodiku, postupy a audítorské testy, Preskúmanie cieľa hodnotenia, bezpečnostných cieľov a požiadaviek na základe profilu rizika, Audit dodržiavania platných zákonov a predpisov týkajúcich sa kybernetickej bezpečnosti, Audit súladu s platnými normami týkajúcimi sa kybernetickej bezpečnosti, Vykonanie plánu auditu a zber dôkazov a meraní, Udržiavanie a ochrana integrity záznamov auditu, Vypracovanie a oznamovanie správ o posudzovaní zhody, zabezpečovaní, audite, certifikácii a údržbe

CYBERSECURITY EDUCATOR

- Cybersecurity Awareness Specialist, Cybersecurity Trainer Faculty in Cybersecurity (Professor, Lecturer)
- Zlepšuje vedomosti, zručnosti a kompetencie ľudí v oblasti kybernetickej bezpečnosti.
- Navrhuje, vyvíja a realizuje programy zamerané na zvyšovanie povedomia, školenia a vzdelávanie v oblasti kybernetickej bezpečnosti a tém súvisiacich s ochranou údajov. Využíva vhodné metódy, techniky a nástroje výučby a školenia na komunikáciu a posilňovanie kultúry kybernetickej bezpečnosti, schopností, vedomostí a zručností ľudských zdrojov. Propaguje dôležitosť kybernetickej bezpečnosti a konsoliduje ju v organizácii.
- Výstupy: Program zvyšovania povedomia o kybernetickej bezpečnosti, školiace materiály o kybernetickej bezpečnosti
- Hlavné úlohy: Vytvárať, aktualizovať a poskytovať osnovy a vzdelávacie materiály v oblasti kybernetickej bezpečnosti a ochrany údajov pre školenia a zvyšovanie povedomia na základe obsahu, metód, nástrojov a potrieb účastníkov školení. Organizovať, navrhovať a realizovať aktivity na zvyšovanie povedomia o kybernetickej bezpečnosti a ochrane údajov, semináre, kurzy, praktické školenia. Monitorovať, hodnotiť a podávať správy o účinnosti školení. Hodnotiť a podávať správy o výkone účastníkov školení. Hľadať nové prístupy k vzdelávaniu, školeniam a zvyšovaniu povedomia.

CYBERSECURITY IMPLEMENTER

- Cybersecurity Developer , Cybersecurity Engineer Development, Security & Operations (DevSecOps) Engineer
- Vyvíjať, nasadzovať a prevádzkovať riešenia v oblasti kybernetickej bezpečnosti (systémy, aktíva, softvér, opatrenia a služby) v infraštruktúrach a produktoch.
- Zabezpečuje technický vývoj, integráciu, testovanie, implementáciu, prevádzku, údržbu, monitorovanie a podporu riešení v oblasti kybernetickej bezpečnosti. Zabezpečuje dodržiavanie špecifikácií a požiadaviek na zhodu, zaručuje spoľahlivý výkon a rieši technické problémy súvisiace s riešeniami v oblasti kybernetickej bezpečnosti (systémy, aktíva, softvér, kontroly a služby), infraštruktúrami a produktmi organizácie.
- Výstupy: Riešenia v oblasti kybernetickej bezpečnosti
- Hlavné úlohy: Vývoj, implementácia, údržba, aktualizácia a testovanie produktov v oblasti kybernetickej bezpečnosti, poskytovanie podpory v oblasti kybernetickej bezpečnosti používateľom a zákazníkom, integrácia riešení v oblasti kybernetickej bezpečnosti a zabezpečenie ich spoľahlivého fungovania, bezpečné konfigurovanie systémov, služieb a produktov, údržba a aktualizácia bezpečnosti systémov, služieb a produktov, implementácia, aplikácia a správa bezpečnostných aktualizácií produktov s cieľom odstrániť technické zraniteľnosti.

CYBERSECURITY RESEARCHER

- Cybersecurity Research Engineer Chief Research Officer (CRO) in cybersecurity Senior Research Officer in cybersecurity Research and Development (R&D) Officer in cybersecurity
- Vykonáva výskum v oblasti kybernetickej bezpečnosti a výsledky zapracúva do riešení v oblasti kybernetickej bezpečnosti. Vykonáva základný a aplikovaný výskum a podporuje inovácie v oblasti kybernetickej bezpečnosti prostredníctvom spolupráce s ďalšími zainteresovanými stranami. Analyzuje trendy a vedecké poznatky v oblasti kybernetickej bezpečnosti.
- Výstupy: Publikácia v oblasti kybernetickej bezpečnosti
- Hlavné úlohy: Analyzovať a hodnotiť technológie, riešenia, vývoj a procesy v oblasti kybernetickej bezpečnosti, vykonávať výskum, inovácie a vývoj v témach súvisiacich s kybernetickou bezpečnosťou, manifestovať a generovať nápady v oblasti výskumu a inovácií, posúvať súčasný stav techniky v témach súvisiacich s kybernetickou bezpečnosťou, pomáhať pri vývoji inovatívnych riešení v oblasti kybernetickej bezpečnosti, vykonávať experimenty a vyvíjať dôkazy koncepcie, pilotné projekty a prototypy riešení v oblasti kybernetickej bezpečnosti, publikovať a prezentovať vedecké práce a výsledky výskumu a vývoja.

CYBERSECURITY RISK MANAGER

- Information Security Risk Analyst Cybersecurity Risk Assurance Consultant
- Riadiť riziká organizácie súvisiace s kybernetickou bezpečnosťou v súlade so stratégiou organizácie. Vytvárať, udržiavať a komunikovať procesy a správy týkajúce sa riadenia rizík.
- Neustále riadi (identifikuje, analyzuje, hodnotí, odhaduje, zmierňuje) riziká súvisiace s kybernetickou bezpečnosťou infraštruktúr, systémov a služieb IKT prostredníctvom plánovania, uplatňovania, podávania správ a komunikácie analýzy, hodnotenia a riešenia rizík. Stanovuje stratégiu riadenia rizík pre organizáciu a zabezpečuje, aby riziká zostali na prijateľnej úrovni pre organizáciu, a to výberom opatrení na zmiernenie rizík a kontrolných mechanizmov.
- Výstupy: Správa o hodnotení rizík kybernetickej bezpečnosti, akčný plán na odstránenie rizík kybernetickej bezpečnosti
- Hlavné úlohy: Vypracovať stratégiu riadenia rizík kybernetickej bezpečnosti organizácie, spravovať inventár majetku organizácie, identifikovať a posudzovať hrozby a zraniteľnosti systémov IKT súvisiace s kybernetickou bezpečnosťou, identifikovať hrozby vrátane profilov útočníkov a odhadovať potenciál útokov, posudzovať riziká kybernetickej bezpečnosti a navrhovať najvhodnejšie možnosti riešenia rizík, vrátane bezpečnostných kontrol a zmierňovania a predchádzania rizikám, ktoré najlepšie zodpovedajú stratégii organizácie, zabezpečiť, aby všetky riziká kybernetickej bezpečnosti zostali na prijateľnej úrovni pre majetok organizácie.

DIGITAL FORENSICS INVESTIGATOR

- Digital Forensics Analyst Cybersecurity & Forensic Specialist
- Zabezpečit', aby vyšetrovanie kyberkriminality odhalilo všetky digitálne dôkazy na preukázanie škodlivej činnosti.
- Prepojit' artefakty s fyzickými osobami, zachytit', obnovit', identifikovat' a uchovat' údaje, vrátane prejavov, vstupov, výstupov a procesov digitálnych systémov, ktoré sú predmetom vyšetrovania. Poskytovat' analýzu, rekonštrukciu a interpretáciu digitálnych dôkazov na základe kvalitatívneho posúdenia. Predložit' nestranný kvalitatívny pohľad bez interpretácie výsledných zistení.
- Výstupy: Výsledky digitálnej forenznej analýzy, digitálne stopy (dôkazy)
- Hlavné úlohy: Identifikovat', obnovit', extrahovat', zdokumentovat' a analyzovat' digitálne dôkazy, uchovávat' a chránit' digitálne dôkazy a sprístupnit' ich oprávneným zainteresovaným stranám, kontrolovat' prostredie s cieľom nájst' dôkazy o neoprávnených a nezákonných činnostiach.

