**Stratégia kybernetickej bezpečnosti**



# Obsah

[Obsah 2](#_Toc122421169)

[Správa dokumentu 4](#_Toc122421170)

[Úvod 5](#_Toc122421171)

[2.1 Rozsah platnosti 5](#_Toc122421172)

[2.2 Legislatívny a metodický rámec 6](#_Toc122421173)

[2.2.1 Legislatíva 6](#_Toc122421174)

[2.2.2 Strategické dokumenty 6](#_Toc122421175)

[2.2.3 Bezpečnostné štandardy 6](#_Toc122421176)

[Bezpečnostné ciele z hľadiska kybernetickej bezpečnosti 7](#_Toc122421177)

[3.1 Piliere informačnej a kybernetickej bezpečnosti 7](#_Toc122421178)

[3.2 Strategické bezpečnostné ciele kybernetickej bezpečnosti 7](#_Toc122421179)

[Vyhodnocovanie bezpečnostných cieľov 9](#_Toc122421180)

[4.1 Spôsob vyhodnocovania bezpečnostných cieľov 9](#_Toc122421181)

[4.2 Kritériá vyhodnocovania, spôsoby priebežného hodnotenia primeranosti a spôsoby kontroly postupov využívaných na dosahovanie bezpečnostných cieľov 9](#_Toc122421182)

[Úlohy štatutárneho orgánu a vyhlásenie o podpore pri zabezpečovaní kybernetickej bezpečnosti 10](#_Toc122421183)

[5.1 Úlohy štatutárneho orgánu pri zabezpečovaní kybernetickej bezpečnosti 10](#_Toc122421184)

[5.2 Vyhlásenie štatutárneho orgánu o záväzku o podpore kybernetickej bezpečnosti 10](#_Toc122421185)

[Riadenie kybernetickej bezpečnosti 11](#_Toc122421186)

[6.1 Všeobecné zodpovednosti a povinnosti v oblasti kybernetickej bezpečnosti 12](#_Toc122421187)

[6.2 Špecifické zodpovednosti a povinnosti v oblasti kybernetickej bezpečnosti 12](#_Toc122421188)

[6.3 Určenie bezpečnostných rolí potrebných na riadenie kybernetickej bezpečnosti 14](#_Toc122421189)

[6.3.1 Riadiaca zložka 14](#_Toc122421190)

[6.3.2 Výkonná zložka 15](#_Toc122421191)

[6.3.3 Kontrolná zložka 18](#_Toc122421192)

[Základný rámec na riadenie aktív 19](#_Toc122421193)

[7.1 Identifikácia a evidencia aktív 19](#_Toc122421194)

[7.2 Klasifikácia informácií a kategorizácia sietí a informačných systémov 19](#_Toc122421195)

[7.2.1 Klasifikácia informácií 20](#_Toc122421196)

[7.2.2 Kategorizácia sietí a informačných systémov 21](#_Toc122421197)

[Základný rámec riadenia rizík 22](#_Toc122421198)

[8.1 Identifikácia zraniteľností 22](#_Toc122421199)

[8.2 Identifikácia hrozieb 22](#_Toc122421200)

[8.3 Identifikácia a analýza rizík s ohľadom na aktívum 23](#_Toc122421201)

[8.4 Určenie vlastníka rizika 23](#_Toc122421202)

[8.5 Implementácia bezpečnostných opatrení v závislosti od identifikovaných rizík 23](#_Toc122421203)

[8.6 Analýza funkčného dopadu 24](#_Toc122421204)

[8.7 Pravidelné preskúmavanie identifikovaných rizík 24](#_Toc122421205)

[Rozsah a periodicita overovania stavu kybernetickej bezpečnosti 25](#_Toc122421206)

[9.1 Audit kybernetickej bezpečnosti 25](#_Toc122421207)

[9.2 Interné preverovanie kybernetickej bezpečnosti 25](#_Toc122421208)

[Revízia bezpečnostnej stratégie 26](#_Toc122421209)

[Prílohy 27](#_Toc122421210)

[11.1 Kritériá vyhodnocovania, spôsoby priebežného hodnotenia primeranosti a spôsoby kontroly postupov využívaných na dosahovanie bezpečnostných cieľov 27](#_Toc122421211)

# Správa dokumentu

Dokument „Stratégia kybernetickej bezpečnosti“ je vzorovým dokumentom slúžiacim pre potreby orgánov verejnej moci. Vytvorený vzor dokumentu nie je povinný na použitie a ani nie je záväzný. Dokument je poskytnutý voľne a bezplatne na využitie podľa potrieb konkrétnej organizácie.

Vytvorený dokument má aj svoj metodický rozmer, takže je ho možné použiť i pre potreby vzdelávania pracovníkov organizácií v oblasti kybernetickej a informačnej bezpečnosti.

Vytvorené dokument nie je určený na ďalší predaj alebo akúkoľvek inú komerčnú či obchodnú činnosť.

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej aj „MIRRI“) nezodpovedá za nesprávne použitie predmetného dokumentu zo strany organizácie. Správne použitie a implementácia bezpečnostných opatrení je plne v kompetencii a zodpovednosti konkrétnej organizácie. Dokument je potrebné upraviť na základe reálnych potrieb a špecifického prostredia organizácie.

MIRRI si vyhradzuje právo na zmenu/úpravu predmetného dokumentu alebo čiastkových textov a tabuliek, a to v potrebnom rozsahu vrátane zmien verzií dokumentov. Dokument je výstupom pilotného projektu na ktorý nadväzuje Reforma Štandardizácia technických a procesných riešení kybernetickej a informačnej bezpečnosti (Plán obnovy a odolnosti).

Súčasťou každého dokumentu adaptovaného do prostredia organizácie je aj nasledovný zmenový list obsahujúci informácie minimálne v nasledovnom rozsahu:

|  |  |
| --- | --- |
| **Verzia** |  |
| **Garant dokumentu** |  |
| **Dátum poslednej revízie** |  |
| **Dátum vydania** |  |
| **Dátum účinnosti** |  |

# Úvod

Stratégia kybernetickej bezpečnosti (ďalej aj „Bezpečnostná stratégia“ alebo „tento dokument“) je východiskový strategický dokument, ktorý komplexne určuje strategický prístup organizácie k zabezpečovaniu kybernetickej bezpečnosti.

