

ZODPOVEDNOSTNÉ VZŤAHY V KYBERNETICKEJ BEZPEČNOSTI

MODUL 4 „Zodpovednosť osôb pre vybrané bezpečnostné role“

Syllabus



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Financované EÚ NextGenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu č. 17R05-04-V01-00002.

Rozsah:

10 vyučovacích hodín. Vyučovací hodina má 45 min. Modul sa delí na 2 časti s časovou dotáciou 5 vyučovacích hodín pre každú časť modulu.

Obsah a forma vzdelávania:

Modul 4 skúma zodpovednostné vzťahy osôb pre vybrané bezpečnostné role, pričom vychádza z požiadaviek na znalostné štandardy v oblasti kybernetickej bezpečnosti pre rôzne role, ako sú špecialista a manažér kybernetickej bezpečnosti podľa vyhlášky č. 492/2022 Z. z. Zameriava sa na riadenie bezpečnosti, hrozieb a rizík, aplikáciu bezpečnostných opatrení, výkon operatívnych bezpečnostných činností, riadenie súladu a posudzuje súkromnoprávnu a verejnoprávnu zodpovednosť.

Modul v sebe zahŕňa aj rôzne cvičenia, prípadové štúdie pre účastníkov, ktoré im pomôžu prepojiť teoretické poznatky s praktickými zručnosťami. Modul sa uskutoční prezenčne a/alebo v rámci virtuálnej miestnosti (MS TEAMS), kde bude zachovaný reálny čas interakcie a možnosť okamžitých otázok, diskusií a spolupráce medzi účastníkmi. Vzdelávanie v rámci modulu bude rozdelené na 2 časti s časovou dotáciou 5 vyučovacích hodín pre každú časť modulu.

Osnova:**Časť 1**

- European Cybersecurity Skills Framework (ECSF) a vyhláška NBÚ č. 492/2022 Z. z.
- Prepojenie ECSF s inými normami a rámcami EÚ
- Bezpečnostné role a zodpovednosť
- Znalostné štandardy, zodpovednosti, rozdiely a vzájomne vzťahy medzi jednotlivými rolami v oblastiach riadenie bezpečnosti, riadenie hrozieb a rizík, aplikáciu bezpečnostných opatrení, výkon operatívnych bezpečnostných činností, riadenie súladu

Časť 2

- Trestnoprávna a administratívna zodpovednosť konkrétnych rolí
- Zodpovednosť osôb najmä pri rozhodovaní o rizikách a implementácii opatrení, pri riešení kybernetických bezpečnostných incidentov
- Modelové situácie na rozlíšenie zodpovednosti jednotlivcov a analýza prípadových štúdií a súdnych rozhodnutí
- Zodpovednosť osôb pri riadení bezpečnosti, hrozieb a rizík, aplikáciu bezpečnostných opatrení, výkon operatívnych bezpečnostných činností, riadenie súladu
- Civilná zodpovednosť konkrétnych rolí (zodpovednosť v pracovnoprávných vzťahoch ako aj zodpovednosť v obchodných (dodávateľských) vzťahoch)
- Modelové situácie na rozlíšenie zodpovednosti jednotlivcov a analýza prípadových štúdií a súdnych rozhodnutí

Výsledky vzdelávania:

Po absolvovaní modulu účastníci dokážu:

- identifikovať bezpečnostné roly podľa ENISA CSF a vyhlášky NBÚ č. 492/2022 Z. z. a ich úlohy v organizácii,
- vysvetliť rozdiely medzi zodpovednosťou odborných zamestnancov, špecialistov a manažérov v oblasti kybernetickej bezpečnosti,
- analyzovať právne dopady (trestné, správne, civilné) jednotlivých rozhodnutí v oblasti kybernetickej bezpečnosti,
- aplikovať právne a etické princípy zodpovednosti pri riadení rizík, implementácii opatrení a riešení incidentov.

IT manažér:

- porozumieť významu bezpečnostných rolí a zodpovednosti v rámci riadenia kybernetickej bezpečnosti v organizácii,

- určiť zodpovednosti jednotlivých rolí a ich vplyv na celkový systém riadenia bezpečnosti informácií,
- vedieť definovať zodpovednosti zamestnancov pri obstarávaní, správe a rozvoji IKT infraštruktúry,
- vyhodnocovať efektívnosť opatrení a dohliadať na dodržiavanie požiadaviek regulačných rámcov z pohľadu manažéra,
- presadzovať interné politiky kybernetickej bezpečnosti s ohľadom na právnu zodpovednosť jednotlivých rolí,
- využiť prípadové štúdie a modelové situácie na pochopenie dôsledkov rozhodnutí v rámci bezpečnostného tímu.

Informatik:

- porozumieť podstate požiadaviek vyplývajúcich z pridelených rolí,
- identifikovať zraniteľnosti a hrozby z pohľadu rôznych bezpečnostných rolí (napr. architekt, analytik, tester),
- porozumieť zručnostiam a povinnostiam vo svojom technologickom prostredí v súlade s rolou a zodpovednosťou,
- kvalifikovane komunikovať s manažérom kybernetickej bezpečnosti alebo audítorom,
- využiť prípadové štúdie a modelové situácie na pochopenie dôsledkov rozhodnutí v rámci bezpečnostného tímu.

Zamestnanec v oblasti kybernetickej bezpečnosti:

- pochopiť a uplatniť právne a etické požiadavky zodpovedajúce jeho bezpečnostnej roli,
- navrhovať a zdôvodňovať opatrenia a stratégie v kontexte svojej roly,
- analyzovať právne dôsledky nesprávneho výkonu činností a z toho vyplývajúcu osobnú zodpovednosť,
- využiť prípadové štúdie a modelové situácie na pochopenie dôsledkov rozhodnutí v rámci bezpečnostného tímu.

Literatúra:

ANDRAŠKO, J. – MESARČÍK, M. – SOKOL, P. Právo kybernetickej bezpečnosti. Učebnica. Právnická fakulta, Univerzita Komenského v Bratislave, 2022.

KLIMEK L. a kol. Počítačová kriminalita v európskych súvislostiach. 1. vyd., Bratislava: Wolters Kluwer, 2016, ISBN 9788081685385

MAKATURA, I.: Základy bezpečnostných opatrení, Príručka manažéra kybernetickej bezpečnosti. Žilina: EUROKÓDEX, s.r.o., 2023

NONNEMANN, F., ČERVENÝ, V., VÍTEK, D. Kybernetický bezpečnostní incident 3D: IT, právo a compliance. Praha: WoltersKluwer ČR, 2022

POLČÁK, R.; HARAŠTA, J.; STUPKA, V. Právní problémy kybernetické bezpečnosti. 1. vyd. Brno : Masarykova univerzita, Právnická fakulta, 2016. Spisy Právnické fakulty MU, řada teoretická, edice Scientia, sv. č. 576

POLČÁK, R., 2024. Právo informačních technologií. 2. vydání Praha: Wolters Kluwer. ISBN 978-80-286-0059-4.

Prehľad legislatívy:

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti

Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe

Zákon č. 367/2024 Z. z. o kritickej infraštruktúre

Zákon č. 300/2005 Z. z. Trestný zákon

Zákon č. 311/2001 Z. z. Zákonník práce

Zákon č. 40/1964 Zb. Občiansky zákonník

Zákon č. 513/1991 Zb. Obchodný zákonník

Vyhláška NBÚ SR č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

Vyhláška ÚPVII č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy

Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2)

Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti)

Smernica Európskeho parlamentu a Rady 2014/53/EÚ zo 16. apríla 2014 o harmonizácii právnych predpisov členských štátov týkajúcich sa sprístupňovania rádiových zariadení na trhu, ktorou sa zrušuje smernica 1999/5/ES

Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy

Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti)

Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora

Vykonávacie nariadenie Komisie (EÚ) 2024/2690 zo 17. októbra 2024, ktorým sa stanovujú pravidlá uplatňovania smernice (EÚ) 2022/2555, pokiaľ ide o technické a metodické požiadavky na opatrenia na riadenie kybernetických rizík a o bližšie určenie prípadov, v ktorých sa incident považuje za významný, vo vzťahu k poskytovateľom služieb DNS, správcom názvov TLD, poskytovateľom služieb cloud computingu, poskytovateľom služieb dátového centra, poskytovateľom sietí na sprístupňovanie obsahu, poskytovateľom riadených služieb, poskytovateľom riadených bezpečnostných služieb, poskytovateľom online trhov, internetových vyhľadávačov a platforiem služieb sociálnej siete a poskytovateľom dôveryhodných služieb

Ďalšie zdroje:

- European Union Agency For Cybersecurity (ENISA): European Cybersecurity Skills Framework Role Profiles, Septemeber 2022, dostupné [TU](#).