

Registr opatření dle vyhlášky NBU

Vyloučeno	Instalováno	Zahrnout do plánu implementace	Rozsah		§ vyhlášky	Popis protiopatření
			KII	V/S		
I. ORGANIZAČNÍ OPATŘENÍ						
x	x	x	x	x	3	Systém řízení bezpečnosti informací
	x		x			Stanovení (s ohledem na aktiva a organizační bezpečnost) rozsahu a hranic systému řízení bezpečnosti informací a určení, kterých organizačních částí a technických prvků se systém řízení bezpečnosti informací týká.
		x	x	x		Řízení rizika podle opatření §4.
	x		x	x		Vytvoření a schválení bezpečnostní politiky v oblasti systému řízení bezpečnosti informací, která obsahuje hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací a na základě bezpečnostních potřeb a výsledků hodnocení rizik stanoví bezpečnostní politiku v dalších oblastech podle § 5 a zavede příslušná bezpečnostní opatření.
	x		x			Monitoring účinnost bezpečnostních opatření.
	x		x			Vyhodnocení vhodnosti a účinnosti bezpečnostní politiky podle § 5.
	x		x			Provedení auditu kybernetické bezpečnosti podle § 15, a to nejméně jednou ročně
	x		x			Vyhodnocení účinnosti systému řízení bezpečnosti informací, které obsahuje hodnocení stavu systému řízení bezpečnosti informací včetně revize hodnocení rizik, posouzení výsledků provedených kontrol a auditů kybernetické bezpečnosti a dopadů kybernetických bezpečnostních incidentů na systém řízení bezpečnosti informací, a to nejméně jednou ročně.
	x		x			Aktualizace systému řízení bezpečnosti informací a příslušné dokumentace na základě zjištění z auditů kybernetické bezpečnosti, výsledků vyhodnocení účinnosti systému řízení bezpečnosti informací a v souvislosti s prováděnými nebo plánovanými změnami.
	x		x			Řízení provozu a zdrojů systému řízení bezpečnosti informací, zaznamenávání činností spojených se systémem řízení bezpečnosti informací a řízením rizik.
	x			x		provádí aktualizaci zprávy o hodnocení aktiv a rizik, bezpečnostní politiky, plánu zvládání rizik a plánu rozvoje bezpečnostního povědomí, a to nejméně jednou za tři roky nebo v souvislosti s prováděnými nebo plánovanými změnami.
	x	x	x	x	4	Řízení rizik
	x	x		x		Určení metodiky pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik včetně stanovení kritérií pro přijatelnost rizik.
	x		x	x		Identifikace a hodnocení důležitosti aktiv, které patří do rozsahu systému řízení bezpečnosti informací (zpracování výstupů do zprávy o hodnocení aktiv a rizik)
	x		x	x		Identifikace rizik (posouzení hrozeb a zranitelností, (posouzení možných dopadů na aktiva), hodnocení identifikovaných rizik, určení a schválenípřijatelných rizik a zpracování zprávy o hodnocení aktiv a rizik.
	x		x	x		Zpracování (na základě bezpečnostních potřeb a výsledků hodnocení rizik) prohlášení o aplikovatelnosti, které obsahuje přehled vybraných a zavedených bezpečnostních opatření.
	x		x	x		Zpracování a zavedení plánu zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání rizik, určení osoby odpovědné za prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení a popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními.
	x		x	x		Zohlednění (bez zbytečného odkladu) reaktivní a ochranná opatření vydaná NBU v hodnocení rizik a v případě, že hodnocení rizik aktualizované o nové zranitelnosti spojené s realizací reaktivního nebo ochranného opatření překročí stanovená kritéria pro přijatelnost rizik, doplnění plánu zvládání rizik
	x		x	x	5	Bezpečnostní politika
	x		x			Stanovení bezpečnostní politiky v oblastech: a) až u) (20 oblastí).
	x			x		Stanoví bezpečnostní politiky v oblastech a) až n) (14 oblastí).
	x		x	x		Pravidelné hodnocení účinnost bezpečnostní politiky a její aktualizace.
	x		x	x	6	Organizační bezpečnost
	x		x	x		Zavedení organizace řízení bezpečnosti informací („organizační bezpečnost“), v rámci které se určí výbor pro řízení kybernetické bezpečnosti a bezpečnostní role a jejich práva a povinnosti.

