ZODPOVEDNOSTNÉ VZŤAHY V KYBERNETICKEJ BEZPEČNOSTI

MODUL 2 „Zodpovednosť regulovaných subjektov“

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 2 sa zaoberá zodpovednosťou regulovaných subjektov v oblasti kybernetickej bezpečnosti, vrátane implementácie bezpečnostných opatrení a riadenia zmluvných vzťahov v rámci dodávateľského reťazca. Taktiež pokrýva postupy pri bezpečnostných incidentoch, riadenie a oznamovanie zraniteľností, a analyzuje súkromnoprávnu a verejnoprávnu zodpovednosť, ako aj možnosti poistenia kybernetických rizík.

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 dotáciu 5 vyučovacích hodín pre každú časť modulu.

Osnova:

Časť 1

- Vzťah medzi technickými normami a reguláciou (vrátane harmonizovaných európskych noriem), činnosť normalizačných orgánov a judikatúra
- Certifikácia bezpečnosti IKT produktov a služieb (Akt o kybernetickej bezpečnosti)
- Prehľad európskej a slovenskej legislatívy v oblasti kybernetickej bezpečnosti a ich súvislosti (smernica NIS2, Zákon o kybernetickej bezpečnosti, smernica CER, Nariadenie DORA, Nariadenie CSA, Nariadenie CRA, AI Akt a ďalšie). Predstavenie návrhov nových európskych právnych predpisov ako Digital Omnibus, revízia Nariadenia CSA (CSA2), a revízia smernice NIS2.
- Právne povinnosti regulovaných subjektov podľa zákona č. 69/2018 Z. z. po transpozícii smernice NIS2. Osobitnosti slovenskej transpozície a zmena koncepcie regulácie. Vecná a osobná pôsobnosť zákona. Vykonávacie predpisy. Sektorové právne prepisy.
- Právne aspekty analýzy rizík a prijímanie bezpečnostných opatrení. Vyhláška o bezpečnostných opatreniach a Vykonávacie nariadenie Komisie č. 2024/2690. Porovnanie s technickou normou STN ISO/IEC 27001:2023. Sektorové bezpečnostné štandardy.

Časť 2

- Zodpovednosť v dodávateľskom reťazci a riadenie bezpečnosti tretích strán. Právne vzťahy medzi prevádzkovateľom a dodávateľom IKT služieb a produktov
- Riešenie kybernetických bezpečnostných incidentov a iných bezpečnostných udalostí a ich vzťah s ďalšími reguláciami (nariadenia GDPR, CRA, AI Akt)
- Zodpovednosť za zraniteľnosti a ich oznamovanie. Koncept koordinovaného oznamovania zraniteľností (aj v kontexte nariadenia CRA)
- Postavenie a úlohy národnej jednotky CSIRT (SK-CERT) a povinnosti regulovaných subjektov
- Audit a samohodnotenie
- Dohľad a právomoci Národného bezpečnostného úradu
- Zodpovednosť v zmluvných a mimozmluvných právnych vzťahoch
- Poistenie kybernetických rizík

Výsledky vzdelávania:

Po absolvovaní modulu účastníci dokážu:

- vysvetliť základnú štruktúru a vzťahy medzi kľúčovými európskymi a slovenskými právnymi predpismi v oblasti kybernetickej bezpečnosti;
- identifikovať právne povinnosti subjektov regulovaných podľa zákona o kybernetickej bezpečnosti vrátane požiadaviek na bezpečnostné opatrenia, analýzu rizík, riadenie incidentov a oznamovanie zraniteľností;
- rozlíšiť a aplikovať právne pravidlá týkajúce sa spolupráce s dodávateľmi IKT produktov a služieb, vrátane zodpovednosti v dodávateľskom reťazci a požiadaviek na zmluvné vzťahy v kontexte riadenia tretích strán;
- porozumieť úlohy orgánov ako NBÚ, SK-CERT, možnosti auditu a samohodnotenia v systéme dohľadu a určiť postupy pri kontrole plnenia povinností;

IT manažér:

- porozumieť významu kybernetickej bezpečnosti pre chod organizácie v kontexte 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 a vyhlášky NBÚ o bezpečnostných opatreniach,
- určiť zodpovednosti zamestnancov pri správe IKT služieb a bezpečnostnej politike,
- osvojiť si metódy a prístupy hodnotenia efektívnosti opatrení, vrátane samohodnotenia a auditu,
- zabezpečiť plnenie požiadaviek 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 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 zákona o kybernetickej bezpečnosti,
- porozumieť zraniteľnostiam, hrozbám a rizikám v oblasti informačnej bezpečnosti, vrátane koordinovaného oznamovania zraniteľností podľa zákona o kybernetickej bezpečnosti,
- 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 zákona o 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.: Terminologické zmeny v novele zákona o kybernetickej bezpečnosti. Dostupné TU.
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

PAČKA, R.: CSIRT: v přední linii boje proti kybernetickým hrozbám. Brno: Centrum pro studium demokracie a kultury, o.p.s. (CDK): Masarykova Univerzita, 2019.

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. 227/2025 Z.z. o bezpečnostných opatreniach

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)

Smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES

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

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): Developing National Vulnerabilities Programmes, Február 2023 dostupné TU.