ISSN 1339-3189 1/2023

Mladá veda

Young Science

www.mladaveda.sk

Mladá veda
Young Science

MEDZINÁRODNÝ VEDECKÝ ČASOPIS MLADÁ VEDA / YOUNG SCIENCE

Číslo 1, ročník 11., vydané v marci 2023
ISSN 1339-3189
Kontakt: info@mladaveda.sk, tel.: +421 908 546 716, www.mladaveda.sk
Fotografia na obálke: Prichádza jar. © Branislav A. Švorc, foto.branisko.at

VYDAVATEĽ
Vydavateľstvo UNIVERSUM, spol. s r. o.
www.universum-eu.sk
Javorinská 26, 080 01 Prešov
Slovenská republika

Mladá veda
Young Science
ISSN 1339-3189

Vol. 11 (1), pp. 229-236

ELEMENTY INFORMAČNEJ A KYBERNETICKEJ BEZPEČNOSTI V REGIONÁLNEJ SAMOSPRÁVE

ELEMENTS OF INFORMATION AND CYBER SECURITY IN REGIONAL SELF-GOVERNMENT

Jana Béreš Furmanová [1]

Autorka pôsobí ako interný doktorand na Vysokej škole bezpečnostného manažérstva v Košiciach. Vo svojej dizertačnej práci sa venuje problematike novodobej bezpečnosti a ochrane procesov v regionálnej samospráve.

The author works as an internal doctoral student at the University of Security Management in Košice. In his dissertation, he deals with the issue of new-age security and protection of processes in regional self-government.

Abstract
The article is interested in describing the basic legislative procedures for the creation of effective protection of the level of public administration - a self-governing region against incidents of the current modern infrastructure in the field of information and cyber systems. Among the most important steps in the preparation and implementation of an appropriate security directive and the introduction of measures in information and cyber security are the role and position of the cyber security manager, the advisory body - the security committee of the self-governing region, as well as the significant importance of the audit of critical threats and rules in the field of information and cyber security. The creation of suitable security rules is increasingly coming to the fore even in relatively non-progressive public administration, compared to the private sector and large ICT corporations, which are advancing at a breakneck pace when it comes to cyber security.
Key words: cyber security, security manager, security comitee, audit of cyber security, self-government, region

Abstrakt
Článok má záujem popísať základné legislatívne postupy na vytvorenie efektívnej ochrany úrovne verejnej správy – samosprávneho kraja pred incidentmi súčasnej modernej infraštruktúry v oblasti informačných a kybernetických systémov. Medzi najdôležitejšie kroky pri príprave a realizácii vhodnej bezpečnostnej smernice a zavádzaní opatrení v

[1] Adresa pracoviska: JUDr. Ing. Jana Béreš Furmanová, MBA, LL.M, Vysoká škola bezpečnostného manažmentu, Košťova 1, 040 01 Košice
E-mail: furmanovajana@gmail.com

informačnej a kybernetickej bezpečnosti patrí úloha a postavenie manažéra kybernetickej bezpečnosti, poradného orgánu - bezpečnostného výboru samosprávneho kraja, ako aj výrazná dôležitosť auditu kritických hrozieb a pravidiel v oblasti informačnej a kybernetickej bezpečnosti. Kreovanie vhodných bezpečnostných pravidiel sa dostáva čoraz viac do popredia už aj v relatívne neprogresívnej verejnej správe, a to v porovnaní s privátnym sektorom a veľkými IKT korporáciami, ktoré v otázke kybernetickej bezpečnosti napredujú míľovým tempom.
Kľúčové slová: kybernetická bezpečnosť, bezpečnostný manažér, bezpečnostný výbor, audit kybernetickej bezpečnosti, samospráva, samosprávny kraj

Úvod

Nevyhnutnosť zavádzania novodobých elementov kybernetickej bezpečnosti sa čoraz viac prejavuje aj v zložkách verejnej správy, obzvlášť v regionálnom (župnom) zriadení, pri narastajúcich hrozbách kybernetických incidentov. Článok si kladie za úlohu navrhnúť optimálne technické, organizačné a personálne opatrenia, ktorých implementáciou krajská samospráva bude deklarovať cieľ, dosiahnuť súlad s legislatívnymi požiadavkami vyplývajúcimi z príslušnej legislatívy o kybernetickej bezpečnosti minimálne na úrovni 80%. Zároveň článok navedie možnosti priblíženia sa z pohľadu kybernetickej bezpečnosti vo verejnej správe k operačnému programu integrovaná infraštruktúra, v prioritnej osi 7 – Informačná spoločnosť, so zameraním na „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS“ a v neposlednom rade aj plnenie požiadaviek Národného bezpečnostného úradu v aktuálnej situácii prebiehajúceho konfliktu na Ukrajine.

