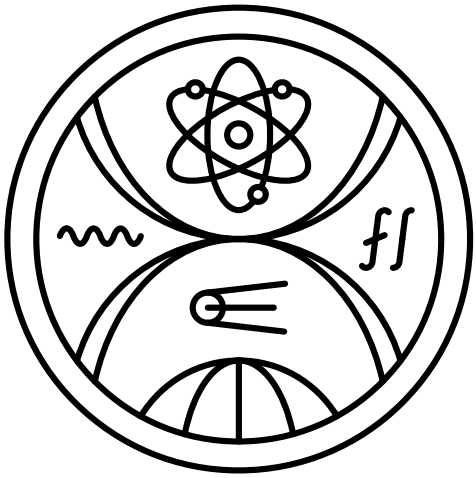
Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

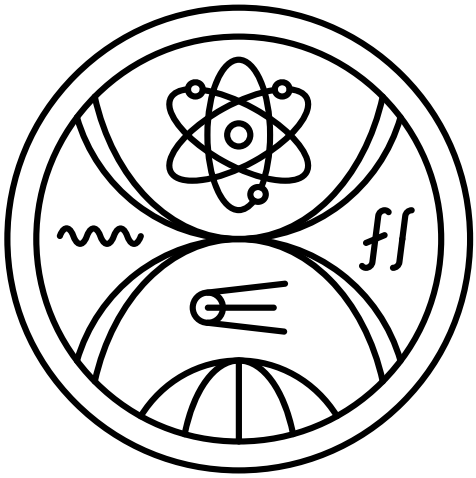


Analýza rizík

Diplomová práca

2026
Anton Kica

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky



Analýza rizík

Diplomová práca

Študijný program:	Informatika
Študijný odbor:	Informatika
Školiace pracovisko:	Katedra informatiky
Školiteľ:	doc. RNDr. Daniel Olejár, PhD.

Bratislava, 2026
Anton Kica

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Bc. Anton Kica
Študijný program: informatika (Jednoodborové štúdium, magisterský II. st., denná forma)
Študijný odbor: informatika
Typ záverečnej práce: diplomová
Jazyk záverečnej práce: slovenský
Sekundárny jazyk: anglický

Názov: Podporný systém pre analýzu rizík
Auxiliary system for risk analysis

Anotácia: Vlastníci (správcovia) informačných systémov verejnej správy (ISVS) sú podľa zákona č. 95/2019 Z.z. povinní vypracovať bezpečnostný projekt na ISVS. Základom bezpečnostného projektu je analýza rizík. Táto povinnosť sa v SR týka niekoľko tisíc subjektov. Na Slovensku je však nedostatok odborníkov na kybernetickú a informačnú bezpečnosť (KIB), ktorí by bezpečnostné projekty vypracovali.
Riešením by mohol byť interaktívny expertný systém. Vytvorenie plnohodnotného expertného systému je však úloha pre profesionálny tím. Cieľom diplomovej práce je preto návrh a čiastočná implementácia jednoduchého modulárneho systému na analýzu rizík pre ISVS tretej (najnižšej) kategórie a návrh projektu na dopracovanie plnohodnotného systému.
Diplomant
• Naštuduje releventnú legislatívu a identifikuje povinnosti správcu ISVS a zákonné požiadavky na bezpečnostný projekt,
• Naštuduje metodiky analýzy rizík podľa noriem ISO/IEC 27005 a BSI štandardu 200-3.
• Navrhne modulárny interaktívny system, ktorý
o Používateľa oboznámi s jeho zákonnými povinnosťami,
o Vysvetlí mu postup pri analýze rizík,
o Pre vybrané aktíva mu pomôže vykonať analýzu rizík a navrhnúť opatrenia*),
o Pomôže mu vytvoriť dokumentáciu vykonanej analýzy rizík.
Výstupom diplomovej práce bude
• Analytická časť (zákonné povinnosti)
• Návrh metodiky analýzy rizík
• Popis systému (technická špecifikácia, data, požiadavky na budúce moduly, …)
• Používateľská dokumentácia
• samotný system
• návrh postupu a odhad zdrojov potrebných na vytvorenie plnohodnotného systému.

