AGENTÚRA EURÓPSKEJ ÚNIE
PRE KYBERNETICKÚ
BEZPEČNOSŤ


# UŽÍVATEĽSKÁ PRÍRUČKA

## EURÓPSKY RÁMEC ZRUČNOSTI V OBLASTI KYBERNETICKEJ BEZPEČNOSTI (ECSF)

SEPTEMBER 2022

# O AGENTÚRE ENISA

Agentúra Európskej únie pre kybernetickú bezpečnosť, ENISA, je agentúrou Únie, ktorá sa zameriava na dosiahnutie vysokej spoločnej úrovne kybernetickej bezpečnosti v celej Európe. Agentúra Európskej únie pre kybernetickú bezpečnosť zriadená v roku 2004 a posilnená Aktom EÚ o kybernetickej bezpečnosti prispieva ku kybernetickej politike EÚ, zvyšuje dôveryhodnosť IKT produktov, služieb a procesov so systémami certifikácie kybernetickej bezpečnosti, spolupracuje s členskými štátmi a orgánmi EÚ a pomáha Európe pripraviť sa na kybernetické výzvy budúcnosti. Prostredníctvom výmeny poznatkov, budovania kapacít a zvyšovania informovanosti, agentúra spolupracuje so svojimi kľúčovými zainteresovanými stranami s cieľom posilniť dôveru v prepojenú ekonomiku, zvýšiť odolnosť infraštruktúry Únie a v konečnom dôsledku zabezpečiť digitálnu bezpečnosť európskej spoločnosti a občanov. Viac informácií o agentúre ENISA a jej práci nájdete tu: www.enisa.europa.eu.

## KONTAKT

Pre kontaktovanie redaktora použite euskills@enisa.europa.eu.

## POĎAKOVANIE

Tento rámec je výsledkom odborného stanoviska a dohody pracovnej skupiny ad hoc pre rámec zručností, ktorú tvoria Agata BEKIER, Vladlena BENSON, Jutta BREYER*, Fabio DI FRANCO, Sara GARCIA, Athanasios GRAMMATOPOULOS, Markku KORKIAKOSKI, Csaba KRASZNAY, Haralambos MOURATIDIS, Christina GEORGHIADOU, Erwin ORYE*, Edmundas PIESARSKAS, Nineta POLEMI*, Paresh RATHOD*, Antonio SANNINO, Fred VAN NOORD, Richard WIDH, Nina OLESEN a Jan HAJNY.

Fabio DI FRANCO a Athanasios GRAMMATOPOULOS viedli túto činnosť pre agentúru ENISA.

## PRÁVNE OZNÁMENIE



## UPOZORNENIE O AUTORSKÝCH PRÁVACH

*Spravodajca ad-hoc pracovnej skupiny pre európsky rámec zručností v oblasti kybernetickej bezpečnosti

ISBN: 978-92-9204-584-5 – DOI: 10.2824/859537

# Obsah

# ZHRNUTIE

**Cieľom európskeho rámca zručnosti v oblasti kybernetickej bezpečnosti (ECSF) je posilniť európsku kultúru kybernetickej bezpečnosti poskytovaním spoločného európskeho jazyka vo všetkých komunitách, čo predstavuje zásadný krok vpred smerom k digitálnej budúcnosti Európy.**

Nedostatok pracovnej sily v oblasti kybernetickej bezpečnosti a nedostatok zručností sú hlavným problémom tak hospodárskeho rozvoja, ako aj národnej bezpečnosti. Pri skúmaní tohto problému agentúra ENISA identifikovala potrebu komplexného prístupu Európy na vymedzenie súboru úloh a zručností kybernetickej bezpečnosti, ktoré by sa mohli využiť na zníženie nedostatku a medzery v zručnostiach. Agentúra ENISA pracovala na vývoji takéhoto rámca a predstavuje **európsky rámec zručnosti v oblasti kybernetickej bezpečnosti (ECSF)**, ktorého cieľom je posilniť európsku kultúru kybernetickej bezpečnosti tým, že poskytne spoločný európsky jazyk vo všetkých komunitách a urobí zásadný krok smerom k digitálnej budúcnosti Európy.

ECSF poskytuje praktický nástroj **na podporu identifikácie a formulácie úloh, kompetencií, zručností a znalostí súvisiacich** s úlohami európskych **odborníkov v oblasti kybernetickej bezpečnosti.** Hlavným účelom rámca je **vytvoriť spoločné porozumenie** medzi jednotlivcami, zamestnávateľmi a poskytovateľmi vzdelávacích programov v členských štátoch EÚ, čím sa z neho stane cenný nástroj na preklenutie priepasti medzi profesionálnym pracoviskom kybernetickej bezpečnosti a vzdelávacími prostrediami.

Rámec opisuje najdôležitejšie požiadavky profesionálneho pracoviska pre kybernetickú bezpečnosť vymedzením **súboru 12 typických profilov profesionálnych rolí v oblasti kybernetickej bezpečnosti**. Tieto profily poskytujú spoločné chápanie hlavných úloh kybernetickej bezpečnosti a zručností potrebných v profesionálnom kontexte kybernetickej bezpečnosti, čo z neho robí dokonalú referenciu pre zručnosti a znalosti v oblasti profilovania, ktoré potrebujú odborníci v oblasti kybernetickej bezpečnosti. Rámec bol navrhnutý tak, aby bol ľahko zrozumiteľný a dostatočne komplexný na to, aby poskytoval primerané podrobné informácie o kybernetickej bezpečnosti, ako aj dostatočne flexibilný, aby umožnil prispôsobenie na základe potrieb každého používateľa. Začlenením všetkých zainteresovaných strán sa rámec vzťahuje na všetky typy organizácií a podporuje rozvoj všetkých profesií v oblasti kybernetickej bezpečnosti.

ECSF je výsledkom práce ad hoc pracovnej skupiny agentúry ENISA pre európsky rámec zručností v oblasti kybernetickej bezpečnosti[1], ktorú tvoria odborníci zastupujúci rôzne názory. Vypracovaný rámec je založený na analýze existujúcich rámcov, výsledkoch a zisteniach z výskumu potrieb trhu a na dohode medzi odborníkmi. Prípadové štúdie používateľov a orientačné príklady inšpirované rôznymi pracoviskami a vzdelávacími prostrediami demonštrujú praktickú implementáciu tohto rámca a podporujú túto prácu.

Zistilo sa, že hlavnými výhodami používania ECSF sú:

- zabezpečenie spoločnej terminológie a spoločného porozumenia, pokiaľ ide o odborníkov v oblasti kybernetickej bezpečnosti v celej EÚ;
- určenie súboru kritických zručností potrebných z hľadiska pracovnej sily v oblasti kybernetickej bezpečnosti na podporu jej ďalšieho rozvoja a zlepšovania;
- podpora harmonizácie programov vzdelávania, odbornej prípravy a rozvoja pracovnej sily v oblasti kybernetickej bezpečnosti.

[1] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls

Táto používateľská príručka ECSF poskytuje komplexný prehľad o hlavnom rozsahu pôsobnosti, rámcových zásadách a možnostiach použitia ECSF. Hlavným účelom príručky je zabezpečiť, aby bol ECSF ľahko dostupný, zrozumiteľný a použiteľný pre všetky zainteresované strany s aktívnou úlohou alebo potrebou primerane kvalifikovaných odborníkov v oblasti kybernetickej bezpečnosti.

# 1. ÚVOD

Nedostatok zručností v oblasti kybernetickej bezpečnosti je jednou z kľúčových výziev, ktoré je potrebné riešiť v záujme kybernetickej bezpečnosti Európskej únie. Presnejšie povedané, na trhu práce chýba skúsený a kvalifikovaný personál, ktorý by mohol prevziať úlohu v oblasti kybernetickej bezpečnosti a ktorý dokáže dostatočne riešiť vyvíjajúce sa kybernetické hrozby a vznikajúce výzvy v oblasti kybernetickej bezpečnosti. Medzery v zručnostiach v oblasti kybernetickej bezpečnosti majú niekoľko základných faktorov. Patrí medzi ne nedostatočná úroveň pochopenia kompetencií a zručností potrebných v disciplíne kybernetickej bezpečnosti medzi rôznymi aktérmi na trhu so zručnosťami kybernetickej bezpečnosti. V priebehu rokov sa to stalo dobre zdokumentovaným problémom[2], ktorý naďalej výrazne ovplyvňuje krajiny na európskej a medzinárodnej úrovni.

**ECSF poskytuje otvorený európsky nástroj na vytvorenie spoločného chápania profilov profesionálnych rolí v oblasti kybernetickej bezpečnosti a spoločných mapovaní s primeranými požadovanými zručnosťami a kompetenciami.**

Na zníženie súčasnej a budúcej medzery a nedostatku zručností je potrebných viac odborníkov v oblasti kybernetickej bezpečnosti s vhodnými súbormi zručností. Na tento účel zostávajú európsky program v oblasti zručností, akčný plán[3] digitálneho vzdelávania[4] a pakt o zručnostiach[5] aj naďalej dôležitými nástrojmi na mobilizáciu zainteresovaných strán, aby spolupracovali na dosahovaní cieľov digitálneho desaťročia[6] vytvorením väčšieho počtu lepších príležitostí na odbornú prípravu.

V tejto súvislosti agentúra ENISA v decembri 2020 spustila ad hoc pracovnú skupinu pre európsky rámec zručností[7] v oblasti kybernetickej bezpečnosti. Spojila sa multidisciplinárna skupina odborníkov s cieľom podporiť harmonizáciu koncepcií vzdelávania, odbornej prípravy a rozvoja pracovnej sily v oblasti kybernetickej bezpečnosti. Vyvinutý rámec (ECSF) poskytuje otvorený európsky nástroj na vytvorenie spoločného chápania profilov profesionálnych rolí v oblasti kybernetickej bezpečnosti a spoločných mapovaní s potrebnými zručnosťami a kompetenciami. Táto práca poskytuje základ pre spojenie síl do programu budovania kapacít európskej pracovnej sily v oblasti kybernetickej bezpečnosti v súlade s pretrvávajúcim dopytom na trhu.

**Konečným rozsahom rámca ECSF sú odborníci v oblasti kybernetickej bezpečnosti, pričom dôraz sa kladie aj na odborníkov, ktorí nie sú v oblasti kybernetickej bezpečnosti a potrebujú komplexný pohľad na túto disciplínu.**

## 1.1 CIEĽOVÉ PUBLIKUM

Hoci konečným rozsahom obsahu rámca ECSF sú odborníci v oblasti kybernetickej bezpečnosti, osobitný dôraz sa kladie aj na cieľové skupiny odborníkov, ktorí nie sú v oblasti kybernetickej bezpečnosti, ktorí potrebujú komplexný pohľad na túto disciplínu. Vďaka tomuto zameraniu je rámec ľahko zrozumiteľný pre všetky zainteresované strany.

Cieľovou skupinou ECSF sú vedúce tímy organizácií, ľudské zdroje a funkcie kybernetickej bezpečnosti, odborníci v oblasti kybernetickej bezpečnosti, nováčikovia a kybernetickí nadšenci, ako aj poskytovatelia vzdelávacích programov všetkých typov vo verejnom a súkromnom kontexte, odvetvové združenia, výskumní pracovníci na trhu a tvorcovia politík.

## 1.2 ŠTRUKTÚRA PRÍRUČKY

Užívateľská príručka je štruktúrovaná nasledovne:

- V kapitole 1 sa uvádzajú kľúčové výzvy, ktoré zdôrazňujú potrebu vytvoriť rámec pre zručnosti kybernetickej bezpečnosti, ako aj cieľovú skupinu pre túto prácu;

[2] ENISA, 2020, Vývoj zručnosti v oblasti kybernetickej bezpečnosti v EU https://www.enisa.europa.eu/publications/the-status-of education-in-the-european-union
[3] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1196
[4] https://education.ec.europa.eu/focus-topics/digital-education/action-plan
[5] https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1197
[6] https://digital-strategy.ec.europa.eu/en/node/157
[7] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls

- V kapitole 2 sa uvádzajú zásady návrhu ECSF, ako aj kľúčové prínosy jeho používania;
- V kapitole 3 sa vysvetľujú rôzne použitia ECSF z rôznych hľadísk.

Okrem toho dokument obsahuje dve (2) prílohy, ktoré podporujú používateľskú príručku ECSF a jej ciele:

- Príloha A spája ECSF s inými normami a rámcami EÚ. Cieľom tejto prílohy je prepojiť ECSF s existujúcimi uznávanými európskymi normami a rámcami, ktoré sú relevantné pre túto prácu.

- V prílohe B sa uvádza zoznam prípadov použitia ECSF. Cieľom tejto prílohy je poskytnúť reálne scenáre s cieľom ukázať praktické vykonávanie tohto rámca.

# 2. POCHOPENIE ECSF

ECSF pozostáva z reprezentatívneho súboru 12 profilov rolí pre odborníkov v oblasti kybernetickej bezpečnosti (uvedených na obrázku 1), ktoré sa zvyčajne vyžadujú a uplatňujú v organizáciách nasadzujúcich odborníkov v oblasti kybernetickej bezpečnosti. Každý profil je definovaný spoločnou šablónou, ktorá obsahuje kľúčové kritériá množiny (t. j. názov, alternatívne názvy, súhrnné vyhlásenie, úloha, hlavné úlohy, kľúčové zručnosti, kľúčové znalosti, elektronické kompetencie). Obsah každého kritéria je prispôsobený každej úlohe, ale podlieha možnej adaptácii s cieľom umožniť pružnú implementáciu s cieľom splniť špecifické situácie a požiadavky.

**Obrázok 1:** 12 profilov rolí ECSF pre odborníkov v oblasti


**ECSF zavádza reprezentatívny súbor 12 profilov rolí pre odborníkov v oblasti kybernetickej bezpečnosti (zvyčajne sa vyžaduje a uplatňuje v rámci organizácií) vo formáte zameranom na prax venovanom profesionálnej oblasti kybernetickej bezpečnosti.**

12 profilov rolí pre profesionálov v oblasti kybernetickej bezpečnosti sa poskytuje vo formáte zameranom na profesionálnu kybernetickú bezpečnosť dohodnutom na úrovni EÚ. Profily sú ľahko zrozumiteľné a ponúkajú alternatívne vstupné body podľa kontextu, perspektívy a potreby. Prostredníctvom týchto profilov možno ECSF použiť ako spoločný referenčný a komunikačný nástroj, ktorý možno použiť v rôznych organizáciách a krajinách na spoločné, vzájomné vnútorné a vonkajšie porozumenie.

Štruktúra každého profilu rolí je uvedená v tabuľke 1.

**Tabuľka 1: Zložky profilu každej roly ECSF**

| Názov profilu | Názov profesionálneho profilu každej roly |
|---|---|
| Alternatívny názov (názvy) | Zoznam typických alternatívnych názvov pod rovnakým profilom. |
| Súhrnný výkaz | Označuje hlavný účel profilu. |
| Poslanie | Popisuje zdôvodnenie profilu. |
| Výstup (výsledky) | Zoznam typických výsledkov profilu, v ktorom sa vysvetľuje aj relevantnosť profilu z neexpertného hľadiska. |
| Hlavná úloha (hlavné úlohy) | Zoznam typických úloh vykonávaných profilovanou rolou. |
| Kľúčové zručnosti | Zoznam schopností potrebných na vykonávanie pracovných funkcií a povinností úlohy. Mäkké zručnosti a etika sú v niektorých prípadoch explicitné. |
| Kľúčové znalosti | Zoznam základných znalostí potrebných na vykonávanie pracovných funkcií a povinností v rámci profilovanej role. |
| Elektronické kompetencie (EN16234-1 e-CF) | Napojenie na rámec elektronických kompetencií (e-CF) EN16234-1- Spoločný európsky rámec pre odborníkov v oblasti IKT vo všetkých odvetviach. |

Ako sa uvádza v tabuľke 1, profil každej roly je vyplnený súborom opisných položiek určených na poskytnutie prehľadu úlohy z hľadiska jej opisu, úloh a kompetencií. Názvy a typické alternatívne názvy sa môžu použiť ako rýchly odkaz na usmernenie používateľov ECSF k najvhodnejším profilom rolí pre ich uplatňovanie.

**Zložky** profilov rolí **sa môžu zmeniť** tak, aby lepšie pokrývali potreby zainteresovaných strán, **a profily** rolí (z ECSF a iných rámcov) **sa môžu zmiešať** z rovnakého dôvodu. Viac informácií o uplatňovaní ECSF je uvedených v kapitole 3.

**Mäkké zručnosti** (nazývané aj prierezové, prenosné alebo behaviorálne zručnosti) sú komponenty, ktoré sú potrebné v každom súbore odborných zručností; takéto zručnosti sú preto potrebné aj pre odborníkov v oblasti kybernetickej bezpečnosti. Široká škála zručností spadá pod mäkké zručnosti, ako sú schopnosti komunikovať, spolupracovať s ostatnými, podávať správy, ovplyvňovať, kriticky myslieť a riadiť čas a stres. Kľúčové mäkké zručnosti sú začlenené do zložky kľúčových zručností.

Napríklad profil roly Hlavný úradník pre bezpečnosť informácií (CISO) zahŕňa ako kľúčové zručnosti schopnosti ovplyvňovať, viesť, komunikovať, spolupracovať a kolaborovať. To všetko sú základné zručnosti, ak má CISO dosiahnuť svoje úlohy a povinnosti. Na základe potrieb zainteresovaných strán by sa do profilu CISO mohlo pridať viac mäkkých zručností alebo sa môže vykonať mapovanie s rámcom mäkkých zručností.

**Etika** je tiež dôležitým prierezovým prvkom, ktorý má vplyv na všetky aspekty kybernetickej bezpečnosti, a preto je základným prvkom zručností v rámci európskeho rámca pre zručnosti v oblasti kybernetickej bezpečnosti (ECSF). V kontexte kybernetickej bezpečnosti je etika o tom, aké rozhodnutia sú v súlade s našimi hodnotami a čo je morálne prijateľné pre vlastníka údajov aj pre organizáciu. Keďže odborníci v oblasti kybernetickej bezpečnosti by mohli získať privilegovaný prístup k rôznym typom informácií, dokonca aj k citlivým informáciám, etické povedomie je dôležitou hodnotou, ktorú by mali mať. Okrem toho je

etické rozhodovanie dôležitou zručnosťou, ktorú by odborníci v oblasti kybernetickej bezpečnosti mali mať ako ich rozhodnutia sa týkajú iných jednotlivcov. Podobne ako v prípade mäkkých zručností ECSF výslovne analyzoval, či je etická stránka odvetvia v súlade s európskymi hodnotami a etikou.

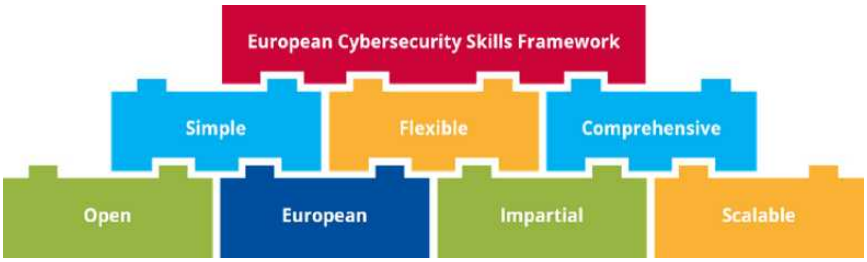
Zainteresovaná strana by mohla vykonať podrobnejšiu analýzu mäkkých a etických zručností, keďže rámec je flexibilný a prispôsobivý.

## 2.2 ZÁSADY NÁVRHU ECSF

Európsky rámec zručností v oblasti kybernetickej bezpečnosti je založený na niekoľkých zásadách určených na pokrytie potrieb zainteresovaných strán. To umožňuje jednoduché pochopenie, prijatie a uplatňovanie rámca pri súčasnom zachovaní relevantnosti a vplyvu v krátkodobom a dlhodobom horizonte.

**ECSF je založený na zásadách navrhnutých na pokrytie potrieb zainteresovaných strán a ponúka jednoduché pochopenie, prijatie a uplatňovanie pri súčasnom zachovaní relevantnosti a vplyvu v krátkodobom a dlhodobom horizonte.**

**Obrázok 2:** Zásady navrhovania ECSF




### 2.1.1 Jednoduchý, ale komplexný

Rámec je navrhnutý tak, aby bol vhodne všeobecný, aby sa zabezpečilo, že bude ľahko zrozumiteľný a uplatňovaný širším publikom. Zároveň je dostatočné detailný na to, aby bolo možné poskytnúť podrobné informácie o kybernetickej bezpečnosti. Tieto atribúty uľahčujú využívanie rámca v širokom spektre činností a prostredí a zainteresovanými stranami z rôznych prostredí (napr. organizácie rôznej veľkosti, technické odborné znalosti rôznej intenzity a podnikateľské sektory s rôznymi hlavnými činnosťami).