V nasledujúcich riadkoch popíšme základné legislatívne postupy na vytvorenie efektívnej ochrany úrovne verejnej správy – samosprávneho kraja pred incidentmi súčasnej modernej infraštruktúry v oblasti informačných a kybernetických systémov. Medzi najdôležitejšie kroky pri príprave a realizácii vhodnej bezpečnostnej smernice a zavádzaní opatrení v informačnej a kybernetickej bezpečnosti patrí úloha a postavenie manažéra kybernetickej bezpečnosti, poradného orgánu - bezpečnostného výboru samosprávneho kraja, ako aj výrazná dôležitosť auditu kritických hrozieb a pravidiel v oblasti informačnej a kybernetickej bezpečnosti. Kreovanie vhodných bezpečnostných pravidiel sa dostáva čoraz viac do popredia už aj v relatívne neprogresívnej verejnej správe, a to v porovnaní s privátnym sektorom a veľkými IKT korporáciami, ktoré v otázke kybernetickej bezpečnosti napredujú míľovým tempom.

Manažér kybernetickej bezpečnosti samosprávneho kraja

Manažér kybernetickej bezpečnosti je v samosprávnom kraji riadiaca pracovná pozícia, pre ktorú sa často uvádza aj skratka „CISO“ (z anglického „Chief Information Security Officer“). Má mať možnosť komunikovať a predkladať návrhy a oznamovať informácie v oblasti kybernetickej bezpečnosti priamo štatutárnemu orgánu samosprávneho orgánu. Manažér kybernetickej bezpečnosti nesmie byť „hlboko utopený“ v štruktúre organizácie. V komplikovaných a rozsiahlych organizačných štruktúrach akou je aj štruktúra samosprávneho kraja (respektíve jeho úradu) je však akceptovateľné, ak sa právomoc priameho prístupu ku štatutárnemu orgánu upraví procesne, napríklad interným predpisom. Postavenie manažéra

kybernetickej bezpečnosti musí byť nezávislé od útvaru zaisťujúceho prevádzku informačných a komunikačných technológií. Úlohou manažéra kybernetickej bezpečnosti je najmä zaistiť odolnosť organizácie voči kybernetickým bezpečnostným hrozbám, riadiť súvisiace riziká a riešiť bezpečnostné incidenty. Manažér kybernetickej bezpečnosti je často „bezpečnostnou protiváhou“ útvarom vývoja a prevádzky informačných a komunikačných technológií. Výrazne sa podieľa na ochrane aktív samosprávneho kraja, niekedy dokonca musí rozhodnúť o zastavení rizikovej činnosti kraja, samozrejme, v závislostí od jeho kompetencií. Ak by manažér kybernetickej bezpečnosti bol závislý od prevádzky a vývoja technologických služieb, existuje riziko, že rozhodnutia v oblasti kybernetickej bezpečnosti budú aj v krízových situáciách ovplyvnené najmä cieľmi útvarov zodpovedných za informačné a komunikačné technológie a prevádzku samosprávneho kraja. Ďalšie úlohy manažéra kybernetickej bezpečnosti samosprávneho kraja sú v oblasti riadenia bezpečnosti. K strategickému riadeniu informačnej a kybernetickej bezpečnosti kraja patrí najmä vypracovanie a prezentácia bezpečnostnej stratégie a koncepcie, implementácia procesov informačnej a kybernetickej bezpečnosti podľa všeobecne záväzných právnych predpisov a ostatných interných riadiacich aktov, taktiež zabezpečenie vypracovania, udržiavania a aktualizácie bezpečnostnej dokumentácie informačnej a kybernetickej bezpečnosti či návrh požiadaviek na rozpočet a na iné zdroje súvisiace s financovaním bezpečnostných opatrení a procesov. Dôležité je aj personálne hľadisko - metodické usmerňovanie správcov a gestorov informačných a komunikačných technológií, vlastníkov procesov, vlastníkov aktív, vedúcich zamestnancov a ďalších zodpovedných zamestnancov vo vzťahu k dosahovaniu bezpečnostných cieľov samosprávneho kraja, poskytovanie informácií bezpečnostnému výboru aj štatutárnemu orgánu o stave informačnej a kybernetickej bezpečnosti alebo o závažných bezpečnostných rizikách, incidentoch a významných bezpečnostných udalostiach. V oblasti manažmentu hrozieb a rizík patria k úlohám manažéra kybernetickej bezpečnosti najmä identifikácia, analýza a monitoring bezpečnostných hrozieb a rizík, návrh opatrení na zamedzenie dopadov bezpečnostných udalostí, zabezpečenie hodnotenia technickej zraniteľnosti systémov, detekcia, evidencia a prevencia kybernetických incidentov, prípadne spracovanie funkčného plánu kontinuity a obnovy činností kraja (tzv. Business Continuity Management), vrátane plánovania obnovy systémov po havárii (tzv. Disaster Recovery Planning).

