KRÍZOVÝ MANAŽMENT
DOI 10.26552/krm.C.2024.2.53-59
ISSN – 1336 – 0019 (tlač)
ISSN – 2730 – 0544 (online)

VÝZVY V PROCESE IDENTIFIKÁCIE RIZÍK V MANAŽMENTE INFORMAČNEJ BEZPEČNOSTI

CHALLENGES IN THE RISK IDENTIFICATION PROCESS IN INFORMATION SECURITY MANAGEMENT

KATARÍNA KAMPOVÁ, TOMÁŠ LOVEČEK

ABSTRACT: *The article focuses on risk identification as a crucial process within the broader framework of information security management. It highlights the challenges posed by inconsistent legislative requirements and the need for harmonization through international standards, specifically STN ISO/IEC 27005:2023. The authors discuss the importance of a systematic approach to risk management, detailing how the accurate identification of risks influences subsequent phases like analysis, evaluation, and treatment of risks. The article also compares current cybersecurity legislation with international standards, offering insights into best practices for effective risk management in organizations. The conclusions emphasize the need for integrating these standards to ensure consistency and resource efficiency in practice.*

KEYWORDS: *Information Security Management. Risk Identification. Cybersecurity Standards. Risk Management Process.*

ÚVOD

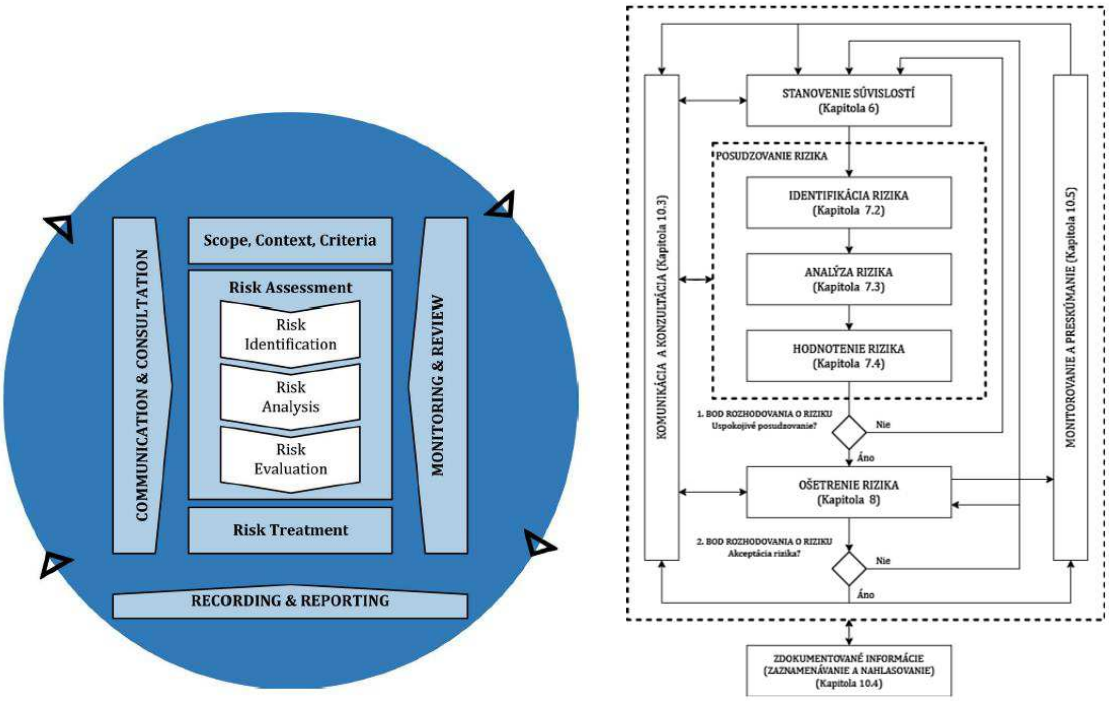
Posudzovanie, hodnotenie, riadenie a analýza rizík patria medzi kľúčové legislatívne požiadavky v oblasti informačnej bezpečnosti. Tieto požiadavky sa uplatňujú v rôznych oblastiach, ako je ochrana osobných údajov, kybernetická bezpečnosť, ochrana utajovaných informácií a bezpečnosť informačných systémov verejnej správy či bánk. V praxi sa však objavili problémy, ktoré vyplývajú z toho, že tieto legislatívne predpisy vznikali v rôznych časových obdobiach a pod záštitou rôznych štátnych orgánov, ako napríklad Úradu na ochranu osobných údajov alebo Národného bezpečnostného úradu. Hlavnou výzvou je terminologická a procesná nesúrodosť týchto predpisov, čo sťažuje ich aplikáciu v organizáciách, ktoré musia tieto rozdielne požiadavky implementovať. Situácia sa ešte komplikuje, keď subjekty spadajú pod viaceré legislatívne rámce, napríklad GDPR, zákon o kybernetickej bezpečnosti a zákon o informačných technológiách verejnej správy. Táto nejednotnosť nielen zvyšuje nároky na zdroje, ale môže ohroziť dlhodobú udržateľnosť manažérstva informačnej bezpečnosti v organizácii. Preto je nevyhnutné harmonizovať procesy posudzovania rizík informačnej bezpečnosti prostredníctvom výberu vhodného systému manažérstva rizík, ktorý by bol univerzálne použiteľný. Medzinárodné technické normy, ako STN ISO/IEC 27005:2023, poskytujú základ pre vytvorenie takéhoto rámca, pričom táto norma prináša významné zmeny a zosúlaďuje posudzovanie rizík so všeobecným štandardom pre manažérstvo rizík ISO 31000:2018. To z nej robí vhodný etalón pre efektívne posudzovania rizík v oblasti informačnej bezpečnosti.