To sa dosiahlo uplatnením primeranej úrovne podrobnosti obsahu ECSF, ktorá nie je príliš špecifická ani príliš abstraktná. ECSF ponúka 12 profilov a pokrýva široké spektrum rôznych pracovných činností, ale zachováva ľahko použiteľný formát.

### 2.1.2 Flexibilný a škálovateľný

Prijatím modulárneho prístupu a flexibilnej štruktúry umožňuje rámec rozšíriť alebo používať každý komponent nezávisle. Tieto charakteristiky podporujú ďalšie rozšírenie ECSF a/alebo prepojenie na iné rámce s cieľom rozšíriť jeho uplatňovanie.

Pri uplatňovaní tejto flexibility sa profily a ich zložky, ako sú vymedzené v ECSF, môžu uplatňovať podľa jednotlivých modulov, aby sa každý z nich prispôsobil špecifickým potrebám. Táto flexibilita zabezpečuje relevantnosť rámca v priebehu rokov a umožní aj jednoduché aktualizácie rámca v budúcnosti.

### 2.1.3 Otvorený a nestranný

Rámec bol vypracovaný na základe podnetov od veľkej a rôznorodej pracovnej skupiny profesionálnych odborníkov na kybernetickú bezpečnosť. S cieľom vytvoriť nestranný rámec agentúra ENISA zriadila túto skupinu z rôznych odborníkov z rôznych prostredí. Zapojením odborníkov z rôznych prostredí sa v procese rozvoja rámca uplatňoval prístup založený na

viacerých perspektívach, ktorý odstránil akúkoľvek zaujatosť voči konkrétnym oblastiam záujmu. Okrem toho je rámec ako publikácia agentúry ENISA verejne dostupný, prístupný a otvorený.

Profily a zložky ECSF boli vyvinuté na základe perspektívy viacerých zainteresovaných strán so zameraním nielen na zamestnanosť v oblasti kybernetickej bezpečnosti, ale aj z hľadiska poskytovateľov vzdelávacích programov. Okrem toho sa pravdivosť rámca posilnila zapojením a preskúmaniami od rôznych ďalších zainteresovaných strán.

### 2.1.4 Európsky

Na základe požiadavky minimalizovať medzery v zručnostiach v oblasti kybernetickej bezpečnosti a nedostatok pracovnej sily v celej Európe musel byť ECSF v súlade s osobitnými európskymi požiadavkami, aby sa európskym organizáciám umožnilo jednoduché prijatie a používanie. Toto smerovanie bolo založené na dodržiavaní existujúcich európskych noriem a rámcov.

ECSF sa dobre spája so súčasným európskym profesionálnym prostredím v oblasti IKT, aby sa zabezpečilo jednoduché využívanie a široké uznanie. ECSF najlepšie využíva existujúce skúsenosti a štruktúry a poskytuje konzistentné prepojenia s príslušnými odbornými normami a rámcami EÚ v oblasti IKT. Profily vymedzené v rámci sú navrhnuté tak, aby boli v súlade s európskymi zákonmi a inými právnymi predpismi a doplňali ich a aby posilnili prístupy k európskej etike identifikované na európskom trhu. ECSF berie do úvahy požiadavky na ochranu údajov a súkromia stanovené európskymi nariadeniami, spoločné pracovné úlohy požadované európskym trhom a európske normy a rámce používané v odvetví IKT.

## 2.2 HLAVNÉ VÝHODY, KTORÉ POSKYTUJE ECSF

ECSF je ľahko použiteľný, ale komplexný nástroj. Vychádza z nedávnych štúdií trhu, spolupráce odborníkov na kybernetickú bezpečnosť a analýzy širšieho prostredia rámcov kybernetickej bezpečnosti a IKT. Vyjadruje tak relevantné potreby európskeho trhu. Pozostáva z 12 typických odborných úloh v oblasti kybernetickej bezpečnosti so súvisiacim súhrnným vyhlásením, poslaním, pozorovateľnými výsledkami (výsledkami), úlohami, kompetenciami, zručnosťami, úrovňami znalostí a odbornej spôsobilosti, ako sa vyžaduje a uplatňuje v kontexte práce v Európe, ktoré sa majú chápať a používať v celej Európe.

**ECSF poskytuje jednoznačný odkaz na identifikáciu a zníženie súčasnej a budúcej medzery a nedostatkov v zručnostiach v oblasti kybernetickej bezpečnosti.**

ECSF poskytuje jednoznačný odkaz na identifikáciu a zníženie súčasnej a budúcej medzery a nedostatkov v zručnostiach v oblasti kybernetickej bezpečnosti. Je všeobecný, ale zároveň dostatočne podrobný na to, aby sa trhu EÚ poskytla jasná taxonómia zručností, kompetencií a povolaní pracovnej sily v oblasti kybernetickej bezpečnosti. Okrem toho sa môže ľahko prepojiť s inými existujúcimi štruktúrami a rámcami v súvisiacich oblastiach.

Používanie ECSF ako spoločného európskeho jazyka pre profesionálne kybernetické-bezpečnostné úlohy, zručnosti, znalosti a kompetencie ponúka mnoho výhod, z ktorých niektoré sú uvedené nižšie.

1. Používanie ECSF zabezpečuje spoločnú terminológiu a spoločné porozumenie medzi kybernetickou bezpečnosťou (pracovisko, nábor) a ponukou (kvalifikácia, odborná príprava, hodnotenie a uznávanie) v celej EÚ.
2. ECSF podporuje identifikáciu kritických požiadaviek na súbor zručností z hľadiska pracovnej sily. Umožňuje poskytovateľom vzdelávacích programov podporovať rozvoj kritických zručností a tvorcom politík podporovať cielené iniciatívy na zmiernenie zistených nedostatkov v zručnostiach.
3. ECSF pomáha pri pochopení profesionálnych úloh v oblasti kybernetickej bezpečnosti a požadovaných základných zručností a príslušných právnych predpisov.

Najmä neodborníci a oddelenia ľudských zdrojov sú schopné lepšie pochopiť požiadavky na plánovanie zdrojov kybernetickej bezpečnosti, nábor a plánovanie kariéry.

4. ECSF podporuje harmonizáciu v oblasti vzdelávania, odbornej prípravy a rozvoja pracovnej sily v oblasti kybernetickej bezpečnosti. Používanie spoločného európskeho jazyka v zručnostiach a úlohách kybernetickej bezpečnosti sa okrem toho priamo týka celej profesionálnej oblasti IKT.

5. ECSF prispieva k dosiahnutiu lepšej odolnosti proti kybernetickým útokom a k zabezpečeniu bezpečných systémov IKT v celej spoločnosti. Poskytuje štandardnú štruktúru a poskytuje poradenstvo o tom, ako presadzovať budovanie kapacít európskej pracovnej sily v oblasti kybernetickej bezpečnosti.

ECSF poskytuje ďalšie výhody na základe typu zainteresovaných strán. Príklad hlavných zainteresovaných strán a kľúčových súvisiacich hlavných prínosov je uvedený v obrázku 3.

Obrázok 3: Príklad hlavných príjemcov ECSF, ktorý vyjadruje potrebu spoločnej definície manažéra pre riziká kybernetickej bezpečnosti


Podrobný zoznam potenciálnych aplikácií a prínosov využívania ECSF na základe zainteresovaných strán je uvedený v tabuľke 2.

**Tabuľka 2:** Potenciálne aplikácie a prínosy ECSF pre zainteresované strany

| Zainteresovaná strana | Výhody využívania ECSF |
|---|---|
| Organizácie | • podporuje rozvoj stratégie kybernetickej bezpečnosti a organizačnej štruktúry<br>• podporuje rozvoj plánovania ľudských zdrojov v oblasti kybernetickej bezpečnosti<br>• poskytuje podporu v procese prijímania zamestnancov, najmä:<br>  ○ identifikácia požiadaviek na kybernetickú bezpečnosť<br>  ○ hodnotenie kandidátov na kybernetickú bezpečnosť<br>• poskytuje analýzu úloh a medzery zručnosti kybernetickej bezpečnosti a následnú prognózu potreby na individuálnej, tímovej alebo organizačnej úrovni<br>• definuje plány rozvoja a odbornej prípravy na individuálnej, tímovej alebo organizačnej úrovni<br>• podporuje hodnotenie rolí kybernetickej bezpečnosti tým, že pomáha pri budovaní prispôsobených šablóny pre rolí kybernetickej bezpečnosti<br>• poskytuje spoločný a ľahko zrozumiteľný jazyk pre ponuky v oblasti kybernetickej bezpečnosti, verejné obstarávanie, voľné pracovné miesta a audity |
| Poskytovatelia vzdelávacích programov | • podporuje navrhovanie vzdelávacích programov a učebných plánov, prepracovanie a údržba<br>• ponúka spoluprácu medzi inštitúciami a mobilitu vo vzdelávacích programoch, napr. celoeurópske vzdelávacie programy viacerých inštitúcií<br>• podporuje ponuku vzdelávacích programov a zvyšuje informovanosť<br>• pozície výsledkov vzdelávania v reálnom kontexte pracoviska<br>• podporuje procesy hodnotenia a uznávania<br>• poskytuje študentom kariérnu orientáciu študentom |
| Jednotlivci | • podporuje jednotlivcov pri ich samostatnom výbere profesionálnej kariéry a pozícii<br>• rozširuje perspektívy vzdelávania, otvára nové kariérne dráhy a podporuje profesionálneho rozvoju na podporu zvyšovania kvalifikácie a rekvalifikácie zručností<br>• pomáha pochopiť praktické požiadavky na pracovisku a očakávania pracovných miest vo väčšom detailnom rozsahu<br>• identifikuje formálne a neformálne vzdelávacie cesty<br>• poskytuje podporu pri budovaní kariérnych cesty |
| Profesionálne združenia | • umožňuje konsolidáciu komunít zainteresovaných strán na podporu výmeny poznatkov,<br>• nový vývoj, zlepšenia a ďalšie vykonávanie v členských štátoch EÚ<br>• poskytuje podporu pri vykonávaní analýzy trhu a prezentácii výsledkov v spoločnom jazyk<br>• pomáha poskytovať komplexné odborné poradenstvo v sektore kybernetickej bezpečnosti |
| Tvorcovia politík a zainteresované strany verejnej správy | • podporuje spoločné porozumenie v oblasti kybernetickej bezpečnosti<br>• stimuluje prioritné plánovanie a budovanie kapacít v oblasti kybernetickej bezpečnosti<br>• umožňuje mapovať mnohé iniciatívy kybernetickej bezpečnosti založené na profiloch ECSF<br>• podporuje politické iniciatívy založené na analýze údajov |
| Všetko | • ponúka spoločný jazyk pre všetky zainteresované strany<br>• urýchľuje spoluprácu poskytnutím spoločného referenčného východiskového bodu<br>• poskytuje spoločný odkaz na zhromažďovanie a prezentáciu odborníkov v oblasti kybernetickej bezpečnosti<br>• informácie a potreby na všetkých úrovniach, na vnútroštátnej, európskej a medzinárodnej úrovni |

# 3. UPLATNENIA ECSF

Táto kapitola ukazuje, ako možno Európsky rámec zručností v oblasti kybernetickej bezpečnosti (ECSF) uplatňovať modulárnym a flexibilným spôsobom založeným na potrebách rôznych zainteresovaných strán.

Špecifické použitie a praktické použitie závisia od mnohých faktorov, ako je perspektíva trhu, veľkosť organizácie, kontext konkrétnej výkonnosti a celkový účel.

12 profilov rolí pre odborníkov v oblasti kybernetickej bezpečnosti vymedzených ECSF sú flexibilným nástrojom a štandardnou európskou referenciou pre prispôsobené používanie v konkrétnom kontexte.

**12 profilov rolí definovaných ECSF je flexibilným nástrojom a štandardnou európskou referenciou pre individuálne použitie v konkrétnom kontexte.**

Táto všeobecná päťstupňová príručka poskytuje základnú orientáciu:

**Obrázok 4:** Modulárna päťstupňová príručka na uplatňovanie ECSF


1. Analyzovať situáciu cieľového prostredia.
Zhromažďovať a spracúvať vhodné informácie potrebné o stave cieľového prostredia súvisiaceho s kybernetickou bezpečnosťou (napr. organizácia) na vytvorenie východiskovej hodnoty. Identifikovať zúčastnené strany a cieľ, ktorý sa má dosiahnuť.

2. Identifikovať konkrétne ciele, ktoré sa majú dosiahnuť.
Preskúmať stav cieľového prostredia a identifikovať všetky konkrétne požiadavky súvisiace s kybernetickou bezpečnosťou, ktoré sa majú pokryť, alebo akýkoľvek cieľ, ktorý sa má dosiahnuť v cieľovom prostredí. V závislosti od situácie môže byť možné použiť ECSF ako taxonómiu na identifikáciu predmetných cieľov.

3. Vybrať príslušné zložky ECSF.
Preskúmať profily ECSF a vybrať profily, ktoré sú relevantné pre konkrétnu situáciu. Potom vybrať zložky, ktoré pomáhajú pokryť potreby alebo dosiahnuť požadované ciele cieľového prostredia.

4. Prispôsobovať vybrané komponenty podľa vašich potrieb.
Vykonať vhodné zmeny vo vybraných komponentoch, aby lepšie vyhovovali konkrétnej situácii a/alebo cielenému prostrediu. Profily ECSF a/alebo ich zložky možno zmiešať, rozdeliť alebo uviesť do kontextu špecifického odvetvia podľa potrieb každej situácie.

5. Aplikovať prispôsobené komponenty do cieľového prostredia.
Prijať opatrenia s použitím prispôsobených komponentov ECSF na pokrytie cieľov súvisiacich s bezpečnosťou, ktoré sú potrebné na zlepšenie situácie v cieľovom prostredí a na dosiahnutie organizačného cieľa.

V tabuľke 3 sú uvedené niektoré orientačné príklady uplatnení ECSF podľa vyššie uvedených piatich krokov.

**Tabuľka 3: Modulárny prístup ECSF v praxi**

| Príklad | Krok | Popis |
|---|---|---|
| **Zamestnávať odborníkov v oblasti kybernetickej bezpečnosti v organizácii** | 1. Analyzovať | Analyzovať súčasný stav organizácie súvisiaci s kybernetickou bezpečnosťou. |
| | 2. Identifikovať | Identifikovať nedostatok personálu na zvládnutie nárastu problémov v oblasti kybernetickej bezpečnosti. |
| | 3. Vybrať | Vyberať príslušnú úlohu z profilu ECSF, ktorý vyjadruje zistený nedostatok špecifických zručností alebo medzera v nich. |
| | 4. Prispôsobiť | Kombinovať profily ECSF s úlohami, ktoré sú zaujímavé pre organizáciu, a štruktúrovať nové úlohy s aktualizovanými úlohami, zručnosťami a vedomosťami s cieľom uspokojiť meniace sa organizačné potreby a vytvoriť zmenené kybernetickej bezpečnosti úlohy. |
| | 5. Aplikovať | Použite novovytvorený profil na vytvorenie voľných pracovných miest zameraných na špecifické potreby organizácie. |
| **Zlepšovať zručnosti v oblasti kybernetickej bezpečnosti** | 1. Analyzovať | Pochopiť obchodné ciele a stratégiu organizácie. |
| | 2. Identifikovať | Identifikovať nedostatok odborných znalostí a personálu v oblastiach súvisiacich s kybernetickou bezpečnosťou. |
| | 3. Vybrať | Použiť profil(-y) ECSF na identifikáciu súvisiacich zručností a znalostí, ktoré organizácii chýbajú. |
| | 4. Prispôsobiť | Analyzovať vybrané zručnosti a znalosti z ECSF s cieľom identifikovať potreby odbornej prípravy odborníka v oblasti kybernetickej bezpečnosti s cieľom uspokojiť potreby organizácie. |
| | 5. Aplikovať | Identifikovať zásahy v oblasti odbornej prípravy na posilnenie kompetencií pracovnej sily organizácie. |
| **Robiť vlastné kariérne rozhodnutia** | 1. Analyzovať | Vyberať si kariérnu cestu, o ktorú máte záujem. |
| | 2. Identifikovať | Identifikovať svoje nedostatočné zručnosti a znalosti potrebné na prechod do sektora kybernetickej bezpečnosti. |
| | 3. Vybrať | Určiť profil(-y) ECSF, ktorý považujete za užitočný z hľadiska kariérneho rastu, a využiť súvisiace zručnosti, znalosti a kompetencie ako usmernenia na rekvalifikáciu a zvyšovanie úrovne zručností. |
| | 4. Prispôsobiť | Zlepšiť vybrané profily ECSF zahrnutím dodatočných zručností a znalostí založených na individuálnych potrebách. |

| | | |
|---|---|---|
| | 5.Aplikovať | Určiť program odbornej prípravy zahŕňajúci väčšinu zručností a rozvoja znalostí potrebných na rekvalifikáciu alebo zvýšenie kvalifikácie pre daný profil. |

## 3.1 ZAMESTNÁVAŤ ODBORNÍKOV V OBLASŤI KYBERNETICKEJ BEZPEČNOSTI – APLIKOVAŤ ECSF AKO ORGANIZÁCIU

ECSF poskytuje štandardný referenčný súbor 12 typických rolí, ktoré vykonávajú odborníci v oblasti kybernetickej bezpečnosti z organizačného hľadiska a ktorý pokrýva kybernetickobezpečnostné potreby organizácií a procesy kybernetickej bezpečnosti, ktoré je potrebné dodržiavať s cieľom zabezpečiť ich podnikanie, produkty, služby a ich dodávateľské reťazce. Rámec tak poskytuje cennú príručku a plán nielen na budovanie, rozširovanie a prevádzku funkcií súvisiacich s kybernetickou bezpečnosťou v rámci organizácie, ale aj na zabezpečenie plnenia jej poslania, vízie a cieľov súvisiacich s kybernetickou bezpečnosťou. Organizácia tak môže využívať ECSF ako východiskový bod alebo príručku na rýchly a jednoduchý prístup k primárnym úlohám potrebným na riadenie svojich kybernetickobezpečnostných rizík a budovanie prístupu ku kybernetickej bezpečnosti. Profily ECSF zároveň poskytujú spoločné porozumenie medzi zúčastnenými stranami, pokiaľ ide o kybernetickobezpečnostné úlohy organizácie.

Tri orientačné príklady, ktoré sú uvedené neskôr v tejto kapitole, majú za cieľ ukázať praktické vykonávanie rámca v týchto oblastiach:

I. zlepšenie postupov malej spoločnosti v oblasti kybernetickej bezpečnosti;
II. náborový proces veľkej spoločnosti so zvyšujúcimi sa požiadavkami na dodržiavanie predpisov;
III. plánovanie zdrojov vo veľkej organizácii v oblasti kybernetickej bezpečnosti.

Príklad I: *Posilnenie postupov malej spoločnosti v oblasti kybernetickej bezpečnosti* predstavuje uplatňovanie ECSF na riešenie potrieb malej spoločnosti, ktorá sa snaží zlepšiť svoju kybernetickú štruktúru a prax. Ukazuje, ako by spoločnosť mohla využívať ECSF na podporu rozvoja stratégie kybernetickej bezpečnosti vrátane plánovania ľudských zdrojov pre kybernetickú bezpečnosť a plánovania obstarávania kybernetickej bezpečnosti.

Používaním ECSF ako východiskového bodu alebo ako sprievodcu nemusí spoločnosť vymýšľať ani skúmať základné úlohy potrebné na zlepšenie svojho postoja v oblasti kybernetickej bezpečnosti. Úlohy môžu byť udelené rôznym osobám alebo môžu byť zlúčené len jednou alebo len niekoľkými osobami v závislosti od stratégie, požiadaviek, potrieb a rozpočtu.

Príklad tiež ukazuje, ako môže ECSF podporiť organizáciu v procese prijímania zamestnancov tým, že identifikuje úlohy a zodpovednosti v oblasti kybernetickej bezpečnosti, ktoré sú potrebné v rámci malej spoločnosti. V tomto príklade sa poskytuje aj kybernetickobezpečnostná úloha a analýza chýbajúcich zručností a následné prognózy potrieb na organizačnej úrovni. Okrem podpory procesov ľudských zdrojov pri prijímaní zamestnancov poskytuje ECSF aj spoločný jazyk na obstarávanie služieb kybernetickej bezpečnosti.

**Príklad I: Posilnenie postupov malej spoločnosti v oblasti kybernetickej bezpečnosti**

Malá spoločnosť v oblasti cloudových služieb sa stala úspešnou len niekoľko mesiacov po tom, čo zakladatelia, súrodenci Alicia a Max implementovali svoj nápad na inovatívne riešenie. Alicia bola expert „techie“ génius, zatiaľ čo Max bol marketingový génius. Bohužiaľ, ani jeden z nich nemal skúsenosti s fungovaním alebo budovaním spoločnosti. Po roku sa

spoločnosť začala rozbiehať, a tak sa presťahovali do vlastnej kancelárie a zamestnávali zamestnancov, aby podnikli. Počas tohto expanzná fáza, nikto neuvažoval o organizácii spoločnosti. Mnohé úlohy a povinnosti sa zdieľali a výzvy sa riešili ad hoc. Našťastie sa počas tejto prechodnej fázy nevyskytol žiadny vážny kybernetický-bezpečnostný incident.