Stratégia kybernetickej bezpečnosti je vypracovaná v súlade s požiadavkami zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej aj „zákon o kybernetickej bezpečnosti“) a súvisiacich vykonávacích predpisov a obsahuje určenie:

1. bezpečnostných cieľov z hľadiska kybernetickej bezpečnosti,
2. spôsobu vyhodnocovania bezpečnostných cieľov, kritérií vyhodnocovania dosahovania bezpečnostných cieľov, spôsobov priebežného hodnotenia ich primeranosti a spôsobov kontroly postupov využívaných na dosahovanie bezpečnostných cieľov,
3. úloh štatutárneho orgánu prevádzkovateľa základnej služby pri zabezpečovaní kybernetickej bezpečnosti a vyhlásenie o záväzku o podpore kybernetickej bezpečnosti,
4. všeobecných a špecifických zodpovedností a povinností v oblasti kybernetickej bezpečnosti a určenie príslušných bezpečnostných rolí potrebných na riadenie kybernetickej bezpečnosti vrátane určenia rozsahov činností, kompetencií a úloh; rozdelenie rolí na riadiacu zložku, výkonnú zložku a kontrolnú zložku, pričom riadiaca zložka je priamo riadená prevádzkovateľom základnej služby a kontrolná zložka je nezlučiteľná so všetkými ostatnými zložkami,
5. základného rámca na riadenie aktív podľa § 6, od ktorých závisí činnosť sietí a informačných systémov,
6. základného rámca riadenia rizík podľa § 6 v súvislosti s aktívami, od ktorých závisí činnosť sietí a informačných systémov a určenie bezpečnostných opatrení podľa oblastí v zmysle § 20 ods. 3 zákona v závislosti od identifikovaných rizík,
7. rozsahu a periodicity overovania stavu kybernetickej bezpečnosti prostredníctvom auditu kybernetickej bezpečnosti vrátane zhodnotenia súladu bezpečnostnej stratégie a bezpečnostných politík s požiadavkami zákona, iného všeobecne záväzného právneho predpisu, vnútorných predpisov a zmluvnými záväzkami,
8. postupu a zodpovedností pri revízii bezpečnostnej dokumentácie schvaľovanej prevádzkovateľom základnej služby vrátane periodicity pravidelných revízií a jej aktualizácií po každej zmene majúcej na ňu vplyv, ako aj z dôvodov mimoriadnych revízií.

Stratégia kybernetickej bezpečnosti určuje ciele, ktoré je potrebné na základe výsledkov analýzy rizík kybernetickej bezpečnosti dosiahnuť (spolu s uvedením základných princípov na ich dosiahnutie) a určuje právomoci a zodpovednosti za riadenie kybernetickej bezpečnosti, riadenie rizík kybernetickej bezpečnosti a aktualizáciu bezpečnostnej dokumentácie.

Na základe tejto Bezpečnostnej stratégie sa prijíma Bezpečnostná politika kybernetickej bezpečnosti a ďalšie bezpečnostné politiky v rámci organizácie.

## Rozsah platnosti

Bezpečnostná stratégia kybernetickej bezpečnosti sa vzťahuje na všetky informácie, siete, informačné systémy a zamestnancov organizácie.

## Legislatívny a metodický rámec

### Legislatíva

Legislatívny rámec pre vypracovanie bezpečnostnej stratégie pozostáva z najmä z dokumentov uvedených v Bezpečnostnej politike kybernetickej bezpečnosti v rámci Prílohy č. 1.

### Strategické dokumenty

Strategickými dokumentmi, ktoré boli pri vytváraní bezpečnostnej stratégie adresované sú:

* Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,
* Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025,
* Národná stratégia pre informačnú bezpečnosť v Slovenskej republike,
* Systém vzdelávania v oblasti informačnej bezpečnosti v SR,
* Národná stratégia Slovenskej republiky pre digitálnu integráciu.

### Bezpečnostné štandardy

Východiskovými normami a štandardmi, z ktorých táto bezpečnostná stratégia vychádza sú:

* medzinárodná norma ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ku dňu prijatia tohto dokumentu nebol ešte vydaný slovenský preklad danej normy),
* medzinárodná norma ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls (ku dňu prijatia tohto dokumentu nebol ešte vydaný slovenský preklad danej normy),
* medzinárodná norma ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks (ku dňu prijatia tohto dokumentu nebol ešte vydaný slovenský preklad danej normy),
* medzinárodná norma STN ISO/IEC 27031 Informačné technológie. Bezpečnostné metódy. Návody pre pripravenosť informačných a komunikačných technológií na zabezpečenie kontinuity činnosti,
* medzinárodná norma STN EN ISO 22301 Ochrana spoločnosti. Systémy manažérstva kontinuity podnikania. Požiadavky,
* medzinárodná norma STN EN ISO 22313 Ochrana spoločnosti. Systémy manažérstva kontinuity podnikania. Usmernenie k používaniu normy ISO 22301.

# Bezpečnostné ciele z hľadiska kybernetickej bezpečnosti

## Piliere informačnej a kybernetickej bezpečnosti

Hlavnými piliermi informačnej a kybernetickej bezpečnosti sú:

* dôvernosť,
* integrita,
* dostupnosť.

Zákon o kybernetickej bezpečnosti definuje uvedené piliere nasledovne:

* dôvernosť – záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom,
* integrita – záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené,
* dostupnosť – záruka, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná.

## Strategické bezpečnostné ciele kybernetickej bezpečnosti

Hlavnými strategickými bezpečnostnými cieľmi z pohľadu kybernetickej bezpečnosti sú:

1. Informačná a kybernetická bezpečnosť ako základná súčasť DNA organizácie.
2. Dôveryhodná organizácia pripravená na hrozby.
3. Riadiť kybernetickú bezpečnosť v súlade s požiadavkami platnej legislatívy SR aj EÚ, medzinárodnými štandardmi.
4. Zabezpečovať primeranými technickými, organizačnými a personálnymi bezpečnostnými opatreniami ochranu dôvernosti, integrity a dostupnosti informačných aktív.
5. Zabezpečovať primeranými technickými, organizačnými a personálnymi opatreniami ochranu informácií v informačných systémoch, vrátanie osobných údajov pred odcudzením, nedostupnosťou, poškodením, neoprávneným prístupom, zmenou a rozširovaním.
6. Implementovať a udržiavať plán reakcie na kybernetické bezpečnostné incidenty.
7. Podieľať sa na zaistení kontinuity činností spoločnosti v prípade kybernetických bezpečnostných incidentov.
8. Zvyšovať povedomie o informačnej a kybernetickej bezpečnosti všetkých zamestnancov a vedenia.
9. Riadiť riziká kybernetickej bezpečnosti s cieľom implementovať efektívne opatrenia na ich minimalizáciu.
10. Zaistiť bezpečnú prevádzku a správu informačných systémov.
11. Zabezpečiť dôvernosť, dostupnosť a integritu najmä osobných údajov a iných dôležitých informačných aktív, fyzických a právnických osôb pri ich spracúvaní.
12. Minimalizácia finančných a iných strát súvisiacich s narušením prevádzky informačných systémov.
13. Zaistenie poskytovania služieb informačného systému užívateľom informačného systému v stanovenej kvalite a rozsahu aj pri neštandardných (havarijných) stavoch informačného systému.
14. Ochrana dobrého mena organizácie.

# Vyhodnocovanie bezpečnostných cieľov

V tejto kapitole sú uvedené požiadavky súvisiace s vyhodnocovaním bezpečnostných cieľov v štruktúre požadovanej vyhláškou Národného bezpečnostného úradu č. 362/2018 Z. z., ktorými sú:

* spôsob vyhodnocovania bezpečnostných cieľov,
* kritériá vyhodnocovania dosahovania bezpečnostných cieľov,
* spôsoby priebežného hodnotenia ich primeranosti,
* spôsoby kontroly postupov využívaných na dosahovanie bezpečnostných cieľov.