V oblasti aplikácie bezpečnostných opatrení bezpečnostný manažér riadi najmä spracovanie návrhov, ich implementáciu, zmeny a optimalizáciu bezpečnostných riešení s víziou ich bezproblémového prevádzkovania, ďalej riadenie bezpečnostnej architektúry a predkladanie odborných stanovísk k novým zmenám v IT infraštruktúre, ktoré môžu mať potenciálny vplyv na bezpečnosť informačných aktív samosprávneho kraja. Tento manažér ma za úlohu viesť tím zamestnancov útvaru informačnej a kybernetickej bezpečnosti, ak je takýto organizačný útvar zriadený. K parciálnym úlohám tiež patrí aj zabezpečenie udržateľnosti organizačných opatrení vrátane vyspelosti bezpečnostných procesov, zaistenie uplatňovania princípu oddelenia právomocí a zodpovedností v celej organizačnej štruktúre kraja tak, aby rovnaká osoba nebola zodpovedná za vykonávanie a zároveň aj schvaľovanie alebo kontrolu bezpečnostne relevantných aktivít a činností. V oblasti riadenia súladu zohráva úlohu v procesoch zaručenia súladu (tzv. Compliance Management) v oblasti informačnej a

kybernetickej bezpečnosti, zabezpečení pravidelného preskúmavania stavu kybernetickej a informačnej bezpečnosti, vyhodnocovaní plnenia vnútorných predpisov súvisiacich s riadením kybernetickej bezpečnosti, poskytovaní súčinnosti internému a externému auditu informačnej a kybernetickej bezpečnosti, navrhovanie metrík a kľúčových indikátorov pre sledovanie vývoja a stavu bezpečnosti a vývoja bezpečnostných rizík, zabezpečovanie školení zamestnancov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti, zabezpečovanie kontinuálneho vzdelávania pre pracovné roly relevantné z hľadiska kybernetickej bezpečnosti, zabezpečovanie budovania bezpečnostného povedomia pre oblasť informačnej a kybernetickej bezpečnosti a ochrany osobných údajov a spolupráca s orgánmi verejnej moci a orgánmi činnými v trestnom konaní.

Výbor pre bezpečnosť v samosprávnom kraji

V zmysle vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu (2020), ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy je potreba zriadenia bezpečnostného výboru samosprávneho kraja pre oblasť informačnej a kybernetickej bezpečnosti ako svoj stály poradný orgán na zabezpečenie odborného riadenia v oblasti informačnej a kybernetickej bezpečnosti, ktorý zriadi predseda samosprávneho kraja. Výbor je poradným orgánom predsedu samosprávneho kraja pre oblasť informačnej a kybernetickej bezpečnosti najmä vo vzťahu k plneniu legislatívnych požiadaviek definovaných zákonom o kybernetickej bezpečnosti, zákonom o ochrane osobných údajov, ako aj vo vzťahu k požiadavkám normy STN ISO/IEC 27001 - systému riadenia informačnej bezpečnosti.