Nakoniec spoločnosť získala určitú mediálnu expozíciu, ktorá sa stala virálnou, čo viedlo k zvýšenému záujmu nových investorov a klientov o malý startup. Väčší klienti a investori však požadovali uistenie a dôkaz o primeraných bezpečnostných opatreniach a organizačnej štruktúre predtým, ako sa zapoja do spoločnosti. Zakladatelia si uvedomili, že budú musieť skutočne formovať veci vo svojej organizácii. Boli si vedomí toho, že kľúčom k úspechu organizácie boli zamestnanci a na to, aby organizácia mohla prosperovať a ponúkať odolné služby, bolo nevyhnutné vymedziť ich úlohy a zodpovednosti v oblasti kybernetickej bezpečnosti. Otázkou však bolo, aké usporiadanie organizácie bolo potrebné a aké úlohy a aké kompetencie potrebovala organizácia?

Financovatelia využili ECSF a zistili, že ich organizácia vyžaduje päť kľúčových úloh na podporu ich základnej úrovne kybernetickej bezpečnosti:

- Hlavný úradník pre bezpečnosť informácií (CISO)
- Úradník pre kybernetické právo
- Architekt kybernetickej bezpečnosti
- Implementátor kybernetickej bezpečnosti
- Koordinátor reakcie na kybernetické incidenty

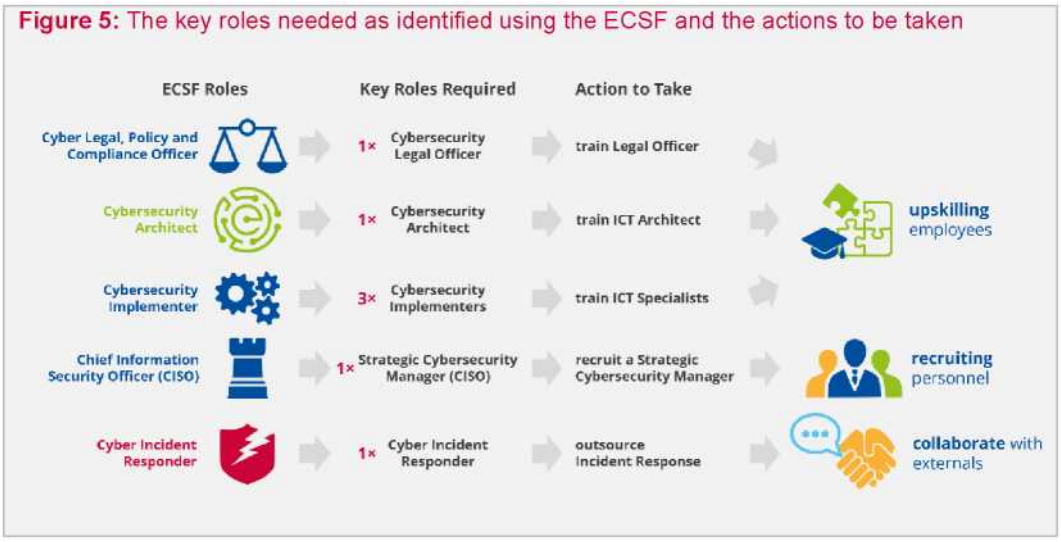
Pri internom **pohľade na to**, či ich **zamestnanci** boli schopní **plniť tieto úlohy**, zistili, že ich právna úradníčka už riadila súlad s právnymi a regulačnými rámcami a že mala záujem o **obohatenie** svojich **kompetencií v oblasti ochrany súkromia** a právnych záležitostí **v oblasti kybernetickej bezpečnosti**. Oddelenie ľudských zdrojov by mohlo **podporovať zvyšovanie úrovne zručností pomocou** zoznamu kľúčových **znalostí** a **zručností** získaných **z ECSF.**

Architekt IKT organizácie mal predchádzajúce skúsenosti s navrhovaním bezpečných sietí, a preto s dodatočnou **odbornou prípravou na aktualizáciu a obohacovanie** jeho **kompetencií** mohol **pokryť** aj architektonické požiadavky **kybernetickej bezpečnosti organizácie**.

Správcovia systému sa riadili mnohými najlepšími postupmi v oblasti kybernetickej bezpečnosti, ale väčšinou pracovali ad hoc bez stratégie alebo štruktúry. V dôsledku toho zakladatelia **identifikovali potrebu náboru hlavného úradníka pre bezpečnosť informácií (CISO).** Náborový úradník bol poverený vypracovaním **opisu práce na základe profilu CISO ECSF** a uvedením voľných pracovných miest na svojej webovej stránke.

Nakoniec sa zistilo, že funkcie reakcie na incidenty spoločnosti musia fungovať 24 hodín denne 7 dní v týždni, aby sa zabezpečila nepretržitá prevádzka služieb.

**Obrázok 5: Potrebné kľúčové úlohy identifikované pomocou ECSF a opatrenia, ktoré sa majú prijať**




Príklad I ukázal, aký užitočný môže byť ECSF pre nasledujúce výhody:

- pochopenie úloh v oblasti kybernetickej bezpečnosti
- identifikácia požiadaviek na pracovnú silu
- hodnotenie procesov a štruktúry
- rekvalifikácia a/alebo zvyšovanie úrovne zručností zamestnancov
- podpora náborového procesu
- budovanie kapacít v oblasti kybernetickej bezpečnosti
- budovanie kyberneticko-bezpečnej a dôveryhodnej organizácie
- budovanie odolnosti proti kybernetickým útokom

**Obrázok 6: Výhody používania ECSF, ako je znázornené na príklade I**


***Príklad II:*** *Vypracovanie opisu práce* preukazuje uplatňovanie ECSF pri vytváraní opisu práce. Ukazuje, ako môže byť ECSF prospešný z hľadiska ľudských zdrojov bez toho, aby bolo potrebné dôkladne pochopiť povolanie v oblasti kybernetickej bezpečnosti. Tento príklad ukazuje, ako možno vytvoriť voľné pracovné miesto a ako zabrániť vytváraniu zavádzajúcich alebo mätúcich očakávaní a ako prilákať primerane kvalifikovaných pracovníkov. Ukazuje tiež, ako kombinovať zložky profilu úloh ECSF a ako ich prispôsobiť podľa pracovných potrieb organizácie. Tento príklad ukazuje, ako môže organizácia použiť ECSF na vytvorenie opisu

úlohy. Dokonca aj bez zázemia v oblasti ľudských zdrojov je možné definovať úlohy, zručnosti a znalosti požadované od kandidáta na nábor tým, že poznáte poslanie úlohy. Okrem poskytovania podpory procesu prijímania zamestnancov môže ECSF spoločnosti pomôcť aj pri definovaní plánov odbornej prípravy pre novoprijatých zamestnancov. Je pozoruhodné, že ECSF poskytuje nielen spoločný jazyk pre obstarávanie kybernetickej bezpečnosti, ale aj na účely auditu, najmä ak sa uplatňuje zásada zodpovednosti a vyžaduje sa zásadné a jasné oddelenie povinností.

**Príklad II: Vypracovanie popisu práce**

Veľká poisťovňa rozširuje svoje portfólio o kyberneticko-bezpečnostné poistenie, pretože mnohí zákazníci hľadajú túto službu. Po miernej internej reštrukturalizácii a aktualizácii personálneho inventára sa spoločnosť rozhodne pridať kybernetickú bezpečnosť do oddelenia dodržiavania predpisov. V dôsledku toho vedenie oddelenia pre dodržiavanie predpisov dospelo k záveru, **že na podporu nového poslania je potrebné prijať úradníka pre kybernetické dodržiavanie predpisov.**

**ECSF môže byť použitý ako sprievodca a detailný postup poskytujúce a bežné pochopenie medzi zúčastnenými stranami ohľadom rolí organizácie kybernetickej bezpečnosti.**

Personálne oddelenie spoločnosti má za úlohu **nájsť a prijať najvhodnejšieho kandidáta**. Keďže kybernetická bezpečnosť je pre organizáciu novou oblasťou, HR musí tiež **vytvoriť opis roly**. Na definovanie tejto novej roly **HR vedie rozhovory** so skúsenými **manažérmi a zamestnancami** s cieľom **identifikovať potreby** a **kľúčové úlohy** pre túto pozíciu. Tieto potreby sa identifikujú a kľúčové úlohy sa vyberajú takto:

- zabezpečiť súlad s normami, zákonmi a nariadeniami, zákonmi a inými právnymi predpismi v oblasti ochrany osobných údajov a poskytovať právne poradenstvo a usmernenia,
- identifikovať a zdokumentovať nedostatky v dodržiavaní predpisov;
- vypracovať plán auditu, v ktorom sa opisujú rámce, štandardy, postupy a audítorské testy;
- vykonať plán auditu a zhromaždiť dôkazy a merania; • vypracovať a oznámiť výsledky auditu (podávanie správ).

Zodpovedný pracovník pre ľudské zdroje uznáva, že ide o zložitú úlohu a že nie sú k dispozícii žiadne vzory na prijímanie zamestnancov, ktoré by zodpovedali tejto úlohe. Preto musí manažment vytvoriť a schváliť **nový opis roly a šablónu.**

Pracovník pre ľudské zdroje, ktorý teraz **využíva ECSF, analyzuje rôzne roly v jeho rámci.** Špecifikované povinnosti sú zahrnuté **v kľúčových úlohách identifikovaných v úlohách úradníka pre kybernetické právo, politiku a dodržiavanie predpisov a audítora kybernetickej bezpečnosti.**

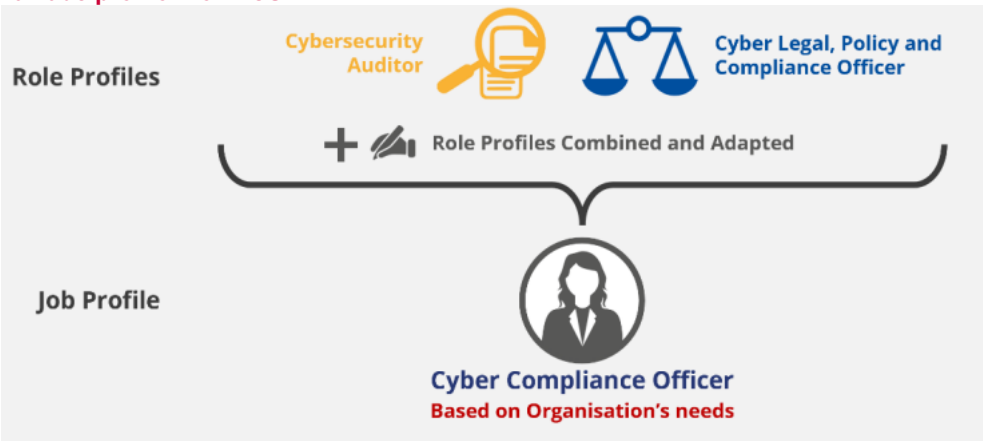
**Na vykonávanie týchto úloh** sú identifikované **zručnosti a požadované znalosti** nasledovné:

- Zručnosti
  - pochopiť dôsledky zmien právneho rámca na stratégiu a politiky organizácie v oblasti kybernetickej bezpečnosti a ochrany údajov;
  - dodržiavať a uplatňovať rámce, normy a metodiky auditu;
  - uplatňovať audítorské nástroje a techniky;
  - pracovať ako súčasť tímu a spolupracovať s kolegami.
- Vedomosti
  - pokročilé znalosti o národnej, európskej a medzinárodnej kybernetickej bezpečnosti a súvisiacich normách, právnych predpisoch, politikách a nariadeniach v oblasti ochrany súkromia,
  - znalosti súladu s predpismi v oblasti informačnej bezpečnosti a regulačných požiadaviek na medzinárodnej a vnútroštátnej úrovni a na úrovni EÚ;

- základné chápanie uchovávania, spracovania a ochrany údajov v rámci systémov, služieb a infraštruktúr.

Nový opis úloh prispôsobený potrebám spoločností sa teraz môže vytvoriť mapovaním a kombinovaním častí profilu pre úlohu úradníka pre kybernetickú legislatívu, politiku a dodržiavanie predpisov a časti profilu pre úlohu audítora kybernetickej bezpečnosti. Je dôležité, že mapovaním rámca je táto nová jedinečná úloha založená na základnom obsahu ECSF. To poskytuje jednotnú a štruktúrovanú úlohu, ktorú možno vysledovať až k jej vzniku.

**Obrázok 7: Profil pracovných miest v oblasti kybernetickej bezpečnosti vytvorený na základe profilov rolí ECSF**




Po tomto priradení k ECSF je požadovaný opis rolí k dispozícii a môže sa použiť na vypracovanie úlohy a následného opisu práce, ktoré HR potrebuje na získanie interného schválenia a uverejnenie na webovom sídle spoločnosti v oblasti náboru zamestnancov. Ďalšie prvky, ako napríklad profilová služobná cesta, sa môžu použiť ako úvodný text na uverejnenie tohto voľného pracovného miesta.

Príklad II preukázal, aký užitočný môže byť ECSF pre tieto prínosy:

- pochopenie úloh v oblasti kybernetickej bezpečnosti • identifikácia požiadaviek na pracovnú silu
- určenie požiadaviek na úlohu
- podpora náborového procesu • podpora vytvárania prispôsobenej šablóny voľných pracovných miest
- používanie spoločného jazyka pre voľné pracovné miesta.

**Obrázok 8: Prínosy použitia ECSF, ktoré sú uvedené v príklade II**


***Príklad III:*** *Veľká spoločnosť s hlavným podnikaním mimo IKT musí zriadiť kybernetickobezpečnostné oddelenie*, demonštruje uplatňovanie ECSF pri vytváraní nového oddelenia kybernetickej bezpečnosti a príprave stratégie kybernetickej bezpečnosti pre spoločnosť. Navrhuje sa v ňom aj kategorizácia 12 profilov do štyroch (4) makro oblastí na účely porozumenia a komunikácie na vysokej úrovni. Ukazuje, ako by veľká organizácia mohla využívať ECSF na podporu rozvoja stratégie kybernetickej bezpečnosti vrátane plánovania ľudských zdrojov a rozvoja talentov v oblasti kybernetickej bezpečnosti.

**Príklad III:** Veľká spoločnosť s hlavným podnikaním mimo IKT potrebuje zriadiť kybernetickobezpečnostné oddelenie

Veľká spoločnosť s hlavnou činnosťou, ktorá nesúvisí s IKT alebo službami kybernetickej bezpečnosti, si uvedomila potrebu chrániť svoje cenné aktíva pred kybernetickými hrozbami. Prijatá obchodná stratégia v skutočnosti zahŕňala rozsiahly plán digitalizácie obchodných procesov a závislosť od IKT sa v prípade kritických obchodných operácií stávala výrazne vyššou.

Keďže spoločnosť nemala žiadne interné odborné znalosti na riešenie kybernetickobezpečnostných rizík, správna rada sa rozhodla najať hlavného úradníka pre bezpečnosť informácií (CISO) **ktorý by definoval celkovú stratégiu kybernetickej bezpečnosti** v súlade s obchodnými cieľmi spoločnosti. To by si tiež vyžadovalo **zriadenie oddelenia pre riešenie kybernetickobezpečnostných rizík.**

Novo vymenovaná CISO, **používala ECSF ako usmernenie a ako** solídnu **referenciu pre kybernetickobezpečnostné role potrebné** na zvládnutie jeho kybernetickobezpečnostných rizík. Využívala ho ako **flexibilný nástroj** na **vytvorenie kybernetickobezpečnostného oddelenia**. Uznala tiež, že na poskytnutie jasnej schémy by bolo užitočné zaradiť r**oly ECSF do rámca okruhu riadenia** do štyroch (4) makro oblastí: a) plánovanie, b) vykonávanie, c) operácia a d) zlepšenie.

**Obrázok 9:** Zaradenie profilov rolí ECSF do kontextu riadiaceho kruhu


V makro oblasti plánovania boli stanovené priority a ciele, vypracované stratégie, politiky a akčné plány, definované štruktúry, pridelené zdroje. V tejto makro oblasti mali prirodzenú polohu CISO, úradníka pre kybernetické právo, politiku a dodržiavanie predpisov, manažéra pre riziká kybernetickej bezpečnosti, a architekt kybernetickej bezpečnosti.

Vykonávanie opatrení v oblasti kybernetickej bezpečnosti (implementátor) a odborná príprava a zvyšovanie informovanosti (pedagóg) boli pridelené makro oblasti vykonávania.

Každodenné operácie boli najhmatateľnejšou oblasťou. V reakcii na incidenty (vrátane tímov SOC) sú forenzné činnosti každodennou činnosťou špecialistov na kybernetickú bezpečnosť. Profil spravodajských informácií o hrozbách sa tiež považoval za operačnú oblasť, keďže títo odborníci pracujú na operačných údajoch s využitím viacerých zdrojov.

Penetračný tester (testovanie súčasných a vznikajúcich hrozieb), výskumník (prinášanie nových technológií a riešení) a audítor (identifikácia nedostatkov) podporujú fázu zlepšovania.

Keďže však ECSF je flexibilným nástrojom na individuálne použitie v konkrétnom kontexte, CISO **uplatnil päťstupňovú príručku s cieľom prispôsobiť profily rolí svojim špecifickým potrebám a cieľom**. Analýza profilov ECSF jej pomohla **definovať plány zdrojov** potrebné na dosiahnutie cieľa podniku.

V makro oblasti plánovania sa rozhodla:

- mať na starosti úlohy súvisiace s politikou a dodržiavaním predpisov s cieľom zefektívniť organizačnú štruktúru;

- najať architekta kybernetickej bezpečnosti, ktorý by pomohol vymedziť celkovú stratégiu architektúry s cieľom zvládnuť riziká kybernetickej bezpečnosti a zabezpečiť riešenia zabezpečené už v štádiu návrhu na podporu digitálnej transformácie;

- najať manažéra pre riziká kybernetickej bezpečnosti, ktorý by pomohol posúdiť pozíciu podnikového rizika v oblasti kybernetickej bezpečnosti a pomohol by definovať akčné plány na riadenie identifikovaných rizík.

V makro oblasti vykonávania využila **zložky zručností a znalostí ECSF**, aby **pochopila, aké zvýšenie úrovne zručností by bolo potrebné** na mobilizáciu dostupných interných zdrojov, alebo sa prípadne rozhodla zamestnať sa externe. Nadnárodná spoločnosť mala existujúci tím inštruktorov v inej oblasti. Neexistoval však žiadny špecializovaný tím na navrhovanie a vedenie kurzov informovanosti o kybernetickej bezpečnosti alebo odbornej prípravy. CISO **skúmala, či niektorí školitelia mali zručnosti a znalosti uvedené v ECSF a záujem pripojiť sa k jej novému tímu.**

V makro oblasti operácií CISO skúmala, ako riadiť každodenné kyberneticko-bezpečnostné operácie a rozhodla sa **zriadiť centrá globálnych bezpečnostných operácií s osobami reagujúcimi na incidenty, ktoré pracujú na rôznych kontinentoch, aby poskytovali podporu 24 hodín denne a 7 dní v týždni.** Okrem toho **bol zamestnaný špecialista na spravodajské informácie o kybernetických hrozbách**, aby poskytol operatívne poznatky na usmernenie lovu hrozieb a zmiernenia rizika. CISO dospela k záveru, že **nie je potrebné najať digitálneho forenzného vyšetrovateľa**, ale skôr **zapojiť špecializovanú poradenskú spoločnosť** pre akékoľvek **forenzné potreby.**

V makro oblasti zlepšenia sa CISO rozhodla zamestnať **externého poskytovateľa služieb na penetračné testovanie** s cieľom otestovať odolnosť podnikovej infraštruktúry a aplikácií. CISO takisto posúdila kapacitu tímu pre vnútorný audit a rozhodla sa **najať audítora kybernetickej bezpečnosti** na audit politík súvisiacich s bezpečnosťou. CISO nepociťovala potrebu najať výskumníka v oblasti kybernetickej bezpečnosti, keďže výskum kybernetickej bezpečnosti bol mimo rozsahu jej organizácie.

Stručne povedané, príklad III poukázal na to, aké užitočné môže byť ECSF pre tieto prínosy:

- pochopenie úloh v oblasti kybernetickej bezpečnosti
- pomoc pri vytváraní organizačnej štruktúry určujúcej požiadavky na kyberneticko-bezpečnostné úlohy
- pomoc pri plánovaní ľudských zdrojov
- zvyšovanie úrovne zručností zamestnancov
- podpora hodnotenia uchádzačov
- používanie spoločnej terminológie pre spoluprácu.