					Určení bezpečnostních rolí: a) manažer kybernetické bezpečnosti, b) architekt kybernetické bezpečnosti, c) auditor kybernetické bezpečnosti, d) garant aktiva
	x		x		
	x		x	x	Odborné školení osob, které zastávají bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí podle § 9
	x		x	x	7 Stanovení bezpečnostních požadavků pro dodavatele
	x		x	x	Stanovení pravidel pro dodavatele, která zohledňují potřeby řízení bezpečnosti informací, a řídí své dodavatele nebo jiné externí subjekty, které se podílejí na rozvoji, provozu nebo zajištění bezpečnosti. Rozsah zapojení dodavatelů dokumentuje písemnou smlouvou, jejíž součástí je ustanovení o bezpečnosti informací.
	x		x		Hodnocení rizik, která jsou spojena s dodávkami od jednotlivých dodavatelů před uzavřením smlouvy.
	x		x		Smlouvy s dodavateli o úrovni služeb, které stanoví způsoby a úroveň realizace bezpečnostních opatření a určí vztah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.
		x	x		Pravidelné hodnocení rizik a pravidelná kontrola zavedených bezpečnostních opatření u služeb poskytovaných jednotlivými dodavateli a odstranění zjištěných nedostatků po dohodě s dodavatelem.
	x		x	x	8 Řízení aktiv
	x		x	x	Identifikace a evidence primárních aktiv.
	x		x	x	Určení garantů aktiv, kteří jsou odpovědní za primární aktiva.
	x		x	x	Hodnocení důležitosti primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti a zařadí je do jednotlivých úrovní
		x	x		Identifikace a evidence podpůrných aktiv.
		x	x		Určení garantů aktiv, kteří jsou odpovědní za podpůrná aktiva.
		x	x		Určení vazby mezi primárními a podpůrnými aktivy a hodnocení důsledků závislosti mezi primárními a podpůrnými aktivy.
	x		x	x	Stanovení pravidel ochrany nutných pro zabezpečení jednotlivých úrovní aktiv tím, že se 1. určí způsoby rozlišování jednotlivých úrovní aktiv, 2. stanoví pravidla pro manipulaci a evidenci s aktivy podle úrovní aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv, 3. stanoví přípustné způsoby používání aktiv.
	x		x	x	Zavedení pravidel ochrany odpovídající úrovni aktiv.
	x		x	x	Určení způsobů pro spolehlivé smazání nebo ničení paměťových médií s ohledem na úroveň aktiv.
	x		x	x	9 Bezpečnost lidských zdrojů
	x		x	x	Stanovení plánu rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a rozsah potřebných školení a určí osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny,
	x		x	x	Poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení (v souladu s plánem vzdělávání zaměstnanců).
	x		x	x	Kontrola dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.
	x		x	x	Vrácení svěřených aktiv a odebrání přístupových oprávnění při ukončení smluvního vztahu s uživateli, administrátory nebo osobami zastávajícími bezpečnostní role.
	x		x	x	Vedení záznamů o školení které obsahují předmět školení a seznam osob, které školení absolvovaly.
	x		x		Stanovení pravidel pro určení osob, které budou zastávat bezpečnostní role, role administrátorů nebo uživatelů.
	x		x		Hodnocení účinnosti plánu rozvoje bezpečnostního povědomí (vzdělávání), provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí.
	x		x		Určení pravidel a postupů pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.
	x		x		Zajištění změny přístupových oprávnění při změně postavení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.
	x		x	x	10 Řízení provozu a komunikací
		x	x	x	Detekce kybernetických bezpečnostních událostí (pomocí technických nástrojů uvedených v § 21 až 23), pravidelné vyhodnocování získaných informací a reakce na zjištěné nedostatky v souladu s § 13.
	x		x	x	Zajištění bezpečný provozu komunikačních technologií, stanovení souvisejících provozních pravidel a postupů.
	x		x	x	Provádění pravidelného zálohování a prověřování použitelnosti provedených záloh.
	x		x		Zajištění oddělení vývojového, testovacího a produkčního prostředí.
x			x		Řešení reaktivních opatření vydaných NBU tím, že organizace posoudí očekávané dopady reaktivního opatření na informační systém a na zavedená bezpečnostní opatření, vyhodnotí možné negativní účinky a bez zbytečného odkladu je oznámí Úřadu