*) modularita systému spočíva v uniformnom prístupe k analýze rizík pre jednotlivé aktíva, čo umožňuje pridávať do systému ďalšie aktíva (a ich analýzu rizík)

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

Cieľ:
• Navrhne modulárny interaktívny system, ktorý
o Používateľa oboznámi s jeho zákonnými povinnosťami,
o Vysvetlí mu postup pri analýze rizík,
o Pre vybrané aktíva mu pomôže vykonať analýzu rizík a navrhnúť opatrenia*),
o Pomôže mu vytvoriť dokumentáciu vykonanej analýzy rizík.

Literatúra:
1. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ZoKB)
2. Vyhláška Národného bezpečnostného úradu, č. 362/2018 Z.z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
3. Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
4. Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z.,
5. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy
6. ISO/IEC 27001 — Information security management systems — Requirements.
7. ISO/IEC 27002 — Code of practice for information security management.
8. ISO/IEC 27005 — Information security, cybersecurity and privacy protection — Guidance on managing information security risks
9. BSI Standard 200-1 Information Security Management Systems (ISMS)
10. BSI Standard 200-2 IT Grundschutz Methodology,
11. IT-Grundschutz Compendium, BSI 2019
12. BSI Standard 200-3 Risk Analysis based on IT-Grundschutz
13. BSI Standard 100-4 Business Continuity Management

Kľúčové slová: analýza rizík

Vedúci: doc. RNDr. Daniel Olejár, PhD.
Katedra: FMFI.KI - Katedra informatiky
Vedúci katedry: prof. RNDr. Martin Škoviera, PhD.

Spôsob sprístupnenia elektronickej verzie práce:
prípustná pre vlastnú VŠ

Dátum zadania: 16.12.2024

Dátum schválenia: 07.02.2025 prof. RNDr. Rastislav Kráľovič, PhD.
garant študijného programu

.....
študent

.....
vedúci práce

Poďakovanie: You can thank anyone who helped you with the thesis here (e.g. your supervisor).

Abstrakt

Slovenský abstrakt v rozsahu 100–500 slov, jeden odstavec. Abstrakt stručne sumarizuje výsledky práce. Mal by byť pochopiteľný pre bežného informatika. Nemal by teda využívať skratky, termíny alebo označenie zavedené v práci, okrem tých, ktoré sú všeobecne známe.

Kľúčové slová: Slovak, keywords, here

Abstract

Abstract in the English language (translation of the abstract in the Slovak language).

Keywords: English, keywords, here

Obsah

Zoznam obrázkov

Úvod

0.1 Motivácia

V poslednej dobe sa do popredia svetových a regionálnych udalostí dostali mnohé kybernetické útoky. Prakticky hneď začiatkom roka 2025 sa Slovensko stalo cieľom tzv. kybernetického útoku, kedy hackerská skupina zaútočila na informačné systémy Úradu geodézie, kartografie a katastra SR (ÚGKK)[1][1]. Tento útok vyradil štátnu elektronickú službu katastra, pričom hackeri zašifrovali ostré (produkčné) dáta a údajne si pýtali výkupné v hodnote niekoľkých miliónov dolárov[2].

TODO Info z 2023 o audite katastra..?

Pár dni po útoku zverejnil jeden užívateľ na socialnej sieti LinkedIn príspevok[3], v ktorom vykonal „*post portem* analýzu perimetra Katastra z verejných zdrojov“ pomocou nástroja Shodan. V tejto analýze autor identifikoval mnohé zraniteľnosti informačného systému — zastarané verzie protokolu TLS (verzie 1.1 a 1.2), zastarané verzie PHP a Apache Server (z rokov 2009 a 2010), otvorené porty (123 — NTP a 161 — SNMP)[2] alebo 230 softvérový zraniteľností[3]. V jednoduchosti, mimo iných problémov, bolo zanedbané patchovanie služieb a systémov, čo vytváralo potenciálny uhol útoku pre útočníka[4].

Obnova funkcionality katastra nebola kompletná ani ešte začiatkom februára[4], pričom nebolo jasné, či má štát dostupné kompletné zálohy dát na obnovu systému. Čo však vcelku zrejmé bolo, že štát nemal dostupné komplexné zálohy na rýchlu obnovu systému. Nedostupnosť tohto systému vedie k mnohým komplikáciam života občanov alebo k ekonomickým stratám.

Kybernetické útoky nie sú v súčastnosti ničím výnimočným a dochádza k nim prakticky každý deň (pričom drvivá väčšina z nich je neúspešná). Nedávno došlo k útoku aj na ďalšie inštitúcie Slovenska (Všeobecnú zdravotnú poisťovňu[5] alebo

[1]Konkrétny deň útoku nebol jasne určený, oznam na portáli ÚGKK bol zverejnený 7. januára, no sú náznaky, že útok prebehol už v nedeľu 5. januára, kedy už bol systém nedostupný.