**Obrázok 10:** Prínosy použitia ECSF preukázané v príklade III


## 3.2 ZRUČNOSTI ODBORNÍKOV V OBLASTI KYBERNETICKEJ BEZPEČNOSTI – APLIKOVAŤ ECSF AKO POSKYTOVATEĽA VZDELÁVANIA

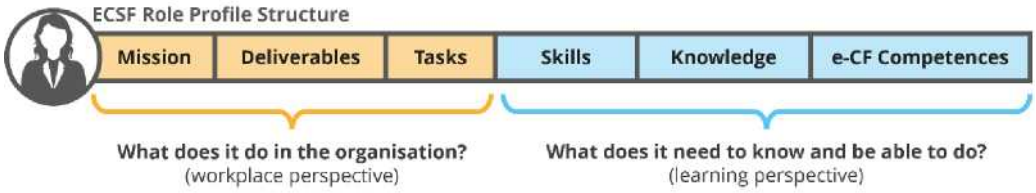
ECSF ponúka poskytovateľom vzdelávacích programov a vzdelávacích inštitúcií všetkých typov, ako sú vysokoškolské vzdelávanie, odborné vzdelávanie a príprava (OVP) alebo akýkoľvek iný vzdelávací program alebo odborná príprava v oblasti kybernetickej bezpečnosti, spoločný jazyk a slovnú zásobu na rozvoj odborných zručností v oblasti kybernetickej bezpečnosti. Vymedzené profily úloh poskytujú kyberneticko-bezpečnostný prístup na pracovisku založený na európskej úrovni s cieľom prepojiť súčasné požiadavky na odbornú prax s učebnými osnovami a vzdelávacími programami súvisiacimi s kybernetickou bezpečnosťou.

ECSF definuje typické požiadavky profilu z dvoch základných hľadísk.

- Čo robí táto rola v organizácii? Zaoberá sa pohľadom na pracovisko (profilové sekcie o poslaní, výsledkoch a úlohách)

- Čo táto rola potrebuje vedieť a byť schopná urobiť? Riešiť perspektívu vzdelávania (profilové sekcie o zručnostiach, znalostiach a kompetencie z e-CF)

**Obrázok 11:** Profily úloh ECSF súvisiace s perspektívou pracoviska a vzdelávania




ECSF umiestňuje vzdelávacie výstupy v reálnej situácii na pracovisku. Najmä opisy rolí v profiloch ECSF umožňujú poskytovateľom vzdelávacích programov prehodnocovať svoje učebné plány štruktúrovaným a systematickým spôsobom, a to aj z hľadiska odborníkov z praxe.

Ako je znázornené v prílohe B.2, ECSF by mohol prispieť k niekoľkým činnostiam v akademických inštitúciách.

- ECSF by mohol slúžiť na rozvoj alebo aktualizáciu výsledkov kurzov a ich zosúladenie s potrebami trhu práce. Zručnosti, znalosti a kompetencie v rámci rolového profilu sa

môžu použiť na usmernenie fázy navrhovania učebných plánov a na podporu vytvárania požadovaných vzdelávacích výstupov. Napríklad pri analýze vzdelávacích potrieb konkrétneho povolania v oblasti kybernetickej bezpečnosti poskytuje zosúladený profil ECSF solídny východiskový bod na pochopenie súvisiacich vzdelávacích požiadaviek.

- ECSF by mohol slúžiť ako nástroj spolupráce na vytváranie spoločných akademických programov a na umožnenie mobility študentov.

- ECSF by mohol slúžiť ako základ pre vymedzenie rámca pre učebné osnovy kybernetickej bezpečnosti, ktorý by univerzitám pomohol zmapovať hlavné zameranie ich programu kybernetickej bezpečnosti a oznámiť ho študentom.

  Ako je znázornené v prílohe B.1, ECSF rieši niektoré z výziev identifikovaných v európskom prostredí odborných kvalifikácií v oblasti kybernetickej bezpečnosti. Najmä:

- ECSF podporuje medzi oblastnú a medziodvetvovú terminológiu týkajúcu sa zručností v oblasti kybernetickej bezpečnosti;

- ECSF by mohol podporovať rozvoj integrovanej platformy pre zručnosti na poskytovanie aktuálnych informácií o trhu práce, kompetenciách, kurzoch odbornej prípravy, certifikačných systémoch a kariérnom pláne.

**ECSF ponúka poskytovateľo m vzdelávacích programov a vzdelávacích inštitúcií všetkých typov spoločný jazyk a slovnú zásobu na rozvoj odborných zručností v oblasti kybernetickej bezpečnosti.**

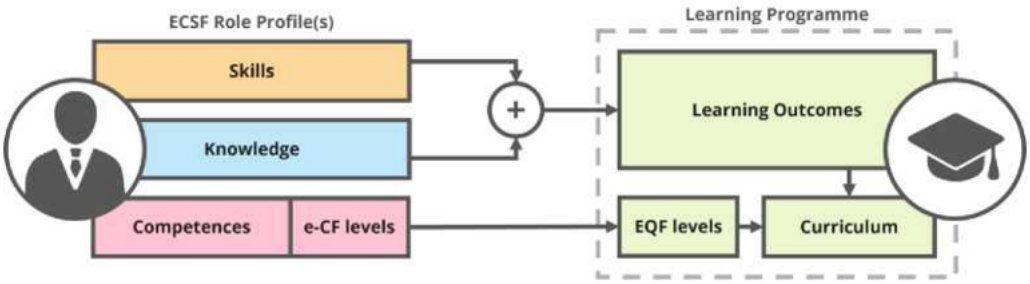
**Obrázok 12:** Výhody využívania ECSF ako poskytovateľa vzdelávania


V kontexte rozvoja kvalifikácií v oblasti kybernetickej bezpečnosti a navrhovania učebných osnov slúžia profily úloh ECSF ako komunikačný nástroj medzi zamestnávateľmi a pedagógmi na zlepšenie konzultačného procesu a výsledkov spolupráce. Zamestnávateľ môže rýchlo vymedziť požadované činnosti alebo úlohy a pracovať spätne s cieľom identifikovať kompetencie, zručnosti a vedomostné pedagóga by mali zahrnúť do učebných osnov. Tento prístup výrazne urýchľuje tvorbu učebných plánov dohodnutých medzi zamestnávateľmi, vládami a pedagógmi.

Obrázok 13 znázorňuje, ako možno časti profilov rolí ECSF venované kompetenciám, znalostiam a zručnostiam použiť na definovanie výsledkov vzdelávania, určenie vhodných úrovní vzdelávacích programov a vytvorenie učebných plánov pre povolania v oblasti kybernetickej bezpečnosti. Keďže vedomosti a zručnosti, rovnako ako všetok obsah opisov úloh, sú uvedené ako usmerňujúce príklady pružného prispôsobenia sa kontextu, môžu sa

použiť aj iné zdroje[8].

**Obrázok 13:** Profily ECSF, ktorými sa riadi odborné vzdelávanie v oblasti kybernetickej bezpečnosti




## Prepojenie úrovní vzdelávania (EKR) a úrovne odbornej spôsobilosti na pracovisku (e-CF)

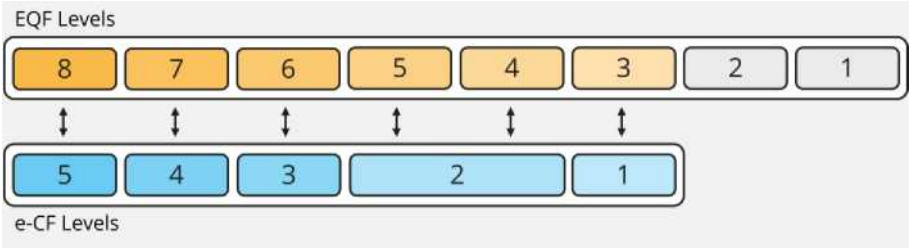
**Európsky kvalifikačný rámec (EKR)** je spoločný európsky referenčný rámec pre kvalifikácie. Účelom EKR je porovnať kvalifikácie a výsledky vzdelávania, ktoré vznikajú v rôznych krajinách a vo vnútroštátnych vzdelávacích systémoch. EKR je založený na Odporúčanie o európskom kvalifikačnom rámci pre celoživotné vzdelávanie, ktoré Európsky parlament a Rada prijali 23. apríla 2008[9].

EKR definuje osem (8) úrovní dosiahnutého vzdelania s deskriptormi, ktoré rozlišujú jednotlivé úrovne. Kritérium pre každú úroveň je založené na posúdení znalostí, zručností, zodpovednosti a autonómie.

**Európsky rámec elektronických kompetencií (e-CF)**, norma EN 16234 – 1, ktorý používa ECSF, je spoločným európskym rámcom pre odborné spôsobilosti, znalosti a zručnosti v oblasti IKT[10]. Týka sa kompetencií podľa potreby a uplatňovaných na pracovisku. V dimenzii 3 e-CF sa vymedzujú úrovne spôsobilosti pochádzajúce z odbornosti na pracovisku. Existuje päť (5) vymedzených úrovní eKompetencie e-1 až e-5, ktoré súvisia s úrovňami vzdelávania EKR 3 až 8 (úrovne EKR 1 a 2 nie sú v tomto kontexte relevantné).

Vzťah medzi úrovňami e-CF e-1 až e-5 s úrovňami EKR 3 – 8 je znázornený nižšie:

**Obrázok 14:** Vzťah medzi úrovňami EKR a e-KF




[8] Oddiely o zručnostiach, znalostiach a spôsobilostiach ECSF nie sú ani vyčerpávajúce, ani obmedzujúce, čo umožňuje používateľovi obohatiť ich aj o externé zdroje, napr. orgán znalostí v oblasti kybernetickej bezpečnosti (CyBOK) https://www.cybok.org Klasifikácia https://joint-research-centre.ec.europa.eu/publications/unified-conceptual-framework-tasks-skills-and-competences_en

[9] Európsky kvalifikačný rámec pre celoživotné vzdelávanie

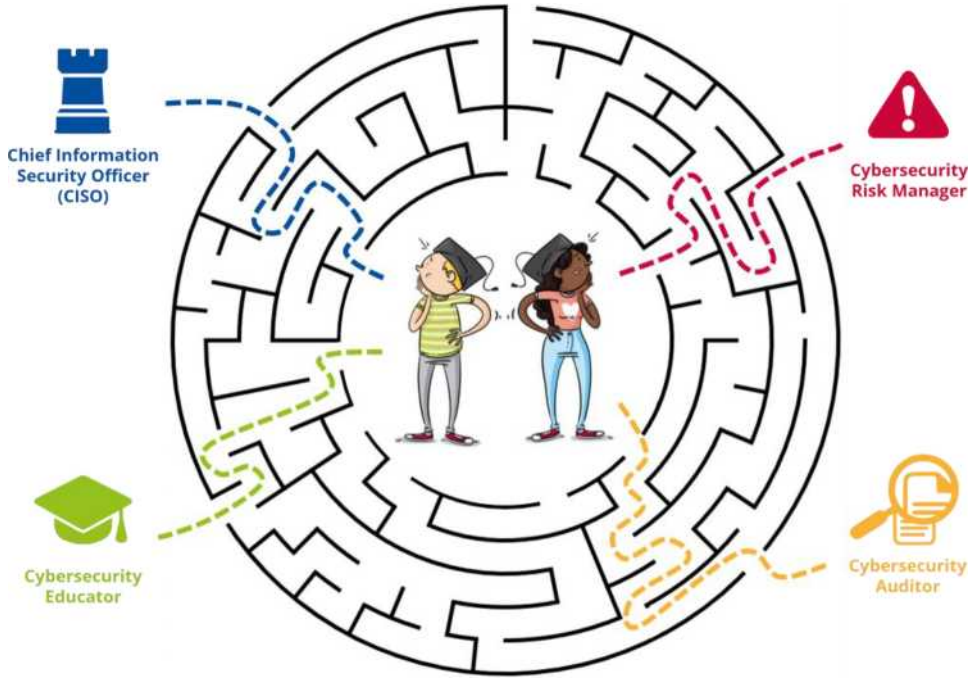
[10] EN16234 – 1:2019: rámec elektronických kompetencií (e-CF) – spoločný európsky rámec pre odborníkov v oblasti IKT vo všetkých odvetviach

Vzhľadom na tento systematicky rozvinutý vzťah je možné prepojiť úrovne odbornej spôsobilosti e-CF s úrovňami vzdelávania EKR. Vzťah, vzhľadom na rozdielnu povahu každého rámca, nie je úplne rovnocenný. Môže sa však uplatňovať s cieľom zvýšiť transparentnosť a **poskytnúť spoločný jazyk medzi požiadavkami na odbornú spôsobilosť na pracovisku a súvisiacou kvalifikáciou vzdelávacích inštitúcií**[11]. Úrovne kompetencií e-CF začlenené do profilov rolí ECSF sa preto môžu použiť ako všeobecná príručka pre požadované úrovne vzdelania.

## 3.3 ROBIŤ VLASTNÉ KARIÉRNE ROZHODNUTIA – APLIKOVAŤ ECSF AKO INDIVIDUÁLNEHO ODBORNÍKA

Spoločný jazyk, ktorý definuje ECSF, sa môže použiť na odstránenie akýchkoľvek nejasností medzi profesionálnymi úlohami v oblasti kybernetickej bezpečnosti a vzdelávacími programami v oblasti kybernetickej bezpečnosti. Poskytnutím spoločného jazyka a jasného opisu pracovných rolí v oblasti kybernetickej bezpečnosti, úloh, ktoré majú vykonávať, ako aj zručností, kompetencií a požadovaných znalostí, môže ECSF vybudovať spoločné porozumenie a poskytnúť zrozumiteľnosť potrebnú na prilákanie nových jednotlivcov do oblasti kybernetickej bezpečnosti alebo na pomoc pri plánovaní ich kariérnych dráh.

**Obrázok 15:** Používanie ECSF na definovanie kariérnych dráh jednotlivca




Odborníci, ktorí už pracujú na pozíciách súvisiacich s kybernetickou bezpečnosťou, môžu využiť ECSF ako návod na pokrok vo svojej oblasti. Zmapovaním svojich zručností a znalostí do profilov záujmových rolí ECSF môžu jednotlivci identifikovať akékoľvek chýbajúce zručnosti alebo vedomosti, ktoré potrebujú na rozvoj, zvládnutie alebo učenie sa, aby boli pripravení pokryť budúce požiadavky na zamestnanie alebo možný prechod medzi kyberneticko-bezpečnostnými úlohami počas svojej profesionálnej kariéry. Pomáha to viesť dialóg medzi zamestnancami a zamestnávateľmi pri plánovaní kontinuálneho vzdelávania v oblasti kybernetickej bezpečnosti. Keďže ECSF označuje formálne aj neformálne vzdelávacie dráhy, pomáha aj novým účastníkom, ktorí nevedia, kde začať. Pridávanie predchádzajúcich vedomostí a kompetencií je často jednoduchšou cestou, ako začať úplne nanovo. Príloha B.6 sa zaoberá touto témou a poskytuje hlbšie poznatky a príklady v rámci „individuálneho kariérneho rozhodovania“ s využitím ECSF.

**ECSF môže vybudovať spoločné porozumenie a poskytnúť zrozumiteľnosť potrebnú na prilákanie nových jednotlivcov do oblasti kybernetickej bezpečnosti alebo na pomoc pri plánovaní ich kariérnych dráh.**

[11] Ďalšie praktické usmernenia sú uvedené na: CEN/TS 17699:2022 Usmernenia pre vypracovanie odborných učebných plánov v oblasti IKT v rozsahu pôsobnosti normy EN16234 – 1 (e-CF)

Pomocou ECSF ako východiskového scenára môže jednotlivec identifikovať požadované kompetencie a zručnosti na prechod z jednej úlohy na druhú alebo na identifikáciu súčasných potrieb v oblasti odbornej prípravy.

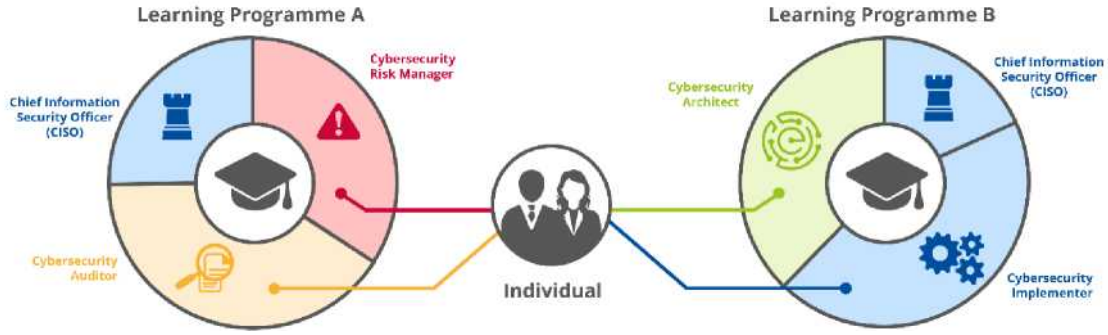
Spoločný jazyk definovaný v ECSF môže byť užitočný pre jednotlivcov, ktorí hľadajú prácu v oblasti kybernetickej bezpečnosti. ECSF môže pomôcť pri filtrovaní pracovných miest a pochopení opisu pracovných miest, pričom môže uľahčiť aj celkovú mobilitu v rámci kybernetickej bezpečnosti tým, že priradí zručnosti, znalosti a kompetencie jednotlivca k ECSF.

Kybernetická bezpečnosť je dobrou kariérnou príležitosťou aj pre jednotlivcov, ktorí sa v súčasnosti špecializujú na iné oblasti, a preto rekvalifikácia ľudí a ich presun do oblasti kybernetickej bezpečnosti je dobrým spôsobom, ako uspokojiť potreby pracovnej sily na trhu a znížiť medzery v pracovnej sile v tejto oblasti. Keďže kybernetická bezpečnosť je multidisciplinárnym predmetom, takáto kariérna zmena by mohla byť rýchlejšia pre jednotlivcov, ktorí sa nachádzajú v blízkosti jedného z hlavných aspektov tejto oblasti[12].

- **technické** – súvisiace s technológiami, konkrétnymi technologickými prístupmi a riešeniami, ktoré možno použiť na boj proti počítačovej kriminalite a kybernetickému terorizmu;
- **ľudské** – súvisiace s ľudskými faktormi, behaviorálnymi aspektmi, otázkami súkromia, ako aj zvyšovaním povedomia a znalostí spoločnosti o počítačovej kriminalite a teroristických hrozbách;
- **organizačné** – súvisiace s procesmi, postupmi a politikami v rámci organizácií, ako aj spolupráca (verejno-súkromná, verejná) medzi organizáciami;
- **regulačné** – súvisiace s ustanoveniami zákona, normalizácie a forenznej vedy.

Vďaka jasnému pochopeniu hlavných profilov kyberneticko-bezpečnostných rolách v tejto oblasti a spoločnému jazyku kybernetickej bezpečnosti v širšom spektre odvetví, ako ich poskytuje ECSF, môžu jednotlivci, ktorí sa snažia prejsť na kybernetickú bezpečnosť, využiť ECSF ako východiskový bod na identifikáciu zručností a znalostí špecifických kompetencií, ktoré potrebujú na prechod.

**Obrázok 16:** Využívanie ECSF na analýzu a porovnanie vzdelávacích programov v oblasti kybernetickej bezpečnosti




Či už jednotlivec pracuje v oblasti kybernetickej bezpečnosti (s cieľom rozšíriť svoje vedomosti), je v súčasnosti zamestnaný v inej oblasti (hľadá zmenu kariéry) alebo hľadá akademické vzdelanie (v budúcnosti chce pracovať v oblasti kybernetickej bezpečnosti), ECSF môže pomôcť pri pochopení hlavných profilov kyberneticko-bezpečnostných rolách (poskytnutím opisu a analýzou úloh, zručností, vedomostí a kompetencií), ako aj pomôcť pri analýze a porovnávaní dostupných vzdelávacích programov (mapovanie výsledkov

[12] https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity

vzdelávania s požadovanými zručnosťami a znalosťami profilov kybernetickej bezpečnosti podľa preferencií).

## 3.4 BUDOVANIE KOMUNÍT V OBLASTI KYBERNETICKEJ BEZPEČNOSTI – APLIKOVAŤ ECSF AKO PROFESIONÁLNE ZDRUŽENIE

ECSF vytvára spoločnú terminológiu a spoločné chápanie profilov rolí odborníkov v oblasti kybernetickej bezpečnosti. Profesijné združenia ho teda môžu používať ako normu na zabezpečenie toho, aby sa ich práca mohla používať a uplatňovať v celej EÚ, čím sa odstránia nejasnosti v terminológii a akýkoľvek nedostatok porozumenia.