Spôsob vyhodnocovania bezpečnostných cieľov je uvedený v bode 4.1, ostatné náležitosti sú adresované v bode 4.2 tohto dokumentu.

## Spôsob vyhodnocovania bezpečnostných cieľov

Vyhodnocovanie bezpečnostných cieľov sa vykonáva dvojstupňovo. Vyhodnocovanie bezpečnostných cieľov vykonávajú nasledovné entity:

* bezpečnostný výbor,
* manažér kybernetickej a informačnej bezpečnosti.

Periodicita vyhodnocovania bezpečnostných cieľov je uvedená v nasledujúcej tabuľke:

|  |  |
| --- | --- |
| Entita | Frekvencia vyhodnocovania bezpečnostných cieľov |
| Bezpečnostná výbor | ročná báza |
| Manažér kybernetickej a informačnej bezpečnosti | štvrťročná báza |

Vyhodnocovanie bezpečnostných cieľov spočíva najmä v:

* odpočte plnenia už nastavených bezpečnostných cieľov (bod 3.2 tohto dokumentu),
* návrhu opatrení potrebných na dosiahnutie bezpečnostných cieľov v súlade so stanoveným plánom plnenia bezpečnostných cieľov,
* prehodnocovaní kritérií vyhodnocovania dosahovania bezpečnostných cieľov, spôsobov priebežného hodnotenia ich primeranosti, spôsobov kontroly postupov využívaných na dosahovanie bezpečnostných cieľov (vyžaduje sa súhlas Bezpečnostného výboru),
* prípadnej modifikácii bezpečnostných cieľov (vyžaduje sa súhlas bezpečnostného výboru),
* stanovovaní nových bezpečnostných cieľov (vyžaduje sa súhlas bezpečnostného výboru).

## Kritériá vyhodnocovania, spôsoby priebežného hodnotenia primeranosti a spôsoby kontroly postupov využívaných na dosahovanie bezpečnostných cieľov

Kritériá vyhodnocovania, spôsoby priebežného hodnotenia primeranosti a spôsoby kontroly postupov využívaných na dosahovanie bezpečnostných cieľov sú uvedené v prílohe tohto dokumentu.

# Úlohy štatutárneho orgánu a vyhlásenie o podpore pri zabezpečovaní kybernetickej bezpečnosti

## Úlohy štatutárneho orgánu pri zabezpečovaní kybernetickej bezpečnosti

Hlavnými úlohami vedenia v oblasti kybernetickej bezpečnosti je – prostredníctvom príslušných organizačných zložiek – zabezpečiť najmä:

* ochranu všetkých informačných aktív,
* funkčnosť bezpečnostného výboru,
* podporu plnenia úloh kybernetickej bezpečnosti presadzovaním bezpečnostnej stratégie kybernetickej bezpečnosti, politík, smerníc a ďalších interných predpisov súvisiacich s informačnou a kybernetickou bezpečnosťou,
* podporu kybernetickej bezpečnosti prostredníctvom vyčlenenia dostatočného objemu finančných prostriedkov určených na zabezpečenie plnenia úloh kybernetickej bezpečnosti,
* súlad so zákonom o kybernetickej bezpečnosti a súvisiacimi vykonávacími predpismi,
* súlad s ďalšími právnymi predpismi obsahujúcimi element informačnej a kybernetickej bezpečnosti,
* kontrolu dodržiavania pravidiel kybernetickej bezpečnosti.

Povinnosti z vyššie uvedených hlavných úloh sú delegované na jednotlivé organizačné útvary podľa kompetencií a zodpovedností stanovenými v organizačnom poriadku.

Na zabezpečenie dohľadu nad dodržiavaním kybernetickej bezpečnosti vedenie zriadilo bezpečnostný výbor.

V procese implementácie požiadaviek zákona o kybernetickej bezpečnosti a súvisiacich vykonávacích predpisov vedenie vymenovalo manažéra kybernetickej a informačnej bezpečnosti, ktorému udelilo povinnosti a právomoci súvisiace s definovaním, udržiavaním a dodržiavaním kybernetickej bezpečnosti v rámci organizácie.

## Vyhlásenie štatutárneho orgánu o záväzku o podpore kybernetickej bezpečnosti

Vedenie organizácie – rešpektujúc úlohy uvedené v bode 5.1 tohto dokumentu – schválením tejto bezpečnostnej stratégie kybernetickej bezpečnosti vyhlasuje plnú podporu zabezpečovaniu a rozvoju kybernetickej bezpečnosti.

# Riadenie kybernetickej bezpečnosti

Riadenie kybernetickej bezpečnosti sa realizuje prijímaním bezpečnostných opatrení najmä v týchto oblastiach:

* organizácia informačnej bezpečnosti,
* riadenie aktív, hrozieb a rizík,
* personálna bezpečnosť,
* riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,
* technické zraniteľnosti systémov a zariadení,
* riadenie bezpečnosti sietí a informačných systémov,
* riadenie prevádzky,
* riadenie prístupov,
* kryptografické opatrenia,
* riešenie kybernetických bezpečnostných incidentov,
* monitorovanie, testovanie bezpečnosti a bezpečnostné audity,
* fyzická bezpečnosť a bezpečnosť prostredia,
* riadenie kontinuity procesov.

Bezpečnostnými opatreniami podľa zákona o kybernetickej bezpečnosti sú:

* úlohy,
* procesy,
* role a
* technológie.

v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov.

Bezpečnostné opatrenia realizované v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti sa prijímajú s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovaných IT služieb.

Bezpečnostné opatrenia prijímané zo strany organizácie sú:

* všeobecné,
* realizované v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov,
* v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti pre všetky siete a informačné systémy, ktoré sa realizujú na základe špecifík kategorizácie sietí a informačných systémov,
* v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti.

Bezpečnostné opatrenia prijímané v rámci organizácie zahŕňajú najmenej:

* detekciu kybernetických bezpečnostných incidentov,
* evidenciu kybernetických bezpečnostných incidentov,
* postupy riešenia a riešenie kybernetických bezpečnostných incidentov,
* určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,
* pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania.

Bezpečnostné opatrenia sa vždy prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá je aktuálna a zodpovedá reálnemu stavu.

## Všeobecné zodpovednosti a povinnosti v oblasti kybernetickej bezpečnosti

Všeobecné zodpovednosti a povinnosti v oblasti kybernetickej bezpečnosti sa vzťahujú na všetkých zamestnancov organizácie a tretie strany, ktoré sú s organizáciou v obchodnom alebo inom vzťahu.