x		x			Řešení reaktivních opatření vydaných NBU tím, že organizace stanoví způsob rychlého provedení reaktivního opatření, který minimalizuje možné negativní účinky, a určí časový plán jeho provedení.
	x	x			Zajištění bezpečnosti a integrity komunikačních sítí a bezpečnosti komunikačních služeb.
	x	x			Určení pravidel a postupů pro ochranu informací, které jsou přenášeny komunikačními sítěmi.
	x	x			Výměna a předávání informací na základě pravidel stanovených právními předpisy za současného zajištění bezpečnosti informací a dokumentace těchto pravidel.
	x	x			Výměna a předávání informací na základě písemných smluv, jejichž součástí je ustanovení o bezpečnosti informací (s ohledem na klasifikaci aktiv).
x	x		x	x	11 Řízení přístupu a bezpečné chování uživatelů
	x		x	x	Řízení přístupu k informačním prostředkům a přidělení jednoznačného identifikátoru každému uživateli (na základě provozních a bezpečnostních potřeb).
	x		x	x	Zavedení nezbytných bezpečnostních opatření, která slouží k zajištění ochrany údajů, které jsou používány pro přihlášení uživatelů a administrátorů a která brání ve zneužití těchto údajů neoprávněnou osobou.
	x		x		Přidělení samostatného identifikátoru přistupujícím aplikacím.
	x		x		Omezení přidělování administrátorských oprávnění.
	x		x		Přidělováníje a odebrání přístupových oprávnění v souladu s politikou řízení přístupu.
	x		x		Pravidelné přezkoumání nastavení přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách nebo rolích.
		x	x		Použití nástroje pro ověřování identity uživatelů podle § 18 a nástroje pro řízení přístupových oprávnění podle § 19.
	x		x		Zavedení bezpečnostních opatření potřebných pro bezpečné používání mobilních zařízení.
	x		x	x	12 Akvizice, vývoj a údržba
x	x		x	x	Stanovení bezpečnostních požadavků na změny informačních systémů spojených s jejich akvizicí, vývojem a údržbou a zahrnutí do projektu akvizice, vývoje a údržby systému.
	x		x		Identifikace, hodnocení a řízení rizik souvisejících s akvizicí, vývojem a údržbou informačního systému.
	x		x		Zajištění bezpečnosti vývojového prostředí a ochrany používaných testovacích dat.
	x		x		Bezpečnostní testování změn informačních systémů před jejich zavedením do provozu.
	x		x	x	13 Zvládání kybernetických bezpečnostních událostí a incidentů
	x		x	x	Zajištění identifikace a oznamování kybernetických bezpečnostních událostí ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a vedení záznamů o oznámeních.
	x		x	x	Vyhodnocení oznámených kybernetických bezpečnostních událostí a kybernetických bezpečnostních událostí detekovaných technickými nástroji podle § 21 až 23.
	x		x	x	Klasifikace kybernetických bezpečnostních incidentů, přijímání opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu.
			x		Hlášení kybernetického bezpečnostního incidentu podle § 32 a sběr věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu
	x		x	x	Prošetření a určení příčiny kybernetického bezpečnostního incidentu, vyhodnocení účinnosti řešení kybernetického bezpečnostního incidentu a na základě vyhodnocení stanovení nutných bezpečnostních opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu.
x	x		x	x	Vedení dokumentace o zvládání kybernetických bezpečnostních incidentů.
	x		x	x	14 Řízení kontinuity činností
	x		x	x	V rámci řízení kontinuity činností stanovení: a) práv a povinností garantů aktiv, administrátorů a osob zastávajících bezpečnostní role, b) cílů řízení kontinuity činností, c) strategii řízení kontinuity činností, která obsahuje naplnění cílů podle písmene b).
	x		x		Vyhodnocení a dokumentace možných dopadů kybernetických bezpečnostních incidentů a posouzení možných rizik souvisejících s ohrožením kontinuity činností.
	x		x		Stanovení, aktualizace a pravidelné testování plánů kontinuity informačních systémů.
		x	x		Realizace opatření pro zvýšení odolnosti informačních systémů vůči kybernetickému bezpečnostnímu incidentu a využívání nástroje pro zajišťování úrovně dostupnosti podle § 26
			x		Stanovení a aktualizace postupů pro provedení opatření vydaných NBU podle § 13 a 14 zákona, ve kterých zohlední: 1. výsledky hodnocení rizik provedení opatření, 2. stav dotčených bezpečnostních opatření a 3. vyhodnocení případných negativních dopadů na provoz a bezpečnost informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury
	x		x	x	15 Kontrola a audit kybernetické bezpečnosti
	x		x	x	Posuzování souladu bezpečnostních opatření s obecně závaznými právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky, určení opatření pro jeho prosazování.
	x		x	x	Pravidelné kontroly dodržování bezpečnostní politiky (včetně dokumentace kontrol) a zohlednění výsledků kontrol v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik.
x	x		x		Provedení auditu kybernetické bezpečnosti (osobou s odbornou kvalifikací), která hodnotí správnost a účinnost zavedených bezpečnostních opatření.
	x		x		Provádění kontrol zranitelnosti technických prostředků pomocí automatizovaných nástrojů a jejich odborné vyhodnocení a reakce na zjištěné zranitelnosti.

II. TECHNICKÁ OPATŘENÍ

x		x	x	16	Fyzická bezpečnost
x		x	x		Nezbytná technická opatření k zamezení neoprávněnému vstupu do vymezených prostor, kde jsou zpracovávány informace a umístěna technická aktiva.
x		x	x		Nezbytná technická opatření k zamezení poškození a zásahům do vymezených prostor, kde jsou uchovány informace a umístěna technická aktiva.
x		x	x		Technická opatření pro předcházení poškození, krádeží nebo kompromitace aktiv nebo přerušení poskytování služeb IT
x		x			Uplatnění prostředků fyzické bezpečnosti: a) pro zajištění ochrany na úrovni objektů, b) pro zajištění ochrany v rámci objektů zajištěním zvýšené bezpečnosti vymezených prostor, ve kterých jsou umístěna technická aktiva informačního systému, c) pro ochranu informací a jednotlivých technických aktiv.
x		x	x	17	Nástroj pro ochranu integrity komunikačních sítí
x		x	x		Řízení bezpečného přístupu mezi vnější a vnitřní sítí (pro ochranu integrity rozhraní vnější komunikační sítě).
x		x	x		Zavedení segmentace zejména použitím demilitarizovaných zón jako speciálního typu sítě používaného ke zvýšení bezpečnosti aplikací dostupných z vnější sítě a k zamezení přímé komunikace vnitřní sítě s vnější sítí.
x		x	x		Zavedení kryptografických prostředků (§ 25) pro vzdálený přístup, vzdálenou správu nebo pro přístup pomocí bezdrátových technologií.
x		x	x		Zavedení opatření pro odstranění nebo blokování přenášovaných dat, které neodpovídají požadavkům na ochranu integrity komunikační sítě.
	x	x			Využití nástrojů pro ochranu integrity vnitřní komunikační sítě, které zajistí její segmentaci.
x		x	x	18	Nástroje pro ověřování identity uživatelů
x		x	x		Nástroj pro ověření identity uživatelů a administrátorů informačního systému.
	x	x	x		Nástroj pro ověření identity uživatelů a administrátorů informačního systému, který zajišťuje ověření jejich identity před zahájením jejich aktivit v informačním systému.
					Nástroj pro ověřování identity uživatelů, který používá autentizaci pouze heslem a zajišťuje: a) minimální délku hesla osm znaků, b) minimální složitost hesla tak, že heslo bude obsahovat alespoň 3 z následujících čtyř požadavků 1. nejméně jedno velké písmeno, 2. nejméně jedno malé písmeno, 3. nejméně jednu číslici nebo 4. nejméně jeden speciální znak, zejména „“, „“, „!“, „?“, c) maximální dobu pro povinnou výměnu hesla nepřesahující sto dnů; tento požadavek není vyžadován pro samostatné identifikátory aplikací.
x		x	x		Nástroj pro ověření identity, který: 1. zamezí opětnému používání dříve používaných hesel a neumožní více změn hesla jednoho uživatele během stanoveného období, které musí být nejméně 24 hodin a 2. provádí opětné ověření identity po určené době nečinnosti,
x		x			Využití nástroje pro ověřování identity účtů administrátorů. V případě, že tento nástroj využívá autentizaci hesla, zajistí prosazení minimální délky hesla patnáct znaků.
x		x	x	19	Nástroje pro řízení přístupových oprávnění
x		x	x		Nástroj pro řízení přístupových oprávnění, který zajistí řízení oprávnění: a) pro přístup k jednotlivým aplikacím a datům, b) pro čtení dat, pro zápis dat a pro změnu oprávnění.
x		x	x		Nástroj pro řízení přístupových oprávnění, který zaznamenává použití přístupových oprávnění v souladu s bezpečnostními potřebami a výsledky hodnocení rizik.
x		x	x	20	Nástroj pro ochranu před škodlivým kódem
x		x	x		Nástroj pro ochranu před škodlivým kódem, který zajistí ověření a stálou kontrolu a) komunikace mezi vnitřní sítí a vnější sítí, b) serverů a sdílených datových úložišť, c) pracovních stanic.
x		x	x		provádí pravidelnou aktualizaci nástroje pro ochranu před škodlivým kódem, jeho definic a signatur
x		x	x	21	Nástroj pro zaznamenávání činností informačních prostředků (KII, VIS), jejich uživatelů a administrátorů
x		x	x		používá nástroj pro zaznamenávání činností, který zajistí a) sběr informací o provozních a bezpečnostních činnostech, zejména typ činnosti, datum a čas, identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a místa činnosti a úspěšnost nebo neúspěšnost činnosti, b) ochranu získaných informací před neoprávněným čtením nebo změnou.

x	x	x		Nástroj pro zaznamenávání činnosti zaznamenává: a) přihlášení a odhlášení uživatelů a administrátorů, b) činnosti provedené administrátory, c) činnosti vedoucí ke změně přístupových oprávnění, d) neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů, e) zahájení a ukončení činností technických aktiv, f) automatická varovná nebo chybová hlášení technických aktiv, g) přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností a h) použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.
x	x			Uchování záznamů činností (nejméně po dobu tří měsíců).
x	x	x		Zajištění nejméně jednou za 24 hodin synchronizaci jednotného systémového času technických aktiv patřících do informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.
x		x	x	22 Nástroj pro detekci kybernetických bezpečnostních událostí
x		x	x	Nástroj pro detekci kybernetických bezpečnostních událostí, který vychází ze stanovených bezpečnostních potřeb a výsledků hodnocení rizik a který zajišť ověření, kontrolu a případně zablokování komunikace mezi vnitřní komunikační sítí a vnější sítí.
	x	x		Nástroj pro detekci kybernetických bezpečnostních událostí, které zajišť ověření, kontrolu a případně zablokování komunikace a) v rámci vnitřní komunikační sítě, b) serverů.
x	x	x		23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
	x	x		Nástroj pro sběr a průběžné vyhodnocení kybernetických bezpečnostních událostí, který v souladu s bezpečnostními potřebami a výsledky hodnocení rizik zajišť a) integrovaný sběr a vyhodnocení kybernetických bezpečnostních událostí z informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury, b) poskytování informací pro určené bezpečnostní role o detekovaných kybernetických bezpečnostních událostech v informačním systému kritické informační infrastruktury nebo komunikačním systému kritické informační infrastruktury a c) nepřetržité vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování určených bezpečnostních rolí.
	x	x		Pravidelná aktualizaci nastavení pravidel pro vyhodnocování kybernetických bezpečnostních událostí a včasné varování, aby byly omezovány případy nesprávného vyhodnocení událostí nebo případy falešných varování.
	x	x		Využívání informací, které jsou připraveny nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí, pro optimální nastavení bezpečnostních opatření.
x		x	x	24 Aplikační bezpečnost
x		x	x	Bezpečnostní testy zranitelnosti aplikací, které jsou přístupné z vnější sítě, a to před jejich uvedením do provozu a po každé zásadní změně bezpečnostních mechanismů.
x		x		Trvalá ochrana aplikací a informací dostupných z vnější sítě před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou.
x		x		Trvalá ochrana transakcí před jejich nedokončením, nesprávným směřováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním.
x		x	x	25 Kryptografické prostředky
x		x	x	Pro používání kryptografické ochrany stanovení: a) úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu, b) pravidla kryptografické ochrany informací při přenosu po komunikačních sítích nebo při uložení na mobilní zařízení nebo vyměnitelná média,
x		x	x	V souladu s bezpečnostními potřebami a výsledky hodnocení rizik použití kryptografických prostředků, které zajišť ochranu důvěrnosti a integrity předávaných nebo ukládaných dat a prokázání odpovědnosti za provedené činnosti.
x		x		Pro používání kryptografických prostředků stanovení systému správy klíčů, který zajišť generování, distribuci, ukládání, archivaci, změny, ničení, kontrolu a audit klíčů.
x		x		Používání odolných kryptografických algoritmů a kryptografických klíčů.
x		x	x	26 Nástroj pro zajišťování úrovně dostupnosti
x		x	x	Nástroj pro zajišťování úrovně dostupnosti informací, který zajišť dostupnost informačního systému pro splnění cílů řízení kontinuity činností.
	x	x		Zálohování důležitých technických aktiv informačního systému 1. využitím redundance v návrhu řešení, 2. zajištěním náhradních technických aktiv v určeném čase.
	x	x	x	27 Bezpečnost průmyslových a řídicích systémů

x

x

Nástroje, které zajistí:

- a) omezení fyzického přístupu k síti a zařízením průmyslových a řídicích systémů,
- b) omezení propojení a vzdáleného přístupu k síti průmyslových a řídicích systémů,
- c) ochranu jednotlivých technických aktiv průmyslových a řídicích systémů před využitím známých zranitelností a
- d) obnovení chodu průmyslových a řídicích systémů po kybernetickém bezpečnostním incidentu.

III. BEZPEČNOSTNÍ DOKUMENTACE

x

x

x

28

Bezpečnostní dokumentace

Vedení a aktualizace bezpečnostní dokumentaci, která obsahuje:

- a) bezpečnostní politiku podle § 5
- b) zprávy z auditu kybernetické bezpečnosti podle § 3
- c) zprávy z přezkoumání systému řízení bezpečnosti informací podle § 3
- d) metodiku pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik podle § 4
- e) zprávu o hodnocení aktiv a rizik podle § 4
- f) prohlášení o aplikovatelnosti podle § 4
- g) plán zvládání rizik podle § 4
- h) plán rozvoje bezpečnostního povědomí podle § 9
- i) zvládání kybernetických bezpečnostních incidentů podle § 13
- j) strategii řízení kontinuity činností podle § 14

x

x

Vedení bezpečnostní dokumentaci tak, aby záznamy o provedených činnostech byly úplné, čitelné, snadno identifikovatelné a aby se daly snadno vyhledat. Opatření potřebná k identifikaci, uložení, ochraně, vyhledání, době platnosti a uspořádání záznamů o provedených činnostech dokumentuje.

x

x

Doporučená struktura bezpečnostní dokumentace je stanovena v příloze č. 4 k této vyhlášce.