1. KĽÚČOVÉ POŽIADAVKY NA MANAŽÉRSTVO RIZÍK V OBLASTI INFORMAČNEJ BEZPEČNOSTI

Systém manažérstva informačnej bezpečnosti (ISMS) je podľa normy ISO/IEC 27000 (2018) základným rámcom, ktorý obsahuje pravidlá, smernice, postupy a zdroje potrebné na ochranu informačných aktív organizácie. Tento systém sa zameriava na systematické riadenie bezpečnosti informácií prostredníctvom zavádzania, monitorovania, hodnotenia a neustáleho zlepšovania bezpečnostných procesov. Cieľom ISMS je nielen ochrana informačných aktív, ale aj dosahovanie bezpečnostných cieľov organizácie. V súlade s normou ISO/IEC 27001 (2022) je dôležité, aby organizácia pri vytváraní ISMS identifikovala riziká a príležitosti, ktoré môžu ovplyvniť jej činnosť. Tento proces zahŕňa zohľadnenie vnútorných a vonkajších faktorov, ktoré môžu ovplyvniť dosahovanie bezpečnostných cieľov. Kľúčovými cieľmi sú zabezpečenie úspešného fungovania ISMS, predchádzanie negatívnym dopadom, ich minimalizácia a neustále zlepšovanie bezpečnostných procesov.

Identifikácia rizík a príležitostí vedie k návrhu opatrení, ktoré musia byť integrované do systému manažérstva informačnej bezpečnosti, pričom sa posúdenie rizík stáva neoddeliteľnou súčasťou tohto systému. Posúdenie rizík informačnej bezpečnosti podľa ISO/IEC 27001 (2022) zahŕňa niekoľko krokov: stanovenie kritérií pre riziká, konzistentné a opakovateľné posúdenie rizík, identifikáciu rizík spojených s dôvernosťou, integritou a dostupnosťou informácií, a následnú analýzu týchto rizík. Táto analýza zahŕňa hodnotenie pravdepodobnosti výskytu rizík a potenciálnych dôsledkov, pričom sa určuje úroveň rizika. Výsledky sa porovnávajú s preddefinovanými kritériami a riziká sú prioritizované pre ďalšie opatrenia. Organizácia musí následne definovať proces ošetrenia rizík informačnej bezpečnosti, ktorý zahŕňa výber vhodných opatrení na základe vykonanej analýzy rizík. Súčasťou tohto procesu je vytvorenie plánu na zvládnutie rizík a získanie súhlasu vlastníkov rizík, vrátane akceptovania zvyškových rizík.