Všeobecnými zodpovednosťami a povinnosťami v oblasti kybernetickej bezpečnosti sú najmä:

* dodržiavanie všetkých povinností vyplývajúcich z platnej bezpečnostnej dokumentácie,
* dodržiavanie zásady najnižších privilégií („need to know“), podľa ktorej sú každému používateľovi obmedzené privilégiá v maximálnom rozsahu potrebnom na splnenie pridelených úloh,
* dodržiavanie oddeľovania zodpovedností, podľa ktorej žiaden používateľ nemá oprávnenie pristupovať, upravovať alebo používať aktíva prevádzkovateľa základnej služby bez autorizácie alebo overenia identity,
* rešpektovanie jasného vymedzenia právomoci, povinnosti a zodpovednosti, ktoré sú súčasťou pracovnej náplne alebo obdobného opisu pracovných činností,
* dodržiavanie požiadavky „čistého stola“, t. j. odkladanie dokumentov a médií s citlivými údajmi do vyhradených uzamykateľných priestorov po ukončení práce alebo pracovnej doby,
* aktívne zvyšovanie bezpečnostného povedomia aktívnou účasťou na vzdelávacom programe.

## Špecifické zodpovednosti a povinnosti v oblasti kybernetickej bezpečnosti

Špecifickými zodpovednosťami a povinnosťami v oblasti kybernetickej bezpečnosti sa rozumejú také zodpovednosti a činnosti, ktoré realizujú roly zodpovedné za riadenie a výkon kybernetickej bezpečnosti.

Medzi špecifické zodpovednosti a povinnosti v oblasti kybernetickej bezpečnosti patria najmä:

* uplatňovanie zásady dodržiavania a vykonávania nezávislého hodnotenia, merania a preskúmavania efektivity a účinnosti prijatých opatrení na ošetrenie rizík,
* zabezpečovanie manažmentu digitálnej identity zamestnancov a technických zariadení,
* zabezpečovanie monitorovania prevádzky informačných systémov,
* zabezpečovanie ochrany informačných a komunikačných systémov pred počítačovými a ľudskými infiltráciami, spywarom a spamom,
* zabezpečovanie zálohovania a archivácie údajov v elektronickej podobe,
* zabezpečovanie konfiguračného a zmenového manažmentu, distribúciu opráv a servisných balíkov pre operačné systémy a aplikácie,
* zabezpečovanie riešenia bezpečnostných incidentov (incident handling) a chybových stavov s prepojením na ServiceDesk,
* vykonávanie bezpečnostnej klasifikácie všetkých systémov a aplikácií v súlade s požiadavkami platných právnych predpisov SR,
* určenie minimálnej úrovne bezpečnosti pre jednotlivé kategórie systémov, údajov a dokumentov podľa schválenej klasifikačnej schémy (vrátane outsorcovaných systémov),
* priradenie vlastníctva k všetkým informačným a komunikačným aktívam organizácie – systémom a aplikáciám – v zmysle určenia zodpovednosti konkrétnych osôb za správu a riadenie príslušných aktív,
* zabezpečovanie obstarávania takých bezpečnostných subsystémov a zariadení, ktoré umožňujú ich integráciu do väčších bezpečnostných systémov a spĺňajú medzinárodné normy a štandardy,
* implementácia bezpečnosti počas celého životného cyklu prevádzkových a informačných subsystémov a objektov, už od etapy špecifikácie a zadania,
* zabezpečovanie posúdenia nového informačného systému pred uvedením do prevádzky organizačným útvarom zodpovedným za kybernetickú bezpečnosť,
* budovanie nových informačných systémov tak, aby umožňovali vytváranie záznamov o svojej bezpečnostne relevantnej činnosti na účely bezpečnostného auditu,
* vykonávanie pravidelného testovania funkčnosti implementovaných bezpečnostných prvkov, zariadení a subsystémov,
* udržiavanie bezpečnostnej dokumentácie takým spôsobom, aby bola aktuálna a zodpovedala reálnemu stavu,
* vypracovanie plánov kontinuity činností pre všetky kritické informačné a komunikačné systémy,
* vykonávanie analýzy rizík najmenej pre kritické informačné a komunikačné systémy,
* vykonávanie pravidelného bezpečnostného auditu prevádzkovaných (vrátane outsorcovaných) informačných a komunikačných systémov a služieb,
* oddeľovanie:
* prevádzkových rolí od bezpečnostných rolí,
* výkonných rolí od kontrolných rolí,
* zabezpečovanie, aby prostriedky vynakladané na bezpečnosť informačných a komunikačných systémov boli úmerné rizikám, ktoré sa ich využitím majú eliminovať,
* zvyšovanie bezpečnostného povedomia používateľov informačných a komunikačných systémov v rámci vzdelávacieho programu.

## Určenie bezpečnostných rolí potrebných na riadenie kybernetickej bezpečnosti

Bezpečnostné roly potrebné na riadenie kybernetickej bezpečnosti sa rozdeľujú na tieto zložky:

* riadiacu,
* výkonnú,
* kontrolnú.

Nižšie v texte sú uvedené rozsahy činností, kompetencií a úloh jednotlivých rolí.

### Riadiaca zložka

Za koncepčné a metodické riadenie kybernetickej a informačnej bezpečnosti je zodpovedné vedenie organizácie. V prípade, že má organizácia zriadený bezpečnostný výbor, tak môže túto úlohu zveriť tomuto výboru.

Vedenie organizácie, príp. bezpečnostný výbor, rieši a vyjadruje sa najmä k:

* strategickým otázkam týkajúcich oblasti kybernetickej a informačnej bezpečnosti,
* výkonnosti organizácie v plnení strategických bezpečnostných cieľov vzhľadom na výkonnostný rámec stanovený v Bezpečnostnej stratégii kybernetickej bezpečnosti,
* pokroku dosiahnutému pri plnení bezpečnostných cieľov v oblasti kybernetickej a informačnej bezpečnosti,
* realizácii komunikačnej stratégie týkajúcej sa kybernetickej a informačnej bezpečnosti dovnútra organizácie,
* realizácii projektov v oblasti kybernetickej a informačnej bezpečnosti,
* dosiahnutému pokroku v rámci realizácie projektov a opatreniam na presadzovanie udržateľného rozvoja kybernetickej a informačnej bezpečnosti v rámci organizácie,
* pokroku v implementácii bezpečnostných opatrení kybernetickej a informačnej bezpečnosti v organizačnej, personálnej a technickej oblasti,
* k ročnému indikatívnemu plánu projektov kybernetickej a informačnej bezpečnosti a bezpečnostných opatrení kybernetickej a informačnej bezpečnosti v organizačnej, personálnej a technickej oblasti,
* následným úlohám a opatreniam prijatým vzhľadom na zistenia hodnotení,
* všetkým závažným kybernetickým bezpečnostným incidentom v organizácii,
* rozširovaniu bezpečnostných opatrení pre potreby zabezpečenia kybernetickej a informačnej bezpečnosti,
* plánu vzdelávania zamestnancov zameraného na kybernetickú a informačnú bezpečnosť,
* účinnosti prijatých bezpečnostných opatrení,
* vykonávaniu auditov kybernetickej bezpečnosti,
* obsahu zmlúv s externými subjektmi a odsúhlasuje ich obsah z hľadiska požiadaviek kybernetickej a informačnej bezpečnosti.