**ECSF vytvára spoločnú terminológiu a spoločné chápanie profilov rolí odborníkov v oblasti kybernetickej bezpečnosti a môže tak eliminovať zmätok v terminológii a akýkoľvek nedostatok porozumenia.**

Profesijné organizácie môžu použiť rámec na vykonávanie analýz trhu pomocou profilov rolí ECSF a prezentovať výsledky v spoločnom jazyku. Očakáva sa napríklad, že ECSF bude užitočný pri zdôrazňovaní profilov, ktoré chýbajú na trhu, pracovných miest v oblasti kybernetickej bezpečnosti, ktoré sú veľmi žiadané a legislatívne aspekty niektorých profesionálnych profilov pracovných miest. Okrem toho sa profesijné združenia môžu prostredníctvom ECSF ako spoločnej terminológie usilovať o odborné usmernenie v sektore kybernetickej bezpečnosti, ako sa uvádza v prílohe B.5.

Využívanie ECSF umožňuje aj konsolidáciu spoločenstva zainteresovaných strán s cieľom podporiť nový vývoj, zlepšenia a ďalšie vykonávanie v členských štátoch EÚ. Takýto rámec spolupráce umožňuje interakciu medzi ľuďmi, ktorej výsledkom sú výhody, ako je výmena poznatkov, identifikácia trendov na úrovni EÚ, činnosti partnerského učenia, uplatňovanie multidisciplinárnych prístupov a posilnenie postavenia s cieľom prispôsobiť a prispôsobiť ECSF špecifickým požiadavkám.

Celkovo môžu profesijné združenia pre kybernetickú bezpečnosť využívať ECSF ako nástroj na založenie svojich činností na zabezpečenie ich uplatniteľnosti v celej EÚ s cieľom dosiahnuť lepšie vytvrdzovanie proti kybernetickým útokom v celej EÚ ako spoločnosti.

## 3.5 POSILNENIE POSTAVENIA ODVETVIA STRATEGICKY – APLIKOVAŤ ECSF AKO TVORCU POLITIKY

S ECSF zabezpečuje kľúčová profesionálna komunita jasnú viditeľnosť, pretože používanie rámca vytvára spoločné chápanie toho, čo robia odborníci na kybernetickú bezpečnosť. ECSF preto poskytuje nástroj na analýzu a zdieľanie kritických zberov údajov a štatistík súvisiacich s kybernetickou bezpečnosťou v spoločnej a zrozumiteľnej terminológii pre celú EÚ. Takéto údaje sú dôležité pre tvorcov politík, pretože získavajú lepší prehľad o stave pracovnej sily v oblasti kybernetickej bezpečnosti v celej EÚ, čo im umožňuje pochopiť a odhadnúť budúce potreby odborníkov v oblasti kybernetickej bezpečnosti, pokiaľ ide o kvantitu a kvalitu. Takéto strategické vstupy pomáhajú aktualizovať a udržiavať samotný ECSF, aby jeho význam v budúcnosti zostal platný. Okrem toho, vymedzením spoločnej terminológie umožňuje ECSF cezhraničnú spoluprácu medzi tvorcami politík prostredníctvom výmeny údajov a informácií.

Vzhľadom na štruktúrovaný prístup k veľmi rôznorodému trhovému prostrediu predstavujú profily rolí ECSF cenný nástroj na podporu tvorcov politík, prieskumníkov trhu a iných zainteresovaných strán, ktoré majú vplyv a úlohu strategicky posilniť toto odvetvie. Profily ECSF môžu byť užitočné pre štúdie údajov o ponuke a dopyte, ktoré sa uskutočňujú na vnútroštátnej, európskej a medzinárodnej úrovni. Profily poskytujú spoločnú a dohodnutú definíciu na uľahčenie zberu spoľahlivých a porovnateľných údajov na trhu práce v oblasti kybernetickej bezpečnosti vrátane ponuky a dopytu po rôznych typoch odborníkov v oblasti kybernetickej bezpečnosti a súvisiacich požiadaviek na konkrétne zručnosti.

**Vzhľadom na štruktúrovaný prístup k veľmi rôznorodému trhovému prostrediu predstavujú profily úloh ECSF cenný nástroj na podporu tvorcov politík, prieskumníkov trhu a iných zainteresovaných strán, ktoré majú vplyv a úlohu strategicky posilniť toto odvetvie.**

Procesy tvorby politík zamerané na kybernetickú bezpečnosť môžu využívať zber údajov v čase rozhodovania, napr. ustanovenia o financovaní, investičné priority a obdobia intervencie. Okrem hlavných činností každého profilu môžu činnosti, ktoré vykonávajú, prispieť k vytváraniu a zhromažďovaniu príslušných súborov údajov, ktoré môžu podporiť politické rozhodnutia. V prílohe B.3 sa uvádza, ako roztrieštené informácie predstavujú výzvu pri prijímaní rozhodnutí a opatrenia, ktoré INCIBE prijíma pri riešení tejto výzvy s podporou ECSF. Začlenením ECSF ako homogénneho rámca na vymedzenie profilov kybernetickej bezpečnosti získajú členské štáty EÚ cennú podporu pri dosahovaní svojich cieľov zvyšovania talentov v oblasti kybernetickej bezpečnosti a zosúladenia so zvyškom krajín na európskej úrovni.

# 4. POJMY A DEFINÍCIE

| Termín | Definícia | Zdroj |
|---|---|---|
| **kybernetická bezpečnosť** | Akákoľvek činnosť potrebná na ochranu sietí a informačných systémov, používateľov takýchto systémov a iných osôb postihnutých kybernetickými hrozbami. | Mandát agentúry ENISA [nariadenie (EÚ) 2019/881] |
| **kybernetická hrozba** | Akákoľvek prípadná okolnosť, udalosť alebo činnosť, ktorá by mohla poškodiť, narušiť alebo inak nepriaznivo ovplyvniť siete a informačné systémy, používateľov takýchto systémov a iné osoby. | Mandát agentúry ENISA [nariadenie (EÚ) 2019/881] |
| **Informačné a komunikačné technológie** | IKT sú informačné a komunikačné technológie. Používa sa v mnohých rôznych kontextoch a z technického hľadiska sa IKT týkajú digitálnych počítačov a internetových (komunikačných) systémov vrátane softvéru, hardvéru a sietí. Z hospodárskeho a politického hľadiska sa IKT týkajú medzi odvetvia podnikov vrátane výrobcov, dodávateľov výrobkov alebo poskytovateľov služieb v oblasti IKT. | EN16234 – 1:2019 rámec elektronických kompetencií (e-CF) |
| **kompetencie** | Preukázaná schopnosť aplikovať vedomosti, zručnosti a postoje na dosiahnutie pozorovateľných výsledkov. Príklady sú B.1. Vývoj aplikácií a E.3. Riadenie rizík. | EN16234 – 1:2019 rámec elektronických kompetencií (e-CF) |
| **zručnosť** | Schopnosť vykonávať riadiace alebo technické činnosti a úlohy na kognitívnej alebo praktickej úrovni; vedieť, ako to urobiť. | EN16234 – 1:2019 rámec elektronických kompetencií (e-CF) |
| **mäkké zručnosti** | Interaktívne zručnosti používané na úspešné zapájanie sa do situácií na pracovisku; môže sa týkať kvality práce, sociálnej interakcie alebo emócií.<br>(tiež nazývané prierezové, prenosné alebo behaviorálne zručnosti) | EN16234 – 1:2019 rámec elektronických kompetencií (e-CF) |
| **znalosť** | Súbor skutočností, ktoré sa majú uplatniť v oblasti práce alebo štúdia; vedieť, čo robiť. | EN16234 – 1:2019 rámec elektronických kompetencií (e-CF) |
| **postoj** | Reprezentácia ľudského prvku elektronickej kompetencie; odráža sa v nej, ako človek integruje vedomosti a zručnosti a primerane ich uplatňuje v kontexte. | EN16234 – 1:2019 rámec elektronických kompetencií (e-CF) |
| **výsledok vzdelávania** | Vyhlásenie o tom, čo človek vie, chápe a môže vykonávať po ukončení vzdelávacieho procesu | Európsky kvalifikačný rámec (EKR) |
| **profil rolí** | Náčrt alebo všeobecný dokument, ktorý preukazuje vzťah medzi konkrétnymi činnosťami alebo úlohami v role a individuálnymi zručnosťami, kompetenciami a vedomosťami potrebnými na ich vykonávanie. | Kreatívne vedenie – Talent Management<br>CWA profily IKT |

| | | |
|---|---|---|
| | Na rozdiel od konkrétnej práce sa rola odvíja od organizačnej potreby niečo urobiť. Pridelení zamestnanci môžu splniť organizačné požiadavky vykonávaním všetkých alebo časti úloh, ktoré sú potrebné na zabezpečenie ich role. | |
| **profil pracovného miesta** | Kontextovo špecifický a podrobný opis toho, čo zamestnanec robí, aby zabezpečil, že zamestnanec nemá žiadne pochybnosti o svojich úlohách, povinnostiach, povinnostiach a často aj o tých, ktorým podáva správu. Zvyčajne obsahuje presné informácie o požadovaných kompetenciách, zručnostiach a znalostiach a praktické informácie o zdraví a bezpečnosti a odmeňovaní. | Profily IKT CWA |
| **úroveň odbornej spôsobilosti** | Jasné označenie stupňa zvládnutia, ktoré umožňuje odborníkovi splniť požiadavky na výkon spôsobilosti. EN 16234 – 1 (e-CF) zahŕňa úrovne odbornej spôsobilosti e-1 až e-5. E-CF charakterizuje úrovne odbornej spôsobilosti kombináciou úrovní vplyvu v rámci komunity, zložitosti kontextu a autonómie. | EN16234 – 1:2019 rámec elektronických kompetencií (e-CF) |
| **úroveň vzdelávania** | Označuje triedu a môže byť reprezentovaná formálnou kvalifikáciou. Úrovne vzdelávania sa vo všeobecnosti odvodzujú od vzdelávacieho systému alebo indikujú zaradenie do taxonómie intelektuálneho alebo vzdelávacieho správania (ako je zapamätanie si, uplatňovanie, tlmočenie) a majú vzťah k úrovniam odbornej spôsobilosti, ale treba ich odlíšiť. | EN16234 – 1:2019 rámec elektronických kompetencií (e-CF) |

# 5. REFERENCIE

Mandát agentúry ENISA, nariadenie (EÚ) 2019/881, https://eur-lex.europa.eu/eli/reg/2019/881/oj

Európske profily profesionálnych úloh v oblasti IKT, CWA 16458

https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:67523,412798&cs=17991 76DA0D15C74D91B71423CAD4A9A3

EN 16234 – 1:2019 Rámec elektronických kompetencií (e-CF), Spoločný európsky rámec pre odborníkov v oblasti IKT vo všetkých odvetviach

CEN/TS 17699:2022 Usmernenia pre vypracovanie odborných učebných osnov IKT v rozsahu pôsobnosti normy EN 16234 – 1 (e-CF)

CEN/TS 17834:2022 Európsky profesijný etický rámec pre profesiu v oblasti IKT (etika IKT v EÚ)

Európsky kvalifikačný rámec (EKR)

ESCO Európska viacjazyčná klasifikácia zručností, kompetencií a povolaní, http://www.ec.europa.eu/esco

Etický kódex IFIP

Životný cyklus reakcie na incidenty NIST

Národná iniciatíva pre vzdelávanie v oblasti kybernetickej bezpečnosti (NICE) Národného inštitútu pre normy a technológie USA

Národné stratégie kybernetickej bezpečnosti (NCSS), https://www.enisa.europa.eu/topics/national-cyber-security-

stratégie/stratégie národnej kybernetickej bezpečnosti-usmernenia-nástroje

Orgán znalostí kybernetickej bezpečnosti (CyBOK) prostredníctvom Národného programu kybernetickej bezpečnosti Spojeného kráľovstva a Univerzity v Bristole, https://www.cybok.org

JRC, taxonómia a glosár pre kybernetickú bezpečnosť Európskou komisiou,

https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf

Európsky program v oblasti zručností, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1196

Akčný plán digitálneho vzdelávania, https://education.ec.europa.eu/focus-topics/digital-education/about/digital-education- Akčný plán

Pakt o zručnostiach, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1197

Vedenie digitálneho desaťročia, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1197

ENISA, Forenzná analýza, analýza webových serverov, príručka, dokument pre učiteľov, 2016,

https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016- resources/exe3_forensic_analysis_iii-handbook

Rada Európy, Elektronické dôkazy v občianskych a správnych konaniach, usmernenia a vysvetlivky memorandum, 2019, https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5

# PRÍLOHA A: PREPOJENIE ECSF S INÝMI NORMAMI A RÁMCAMI EÚ

ECSF je rámec na podporu profesionálnej oblasti kybernetickej bezpečnosti v EÚ. Prepojenie existujúcich uznávaných európskych štruktúr s významom pre profesionálnu kybernetickú oblasť EÚ bolo životne dôležitou zásadou navrhovania ECSF (pozri oddiel 2.1).

Nasledujúce odseky poskytujú stručný prehľad hlavných noriem a rámcov, s ktorými sa ECSF spája.

## A.1 EN16234-1 E-CF SPOLOČNÝ EURÓPSKY REFERENČNÝ RÁMEC PRE ODBORNÍKOV V OBLASTI IKT VO VŠETKÝCH ODVETVIACH

Európsky norma (EN) 16234 – 1 Európsky rámec elektronických kompetencií (e-CF) poskytuje odkaz na 41 kompetencií, ktoré sa uplatňujú na pracovisku informačných a komunikačných technológií (IKT), pričom sa používa štandardný európsky jazyk pre kompetencie, zručnosti, znalosti a úrovne odbornej spôsobilosti, ktoré možno pochopiť v celej Európe. Hlavným cieľom tejto normy je poskytnúť spoločný európsky jazyk pre kompetencie, zručnosti, znalosti a odbornosť v oblasti IKT podľa požiadaviek a uplatňovaných organizáciami a odborníkmi. Týmto spôsobom majú všetky zainteresované strany v sektore vrátane verejného a súkromného sektora a jednotlivcov prístup k spoločnej referencii. Norma bola vytvorená ako nástroj na podporu vzájomného porozumenia a zabezpečenie transparentnosti jazyka prostredníctvom formulovania kompetencií požadovaných a zavedených odborníkmi v oblasti IKT. Táto norma je štruktúrovaná vo viacerých dimenziách. Rozmery odzrkadľujú oblasti plánovania podnikania a ľudských zdrojov a zahŕňajú usmernenia týkajúce sa pracovných miest a pracovnej spôsobilosti. Okrem toho táto norma pridáva prierezovú zložku, ktorá poskytuje základné všeobecné deskriptory IKT pre úspešné uplatňovanie kompetencií e-CF v kontexte pracoviska

**Tabuľka 4:** Prehľad EN16234 – 1 (e-CF). Zdroj: CEN 2019

| Dimenzia 1<br>5 oblastí e-CF | Dimenzia 2<br>41 identifikovaných elektronických kompetencií | Dimenzia 3<br>5 úrovne odbornej spôsobilosti v oblasti elektronických kompetencií | | | | |
|---|---|---|---|---|---|---|
| | | e-1 | e-2 | e-3 | e-4 | e-5 |
| A. Plánovať | A.1. Zosúladenie informačných systémov a obchodnej stratégie | | | | | |
| | A.2. Riadenie úrovne služieb | | | | | |
| | A.3. Rozvoj podnikateľského plánu | | | | | |
| | A.4. Plánovanie produktov/služieb | | | | | |
| | A.5. Architektonický dizajn | | | | | |
| | A.6. Dizajn aplikácie | | | | | |
| | A.7. Monitorovanie technologických trendov | | | | | |
| | A.8 Riadenie udržateľnosti | | | | | |
| | A.9. Inovácia | | | | | |
| | A.10. Skúsenosti používateľov | | | | | |
| B. Vybudovať | B.1. Vývoj aplikácií | | | | | |
| | B.2. Integrácia komponentov | | | | | |
| | B.3. Testovanie | | | | | |
| | B.4. Nasadenie riešenia | | | | | |
| | B.5. Výroba dokumentácie | | | | | |
| | B.6. Inžinierstvo systémov IKT | | | | | |
| C. Operovať | C.1. Podpora používateľov | | | | | |
| | C.2. Podpora zmeny | | | | | |
| | C.3. Doručovanie služieb | | | | | |
| | C.4. Riadenie problémov | | | | | |
| | C.5. Riadenie systémov | | | | | |
| D. Umožňovať | D.1. Rozvoj stratégie informačnej bezpečnosti | | | | | |
| | D.2. Rozvoj stratégie kvality IKT | | | | | |
| | D.3. Poskytovanie vzdelávania a odbornej prípravy | | | | | |
| | D.4. Nákup | | | | | |
| | D.5. Vývoj predaja | | | | | |
| | D.6. Digitálny marketing | | | | | |
| | D.7. Dátová veda a analytika | | | | | |
| | D.8 Správa zmlúv | | | | | |
| | D.9. Personálny rozvoj | | | | | |
| | D.10. Správa informácií a znalostí | | | | | |
| | D.11. Identifikácia potrieb | | | | | |
| E. Riadiť | E.1. Prognóza vývoja | | | | | |
| | E.2. Riadenie projektov a portfólií | | | | | |
| | E.3. Riadenie rizík | | | | | |
| | E.4. Spravovanie vzťahov | | | | | |
| | E.5. Zlepšenie procesu | | | | | |
| | E.6. Riadenie kvality IKT | | | | | |
| | E.7. Riadenie obchodných zmien | | | | | |
| | E.8 Riadenie informačnej bezpečnosti | | | | | |
| | E.9. Riadenie informačných systémov | | | | | |

e-CF poskytuje konzistentné prepojenia v súvislosti s kvalifikáciami v oblasti IKT a inými rámcami relevantnými pre tento sektor (najmä EQF, DigComp, európske profily profesionálnych úloh v oblasti IKT, behaviorálne zručnosti, ESCO, EQANIE, SFIA, Nadačný orgán znalostí pre profesiu v oblasti IKT, ISO a iné priemyselné normy IKT).

Pre každú kybernetickú úlohu bol na úrovni aplikácie vybraný súbor príslušných kompetencií v oblasti e-CF ako integrovaný prvok opisu profilu pre úlohu profesionála v oblasti kybernetickej bezpečnosti.

## A.2 EURÓPSKE PROFILY PROFESIONÁLNYCH ROLÍ V OBLASTI IKT

CWA 16458 Európske profily profesionálnych rolí v oblasti IKT poskytujú všeobecný súbor typických úloh, ktoré vykonávajú odborníci v oblasti IKT v akejkoľvek organizácii, pokrývajúci celý obchodný proces IKT. Celkovo tridsať profilov poskytuje dobrý východiskový bod a inšpiráciu na vytvorenie viac kontextovo špecifických a flexibilných profilov založených na organizačných úlohách, jednotlivých opisoch pracovných miest alebo subdoménnych špecializáciách z rôznych kontextov. Uplatňovaním kompetencií v oblasti e-CF na vytváranie profilov IKT poskytujú európske profily profesionálnych úloh v oblasti IKT aj nástroj a vstupný bod pre aplikáciu e-CF pre jednotlivcov a organizácie, ktoré chcú pracovať s e-CF.

Európske profily profesionálnych úloh v oblasti IKT sa opisujú použitím konzistentného formátu, ktorý obsahuje tieto prvky: súhrnné vyhlásenie, vyhlásenie o poslaní, výsledky, hlavné úlohy, elektronické kompetencie a oblasti kľúčových ukazovateľov výkonnosti (KPI)[13].

Prijatím najvhodnejších prvkov európskeho dohodnutého systému opisu profilu IKT založeného na praxi sa profily ECSF stávajú porovnateľnými a poskytujú jedinečný, ľahko dostupný a komplexný prehľad požiadaviek pre európskych odborníkov v oblasti kybernetickej bezpečnosti. Tieto podrobné profily s vysokým obsahom majú voľné odkazy na všeobecné úlohy začlenené do celkového súboru európskeho profesijného profilu IKT. Z pohľadu používateľov ECSF možno dôveru v udržateľnosť štruktúry vytvoriť prostredníctvom jej prepojenia s európskymi profilmi IKT, ale s cielenou aplikáciou pre kybernetickú komunitu.

## A.3 EURÓPSKY KVALIFIKAČNÝ RÁMEC

EÚ vyvinula európsky kvalifikačný rámec (EKR) ako prekladateľský nástroj na uľahčenie zrozumiteľnosti a porovnateľnosti národných kvalifikácií. Cieľom EKR je podporovať cezhraničnú mobilitu študentov a pracovníkov a podporovať celoživotné vzdelávanie a profesijný rozvoj v celej Európe.

