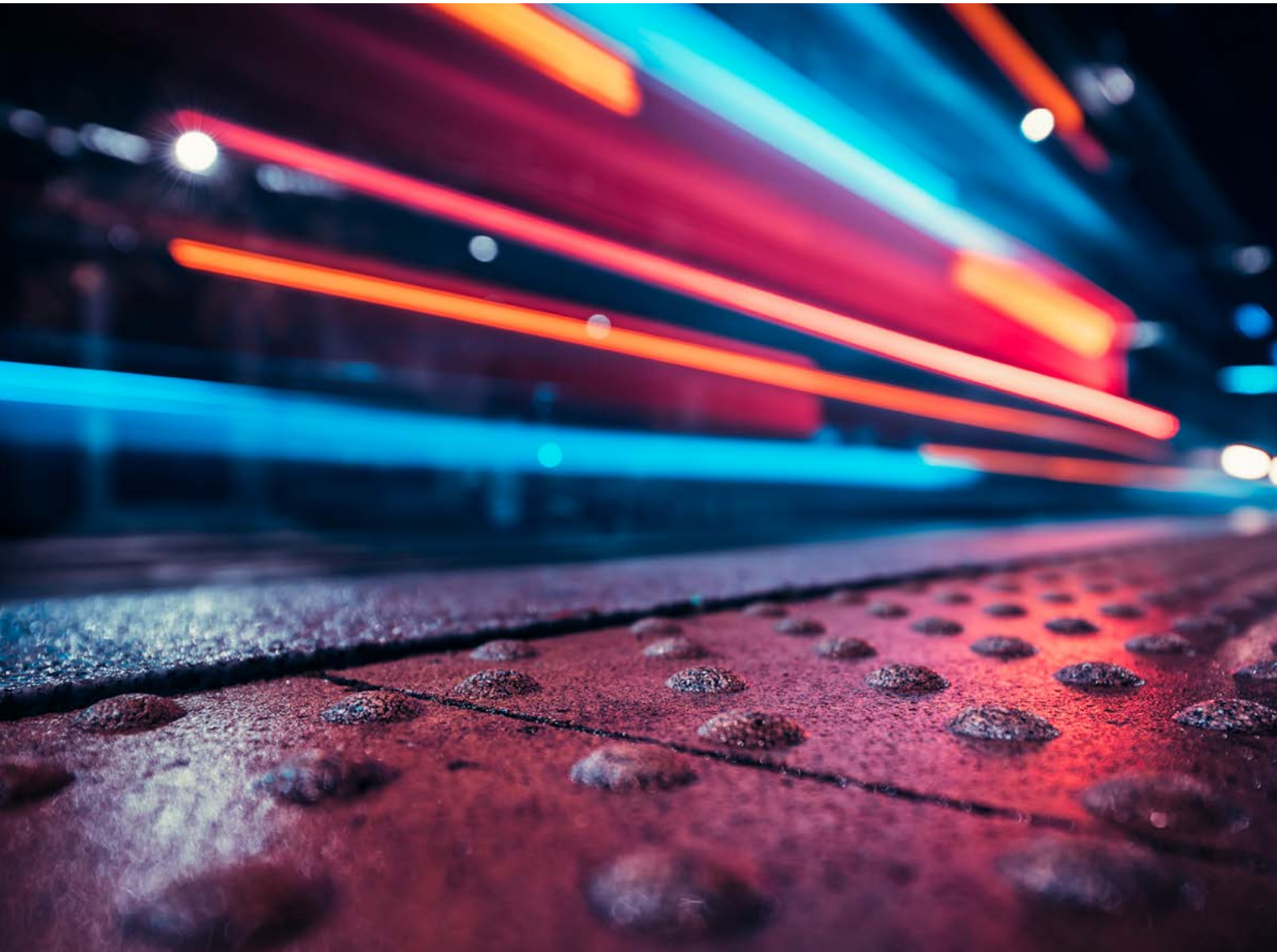
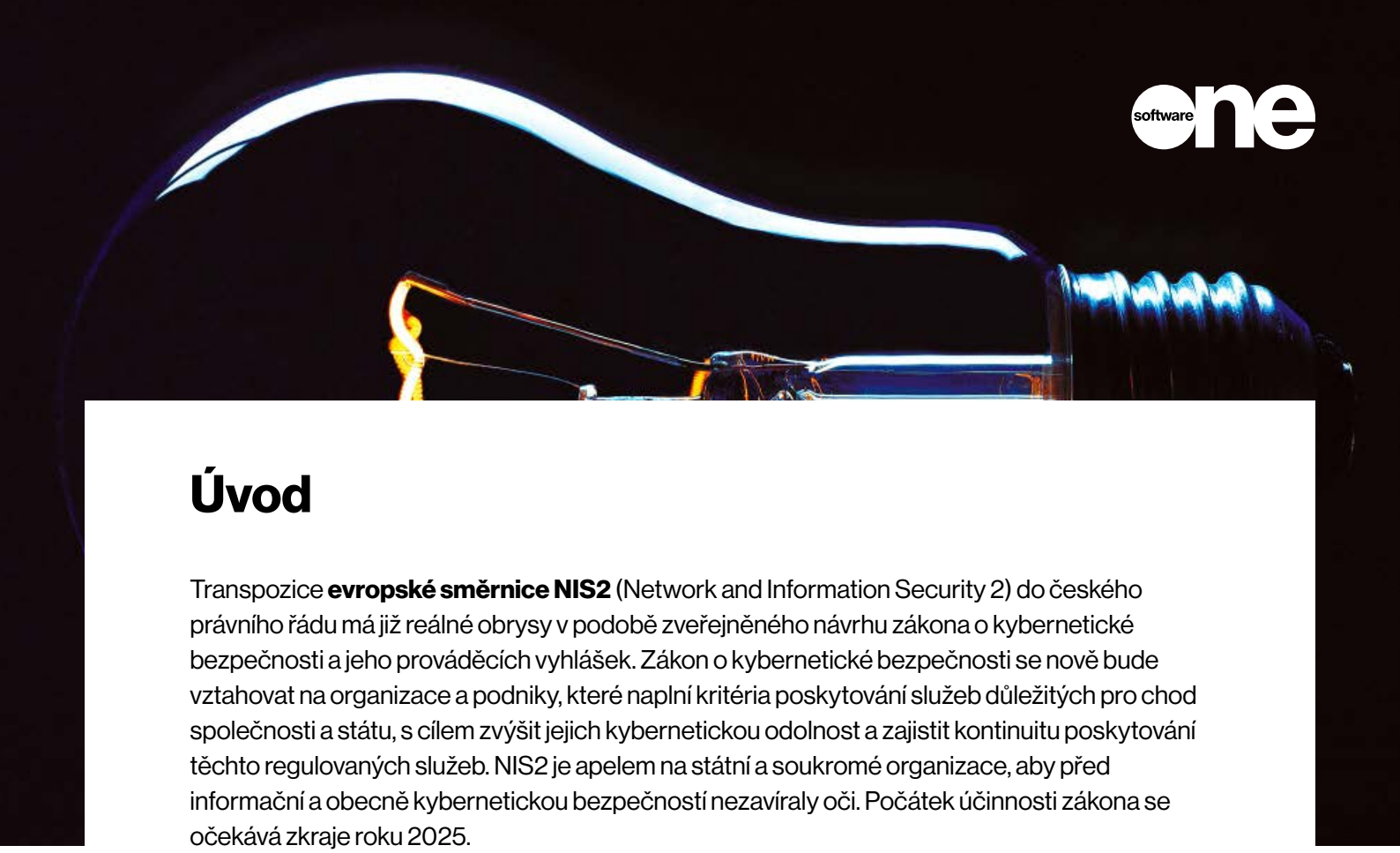
Průvodce řízením informační bezpečnosti