Norma STN ISO/IEC 27005 (2023) upravuje proces posudzovania a ošetrenia rizík v súlade s princípmi ISO 31000 (2018). Táto harmonizácia terminológie a postupov bola síce súčasťou starších verzií noriem, ale v plnej miere bola zavedená až v revízii z roku 2022 (Obrázok 1).



b)

Obrázok 1 a) Proces manažmentu rizík (ISO 31000:2018) b) Proces riadenia rizík informačnej bezpečnosti (STN ISO/IEC 27005:2023)

Podľa ISO/IEC 27000 (2020) riziko (angl.: Risk) je účinok (odchýlka od očakávania - pozitívna alebo negatívna) neistoty (stav aj čiastočného nedostatku informácií súvisiacich s pochopením alebo znalosťou udalosti, jej následku alebo možnosťou výskytu, že nastane) na dosiahnutie cieľov. Podľa STN ISO/IEC 27005 (2023) riziká informačnej bezpečnosti môžu byť spojené s možnosťou, že hrozby zneužijú zraniteľnosti informačného aktíva alebo skupiny informačných aktív a spôsobia tak organizácii škodu.

Podľa ISO/IEC 27000 (2018) riadenie/manažment/manažérstvo rizika (angl.: Risk management) je systematické uplatňovanie politík riadenia, procedúr a postupov pri činnostiach komunikácie, konzultácií, stanovenia súvislostí a identifikácie, analýzy, hodnotenia, ošetrenia, monitorovania a preskúmania rizika. Posúdenie rizika (angl.: Risk assessment) je celkový proces identifikácie rizika, analýzy rizika a hodnotenia rizika. Pre komplexné scenáre rizík sa odporúča vykonávať iteratívne posúdenie, kde každé kolo prináša detailnejšie informácie o príčinách rizík. Tento proces sa opakuje,

až pokým nie sú jasne identifikované všetky kľúčové faktory rizika. Agregácia rizík sa realizuje len v prípade, že sú riziká vzájomne prepojené, napríklad v prípade dátových centier vystavených rôznym druhom rizík (záplavy, požiar, výpadky energie), kde však každé riziko vyžaduje samostatné opatrenia. Teda identifikácia rizika zahŕňa vyhľadávanie a opis rizík, vrátane ich zdrojov, príčin a dôsledkov. Analýza rizika poskytuje základ pre určenie úrovne rizika, na základe čoho sa rozhoduje o ďalšom postupe. Ošetrenie rizík môže zahŕňať rôzne prístupy, ako napríklad vyhnutie sa riziku, zníženie jeho pravdepodobnosti, zdieľanie rizika s treťou stranou alebo prijatie rizika s cieľom využiť príležitosť. Zmiernenie negatívnych dôsledkov rizík je často označované ako zmiernenie, eliminácia, prevencia alebo zníženie rizika. Tento prístup poskytuje organizáciám jasný rámec na efektívne riadenie a ochranu svojich informačných aktív, pričom kľúčovým prvkom je neustále zlepšovanie procesov manažmentu rizík.

2. PROCES IDENTIFIKÁCIE RIZÍK INFORMAČNEJ BEZPEČNOSTI A SCENÁRE RIZÍK

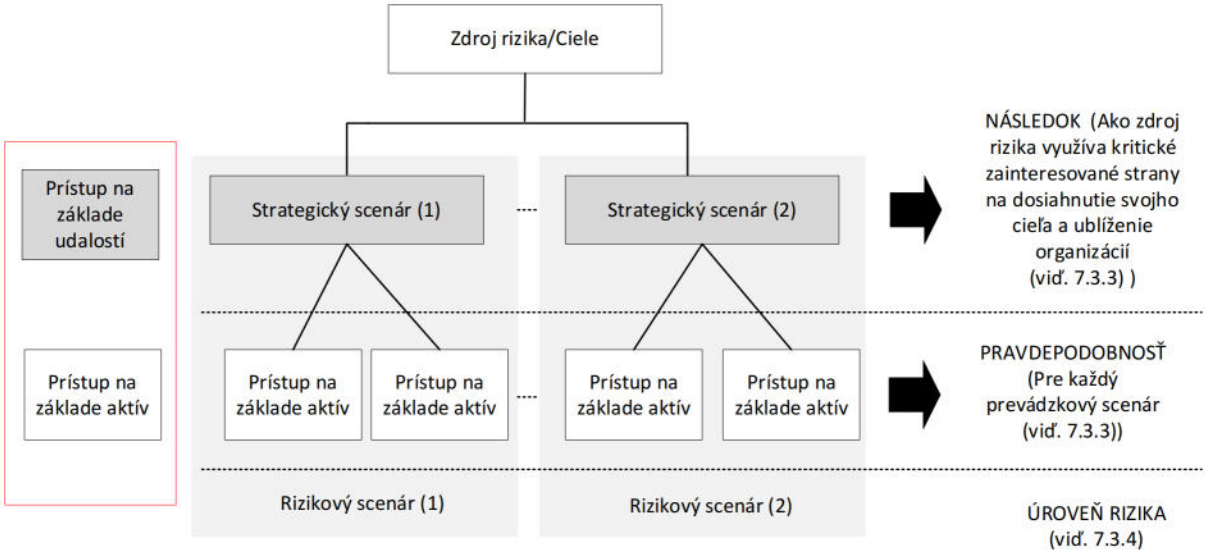
Identifikácia rizík predstavuje kľúčový a počiatočný krok v rámci posudzovania rizík informačnej bezpečnosti. Tento proces je zásadný nielen z hľadiska náročnosti na zdroje, ale aj preto, že priamo ovplyvňuje ďalšie fázy, ako sú analýza, hodnotenie a ošetrenie rizík. Správna identifikácia rizík je základom pre presné určenie pravdepodobnosti a následkov, čo umožňuje následné hodnotenie rizík a implementáciu adekvátnych bezpečnostných opatrení. Nesprávna alebo neúplná identifikácia rizík môže viesť k zavádzaniu neúčinných opatrení, ktoré ohrozujú bezpečnostný systém organizácie.

Identifikácia rizík zahŕňa vyhodnotenie potenciálnych hrozieb, ktoré môžu narušiť dôvernosť, integritu alebo dostupnosť informácií. Výsledkom tohto procesu by mal byť zoznam scenárov rizík, ktoré zahŕňajú identifikáciu zdrojov rizík a udalostí, ktoré môžu ohroziť ciele informačnej bezpečnosti organizácie. Podľa normy ISO 31000 (2018) môžu zdroje rizík pochádzať z ľudských, technických alebo environmentálnych faktorov. Udalosť, ako ju definuje ISO 11073 (2022), je zmena okolností alebo výskyt, ktorý môže viesť k rôznym dôsledkom. V kontexte informačnej bezpečnosti môžu tieto dôsledky vyvolať reťazovú reakciu, ktorá sa môže šíriť buď lineárne (domino efekt), alebo kumulatívne (kaskádový efekt). Norma ISO/IEC 27002 (2020) rozlišuje medzi udalosťou informačnej bezpečnosti, ktorá naznačuje možné porušenie bezpečnosti, a incidentom informačnej bezpečnosti, ktorý predstavuje jeden alebo viac nežiaducich javov ohrozujúcich prevádzku a bezpečnosť organizácie.

Každé riziko vzniká v dôsledku hrozieb, ktoré zneužívajú zraniteľnosti informačných aktív. Podľa normy ISO/IEC 27032 (2023) hrozba predstavuje potenciálnu príčinu incidentu, ktorá môže ohroziť systém alebo organizáciu. Na identifikáciu konkrétnych hrozieb sa používajú databázy ako MITRE ATT&CK, ktoré poskytujú prehľad aktuálnych techník a taktík využívaných pri kybernetických útokoch. Zraniteľnosť, ako ju definuje ISO/IEC 27000 (2018), je slabé miesto v aktíve alebo opatrení, ktoré môže byť zneužité hrozbou. Na identifikáciu zraniteľností sa využívajú databázy ako CVE (Common Vulnerabilities and Exposures), ktoré obsahujú informácie o známych zraniteľnostiach hardvéru, softvéru a ďalších aktív.

Aktívum je akýkoľvek prvok, ktorý má pre organizáciu hodnotu, vrátane informácií, systémov a podporných technológií. Podľa normy ISO/IEC 27032 (2023) sa informačné aktívum definuje ako znalosti alebo údaje, ktoré sú pre organizáciu cenné. Informačný systém, ktorý spravuje tieto aktíva, predstavuje zoskupenie technických a organizačných komponentov na spracovanie informácií.

Identifikácia rizík sa zakladá na vytvorení reťazca udalostí, ktorý zahŕňa zdroje hrozieb, samotné hrozby, zraniteľnosti a aktíva. Tento proces umožňuje komplexné posúdenie rizík v rámci celkového ekosystému organizácie. Podľa normy ISO/IEC 27005 (2023) identifikácia zdrojov rizík môže byť založená buď na prístupe zameranom na udalosti alebo na aktívach. Prístup založený na udalostiach začína všeobecným scenárov rizík a prechádza do detailov, zatiaľ čo prístup založený na aktívach sa začína analyzovaním jednotlivých aktív a postupne sa rozvíja do komplexného scenára (Obrázok 2).



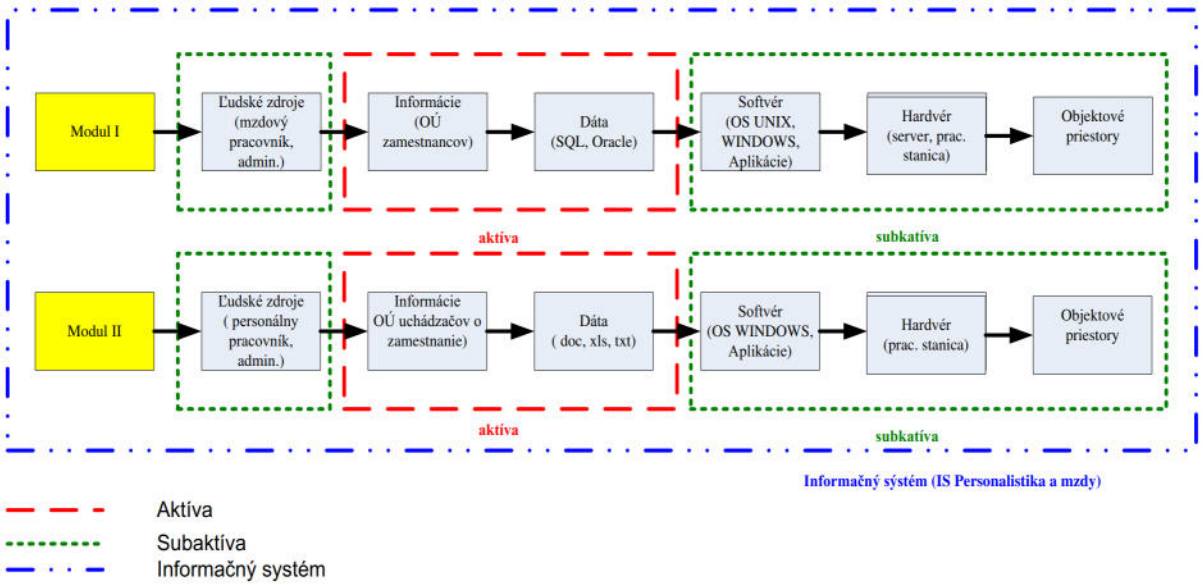
Obrázok 2 Posúdenie rizika na základe rizikových scenárov (STN ISO/IEC 27005:2023)

Norma odporúča kombináciu oboch prístupov, pretože prístup založený na aktívach môže poskytnúť konkrétny pohľad na prevádzkové scenáre, ktoré zase prispievajú k lepšiemu pochopeniu udalostných scenárov. Organizácie, ktoré zvolia len jeden z týchto prístupov, riskujú neúplnosť v tvorbe scenárov rizíik, čo môže ovplyvniť objektivitu stanovenia úrovne rizika a následne viesť k nedostatočným opatreniam na jeho ošetrenie. Strategický scenár sa zameriava na popis koncovej udalosti, ktorá je často spojená so stratou kľúčového atribútu primárneho aktíva, ako sú dostupnosť, dôvernosť alebo integrita. Prevádzkový, resp. operačný scenár na druhej strane zahŕňa udalosti, techniky a vektory útoku, ktoré vedú k tejto koncovej udalosti (Tabuľka 1). Kombináciou oboch prístupov môže organizácia identifikovať kritické faktory a lepšie pochopiť, ako sa kumulujú jednotlivé dôsledky.

Tabuľka 1 Strategické a operačné scenáre rizika (STN ISO/IEC 27005:2023)

Zdroj rizika	**Cieľ DES**	**Scenár strategických rizík (prístup založený na udalostiach)**	**Scenár operačného rizika (prístup založený na aktívach)**
Autoritársky štát	Získanie strategického vektora útoku	Podvracanie kritickej infraštruktúry	Nasadenie skrytého a perzistentného malvéru v dodávateľskom reťazci
Organizovaný zločin	Rozvoj nezákonných činností	Využívanie prístavnej infraštruktúry	Infiltrácia do odborovej organizácie prístavných robotníkov
			Prevzatie kontroly nad počítačovým systémom riadenia toku
		Karuselový daňový podvod	Vytváranie fiktívnych spoločností na vykonávanie falošných výmen na trhu s uhlíkovou daňou
		Vydieranie	Distribúcia ransomvéru
Agresívne podnikanie	Získanie trhového monopolu	Ovplyvňovanie regulačného orgánu	Korumpovanie osoby s rozhodovacou právomocou
		Odstránenie konkurentov	Kampaň hanobenia na sociálnych sieťach

Na uľahčenie procesu identifikácie rizík môžu byť aktíva usporiadané do hierarchickej štruktúry, čo zjednoduší odkazy na konkrétne aktíva v rámci hodnotenia rizík. Podľa metodiky Národného bezpečnostného úradu (2021) je pre veľké organizácie výhodnejší systémový prístup, ktorý sa zameriava na hodnotenie rizík z hľadiska procesov a informačných systémov, zatiaľ čo menšie organizácie môžu preferovať komponentovo orientovaný prístup, ktorý analyzuje jednotlivé prvky, ako sú zariadenia a aplikácie. Loveček (2008) zdôrazňuje význam modulárneho prístupu, ktorý hodnotí prvky informačného systému ako celok (Obrázok 3). Pri tomto prístupe sa primárne aktíva, ako sú dáta a informácie, analyzujú spolu so subaktívami, ako sú hardvér a softvér, ktoré sú nevyhnutné na spracovanie týchto informácií.



Obrázok 3 Príklad vytvárania modulov aktív v informačných systémoch (Loveček, 2008)

Identifikácia rizík a tvorba rizikových scenárov/scénarov rizík sú neoddeliteľnou súčasťou manažérstva informačnej bezpečnosti. Využitie kombinácie prístupov založených na udalostiach a aktívach poskytuje organizáciám komplexný náhľad na ich bezpečnostné riziká. Tento systematický prístup umožňuje presné hodnotenie rizík, podporuje efektívnu ochranu informačných aktív a zabezpečuje dlhodobú udržateľnosť bezpečnostných procesov.

3. PROCES MANAŽMENTU RIZÍK V LEGISLATÍVNYCH POŽIADAVKÁCH INFORMAČNEJ BEZPEČNOSTI

Legislatívne požiadavky týkajúce sa informačnej bezpečnosti vznikali postupne a pod rôznymi gesciami ústredných orgánov štátnej správy, čo spôsobilo terminologickú a procesnú nejednotnosť. Tento nesúlad predstavuje pre organizácie komplikácie pri implementácii týchto požiadaviek do svojho interného prostredia. Medzi dôležité legislatívne rámce patrí zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti, ktorý stanovuje bezpečnostné opatrenia pre organizácie, vrátane posudzovania rizík kybernetickej a informačnej bezpečnosti (KIB). Zákon zdôrazňuje, že bezpečnostné opatrenia sa prijímajú na základe analýzy rizík, ktorá určuje pravdepodobnosť vzniku škodlivých udalostí.

Špecifikácie pre bezpečnostné opatrenia v oblasti riadenia rizík KIB sú uvedené vo vyhláške Národného bezpečnostného úradu (NBÚ) č. 362/2018 Z.z. Táto vyhláška je podporená metodikou analýzy rizík vydanej v roku 2021 NBÚ, ktorá sa opiera o medzinárodné normy ako ISO/IEC 27005 a ISO 31000. Napriek tomu, že NBÚ odkazuje na tieto normy, metodika nie vždy korešponduje s novou revíziou normy ISO/IEC 27005 z roku 2022, ktorá zaviedla nové terminologické a procesné prístupy. Jedným z hlavných nesúladov je používanie termínu analýza rizík, ktorý podľa medzinárodných noriem predstavuje len jednu z fáz procesu posudzovania rizík.

Podľa vyhlášky NBÚ proces riadenia rizík KIB zahŕňa identifikáciu zraniteľností, hrozieb a rizík spojených s aktívami, pričom sa určuje vlastník rizika a implementujú sa bezpečnostné opatrenia. Tento proces však nie je v súlade s normou ISO/IEC 27005 (2022), ktorá zdôrazňuje, že identifikácia aktív, zraniteľností a hrozieb je súčasťou širšieho procesu identifikácie rizík, ktorý je začlenený do celkového posudzovania rizík. Vyhláška NBÚ tiež vynecháva fázu hodnotenia rizík, ktorá je nevyhnutná pre správne implementovanie bezpečnostných opatrení.

Ďalším rozdielom je zahrnutie analýzy funkčného dopadu (Business Impact Assessment - BIA) do procesu posudzovania rizík. Podľa metodiky NBÚ je analýza funkčného dopadu kľúčová pre určenie kritickosti aktív, pričom sa zameriava na dostupnosť služieb. V skutočnosti je BIA len jednou z možných

metód používaných na stanovenie veľkosti dôsledkov v procese analýzy rizík. Tento nesúlad vnímania BIA medzi vyhláškou NBÚ a medzinárodnými normami vyžaduje harmonizáciu. Vo vyhláške NBÚ sa taktiež uvádza princíp najhoršieho scenára (Worst Case Scenario) na určenie úrovne rizika. Tento prístup však neodzrkadľuje kritériá rizík uvedené v normách ISO, ktoré sa zameriavajú na kombináciu pravdepodobnosti a dôsledkov. Vhodnejšie by bolo používať prístup založený na udalostiach alebo aktívach, ktoré umožňujú komplexnejšiu identifikáciu rizík a stanovenie objektívnej úrovne rizika.

Na legislatívnej úrovni existujú aj ďalšie relevantné právne predpisy, ako je zákon č. 95/2019 Z.z. o informačných technológiách verejnej správy, ktorý od organizácií vyžaduje zabezpečenie riadenia rizík a bezpečnosti informačných technológií. Organizácie musia identifikovať významné aktíva, určiť ich vlastníkov a zdokumentovať proces posudzovania rizík. Tento zákon tiež vyžaduje vypracovanie vnútorného riadiaceho aktu, ktorý zahŕňa analýzu rizík, periodicitu vykonávania týchto analýz a spôsob dokumentácie bezpečnostných opatrení. Okrem toho, nariadenie GDPR a zákon č. 18/2018 Z.z. o ochrane osobných údajov upravujú ochranu osobných údajov vyžadujú od organizácií vykonávanie posúdenia vplyvu na ochranu údajov (Data Protection Impact Assessment - DPIA). Tento proces je neoddeliteľnou súčasťou riadenia rizík v oblasti ochrany súkromia a osobných údajov.

V legislatívnych rámcoch pre informačnú bezpečnosť, vrátane zákona o kybernetickej bezpečnosti a zákona o informačných technológiách verejnej správy, existuje evidentný nesúlad medzi terminológiou a procesmi v týchto právnych predpisoch s medzinárodnými normami, ktoré by mali byť základom pre riadenie rizík. Harmonizácia týchto právnych predpisov s medzinárodnými normami by zjednodušila aplikáciu legislatívnych požiadaviek v praxi a prispela k efektívnejšiemu riadeniu rizík v oblasti informačnej bezpečnosti.

ZÁVER

Manažment rizík v informačnej bezpečnosti je neoddeliteľnou súčasťou ochrany citlivých dát a zabezpečenia nepretržitého fungovania organizácií. Identifikácia rizík ako prvotný krok je zásadná, pretože jej presnosť a úplnosť priamo ovplyvňujú úspešnosť nasledujúcich krokov v analýze a riadení rizík. Ak sa nevenuje dostatočná pozornosť zosúladeniu legislatívnych požiadaviek s technickými normami, môže to viesť k nedorozumeniam a zvýšeným nárokom na zdroje organizácií. Preto je kľúčové integrovať medzinárodné normy, ako je STN ISO/IEC 27005:2023, ktoré poskytujú jednotný a overený rámec pre riadenie rizík. Tieto normy nielenže uľahčujú procesy, ale zároveň zabezpečujú konzistentnosť a efektívnosť pri riadení bezpečnosti v praxi. Pre organizácie je nevyhnutné, aby sa neustále prispôsobovali aktuálnym normám a optimalizovali svoje postupy na hodnotenie rizík v súlade s najnovšími štandardmi a osvedčenými postupmi. Výber medzi prístupom založeným na udalostiach a prístupom založeným na aktívach závisí od špecifických potrieb a kontextu organizácie. Prístup orientovaný na udalosti je vhodný pre organizácie, ktoré musia flexibilne reagovať na konkrétne hrozby, zatiaľ čo prístup orientovaný na aktíva umožňuje lepšie preventívne pokrytie bezpečnostných rizík. Kombinácia oboch prístupov môže byť optimálnym riešením, ktoré poskytuje komplexný a prispôsobivý prístup k riadeniu rizík. Týmto spôsobom organizácie získajú efektívnu stratégiu, ktorá ich lepšie chráni pred bezpečnostnými hrozbami.

Neustále zlepšovanie postupov posudzovanie rizík je kľúčové nielen z pohľadu plnenia legislatívnych požiadaviek, ale aj z pohľadu celkovej bezpečnostnej stratégie organizácie. Investície do lepšieho chápania rizík, ich zdrojov a potenciálnych dôsledkov môžu významne prispieť k zvýšeniu odolnosti organizácie voči kybernetickým hrozbám a iným bezpečnostným rizikám. Integrácia osvedčených medzinárodných postupov do vnútorných systémov riadenia bezpečnosti zároveň posilňuje celkovú dôveryhodnosť a stabilitu organizácie na trhu.

POĎAKOVANIE

Financované EÚ NextGenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu č. 17R05-04-V01-00005.

LITERATÚRA

Jens Rasmussen: Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering, September 1986, ISBN:978-0-444-00987-6, 228 str.

Tomáš Loveček, Bezpečnostné systémy : Bezpečnosť informačných systémov, Poledňák Pavel (Redaktor, editor). - 1. vyd. - Žilina : Žilinská univerzita, 2007. - 246 s. - ISBN 978-80-8070-767-5.

ISO 11073:2022 Risk management – Vocabulary

ISO/IEC TR 13335-3:1998 Information technology — Guidelines for the management of IT SecurityPart 3: Techniques for the management of IT Security

ISO/IEC 20000-1:2018 Information technology — Service managementPart 1: Service management system requirements

ISO/IEC 27000:2018 ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — RequirementsISO/IEC 27002:2020

ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks

STN ISO/IEC 27005: 2023 Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti.

ISO/IEC 27005:2008 Information technology — Security techniques — Information security risk managementISO/IEC 27032:2023

ISO 31000:2018 Risk management — Guidelines

ISO 55001:2014 - Management systems — Requirements

EN IEC 31010:2019 Risk management — Risk assessment techniques

NIST Special Publication 800-39 Managing Information Security Risk, NIST Special Publication 800-30 Rev. 1 Guide for Conducting Risk Assessments

Národný bezpečnostný úrad, Metodika analýzy rizík kybernetickej bezpečnosti. Metodika analýzy rizík pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti, 2021. Dostupná na: https://www.nbu.gov.sk/data/att/409.pdf

Katarína Kampová, doc. Ing. PhD.

Fakulta bezpečnostného inžinierstva, Katedra bezpečnostného manažmentu, Univerzitná 8215/1, 010 26 Žilina, Slovakia e-mail:katarina.kampova@uniza.sk

Tomáš Loveček, prof. Ing. PhD.

Fakulta bezpečnostného inžinierstva, Katedra bezpečnostného manažmentu, Univerzitná 8215/1, 010 26 Žilina, Slovakia

e-mail:tomas.lovecek@uniza.sk