Výbor je potrebné definovať v spracovanom dokumente, ktorý upraví postavenie, pôsobnosť, zloženie a úlohy bezpečnostného výboru samosprávneho kraja. Bezpečnostný výbor samosprávneho kraja má plniť najmä úlohy inicializované manažérom kybernetickej bezpečnosti, posudzovať primeranosť technických, organizačných a personálnych opatrení formulovaných manažérom kybernetickej bezpečnosti, overovať návrhy na revíziu bezpečnostnej politiky a nadväzných bezpečnostných smerníc samosprávneho kraja. Výbor posudzuje tiež vplyvy na ochranu údajov, ako aj ďalšie dokumenty týkajúce sa informačnej a kybernetickej bezpečnosti, ochrany osobných údajov a zabezpečenia súladu s požiadavkami Nariadenia Európskeho parlamentu a Rady EÚ (2016), ale aj zákona o informačných technológiách vo verejnej správe (2019), vyhlášok Národného bezpečnostného úradu (2018, 2019), alebo vyhlášok Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu (2020, 2020)

Na základe prijatého uznesenia z rokovania bezpečnostný výbor predkladá predsedovi samosprávneho kraja na schválenie návrh zodpovednosti za implementáciu a uplatňovanie jednotlivých opatrení a postupov kybernetickej bezpečnosti a informačnej bezpečnosti v podmienkach samosprávneho kraja. Zároveň výbor samosprávneho kraja poskytuje podporu manažérovi kybernetickej bezpečnosti pri koordinácii a metodickom riadení plnenia stanovených opatrení a požiadaviek v oblasti informačnej a kybernetickej bezpečnosti vyplývajúcich z bezpečnostnej politiky, legislatívy a smerníc v podmienkach kraja. Pripomienkuje opatrenia a postupy navrhnuté manažérom kybernetickej bezpečnosti na zvýšenie a udržanie primeranej informačnej bezpečnosti a zabezpečenie súladu s

bezpečnostnou legislatívou najmä pri zásadných zmenách v informačnom systéme, ktoré predkladá predsedovi. Výbor koordinuje a prerokúva procesy, roly, stratégie a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov. Prerokúva aktivity súvisiace s informačnou bezpečnosťou, podozrivé udalosti a navrhuje odporúčania pre predsedu k prípadným kybernetickým a bezpečnostným incidentom. Metodicky výbor usmerňuje aktualizáciu a dopracovanie internej dokumentácie pre riadenie informačnej a kybernetickej bezpečnosti, navrhuje a prerokúva súvisiace dokumenty a odporúčania ako aj smernice pri ochrane osobných údajov, taktiež prijíma postupy navrhnuté manažérom kybernetickej bezpečnosti na budovanie bezpečnostného povedomia a osvety zamestnancov úradu kraja.

Bezpečnostný výbor samosprávneho kraja je spravidla zložený zo stálych členov - zamestnancov samosprávneho kraja vyplývajúcich z ich pracovnej pozície. Na čele je predseda výboru a na jeho zasadnutiach sa môžu zúčastniť aj ďalšie osoby prizvané predsedom. Prizvané osoby majú však len poradný charakter a nemajú hlasovacie právo. Zasadania výboru sú neverejné.

Audit kybernetickej bezpečnosti v samosprávnom kraji

Za audit kybernetickej bezpečnosti považujeme metódu získavania dôkazov o stave bezpečnosti v samosprávnom kraji. Úlohou tohto auditu je posúdiť zhodu prijatých bezpečnostných opatrení s požiadavkami podľa zákona o kybernetickej bezpečnosti (2018). Auditom sa určuje efektívnosť implementovaných opatrení a spôsob ich prevádzkovania ako aj vykonávania v prostredí samosprávneho kraja. Na základe toho je možné prijímať opatrenia na odstránenie neodhalených rizík a nápravu a predchádzať tak riziku kybernetických bezpečnostných incidentov. Výsledkom auditu je záverečná správa o výsledkoch auditu kybernetickej bezpečnosti samosprávneho kraja. Po vypracovaní záverečnej správy o výsledkoch auditu kybernetickej bezpečnosti, ktorá sa predkladá Národnému bezpečnostnému úradu. Navrhované opatrenia vyplývajúce z tejto správy možno podľa ich charakteru deliť na technické, organizačné a personálne. Ich implementáciou samosprávny kraj bude deklarovať cieľ, a to dosiahnutie súladu s legislatívnymi požiadavkami minimálne na úrovni 80% v horizonte do dvoch rokov od posledného auditu. Aktívna účasť manažmentu samosprávneho kraja je nevyhnutným predpokladom k úspešnej implementácii opatrení, a to najmä pri schvaľovaní zdrojov potrebných k realizácii opatrení a pri zabezpečení potrebnej podpory pre bezpečnostné opatrenia. Tento procesný postup je zároveň transpozíciou smernice Európskeho parlamentu a Rady EÚ (2016) o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v EÚ.