PENETRATION TESTER

- Pentester, Ethical Hacker , Vulnerability Analyst , Cybersecurity Tester, Offensive Cybersecurity Expert , Defensive Cybersecurity Expert, Red Team Expert, Red Teamer
- Posudzuje účinnosť bezpečnostných opatrení odhaľuje a využíva zraniteľnosti a posudzuje ich kritickosť v prípade, že ich zneužijú aktéri hrozieb. Plánuje, navrhuje, implementuje a vykonáva penetračné testovanie a útočné scenáre s cieľom vyhodnotiť účinnosť nasadených alebo plánovaných bezpečnostných opatrení. Identifikuje zraniteľnosti alebo zlyhania technických a organizačných kontrol, ktoré ovplyvňujú dôvernosť, integritu a dostupnosť produktov IKT (napr. systémov, hardvéru, softvéru a služieb)..
- Výstupy: Správa o výsledkoch posúdenia zraniteľnosti, správa o penetračných testoch
- Hlavné úlohy: Identifikovať, analyzovať a posudzovať technické a organizačné zraniteľnosti kybernetickej bezpečnosti, identifikovať vektory útokov, odhaľovať a demonštrovať zneužitie technických zraniteľností kybernetickej bezpečnosti, testovať súlad systémov a prevádzky s regulačnými normami, vyberať a vyvíjať vhodné techniky penetračných testov, organizovať testovacie plány a postupy pre penetračné testy, zavádzať postupy pre analýzu a vykazovanie výsledkov penetračných testov, dokumentovať a vykazovať výsledky penetračných testov zainteresovaným stranám.

Mapovanie medzi ESCO a ECSF

- ESCO je viacjazyčná Európska klasifikácia zručností, kompetencií, kvalifikácií a povolaní. (Európska Komisia)
- ECSF a klasifikácia ESCO majú spoločný cieľ: analyzovať trh práce z hľadiska profesijných rolí a požadovaných zručností, hoci z rôznych perspektív. ESCO sa zameriava na klasifikáciu celého trhu práce EÚ v rôznych sektoroch, zatiaľ čo ECSF poskytuje zameranú analýzu profilov rolí špecifických pre sektor kybernetickej bezpečnosti. Počas procesu aktualizácie, ktorý viedol k vydaniu verzie ESCO 1.2, ENISA úzko spolupracovala s tímom ESCO. Využitím ECSF bolo v klasifikácii ESCO vykonaných niekoľko vylepšení, aby presnejšie reprezentovala povolania a zručnosti požadované v oblasti kybernetickej bezpečnosti. V dôsledku tejto spolupráce ESCO v1.2 teraz zahŕňa 5 povolaní, ktoré sú priamo zosúladené s 5 profilmi rolí ECSF v oblasti kybernetickej bezpečnosti.

Vyhláška NBÚ č. 492/2022

Vyhláška č. 492/2022

- Nadobudla účinnosť 1.1.2023
- 11 rolí (chýba výslovne rola výskumníka)
- Minimálne odborné znalosti pre jednotlivých používateľov sietí a informačných systémov vykonávajúcich činnosti a úlohy v oblasti kybernetickej bezpečnosti, pričom však nezasahuje do politiky a tvorby pracovných miest
- Zodpovednosť osôb v oblasti kybernetickej bezpečnosti, má byť zadefinovaná jednoznačne, prostredníctvom rolí.
- S rolami je spojená množina povinností a oprávnení pri inicializácii, návrhu, vývoji, používaní a prevádzke siete alebo informačného systému.

Bezpečnostné role

1. Špecialista kybernetickej bezpečnosti
2. Manažér kybernetickej bezpečnosti
3. Audítor kybernetickej bezpečnosti
4. Tester kybernetickej bezpečnosti
5. Architekt kybernetickej bezpečnosti
6. Špecialista riadenia rizík
7. Špecialista pre analýzu digitálnych stôp
8. Špecialista pre riadenie súladu
9. Špecialista pre riešenie kybernetických incidentov
10. Analytik kybernetickej bezpečnosti
11. Lektor kybernetickej bezpečnosti

ECSF má 12 rolí (napr. CISO, Incident Responder, Legal/Policy & Compliance, CTI Specialist, Architect, Auditor, Educator, Implementer, Researcher, Risk Manager, Digital Forensics, Penetration Tester).
ECSF má samostatne CTI Specialist a Cybersecurity Researcher.

Vyhláška(prílohy 4–14) pokrýva veľmi podobné role (manažér, audítor, tester, architekt, špecialista rizík, digitálne stopy, súlad, incidenty, analytik KB, lektor KB, a špecialista KB).

Vyhláška NBÚ č. 492/2022 vs ECSF

- V ZoKB sú zakotvené iba dve roly z ECSF, ktorých činnosť by mala byť pre prevádzkovateľov záväzná a ktoré by mali spĺňať stanovený znalostný štandard:
- audítor KB, keďže podľa § 29 ods. 3 ZoKB audit kybernetickej bezpečnosti vykonáva certifikovaný audítor kybernetickej bezpečnosti, ktorým je fyzická osoba, spoločník, štatutárny orgán alebo zamestnanec právnickej osoby,
- manažér KB, keďže v zmysle § 20 ods. 4 ZoKB bezpečnostné opatrenia musia zahŕňať najmenej určenie manažéra kybernetickej bezpečnosti.
- Pre obidve tieto roly existujú certifikačné schémy a aj akreditovaní poskytovatelia certifikačných testov.
- Znalostné štandardy sú pre jednotlivé roly kybernetickej bezpečnosti odporúčané, okrem tých rolí, o ktorých to ustanovuje zákon, teda manažér kybernetickej bezpečnosti [§ 20 ods. 4 písm. a) zákona] a audítor kybernetickej bezpečnosti (§ 29 ods. 3 zákona). Pre osobu manažéra kybernetickej bezpečnosti a certifikovaného audítora kybernetickej bezpečnosti znalostné štandardy predstavujú záväzný rámec.

Vyhláška NBÚ č. 492/2022 vs ECSF

- Právna povaha a účel ECSF (ENISA) je nezáväzný európsky rámec pre pracovné roly v kyberbezpečnosti, použiteľný pre HR, vzdelávanie a plánovanie pracovnej sily naprieč EÚ.
- Vyhláška NBÚ 492/2022 je záväzný vykonávací predpis k ZoKB; stanovuje znalostné štandardy pre roly, ktoré majú slúžiť na preukazovanie minimálnych požiadaviek na výkon roly a budovanie povedomia.
- ECSF definuje rolu cez opis práce a výstupov. Vyhláška definuje rolu ako súbor vedomostí, zručností a kompetencií, pričom vedomosti sú často rozpísované a ku každej položke je priradená úroveň BL (Bloomova taxonómia)
- Prílohy vyhlášky idú do výrazne detailnejšej úrovne znalostí (napr. OSI model, protokoly, sieťové zariadenia, kryptografické mechanizmy, hardvér, OT/ICS, cloud, riziká. . .)
- Vyhláška výslovne pripúšťa kolektívne splnenie znalostných štandardov „zdieľaním“ medzi osobami/rolami (t.j. organizácia nemusí mať jedného človeka, ktorý pokryje všetko)

Znalostné štandardy

- Znalostné štandardy
- tzv. taxonómia vzdelávacích cieľov, je hierarchicky usporiadaná miera náročnosti a rozsahu vedomostí.
- Vyhláška sa odkazuje na taxonómiu poznávacích cieľov podľa B. S. Bloom a BL 1 – BL 6 (zapamätanie, pochopenie, aplikácia, analýza, syntéza, posúdenie)
- Syntéza je schopnosť opätovne spojiť rôzne časti alebo prvky konceptu do jednotného systému alebo celku.
- Posúdenie je schopnosť dospieť k prehľadu a posúdiť hodnotu a relatívny prínos

Iné ako bezpečnostné role

- Ostatné iné ako bezpečnostné pracovné roly, ktoré prichádzajú do styku s kybernetickým priestorom
- bez špecifikácie znalostného štandardu
- aspoň minimálnu úroveň kvalifikácie aj pre roly, ktoré nie sú priamo zainteresované v odbore kybernetická bezpečnosť. Tieto odporúčania sú taxatívne vymenované v prílohe č. 1 k vyhláške č. 492/2022 Z. z. – Charakteristika vzdelávacích potrieb.
- Rozdelenie používateľov nie je to isté čo pracovné role v kybernetickej bezpečnosti.

1. laici – používatelia IKT mimo kontextu výkonu konkrétneho povolania a bez vzťahu k sieti alebo informačnému systému,
2. odborní zamestnanci – používatelia, ktorí pri výkone konkrétneho povolania využívajú siete alebo informačné systémy,
3. manažéri – riadiaci zamestnanci, ktorí nie sú IT manažérmi a ktorí spravidla zodpovedajú za príslušný proces alebo skupinu,
4. IT manažéri – riadiaci zamestnanci organizačných jednotiek zodpovedných za poskytovanie IT služieb, návrh, implementáciu, obstaranie, prevádzku, údržbu a posudzovanie IKT,
5. informatici – zamestnanci zodpovední za poskytovanie IT služieb, návrh, implementáciu, obstaranie, prevádzku, údržbu a posudzovanie IKT.

Role a zručnosti

- Tvorba názvov pracovných pozícií a ich pracovných náplní sa určuje prevádzkovateľom základnej služby.
- Prílohy č. 4 až 14, vrátane znalostného štandardu,
- Zručnosti - schopnosti uplatňovať vedomosti v praxi a využívať ich na plnenie úloh a riešenie problémov
- Pre príslušnú rolu sú posudzované v kontexte kompetencií, potrebných na vykonávanie určitej pracovnej činnosti v konkrétnom odvetví
- Domény:

1. **Riadenie bezpečnosti**
2. **Riadenie hrozieb a rizík**
3. **Aplikácia bezpečnostných opatrení**
4. **Výkon operatívnych bezpečnostných činností**
5. **Riadenie súladu**

Riadenie bezpečnosti

- Štatutárna zodpovednosť za riadenie bezpečnosti (*Security Governance*)
- Výkonná zodpovednosť za riadenie bezpečnosti (*Security Operations*).

Štatutárne vedenie

- Zodpovednosť za dodržiavanie kybernetickej bezpečnosti je **súčasťou širšej povinnosti** vykonávať svoju pôsobnosť **s odbornou starostlivosťou a v súlade so záujmami právnickej osoby a všetkých jej spoločníkov** (akcionárov) - najmä § 135a ods. 1, § 194 ods. 5 Obchodného zákonníka
- Osobitné povinnosti podľa ZoKB, najmä:

1) **Schvaľovanie bezpečnostnej stratégie a politík**
2) **Riadenie rizík vrátane zmiernenia, presunu či akceptácie rizika**
3) Zabezpečenie primeraných finančných, materiálno-technických a personálnych kapacít
4) Pravidelné informovanie sa o stave KB (napr. formou reportov), **prijímanie návrhov a informácií od manažéra KB.**

Štatutárne vedenie

- Vedenie organizácie musí:

1. prijať celkovú zodpovednosť za KIB v organizácii
2. byť dobrým príkladom pri dodržiavaní bezpečnostných požiadaviek a opatrení
3. vymenovať zamestnancov zodpovedných za KIB a poskytnúť im potrebné oprávnenia a zdroje
4. pravidelne dostávať informácie o stave KIB v organizácii, možných rizikách vyplývajúcich z chýbajúcich alebo nedostatočných bezpečnostných opatrení

Manažér KB

- Predkladá **návrhy a oznamuje informácie v oblasti KB priamo štatutárnemu orgánu** PZS
- Riadi aplikáciu **bezpečnostných opatrení (vrátane navrhovania rozpočtu,** súvisiaceho s bezpečnostnými opatreniami)
- Zabezpečuje ošetrovanie bezpečnostných **hrozieb** a hodnotenia **zraniteľností**
- Riadi vyšetrovanie a nápravu následkov KB **incidentov**

Manažér KB

1. presadzuje KB v organizácii, riadi a koordinuje aplikáciu bezpečnostných opatrení
2. musí mať primeranú kvalifikáciu a dostatočné podmienky na jej zvyšovanie
3. musí mať k dispozícii dostatočné zdroje
4. musí mať možnosť podávať správy/hlásenia priamo vedeniu organizácie
5. musí byť zapojený v počiatočnej fáze rozsiahlych projektov, ako napr. zavedenia novej aplikácie alebo IT systému

- Ak na funkciu manažéra organizácia nemá vhodného zamestnanca, organizácia musí nájsť a vymenovať externého manažéra.

Manažér KB – zákonné požiadavky

- Každý MKB musí (§ 20 ods. 4 ZoKB)
  - ➢ byť pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení **nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií** a
  - ➢ spĺňať **znalostné štandardy**

Platí rovnako pre interného aj externého MKB!

Manažér KB – zručnosti

- **Riadenie bezpečnosti**

1) strategické riadenie kybernetickej bezpečnosti organizácie

2) vypracovanie a prezentácia bezpečnostných stratégií a konceptov

3) implementácia a riadenie procesov kybernetickej bezpečnosti podľa všeobecne záväzných právnych predpisov, bezpečnostnej stratégie a ostatných interných riadiacich aktov

4) zabezpečenie, vypracovanie, udržiavanie a aktualizácie bezpečnostnej dokumentácie kybernetickej bezpečnosti a ďalších interných riadiacich aktov vo vzťahu k bezpečnosti organizácie

5) návrh požiadaviek na rozpočet a na iné zdroje súvisiace s bezpečnostnými opatreniami a procesmi relevantnými z hľadiska kybernetickej bezpečnosti vrátane riadenia nákladov a riadenia investícií

6) metodické usmerňovanie správcov a gestorov IKT, vlastníkov procesov, vlastníkov aktív, vedúcich zamestnancov a ďalších zodpovedných zamestnancov vo vzťahu k dosahovaniu bezpečnostných cieľov organizácie

7) poskytovanie informácií bezpečnostnému výboru alebo štatutárnemu orgánu o stave kybernetickej bezpečnosti v organizácii, o závažných bezpečnostných rizikách, kybernetických bezpečnostných incidentoch a významných bezpečnostných udalostiach

8) riadenie kybernetickej bezpečnosti vo vzťahu s dodávateľmi a pri obstarávaní a vývoji softvéru a systémov

Manažér KB – zručnosti

- **Riadenie hrozieb a rizík**

1) implementácia a manažment procesov identifikácie, analýzy a monitoringu bezpečnostných hrozieb a rizík

2) posudzovanie hrozieb a rizík

3) návrh opatrení na ošetrovanie rizík a na zamedzenie dopadov bezpečnostných udalostí

4) zabezpečovanie procesov hodnotenia technických zraniteľností systémov

5) manažment procesov detekcie, riešenia, evidencie a prevencie kybernetických bezpečnostných incidentov

6) zabezpečenie funkčných plánov kontinuity a obnovy činností organizácie

7) koordinácia a riadenie procesov obnovy prevádzkových činnosti (tzv. Business Continuity Management) vrátane riadenia procesov plánovania obnovy systémov po havárii (tzv. Disaster Recovery Planning)

Manažér KB – zručnosti

- **Aplikácia bezpečnostných opatrení**

1) riadenie návrhov, implementácie, zmien a optimalizácie bezpečnostných riešení s víziou a konceptom ich bežného prevádzkovania

2) zabezpečovanie implementácie technických a organizačných bezpečnostných opatrení

3) riadenie bezpečnostnej architektúry

4) predkladanie odborných stanovísk k novým zmenám v IT infraštruktúre, ktoré môžu mať potenciálny vplyv na bezpečnosť informačných aktív organizácie

5) monitorovanie plnenia a efektivity bezpečnostných mechanizmov a opatrení

Manažér KB – zručnosti

- **Výkon operatívnych bezpečnostných činností**

1) manažment výkonu činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe

2) vedenie tímu zamestnancov útvaru informačnej a kybernetickej bezpečnosti, ak je taký organizačný útvar zriadený

3) návrh a aplikácia metodík pre klasifikáciu informačných aktív a kategorizáciu sietí a informačných systémov

4) riadenie bežnej prevádzky technických bezpečnostných opatrení

5) zabezpečovanie udržateľnosti organizačných opatrení vrátane vyspelosti bezpečnostných procesov

6) zaistenie uplatňovania princípu oddelenia právomocí a zodpovedností v celej organizačnej štruktúre organizácie

7) základy projektového manažmentu

Manažér KB – zručnosti

- **Riadenie súladu**

1) riadenie procesov zaručenia súladu (Compliance Management) v oblasti kybernetickej bezpečnosti

2) zabezpečenie pravidelného preskúmavania stavu kybernetickej a informačnej bezpečnosti

3) vyhodnocovanie plnenia vnútorných predpisov súvisiacich s riadením kybernetickej bezpečnosti

4) poskytovanie súčinnosti internému a externému auditu kybernetickej bezpečnosti

5) navrhovanie metrík a kľúčových indikátorov pre sledovanie vývoja a stavu bezpečnosti a vývoja bezpečnostných rizík

6) zabezpečovanie školení zamestnancov v oblasti kybernetickej bezpečnosti

7) zabezpečovanie kontinuálneho vzdelávania pre pracovné roly relevantné z hľadiska kybernetickej bezpečnosti

8) zabezpečovanie budovania bezpečnostného povedomia pre oblasť informačnej a kybernetickej bezpečnosti a ochrany osobných údajov

9) spolupráca s orgánmi verejnej moci a orgánmi činnými v trestnom konaní

Manažér KB – vzdelanie a prax

- Úplné stredné všeobecné alebo úplné stredné odborné: najmenej **7 rokov** praxe v oblasti informačných technológií z toho najmenej **5 rokov** praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT
- Vysokoškolské I. Stupňa: : najmenej **5 rokov** praxe v oblasti informačných technológií z toho najmenej **3 rokov** praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT
- Vysokoškolské II. a III. stupňa: najmenej **3 rokov** praxe v oblasti informačných technológií z toho najmenej **1 rok** praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT

- Platí, že, medzinárodný certifikát sa považuje za započítateľnú odbornú prax 1 rok

Špecialista riadenia rizík – zručnosti

- **Riadenie bezpečnosti**
- podpora riadenia informačnej a kybernetickej bezpečnosti organizácie
- **Riadenie hrozieb a rizík**

a) implementácia procesov a nástrojov identifikácie, analýzy a monitoringu bezpečnostných hrozieb a rizík

b) posudzovanie hrozieb a rizík

c) návrh opatrení na ošetrovanie rizík

d) účasť v procesoch obnovy prevádzkových činnosti (tzv. Business Continuity Management) vrátane účasti v riadení procesov plánovania obnovy systémov po havárii (tzv. Disaster Recovery Planning)

Špecialista riadenia rizík – zručnosti

- **Aplikácia bezpečnostných opatrení**

a) podpora riadenia bezpečnostnej architektúry

b) monitorovanie plnenia a efektivity bezpečnostných mechanizmov a opatrení

- **Výkon operatívnych bezpečnostných činností**

a) výkon činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe

b) aplikácia metodík pre klasifikáciu informačných aktív a kategorizáciu sietí a informačných systémov

- **Riadenie súladu**

a) pravidelné preskúmavanie stavu kybernetickej a informačnej bezpečnosti

b) poskytovanie súčinnosti internému a externému auditu informačnej a kybernetickej bezpečnosti

Špecialista KB - zručnosti

- zodpovedný za plnenie špecifických úloh v rámci svojej špecializácie v kybernetickej bezpečnosti

- **Riadenie bezpečnosti**

1) podpora riadenia informačnej a kybernetickej bezpečnosti organizácie

2) implementácia procesov informačnej a kybernetickej bezpečnosti podľa všeobecne záväzných právnych predpisov, bezpečnostnej stratégie a ostatných interných riadiacich aktov

3) metodické usmerňovanie správcov a gestorov informačných a komunikačných technológií, vlastníkov procesov, vlastníkov aktív, vedúcich zamestnancov a ďalších zodpovedných zamestnancov vo vzťahu k dosahovaniu bezpečnostných cieľov organizácie

4) riadenie informačnej a kybernetickej bezpečnosti vo vzťahu s dodávateľmi a pri zaobstarávaní, projektovaní a vývoji softvéru a systémov

5) správa bezpečnosti informačných aktív organizácie

Špecialista KB - zručnosti

- **Riadenie hrozieb a rizík**

1) implementácia procesov a nástrojov identifikácie, analýzy a monitoringu bezpečnostných hrozieb a rizík

2) posudzovanie hrozieb a rizík a návrh opatrení na ošetrovanie rizík

3) hodnotenie technických zraniteľností systémov

4) detekcia, riešenie, evidencia a prevencia kybernetických bezpečnostných incidentov

5) podpora procesov obnovy prevádzkových činnosti (tzv. Business Continuity Management) vrátane riadenia procesov plánovania obnovy systémov po havárii (tzv. Disaster Recovery Planning)

Špecialista KB - zručnosti

- **Aplikácia bezpečnostných opatrení**

1) zabezpečovanie implementácie zmien a optimalizácie technických a organizačných bezpečnostných opatrení

2) zabezpečovanie návrhov, zmien a integrácie bezpečnostných technológií a riešení

3) podpora riadenia bezpečnostnej architektúry

4) predkladanie odborných stanovísk k novým zmenám v IT infraštruktúre, ktoré môžu mať potenciálny vplyv na bezpečnosť informačných aktív organizácie

5) monitorovanie plnenia a efektivity bezpečnostných mechanizmov a opatrení

Špecialista KB - zručnosti

- **Výkon operatívnych bezpečnostných činností**

1) výkon činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe

2) aplikácia metodík pre klasifikáciu informačných aktív a kategorizáciu sietí a informačných systémov

3) prevádzka technických bezpečnostných opatrení

4) zabezpečovanie udržateľnosti organizačných opatrení vrátane vyspelosti bezpečnostných procesov

5) riadenie projektov v kybernetickej bezpečnosti

Špecialista KB - zručnosti

- **Riadenie súladu**

1) pravidelné preskúmavanie stavu kybernetickej a informačnej bezpečnosti

2) poskytovanie súčinnosti internému a externému auditu informačnej a kybernetickej bezpečnosti

3) zabezpečovanie školení zamestnancov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti

4) budovanie bezpečnostného povedomia pre oblasť informačnej a kybernetickej bezpečnosti a ochrany osobných údajov

