ZODPOVEDNOSTNÉ VZŤAHY V KYBERNETICKEJ BEZPEČNOSTI

MODUL 3 „Zodpovednosť v osobitných oblastiach"

Syllabus

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

Rozsah:
10 vyučovacích hodín. Vyučovacia hodina má 45 min. Modul sa delí na 2 časti s časovou dotáciu 5 vyučovacích hodín pre každú časť modulu.

Obsah a forma vzdelávania:
Modul 3 sa sústreďuje na zodpovednosť v špecifických oblastiach kybernetickej bezpečnosti, zahŕňajúc ITVS/ISVS, kritickú infraštruktúru, OT/ICS, finančný sektor, telekomunikácie, ochranu osobných údajov, umelú inteligenciu a ESG. Tento modul poskytuje náhľad do právnych a regulačných požiadaviek týkajúcich sa kybernetickej bezpečnosti vo vybraných sektoroch a súvisiacich prepojených oblastiach.

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, 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 dotáciu 5 vyučovacích hodín pre každú časť modulu.

Osnova:
Časť 1
- Právna regulácia a zodpovednosť v sektore ISVS (ITVS) a ich špecifiká (zákon o ITVS a vyhlášky). Postavenie a úlohy Vládnej jednotky CSIRT a povinnosti regulovaných subjektov.
- Právna regulácia a zodpovednosť v oblasti kritickej infraštruktúry a OT/ICS systémov (CRA nariadenie, smernica RED, Nariadenie o strojových zariadeniach)
- Sektorové špecifiká: energetika, doprava

Časť 2
- Kybernetická bezpečnosť a regulácia ochrany osobných údajov (GDPR, Smernica 2016/680, European Health Data Space nariadenie, Data Governance Act). Judikatúra Súdneho dvora EÚ.
- Kybernetická bezpečnosť vo finančnom sektore (nariadenie DORA a príslušné delegované a implementačné akty Komisie - ITS/RTS)
- AI Akt a zodpovednosť za bezpečné použitie systémov a modelov AI
- ESG a kybernetická bezpečnosť – vplyv regulácií na hodnotenie a vykazovanie rizík
- Príklady incidentov a právne dôsledky. Judikatúra Súdneho dvora EÚ.

Výsledky vzdelávania:
Po absolvovaní modulu účastníci dokážu:
- vysvetliť právny rámec a zodpovednosti subjektov v oblasti ISVS, kritickej infraštruktúry a kybernetickej bezpečnosti,
- identifikovať a interpretovať právne požiadavky podľa nariadení GDPR, DORA, AI Akt, Data Governance Act a CRA a ich vplyv na prevádzku IT systémov,
- posúdiť vplyv vybraných európskych nariadení na procesy riadenia rizík, incidentov, súladu bezpečnosti v organizácii,
- analyzovať právne následky kybernetických incidentov na základe judikatúry Súdneho dvora EÚ a príkladov z praxe.

IT manažér:
- porozumieť významu kybernetickej bezpečnosti pre chod organizácie v kontexte sektorovej regulácie kybernetickej bezpečnosti,
- identifikovať jednotlivé oblasti kybernetickej bezpečnosti podľa právnych požiadaviek a technických noriem (napr. STN ISO/IEC 27001:2023),
- porozumieť systému riadenia bezpečnosti informácií a informačných aktív a aplikovať ich prostredníctvom sektorových predpisov regulácie kybernetickej bezpečnosti,
- určiť zodpovednosti zamestnancov pri správe IKT služieb a bezpečnostnej politike,

- osvojiť si metódy a prístupy hodnotenia efektívnosti opatrení,
- zabezpečiť plnenie požiadaviek sektorovej regulácie kybernetickej bezpečnosti počas celého životného cyklu IKT systémov a ich komponentov,
- presadzovať a udržiavať politiky kybernetickej bezpečnosti v súlade s reguláciou kybernetickej bezpečnosti.

Informatik:
- doplniť odborné znalosti o sektorovej regulácie kybernetickej bezpečnosti a ich dopady na IKT a IT služby,
- pochopiť bezpečnostné požiadavky v súlade so zákonom o kybernetickej bezpečnosti,
- rozpoznať a reagovať na zraniteľnosti a hrozby v prostredí IKT služieb, vrátane požiadaviek na ich oznamovanie,
- efektívne komunikovať so špecialistami kybernetickej bezpečnosti, posudzovať návrhy opatrení a zapájať sa do riadenia rizík.

Zamestnanec v oblasti kybernetickej bezpečnosti:
- poznať právne a etické povinnosti podľa sektorovej regulácie kybernetickej bezpečnosti,
- porozumieť zraniteľnostiam, hrozbám a rizikám v oblasti informačnej bezpečnosti, vrátane koordinovaného oznamovania zraniteľností,
- navrhovať a prezentovať bezpečnostné politiky a stratégie v súlade s aktuálnou právnou úpravou,
- využívať metódy vyhodnocovania bezpečnosti a výsledky aplikovať v procesoch organizácie,
- spolupracovať s informatikmi a právnikmi pri návrhu opatrení podľa sektorových regulácii kybernetickej bezpečnosti.

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

MAKATURA, I.: Technická normalizácia v informačnej a kybernetickej bezpečnosti. In: Bezpečnosť v praxi [on-line]. Žilina: Poradca podnikateľa, 2024. ISSN 2729-885X. Dostupné TU.

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 vydaní 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

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)

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)

Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/868 z 30. mája 2022 o európskej správe údajov a o zmene nariadenia (EÚ) 2018/1724 (akt o správe údajov)

Nariadenie Európskeho parlamentu a Rady (EÚ) 2025/327 z 11. februára 2025 o európskom priestore pre zdravotné údaje a o zmene smernice 2011/24/EÚ a nariadenia (EÚ) 2024/2847

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

Delegované nariadenie Komisie (EÚ) 2024/1774 z 13. marca 2024, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa spresňujú nástroje, metódy, postupy a politiky riadenia IKT rizika a zjednodušený rámec riadenia IKT rizika

Delegované nariadenie Komisie (EÚ) 2024/1772 z 13. marca 2024, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa bližšie určujú klasifikačné kritériá incidentov súvisiacich s IKT a kybernetických hrozieb, stanovujú prahové hodnoty významnosti a spresňujú podrobnosti správ o závažných incidentoch

Delegované nariadenie Komisie (EÚ) 2024/1773 z 13.marca 2024, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, ktorými sa bližšie spresňuje podrobný obsah politiky v súvislosti so zmluvnými dojednaniami o využívaní IKT služieb podporujúcich kritické alebo dôležité funkcie a poskytovaných externými poskytovateľmi IKT služieb

Delegované nariadenie Komisie (EÚ) 2025/301 z 23. októbra 2024, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa stanovuje obsah a lehoty na počiatočné oznámenie, a priebežnú a záverečnú správu o závažných incidentoch súvisiacich s IKT a obsah dobrovoľného oznamovania v prípade významných kybernetických hrozieb

Vykonávacie nariadenie Komisie (EÚ) 2024/2956 z 29. novembra 2024, ktorým sa stanovujú vykonávacie technické predpisy na uplatňovanie nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o štandardné vzory registra informácií

Delegované nariadenie Komisie (EÚ) 2024/1502 z 22. februára 2024, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 spresnením kritérií na určenie externých poskytovateľov IKT služieb ako kritických pre finančné subjekty

Delegované nariadenie Komisie (EÚ) 2025/295 z 24. októbra 2024, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy týkajúce sa harmonizácie podmienok umožňujúcich vykonávanie činností dozoru

Delegované nariadenie Komisie (EÚ) 2024/1505 z 22. februára 2024, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 určením výšky poplatkov za dozor, ktoré má hlavný orgán dozoru účtovať kritickým externým poskytovateľom IKT služieb, a spôsobu úhrady uvedených poplatkov

Ďalšie zdroje:
European Union Agency For Cybersecurity (ENISA): Cyber Resilience Act implementation via EUCC and its applicable technical elements, Február 2025 dostupné TU.