Opatrenia môžu pomôcť preventívne predchádzať hrozbám pre samosprávny kraj, znížiť jeho známe zraniteľnosti, chrániť jeho systém pred kybernetickými hrozbami aj v prípade, že sa hrozba už uplatnila a jej následkom bola škodlivá udalosť. Úlohou aplikovaných preventívnych bezpečnostných opatrení je takéto udalosti včas odhaliť a obmedziť ich negatívny vplyv. Cieľom následných reaktívnych opatrení je aj zaručenie odškodnenia strát vyvolaných škodlivou udalosťou alebo získať dôkazné prostriedky pre pokračovanie v právnom konaní smerujúcom k potrestaniu páchateľov, vymoženiu škody

alebo vyvodenie zodpovednosti v rámci pracovnoprávneho vzťahu. Dosiahnuté bezpečnostné ciele umožňujú získať záruku, že komponenty informačnej architektúry môžu byť považované za dôveryhodné a spoľahlivé. Spoľahlivosť informácie je determinovaná tromi jej základnými bezpečnostnými atribútmi: dôvernosťou, dostupnosťou a integritou. Z toho vyplýva, že opatrenia zaručujúce bezpečnosť a spoľahlivosť komponentov informačnej architektúry by mali smerovať najmä k zabezpečeniu dôvernosti, dostupnosti a integrity. Bezpečnostná architektúra je medziodborová problematika, ktorá sa tiahne naprieč celou podnikovou architektúrou. Možno ju opísať ako ucelený súbor pohľadov a artefaktov informačnej a kybernetickej bezpečnosti, ochrany súkromia a operačného rizika vrátane bezpečnostných cieľov a bezpečnostných služieb. Zákon o kybernetickej bezpečnosti (2018) aj po svojej novelizácii naďalej zachováva princíp technickej neutrality. Je teda výhradne na rozhodnutí vedenia samosprávneho kraja, aký rozsah bezpečnostných opatrení sa rozhodne implementovať vo svojom prostredí. Podstatou neskoršieho posúdenia zo strany audítora je efektivita bezpečnostných opatrení, teda v konečnom dôsledku posudzovanie úrovne dosiahnutých spôsobilostí, teda úloh, procesov, rolí a technológií v organizačnej, personálnej i technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov. Vyhláška Národného bezpečnostného úradu (2018) chápe bezpečnostné opatrenia sú buď všeobecné, ustanovujúce obsah bezpečnostných opatrení a štruktúru bezpečnostnej dokumentácie, alebo sektorové, ktoré sa realizujú na základe určitých špecifík kategorizácie sietí a informačných systémov. Dôvodom ich existencie a účinkom všeobecne záväzných nariadení je úmysel zákonodarcu riešiť reálne špecifiká niektorých odvetví, napríklad energetiky, leteckej dopravy, zdravotníctva, alebo priemyselnej výroby. Problémom z úrovne samosprávneho kraja je skutočnosť, že príslušná vyhláška Úradu podpredsedu vlády pre investície a informatizáciu (2020) efektívne nedefinuje žiadne špecifiká sektoru verejnej správy a teda v porovnaní s vyhláškou NBÚ neprináša žiadne požiadavky na bezpečnostné opatrenia navyše.

Záver

Obdobie posledných rokov prináša svedectvo zintenzívňujúcich sa informačných a kybernetických útokov aj vo fungovaní regionálnej samosprávy. Aktuálne je kritická enormná zraniteľnosť systémov v samosprávach, ktorá je označovaná aj kódmi ako napríklad CVE-2022-42856 a takáto zraniteľnosť je aktívne zneužívaná útočníkmi. Zraniteľnosť sa udáva v takzvaných číselných vyjadreniach „CVSS skóre“, pričom najvyššie z nich v prípade viacerých zraniteľností dosahuje hodnotu 9,8 z 10 číselných bodov. Pre ilustráciu je v takejto kritickej zraniteľnosti aj operačný systém Apple iOS vo verzii staršej ako 12.5.7. V prípade zistenia kybernetického bezpečnostného incidentu v samospráve je potrebné útok bezodkladne nahlásiť Národnému centru kybernetickej bezpečnosti „SK-CERT“ (incident@nbu.gov.sk). V súčasnosti Národný bezpečnostný úrad čoasto vyhlasuje varovania pred zvýšeným rizikom kybernetických bezpečnostných incidentov prorusky orientovaných komunitných hackerských skupín na slovenské ciele vo vzťahu k zabezpečeniu sietí a informačných systémov verejnej správy vrátane prvkov kritickej infraštruktúry a iných organizácií. NBÚ vydáva takéto varovania najmä na základe informácií, ktoré získal vlastnou činnosťou a spoluprácou s ďalšími bezpečnostnými zložkami štátu. Na ochranu pred útokmi