EKR je 8-úrovňový rámec založený na výsledkoch vzdelávania[14] pre všetky typy kvalifikácií. Slúži ako prekladateľský nástroj medzi rôznymi rámcami národných kvalifikácií. Tento rámec pomáha zlepšiť transparentnosť, porovnateľnosť a prenosnosť kvalifikácií ľudí a umožňuje porovnávanie kvalifikácií z rôznych krajín a inštitúcií.

EKR sa vzťahuje na všetky typy a všetky úrovne kvalifikácií a využívanie vzdelávacích výstupov objasňuje, čo človek vie, chápe a je schopný urobiť. Úroveň sa zvyšuje podľa úrovne vzdelávania, pričom úroveň 1 je najnižšia a 8 najvyššia. Čo je najdôležitejšie, EKR úzko súvisí s národnými kvalifikačnými rámcami[15], takže poskytuje komplexnú mapu všetkých typov a úrovní kvalifikácií v Európe, ktoré sú čoraz prístupnejšie prostredníctvom kvalifikačných databáz. EKR bol zriadený v roku 2008 a neskôr revidovaný v roku 2017[16].

Profily ECSF obsahujú kompetencie v oblasti e-CF a úlohy na úrovni e-CF, ktoré poskytujú konzistentné prepojenie s úrovňami EKR (pozri oddiel 3.2). Tento orientačný vzťah poskytuje most v porozumení medzi poskytovaním vzdelávacích programov a požiadavkami na pracovisku.

## A.4 ESCO – EURÓPSKA KLASIFIKÁCIA ZRUČNOSTÍ, KOMPETENCIÍ A POVOLANÍ

ESCO je viacjazyčná klasifikácia európskych zručností, kompetencií, kvalifikácií a povolaní. Hlavným účelom ESCO je poskytnúť slovník, ktorý popisuje, identifikuje a klasifikuje odborné povolania a zručnosti relevantné pre trh práce EÚ, vzdelávanie a odbornú prípravu a

[13] CWA 16458 Európske profily profesionálnych úloh v oblasti IKT

[14] https://europa.eu/europass/en/description-eight-eqf-levels

[15] https://europa.eu/europass/en/national-qualifications-frameworks-nqfs

[16] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017H0615(01) &od=SK

systematicky preukazuje vzťahy medzi týmito povolaniami a zručnosťami. ESCO riadi Európska komisia, ktorá je zodpovedná za aktualizáciu klasifikácie. Zdroj ESCO podporuje dve kľúčové stratégie EÚ v tejto oblasti, stratégiu Európa 2020 a program v oblasti zručností pre Európu[17].

Cieľom ESCO je opísať všetky povolania na európskom trhu práce, a teda aj kybernetickú bezpečnosť. Preto je užitočné vytvoriť orientačné mapovanie medzi profilmi rolí ECSF a niektorými profilmi ESCO.

V tabuľke 5 sú uvedené viaceré povolania ESCO súvisiace s kybernetickou bezpečnosťou spolu s orientačným mapovaním profilov rolí ECSF. Vzhľadom na to, že vzťah medzi nimi nie je vždy jeden k jednému, boli definované nasledujúce vzťahy na vysvetlenie príslušných spojení:

- je – Toto zamestnanie ESCO možno priradiť k zodpovedajúcemu profilu roly ECSF, pričom obe opisujú rovnakú kyberneticko-bezpečnostnú rolu.
- môže zahŕňať – Toto povolanie ESCO môže na základe kontextu zahŕňať uvedený profil role ECSF. (Toto je orientačné mapovanie.)
- môžu byť zahrnuté – Niektoré aspekty tohto povolania ESCO môžu opisovať uvedené časti profilu roly ECSF. (Toto je orientačné mapovanie.)

**Tabuľka 5:** Profily ESCO a profily ECSF

| Kód ESCO | ESCO Zamestnanosť | Vzťah | Profil roly ECSF |
|---|---|---|---|
| 2149.2.8 | Výskumný inžinier | môže zahŕňať | Výskumník v oblasti kybernetickej bezpečnosti |
| 2310.1 | Vysokoškolský pedagóg | môže zahŕňať | Pedagóg v oblasti kybernetickej bezpečnosti |
| 2356 | Školiteľ informačných technológií | môže zahŕňať | Pedagóg v oblasti kybernetickej bezpečnosti |
| 2511.18 | IT audítor | môže zahŕňať | Audítor kybernetickej bezpečnosti |
| 2519.2 | Vedúci audítor IKT | môže zahŕňať | Audítor kybernetickej bezpečnosti |
| 2529.1 | Hlavný úradník pre bezpečnosť IKT | je | Hlavný úradník pre bezpečnosť informácií (CISO) |
| 2529.2 | Odborník na digitálnu forenznú oblasť | je | Digitálny forenzný vyšetrovateľ |
| 2529.3 | Vstavaný inžinier bezpečnostných systémov | môžu byť zahrnuté | Implementátor pre kybernetickú bezpečnosť |
| 2529.4 | Etický hacker | je | Penetračný tester |
| 2529.6 | Správca bezpečnosti IKT | môžu byť zahrnuté | Implementátor pre kybernetickú bezpečnosť |
| 2529.7 | Bezpečnostný inžinier IKT | môžu byť zahrnuté | Architekt kybernetickej bezpečnosti |
| 2529.7 | Bezpečnostný inžinier IKT | môžu byť zahrnuté | Implementátor pre kybernetickú bezpečnosť |
| 2619.4 | Úradník pre ochranu údajov | je | Úradník pre kybernetické právo, politiku a dodržiavanie predpisov |

*Dôležitá poznámka*: Vzťah medzi povolaním ESCO a profilom rolí ECSF nepredstavuje rovnocennosť; ponúka najlepšiu aproximáciu, ktorú čitatelia možno budú chcieť preskúmať.

[17] https://ec.europa.eu/social/main.jsp?catId=1326&langId=en

# PRÍLOHA B: PRÍPADY POUŽITIA

V prípade použitia sa uvádza, prečo a ako organizácia používa ECSF, pričom sa zdôrazňuje rozmanitosť prístupov a prínosov. Táto príloha je zbierkou prípadov, ktoré boli verejne dostupné 20. júla 2022.

*Nasledujúce prípady použitia sú len ilustračnými príkladmi. Informácie a obsah zahrnutý v týchto prípadoch by sa nemali považovať za potvrdenie alebo validačné vyhlásenie agentúry ENISA. Použitie týchto príkladov by sa malo vnímať skôr ako inšpiratívne prípady než ako východiskové podmienky alebo referenčné hodnoty.*

## B.1 PRÍPAD POUŽITIA Z PROJEKTU CONCORDIA H2020

Táto časť obsahuje časti z prípadu použitia, ktorý napísal projekt CONCORDIA H2020[18].

### Smerom k integrovanej platforme pre zručnosti v oblasti kybernetickej bezpečnosti založenej na európskom rámci pre zručnosti v oblasti kybernetickej bezpečnosti

#### Ťažko pochopiť tréningy veľký obraz

Všetky zainteresované strany stále naliehavo pociťujú potrebu chrániť sa pred hrozbami pre informácie a operácie, zachovať kybernetickú pozíciu organizácie a zvýšiť odolnosť voči takýmto hrozbám. Základným prvkom na splnenie týchto potrieb je existencia kybernetický-kompetentných odborníkov. A kompetencie v oblasti kybernetickej bezpečnosti sú potrebné nielen pre špecializovaných odborníkov (externých alebo interných pre organizáciu), ale aj pre všetkých zamestnancov organizácie, aj keď nie sú priamo zapojení do procesov a činností v oblasti kybernetickej bezpečnosti.
Pokiaľ ide o odborníkov v oblasti kybernetickej bezpečnosti, v rôznych publikáciách sa stále uvádza nedostatok zručností v oblasti kybernetickej bezpečnosti, v ktorých sa uvádza, že prvé tri kompetencie chýbajú alebo nie sú dostatočne pokryté existujúcimi odborníkmi[19]. Na druhej strane rôzne európske a medzinárodné organizácie ponúkajú značné množstvo kurzov a školení súvisiacich s kybernetickou bezpečnosťou. Jednoduchým vyhľadávaním na internete sa odhalí mnoho kurzov, ktoré sa týkajú oblasti kybernetickej bezpečnosti, bez toho, aby sa poskytol jasný obraz o ponúkaných kompetenciách alebo o tom, ako by sa mohli týkať konkrétnej úlohy. Na doplnenie tohto zmätku existujú kurzy odbornej prípravy, ktoré podľa všetkého riešia jednu konkrétnu úlohu (napr. CISO), majú podobné názvy, ale majú odlišné učebné osnovy.

Preto vo viacerých prípadoch poskytnuté informácie zamieňajú stážistu o tom, čo a ako by mal vnímať koncepcie kybernetickej bezpečnosti, ako aj o tom, ako ich využiť na pokrytie ich profesionálnych potrieb. Okrem toho sa kurzy pre odborníkov propagujú na rôznych platformách a je ťažké ich porovnať, pokiaľ ide o zahrnuté kompetencie a riešený profil rolí. To sťažuje jednotlivcovi vybudovať si jasnú kariérnu dráhu a identifikovať príležitosti na rozvoj.

[18] https://www.concordia-h2020.eu/blog-post/towards-an-integrated-platform-for-skills-in-cyberbuilt-on-the-european- rámec pre kybernetický-zručnosť/

[19] https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2022/state-of-the-cybersecurity-workforce-new- isaca-výskum-show-retention-ťažkosti-v-roky

## CONCORDIA mapa kurzov pre profesionálov v oblasti kybernetickej bezpečnosti

V snahe riešiť tieto výzvy sme vytvorili mapu kurzov a školení pre profesionálov v oblasti kybernetickej bezpečnosti[20]. Na mape sa zobrazujú štruktúrované informácie o existujúcej európskej ponuke krátkych kurzov/školení a poskytujú sa rôzne filtre, aby sa zjednodušila konkrétna potreba rozvoja zručností s ponukou.[...]

Môžete si vybrať triedenie kurzov na základe príslušnej úrovne kybernetickej bezpečnosti (zariadenie, sieť-, softvér/systém, údaje/aplikácia –, User-Centric) alebo na základe relevantnosti pre odvetvie priemyslu (napr. telekomunikácie, financie, doprava e-mobilita, elektronické zdravotníctvo alebo obrana), ale aj podľa formátu (osobné, online, zmiešané) a načasovania kurzu/odbornej prípravy.

## Chýbajúca kľúčová zložka – riešenie povolené ECSF

Hoci na mape CONCORDIA ponúkame veľké množstvo filtrov, ktoré používateľom pomôžu ľahšie identifikovať kurz(-y) záujmu, v databáze chýba kľúčová zložka – odkazy na profily rolí, ktorými sa každý kurz zaoberá prostredníctvom znalostí a zručností. V európskom rámci kompetencií pre odborníkov v oblasti IKT, ktorý je k dispozícii v čase vypracovania mapy, sa vymedzuje 30 profilov rolí a 40 súvisiacich kompetencií, ale je ťažké ich spájať s osobitosťami oblasti kybernetickej bezpečnosti.

Išlo o výzvu ekosystému vzdelávania v oblasti kybernetickej bezpečnosti, ktorý sme označili už pred dvoma rokmi a zachytili sme ho v pláne pre vzdelávanie CONCORDIA v21 rámci okruhu C5: Rôznorodosť terminológie súvisiacej s kompetenciami. Tento nedostatok prierezovej domény a medzi odvetvovej terminológie súvisiacej s kybernetickobezpečnostnými zručnosťami potrebnými pre konkrétnu úlohu sťažuje spoločnostiam obsadzovanie otvorených pozícií. Je pre nich ťažké zosúladiť kritériá prijímania do zamestnania so štúdiami a kvalifikáciami uvedenými v životopisoch uchádzačov z dôvodu používania neštandardnej terminológie. Jednotlivci zase nedokážu ľahko identifikovať zručnosti, ktoré potrebujú na to, aby uspokojili dopyt na trhu. A nakoniec, poskytovatelia kurzov majú ťažkosti pri navrhovaní učebných osnov, ktoré zodpovedajú potrebám trhu. V rámci plánu CONCORDIA sme sa zaviazali k jednej platforme hosťujúcej všetky existujúce programy súvisiace s kybernetickou bezpečnosťou (univerzitná úroveň a doktorandské programy, krátke kurzy a školenia pre profesionálov). [...]

Platforma by mala zvážiť zber obsahu pomocou kategórií založených na štandardnej terminológii (vrátane špecifického rámca zručností). Kategórie by sa ďalej používali ako filtre pre rôzne otázky databázy kurzov. Zdá sa, že 12 profilov rolí vymedzených v súčasnej verzii európskeho rámca pre zručnosti v oblasti kybernetickej bezpečnosti (ECSF) je prirodzeným riešením.

## Prínos pre zainteresované strany

Prijatie štandardného lexikónu, ako je ten, ktorý navrhuje ESCF, vrátane profilov rolí v oblasti kybernetickej bezpečnosti pomôže spoločnostiam identifikovať správne talenty pre pracovné miesta, ako aj poskytovateľom vzdelávania, aby lepšie formovali svoje učebné osnovy tak, aby zodpovedali potrebám kybernetickej pracovnej sily. Použitím rovnakej terminológie a použitím celoeurópskeho rámca zručností na opis pracovných miest by opis kurzu a profil rolí pomohli jednotlivcom vybrať správne vzdelávacie moduly na podporu ich kariérneho postupu

[20] https://www.concordia-h2020.eu/map-courses-cyber-professionals/
21 https://www.concordia-h2020.eu/wp-content/uploads/2021/10/roadmaps-05-Education.pdf

a lepšie filtrovať otváranie pracovných miest podľa ich kompetencií a úrovne odborných znalostí. A napokon, tvorcovia politík by boli schopní zhromažďovať štruktúrovanejšie údaje na úrovni krajiny/regiónu na podporu budúceho rozvoja politiky a mali by pevný základ pri koordinácii s vonkajšími krajinami pri riešení globálnych výziev v oblasti kybernetickej bezpečnosti.

### Smerom k integrovanej platforme pre zručnosti

Na základe databázy kurzov a školení pre odborníkov v oblasti kybernetickej bezpečnosti CONCORDIA sa projekt REWIRE[22] snaží podniknúť ďalšie kroky smerom k integrácii príslušného obsahu súvisiaceho s kyberneticko-bezpečnostnými zručnosťami. Platforma REWIRE CyberABILITY – v súčasnosti vo fáze navrhovania – bude poskytovať aktuálne informácie o trhu práce, kompetenciách, kurzoch odbornej prípravy, certifikačných schémach a kariérnom pláne.

## B.2 PRÍPAD POUŽITIA Z PROJEKTU SPARTA H2020

Táto časť obsahuje časti z prípadu použitia napísaného projektom SPARTA H2020[23].

### Zlepšenie vysokoškolského vzdelávania pomocou ECSF a návrhára učebných osnov SPARTA

#### Úvod

V tomto prípade použitia sa uvádzajú odporúčania, ako možno ECSF použiť na formovanie vzdelávacích programov, ktoré sú spojené s kybernetickou bezpečnosťou. Keďže ECSF preukazuje štruktúru profilov na vysokej úrovni z hľadiska odborníkov z praxe vrátane hlavných úloh, príslušných znalostí a zručností, môže to poskytnúť cielenejší prístup k budovaniu špecializovaných a komplexných študijných programov prispôsobených konkrétnym profilom namiesto toho, aby sa vzťahovali na kybernetickú bezpečnosť vo všeobecnosti.

#### Výzva

Vzdelávacie inštitúcie zostavujú svoje učebné osnovy vzhľadom na kompletnú cestu – počnúc základnými kurzami, ktoré sú potrebné na to, aby sa študent učil ako základ pre ďalší súbor nadväzujúcich kurzov, ktoré sú často špecifické pre kybernetickú bezpečnosť. Výber kurzov, ktoré sa majú zahrnúť do učebných osnov kybernetickej bezpečnosti, však závisí od inštitúcie.
Každá vzdelávacia inštitúcia má svoje vlastné špecifické prostredie (určené napr. infraštruktúrou, vybavením, odbornými znalosťami učiteľov, zložením existujúcich programov atď.) a neexistuje univerzálny spôsob, ako by sa učebné osnovy mali zostavovať.

Poskytovatelia vzdelávania sa líšia v tom, na akú konkrétnu subdoménu kybernetickej bezpečnosti by sa chceli zamerať. Niektorí poskytovatelia sú veľmi technickí a zameriavajú sa napr. na informatiku, niektorí viac sociálne orientovaní, so zameraním na právne a spoločenské aspekty. Preto je interoperabilita medzi výslednými študijnými programami a spoločným jazykom v súčasnosti významnou výzvou.
Niektoré akademické programy nevytvárajú zručnosti a kompetencie, ktoré pripravujú študentov na konkrétne pracovné úlohy dostupné na trhu práce. To predstavuje výzvu pre študentov, ktorí nechápu, aké sú možnosti zamestnania na konci ich štúdia.

[22] https://rewireproject.eu/
[23] https://sparta.eu/assets/pdf/ECSF%20Training%20and%20education%20use%20case%20with%20SPARTA%20Curricula%20Designer.pdf

**Riešenie, ktoré umožňuje ECSF**

ECSF môže prispievať k týmto činnostiam, ktoré riešia uvedené výzvy:

- Hodnotenie: Opis profilov umožňuje inštitúciám prehodnocovať svoje učebné osnovy štruktúrovaným a systematickým spôsobom a pochopiť názor odborníkov z praxe. To umožňuje pochopiť, pre aký profil sa inštitúcia zameriava najmä na svojich absolventov.
- Zlepšenie: Môže sa vykonať na základe hodnotenia. To je obzvlášť dôležité vzhľadom na súbor znalostí/zručnosti pripisovaných špecifickému profilu.
- Zameranie: Vzdelávanie poskytované univerzitami sa môže líšiť v spôsobe, akým riešia základné kompetencie. Niektorí môžu byť viac zameraní na špecifické technologické kurzy, niektoré na právo, iné na forenznú oblasť atď. Keďže majú ECSF na spoluprácu, môžu zmapovať svoje základné kompetencie do rôznych oblastí kurzov, ktoré sú dôležité pre vymedzené profily. To umožňuje inštitúcii vytvárať účinnejšie cielené programy interne zamerané na hlavné kompetencie.
- Spolupráca: ECSF poskytuje poskytovateľom vzdelávania spoločný jazyk a slovnú zásobu na opis ich kurzov, vytváranie spoločných programov a umožnenie mobility študentov.

Pri uplatňovaní ECSF na vzdelávanie v oblasti kybernetickej bezpečnosti sa odporúča tento prístup:

- Kurzy v učebných osnovách možno zaradiť do kategórií Základná alebo kybernetická bezpečnosť. Základné kurzy sú tie, ktoré nemusia byť priamo spojené s ECSF, ale ktoré slúžia ako predpoklad pre neskoršie štúdie. Napríklad základná kryptológia je predpokladom pre kryptoanalýzu alebo pokročilú kryptológiu; Teória čísel je potrebná pre väčšinu stredne pokročilých a pokročilých počítačových kurzov.
- Po určení základných kurzov možno navrhnúť kurzy kybernetickej bezpečnosti s cieľom riešiť požiadavky pracovných rolí, na ktoré sa študenti zameriavajú. Prepojenie sa uskutočňuje na základe obsahu jednotlivých kurzov, ktoré možno prepojiť s profilmi a nakoniec s pracovnými rolami. Konkrétne kroky [...] sú:
    a. Pre konkrétnu pracovnú úlohu 1 poskytovatelia vzdelávania nájdu príslušné profily (profil 1 a profil 12 v našom príklade). Toto mapovanie označené hnedými šípkami by mali špecifikovať inzerenti/zamestnávatelia pracovných miest.
    b. Poskytovatelia vzdelávania identifikujú potrebné znalosti a zručnosti pre vybrané profily. Tieto požiadavky definuje ECSF označený modrými šípkami.
    c. Poskytovatelia vzdelávania navrhujú nové alebo opätovne používajú existujúce kurzy (v našich príkladoch 1, 2, 3, 4), ktoré sa zaoberajú vedomosťami a zručnosťami identifikovanými vo vyššie uvedenom kroku. Toto mapovanie medzi kurzami a ich obsahom musia vykonávať správcovia kurzov.
    d. Všetky potrebné kurzy (a všetky predpoklady pre ne, všeobecné kurzy, ktoré sa netýkajú kybernetickej bezpečnosti, iné kurzy na rozšírenie rozsahu študentov atď.), jadro učebných osnov je pripravené.
- Samozrejme, ECSF sa môže použiť aj úplne opačným spôsobom: najprv skomponovať učebné osnovy z jednotlivých kurzov, analyzovať poskytnuté znalosti a zručnosti, využívať ECSF na identifikáciu profilov a napokon nájsť pracovné úlohy, ktoré sú podporované učebnými osnovami. Toto mapovanie odhaľuje, aké presné znalosti a zručnosti sa už nachádzajú v učebných osnovách alebo na druhej strane, čo chýba a čo by sa malo zdôrazniť alebo pridať do kurzov. ECSF tak

pomáha štruktúrovať učebné osnovy tak, aby lepšie zodpovedali očakávaným profilom a pracovnými rolami.