### Výkonná zložka

**Manažér kybernetickej a informačnej bezpečnosti**

Rola manažéra kybernetickej a informačnej bezpečnosti má oporu v § 5 vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z.

Rola manažéra kybernetickej a informačnej bezpečnosti má oporu v § 5 vyhlášky NBÚ č. 362/2018 Z. z., ktorý stanovuje obsah bezpečnostných opatrení pre oblasť podľa § 20 ods. 3 písm. a) zákona o kybernetickej bezpečnosti.

Manažér kybernetickej a informačnej bezpečnosti je zodpovedný za predchádzanie kybernetickým bezpečnostným incidentom a minimalizovanie vplyvu kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania služieb organizácie.

Manažér kybernetickej a informačnej bezpečnosti musí spĺňať znalostné štandardy na funkciu manažéra kybernetickej a informačnej bezpečnosti a musí byť nezávislý od riadenia prevádzky a vývoja IT služieb.

Profil manažéra kybernetickej a informačnej bezpečnosti je zhrnutý v tabuľke nižšie (z neho sú potom vyvodené jeho zodpovednosti a právomoci).

|  |  |
| --- | --- |
| Oblasť | Charakteristika |
| Mandát | Zodpovednosť za operatívne riadenie oblasti kybernetickej bezpečnosti |
| Rozsah činnosti / zodpovednosť | Riadenie oblasti kybernetickej bezpečnosti a jej monitorovanie pre všetky IS v správe organizácie ako poskytovateľa základnej služby |
| Rozhodovacie právomoci | Návrh odporúčaní a konceptov pre implementáciu dostatočných kontrolných mechanizmov a procesov pre oblasť riadenia a monitorovania kybernetickej bezpečnosti |
| Eskalácia / reportovanie | Manažér kybernetickej a informačnej bezpečnosti reportuje a eskaluje prípadné problémy priamo bezpečnostnému výboru / vedeniu organizácie |

Manažér kybernetickej a informačnej bezpečnosti najmä:

* spolupracuje pri príprave východiskového strategického dokumentu, ktorý určuje prístup k zabezpečovaniu kybernetickej bezpečnosti, t. j. dokumentu „Stratégia kybernetickej bezpečnosti“ a zodpovedá za jej pravidelnú revíziu a aktualizáciu,
* spolupracuje na vyhodnocovaní bezpečnostných cieľov v súlade a v periodicite definovanej dokumentom „Stratégia kybernetickej bezpečnosti“,
* tvorí návrhy politík, smerníc a pravidiel pre oblasť kybernetickej bezpečnosti,
* spolupracuje na príprave rozpočtu pre kybernetickú bezpečnosť,
* spolupracuje pri analýze rizík a pri jej aktualizácii (riziká týkajúce sa kybernetickej bezpečnosti),
* v rámci procesu klasifikácie a evidencie informácii posudzuje odôvodnenia spracovateľov informácií a odsúhlasuje zverejnenie informácií v súlade so zákonom č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov),
* predkladá návrhy a oznamuje informácie v oblasti kybernetickej bezpečnosti priamo bezpečnostnému výboru / vedeniu organizácie,
* spolupracuje pri implementácii nových technických riešení (IT architektúra, riadenie zmien, riadenie projektov a pod.) z pohľadu vplyvu na oblasť kybernetickej bezpečnosti,
* dohliada na prijímanie, dodržiavanie a preverovanie účinnosti prijatých opatrení v oblasti kybernetickej bezpečnosti,
* spolupracuje pri uzatváraní zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona o kybernetickej bezpečnosti s externým dodávateľom, ktorý poskytuje služby týkajúce sa vývoja, implementácie a prevádzky IS v správe organizácie,
* vykonáva pravidelné audity kybernetickej bezpečnosti v zmysle legislatívnych alebo interných plánov, prípadne vykonáva mimoriadne audity podľa potreby (napr. v prípade podozrenia na kybernetický bezpečnostný incident),
* zaisťuje, že ak dôjde ku kybernetickým bezpečnostným incidentom alebo narušeniu dôvernosti, integrity alebo dostupnosti informačných aktív, tieto incidenty sa vyriešia pohotovo a účinne v budú ohlásené v súlade s platnou legislatívou,
* zaisťuje, že budú prijaté opatrenia minimalizujúce možnosť opakovania kybernetických bezpečnostných incidentov.

Manažér kybernetickej a informačnej bezpečnosti taktiež spolupracuje s inými útvarmi v nasledovných oblastiach:

* vyšetrovanie a forenzné analýzy,
* sociálne a personálne aspekty (napr. tzv. „background checks“),
* IT architektúra (najmä z pohľadu kybernetickej bezpečnosti),
* bezpečnostné nástroje,
* kontroly plnenia bezpečnostných opatrení,
* riadenie prístupových práv,
* riadenie zmien a projektov,
* konfiguračný manažment,
* riadenie rizík v oblasti kybernetickej bezpečnosti, identifikácia možných dopadov relevantných hrozieb a pravdepodobnosti ich uplatnenia,
* analýzy funkčného dopadu,
* riadenie vzťahov s dodávateľmi v kontexte dodržiavania pravidiel kybernetickej bezpečnosti,
* stanovovanie a kontrola dodržiavania pravidiel kybernetickej bezpečnosti zo strany zamestnancov a dodávateľov,
* zvyšovanie povedomia o kybernetickej bezpečnosti a zaškoľovanie/preškoľovanie všetkých zamestnancov a dodávateľov,
* inovácie v oblasti kybernetickej bezpečnosti,
* atď.

Manažér kybernetickej a informačnej bezpečnosti je ďalej povinný:

* aktívne spolupracovať s bezpečnostným výborom a plniť úlohy predsedu bezpečnostného,
* pravidelne reportovať stav a výkonnosť kybernetickej bezpečnosti bezpečnostnému výboru / vedeniu organizácie,
* riadiť riešenie kybernetických bezpečnostných incidentov,
* bezodkladne hlásiť závažný kybernetický bezpečnostný incident prostredníctvom jednotného informačného systému kybernetickej bezpečnosti,
* spolupracovať s Národným bezpečnostným úradom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj vlastné informácie dôležité pre riešenie kybernetického bezpečnostného incidentu,
* v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,
* oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka,
* oznámiť a preukázať Národnému bezpečnostnému úradu vykonanie reaktívneho opatrenia a jeho výsledok, v prípade ak bolo prijaté reaktívne opatrenie,
* informovať v nevyhnutnom rozsahu tretiu stranu o hlásenom kybernetickom bezpečnostnom incidente za predpokladu, že by sa plnenie zmluvy s treťou stranou stalo nemožným.

Manažér kybernetickej a informačnej bezpečnosti má právo od iných organizačných útvarov žiadať:

* doplňujúce informácie,
* logy,
* akúkoľvek súvisiacu podpornú dokumentáciu,
* umožnenie kontroly dodržiavania prijatých bezpečnostných opatrení kybernetickej bezpečnosti.

Manažér kybernetickej a informačnej bezpečnosti je nezávislý od riadenia prevádzky a vývoja služieb informačných technológií.