sa organizáciám bezodkladne odporúča mať vytvorené záložné lokality systémov a služieb, respektíve ich redundanciu, do internetu publikovať statické webové stránky, ideálne v externej hostingovej spoločnosti (redakčný systém, inštalovaný vo vnútornej sieti neprístupnej z internetu, vygeneruje HTML súbory, obrázky a štýly, ktoré sú následne prenesené na hostingovú službu), striktne oddeliť citlivé údaje a prevádzkovo kritické aktíva od verejných webových stránok, implementovať bezpečnostnú infraštruktúru schopnú filtrovať IP adresy útočníka vo veľkom objeme s možnosťami nastavenia "geofencingu" – obmedzenie krajín, z ktorých sú umožnené prichádzajúce spojenia, nastavenia firewallových pravidiel a povolenie len vybraných IP adries a podobne. Je zároveň potrebné vynucovať viacfaktorovú autentifikáciu a na vzdialený prístup používať VPN, zakázať všetky porty a protokoly, ktoré nie sú potrebné na prevádzku sietí, systémov a služieb, zmapovať všetky verejné služby samosprávneho kraja, vystavených do internetu a následne úplné vypnúť nepotrebné a nepoužívané systémy, aktualizovať zastarané systémy, odstrániť staré účty a nakonfigurovať mailový server tak, aby sa škodlivé a podozrivé maily nedostali do schránok používateľov či zamestnancov. Politiku hesiel aktualizovať tak, aby zakazovala používať rovnaké heslá na rôzne služby a aby vynucovala používanie silných hesiel alebo heslových fráz. Odporúča sa vyhnúť SMS overovaniu a sociálnemu inžinierstvu (fyzické tokeny). Cloudové služby nie je možné využívať ako úložisko kritických informačných aktív, napríklad obchodného tajomstva, osobných údajov, plánov infraštruktúry, klasifikovaných informácií a podobne. Je tiež dôležité, aby každý zamestnanec vedel, koho kontaktovať v prípade podozrenia na informačný a kybernetický incident a rovnako 24/7 dostupnosť kľúčového personálu kraja v oblasti prevádzky a riadenia kybernetickej bezpečnosti. Aj v organizačnej platforme samosprávneho kraja platí potreba poučiť svojich zamestnancov o rizikách kybernetických bezpečnostných incidentov a informovať ich o zvýšenom riziku útokov. Vzdelávacie aktivity je potrebné robiť adresne, podľa rolí a zodpovedností jednotlivých zamestnancov - bežní používatelia (princípy sociálneho inžinierstva), administrátori (pravidlá bezpečnej infraštruktúry), kyberbezpečnostní špecialisti (špecializované bezpečnostné vzdelávanie).

Tento článok odporúčal na publikovanie vo vedeckom časopise Mladá veda:
Dr.h.c. prof. Ing. Vladimír Klimo, CSc.

Použitá literatúra

1. NARIADENIE Európskeho parlamentu a Rady EÚ č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov
2. VYHLÁŠKA č. 436/2019 Z. z. Národného bezpečnostného úradu o audite kybernetickej bezpečnosti a znalostnom štandarde audítora
3. VYHLÁŠKA č. 362/2018 Z. z. Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
4. VYHLÁŠKA č. 179/2020 Z. z. Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy
5. VYHLÁŠKA č. 78/2020 Z. z. Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu o štandardoch pre informačné systémy verejnej správy

6. VYHLÁŠKA č. 85/2020 Z. z. Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu o riadení projektov
7. ZÁKON č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
8. ZÁKON č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
9. ZÁKON č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov

Mladá veda

Young Science

ISSN 1339-3189