**Výsledok/pridaná hodnota podľa SPARTA**

Projekt Sparta využil rámec zručností v oblasti kybernetickej bezpečnosti na vytvorenie bezplatného nástroja s názvom Dizajn osnov kybernetickej bezpečnosti. Je to jednoduchá webová aplikácia, ktorá pomáha poskytovateľom vzdelávania vytvárať nové študijné programy o kybernetickej bezpečnosti a/alebo analyzovať existujúce študijné programy podľa ich obsahu a odrazu požiadaviek na kyberneticko-bezpečnostné pracovné miesta.

Nástroj [...] umožňuje správcom študijného programu zostaviť svoj študijný program ťahaním a pádom kurzov z ľavej časti do strednej časti. Kurzy, z ktorých administrátori vyvíjajú študijné programy, môžu byť preddefinované alebo vlastné. Pri zostavovaní študijného programu sa štatistické údaje o jeho obsahu zobrazujú v pravej časti. Okrem iných údajov sa poskytujú informácie o tom, aké kompetencie a pracovné rolí sú podporované programom. Pomocou nástroja je ľahké zistiť, aký obsah chýba v študijnom programe a aké konkrétne pracovné rolí sú najvhodnejšie pre absolventov programu. V tomto prípade je rámec pre kyberneticko-bezpečnostné zručnosti jadrom aplikácií, ktoré umožňujú prepojenie zručností a znalostí s pracovnými rolami. [...]

## B.3 PRÍPAD POUŽITIA Z INCIBE

Táto časť obsahuje časti z prípadu použitia napísaného INCIBE[24].

**Prípad použitia od INCIBE**

**Úvod**

Účinnosť ochrany krajiny vo veľkej miere závisí od schopností jej obyvateľov a v tejto súvislosti sa odhaduje, že do roku 2022 by Španielsko mohlo dosiahnuť pracovnú silu v oblasti kybernetickej bezpečnosti takmer 122 284 pracovníkov s deficitom talentov odhadovaným na 24 119. Jednou z hlavných priorít dnešnej administratívy je preto čeliť výzve identifikovať, prilákať, rozvíjať a udržať talenty v rôznych oblastiach kybernetickej bezpečnosti.

Dôkazom tohto záväzku je vypracovanie národnej stratégie kybernetickej bezpečnosti španielskej vlády z roku 2019[25], v ktorej sa zdôrazňuje potreba nielen zaujať obranné a ochranné postavenie pre spoločnosti a občanov, ale aj podporiť posilnenie kybernetického priemyslu, pričom sa uznáva kľúčová úloha, ktorú kybernetická bezpečnosť zohráva v súčasnom prostredí transformácie a neistoty, a príležitosť, ktorú ponúka na zvýšenie konkurencieschopnosti Španielska. V súlade s cieľom 4 stratégie sa v akčnom riadku 5 zdôrazňuje význam posilnenia španielskeho odvetvia kybernetickej bezpečnosti okrem vytvárania a udržania talentov na posilnenie digitálnej autonómie.

Na druhej strane sa plán digitálneho Španielska na rok 2025[26] snaží posilniť páky, ktoré uľahčia návrat na cestu hospodárskeho rastu, a jednou z jeho strategických osí je posilniť kapacitu Španielska v oblasti kybernetickej bezpečnosti s cieľom zmierniť riziká a zvýšiť dôveru v cestu k digitálnemu a udržateľnému hospodárstvu.

Do svojej strategickej osi 4, ktorá je monograficky zameraná na kybernetickú bezpečnosť, zahŕňa opatrenia, ktoré tvoria tri hlavné línie činnosti INCIBE na nadchádzajúce roky: zvyšovanie spôsobilostí občanov a spoločností v oblasti kybernetickej bezpečnosti; posilnenie španielskeho ekosystému kybernetickej bezpečnosti v oblasti jeho priemyslu, výskumu, vývoja a inovácií a talentov v oblasti kybernetickej bezpečnosti; a konsolidácia Španielska ako medzinárodného uzla v tomto sektore. Španielsko Digital 2025 už uznáva kľúčovú úlohu talentov v oblasti kybernetickej bezpečnosti ako hnacej sily tohto odvetvia.

[24] http://www.incibe.es/en/talento-hacker/publications/european-cybersecurity-skills
[25] http://www.incibe.es/en/talento-hacker/publications/european-cybersecurity-skills
[26] https://portal.mineco.gob.es/ca-es/ministerio/estrategias/Pagines/00_Espana_Digital_2025.aspx

Tieto vnútroštátne iniciatívy vytvárajú vhodný scenár, ktorý podporuje výskum, inovácie a zahŕňa najrelevantnejších aktérov hodnotového reťazca, ako sú vzdelávacie inštitúcie a organizácie, aby videli prínos riadenia znalostí, schopností a technologických skúseností, ktoré reagujú na veľké výzvy, ktoré krajina predstavuje z hľadiska kybernetickej bezpečnosti.

Španielsky národný inštitút kybernetickej bezpečnosti (INCIBE), spoločnosť pod ministerstvom hospodárstva a digitálnej transformácie, prostredníctvom štátneho tajomníka pre digitalizáciu a umelú inteligenciu; a referenčný subjekt pre rozvoj kybernetickej bezpečnosti a digitálnej dôvery občanov a spoločností a španielskej akademickej a výskumnej siete (RedIRIS) má za úlohu zlepšiť kybernetickú bezpečnosť a digitálnu dôveru občanov, maloletých a súkromných spoločností v Španielsku.

Jej poslaním je okrem toho ochrana a obrana týchto skupín, podpora španielskeho priemyslu a výskumu, vývoja a inovácií v oblasti kybernetickej bezpečnosti, ako aj identifikácia, generovanie a prilákanie talentov do sektora kybernetickej bezpečnosti.

Kyberneticko-bezpečnostné talenty sú preto základným kameňom činnosti INCIBE. Bez talentu nie je možné vyvinúť silné odvetvie alebo riešenia s vysokou pridanou hodnotou potrebné na účasť na vysoko konkurenčnom trhu, ako je kybernetická bezpečnosť.

Doteraz dostupné informácie o stave talentov v sektore kybernetickej bezpečnosti v Španielsku však boli rôznorodé a roztrieštené a pochádzali z rôznych zdrojov, čo bránilo hlbokému pochopeniu prostredia potrebného na nasmerovanie opatrení. [...]

Preto s cieľom ponúknuť jasnú víziu talentov v oblasti kybernetickej bezpečnosti v Španielsku agentúra INCIBE v marci 2022 uverejňuje výsledky analýzy a diagnostiky talentov v oblasti kybernetickej bezpečnosti na vnútroštátnej úrovni, ktorých proces sa uskutočnil prostredníctvom prísnych analytických priestorov, globálneho pracovného prístupu a participantových a inkluzívnych procesov, v ktorých sa zohľadnili hlavní aktéri ekosystému kybernetickej bezpečnosti. [...]

**Výzva**

Odporúčania vyplývajúce z tohto analytického projektu sú východiskovým bodom na zabezpečenie silného a ziskového odvetvia kybernetickej bezpečnosti, ktoré sa vyznačuje tým, že talenty ľudí sú jadrom iniciatív. V tomto zmysle môže celý hodnotový reťazec kybernetickej bezpečnosti vnímať túto štúdiu ako príležitosť na ďalšie prepojenie a lepšie pochopenie kyberneticko-bezpečnostných talentov v Španielsku.

Preto je potrebné štruktúrovať a uplatňovať účinné postupy, ktoré majú vplyv na riadenie tohto špecifického typu talentov v organizáciách. Význam kybernetickej bezpečnosti pre prežitie organizácií si vyžaduje, aby sa riešil problém identifikácie tohto typu konkrétnych talentov v oblasti kybernetickej bezpečnosti, vývoj náboru a procesu nástupu do lietadla, ako aj prijatie opatrení, ktoré prispievajú k zlepšeniu riadenia a zmierneniu úniku talentov.

Z tohto dôvodu je presadzovanie vnútroštátnych politík koordinovaných administratívou, ktoré sa zameriavajú na posilnenie a podporu iniciatív na to, aby sa kybernetická bezpečnosť stala strategickou prioritou v organizáciách, ako aj štruktúrovanie a štruktúrovanie trasy odbornej prípravy zameranej na výkon kybernetickej bezpečnosti ako profesionálnej činnosti, priority, na ktoré organizácie aj náborové spoločnosti stanovia vo svojich činnostiach zameraných na identifikáciu, prilákanie, nábor a riadenie talentov v oblasti kybernetickej bezpečnosti.

Týmto spôsobom sa stanovuje súbor odporúčaní, ktoré by tento typ agentov (verejná správa, náborové spoločnosti a iné organizácie) mohli realizovať s cieľom zvýšiť talenty v oblasti kybernetickej bezpečnosti v Španielsku a ktoré predstavujú východiskový bod na riešenie výziev, ktoré v tejto súvislosti stoja pred sebou. [...]

### Riešenie, ktoré umožňuje ECSF

Existuje niekoľko faktorov (politických, hospodárskych, sociálnych, technologických, právnych atď.), ktoré môžu ovplyvniť odvetvie kybernetickej bezpečnosti a následne nedostatok talentov, medzery a vo všeobecnosti nesúlad medzi ponukou a dopytom.

Jedným z týchto relevantných faktorov v Európskej únii je nedostatočná normalizácia vymedzenia kyberneticko-bezpečnostných úloh a zručností spojených s týmito úlohami.

Poskytnúť základ pre nepretržitú komunikáciu medzi rôznymi zainteresovanými stranami (vládou, priemyslom, akademickou obcou, tvorcami politík a občanmi). Tento typ nástroja slúži ako základ pre kompetentnejšiu a úplnejšiu pracovnú silu, ktorá rozumie rovnakému jazyku ako ostatní odborníci v Európe. [...]

### Výsledok/pridaná hodnota

V predloženom kontexte sa preto na vnútroštátnej úrovni začali dve iniciatívy, ktoré prinesú hodnotu ECSF, ktorý vypracovala agentúra ENISA a ktoré budú veľmi užitočné. [...] Obe iniciatívy, ktoré sú navzájom koordinované, budú zahŕňať ECSF ako homogénny rámec na vymedzenie profilov kybernetickej bezpečnosti, ktorý Španielsku umožní dosiahnuť jeho ciele v oblasti talentov a zosúladiť sa so zvyškom krajín na európskej úrovni. [...]

## B.4 PRÍPAD POUŽITIA Z EURÓPSKEJ ORGANIZÁCIE PRE KYBERNETICKÚ BEZPEČNOSŤ (ECSO)

Táto časť obsahuje časti z prípadu použitia, ktorý napísala Európska organizácia pre kybernetickú bezpečnosť (ECSO)[27].

### Smerom k harmonizovanému prístupu k vzdelávaniu s európskym rámcom pre zručnosti v oblasti kybernetickej bezpečnosti (ECSF)

Keďže ECSO pracovala na vzdelávaní, odbornej príprave a zručnostiach vo svojej pracovnej skupine 5 od roku 2016, z prvej ruky zaznamenala výzvy, ktoré predstavuje fragmentácia a rozptýlené prístupy, ktoré dnes existujú v rámci kybernetickej bezpečnosti. V tomto blogovom príspevku sa ECSO zaoberá existujúcimi európskymi prístupmi k vzdelávaniu a zvyšovaniu úrovne zručností a zameriava sa na európsky rámec pre zručnosti v oblasti kybernetickej bezpečnosti (ECSF) agentúry ENISA.

Vzdelávanie nie je len výsadou štátu. Neodmysliteľne súvisí aj so spoluprácou medzi vnútroštátnymi subjektmi, širšou komunitou v oblasti kybernetickej bezpečnosti a európskymi orgánmi. Vzhľadom na to je spolupráca kľúčová pri navrhovaní celoeurópskych prístupov k harmonizácii učebných osnov v oblasti kybernetickej bezpečnosti a k riešeniu zručností alebo, konkrétnejšie, nedostatku pracovnej sily. Existuje dostatok príležitostí na využitie spoločného ducha európskej komunity v oblasti kybernetickej bezpečnosti s cieľom poskytnúť praktické riešenia a iniciatívy, ktoré môžu mať vplyv „v praxi“, a Európsky rámec pre zručnosti v oblasti kybernetickej bezpečnosti (ECSF) agentúry ENISA môže v tejto súvislosti zohrávať významnú úlohu.

### Vzdelávanie v oblasti kybernetickej bezpečnosti: perspektíva ECSO

Z pohľadu Európskej organizácie pre kybernetickú bezpečnosť (ECSO), ktorá je reprezentatívnym orgánom európskeho verejno-súkromného ekosystému a komunity v oblasti kybernetickej bezpečnosti, potenciál hodnota ECSF je nezanedbateľná, pokiaľ ide o prepojenie existujúceho úsilia, poskytovanie základných prvkov európskej pracovnej sily v

[27] https://www.ecs-org.eu/newsroom/consolidated-educational-and-recruiting-scheme-the-glue-to-fix-todays-scattered-approach

oblasti kybernetickej bezpečnosti a vytvorenie spoločného rámca a taxonómie na uplatňovanie profilov a zručností. Odborníci na kybernetickú bezpečnosť, poskytovatelia vzdelávania a odbornej prípravy, tvorcovia politík, ako aj odborníci v oblasti náboru môžu profitovať zo širšieho vykonávania ECSF.

**Výzva**

Je zrejmé, že narastá potreba kvalifikovanej pracovnej sily v oblasti kybernetickej bezpečnosti. Rôzne štúdie z celého sveta z priemyslu a akademickej obce potvrdzujú, že dopyt po pracovnej sile v oblasti kybernetickej bezpečnosti je veľmi vysoký a že je ťažké najať kompetentných odborníkov. Vo výročnej štúdii pracovnej sily v oblasti kybernetickej bezpečnosti z roku 2021, ktorú uverejnil člen ECSO (ISC)[28], sa uvádza, že nedostatok odborníkov v oblasti kybernetickej bezpečnosti je na celom svete 2,72 milióna, čo je napriek tomu, že sa znížil z 3,12 milióna v predchádzajúcom roku, stále značný počet. Hoci tieto štúdie poskytujú základ na posúdenie globálnej situácie, skutočnosťou je, že je veľmi ťažké vyčísliť rozsah nedostatku talentov v oblasti kybernetickej bezpečnosti v Európe. Vieme, že dopyt po expertoch nevyhnutne vzrastie v dôsledku rastu trhu kybernetickej bezpečnosti a regulačného prostredia, čo zanechá naliehavú medzeru na vyplnenie väčšieho počtu (a rôznych druhov) odborníkov. [...]

Nie je to však len otázka čísel. Prostredníctvom nedávnej štúdie ECSO o postupoch a trendoch v oblasti náboru ľudských zdrojov zaznamenal ECSO aj nárast času, ktorý v priemere trvá, kým organizácie obsadia svoje kyberneticko-bezpečnostné pozície. Mnohé organizácie uvádzajú, že proces prijímania zamestnancov môže trvať až šesť mesiacov, čo je pomalšie ako v oblasti objednávok, zatiaľ čo iné uvádzajú, že majú ťažkosti s úplným obsadením svojich pozícií v oblasti kybernetickej bezpečnosti. To jasne naznačuje, že existuje nesúlad medzi ponukou a dopytom (t. j. rozdiel medzi akademickou obcou a požiadavkami odvetvia) a faktormi push/pull (t. j. vhodnosť a hodnotenie kandidátov, prilákanie pracovných miest a prínosov). Hlavným problémom pre zamestnávateľov však zostáva všeobecný nedostatok odborníkov na kybernetickú bezpečnosť na celom svete, zatiaľ čo dopyt neustále rastie. Niekoľko organizácií tiež zdôrazňuje zložitosť náboru odborníkov pre oblasť, ktorú nezvládajú. Z prieskumu ECSO takisto vyplynulo, že ako rastúci trend niekoľko kandidátov napriek tomu, že im chýbajú významné kyberneticko-bezpečnostné zručnosti, stále obohacuje svoj životopis o koncepcie kybernetickej bezpečnosti a kľúčové slová.

Tieto výzvy jasne zdôrazňujú potrebu spoločného jazyka na podporu náborového úsilia a význam zváženia multidisciplinárnej povahy kybernetickej bezpečnosti, ktorá je tak jedinečná v tejto oblasti v porovnaní s tradičnejšími profesiami v oblasti IT/IKT. Zatiaľ čo existujúce rámce, ako sú NICE, CyBOK a eCF, poskytujú užitočné usmernenia pre rozvoj zručností, chýba európsky rámec, ktorý poskytuje zastrešujúcu taxonómiu profilu a kariérne dráhy spojené s kybernetickou bezpečnosťou. Uvoľnenie ECSF je preto veľmi aktuálne a zásadné na podporu európskej komunity v oblasti kybernetickej bezpečnosti v priťahovaní, získavaní zručností a rekvalifikácii odborníkov.

**Existuje riešenie**

ECSO bude uplatňovať ECSF viacerými spôsobmi s cieľom posilniť jeho využívanie a využiť jeho potenciál na harmonizáciu vzdelávania a zručností v oblasti kybernetickej bezpečnosti v celej Európe.

[28] https://www.isc2.org/Research/Workforce-Study

ECSO bude:

- mapovať svoje minimálne referenčné učebné osnovy do ECSF a poskytnúť tvorcom kurzov a odborníkom z praxe pohľad z prvej ruky na to, ako čo najlepšie definovať svoje učebné osnovy smerom k špecializovaným kariérnym dráham. To pomôže zabezpečiť, aby univerzitné kurzy primerane odrážali realitu potrieb trhu práce v oblasti kybernetickej bezpečnosti a zároveň umožnili nepretržitú aktualizáciu učebných osnov.

- používať ECSF a príručku na použitie na podporu ľudských zdrojov/prijímania pracovníkov pri vypracúvaní inzerátov o pracovných miestach a organizácii postupov hodnotenia/hodnotenia praktických zručností. Bude vykonávať aj následný prieskum ľudských zdrojov s využitím profilov pracovných miest ECSF, aby sme pochopili, aké úlohy organizácie najviac potrebujú, a postupne si vybudovali kvantitatívne chápanie európskeho trhu práce v oblasti kybernetickej bezpečnosti.

- používať ECSF ako základnú taxonómiu pre dve špecializované platformy, ktoré plánujú nadácia Women4Cyber Foundation a ECSO [...]

**Výsledok a pridaná hodnota**

Pridaná hodnota ECSF pre európsku kybernetickú komunitu je v prvom rade mať spoločný rámec a taxonómiu, na ktorých by sa malo pracovať. To povedie k lepšiemu pochopeniu potrieb v oblasti zručností a praktickej realite rôznych profilov pracovných miest, čo posilní pracovnú silu v oblasti kybernetickej bezpečnosti, a to nielen prostredníctvom účinnejších opatrení v oblasti náboru a uchovávania, ale aj uľahčením vstupu alebo opätovného vstupu väčšieho počtu žien a iných nedostatočne zastúpených skupín (t. j. neurodiverzných) do tejto oblasti. ECSF tým, že zdôrazňuje technické a netechnické aspekty rôznych profilov, prispeje k odstráneniu mylnej predstavy, že kybernetická bezpečnosť je len technická téma, keď sa týka ľudí a procesov. V tejto súvislosti zdôraznenie významu mäkkých (prenosných) zručností v tejto oblasti významne prispeje k prilákaniu väčšieho počtu žien do profesie kybernetickej bezpečnosti. ECSF takisto zníži fragmentáciu prístupov zavedením usmernení zhora nadol, ako kategorizovať mnohostranný charakter povolania v oblasti kybernetickej bezpečnosti. Profily, ktoré navrhuje ECSF, sú dostatočne široké na to, aby mohli podporiť mnohé úlohy, ktoré toto povolanie ponúka, pričom je rozdelené tak, aby bolo zrozumiteľné a použiteľné pre odborníkov z praxe, odborníkov z odvetvia, tvorcov politík, špecialistov na nábor a uchádzačov o zamestnanie.

V ECSO sme presvedčení, že ECSF poskytne významnú hodnotu našej práci a podporí širšiu komunitu konkrétnym nástrojom na harmonizáciu úsilia a preklenutie priepasti medzi dopytom a ponukou odborníkov.

## B.5 PRÍPAD POUŽITIA Z ISC2

Táto časť obsahuje časti z prípadu použitia napísaného (ISC)[229].