**Administrátor informačných systémov**

Primárnou zodpovednosťou administrátora informačných systémov je zabezpečenie správneho a bezporuchového chodu informačných systémov.

**Vedúci zamestnanec**

Vedúci zamestnanci sú do roly zaradení na základe funkcií, ktoré vykonávajú.

Medzi hlavné činnosti vykonávané pracovníkom zaradeným do tejto roly patria:

* zodpovednosť za definovanie pravidiel pre narábanie s údajmi patriacimi do pôsobnosti tejto roly,
* určenie vlastníkov procesov v oblasti jeho pôsobnosti,
* kompetenčná zodpovednosť za zabezpečenie spracovania a zaistenie primeranej úrovne ochrany údajov, ktoré sú v spoločnosti spracovávané a patria do pôsobnosti tejto roly,
* zodpovednosť za riadenie procesov z oblasti jej pôsobnosti,
* zabezpečenie spracovania údajov v rámci týchto procesov v súlade s platnými pravidlami pre narábanie s údajmi,
* výkon kontrolných činností v procesoch z oblasti jeho pôsobnosti.

**Používateľ**

Používateľ je rola, ktorá využíva informačné a komunikačné aktíva na plnenie jemu pridelených úloh.

**Osoba zodpovedná za ochranu osobných údajov**

Osoba určená zo strany organizácie vykonávať dohľad nad ochranou osobných údajov.

### Kontrolná zložka

Kontrolná zložka je nezlučiteľná so všetkými ostatnými zložkami, t. j. s riadiacou a výkonnou.

Za kontrolnú zložku táto bezpečnostná stratégia určuje nasledovné subjekty:

* organizačný útvar, do ktorého kompetencie spadá výkon kontroly,
* organizačný útvar, do ktorého kompetencie spadá výkon interného auditu,
* iná osoba poverená vedením organizácie na výkon kontrolnej činnosti.

Interný audítor alebo iný zamestnanec poverený kontrolnou činnosťou v kontexte kybernetickej a informačnej bezpečnosti predovšetkým:

* vykonáva kontroly, overovania a analýzy dodržiavania stanovených postupov, procedúr a predpisov v jednotlivých procesoch kybernetickej a informačnej bezpečnosti,
* stanovuje metodológiu výkonu kontrol/interného auditu,
* pripravuje plán kontrol/interného auditu,
* identifikuje a analyzuje príčiny neefektívnych/nehospodárnych postupov,
* navrhuje zmeny,
* hodnotí funkčnosť a účinnosť riadenia kybernetickej a informačnej bezpečnosti v organizácii,
* hodnotí systém riadenia rizík, dostupnosti a spoľahlivosti informácii,
* hodnotí súlad so zákonmi, všeobecne platnými právnymi normami a vnútornými predpismi,
* vedie dokumentáciu o vykonaných kontrolách/auditoch.

# Základný rámec na riadenie aktív

V tejto kapitole bezpečnostnej stratégie je popísaný rámec pre riadenie aktív.

Riadenie aktív, hrozieb a rizík je proces spojený s finančnými, zmluvnými a inventarizačnými funkciami na podporu riadenia životného cyklu informačných technológií a konfiguračných položiek.

Účelom riadenia aktív, hrozieb a rizík je zabezpečiť ochranu aktív podľa ich hodnoty.

Rámec pre riadenie aktív pozostáva z týchto hlavných činností:

* identifikácie a evidencia aktív,
* klasifikácie informácií a kategorizácie sietí a informačných systémov.

## Identifikácia a evidencia aktív

Všetky aktíva súvisiace so zariadeniami na spracovanie informácií a informačnými prostriedkami musia byť v rámci spoločnosti identifikované a inventár týchto aktív musí byť centrálne zaznamenaný a riadený.

Riadenie aktív musí pozostávať z identifikácie a evidencie všetkých:

* aktív, od ktorých závisí poskytovanie základnej služby,
* podporných služieb, prostredníctvom ktorých sa zabezpečuje kontinuita základnej služby a jej poskytovanie,
* zodpovedných osôb za identifikáciu a evidenciu aktív,
* vlastníkov aktív.

V rámci riadenia aktív musí byť zabezpečené, že po ukončení pracovného pomeru alebo iného obdobného pracovného vzťahu zamestnancov organizácie a zamestnancov tretích strán sa zadokumentovaným spôsobom vracajú späť všetky zverené aktíva.

## Klasifikácia informácií a kategorizácia sietí a informačných systémov

Rovnaká ochrana sa neuplatňuje pre všetky druhy aktív. Na tento účel sa aktíva klasifikujú a kategorizujú postupom podľa rámca popísaného nižšie.

Klasifikácia informácií a kategorizácia sietí a informačných systémov reflektuje požiadavky kybernetickej bezpečnosti počas celého životného cyklu informácií, siete a informačného systému, a to najmä vo fáze:

* špecifikácie, ako definície požiadaviek a potrieb vedúcich k rozhodnutiu o vzniku informačného systému alebo akéhokoľvek spracúvania informácií,
* návrhu procesu, systému alebo dátovej štruktúry,
* vývoja systému alebo spôsobu spracúvania informácií,
* implementácie systému ako inštalácie, nasadenia, zavedenia alebo oživenia systému, alebo začatia procesu spracúvania informácií,
* prevádzky procesu ako štandardného využívania a údržby systému a údržby informácií,
* zmeny existujúceho, bežiaceho systému alebo spracúvania informácií, rozvoja a inovácie spracúvania podľa aktuálnych potrieb,
* nahradenia systému alebo procesu spracúvania informácií novým systémom alebo procesom,
* vyradenia ako ukončenia procesu spracúvania informácií alebo vyňatia systému z prevádzky.

Informácia sa klasifikuje bez ohľadu na jej formát, spôsob uloženia, systémy, aplikácie alebo nástroje, v ktorých sa nachádza alebo prostredníctvom ktorých sa informácia spracúva alebo prostredníctvom ktorých je prenášaná.

### Klasifikácia informácií

Informácie sa vytvárajú, spracúvajú a ukladajú tak, že ich kvalita a spoľahlivosť je primeraná ich klasifikačnému stupňu.

Každá klasifikovaná informácia má pridelený jeden klasifikačný stupeň dôvernosti, jeden klasifikačný stupeň integrity a jeden klasifikačný stupeň dostupnosti. Bezpečnostné informácie, nastavenia, postupy, smernice a ostatné úkony ohľadom riadenia aktív sa klasifikujú rovnakým alebo vyšším klasifikačným stupňom, akým sú označené informačné aktíva, ktorých riadenie opisujú.

Pri klasifikácii informácií sa uplatňuje odstupňovaný prístup tak, že do nižších úrovní sú zahrnuté také informácie, pri ktorých sú najnižšie nároky na dôvernosť, integritu, dostupnosť a zodpovednosť vrátane zabezpečovania kvality. Informácie sa vytvárajú, spracúvajú a ukladajú tak, že ich kvalita a spoľahlivosť je primeraná ich klasifikačnému stupňu.