5) spolupráca s orgánmi verejnej moci a orgánmi činnými v trestnom konaní

Architekt KB - zručnosti

- **Riadenie bezpečnosti**
- a) podpora riadenia informačnej a kybernetickej bezpečnosti organizácie
- b) vypracovanie a prezentácia bezpečnostných stratégií a konceptov
- c) metodické usmerňovanie správcov a gestorov informačných a komunikačných technológií, vlastníkov procesov, vlastníkov aktív, vedúcich zamestnancov a ďalších zodpovedných zamestnancov vo vzťahu k dosahovaniu bezpečnostných cieľov organizácie

Architekt KB - zručnosti

- **Riadenie hrozieb a rizík**
- a) podpora implementácie procesov a nástrojov identifikácie, analýzy a monitoringu bezpečnostných hrozieb a rizík
- b) návrh opatrení na ošetrovanie rizík a na zamedzenie dopadov bezpečnostných udalostí
- c) hodnotenie technických zraniteľností systémov

Architekt KB - zručnosti

- **Aplikácia bezpečnostných opatrení**
- a) návrhy implementácie, zmien a optimalizácie bezpečnostných technológií a riešení
- b) podpora riadenia bezpečnostnej architektúry
- c) predkladanie odborných stanovísk k novým zmenám v IT infraštruktúre, ktoré môžu mať potenciálny vplyv na bezpečnosť informačných aktív organizácie

Architekt KB - zručnosti

- **Výkon operatívnych bezpečnostných činností**

a) výkon činností súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe

b) aplikácia metodík pre klasifikáciu informačných aktív a kategorizáciu sietí a informačných systémov

c) riadenie projektov v kybernetickej bezpečnosti

- **Riadenie súladu**
- budovanie bezpečnostného povedomia pre oblasť informačnej a kybernetickej bezpečnosti a ochrany osobných údajov

Architekt KB – vzdelanie a prax

- Úplné stredné všeobecné alebo úplné stredné odborné: najmenej **3 roky** praxe v oblasti informačných technológií
- Vysokoškolské I. Stupňa:: najmenej **2 roky** praxe v oblasti informačných technológií
- Vysokoškolské II. a III. stupňa: najmenej **1 rok** praxe v oblasti informačných technológií

Audítor KB - zručnosti

1) navrhovanie a uplatňovanie bezpečnostných stratégií a politík
2) prioritizácia úloh a efektívne priraďovanie zdrojov
3) posudzovanie dôkazov
4) analýza rizík
5) spracovanie úplnej a prehľadnej záverečnej správy o výsledkoch auditu kybernetickej bezpečnosti
6) analýza a hodnotenie bezpečnostných mechanizmov a riešení

Audítor KB – vzdelanie a prax

- Úplné stredné všeobecné alebo úplné stredné odborné: najmenej **10 rokov** praxe v oblasti informačných technológií, z toho najmenej **7 rokov** praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT
- Vysokoškolské I. Stupňa: najmenej **7 rokov** praxe v oblasti informačných technológií, z toho najmenej **5 rokov** praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT
- Vysokoškolské II. a III. stupňa: najmenej **5 rokov** praxe v oblasti informačných technológií, z toho najmenej **3 rokov** praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT

- Špeciálna kvalifikácia:
- a) medzinárodný certifikát z oblasti auditu informačných systémov alebo certifikát manažéra kybernetickej bezpečnosti v zmysle zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti,
- b) zoznam vykonaných auditov s uvedením kontaktu na overiteľnú referenciu

Povinnosti NIS2/ZoKB mapované na role ECSF

- **Aké úlohy a zručnosti sú potrebné na splnenie týchto požiadaviek ZoKB/NIS2?**

- Podľa § 19 ZoKB Povinnosti prevádzkovateľa základnej služby (1) Prevádzkovateľ základnej služby je povinný do 12 mesiacov odo dňa zápisu do registra prevádzkovateľov základnej služby **v závislosti od vykonanej analýzy rizik prijať, dodržiavať a vykonávať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20** a vykonávať ich s cieľom zabezpečovania kybernetickej bezpečnosti a odolnosti.
- Podľa § 24 ZoKB Prevádzkovateľ základnej služby je povinný **hlásiť každý závažný kybernetický bezpečnostný incident.** Prevádzkovateľ základnej služby prostredníctvom jednotného informačného systému kybernetickej bezpečnosti hlási **aj a) významnú kybernetickú hrozbu, o ktorej sa dozvie, b) udalosť odvrátenú v poslednej chvíli, ktorá mohla spôsobiť závažný kybernetický bezpečnostný incident, c) zraniteľnosť** ním prevádzkovaných verejne dostupných sietí a informačných systémov, ktorá podľa dostupných informácií a technických znalostí môže byť zneužitá na spôsobenie závažného kybernetického bezpečnostného incidentu a prevádzkovateľ základnej služby nemohol v primeranom čase prijať opatrenia na jej odstránenie alebo zníženie rizika.

Povinnosti NIS2/ZoKB mapované na role ECSF

- **SCENÁR 1: IMPLEMENTÁCIA BEZPEČNOSTNÝCH OPATRENÍ**
- Vedenie organizácie, ktorá je stredným podnikom, hľadá praktické usmernenie, ako zaviesť opatrenia. Uvedomilo si, že ECSF môže slúžiť ako nástroj na identifikáciu a odstránenie kapacitných medzier v organizácii – či už formou doškolenia (upskilling), rekvalifikácie (reskilling), náboru alebo obstarania externých služieb.
- ECSF je pritom vhodné chápať ako základný rámec na nastavenie rolí, zodpovedností a kompetencií pre kybernetickú bezpečnosť

Scenár 1

- **Organizácia (stredný podnik) identifikovala nasledujúce organizačné úlohy ako nevyhnutné na vytvorenie základných požiadaviek v oblasti kybernetickej bezpečnosti a zabezpečenie súladu s nimi.**
- **1. Definovať a implementovať plány a politiky kybernetickej bezpečnosti** (stratégie a politiky , riadenie vzťahov s dodávateľmi, pravidelne informovať vedenia o plánoch a stratégiách kybernetickej bezpečnosti, plány BCM a DRP.
- **2. Riadiť riziko kybernetickej bezpečnosti** (Vypracovať a uplatňovať politiky v oblasti analýzy rizík, správy aktív a bezpečnosti ľudských zdrojov. Informovať vedenie o rizikách a hrozbách a o opatreniach na riadenie rizík v oblasti kybernetickej bezpečnosti)
- **3. Spolupracovať s orgánmi a ďalšími zainteresovanými stranami** (zdieľanie informácií a poskytovať správy orgánom a ďalším zainteresovaným stranám. Zabezpečiť dodržiavanie záväzných pokynov alebo príkazov orgánov)
- **4. Zabezpečiť dodržiavanie predpisov prostredníctvom auditov kybernetickej bezpečnosti** (nezávislé audity KB, interné audity)
- **5. Dohliadať na dodržiavanie ZoKB a zabezpečovať jej dodržiavanie** (oznamovanie činností, a hlásenie o všetkých zmenách).
- **6. Informovať zainteresované strany o povinnostiach v oblasti dodržiavania predpisov (**Informovať vedenie, že je zodpovedné za schvaľovanie opatrení v oblasti kybernetickej bezpečnosti a musí absolvovať školenie v oblasti kybernetickej bezpečnosti. Zabezpečiť, aby vrcholový manažment vedel, či musí vymenovať zástupcu pre spoločnosti, ktoré nemajú sídlo v EÚ, ale ponúkajú tam svoje služby.)

Scenár 1

- **7. Plánovať, navrhovať a implementovať bezpečnostné riešenia a kontroly** (Plánovať a budovať bezpečné siete a zabezpečiť bezpečné prostredie. Implementovať silné bezpečnostné funkcie, ako je viacfaktorová autentifikácia (MFA), a zabezpečiť bezpečnú komunikáciu pre hlas, video, text a núdzové situácie. Monitorovať opatrenia kybernetickej bezpečnosti, ako sú bezpečné konfigurácie sietí a integrácie systémov, náprava na základe výsledkov riadenia rizík a plánovania a nálezov z auditov)
- **8. Školenia v oblasti kybernetickej bezpečnosti**
- **9. Získavať a analyzovať informácie s cieľom identifikovať hrozby (vrátane near missov, zraniteľností a techník útokov.)**
- **10. Zabezpečte efektívnu reakciu a hlásenie incidentov kybernetickej bezpečnosti.** (plán reakcie na incidenty kybernetickej bezpečnosti. Hodnoťte a hláste všetky zraniteľnosti tímu CSIRT. Identifikovať, analyzovať a nahlásiť závažné incidenty kybernetickej bezpečnosti tímom CSIRT, orgánom a príjemcom služieb.)
- **11. Testovanie bezpečnosti** (penetračné testy a hodnotenia zraniteľnosti s cieľom posúdiť účinnosť riešení kybernetickej bezpečnosti a na požiadanie poskytnúť správy o hodnotení zraniteľnosti a/alebo penetračných testoch príslušným orgánom. Plánovať a priebežne vykonávať bezpečnostné testy (vrátane, ale nielen, pentestov a hodnotení zraniteľnosti) podľa výsledkov procesu riadenia rizík. Dokumentovať zistenia a v prípade kritických zistení uplatňovať primerané zmierňujúce opatrenia.

Krok 1: Obsadenie manažéra KB

- **Ako prvý krok k riešeniu úloh 1, 2 a 3 sa vrcholový manažment rozhodol vymenovať manažéra kybernetickej bezpečnosti, ktorý bude zodpovedný za vypracovanie politiky organizácie v oblasti bezpečnosti sietí a informačných systémov, ako aj za vypracovanie politík, postupov, procesov a plánov týkajúcich sa konkrétnych tém s cieľom stanoviť základné bezpečnostné požiadavky.**
- Očakáva sa, že táto funkcia bude poskytovať strategický dohľad nad programom kybernetickej bezpečnosti subjektu, čím sa podčiarkne záväzok vrcholového manažmentu v oblasti kybernetickej bezpečnosti. Vzhľadom na veľkosť organizácie by táto funkcia mala zahŕňať aj zodpovednosť za riadenie rizík kybernetickej bezpečnosti, vrátane identifikácie navrhovaných nápravných opatrení.
- Na definovanie tejto úlohy vypracoval pracovník ľudských zdrojov popis pracovnej náplne kombináciou prvkov z **profilov úloh CISO a manažéra pre riziká kybernetickej bezpečnosti** podľa ECSF. Po obsadení bola táto úloha formálne označená ako CISO v organigrame organizácie.

Krok 2: Zvýšenie kvalifikácie právnika

- **Právnik, ktorý už riadi dodržiavanie právnych a regulačných rámcov, prejavil záujem o zdokonalenie svojich zručností v oblasti ochrany súkromia a kybernetickej bezpečnosti, aby mohol riešiť úlohy 5 a 6.**
- Oddelenie ľudských zdrojov podporilo jeho zdokonalenie kvalifikácie pomocou zoznamu kľúčových znalostí a zručností z ECSF. Nakoniec sa zdokonalil na pozíciu špecialista pre riadenie súladu.

Krok 3: Zvýšenie kvalifikácie správcov IT a systémov

- IT a systémoví administrátori postupovali podľa rôznych osvedčených postupov a rámcov v oblasti kybernetickej bezpečnosti a pracovali väčšinou ad hoc, bez stratégie alebo štruktúry. Na **riešenie úlohy 7** sa CISO rozhodol zdokonalit' zručnosti IT a systémových administrátorov prostredníctvom cieleného školenia, pri ktorom využil zoznam kľúčových vedomostí a zručností z ECSF v roli Implementátor kybernetickej bezpečnosti (špecialista KB).
- To im umožnilo bezpečne implementovat', prevádzkovat', udržiavat' a podporovat' technické riešenia, vrátane bezpečnej konfigurácie, správy záplat a testovania systémov. Toto zdokonalenie tiež pripravilo IT a systémových administrátorov na efektívnu účast' na riešení incidentov v úzkej spolupráci s externými špecialistami na **riešenie úlohy 10**.

Krok 4: Architekt KB

- Organizácii tiež chýbali interné kompetencie potrebné na navrhovanie a integráciu bezpečných digitálnych riešení. V dôsledku toho sa CISO rozhodol funkciu Architekt KB ad hoc outsourcovať.

Krok 5: Outsourcing spravodajských informácií o kybernetických hrozbách a reakcie na incidenty

- Na riešenie úloh 9 a 10 sa CISO rozhodol outsourcovať reakciu na kybernetické incidenty, spravodajské informácie o kybernetických hrozbách a digitálne forenzné vyšetrovanie špecializovanej organizácii, ktorá je schopná poskytovať nepretržité monitorovanie, pokročilú detekciu hrozieb, digitálnu forenznú analýzu a účinné opatrenia na obmedzenie šírenia (containment), čím zabezpečí rýchlu a koordinovanú reakciu. Role: Cyber Incident Responder, CTI Specialist a Digital Forensic Investigator.
- Boli jasne definované dohody o úrovni služieb (SLA), aby sa stanovili očakávania týkajúce sa reakčného času a kvality služieb. Povinnosti v oblasti reportovania však nebolo možné delegovať, takže CISO si ponechal zodpovednosť za hlásenie incidentov v súlade s regulačnými požiadavkami.
- CISO si uvedomil, že úspešná reakcia na incidenty vyžaduje spoluprácu medzi internými a externými tímami, a uznal potrebu zdokonaliť zručnosti interných IT a systémových administrátorov – túto potrebu rieši krok 3.

Krok 6: Zapojenie externých odborníkov na špecializovanú podporu

- Vzhľadom na nedostatok interných kompetencií sa CISO rozhodol outsourcovať jednorazové úlohy 4, 8 a 11 externým odborníkom na základe analýzy nákladovej efektívnosti a priorizácie úloh. Využitím ECSF identifikoval CISO kľúčové úlohy, ktoré je potrebné outsourcovať, a to konkrétne pravidelné audity kybernetickej bezpečnosti, penetračné testovanie a hodnotenie zraniteľnosti, ako aj špecializované školenia v oblasti kybernetickej bezpečnosti. Role Cybersecurity Auditor, Penetration Tester, Cybersecurity Educator
- Na poskytovanie týchto služieb boli uzatvorené zmluvy so špecializovanými poskytovateľmi, ktoré definujú ich rozsah a časový harmonogram.

Krok 7: Neustále monitorovanie a zlepšovanie

- S cieľom zabezpečiť neustále zlepšovanie a zodpovednosť CISO v spolupráci s vrcholovým manažmentom zaviedol monitorovací mechanizmus založený na jasne definovaných kľúčových ukazovateľoch výkonnosti (KPI) a kritériách úspešnosti. Tieto ukazovatele sa používali na meranie pokroku a účinnosti každého kroku uvedeného v pláne.

Scenár 2

- **SCENÁR 2: IMPLEMENTÁCIA POŽIADAVIEK NA HLÁSENIE A PRE REAKCIU PO INCIDENTE**

- V tomto príklade sa zameriavame výlučne na povinnosti v oblasti reakcie a podávania správ po incidente (Úloha 10) v rámci tej istej stredne veľkej organizácie. Ilustrujeme, ako je možné efektívne splniť požiadavky ZoKB prostredníctvom úloh a spolupráce rolí ECSF v rámci organizácie.
- Aby splnili požiadavky na reakciu na kybernetické incidenty a ich hlásenie, vytvorilo vrcholové vedenie **interný tím kvalifikovaných odborníkov**. Keďže si uvedomovali, že ako stredne veľká spoločnosť nemajú dostatočné interné kapacity, zručnosti ani zdroje na obsadenie špecializovaného interného tímu, využili **tri (3) vopred stanovené pozície: CISO, implementátor kybernetickej bezpečnosti a compliance právnika pre riadenie súladu**, spolu s **externou špecializovanou organizáciou** poskytujúcou služby **v oblasti reakcie na incidenty, spravodajských informácií o hrozbách a digitálnej forenznej analýzy.**
- Cieľom tímu bolo zabezpečiť účinnú reakciu a hlásenie incidentov v oblasti kybernetickej bezpečnosti v plnom súlade s ZoKB.

Krok 1: Vypracovanie plánu reakcie na incidenty a ďalšie udalosti

- Prvým krokom tímu bolo vypracovanie plánu reakcie na incidenty. CISO s podporou externých služieb vypracoval návrh plánu. Úlohy a zodpovednosti boli jasne definované a oznámené celému tímu. Plán reakcie na incidenty obsahoval aj šablóny pre všetky druhy hlásení incidentov a ďalších udalostí (významné hrozby, udalosti odvrátené na poslednú chvíľu a závažné zraniteľnosti) uvedených v § 24 ods. 1 a ods. 5 ZoKB, a v súlade s Vyhláškou NBÚ č. 226/2025 Z.z.

Krok 2: Pripravenosť na reakciu na incidenty a cvičenia

- Po zavedení plánu organizácia podnikla kroky na zabezpečenie pripravenosti prostredníctvom pravidelných testov. CISO v spolupráci s tímom organizoval pravidelné cvičenia reakcie na incidenty, aby posúdil účinnosť plánu. Tieto cvičenia pomohli tímu zoznámiť sa so svojimi úlohami, skrátiť reakčný čas a identifikovať oblasti, ktoré je potrebné zlepšiť.

Krok 3: Detekcia, analýza a klasifikácia incidentu

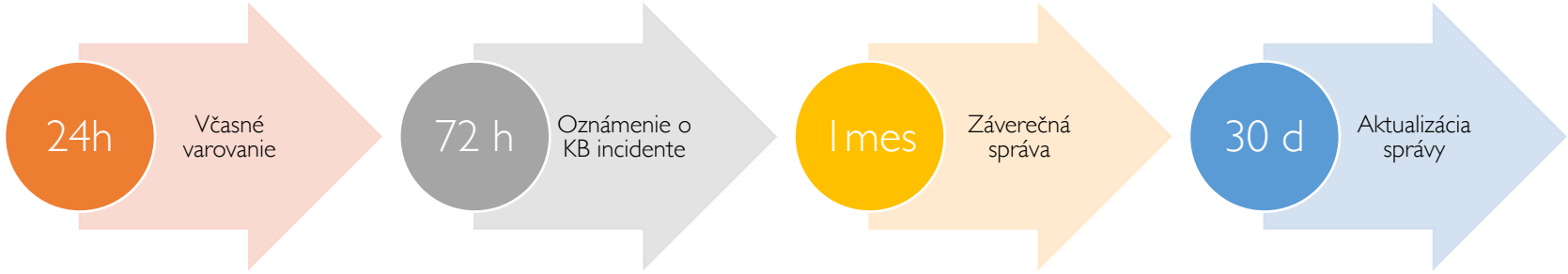
- Špecialista kybernetickej bezpečnosti, systémový administrátor, ktorý bol dodatočne vyškolený na plnenie tejto úlohy, dostal od svojho systému monitorovania siete upozornenie na možný náznak pokusu o exfiltráciu údajov. Špecialista kybernetickej bezpečnosti rýchlo zavolal CISO. CISO spolupracoval a požiadal o podporu externú službu, aby poskytla kontext a informácie o možnom vplyve zistenej aktivity.
- Tím začal svoju analýzu na diaľku a identifikoval sofistikovaný phishingový útok, ktorý obišiel počiatočné ochranné mechanizmy a bol pravdepodobne zodpovedný za podozrivé správanie siete.
- Po počiatočnej analýze CISO klasifikoval incident a posúdil jeho závažnosť, aby určil, či spĺňa prahové hodnoty pre hlásenie podľa ZoKB a Vyhlášky NBÚ č. 226/2025.

Riešenie kybernetického bezpečnostného incidentu	**Bezodkladne**	riešením incidentu je aktivita a postup zamerané na prevenciu, odhaľovanie, analýzu a obmedzovanie incidentu alebo na reakciu naň a zotavenie z neho
Kontaktná osoba pre prijímanie a evidenciu hlásení	**Bez zbytočného odkladu**	určiť osobu, ktorá bude prijímať a evidovať hlásenia. Táto osoba bude komunikovať v prípade incidentu v mene organizácie, typicky to bude bezpečnostný manažér alebo člen CSIRT tímu.

Krok 4: Počiatočné hlásenie – 24-hodinová lehota

- Podľa ZoKB má organizácia 24 hodín na to, aby o incidente informovala SK-CERT, VJ CSIRT . Po klasifikovaní incidentu ako predbežne závažného podľa ZoKB, CISO v spolupráci so špecialistom pre riadenie súladu pripravil počiatočnú správu o včasnom varovaní a informoval o incidente vrcholový manažment. Správa bola vypracovaná na základe technických podrobností, počiatočnej analýzy a opatrení na zmiernenie následkov, ktoré poskytol špecialista kybernetickej bezpečnosti a dodávateľ externých služieb. Správa bola zaslaná cez JISKB na SK-CERT v požadovanej lehote.

Hlásenie závažných kybernetických bezpečnostných incidentov na NBÚ	**Bezodkladne po zistení incidentu**	prostredníctvom jednotného informačného systému kybernetickej bezpečnosti. Možnosť aj dobrovoľného hlásenia každého incidentu/ udalosti.



Krok 5: Podrobná správa do 72 hodín

- V priebehu nasledujúcich 72 hodín musí organizácia poskytnúť správu o incidente, ktorá obsahuje stav správy o včasnom varovaní (ak je to relevantné) z kroku 3, počiatočné posúdenie závažnosti a dopadu spolu s indikátormi kompromitácie. CISO, špecialista kybernetickej bezpečnosti a externé služby úzko spolupracovali, aby odhalili celý rozsah porušenia. Identifikovali vstupný bod, posúdili údaje, ku ktorým bol získaný prístup, a odporučili okamžité opatrenia na zastavenie hrozby.
- CISO a špecialista na riadenie súladu spolupracovali na zostavení podrobnej správy na základe vstupov od dodávateľa externých služieb. Správa obsahovala závažnosť a dopad na služby organizácie a indikátory kompromitácie (t. j. neobvyklá sieťová prevádzka a neoprávnená aktivita používateľov). Komplexná správa bola predložená CSIRT v lehote 72 hodín.

Informovať v nevyhnutnom rozsahu tretiu stranu o hlásenom kybernetickom bezpečnostnom incidente za predpokladu, že by sa plnenie zmluvy stalo nemožným	**Ihneď po hlásení incidentu**	ak NBÚ nerozhodne inak
Súčinnosť	**Bez zbytočného odkladu**	spolupracovať s NBÚ a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu

Krok 6: Komunikácia a priebežné správy

- Po 72-hodinovej správe o incidente musí tím na žiadosť CSIRT predložiť priebežnú správu o aktuálnom stave s uvedením ich závažnosti a dopadu. CISO, špecialista kybernetickej bezpečnosti a dodávateľ externých služieb spolupracovali na zmiernení a zvládnutí incidentu, zhromaždili ďalšie dôkazy a požiadali o podporu CSIRT pri ďalších snahách o zvládnutie incidentu.
- Počas celého procesu CISO udržiaval otvorenú komunikáciu s CSIRT a poskytoval aktualizácie o opatreniach na zmiernenie incidentu. CISO tiež spolupracoval s špecialistom na riadenie súladu, aby zostavil priebežnú správu o stave incidentu na základe informácií od špecialistu kybernetickej bezpečnosti a dodávateľa externých služieb po žiadosti CSIRT.

Zabezpečenie dôkazu	**Bez zbytočného odkladu**	v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní
Podanie trestného oznámenia	**Bez zbytočného odkladu**	ak sa PZS hodnoverným spôsobom dozvie, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka.
Analýza závislosti	**Bez zbytočného odkladu**	Analyzovať závislosti svojich aktív, informačných systémov, využívaných produktov IKT a služieb IKT tretích strán v dodávateľskom reťazci a poskytovaných služieb s cieľom identifikovať možné dopady kybernetického bezpečnostného incidentu.

Krok 7: Záverečná správa

- Do jedného mesiaca od podania správy o incidente musí organizácia predložiť záverečnú správu. Táto správa musí obsahovať komplexný popis incidentu, vrátane typu hrozby alebo základnej príčiny, implementovaných a prebiehajúcich opatrení na zmiernenie následkov a, ak je to relevantné, cezhraničného vplyvu incidentu.
- CISO, špecialista kybernetickej bezpečnosti a dodávateľ externých služieb pokračovali vo svojich snahách a incident úspešne zvládli. Zozbierali tiež ďalšie dôkazy, ktoré budú zahrnuté do záverečnej správy.
- CISO a špecialista pre riadenie súladu spolupracovali s tímom a pripravili záverečnú správu na základe správy špecialistu kybernetickej bezpečnosti o opatreniach na zmiernenie dôsledkov a príspevkov od dodávateľa externých služieb. Počas každého kroku CISO zapojil vrcholový manažment a informoval ho o stave incidentu, prijatých opatreniach, potrebných zdrojoch a implementovaných opatreniach na zmiernenie dôsledkov.

Krok 8: Preskúmanie a následné opatrenia po incidente

- V poslednom kroku sa tím zišiel na preskúmaní po incidente, aby identifikoval poučenia a získané skúsenosti (lesson learned) a posúdil účinnosť opatrení prijatých na predchádzanie budúcim incidentom. Na základe tejto analýzy sa dohodli na posilnení postavenia organizácie v oblasti kybernetickej bezpečnosti prostredníctvom nasledujúcich opatrení, napr.

1. Posilniť koordináciu s externými tímami vytvorením formálnych komunikačných protokolov a vypracovaním jednotného postupu reakcie na incidenty.
2. Revízia postupov hlásenia incidentov, aby sa skrátil reakčný čas a zabezpečilo sa presnejšie dodržiavanie regulačných požiadaviek.

Použitie ECSF v kontexte AI

- **Uvažujeme o kybernetickej bezpečnosti a AI z oboch strán**

- AI ovplyvňuje bezpečnostné role: ako predmet štúdia ako rastúci vektor hrozieb ako príležitosť na zlepšenie
- Každý profil ECSF je dotknutý AI nejakým spôsobom
- AI nie je len „nová technológia“, ale zároveň aj nová hrozba aj nový nástroj – teda zasahuje všetky bezpečnsotné roly.

Použitie ECSF v kontexte AI

- **CTI špecialista, Špecialista na riadenie rizík, Výskumník:** analyzujú AI-súvisiace riziká, monitorujú vznikajúce AI hrozby skúmajú AI zraniteľnosti, aby boli pred bezpečnostnými problémami
- **Pentračný tester, Špecialista na analýzu digitálnych stôp, Špecialista pre riešenie kybernetických incidentov:** Integráciou AI môžu efektívnejšie identifikovať zraniteľnosti, rýchlejšie analyzovať forenzné dáta, reagovať na incidenty rýchlejšie a presnejšie, zlepšiť celkové schopnosti a výkon
- AI tu funguje dvojako: zvyšuje riziká (nové typy útokov) a zároveň zvyšuje efektivitu bezpečnostných tímov (detekcia/forenzná analýza/IR).

Použitie ECSF v kontexte AI

- **Architekt KB, Špecialista KB, Lektor KB:** Potrebujú vedieť ako navrhovať, implementovať a učiť AI-integrované systémy bezpečne
- **Manažér KB, Auditor KB, Špecialista riadenia súladu:** musia adresovať riziká AI a tvoriť politiky, robiť audity AI systémov z hľadiska súladu a bezpečnosti zabezpečiť, aby nasadzovanie AI bolo v súlade s právnymi a etickými štandardmi
- **Dôraz je na governance:** nestačí „AI nasadiť", treba vedieť nastavovať pravidlá, audit a súlad

Použitie ECSF v kontexte AI

- Problém rozdeľujeme na dve hlavné otázky:

1. **Ako kontextualizovať ECSF pre AI?**
2. **Sú profily ECSF ovplyvnené AI technológiami – a ak áno, ako?**

- Prvá otázka je „ako upraviť rámec zručností“, druhá „ako sa mení obsah práce jednotlivých rolí“.

- Podľa § 20 ods. 4 písm. g), i) ZoKB bezpečnostné opatrenia musia zahŕňať aj **určenie a pridelenie úloh, rolí a zodpovednosti** podľa podmienok prevádzkovateľa základnej služby a **zabezpečenie primeraného vzdelávania a preškoľovania pre všetky zavedené roly, ako aj vzdelávanie a budovanie bezpečnostného povedomia** v oblasti kybernetickej bezpečnosti.
- Podrobnosti o vzdelávaní a budovaní bezpečnostného povedomia v kybernetickej bezpečnosti by mala určiť vyhláška NBÚ

Penetračný tester

- Najprv sa zameriame na jeden profil
- Na strane ECSF: profil Penetračný tester
- Na strane AI: viacvrstvový rámec ENISA (Multilayer framework

Množstvo zdrojov o AI bezpečnosti

- Model inversion & extraction (inverzia/extrakcia modelu)
- Adversarial ML
- Data poisoning (adverzariálne útoky, otrava dát)
- AI/ML základy, aplikácia algoritmov AI zraniteľnosti a testovanie
- AI-based tools
- AI-based automation
- AI certifikácie, AI regulácia a etika (napr. AI Akt)
- Príklady zdrojov/nástrojov/rámcov: MITRE ATLAS, MLSecOps, OWASP Top 10 (LLM), OWASP Top 10 for Agentic Applications for 2026

Zdroj: ENISA

Penetračný tester

- **ECSF Penetračný tester:** hodnotí účinnosť bezpečnostných opatrení, odhaľuje a využíva zraniteľnosti a hodnotí ich kritickosť pri zneužití útočníkom

→

- **Penetračný tester špecializovaný na AI:**
- hodnotí účinnosť opatrení **chrániacich AI systémy**,
- odhaľuje a využíva **AI-súvisiace zraniteľnosti**,
- používa **AI-vylepšené nástroje/metodiky** pri penetračných testoch

- Príklad posunu v zručnosti: Sociálne inžinierstvo

→

- Sociálne inžinierstvo **s generatívnou AI**

- Príklad posunu vo vedomostiach: Odporúčania v KB a postupy najlepšej praxe

→

- Odporúčania pre **bezpečnosť a dôveryhodnosť AI systémov**

Cieľom je jasne pomenovať, **ktoré úlohy/zručnosti/vedomosti** AI mení a ako (AI systémy, AI nástroje, AI ako predmet štúdia, AI ako príležitosť)