**Využívanie (ISC)² CISSP CBK na podporu európskeho rámca zručností v oblasti kybernetickej bezpečnosti/profesionálnych komunít v oblasti kybernetickej bezpečnosti**

[29] https://www.isc2.org/-/media/9644E0ED44954F7CAF895D45620213EA.ashx

## Úvod

(ISC)² CISSP CBK – niekedy jednoducho nazývaný „Body of Knowledge“ – odkazuje na rovesníkmi vypracovaný prehľad toho, čo musí kompetentný odborník v oblasti kybernetickej bezpečnosti identifikovať a vlastniť, vrátane vedomostí, zručností, schopností, techník a postupov, aby boli úspešné. CBK (ISC)² je zbierka tém relevantných pre odborníkov v oblasti kybernetickej bezpečnosti po celom svete. Vytvára spoločný rámec podmienok a zásad informačnej bezpečnosti, ktorý umožňuje odborníkom v oblasti kybernetickej bezpečnosti a IT/IKT na celom svete diskutovať, debatovať a riešiť otázky týkajúce sa povolania so spoločným porozumením, taxonómiou a lexikonom. (ISC)² bola vytvorená čiastočne s cieľom agregovať, štandardizovať a udržiavať (ISC)² CBK pre odborníkov v oblasti kybernetickej bezpečnosti na celom svete. CBK (ISC)2 predstavuje hotový zdroj pre súčasných a ašpirujúcich odborníkov v oblasti kybernetickej bezpečnosti na prijatie v rámci ECSF.

## Výzva

Ako agentúra ENISA opisuje vo svojej nedávno uverejnenej správe s názvom Riešenie nedostatku a rozdielov v zručnostiach v oblasti kybernetickej bezpečnosti v EÚ prostredníctvom vysokoškolského vzdelávania, celosvetový nedostatok zručností v oblasti kybernetickej bezpečnosti a nedostatok dostatočnej a kvalifikovanej pracovnej sily vyvoláva obavy, ktoré majú významný vplyv na schopnosť členských štátov EÚ chrániť verejnosť pred rastúcimi hrozbami vyplývajúcimi z neustále sa zvyšujúceho využívania technológií v spoločnosti. Napriek vykonanej práci sú kybernetické útoky a hrozba kybernetických útokov naďalej významným rizikom pre verejnú bezpečnosť. Európske organizácie sa snažia primerane zamestnať svoje tímy v oblasti kybernetickej bezpečnosti. Dôsledky, ktorým sa dá predísť – nesprávne konfigurované systémy, urýchlené nasadenie, neúplná reakcia na incidenty, oneskorené opravy, nedostatočné riadenie rizík – spôsobujú, že mnohé európske organizácie lákajú ciele pre aktérov hrozieb na celom svete.

## Riešenie, ktoré umožňuje ECSF (ako sa riešili výzvy)

S cieľom reagovať na výzvy, ktoré predstavuje nedostatok zručností a nedostatok pracovnej sily, (ISC)² navrhuje riešenie zamerané na pomoc odborníkom v oblasti kybernetickej bezpečnosti identifikovať a mapovať potrebné znalosti, zručnosti, schopnosti, techniky a postupy s profilmi identifikovanými v európskom rámci pre zručnosti v oblasti kybernetickej bezpečnosti (ECSF). (ISC)2 CISSP CBK mapuje niekoľko oblastí zručností a vedomostí v týchto profiloch ECSF:

- 2.1 Hlavný úradník pre bezpečnosť informácií (CISO)
- 2.2 Koordinátor reakcie na kybernetické incidenty
- 2.3 Úradník pre kybernetické právo, politiku a dodržiavanie predpisov
- 2.4 Špecialista na spravodajské informácie o kybernetických hrozbách
- 2.5 Architekt kybernetickej bezpečnosti
- 2.6 Audítor kybernetickej bezpečnosti

Pomocou konceptov zahrnutých v CBK môžu odborníci, ktorí v súčasnosti pracujú vo vyššie uvedených profiloch, alebo tí, ktorí sa snažia pracovať v týchto profiloch, využiť kľúčové zručnosti a oblasti vedomostí z profilov ECSF v kombinácii s (ISC)2 CBK na určenie toho, ako CBK plní vedomosti a zručnosti potrebné na danú pozíciu a kde môže byť potrebné doplniť svoje vzdelanie/odbornú prípravu z iných zdrojov. To umožní uchádzačom vybudovať si cestu vzdelávania/odbornej prípravy na dosiahnutie svojich cieľov. V nasledujúcej tabuľke sa uvádza príklad toho, ako môže súčasný CISO (ISC)2 CISSP CBK použiť na identifikáciu kľúčových zručností a oblastí znalostí z profilu CISO ECSF, ktoré má alebo potrebuje vybudovať. [...]

## Výsledok/Pridaná hodnota

Zamýšľaným prínosom mapovania CBK (ISC)² CISSP CBK pre ECSF je, že vytvorí kariérne poradenstvo a profesionálne vzdelávacie dráhy s cieľom pomôcť súčasným a ašpirujúcim odborníkom v oblasti kybernetickej bezpečnosti identifikovať a získať potrebné odborné znalosti, zručnosti a schopnosti s cieľom rýchlejšie získať a vyplniť otvorené profily, ako sa

uvádza v ECSF, čím sa zmierni nedostatok globálnych zručností v oblasti kybernetickej bezpečnosti a zmenší sa nedostatok kvalifikovanej pracovnej sily.

## B.6 PRÍPAD POUŽITIA Z ISACA

Táto časť obsahuje časti z prípadu použitia napísaného spoločnosťou ISACA[30].

### Individuálne rozhodovanie o kariére: Odborné certifikáty Európsky rámec zručností v oblasti kybernetickej bezpečnosti

#### Úvod

Sabine pracovala ako analytička SOC niekoľko rokov po získaní vysokoškolského titulu a zaujímala sa o to, ako najlepšie napredovať v kariére. Hovorila so svojím mentorom, ktorý jej poradil, že ISACA bola skvelým štartovacím bodom pre jeho kariéru a povzbudila ju, aby preskúmala členstvo a eventuálnu certifikáciu. Musíme si uvedomiť, že vstup do kybernetickej bezpečnosti dáva možnosť pracovať so všetkým, od ľudí a psychológie cez právnu, politickú a riadiacu úroveň až po najnižšiu (alebo najvyššiu) úroveň technickej úrovne. Výzvou je nájsť východiskový bod a potom určiť, aké konkrétne kompetencie sa môžete naučiť, a potom zvládnuť rozšírenie alebo dokonca prechod medzi úlohami v oblasti kybernetickej bezpečnosti. ESCF špecifikuje niekoľko úloh s ich právomocami potrebnými na prácu v rámci tejto konkrétnej úlohy. Všimnite si, že tieto kompetencie nie sú všetko, čo je potrebné pre konkrétnu úlohu, ale len minimum. Pomocou tejto Sabine môže identifikovať nedostatok kompetencií, ak chcete zmeniť úlohu alebo sa presunúť do inej oblasti v rámci kybernetickej bezpečnosti.

#### Výzva

Ako nový odborník v oblasti vysokého dopytu a ako žena v oblasti kybernetickej bezpečnosti, Sabine hľadala pomoc v niekoľkých rôznych oblastiach:

- Kariérne poradenstvo a zdroje – vrátane poverenia – s cieľom pomôcť jej napredovať v kariére
- Sieť rovesníkov a vedúcich predstaviteľov priemyslu, ktorí jej pomôžu zvládať profesionálne výzvy
- Pomoc pri rozvoji mäkkých zručností, ktoré jej pomôžu stať sa dobre zaobleným budúcim lídrom
- Poznatky o prekonávaní výziev a využívaní príležitostí ako ženy kybernetická bezpečnosť
- Informácie, ktoré jej pomôžu dobre vykonávať svoju súčasnú prácu a pomôžu jej pripraviť sa na budúce výzvy vo vyšších funkciách

Každý jednotlivec môže použiť ESCF na to, aby zistil, aké úlohy sú potrebné na zvládnutie takmer akéhokoľvek typu výziev alebo úloh v oblasti kybernetickej bezpečnosti. Aj použitím ESCF ako východiskového scenára môže jednotlivec určiť, ktoré kompetencie sú potrebné na prechod z jednej úlohy na druhú. To bude prínosom pre dialóg medzi zamestnancami a zamestnávateľmi pri plánovaní nepretržitého vzdelávania v oblasti kybernetickej bezpečnosti. To bude prínosom aj pre jednotlivca, ktorý chce vstúpiť do kybernetickej bezpečnosti, ale nie je si istý, kde začať. Pre väčšinu jednotlivcov je pridanie predchádzajúcich vedomostí a kompetencií jednoduchšie ako naučiť sa niečo úplne nové. S poslaním stať sa profesionálom v oblasti kybernetickej bezpečnosti C-suite v tejto náročnej oblasti Sabine skúmala náčrt zodpovedností CISO:

| | |
|---|---|
| Profil 1 CISO Poslanie | Definuje, udržiava a komunikuje víziu, stratégiu, politiky a postupy v oblasti kybernetickej bezpečnosti. Riadi vykonávanie kyberneticko-bezpečnostnej politiky v celej organizácii. Zabezpečuje výmenu informácií s externými a profesijnými orgánmi. |

Ambíciou Sabine je identifikovať nedostatky v jej zručnostiach, aby mohla napredovať v

[30] https://www.isaca.org/training-and-events/careers-home/career-pathway/european-cybersecurity-skills-framework-and-isaca-credentials

kariére s vhodne zosúladenými povereniami na ďalšiu úroveň.

### Riešenie ECSF

Sabine skúmala PROFILE 1 ECSF a identifikovala medzery vo svojich poznatkoch:

| | |
|---|---|
| Kľúčové znalosti | ✓ znalosť noriem kybernetickej bezpečnosti a ochrany súkromia, rámcov, politík, nariadení, právnych predpisov, certifikácií a najlepších postupov<br>Pochopenie etických požiadaviek organizácie kybernetickej bezpečnosti<br>✓ znalosť bezpečnostných kontrol<br>Znalosť modelov kyberneticko-bezpečnostnej vyspelosti<br>✓ znalosť taktiky, techník a postupov kybernetickej bezpečnosti<br>Znalosť riadenia zdrojov<br>Znalosť manažérskych postupov<br>Znalosť rámcov riadenia rizík |

Sabine sa rozhodla vziať radu svojho mentora a zúčastniť sa na miestnom stretnutí pobočky ISACA, aby zistila, či je to správne. Okamžite bola ohromená možnosťami, ktoré ponúka. Pobočka ju srdečne privítala a predstavila ju niekoľkým kľúčovým ľuďom v pobočke – ľudia, ktorí pracovali presne v tom type rolí, ktoré Sabine hľadala a boli by vynikajúcimi mentormi alebo sponzormi.

Certifikačný predseda pobočky informoval Sabine, že certifikácia Certified Information Security Manager (CISM) bude pre ňu veľmi vhodná, pretože demonštruje dobre zaoblené znalosti informačnej bezpečnosti, ako aj silné manažérske zručnosti. Certifikácia je určená pre tých, ktorí majú päť alebo viac rokov skúseností, takže Sabine sa rozhodla urobiť 18-mesačný plán na štúdium a získanie certifikátu.

V ten večer vstúpila do ISACA ako členka a v plnej miere využila zdroje, ktoré združenie ponúkalo na globálnej aj miestnej úrovni. Pripojila sa k online komunitám združenia, začala navštevovať webináre a miestne stretnutia pobočky ponúkané prostredníctvom SheLeadsTech, programu ponúkaného ISACA One in Tech Foundation. Zúčastnila sa takmer na každom stretnutí, ktoré ponúkla miestna pobočka.

Len šesť mesiacov po jej členstve ju oslovil člen pobočky s ponukou práce ako analytik informačnej bezpečnosti vo ich organizácii.

### Výsledok

Sabine je členom ISACA už sedem rokov. Získala certifikát CISM a čoskoro bola povýšená na manažéra informačnej bezpečnosti. Teraz je riaditeľkou informačnej bezpečnosti s jasnou cestou k úlohe CISO.

Okrem nájdenia poverenia a pracovných miest prostredníctvom ISACA, Sabine tiež našla niekoľko zdrojov, ktoré jej pomohli pridať hodnotu pre jej organizáciu. Pred nadobudnutím účinnosti GDPR bola Sabine schopná využiť centrum GDPR Resource Hub, ktoré jej ponúkla ISACA, aby jej pomohla dôkladne pochopiť situáciu a zistiť, aké najkritickejšie kroky mala podniknúť v jej súčasnej úlohe.

Záujem a skúsenosti, ktoré získala v oblasti ochrany súkromia v dôsledku tohto projektu, jej umožnili získať certifikát ISACA Certified Data Privacy Solutions Engineer (CDPSE) prostredníctvom svojho počiatočného prijímacieho programu.

Prezentovala sa na konferenciách ISACA na kapitulnej a na národnej úrovni – s komunikačnými schopnosťami – a minulý rok sa ujala pozície vo vrcholovom paneli. Ako riaditeľka, mala možnosť zamestnať sa na niekoľko pozícií a väčšina jej zamestnancov pochádzala z pobočky ISACA – rovnako ako pred šiestimi rokmi našla svoje prvé povýšenie. Po tom, čo videla hodnotu certifikácie CISM vo svojej vlastnej kariére, začala ponúkať certifikáciu CISM svojmu tímu prostredníctvom podnikových vzdelávacích ponúk ISACA.

Najnovšou oblasťou zamerania pre Sabine, kým sa pripravuje na rolu CISO, je zabezpečiť vznikajúcich technológií. Vzhľadom na zvýšené regulačné zameranie na umelú inteligenciu v Európe najprv nasmerovala svoje úsilie v tejto oblasti a nedávno získala osvedčenie o základoch umelej inteligencie od ISACA.

Sedem rokov po tom, čo prešla dverami svojho prvého stretnutia s pobočkou ISACA Sabine rozšírila svoju sieť o stovky odborníkov na lokálnej úrovni a tisíce ľudí na celom svete.

Je to sebavedomá líderka a rečníčka a teraz je mentorkou pre niekoľko ďalších, ktorí boli raz na jej pozícii. Medzi jej rady pre jej zverencov je vždy sa učiť – a že ISACA, ako globálna vzdelávacia komunita, je skvelým zdrojom.

Sabine načrtla kroky, ktoré by mala podniknúť, aby získala C-suite a plánuje sa ujať úlohy CISO do piatich rokov. Je presvedčená, že jej sieť ISACA a poverenia budú významnou výhodou, pri nasledovaný svojich ciele.

Kariérna cesta:

- Analytik bezpečnostných operácií SOC
- Analytik pre riziká informačnej bezpečnosti
- Manažér informačnej bezpečnosti
- Riaditeľ pre informačnú bezpečnosť

## B.7 PRÍPAD POUŽITIA Z SANS/GIAC

Táto časť obsahuje časti z prípadu použitia napísaného inštitútom SANS a GIAC (Global Information Assurance Certification)[31].

### Prečo sú v oblasti kybernetickej bezpečnosti dôležité rámce a certifikácie pracovnej sily

Smernica o sieťach a informáciách (NIS) II je aktualizáciou existujúceho mandátu Európskej únie. To pomôže podporiť spoločný jazyk kybernetickej bezpečnosti v širšom spektre odvetví hospodárstva a bude si to vyžadovať výmenu informácií medzi členskými štátmi a medzi sektormi. Takéto smernice majú čoraz väčší význam pri zriaďovaní ochranných zábradlí pre kybernetické činnosti. S cieľom chrániť hodnotu akcionárov Komisia pre bezpečnosť a výmenu (SEC) zvažuje kybernetickú správu pre verejne obchodované spoločnosti, v ktorej sa vyžaduje podávanie správ o tom, ako budú ich bezpečnostné tímy riadiť riziká, incidenty a kybernetické odborné znalosti predstavenstva. Správa o zmierňovaní bezpečnostných rizík sa bude viazať na súbory zručností v pracovných rolách.

Rámce pomáhajú formulovať tieto pracovné roly. Väčšina pracovných miest donedávna boli všeobecné zoznamy hľadajúce profesionálov v oblasti kybernetickej bezpečnosti bez dobre definovaných úloh, zručností alebo vedomostí o tom, čo je potrebné na ochranu majetku organizácií. Rámce pracovnej sily, ako je európsky rámec pre zručnosti v oblasti kybernetickej bezpečnosti ECSF (ECSF), začínajú štandardizovať talenty potrebné na pozície odpovedajúceho na kybernetické incidenty, vyšetrovateľa digitálnej forenznej vedy a hlavného úradníka pre informačnú bezpečnosť. Normalizácia umožňuje organizáciám identifikovať správne talenty na zvládanie budúcich hrozieb. Je to v súlade s inými profesiami. Napríklad

[31] https://www.giac.org/blog/why-workforce-frameworks-certifications-matter-cybersecurity/

lekári majú špecializované oblasti, ako sú rádiológovia, pediatri a mozgoví chirurgovia, ktorí majú odborné znalosti potrebné vo svojej oblasti na zabezpečenie správnej liečby.

Certifikácia zohráva dôležitú úlohu pri príprave ľudí na konkrétne pracovné úlohy. Certifikácia potvrdzuje jednotlivca použitím osvedčených postupov a usmernení pre vzdelávacie a psychologické testovanie, ako sú medzinárodné normy ISO/IEC 17024. Príkladom certifikácie, ktorá sa považuje za globálny štandard, je certifikovaný verejný účtovník (CPA). Pracovné skúsenosti môžu niekoho urobiť odborníkom, ale CPA je dobre rešpektovaným základom certifikovaného odborníka a môže byť dokonca požiadavkou na dodržiavanie súladu pri konkrétnych projektoch alebo auditoch.

Niektoré príklady, v ktorých rámce pracovnej sily pomohli napredovať v odvetví kybernetickej bezpečnosti, zahŕňajú:

- Veľké technologické a finančné firmy majú často viacero bezpečnostných tímov, ktoré štandardizujú svoje pracovné úlohy a požiadavky prostredníctvom rámca na rýchle premiestnenie a rotáciu pracovníkov na základe misie.
- Organizácie môžu zmapovať skúsenosti a certifikáciu svojich zamestnancov tak, aby rýchlo zodpovedali zručnostiam zamestnancov s požiadavkami projektu. To je obzvlášť dôležité pre poradenské firmy, technologické firmy a dodávateľov.
- Rámce poskytujú spoločný jazyk pre pracovnú silu vo všetkých odvetviach, ako sú technológie, financie, zdravotná starostlivosť, maloobchod a verejnoprospešné služby, čo umožňuje tímom spolupracovať na ochrane kybernetických a fyzických bezpečnostných hrozieb.
- Rámce poskytujú akademickým inštitúciám šablónu na preklenutie priepasti medzi ich vzdelávacími ponukami a súčasnými zručnosťami v oblasti kybernetickej bezpečnosti, ktoré sú potrebné vo všetkých odvetviach, pričom ich študenti pripravujú na pracovné miesta.

Sans a GIAC chápu význam rámcov a zosúladili kurzy a certifikácie s týmito rámcami. Rámce sú vzorom pre organizácie na štandardizáciu požiadaviek na zamestnanie, aj keď každá organizácia a úloha bude potrebovať určité prispôsobenie spojené s ich konkrétnym poslaním. Pomohli sme navrhnúť a implementovať programy rozvoja pracovnej sily pomocou rámcov ako šablóny pre spoločnosti Fortune 500, vládne agentúry a organizácie všetkých veľkostí.

## O AGENTÚRE ENISA

Agentúra Európskej únie pre kybernetickú bezpečnosť ENISA je agentúrou Únie, ktorá sa zameriava na dosiahnutie vysokej spoločnej úrovne kybernetickej bezpečnosti v celej Európe. Agentúra Európskej únie pre kybernetickú bezpečnosť zriadená v roku 2004 a posilnená Aktom EÚ o kybernetickej bezpečnosti prispieva k kybernetickej politike EÚ, zvyšuje dôveryhodnosť produktov, služieb a procesov IKT so systémami certifikácie kybernetickej bezpečnosti, spolupracuje s členskými štátmi a orgánmi EÚ a pomáha Európe pripraviť sa na budúce kybernetické výzvy. Prostredníctvom výmeny poznatkov, budovania kapacít a zvyšovania informovanosti agentúra spolupracuje so svojimi kľúčovými zainteresovanými stranami s cieľom posilniť dôveru v prepojené hospodárstvo, zvýšiť odolnosť infraštruktúry Únie a v konečnom dôsledku zabezpečiť digitálnu bezpečnosť európskej spoločnosti a občanov. Viac informácií o agentúre ENISA a jej práci nájdete tu: www.enisa.europa.eu.

**ENISA**
Agentúra Európskej únie pre kybernetickú bezpečnosť

**Aténska kancelária**
Agamemnon 14, Chalandri 15231, Attiki, Grécko

**Kancelária v Heraklione**
95 Nikolaou Plastira 700 13 Vassilika Vouton, Heraklion, Grécko

enisa.europa.eu

ISBN: 978-92-9204-583-8
DOI: 10.2824/95989