dle připravovaného zákona a vyhlášek o kybernetické bezpečnosti





Úvod

Transpozice **evropské směrnice NIS2** (Network and Information Security 2) do českého právního řádu má již reálné obrysy v podobě zveřejněného návrhu zákona o kybernetické bezpečnosti a jeho prováděcích vyhlášek. Zákon o kybernetické bezpečnosti se nově bude vztahovat na organizace a podniky, které naplní kritéria poskytování služeb důležitých pro chod společnosti a státu, s cílem zvýšit jejich kybernetickou odolnost a zajistit kontinuitu poskytování těchto regulovaných služeb. NIS2 je apelem na státní a soukromé organizace, aby před informační a obecně kybernetickou bezpečností nezavíraly oči. Počátek účinnosti zákona se očekává zkraje roku 2025.

Připravovaná právní regulace přináší zavedení pravidel a procesů pro řízení bezpečnosti informací (Information Security Management System, ISMS) napříč organizací. Informační bezpečnost se přitom netýká pouze informačních technologií (IT), ale znamená také bezpečnost výrobních technologií, systémů a procesů (OT), fyzickou bezpečnost, personální bezpečnost a zabezpečení celého dodavatelského řetězce. Informace a služby, které organizace vytváří a poskytuje, vyžadují komplexní ochranu. Hrozby totiž nemusejí pocházet pouze z kybernetického prostoru, rizikovými faktory jsou také zaměstnanci a dodavatelé, bez nichž by regulovaná služba nemohla být poskytována.

Jak zjistit, zda se na vás připravovaná regulace vztahuje?

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), který je primárním tvůrcem připravované legislativy, spustil v pilotním režimu PORTÁL NÚKIB s veškerými informacemi o transpozici NIS2 do českého právního řádu. Na tomto portálu budou organizace nahlašovat své kontaktní údaje, regulované služby a bezpečnostní incidenty (platí pro režim „vyšších povinností“), současně je zde připravena i „kalkulačka“ pro určení regulovaných služeb. Typicky se bude regulace vztahovat na velké podniky (dle počtu zaměstnanců či obratu) působící v oblastech průmyslu definovaných směrnicí NIS2, jako jsou například energetika, plynárenství, vodní hospodářství, doprava, poskytování IT služeb, zdravotnictví, ale i potravinářství, chemický průmysl či odpadové hospodářství.

Pro určení, zda se na organizaci nové povinnosti vztahují, platí tato základní pravidla:

1. Organizace poskytuje službu uvedenou ve vyhlášce o regulovaných službách.
2. Organizace splňuje kritéria, která jsou u dané služby uvedena.
3. Organizace se zařadí do daného stupně regulace – režimu vyšších nebo nižších povinností.

Jaký je rozdíl mezi režimem vyšších a nižších povinností?

Ať už se organizace na základě kritérií zařadí do režimu nižších, nebo vyšších povinností, v obou případech platí, že se musí řídit zákonem o kybernetické bezpečnosti a naplňovat jeho opatření. Podle konkrétního režimu se bude organizace řídit prováděcím právním předpisem. Jedná se o dvě vyhlášky, z nichž jedna popisuje povinná opatření pro režim vyšších povinností a druhá pro režim nižších povinností. Jak už úrovně napovídají, režim nižších povinností neobsahuje takové množství bezpečnostních opatření jako režim vyšší. Rozdíly jsou patrné jak v oblasti požadavků na technické zabezpečení, tak v dokumentaci procesů spojených s řízením informační a kybernetické bezpečnosti.

Proč vznikl tento průvodce?

Cílem následujících stran je provést čtenáře oblastmi informační a kybernetické bezpečnosti, které připravovaná legislativa obsahuje a u nichž vyžaduje zavedení bezpečnostních opatření. Snahou však není popsat konkrétní znění pravidel pro režim nižších a vyšších povinností ani uvádět výjimky mezi těmito režimy.

Je rovněž vhodné si uvědomit, že zavedení pravidel informační a kybernetické bezpečnosti a s tím spojené dokumentace procesů do podoby bezpečnostních politik, které požaduje připravovaná legislativa, vychází z velké části z mezinárodně uznávaných standardů, jako jsou například ISO 27001 (a další normy z řady ISO 27000), NIST a další. NIS2 „nevymýšlí kolo“, ale inspiruje se existujícími předpisy a frameworky. Už proto můžete při implementaci systému řízení informační a kybernetické bezpečnosti zvážit i možnost budoucí certifikace vaší společnosti dle ISO 27001.

1 Systém řízení informační bezpečnosti

Čemu se tato oblast věnuje

Informační bezpečnost řeší problematiku zachování důvěrnosti, integrity a dostupnosti informací. Zahrnuje procesy předcházení úniku, ztrátě, nedostupnosti a modifikaci informací a dat a s nimi spojených služeb (které označujeme jako aktiva).

Cíl

Stanovit rozsah činností (služeb), na které se bude systém řízení, tedy procesy spojené s řízením informační bezpečnosti, vztahovat. Cílem připravované legislativy je vztahovat tato pravidla minimálně na identifikované regulované služby.

Co je potřeba řešit

1. Určení rozsahu

Co je ve vaší společnosti nejcennější? Jaké služby a informace to jsou? Jakmile je identifikujete, zjistíte, že důležité informace a služby prostupují napříč celou společností a nejjednodušším způsobem bude aplikovat ISMS na celou organizaci.

2. Stanovení cílů

Stanovte si cíle v rámci řízení ISMS, které v krátkodobém a dlouhodobém horizontu budete plnit s cílem zvyšování zabezpečení svých informací.

3. Stanovení pravidel pro systém řízení

ISMS je postaveno na konceptu neustálého zlepšování. Cyklus je následující:

1. Plánování – Proběhne identifikace rizik a hrozeb pro informační bezpečnost a vytvoří se strategie pro jejich zmírnění.
2. Provádění – Bezpečnostní opatření se implementují podle plánu.
3. Kontrola – Účinnost zavedených opatření je monitorována a hodnocena prostřednictvím auditů a testů.
4. Akce – Na základě výsledků kontroly se provedou potřebné úpravy.

2 Organizační bezpečnost

Čemu se tato oblast věnuje

Podle režimu povinností stanovuje nová legislativa složení týmu bezpečnostních specialistů. Do problematiky informační a kybernetické bezpečnosti se musí aktivně zapojit také vedení společnosti – jeho úkolem bude přidělovat adekvátní finanční a lidské zdroje, zajistit soulad s předpisy, mít k dispozici všechny relevantní informace a také se vzdělávat.

Cíl

Stanovit odpovědnosti vrcholného vedení společnosti a osob v bezpečnostních rolích. Role definuje vyhláška včetně doporučené úrovně znalostí a zkušeností. Bezpečnostní role by měly být oddělené od rolí provozních, aby byla zaručena dostatečná nestrannost i nadhled a eliminována takzvaná provozní slepota.

Co je potřeba řešit

1. Odpovědnost vrcholného vedení společnosti

Vedení společnosti přijme závazek k implementaci a zlepšování ISMS podporou bezpečnostních opatření, přidělováním zdrojů a zaměstnanců. Požadavky na vrcholné vedení jsou součástí připravovaných legislativních předpisů.

2. Stanovení osob do bezpečnostních rolí

Jedná se o tyto role:

- manažer kybernetické bezpečnosti – role odpovědná za systém řízení bezpečnosti informací (v případě organizací, které budou v režimu nižších povinností, se tato role označuje jako „osoba odpovědná za kybernetickou bezpečnost“);
- architekt kybernetické bezpečnosti – role odpovědná za vytvoření návrhu a implementaci bezpečnostních opatření;
- auditor kybernetické bezpečnosti – role odpovědná za provádění nestranného auditu kybernetické bezpečnosti;
- garant aktiva – role odpovědná za zajištění rozvoje, použití a bezpečnosti aktiva, které je jí přiděleno;
- výbor pro řízení kybernetické bezpečnosti – pracovní skupina složená ze zástupců vrcholného vedení společnosti, manažera kybernetické bezpečnosti, garantů a případně dalších odborníků, jejímž cílem je pravidelně projednávat stav a rozvoj systému řízení informační bezpečnosti.

3. Stanovení odpovědnosti bezpečnostních rolí a zdokumentování jejich pracovní náplně

Práva a povinnosti bezpečnostních rolí musejí být zdokumentovány v pracovní smlouvě nebo ve smluvním dodatku. Klíčové činnosti jednotlivých bezpečnostních rolí jsou definovány v příloze připravované vyhlášky.

3 Řízení bezpečnostní politiky a dokumentace

Čemu se tato oblast věnuje

Bezpečnostní dokumentace je souborem politik (směrnic), které jsou vytvořeny pro každou oblast ISMS. Tyto politiky obsahují závazná pravidla pro zaměstnance a dodavatele, podle kterých společnost přistupuje k řízení informační a kybernetické bezpečnosti.

Cíl

Centralizovat, zdokumentovat a řídit informace o tom, jak funguje informační a kybernetická bezpečnost ve společnosti. Budovat znalostní bázi pro případ obměny zaměstnanců nebo mimořádné situace.

Co je potřeba řešit

1. Seznam dokumentace

Seznam nutné dokumentace včetně požadovaného obsahu stanovuje příloha připravované vyhlášky.

2. Pravidelná aktualizace dokumentace

Vytvořením bezpečnostní dokumentace teprve začíná proces jejího pravidelného přezkumu a aktualizace.

3. Dostupnost dokumentace pro zaměstnance a dodavatele

S dokumentací v rozsahu, který je pro ně relevantní, seznamte zaměstnance a dodavatele. Nezapomeňte je informovat o významných změnách a zajistěte jim přístup k dokumentaci.

4 Řízení aktiv

Čemu se tato oblast věnuje

Jako aktivum označujeme v informační bezpečnosti vše, co má pro organizaci hodnotu a co je třeba chránit. Primární aktiva jsou informace, služby, procesy nebo know-how, s nimiž společnost pracuje. Jako podpůrná aktiva označujeme taková, díky kterým mohou primární aktiva fungovat. Jsou to technické a programové prostředky, zaměstnanci, dodavatelé, budovy, pozemky a podobně.