Klasifikačné stupne opisujú citlivosť informácií, údajov alebo ďalších s nimi spojených informačných aktív a odrážajú dôležitosť alebo hodnotu týchto aktív z pohľadu narušenia ich:

* dôvernosti,
* integrity,
* dostupnosti.

**Klasifikácia informácií z hľadiska dôvernosti**

Z hľadiska dôvernosti sú klasifikačné stupne informačných aktív definované ako:

1. verejné,
2. interné,
3. chránené,
4. prísne chránené.

Ak nie je informačné aktívum explicitne klasifikované je považované za interné.

**Klasifikácia informácií z hľadiska integrity**

Z hľadiska integrity sú klasifikačné stupne informačných aktív definované ako:

1. nízka,
2. stredná,
3. vysoká.

**Klasifikácia informácií z hľadiska dostupnosti**

Z hľadiska dostupnosti sú klasifikačné stupne informačných aktív definované ako:

1. nízka
2. stredná,
3. vysoká.

### Kategorizácia sietí a informačných systémov

Kategorizácia sietí a informačných systémov je založená na klasifikácii informácií.

Kategorizácia sietí a informačných systémov sa vykonáva pre každú sieť a informačný systém vytvorením zoznamu vybraných komponentov sietí a informačných systémov, ktorý identifikuje jednotlivé siete a informačné systémy, ich podporné systémy a podsystémy s uvedením ich bezpečnostnej funkcie a zaradenia do príslušných bezpečnostných kategórií.

Zoznam komponentov sietí a informačných systémov identifikujúci jednotlivé siete a informačné systémy sa skladá z textovej, tabuľkovej a grafickej časti tak, že sú jednoznačne definované:

* hranice vybranej siete a informačného systému,
* rozhrania medzi definovanými hranicami,
* bezpečnostné funkcie komponentov, ktoré majú byť zahrnuté v posudzovaní úrovne bezpečnosti,
* požiadavky príslušných regulačných požiadaviek a technických noriem alebo iných vecne obdobných postupov a metód na ich:
* projektovanie,
* vytváranie,
* implementáciu,
* kontrolu.

Siete a informačné systémy tvoriace hranicu medzi rôznymi bezpečnostnými kategóriami v bezpečnostnom systéme sa zaraďujú do vyššej bezpečnostnej kategórie.

Kategorizácia sietí a informačných systémov zohľadňuje, že zlyhanie siete alebo informačného systému v ľubovoľnej bezpečnostnej úrovni nespôsobí zlyhanie vybranej siete a informačného systému zaradeného do bezpečnostnej úrovne s vyššou kategóriou. Pomocné siete a informačné systémy a podsystémy, ktoré pomáhajú funkciám vybraných informačných systémov, musia byť zaradené do príslušnej bezpečnostnej kategórie s ohľadom na zaradenie nadradeného systému.

V rámci organizácie sa rozoznávajú tri kategórie sietí a informačných systémov:

* kategória I,
* kategória II,
* kategória III.

# Základný rámec riadenia rizík

Základný rámec na riadenie rizík pozostáva z týchto hlavných činností:

* identifikácie zraniteľností,
* identifikácie hrozieb,
* identifikácie a analýzy rizík s ohľadom na aktívum,
* určenia vlastníka rizika,
* implementácie bezpečnostných opatrení v závislosti od identifikovaných rizík vrátane informácie, ktoré bezpečnostné opatrenia sú implementované a ktoré bezpečnostné opatrenia nie sú implementované spolu s odôvodnením,
* analýzy funkčného dopadu,
* pravidelného preskúmavania identifikovaných rizík a v závislosti od toho aktualizácie prijatých bezpečnostných opatrení.

## Identifikácia zraniteľností

Okruh potenciálnych zraniteľností, ktorý bude v rámci rámca riadenia rizík spoločnosti uvažovaný je uvedený v prílohe D medzinárodnej normy ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks (ku dňu prijatia tohto dokumentu nebol ešte vydaný slovenský preklad danej normy). V rámci analýzy rizík však môže byť okruh zraniteľností rozšírený.

Zraniteľnosti je možné v závislosti od ich typu principiálne rozdeliť do týchto oblastí:

* organizačné,
* procesné,
* zraniteľnosti súvisiace s manažérskymi procesmi,
* personálne,
* zraniteľnosti súvisiace s fyzickou bezpečnosťou,
* konfiguračné,
* zraniteľnosti súvisiace s hardvérom, softvérom a komunikačnými rozhraniami,
* zraniteľnosti súvisiace so závislosťou na tretích stranách.

## Identifikácia hrozieb

Pre potreby analýzy rizík vykonávanej v organizácii sa zoznam hrozieb združuje do jednotlivých skupín tak, že je:

* možné tento zoznam použiť univerzálne pre väčšinu aktív,
* pre jednotlivé aktíva sú hodnotené len hrozby relevantné pre konkrétne aktívum.

Hrozby sa rozdeľujú podľa ich pôvodu do kategórií najmenej ako:

* úmyselné hrozby pre všetky úmyselné aktivity zamerané na aktíva,
* náhodné hrozby pre všetky ľudské činnosti, ktoré môžu náhodne poškodiť aktíva,
* hrozby spôsobené vplyvom prostredia pre všetky udalosti, ktoré vznikajú nezávisle od ľudskej činnosti.

## Identifikácia a analýza rizík s ohľadom na aktívum

Identifikácia rizika sa vykonáva na základe princípu najhoršieho scenára, ktorý môže nastať aj pri nízkej pravdepodobnosti. Na určenie úrovne identifikovaného rizika má vopred nastavený súbor pravidiel, ktoré umožnia na základe štandardných a opakovateľných postupov určiť merateľné a objektívne úrovne rizika pre najhoršie scenáre.

Analýzou rizík sa určuje pravdepodobnosť vzniku škodlivej udalosti, ktorá môže byť spôsobená zneužitím existujúcej zraniteľnosti aktíva potenciálnou hrozbou v spojitosti s existujúcimi bezpečnostnými opatreniami a identifikáciou dopadov pri narušení:

* dôvernosti,
* integrity,
* dostupnosti aktíva.

Identifikácia a analýza rizík sa musí vykonávať v pravidelných intervaloch alebo aj mimoriadne, ak:

* vzíde požiadavka na jej aktualizáciu,
* pri zásadných zmenách v štruktúre,
* pri zásadných zmenách v legislatíve Slovenskej republiky, s vplyvom na požiadavky na proces analýzy rizík.

## Určenie vlastníka rizika

Vlastníkom rizika je úsek, ktorý:

* disponuje relevantnými informáciami a poznaním aktíva, na ktoré sa vzťahuje konkrétne riziko,
* sa hlási k vlastníctvu identifikovaného rizika,
* má majoritný záujem na mitigácii rizika.

## Implementácia bezpečnostných opatrení v závislosti od identifikovaných rizík

Implementácii organizačných a technických opatrení musí vždy predchádzať ich návrh.