[2]Pomocou útoku na otvorený port protokolu NTP možno zneužiť na amplifikovanie útoku DDoS.

[3]10 z nich bolo CVE a mnohé z nich umožňovali vykonávanie ľubovoľného kódu.

[4]Spomenieme ešte, že autor tiež konštatuje, prečo tieto zraniteľnosti neodhalil systém Achilles vládneho CSIRT a prečo neboli nahlásené jeho zistenia.

Trenčianské vodárne a kanalizácie[6]). Samozrejme, Slovensko nie je žiadnou výnimkou, podobne boli zasiahnutý aj naši severní susedia Poliaci, kde došlo k útoku na spoločnosť EuroCert[7][8][5].

Z pohľadu čísel jeden zdroj uvádza [9], že v druhej polovici roka 2024 každá organizácia na Slovensku čelila v priemere 1443 kybernetickým útokom každý týždeň, pričom toto číslo stúplo až na 2000 v priebehu decembra[6].

Keby pôjdeme o kúsok ďalej a pozrieme sa na Európu, ENISA vydala v septembri 2024 ročnú správu o stave hrozieb v prostredí kybernetickej bezpečnosti[10]. V tejto správe pozorovali 11,709 incidentov a identifikovala niekoľko primárnych hrozieb — ransomvér, malvér, sociálne inžinierstvo, hrozba voči dátam, DoS útoky a manipuláciu informácií. Útoky boli najviac zamerané na verejný sektor a tvorili podiel až 19%(1870 incidentov), najpočetnejšiu skupinu hrozieb tvorili útoky DOS/DDOS/RDOS (46.31%, 2460 incidentov), ransomvér (27.33%, 1450 incidentov) a útok na dáta[7] (18.57%, 840 incidentov).

Týmto krátkym úvodom sme chceli čitateľovi naznačiť a upevniť v tom, že súčasné informačné systémy napojené na internet sú vystavené veľkému počtu hrozieb. Chrániť svoje systému musí každá organizácia, či je malá alebo veľká, pretože potenciálne (v niektorých prípadoch aj reálne) negatívne následky často rádovo prevyšujú náklady, ktoré by mohli organizácie vynaložiť na preventívne opatrenia a systematické riešenie informačnej a kybernetickej bezpečnosti. Nehovoriac o Slovenskej legislatíve, ktorá ukladá veľkému množstvu subjektov mnohé zákonné povinnosti v oblasti informačnej a kybernetickej bezpečnosti. Preto položíme čitateľovi otázku v kontexte predchádzajúcich odstavcov: „Keď už aj veľké inštitúcie ako ÚGKK majú problém so zaistením dostatočnej informačnej a kybernetickej bezpečnosti, o čo lepšie na tom budú malé samosprávy s menšími kapacitami a zdrojmi?“

TODO vieme nájsť aj citáciu záberu z markízy?

Jeden IT expert uviedol pre Rádio Expres[11], že v prepočte na počet obcí nám na Slovensku chýba zhruba 20,000 expertov v oblasti kybernetickej a informačnej bezpečnosti. My si tento problém uvedomujeme a preto by sme aj chceli navrhnúť systematické riešenie, ktorým by sme ho vyriešili. Čím sa dostávame k našej diplomovej práci: „Čo keby existoval expertný systém pre malé samosprávy, ktorý by vedel laikovi pomôcť vysvetliť kybernetickú a informačnú bezpečnosť, identifikovať aktíva, posúdiť potenciálne hrozby a prijať bezpečnostné opatrenia na ošetrenie dopadu rizík?“ Návrhu a zdrojom potrebným na vypracovanie takéhoto systému sa budeme venovať v ďalších častiach práce.

[5]Unikli citlivé údaje, ako napríklad údaje z občianskych preukazov, čísla PESEL (poľská verzia rodných čísel), kontaktné údaje, prihlasovacie mená a heslá.

[6]Najväčší podiel tvorili DoS útoky botnetov s podielom 11.5%.

[7]V zmysle úmyselné narušenie údajov alebo neúmyselný únik údajov.

0.2 Legislatívny rámec

Problematike kybernetickej a informačnej bezpečnosti sa v legislatívnom rámci Slovenskej republiky venujú najmä dva zákony, a to Zákon o kybernetickej bezpečnosti[12](ZoKB) a Zákon o informačných technológiách vo verejnej správe[13](ZoITVS). Oba zákony vychádzajú z medzinárodných štandardov série ISO/IEC 27000, sú navzájom prepojené a vzájomne na seba odkazujú.

69/2018 Z. z., zákon o kybernetickej bezpečnosti

Tento zákon patrí pod pôsobnosť Národného bezpečnostného úradu (NBÚ) a definuje základný subjekt — prevádzkovateľ základnej služby — to je ten, kto je zapísaný v registry prevádzkovateľov základnej služby. Register základných prevádzkovateľov služieb vedie a spravuje NBÚ a v súčasnosti je v ňom zapísaných vyše 1500 subjektov, ako napríklad rôzne obce, mestá, nemocnice a iné.

Analýza rizík sa explicitné spomína v
20, ods. (1):

> [...] Bezpečnostné opatrenia sú realizované na základe vykonanej analýzy rizík a s prihliadnutím na bezpečnostné metodiky a politiky úradu, najnovšie bezpečnostné trendy a medzinárodné normy a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti a prijímajú sa s cieľom [...]

Na subjekty kladie ZoKB rôzne požiadavky v oblasti KIB a ukladá im povinnosť zaviesť bezpečnostné opatrenia v závislostí od kategórie sietí a informačných systémov[8]. Rozsah a podrobnosti bezpečnostných oprávnení upravuje samostatná vyhláška 362/2018 Z. z.[14].

95/2019 Z. z., zákon o informačných technológiách vo verejnej správe

Tento zákon patrí pod pôsobnosť Ministerstva investícií, regionálneho rozvoja a informatizácie (MIRRI) a definuje nasledovné pojmy a subjekty:

- **informačná technológia**, prostriedok alebo postup slúžiaci na spracúvanie údajov alebo informácií v elktronickej podobe (informačný systém, infraštruktúra, informačná činnosť alebo elektronické služby)
- **informačný systém**, funkčný celok zabezpečujúci cieľavedomú informačnú a systematickú činnosť prostredníctvom technických a programových prostriedkov

[8]Kategórie sú tri v závislosti od rozsahu potencionálneho bezpečnostného incidentu.

- **správca**, orgán riadenia zodpovedný za informačnú technológiu na účely poskytovania služby verejnej správy
- **prevádzkovateľ**, osobitným predpisom ustanovený orgán riadenia alebo správcom určená osoba a vykonáva činnosti, ktoré mu určí správca[9]

Rámcovo definuje kompetencie, právomoci a povinnosti správcu pre oblasť KIB, ako napríklad povinnosti pri navrhovaní, akvizícii a obstarávaní informačných systémov alebo povinnosti voči tretím stranám. Podobne, ako pri ZoKB, kategorizácia sietí a informačných systémov je podrobne rozpracovaná vo vyhláške 179/2020 Z. z.[15].

Analýza rizík sa explicitné spomína v
14, ods. (1), písm. h):

> (1) Správca je na úseku plánovania a organizácie informačných technológií verejnej správy povinný
>
> h) zabezpečiť riadenie rizík,

0.3 Základné pojmy

Štandardom v oblasti kybernetickej a informačnej bezpečnosti sa venujú viaceré veľké organizácie, terminológia ešte nie je jednotná, ako to uvádza ENISA vo svojom prehľade o medzerách a prienikoch v štandardizácií[16]. Preto sa v tejto časti budeme venovať terminológii, aby sme mali rovnakú predstavu a pochopenie za jednotlivými pojmami, vychádzať budeme z materiálu „Krátky úvodu do informačnej a kybernetickej bezpečnosti“[17].

informácia

Esenciálny zdroj, bez ktorého organizácia nemôže plniť svoje poslanie. Spracováva sa digitálnymi informačnými a komunikačnými technológiami.

informačná bezpečnosť

Zaoberá sa hrozbami voči informáciám a hľadaním účinných bezpečnostných opatrení na zníženie rizika, ktoré vplýva z naplnenia týchto hrozieb.

informačné a komunikačné technológie, IKT

Metódy, prostriedky a zariadenia slúžiace na záznam, prenos, uchovávanie a spracovanie informácie.

[9] V skrate, správca môže delegovať svoje činnosti, no stále za ňu nesie zodpovednosť.

digitálne informačné a komunikačné technológie, d-IKT

IKT, ktoré vznikli spojením počítačov, telekomunikačných sieti a masovokomunikačných prostriedkov, ktoré využívajú digitálne kódovanie informácie a spoločné komunikačné kanály na prenos údajov.

aktívum

Čokoľvek, čo má pre organizáciu hodnotu. Môže byť hmotné — zariadenie, personál alebo nehmotné — informácia, vedomosť.

hrozba

Objektívne existujúca potenciálna možnosť priamo alebo nepriamo narušiť systém, spracovávanú informáciu alebo iné aktíva organizácie.

riziko

Veličina, ktorá závisí od závažnosti/možného dopadu hrozby a pravdepodobnosti naplnenia hrozby.

správa rizík

Proces identifikácie, odhadu, vyhodnotenia rizík a prójmania opatrení voči nim. Patrí sem tiež monitorovanie zostatkových rizík a pravideln=e prehodnocovanie rizík.

analýza rizík

Proces, ktorý identifikuje, posudzuje, hodnotí a ošetruje riziko.

bezpečnostné opatrenie

Technické, organizačné, právne alebo iné riešenie, ktoré úplne alebo čiastočne odstraňuje zraniteľnosť, znižuje pravdepodobnosť naplnenia hrozby alebo v prípade naplnenia hrozby znižuje jej dopad.

dôvernosť, confidentiality

Bezpečnostná požiadavka, ktorej naplnenie znamená, že prístup k informácií obsiahnutej v správe majú iba povolené osoby.

integrita, integrity

Bezpečnostná požiadavka, ktorej naplnenie znamená, že údaje nie je nemôže zmeniť bez toho, aby to ich vlastník alebo adresát nemohol zistiť.

dostupnosť, availability

Bezpečnostná požiadavka, ktorej naplnenie znamená, že zdroje systému sú k dispozícií oprávnenej osobe vždy alebo od času t, keď o to požiada.

CIA

Anglická skratka iniciálok trojice bezpečnostných požiadaviek — C(onfidentiality), I(ntegrity), A(vailability).

0.4 Organizácie a štandardy venujúce sa analýze rizík

Pri návrhu a vývoji nášho systému budeme vychádzať z medzinárodných štandardov a metodík. Dôvodom je záruka kvalitných podkladov a vedomostí expertov, ktorý majú mnohé praktické skúsenosti z problematikou KIB a súčasne kompatibilita ich riešení s legislatívnymi požiadavkami.

NIST

NIST alebo *angl.* „National Institute of Standards and Technology“ je organizácia Spojených štátov amerických, ktorej cieľom je podpora inovácií a priemyselnej schopnosti pokrokmi v oblasti vedeckých meraní, štandardov a technológií spôsobmi, ktoré obohacujú ekonomickú bezpečnosť a kvalitu našich[10] životov[18]. NIST vypracoval viacero štandardov v oblasti správy rizík, napríklad *NIST Special Publication 800-37*[19] a *NIST Special Publication 800-30*[20].

NIST Special Publication 800-37 *Risk Management Framework for Information Systems and Organizations* poskytuje usmernenie pre implementáciu štruktúrovaného a znovupoužiteľný proces riadenia rizík. Začleňuje prvky bezpečnosti, súkromnosti a riadenia rizík dodávateľského reťazca. Implementácia pozostáva zo siedmych krokov:

1. **príprava** esenciálnych aktivít potrebných pre riadenie bezpečnosť a ochranu súkromia v organizácií — vymedzenie rolí a zodpovedností, identifikácia tolerancie k risku a bezpečnostných požiadaviek a ďalšie

[10] Naších v zmysle občanov Spojených štátov amerických

2. **kategorizácia** systémov a spracovávanej, uchovávanej a prenášanej informácie voči požiadavkám CIA

3. **voľba** bezpečnostných opatrení zo štandardu NIST SP 800-53[**?**] na ochranu systému vychádzajúce z posúdení rizík

4. **implementácia** bezpečnostných opatrení a dokumentácia ich nasadenia

5. **posúdenie** súladu zavedených bezpečnostných opatrení, či sú funkčné a prinášajú požadované výsledky

6. **autorizácia** bezpečnostných opatrení vedením organizácie a určenie, či úroveň rizika systém je akceptovateľná

7. **monitorovanie** bezpečnostných opatrení pomocou logov, skenovania zraniteľností, hodnotenia bezpečnostných opatrení a prispôsobovanie sa novým hrozbám

NIST Special Publication 800-30 *Guide for Conducting Risk Assessments* poskytuje návod, ktorý ma pomôcť organizáciám identifikovať a posúdiť bezpečnostné riziko ich systémov a dát za použitia stratégie *risk-based decision-making*[11]. Implementácia pozostáva zo štyroch krokov:

1. **príprava**, definovanie účelu, rozsahu, predpokladov a zhromaždenie dát pre analýzu rizík

2. **vykonanie** analýzy rizík, a to identifikáciou zdrojov hrozieb, zraniteľností a určením pravdepodobnosti a dopadu

3. **komunikácia** zistení analýzy rizík zainteresovaným stranám, vedúcim a IT oddeleniam

4. **udržiavanie** analýzy rizík, aktualizácia a revidovanie v pravidelných intervaloch

V príručke je každý z týchto krokov ešte rozdelený na podúlohy a obsahuje zoznam kľúčových aktivít pre daný krok.

ISO/IEC 27000

ISO *angl.* „International Organization for Standardization“ je medzinárodne uznávaná organizácia publikujúca svetové štandardy, v oblasti kybernetickej a informačnej bezpečnosti je pre nás zaujímavá séria ISO/IEC 27000[21]. Na základe tejto série sa môže organizácia certifikovať ISO 27001 certifikáciou. Mnohé ďalšie štandardy a príručky sa

[11] Myšlienkou *risk-based decision-making* je vyhodnocovať riziká, príležitosti, potenciálne výsledky a voľba cesty k dlhodobému úspechu.

odkazujú na túto sériu a ich kompatibilitu s jej štandardami. Nás z tejto série bude zaujímať najmä štandard ISO/IEC 27005[22] zameraný na riadenie rizík informačnej bezpečnosti.

Štandard **ISO/IEC 27005** poskytuje štrukturovaný prístup k identifikácií, posudzovaniu a ošetrení rizík kybernetickej a informačnej bezpečnosti. Implementácia pozostáva z piatich krokov:

1. **určenie kontextu**, definovanie rozsahu, cieľa, kritérií rizika, aktív, zainteresovaných strán, biznisových procesov a určenie akceptovateľného rizika

2. **posudzovanie rizika**, identifikácia (hrozieb, zraniteľností a potenciálnych dopadov), analýza (určenie pravdepodobnosti a dopadu každého rizika) a vyhodnotenie (porovnanie voči akceptovateľnému riziku) rizík

3. **ošetrenie rizík**, prijatie bezpečnostných opatrení na zmiernenie, prenos, akceptovanie alebo prenesenie rizika

4. **komunikácia rizík**, zistení analýzy rizík zainteresovaným stranám, vedúcim a IT oddeleniam a zaručenie súladu s biznisovými cieľmi organizácie

5. **monitorovanie a kontrola**, kontinuálne monitorovanie a aktualizácia rizík, vykonanie bezpečnostného auditu a penetračného testovania

BSI

BSI *nem.* „Bundesamt für Sicherheit in der Informationstechnik“ je nemecký spolkový úrad pre informačnú bezpečnosť. BSI vydalo niekoľko štandardov v oblasti kybernetickej a informačnej bezpečnosti, konkrétne BSI-Standard 200-3[23] a IT-Grundschutz-Compendium[24]. Dôležité je tiež spomenúť, že tieto štandardy sú kompatibilné so sériou ISO/IEC 27000.

IT-Grundschutz-Compendium poskytuje štandardizované požiadavky pre typické biznisové procesy (napr. OPS.1.1.3 Patch and Change Management), aplikácie (napr. APP.1.1 Office Products), IT systémy (napr. SYS.1.3 Linux and Unix Servers), komunikačné linky (napr. NET.1.1 Network Architecture and Design) a miestnosti (napr. INF.2 Data Centre and Server Room) popísané v samostatných moduloch IT-Grundschutz.

Hádam najväčiou výhodou IT-Grundschutz-Compendium je zníženie analytického úsilia na organizácie. BSI pre jednotlivé moduly už vykonala analýzu rizík, hrozieb a zraniteľností a vybralo vhodné bezpečnotné požiadavky pre typické scenáre, ktoré si môže organizácia prebrať a implementovať do vlastných bezpečnostných opatrení v závislosti od ich vlastnej situácie, potrieb a zdrojov.

BSI-Standard 200-3 *Risk Analysis based on IT Grundschutz* poskytuje jednoducho aplikovateľné a rozoznateľné procedúry, ktoré organizaciám umožňujú adekvátnu cielenú kontrolu rizík kybernetickej a informačnej bezpečnosti. Je to praktický návod pre analýzu rizík založený na IT-Grundschutz-Compendium opisujúci postupnosť krokov s príkladmi a vysvetleniami. Implementácia pozostáva zo štyroch krokov:

1. **vypracovanie prehľadu hrozieb**, zostavenie zoznamu potenciálnych základných hrozieb, určenie dodatočných hrozieb vyplývajúcich zo špecifických operačných scenárov

2. **klasifikácia rizík**, posudzovanie (určenie pravdepodobnosti a rozsahu škôd) a hodnotenie (určenie kategórie) rizík

3. **ošetrenie rizík**, vyhnutie sa riziku, zníženie rizika (určenie bezpečnostných opatrení), prenos rizika a akceptovanie rizika

4. **konsolidácia bezpečnostného konceptu**, integrovanie dodatočných bezpečnostných opatrení vyplývajúcich z analýzy rizík v bezpečnostnom koncepte

0.5 Výber štandardov pre náš systém

Jednou z výhod štandardov NIST je ich rozsiahlosť a obsažnosť, na druhú stranu ich cieľom sú veľké podniky na pôde Spojených štátov amerických. Nevylučujeme však, že pre manažéra kybernetickej a informačnej bezpečnosti by boli cenným zdrojom znalostí.

Podobne, séria štandardov ISO/IEC 27000 rozsiahle opisuje požiadavky a spôsob vykonania analýzy rizík. Negatívum je, že nevysvetľujú postup tak „ľudsky“, ako štandardy BSI, nie sú verejne dostupné a ani nie sú cenovo najdostupnejšie.

Nakoniec sme sa rozhodli postupovať a vychádzať podľa štandardov BSI. Pre návrh a implementáciu nášho systému sme sa rozhodli vychádzať zo štandardu BSI-Standard 200-3[23] a kompendia IT-Grundschutz-Compendium[24]. Medzi ich hlavné výhody považujeme:

- praktické návody na zavedenie kybernetickej a informačnej bezpečnosti
- vypracovanie analýzy rizík pre štandardné situácie
- modulárny prístup
- verejná dostupnosť
- dobre aplikovateľné v priestore Európskej únie a Slovenskej republiky
- dajú sa dobre prispôsobiť rôzne veľkým/komplexným organizáciám

- kompatibilita so série štandardami ISO/IEC 27000

Legislatíva SR v oblasti KIB vychádzala zo série štandardov ISO/IEC 27000, teda aplikovaním postupov a bezpečnostných opatrení štandardov BSI by sme dosiahli súlad aj s našou legislatívou.

0.6 Požiadavky na systém

Náš systém bude postavený na štandarde BSI-Standard 200-3[23] a moduloch kompendia IT-Grundschutz-Compendium[24]. Používateľovi by mal pomôcť nasledovne:

1. oboznámi ho o jeho zákonných povinnostiach
2. poskytne mu zoznam aktív pre analýzu rizík, z ktorých si zvolí relevantné aktíva
3. prevedie ho postupom analýzy rizík pre konkrétne aktívum
4. navrhne mu bezpečnostné opatrenia na ošetrenie rizík
5. vytvorí bezpečnostnú dokumentáciu vykonanej analýzy rizík

Systém bude navrhnutý modulárne, aby poskytoval jednotný prístup pri analýze rizík a aby mohol byť v budúcnosti ľahko rozšíriteľný. Cieľová skupina nášho systému sú malé samosprávy, ktoré nemajú dostatočné prostriedky alebo kapacity, aby si analýzu rizík sieti a informačných systémov urobili sami.

Naskytá sa otázka, ako navrhnúť takýto systém, aby bol použiteľný, modulárny a intuitívny pre používateľa? Touto otázkou sa budeme zaoberať v ďalších kapitolách.

Literatúra

[1] *Útok na kataster: Hlavný systém nepôjde ešte dlho, do riešenia zapojili zahraničných expertov.* 12. január 2025, https://www.aktuality.sk/clanok/cnfy4sp/utok-na-kataster-hlavny-system-nepojde-este-dlho-do-riesenia-zapojili-zahran

[2] *Čo nové vieme o hacknutí katastra: 7-ciferné výkupné, chabé zálohy dát, hroziaci chaos.* 8. január 2025, https://zive.aktuality.sk/clanok/b5zVECn/co-nove-vieme-o-hacknuti-katastra-7-ciferne-vykupne-chabe-zalohy-dat-hroziac

[3] *Post mortem analýza perimetra Katastra.* 9. január 2025, https://www.linkedin.com/pulse/post-mortem-anal%C3%BDza-perimetra-katastra-martin-fabry-yq8ve/.

[4] *Post mortem analýza perimetra Katastra.* 22. január 2025, https://zive.aktuality.sk/clanok/1RE7Q19/postupne-otvaraju-katastralne-urady-pozrite-si-kde-zoznam-a-mapa/.

[5] *Všeobecná zdravotná poisťovňa pre kybernetické útoky dočasne pozastavila službu eRecept.* 29. január 2025, https://zive.aktuality.sk/clanok/AwmekDY/vseobecna-zdravotna-poistovna-pre-kyberneticke-utoky-docasne-pozastavila-slu

[6] *Hackeri nedávno útočili aj na vodárne slovenského mesta. O časti záloh na katastri vraj útočníci nevedeli.* 20. január 2025, https://zive.aktuality.sk/clanok/aJpHWCW/hackeri-nedavno-utocili-aj-na-vodarne-slovenskeho-mesta-o-casti-zaloh-na-kat

[7] *Pri útoku hackerov v Poľsku unikli osobné údaje obyvateľov.* 17. január 2025, https://zive.aktuality.sk/clanok/ah9V9rF/pri-utoku-hackerov-v-polsku-unikli-osobne-udaje-obyvatelov/.

[8] *Attack on EuroCert – Official Statement.* 15. január 2025, https://eurocert.pl/en/atak-na-eurocert-oswiadczenie/.

[9] *Počet kyberútokov na organizácie na Slovensku vzrástol medziročne o tretinu.* 30. december 2024, https://zive.aktuality.sk/clanok/KoZhOXt/pocet-kyberutokov-na-organizacie-na-slovensku-vzrastol-medzirocne-o-tretinu/

[10] *ENISA THREAT LANDSCAPE 2024*. september 2024, https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf.

[11] *IT expert: Zaplatiť hackerom výkupné nie je dobrá stratégia, útok by sa mohol aj tak zopakovať.* 14 január 2025, 30-minúta https://podmaz.sk/podcast/brano-zavodsky-nazivo/9385994339-it-expert-zaplatit-hackerom-vykupne-nie-je-dobra-strategia-utok-by-sa-mo

[12] *69/2018 Z. z., zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov*. Časová verzia predpisu účinná od 01.01.2025, https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/69/.

[13] *95/2019 Z. z., zákon o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov*. Časová verzia predpisu účinná od 01.01.2025 do 27.06.2025, https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2019/95/.

[14] *362/2018 Z. z., vyhláška Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení*. Časová verzia predpisu účinná od 01.09.2023, https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/362/.

[15] *179/2020 Z. z., vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy* . Časová verzia predpisu účinná od 30.06.2020, https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2020/179/.

[16] *Definition of Cybersecurity, Gaps and overlaps in standardisation*. december 2015, https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity_Definition_Gaps_v1_0.pdf.

[17] *Krátky úvod do informačnej a kybernetickej bezpečnosti a Malý výkladový slovník*. február 2022, https://mirri.gov.sk/wp-content/uploads/2022/02/KB-K1_2_3-uvod-do-KIB_slovnik_ver1.1.pdf.

[18] *About NIST*. https://www.nist.gov/about-nist.

[19] *NIST Special Publication 800-37, Risk Management Framework for Information Systems and Organizations, Revision 2*. 2018.

[20] *NIST Special Publication 800-30, Guide for Conducting Risk Assessments, Revision 1*. 2012.

[21] *ISO/IEC 27000 family, Information security management.* https://www.iso.org/standard/iso-iec-27000-family.

[22] *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks.* https://www.iso.org/standard/80585.html.

[23] *BSI Standard 200-3: Risk Analysis based on IT Grundschutz.* Version 1.0, October 2017, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.pdf?__blob=publicationFile&v=2.

[24] *IT-Grundschutz-Compendium.* Final Draft, 1 February 2022, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2022.pdf?__blob=publicationFile&v=2.