Cíl

Platí, že nemůžeme dostatečně chránit něco, o čem ani nevíme, že to chránit máme. Je proto potřeba identifikovat všechna aktiva ve společnosti, ohodnotit je z pohledu jejich důležitosti (kritičnosti) a určit, jakým způsobem s nimi budeme nakládat a jak je budeme monitorovat a chránit.

Co je potřeba řešit

1. Identifikace aktiv

Při identifikaci postupujeme od úvahy, co je pro společnost klíčové (informace, které vlastní, služby poskytované zákazníkům a další), po detailní rozpis technických aktiv a dodavatelů, kteří umožňují společnosti tyto informace a služby poskytovat. Veďte přehlednou evidenci aktiv, včetně určení vazeb (závislostí) mezi nimi. Každé aktivum by mělo mít přiřazeno svého garanta.

2. Hodnocení aktiv

Po inventarizaci aktiv přichází na řadu úvaha nad tím, jak je pro fungování společnosti dané aktivum kritické a jaké důsledky by mohl mít jeho výpadek. Připravovaná vyhláška o kybernetické bezpečnosti a materiály NÚKIB poskytují návod, jak takové hodnocení provést.

3. Klasifikace informací

Společnost nakládá s různými typy informací a dat, od veřejných, které jsou publikované například na webových stránkách, až po citlivé informace, k nimž má mít přístup pouze úzký okruh osob (firemní strategie, finanční data, výrobní tajemství, osobní údaje a tak dále). Proveďte proto inventarizaci informací, s nimiž společnost pracuje (které to jsou, kdo k nim má mít přístup, kde jsou uloženy), a zaveďte odpovídající klasifikaci. Můžete využít pravidla v připravované vyhlášce nebo uznávaný systém Traffic Light Protocol (TLP).

4. Pravidla pro nakládání s aktivy

Na základě hodnocení aktiv a klasifikace informací vytvořte pravidla pro manipulaci, sdílení, likvidaci a další práci s aktivy.

5 Řízení rizik

Čemu se tato oblast věnuje

Riziko je cokoli, co může ohrozit aktiva společnosti. Rizik v kybernetickém prostoru je obrovské množství a není vhodné podceňovat jejich závažnost nebo pravděpodobnost jejich výskytu. Nástrojem pro identifikaci a hodnocení rizik navázaných na aktiva společnosti je analýza rizik. Přístupů pro vytvoření analýzy rizik je více. Návrh vyhlášky ve vyšším režimu poskytuje i návod na vytvoření takové analýzy rizik.

Cíl

Identifikovat a ohodnotit zranitelnosti i hrozby a určit rizika, která působí na aktiva společnosti. Díky tomu nastavíte odpovídající bezpečnostní opatření pro prevenci před riziky nebo zmírnění jejich dopadů na fungování společnosti.

Co je potřeba řešit

1. Identifikace zranitelností a hrozeb a jejich hodnocení

Při identifikaci zranitelností se snažíte najít slabiny ve vaší organizaci. Hrozby jsou pak problémy vnějšího charakteru, které nedokážete ovlivnit, od přírodních katastrof až po zlé úmysly lidí. Pro lepší orientaci, co je zranitelnost a hrozba, poslouží katalogy zranitelností a hrozeb, které obsahuje technická norma ISO 27001 či návrh vyhlášky ve vyšším režimu. Každá organizace si musí obecné katalogy zranitelností a hrozeb přizpůsobit svým potřebám. Návrh vyhlášky ve vyšším režimu obsahuje rovněž stupnice pro hodnocení zranitelností a hrozeb, které vyjadřují pravděpodobnost jejich výskytu.

2. Výpočet rizik a plán jejich zvládání

Vynásobením hodnoty aktiva, zranitelnosti a hrozby zjistíte míru rizika pro dané aktivum. Pokud jsou rizika neakceptovatelná, hledejte v rámci plánu zvládání rizik vhodná nápravná opatření, jimiž rizika zmírníte, eliminujete nebo přenesete například na dodavatele.

6 Řízení dodavatelů

Čemu se tato oblast věnuje

Dodavatele si organizace často pouští k citlivým informacím nebo je závislá na jejich dodávkách. Útoky na dodavatelské řetězce jsou proto v posledních letech na vzestupu.

Cíl

Nastavit pravidla pro dodavatele tak, aby byla eliminována rizika, která s sebou dodavatelský řetězec přináší.

Co je potřeba řešit

1. Určení významných dodavatelů

Určete dodavatele, kteří vám poskytují klíčové služby. Evidujte je a informujte je o tom, že jsou pro vás významní dle zákona o kybernetické bezpečnosti.

2. Hodnocení rizik spojených s dodavateli

V průběhu smluvního vztahu s významnými dodavateli nebo při výběru nového dodavatele hodnoťte jejich rizika. Pokud se objeví neakceptovatelná rizika, je potřeba stanovit dostatečná bezpečnostní opatření, případně zvážit změnu dodavatele. Pokud je to možné, snažte se vyhnout přílišné závislosti na jednom dodavateli.

3. Bezpečnostní opatření ve smlouvách s dodavateli

Ať už v rámci existujících smluvních vztahů, nebo nově vznikajících smluv, dbejte na ustanovení adekvátních bezpečnostních opatření, jako jsou například pravidla pro dodavatele zohledňující požadavky vlastního ISMS, ustanovení o úrovni poskytovaných služeb (Service Level Agreement, SLA), pravidla bezpečného vývoje či pravidla likvidace dat. Přehled dalších ustanovení, nad kterými je vhodné se zamyslet, obsahuje příloha návrhu vyhlášky.

4. Kontrola dodavatelů

Plnění smluv uzavřených s významnými dodavateli by mělo být pravidelně přezkoumáváno a dodavatel by měl podléhat kontrole ze strany společnosti.

5. Bezpečnost cloudových služeb

Na poskytovatele cloudových služeb aplikujte stejná pravidla jako na ostatní dodavatele. Ověřte si, jestli poskytovatel bude ukládat vaše data na území EU, jakou deklaruje úroveň bezpečnosti a dostupnosti, jaké jsou možnosti zálohování či exportů dat, jestli jsou uložená data šifrována a podobně. Jako indikátor kvalitního poskytovatele cloudových služeb může posloužit jeho zapsání v katalogu cloud computingu podle § 6q zákona č. 365/2000 Sb. (Poskytovatelé cloud computingu zapsaní dle ZoISVS platného od 1/9/2021 – Digitální a informační agentura na gov.cz.)

7 Bezpečnost lidských zdrojů

Čemu se tato oblast věnuje

Nejslabším článkem informační a kybernetické bezpečnosti jsou zaměstnanci. Proto zvyšujte jejich povědomí o informační a kybernetické bezpečnosti vstupními a dalšími pravidelnými školeními. Personální oddělení by mělo provést alespoň základní prověření budoucího zaměstnance, zejména u vyšších manažerských pozic. Při odchodu zaměstnance je třeba odebrat všechna oprávnění a zajistit navrácení firemních technických aktiv.

Cíl

Popsat a nastavit pravidla pro personální činnosti a vzdělávání zaměstnanců v oblasti informační a kybernetické bezpečnosti.

Co je potřeba řešit

1. Pravidla pro řízení personálních procesů

V případě nástupu, odchodu nebo změny pracovní pozice zaměstnance je třeba vytvořit takový proces, aby personální oddělení o změnách včas informovalo IT oddělení. Zaměstnanec by měl dostat přístupová oprávnění k systémům až po absolvování vstupního bezpečnostního školení. Zaměstnanec by měl chápat následky způsobení bezpečnostního incidentu.

2. Vzdělávání zaměstnanců a vedení společnosti

Vytvořte plán vzdělávání zaměstnanců, vedení společnosti, ale i dodavatelů nebo externistů v oblasti informační a kybernetické bezpečnosti. Administrátoři a zástupci bezpečnostních rolí by měli pravidelně absolvovat další odborná školení. O vzdělávání zaměstnanců veďte záznamy v jejich osobní složce. Seznam možných témat poskytuje také příloha připravované vyhlášky ve vyšším režimu.

8 Řízení změn, akvizice, vývoj a údržba

Čemu se tato oblast věnuje

Společnost může procházet různými změnami – od úpravy organizační struktury přes stěhování do nové lokality až po akvizici jiné společnosti, migraci na nové softwarové nástroje či změnu významného dodavatele. Je proto důležité pohlížet na tyto změny z hlediska potenciálních rizik.

Cíl

Určení změn, které mohou mít vliv na informační a kybernetickou bezpečnost, zvážit dopady a rizika spojená s těmito změnami, zavést protiopatření.

Co je potřeba řešit

1. Pravidla postupu realizace změny

Změny by měly být řízeny, dokumentovány a schvalovány bezpečnostními rolemi v organizaci. Před uskutečněním změn by měla mít organizace připravenou projektovou dokumentaci včetně vyhodnocení dopadů a analýzy rizik. Pokud mohou mít změny nepříznivé dopady, měla by být přijata vhodná opatření, aby nedošlo k přerušení poskytování služeb. Změny by měly být testovány a měla by existovat strategie návratu do předchozího stavu (takzvaný roll-back). Po významných změnách by měl proběhnout audit kybernetické bezpečnosti nebo penetrační testování.

2. Pravidla bezpečného vývoje a údržby

Při vývoji nových komponent či systémů uplatňujte princip security-by-design. Oddělte vývojová, testovací a provozní prostředí, nepoužívejte ostrá data mimo produkční systémy, používejte verzování a code review. Veškeré činnosti logujte. Pozor si dejte též na komponenty třetích stran.

9 Audit kybernetické bezpečnosti

Čemu se tato oblast věnuje

Aby byl systém řízení informační bezpečnosti funkční, je potřeba ho pravidelně přezkoumávat z procesního i technického hlediska.

Cíl

Odhalení slabin a nedostatků, kontrola legislativních požadavků, které se často mění, neustálé zlepšování stavu ISMS.

Co je potřeba řešit

1. Vytvoření programu auditu

Audit pomůže pravidelně a nezávisle kontrolovat technické a procesní zajištění bezpečnostních opatření. Je třeba posoudit soulad s nejlepší praxí v oblasti kybernetické bezpečnosti i soulad s legislativními předpisy a porovnat reálný výkon bezpečnostních procesů oproti popisu v bezpečnostní dokumentaci. Audit by měl být také proveden při významných změnách a po kybernetických incidentech.

2. Zpracování auditních zjištění

Auditní výsledky slouží jako body pro budoucí zlepšování. Pokud audit odhalí neakceptovatelné nedostatky, měla by s nimi organizace pracovat jako s riziky, což znamená zaevidovat je v rámci plánu zvládání rizik a zavést taková bezpečnostní opatření, aby byla tato rizika snížena.

10 Bezpečné používání mobilních zařízení

Čemu se tato oblast věnuje

Společnost se musí rozhodnout, zda svým zaměstnancům umožní používat pro práci vlastní notebooky, chytré telefony, nositelnou elektroniku či další zařízení (takzvaný režim BYOD – Bring Your Own Device), nebo zda budou zaměstnanci striktně omezeni na zařízení pod firemní správou.

Cíl

Nastavit technické prostředky pro správu koncových mobilních zařízení tak, aby byla zajištěna bezpečnost firemních informací.

Co je potřeba řešit

Pravidla pro správu firemních a soukromých zařízení používaných pro pracovní účely

Neřízená mobilní zařízení mohou představovat obrovské riziko pro spolehlivý a bezpečný chod společnosti. Doporučuje se zavést centrální správu mobilních zařízení (Mobile Device Management, MDM) a BYOD zakázat, případně alespoň v zařízeních oddělit firemní a soukromé profily.

11 Řízení přístupů a identit

Čemu se tato oblast věnuje

Tato oblast je zaměřena na autentizaci (ověření totožnosti) a autorizaci (ověření oprávnění nebo rolí) uživatelů.

Cíl

Zajistit dostupnost informací a dat uživatelům, kteří je potřebují ke své činnosti.

Co je potřeba řešit

1. Řízení identit a přístupových oprávnění

Každý uživatel musí mít v rámci technických aktiv organizace přidělen jedinečný identifikátor. Administrátorské a uživatelské účty budou odděleny a jako součást systému řízení identit a přístupů bude zaveden životní cyklus uživatelských účtů, včetně pravidelných revizí a kontrol. Za každých okolností se snažte o princip need-to-know, tedy poskytovat přístup pouze k tomu, co uživatel opravdu potřebuje.

2. Autentizační mechanismy a politika hesel

Pokud to technologie umožňuje, zaveďte přihlašování bez používání hesel (takzvané passwordless řešení). Jestliže to možné není, je třeba vyžadovat dostatečně dlouhá, komplexní a unikátní hesla, a to společně s vícefaktorovou autentizaci. Práci s hesly lze uživatelům usnadnit zavedením aplikace na správu hesel.

12 Kybernetické bezpečnostní události a kybernetické bezpečností incidenty

Čemu se tato oblast věnuje

Řízení kybernetických bezpečnostních událostí (KBU) a incidentů (KBI) je klíčovou oblastí nové právní regulace. Tuto oblast ISMS je možné rozdělit na několik navazujících aktivit – detekci, zaznamenávání a vyhodnocování bezpečnostních událostí a následné zvládání bezpečnostních incidentů.

Cíl

Včasná detekce a efektivní zvládnutí událostí a incidentů, aby došlo k co nejmenším škodám na aktivech společnosti a co nejkratší době ochromení jejích činností. Registrovaným subjektům vzniká také povinnost incidenty hlásit Národnímu úřadu pro kybernetickou a informační bezpečnost.

Co je potřeba řešit

1. Stanovení pravidel detekce, používání nástrojů pro detekci a chování uživatelů

Začněte používat technické nástroje, které dokážou zajistit kontrolu síťového provozu, identifikují pokusy o průnik či skenování sítě, detekují škodlivý software a budou řídit oprávnění ke spuštění kódu nebo používání vyměnitelných zařízení. Pravidelně školte zaměstnance v identifikaci neobvyklých aktivit a v možnostech, jak je nahlásit.

2. Zaznamenávání událostí

Zajistěte (nejlépe centrální) sběr logů z provozu aplikací a sítě i uživatelských aktivit. Dle návrhu vyhlášky musejí subjekty v režimu vyšších povinností uchovávat logy po dobu alespoň 18 měsíců.

3. Pravidla vyhodnocování KBU a KBI

Zaveďte nástroj typu SIEM (Security Information and Event Management), který vám pomůže udržovat správné mechanismy pro klasifikaci a vyhodnocování bezpečnostních událostí a incidentů. Pro adekvátní výsledky musí nástroj obsluhovat kvalifikovaní administrátoři a neustále přizpůsobovat jeho pravidla novým výzvám.

4. Zvládání KBU a KBI

V případě, že čelíte kybernetickému útoku nebo bezpečnostnímu incidentu, mějte připravena pravidla a postupy pro efektivní zvládnutí této stresové situace. Především musíte určit odpovědnosti, mít k dispozici správné logy a nahlásit incident odpovídajícím orgánům. V ideálním případě pravidelně simulujte kybernetické incidenty, abyste na ně byli adekvátně připraveni. Po zažehnání kritické situace vyhodnoťte, jak příště postupovat ještě lépe.

13 Řízení kontinuity činností

Čemu se tato oblast věnuje

Řízení kontinuity činností (Business Continuity Management, BCM) stanovuje postupy při řešení mimořádných událostí a incidentů. Součástí BCM je vytvoření plánu kontinuity činností (Business Continuity Plan, BCP) a plánu obnovy po havárii (Disaster Recovery Plan, DRP), které definují postupy, odpovědnosti a kontakty pro řešení havarijních situací. K určení, jaké plány vytvořit, slouží analýza dopadů (Business Impact Analysis, BIA) a analýza rizik (Risk Analysis, RIA).

Cíl

Zajistit co nejrychlejší obnovu klíčových činností po bezpečnostním incidentu, aby se minimalizoval jeho dopad na chod společnosti.

Co je potřeba řešit

1. **Analýzu dopadů (BIA)**
„Dopadovka“ pomáhá identifikovat dopady nefunkčnosti klíčových služeb (aktiv) a ztráty informací na různé oblasti fungování organizace. Pomocí této analýzy se stanovují časy a ukazatele kontinuity, jako jsou SLA (Service Level Agreement), RTO (Recovery Time Objective) a RPO (Recovery Point Objective).

2. **Plány kontinuity činností (BCP)**
Cílem je promyslet scénáře situací, které mohou nastat v případě mimořádných událostí, a mít na tyto situace vytvořeny adekvátní plány, jak postupovat. Bez nich může dojít k nepřiměřenému prodlužování času obnovy chodu organizace, a tedy i k finančním či reputačním ztrátám.

3. **Plány obnovy po havárii (DRP)**
Tyto plány se vytvářejí pro významná technická aktiva, jejichž nefunkčnost může ochromit chod společnosti.

14 Fyzická bezpečnost

Čemu se tato oblast věnuje

Tato oblast se zaměřuje na stanovení postupů pro fyzickou ochranu prostor a v nich umístěných aktiv.

Cíl

Minimalizovat rizika spojená s neoprávněným přístupem a manipulací, poškozením nebo ztrátou fyzických zařízení a dokumentů.

Co je potřeba řešit

1. Fyzické bezpečnostní zóny (perimetry)

V rámci organizace vymezte oblasti, kde jsou zpracovány informace a kde jsou umístěny kritické technické prostředky. Zóny mohou být rozděleny podle možností fyzického přístupu, tedy například podle toho, kde se může pohybovat veřejnost a kde zaměstnanci provozu, administrátoři nebo údržbáři. Cílem je zajištění fyzické ochrany klíčových technických aktiv (serverovna, výrobní robot a podobně).

2. Opatření pro kontrolu vstupu osob, ochranu objektů a aktiv a detekci narušení

Definujte pravidla pro vstup návštěv, instalujte kamerový systém, najměte bezpečnostní službu, zaveďte prostředky řízené kontroly vstupu, požární ochrany a podobně. Otestujte fyzický průnik neznámé osoby do chráněných prostor organizace.

3. Požadavky na zajištění dostupnosti a bezpečnosti infrastruktury

Podle povahy technických aktiv, která provozujete, zajistěte náhradní zdroj napájení elektrickou energií (záložní baterie, diesel agregát), redundantní konektivitu či zabezpečení datových a kabelových rozvodů.

15 Bezpečnost komunikačních sítí

Čemu se tato oblast věnuje

Tato oblast se týká zabezpečení komunikační sítě a vzdáleného přístupu.

Cíl

Zajistit důvěryhodnou a spolehlivou komunikaci v rámci vnitřní sítě i do internetu.

Co je potřeba řešit

Segmentace sítě, vzdálený přístup a dokumentace

Definujte a oddělte různé segmenty sítě, podle toho, jaký typ komunikace v nich má probíhat. Stanovte pravidla vzdáleného přístupu pro zaměstnance a dodavatele. Infrastrukturu a topologii sítě zaneste do dokumentace.

16 Aplikační bezpečnost

Čemu se tato oblast věnuje

Tato oblast zahrnuje nastavení pravidel životního cyklu softwaru používaného ve společnosti, skeny zranitelností, penetrační testy a zlepšování na základě jejich výsledků.

Cíl

Minimalizovat riziko zneužití bezpečnostních chyb a zajistit ochranu aplikací před různými typy útoků.

Co je potřeba řešit

1. Pravidla pro řízení životního cyklu instalovaného softwaru

Stanovte pravidla pro instalaci, konfiguraci, testování, aktualizaci a vyřazování programového vybavení, které využíváte. V případě, že technická aktiva již nejsou podporována výrobcem nebo dodavatelem, využijte maximální možnosti zabezpečení, které technologie umožňuje, a naplánujte jejich brzkou výměnu. Do té doby musí platit jejich přísnější kontrola.

2. Skenování zranitelností

V pravidelných intervalech a po významných změnách skenujte zranitelnosti technických aktiv. Cílem je odhalit potenciální rizika, která mohou být zneužita útočníky, a navrhnout opatření k jejich odstranění nebo zmírnění.

3. Penetrační testování

V pravidelných intervalech a po významných změnách provádějte simulované útoky na vaše systémy, síť nebo aplikace s cílem identifikovat a opravit bezpečnostní zranitelnosti. Penetrační testy by měla provádět renomovaná externí společnost, aby zajistila profesionální a nezávislý výsledek. Nálezy z testů zohledněte v následných bezpečnostních opatřeních.

17 Kryptografie

Čemu se tato oblast věnuje

Tato oblast se zaměřuje na nasazení a používání vhodných kryptografických prostředků, které jsou klíčové pro ochranu informací a dat nebo autentizační služby.

Cíl

Zamezení porušení integrity nebo důvěrnosti informací a dat.

Co je potřeba řešit

Pravidla a postupy pro používání kryptografických prostředků

- Pokud již některé kryptografické prostředky používáte, ověřte si, že jsou aktuálně odolné. NÚKIB za tímto účelem vydává Doporučení v oblasti kryptografických prostředků.
- Zaveďte pravidla pro šifrování síťové komunikace, koncových zařízení, vyměnitelných zařízení, uložených hesel a záloh. Zaveďte, zdokumentujte a automatizujte životní cyklus kryptografických klíčů a certifikátů.

18 Zálohování

Čemu se tato oblast věnuje

Tato oblast se týká zajištění kontinuity fungování primárních a podpůrných aktiv organizace (procesů, informací a dat, technických prostředků).

Cíl

Zajištění dostupnosti poskytovaných služeb v případě výpadku, selhání nebo kybernetického incidentu.

Co je potřeba řešit

1. Architektura zálohování

Na základě hodnocení aktiv zaveďte řešení zálohování, které zajistí dostupnost služeb. Vyvarujte se závislosti na jednom dodavateli nebo jednom typu komponent. Pokud je to možné, zvažte redundanci technických prostředků. Uplatněte princip 3-2-1, tedy 3 kopie aktiv na 2 různých typech nosičů, s 1 kopií na geograficky vzdáleném místě.

2. Plán zálohování

Vypracujte plán, co, kdy, kam a proč zálohujete.

3. Testování a ochrana záloh

Při ukládání testujte integritu záloh. Doporučuje se používat šifrování a vyčlenit zálohovací prostředí do samostatného segmentu sítě. Zajistěte fyzickou bezpečnost záloh a vhodný režim přístupu.

Závěrem

Výše uvedená bezpečnostní opatření a kroky pro jejich realizaci představují rámec nejen pro naplnění legislativních požadavků, ale jsou také osvědčenou praxí ochrany podnikatelské činnosti, dokumentace, sdílení pracovních postupů a know-how.

Právní předpisy nedefinují konkrétní způsoby zavedení pravidel ani konkrétní nástroje, které při naplnění opatření používat. Cílem je nastavit postupy ochrany informační bezpečnosti tak, aby vyhovovala potřebám vaší organizace. Žijeme v kybernetické době a musíme se naučit bránit před hrozbami, které z kyberprostoru vycházejí – nejen v pracovním, ale i v soukromém životě. Nastavovat a respektovat opatření, která nás v kyberprostoru chrání, by měla být naše každodenní rutina, stejně jako si každý den čistíme zuby nebo se rozhlédneme, když přecházíme silnici.

Jaké služby nabízíme?

- Nevíte si rady, zda se na vás bude vztahovat nová kyberbezpečnostní legislativa?
- Nevíte, která regulovaná služba nebo jaký režim povinností se vás týká?
- Potřebujete pomoci s tvorbou bezpečnostní dokumentace?
- Potřebujete konzultaci v některé z výše uvedených oblastí?
- Potřebujete provést srovnávací analýzu (GAP) pro zjištění vašeho souladu s legislativními požadavky?
- Potřebujete se připravit na certifikaci ISO 27001?
- Potřebujete outsourcovat bezpečnostní role?
- Potřebujete provést interní audit?
- Potřebujete konzultaci ohledně technického řešení?

Naše služby pokrývají také bezpečnostní nástroje společnosti Microsoft.

Identity and Access Management

- Nasazení technologií podporujících moderní a silné ověřování, například passwordless řešení, Windows Hello, Microsoft Authenticator nebo bezpečnostní klíče typu FIDO 2;
- nasazení řešení umožňující „single sign-on“ pro aplikace Microsoftu i třetích stran;
- řešení Azure Active Directory, Conditional Access, MFA, Microsoft Defender for Cloud Apps a Application Proxy.

Threat Protection

- Nasazení technologií pro model nulové důvěry (Zero Trust), který spočívá v zajištění silného ověřování identity a validace bezpečnostních podmínek na zařízení před udělením přístupu, stejně jako přidělení nejnižších potřebných oprávnění pro explicitně schválené zdroje);
- monitoring a ochrana před hrozbami namířenými na identity, e-maily, aplikace, data a koncové body;
- nasazení řešení MS Intune, MS 365 Defender, MS Defender for Endpoint, MS Defender for Office365, MS Defender for Identity, MS Defender for Cloud Apps, Azure Sentinel a Azure Defender for IoT.

Information Protection

- Technologie poskytující ochranu informací před jejich neoprávněným získáním, zásahem do jejich integrity či jejich zneužitím při zpracování;
- řešení identifikace, klasifikace a štítkování dat i nápravy případného nesouladu v datech;
- nasazení řešení Microsoft Information Protection, Data Loss Prevention, Microsoft Information Governance, Microsoft Defender for Cloud Apps a Compliance Manager.

Cloud Security and Management

- Nasazení řešení pro zabezpečení cloudového prostředí (aplikací a sítě);
- implementace řešení Azure Security Center, Azure Defender, Azure Firewall, Azure Web Application Firewall, Azure DDos Protection a Azure Frontdoor.

Obraťte se na nás a my vám se zajištěním informační a kybernetické bezpečnosti rádi pomůžeme, bez ohledu na to, zda se na vaši organizaci vztahuje nová legislativa.

KONTAKTUJTE NÁS

SoftwareOne Czech Republic s.r.o.
Vyskočilova 1410/1
140 00 Praha 4

T: +420 241 405 297
E: info.cz@softwareone.com
www.softwareone.cz

Slovníček zkratek

Zkratka	Vysvětlení
BCM	Business Continuity Management (řízení kontinuity organizace) – Holistický proces řízení, který identifikuje možné hrozby a jejich dopady na chod organizace. Popisuje možné scénáře dopadů a poskytuje rámec pro prohlubování odolnosti organizace a její schopnosti účinně reagovat. Tím pomáhá chránit zájmy klíčových zainteresovaných stran, pověst i značku organizace a její činnosti vytvářející hodnoty.
BCP	Business Continuity Plan (plán kontinuity činností) – Dokumentované postupy, které organizace provádí, aby reagovala na incidenty, obnovila svá aktiva, zotavila se z narušení a pokračovala ve své činnosti na předem stanovené úrovni.
BIA	Business Impact Analysis (analýza dopadů) – Proces analýzy provozních funkcí a dopadu, který by na ně narušení mohlo mít.
BYOD	Bring Your Own Device – Použití soukromého mobilního zařízení k pracovním účelům.
DRP	Disaster Recovery Plan (plán obnovy po havárii) – Plán pro záložní postupy, odezvu na nepředvídanou událost a obnovu po havárii.
ISMS	Information Security Management System (systém řízení bezpečnosti informací) – Řeší problematiku zachování důvěrnosti, integrity a dostupnosti informací. Zahrnuje procesy předcházení úniku, ztrátě, nedostupnosti a modifikaci informací a dat a s nimi spojených služeb.
KBU	Kybernetická bezpečnostní událost – Událost, která může způsobit narušení bezpečnosti informací v informačních systémech, bezpečnosti služeb nebo bezpečnosti a integrity sítí.
KBI	Kybernetický bezpečnostní incident – Incident je událost, která není součástí běžných operací a narušuje provoz.
MDM	Mobile Device Management – Softwarové řešení, které umožňuje organizacím spravovat, monitorovat a zabezpečovat mobilní zařízení jejich zaměstnanců.
NIS2	Network and Information Security 2 – Směrnice Evropského parlamentu a Rady 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii.
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost – Gestor kybernetické bezpečnosti a národní autorita pro tuto oblast. Zajišťuje mimo jiné metodickou podporu, provádí kontrolu a vydává opatření.
RIA	Risk Analysis (analýza rizik) – Proces pochopení povahy rizik a určení jejich úrovně.
RPO	Recovery Point Objective (bod obnovy dat) – Určitý bod, k němuž musí být obnoveny informace používané při činnosti, aby po opětovném zahájení provozu mohla být tato činnost znovu vykonávána. Může být rovněž označen jako „maximální ztráta dat“.
RTO	Recovery Time Objective (doba obnovy chodu) – Časový interval následující po incidentu, během kterého musejí být obnoveny produkty, služby nebo činnosti a nahrazeny zdroje.
SIEM	Security Information and Event Management – Systém, jehož úkolem je sběr, analýza a korelace dat o událostech v síti. SIEM systémy kombinují metody detekce a analýzy anomálních událostí v síti a poskytují informace použitelné k řízení sítě i provozovaných služeb.
SLA	Service Level Agreement (dohoda o úrovni služeb) – Smlouva mezi poskytovatelem a příjemcem služby, která definuje parametry technické podpory a parametry poskytované služby včetně způsobu jejich měření a následků, které vyplývají z jejich nedodržení poskytovatelem.
TLP	Traffic Light Protocol – Systém označování informací, který určuje, do jaké míry mohou příjemci sdílet potenciálně citlivé informace.