Návrhu organizačných a technických opatrení vždy predchádza identifikácia zraniteľností (bod 8.1), identifikácia hrozieb (bod 8.2) a identifikácia a analýza rizík s ohľadom na aktívum (bod 8.3).

V závislosti od identifikovaných rizík budú navrhnuté organizačné, personálne alebo technické bezpečnostné opatrenia, ktoré je možné rozdeliť do nasledovných kategórií:

* úlohy,
* procesy,
* role,
* technológie.

Po schválení návrhu, zabezpečení personálnych a finančných kapacít na ich realizáciu sa môžu tieto bezpečnostné opatrenia implementovať.

Pokiaľ ide o opatrenia technického charakteru, vždy sa postupuje podľa nasledovného rámcového postupu:

* vývoj/zakúpenie softvérového/hardvérového vybavenia (ďalej súhrnne aj „technické vybavenie“),
* otestovanie technického vybavenia a schválenie nasadenia do pilotnej prevádzky,
* nasadenie technického vybavenia do pilotnej prevádzky a schválenie nasadenia do produkčnej prevádzky,
* nasadenie technického vybavenia do produkčnej prevádzky.

## Analýza funkčného dopadu

Súčasťou riadenia aktív, hrozieb a rizík je aj analýza funkčného dopadu, ktorá pozostáva z hodnotenia dopadu na činnosť organizácie spôsobeného krízovým scenárom, ktorý môže:

* zasiahnuť zdroje a aktíva podporujúce procesy,
* spôsobiť ohrozenie alebo narušenie kontinuity poskytovanej základnej služby.

## Pravidelné preskúmavanie identifikovaných rizík

Základný rámec pre preskúmavanie rizík možno z pohľadu činností zadefinovať nasledovne:

* dôkladné preskúmanie identifikovaných rizík,
* sledovanie a vyhodnocovanie zmien vnútorného a vonkajšieho prostredia s potenciálnym vplyvom na IT prostredie,
* pravidelné posudzovanie účinnosti navrhovaných bezpečnostných opatrení,
* vytvorenie zoznamu existujúcich a plánovaných bezpečnostných opatrení vo vzťahu k aktívam, využitím predchádzajúcich ohodnotení bezpečnosti a krátkodobých príp. dlhodobých plánov rozvoja bezpečnosti IT prostredie,
* návrh nových organizačných a bezpečnostných opatrení (implementácia opatrení bude realizovaná podľa bodu 8.5 tejto bezpečnostnej stratégie),
* aktualizácia prijatých bezpečnostných opatrení.

# Rozsah a periodicita overovania stavu kybernetickej bezpečnosti

V rámci overovania stavu kybernetickej bezpečnosti v rámci organizácie sa posudzuje najmä súlad bezpečnostnej stratégie kybernetickej bezpečnosti a bezpečnostných politík s požiadavkami:

* zákona,
* vnútorných predpisov,
* zmluvných záväzkov.

Za účelom overovania stavu kybernetickej bezpečnosti sú využívané tieto nástroje:

* audit kybernetickej bezpečnosti v zmysle § 29 zákona o kybernetickej bezpečnosti,
* interné preverovanie kybernetickej bezpečnosti v rámci organizácie.

## Audit kybernetickej bezpečnosti

Schválením tejto bezpečnostnej stratégie deklaruje, že sa podrobí auditu kybernetickej bezpečnosti v zmysle § 29 zákona o kybernetickej bezpečnosti (ďalej aj „audit“), ktorého cieľom je preverenie účinnosti prijatých bezpečnostných opatrení a plnenia požiadaviek stanovených zákonom o kybernetickej bezpečnosti.

Organizácia je povinná preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených zákonom o kybernetickej bezpečnosti vykonaním auditu kybernetickej bezpečnosti v rozsahu stanovenom podľa všeobecne záväzného právneho predpisu, ktorý vydá úrad, a to v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov po každej zmene majúcej významný vplyv na realizované bezpečnostné opatrenia a v určenom časovom intervale.

Audit kybernetickej bezpečnosti vykonáva certifikovaný audítor kybernetickej bezpečnosti, ktorým je fyzická osoba, spoločník, štatutárny orgán alebo zamestnanec právnickej osoby.

Organizácia si je vedomá povinnosti predložiť záverečnú správu o výsledkoch auditu Národnému bezpečnostnému úradu spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu.

## Interné preverovanie kybernetickej bezpečnosti

Interné preverovanie kybernetickej bezpečnosti je realizované prostredníctvom interného auditu, ktorého rozsah určuje príslušná organizačná zložka, do kompetencie ktorej spadá výkon interného auditu.

Interné preverovanie kybernetickej bezpečnosti v rámci sa realizuje minimálne raz ročne.

# Revízia bezpečnostnej stratégie

Bezpečnostná stratégia kybernetickej bezpečnosti sa reviduje a aktualizuje najmenej raz ročne.

Bezpečnostná stratégia kybernetickej bezpečnosti sa aktualizuje aj častejšie, ak:

* vzíde požiadavka na jej aktualizáciu ,
* pri zásadných zmenách v organizácii a štruktúre,
* pri zásadných zmenách v legislatíve Slovenskej republiky, s vplyvom na niektorú oblasť tejto bezpečnostnej stratégie.

Za pravidelnú revíziu a aktualizáciu bezpečnostnej stratégie kybernetickej bezpečnosti zodpovedá manažér kybernetickej a informačnej bezpečnosti.

Bezpečnostnú stratégiu kybernetickej bezpečnosti a všetky jej aktualizácie schvaľuje vedenie organizácie.

#

# Prílohy

## Kritériá vyhodnocovania, spôsoby priebežného hodnotenia primeranosti a spôsoby kontroly postupov využívaných na dosahovanie bezpečnostných cieľov

Dosiahnutie cieľov bezpečnostnej stratégie kybernetickej bezpečnosti bude vyhodnocované na základe nasledujúcich kritérií:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| P. č. | Bezpečnostný cieľ | Kritérium na vyhodnocovanie dosahovania bezpečnostného cieľa | Spôsob priebežného hodnotenia primeranosti cieľov | Spôsob kontroly postupov |
| 1 | Zabezpečovať primeranými technickými, organizačnými a personálnymi bezpečnostnými opatreniami ochranu dôvernosti, integrity a dostupnosti informačných aktív | Početnosť a účinnosť prijatých bezpečnostných opatrení | Spôsoby určuje vedenie organizácie a manažér kybernetickej bezpečnosti | Vyhodnocovanie početnosti a účinnosti prijatých bezpečnostných opatrení |
| 2 | Zvyšovať povedomie o informačnej a kybernetickej bezpečnosti všetkých zamestnancov a vedenia organizácie prostredníctvom rozvoja vzdelávania v oblasti kybernetickej a informačnej bezpečnosti | Úroveň povedomia o kybernetickej a informačnej bezpečnosti všetkých zamestnancov a vedenia organizácie | Spôsoby určuje vedenie organizácie a manažér kybernetickej bezpečnosti | Pravidelné preverovanie úrovne povedomia o kybernetickej a informačnej bezpečnosti všetkých zamestnancov a vedenia organizácie |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |