NIS2 a kybernetická bezpečnost v praxi

Vladimír Karas
Security Consultant

CYBER SECURITY & NETWORK MANAGEMENT
HAS NEVER BEEN EASIER

Směrnice NIS2 a její transpozice do právního řádu ČR

- **Plné znění: „Směrnice Evropského parlamentu a Rady (EU) o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii“**
- **Ze dne 14. prosince 2022, zveřejněná ve věstníku 27. prosince 2022, plné znění na www.nukib.cz**
  - platnost 20. den po zveřejnění, tj. 16. ledna 2023
  - 21 měsíců na promítnutí do právního řádu
  - 144 odstavců recitálu
  - 46 článků
  - 3 přílohy
  - vyžaduje transpozici do národní legislativy
- **Ruší směrnici č. 2016/1148 ze dne 6. července 2016 (NIS)**

Nařízení, směrnice, rozhodnutí, doporučení a stanoviska

- **Nařízení**
  - má obecnou působnost, je závazné v celém rozsahu a přímo použitelné ve všech členských státech
- **Směrnice**
  - je závazná pro každý stát, kterému je určena, pokud jde o výsledek, jehož má být dosaženo, přičemž volba formy a prostředků se ponechává vnitrostátním orgánům
- **Rozhodnutí**
  - je závazné v celém rozsahu; pokud jsou v něm uvedeni ti, jimž je určeno, je závazné pouze pro ně
- **Doporučení a stanoviska**
  - nejsou závazná

Proč je tu NIS2?

- **Rozdíly v implementaci NIS v jednotlivých členských státech**
- **Sjednocení přístupu ke kybernetické bezpečnosti v celé Unii**
- **Důraz je položen na:**
  - roli CSIRT
  - roli CERT (vládní/národní)
  - řízení pomocí rizik
  - kontinuitu činností
  - bezpečnost dodavatelského řetězce
  - řízení kybernetické bezpečnosti např. dle norem řady ISO 27000 (recitál, čl. 79)
- **Důsledek – návrh nového zákona o kybernetické bezpečnosti a jeho doprovodných vyhlášek**

Nový zákon o kybernetické bezpečnosti

- **Garant: NÚKIB**
- **26. ledna 2023 předložen k odborné diskuzi, do 12. března 2023**
- **Nyní předložen k meziresortnímu připomínkovému řízení, do PSP v prvním pololetí 2024**
- **Úplně nová struktura**
  - zákon
  - 8 doprovodných vyhlášek
  - nové resp. povinnosti odpovědných osob
  - odpovědnost statutárního orgánu
    - zákaz činnosti
    - trestní odpovědnost
  - vyšší pokuty – horní hranice 250 mil. Kč nebo 2% celosvětového obratu

Struktura nové legislativy

- **Nový zákon o kybernetické bezpečnosti**
- **Doprovodné vyhlášky**
  - Vyhláška o regulovaných službách
  - Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností
  - Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností
  - Vyhláška o portálu NÚKIB
  - Vyhláška o nepominutelných funkcích stanoveného rozsahu
  - Vyhláška o kritériích rizikovosti dodavatele
  - Vyhláška o autorizovaných inspektorech
  - Vyhláška o bezpečnostních úrovních informačních systémů veřejné správy

Aktuální legislativa a normy

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, a jeho prováděcí vyhláška č. 82/2018 Sb. – bude zrušeno
- Nařízení vlády č. 315/2014 Sb., o kritériích pro určení prvku kritické infrastruktury – bude zrušeno
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích – bude zrušeno
- Zákon č. 240/2000 Sb., krizový zákon – bude novelizováno
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací – bude novelizováno
- Zákon č. 127/2005 SB., o elektronické komunikaci – bude novelizováno
- Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby – bude zrušeno

Nový zákon o kybernetické bezpečnosti – I.

- **Sdružuje dosavadní úpravu několika typů povinných osob do jedné - poskytovatele regulované služby**
- **Poskytovatel regulované služby musí naplňovat kritéria daná Vyhláškou o regulovaných službách**
- **Poskytovateli regulované služby zákon a vyhláška následně na základě služeb přiděluje tzv. režim povinností**
  - režim vyšších povinností
  - režim nižších povinností
- **Každý poskytovatel regulované služby má ve výsledku jen jeden režim a ten stanovuje, jaké povinnosti mu ze zákona plynou**

Nový zákon o kybernetické bezpečnosti – II.

- **Povinnosti poskytovatele regulované služby:**
  - hlásit údaje - souvisí s Vyhláškou o Portálu NÚKIB
  - stanovit rozsah řízení kybernetické bezpečnosti
  - zavádět bezpečnostní opatření – souvisí s Vyhláškou o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností a Vyhláškou o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu nižších povinností
  - hlásit kybernetické bezpečnostní incidenty
  - informovat zákazníky o incidentech a hrozbách
  - provádět protiopatření
  - uplatnit pravidla lokalizace dat (v případě poskytovatelů regulované služby v režimu vyšších povinností)
  - řídit bezpečnost dodavatelského řetězce (v případě poskytovatelů regulované služby v režimu vyšších povinností)
  - podřídit se kontrole inspektorem (v případě poskytovatelů regulované služby v režimu nižších povinností), souvisí s Vyhláškou o inspektorech

Vyhláška o regulovaných službách

- **jaké služby do regulace spadají**
- **jakým službám odpovídají jaké výchozí režimy povinností**
- **definuje okruh povinných osob, na které se vztahuje tzv. mechanismus prověřování bezpečnosti dodavatelského řetězce**
- **dle počtu zaměstnanců a velikosti obratu definuje velikost podniku**
  - střední podnik
  - velký podnik

Regulovaná služba

- **definuje ji příloha vyhlášky a dále**
  - orgán nebo osoba je jediným poskytovatelem této služby v České republice a tato služba je nezbytná pro zachování společenských nebo ekonomických činností ve státě
  - narušení této služby by mohlo mít významný dopad na veřejnou bezpečnost nebo veřejné zdraví
  - narušení této služby by mohlo vyvolat významná systémová rizika, zejména v odvětvích, kde by takové narušení mohlo mít přeshraniční dopad
  - orgán nebo osoba je kritická kvůli svému specifickému významu na regionální nebo celostátní úrovni pro konkrétní odvětví nebo typ služby nebo pro jiná vzájemně propojená odvětví v České republice
- **rozhodnutí NÚKIB**
- **kritická infrastruktura podle krizového zákona**

Které jsou regulované služby – I.

- **Veřejná správa**
  - Výkon svěřených pravomocí
- **Energetika – Elektřina**
  - Výroba elektřiny
  - Provoz přenosové soustavy elektřiny
  - Provoz distribuční soustavy elektřiny
  - Obchod s elektřinou
  - OTE
  - Účastník trhu s elektřinou
  - Provoz dobíjecích stanic

Které jsou regulované služby – II.

- **Energetika - Ropa a ropné produkty**
  - Těžba ropy
  - Zpracování ropy
  - Provoz skladovacího zařízení
  - Provoz ropovodu
  - Provoz produktovodu
  - Výkon činnosti ústředního správce zásob
  - Provoz čerpací stanice pohonných hmot

Které jsou regulované služby – III.

- **Energetika – Plynárenství**
  - Výroba plynu
  - Provoz přepravní soustavy plynu
  - Provoz distribuční soustavy
  - Obchod s plynem
  - Uskladňování plynu
- **Energetika – Teplárenství**
  - Výroba tepelné energie
  - Provoz soustavy zásobování tepelnou energií
- **Energetika – Vodík**
  - Výroba vodíku
  - Skladování vodíku
  - Přeprava vodíku

Které jsou regulované služby – IV.

- **Výrobní průmysl**
  - Výroba počítačů, elektronických a optických přístrojů a zařízení
  - Výroba elektrických zařízení
  - Výroba strojů a zařízení nezařazená pod jiné oddíly klasifikace CZ-NACE, oddíl 28
  - Výroba motorových vozidel (kromě motocyklů), přívěsů a návěsů
  - Výroba ostatních dopravních prostředků a zařízení, oddíl 30 CZ-NACE
- **Potravinářský průmysl**
  - Výroba potravin
  - Zpracování potravin
  - Distribuce potravin

Které jsou regulované služby – V.

- **Chemický průmysl**
  - Výroba nebezpečných chemických látek, směsí nebo přípravků nebo látky
  - Zpracování nebezpečných chemických látek, směsí nebo přípravků nebo látky
  - Skladování nebo distribuce nebezpečných chemických látek, směsí nebo přípravků nebo látky
  - Výroba předmětů uvedených v čl. 3 bodě 3 přímo použitelného předpisu Evropské unie z látek nebo směsí (Nařízení Evropského parlamentu a Rady (ES) č. 1907/2006)
- **Vodní hospodářství**
  - Provozování vodovodu
  - Provozování kanalizace

Které jsou regulované služby – VI.

- **Odpadové hospodářství**
  - Provoz zařízení určeného pro nakládání s odpady
  - Obchodování s odpadem
  - Zprostředkování nakládání s odpadem
  - Přeprava odpadu
- **Letecká doprava**
  - Provoz letecké dopravy
  - Provoz letiště
  - Provoz pomocných zařízení v rámci letiště
  - Řízení letového provozu ve vzdušném prostoru České republiky
  - Bezpečnostní kontrola týkající se nákladu nebo poštovních zásilek
  - Služba odesílání nákladu nebo poštovních zásilek

Které jsou regulované služby – VII.

- **Letecká doprava – pokr.**
  - Služba dodávek palubních zásob
  - Služba při odbavovacím procesu
  - Letové navigační služby
- **Drážní doprava**
  - Stavění vlakových cest na celostátní úrovni
  - Provoz celostátní dráhy
  - Provoz regionální dráhy
  - Provoz veřejně přístupné vlečky
  - Provoz drážní dopravy na celostátní dráze
  - Provoz drážní dopravy na regionální dráze
  - Provoz drážní dopravy na veřejně přístupné vlečce
  - Provoz zařízení služeb

Které jsou regulované služby – VIII.

- **Vodní doprava**
  - Výkon činnosti námořní vodní dopravy
  - Provoz řídícího orgánu přístavu nebo provoz díla nebo zařízení v rámci přístavu
  - Provoz služby lodní dopravě (VTS)
- **Silniční doprava**
  - Činnost subjektu odpovědného za kontrolu řízení provozu
  - Provoz inteligentního dopravního systému
- **Digitální infrastruktura a služby**
  - Poskytování veřejně dostupné služby elektronických komunikací
  - Zajišťování veřejné komunikační sítě
  - Poskytování služby výměnného uzlu internetu (IXP)

Které jsou regulované služby – IX.

- **Digitální infrastruktura a služby – pokr.**
  - Poskytování služby systému překladu jmen domén (DNS)
  - Správa a provoz registru internetových domén nejvyšší úrovně
  - Poskytování služby cloud computingu
  - Poskytování služby datového centra
  - Poskytování služby sítě pro doručování obsahu (CDN)
  - Správa kvalifikovaného systému elektronické identifikace
  - Poskytování řízené služby (MSP)
  - Poskytování řízené bezpečnostní služby (MSSP)
  - Poskytování služby on-line tržiště
  - Poskytování služby internetového vyhledávače
  - Poskytování platformy sociální sítě

Které jsou regulované služby – X.

- **Finanční trh**
  - Výkon činnosti úvěrové instituce
  - Provoz obchodního systému
  - Výkon činnosti ústřední protistrany
- **Zdravotnictví**
  - Poskytování zdravotní péče
  - Poskytování zdravotnické záchranné služby
  - Výkon činnosti referenční laboratoře EU zahrnuté do sítě referenčních laboratoří pro oblast veřejného zdraví
  - Výzkum a vývoj léčivých přípravků
  - Výroba léčivých přípravků
  - Výroba léčivých látek

Které jsou regulované služby – XI.

- **Zdravotnictví – pokr.**
  - Výroba zdravotnických prostředků
  - Výroba diagnostických zdravotnických prostředků in vitro
  - Výroba zdravotnických prostředků považovaných za kriticky důležité v případě mimořádné situace v oblasti veřejného zdraví
- **Věda, vzdělávání, výzkum**
  - Výzkum a vývoj
  - Provozování velké výzkumné infrastruktury
- **Poštovní služby**
  - Poskytování poštovní služby
  - Poskytování kurýrní služby

Které jsou regulované služby – XII.

- **Vojenský průmysl**
  - Výroba vojenského materiálu
  - Obchod s vojenským materiálem
  - Výroba zboží a technologií dvojího užití
  - Vývoz zboží a technologií dvojího užití
  - Zprostředkování zboží a technologií dvojího užití
  - Technická pomoc pro zboží a technologií dvojího užití
  - Tranzit a přeprava zboží a technologií dvojího užití
- **Vesmírný průmysl**
  - Zajištění podpory poskytování služeb využívajících kosmického prostoru

Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby

- **Vyhláška upravuje:**
  - systém řízení bezpečnosti informací,
  - povinnosti vrcholového vedení,
  - obsah a strukturu bezpečnostní dokumentace,
  - kybernetické bezpečnostní události a incidenty a reakci na ně,
  - doporučení v přílohách,
  - způsob likvidace dat, provozních údajů, informací a jejich kopií,
  - role a jejich náplň práce,
  - opatření pro smluvní vztahy
- **Stanoví bezpečnostní opatření, která shodně se Zákonem dělí na**
  - organizační opatření
  - technická opatření

Vrcholové vedení organizace

Povinnosti vedení

Angažovanost vedení

- stanovení politiky a cílů bezpečnosti informací
- zajištění integrace do procesů organizace
- zajištění dostupnosti zdrojů
- sdělování důležitosti SŘBI
- naplnění očekávaných výsledků
- směrování a podpora osob přispíváních k účinnosti SŘBI
- podpora neustálého zlepšování
- podpora dalších manažerských rolí

Leadership

Politika

- přiměřená potřebám organizace
- obsahuje cíle bezpečnosti informací
- obsahuje závazek naplnit požadavky na bezpečnost informací
- obsahuje závazek neustálého zlepšování SŘBI

Organizační role, odpovědnosti a pravomoci

Vedení musí přidělit role, pravomoci a odpovědnosti spojené s bezpečností informací

Systém řízení bezpečnosti informací

dle vyhl. o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností

§ 4
Systém řízení bezpečnosti informací

1) Povinná osoba v rámci systému řízení bezpečnosti informací

a) stanoví cíle systému řízení bezpečnosti informací směřující k zajištění bezpečnosti regulované služby,
b) na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a hodnocení rizik zavede přiměřená bezpečnostní opatření směřující k zajištění bezpečnosti regulované služby,
c) řídí rizika podle § 9,
d) vytvoří a schválí bezpečnostní politiku ve vztahu k řízení kybernetické bezpečnosti, která obsahuje hlavní zásady, cíle systému řízení bezpečnosti informací, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací, a na základě bezpečnostních potřeb a výsledků hodnocení rizik stanoví bezpečnostní politiku a bezpečnostní dokumentaci v dalších oblastech podle § 7,
e) zajistí provedení auditu kybernetické bezpečnosti podle § 17,
f) zajistí vyhodnocení účinnosti systému řízení bezpečnosti informací alespoň jednou ročně, které obsahuje
    1. vyhodnocení cílů systému řízení bezpečnosti informací směřujících k zajištění bezpečnosti regulované služby,
    2. posouzení naplňování plánu zvládání rizik zpracovaného podle § 9 písm. g),
    3. hodnocení stavu systému řízení bezpečnosti informací včetně revize hodnocení rizik,
    4. posouzení výsledků provedených auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti,
    5. výsledky předchozích hodnocení účinnosti systému řízení bezpečnosti informací provedených podle tohoto písmena,
    6. posouzení dopadů kybernetických bezpečnostních incidentů na poskytované služby podle § 16 a na oblast kybernetické bezpečnosti a
    7. posouzení změn, které mohou mít negativní dopad na systém řízení bezpečnosti informací podle § 12,
g) na základě vyhodnocení účinnosti systému řízení bezpečnosti informací podle písmena f) zpracuje zprávu o přezkoumání systému řízení bezpečnosti informací,
h) průběžně identifikuje a následně podle § 12 řídí významné změny,

Systém řízení bezpečnosti informací – pokr.

dle vyhl. o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností

i) aktualizuje systém řízení bezpečnosti informací a příslušnou dokumentaci na základě
   1. zjištění auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti,
   2. výsledků vyhodnocení účinnosti systému řízení bezpečnosti informací,
   3. dopadů kybernetických bezpečnostních incidentů na poskytované služby a
   4. v souvislosti s prováděnými významnými změnami,

j) řídí provoz a zdroje systému řízení bezpečnosti informací a zaznamenává činnosti spojené se systémem řízení bezpečnosti informací a řízením rizik a

k) stanoví proces řízení výjimek z pravidel stanovených podle písm. e).

2) Povinná osoba v případě neplnění povinnosti řízení rizik podle odstavce 1 písm. c)

a) zavede všechna bezpečnostní opatření požadovaná touto vyhláškou,

b) zpracuje o bezpečnostních opatřeních podle písm. a),
   1. prohlášení o aplikovatelnosti podle § 9 odst. 1 písm. f) a
   2. plán zvládání rizik přiměřeně podle § 9 odst. 1 písm. g),

c) zohlední v plánu zvládání rizik
   1. významné změny,
   2. změny stanoveného rozsahu podle § X zákona,
   3. protiopatření podle § X zákona,
   4. kybernetické bezpečnostní incidenty, včetně dříve řešených,
   5. výsledky auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti a
   6. výsledky penetračního testování a skenování zranitelností,

d) v souladu s plánem zvládání rizik zavádí bezpečnostní opatření

Systém řízení bezpečnosti informací - opatření

Systém - znamená pro povinné osoby (v režimu vyšších povinností) zavést bezpečnostní opatření:

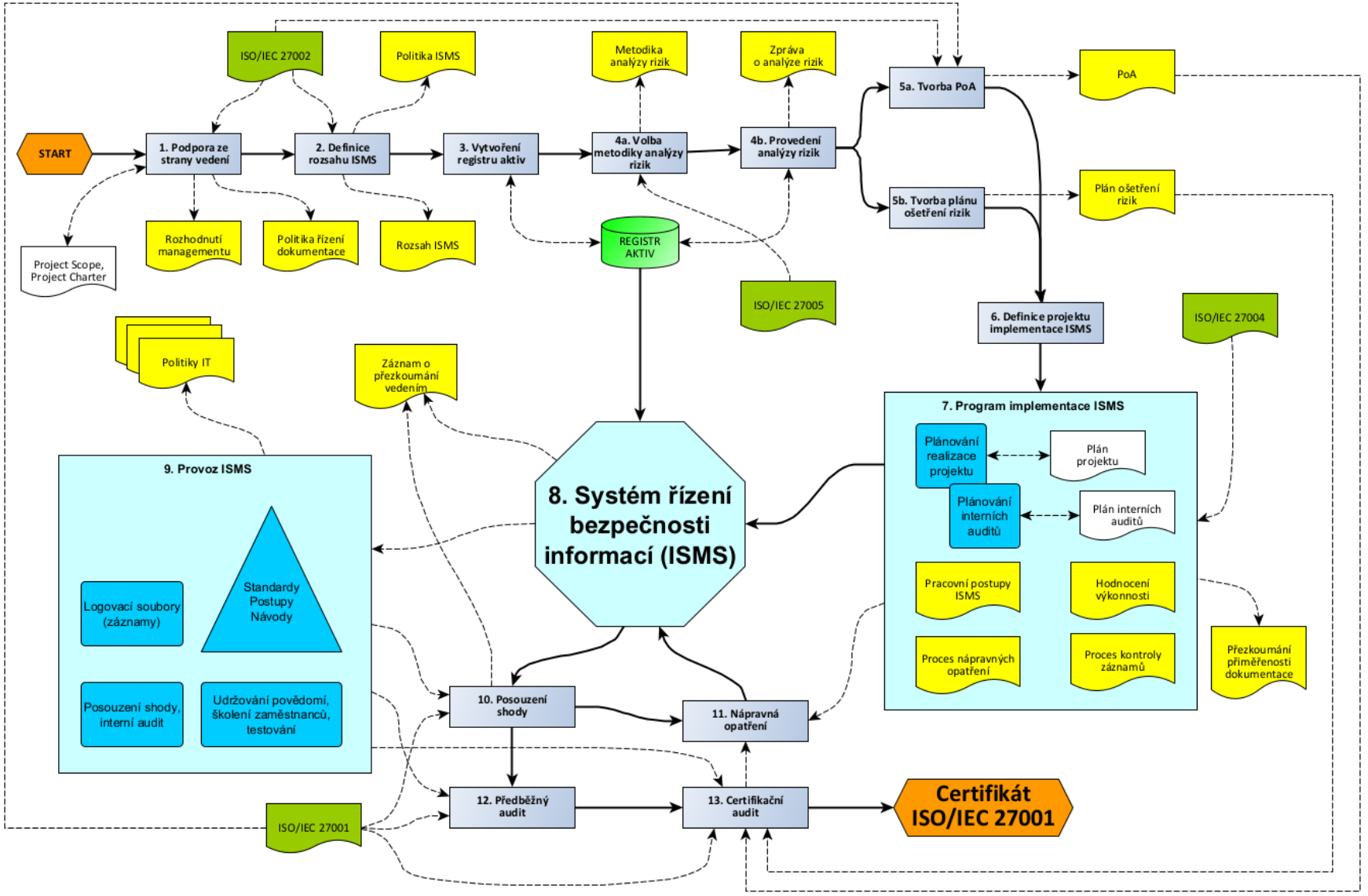
Organizační:

- systém řízení bezpečnosti informací
- povinnosti vrcholového vedení
- bezpečnostní role
- řízení bezpečnostní politiky a bezpečnostní dokumentace
- řízení aktiv
- řízení rizik
- řízení dodavatelů
- bezpečnost lidských zdrojů
- řízení změn
- akvizice, vývoj a údržba
- řízení přístupu
- zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů
- řízení kontinuity činností
- audit kybernetické bezpečnosti

Technická:

- fyzická bezpečnost
- bezpečnost komunikačních sítí
- správa a ověřování identit
- řízení přístupových oprávnění
- detekce kybernetických bezpečnostních událostí
- zaznamenávání bezpečnostních a relevantních provozních událostí
- vyhodnocování kybernetických bezpečnostních událostí,
- aplikační bezpečnost
- kryptografické algoritmy
- zajišťování dostupnosti regulované služby
- zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

Systém řízení bezpečnosti informací - implementace



Manažer kybernetické bezpečnosti - I.

- **Zajištění shody (Compliance):**
  - Vypracovat a udržovat seznam zainteresovaných stran (stakeholders) s vazbou na bezpečnost informací
  - Vypracovat seznam požadavků a očekávání zainteresovaných stran
  - Udržovat kontakty s úřady a zvláštními skupinami zainteresovaných osob
  - Koordinace veškerých aktivit souvisejících s ochranou osobních údajů
- **Řízení dokumentace:**
  - Návrh struktury a obsahu hlavních řídících dokumentů pro zajištění bezpečnosti informací - např. Politika bezpečnosti informací, Prohlášení o aplikovatelnosti, Politika klasifikace informací, Politika řízení přístupu k ICT, Politika bezpečného chování uživatelů, Politika fyzické bezpečnosti, Politika řízení aktiv a rizik atd.
  - Odpovědnost za přezkoumání a aktualizaci hlavních řídících dokumentů

Manažer kybernetické bezpečnosti - II.

- **Řízení rizik:**
  - Stanovení metodiky a metriky analýzy rizik
  - Řízení a koordinace procesu analýzy rizik
  - Návrh opatření ke zvládání rizik
  - Návrh lhůt pro implementaci opatření ke zvládání rizik
- **Lidské zdroje:**
  - Definice základních bezpečnostních pravidel a mechanismů pro každou etapu pracovněprávního vztahu
  - Příprava plánu školení a udržování povědomí zaměstnanců o informační bezpečnosti
  - Nepřetržité provádění činností spojených s udržováním a zvyšováním povědomí
  - Stanovení pravidel a obsahu školení nových zaměstnanců o bezpečnostních tématech
  - Návrh pravidel pro řešení případů porušení bezpečnostních politik zaměstnanci

Manažer kybernetické bezpečnosti - III.

- **Vztahy s vrcholovým vedením organizace:**
  - Návrh a aktualizace cílů informační bezpečnosti
  - Příprava zprávy o výsledcích kontrolní činnosti
  - Předkládání návrhů na zlepšení bezpečnosti informací a návrhů nápravných opatření
  - Návrh rozpočtu a dalších požadovaných zdrojů k zajištění bezpečnosti informací
  - Předkládání významných požadavků zainteresovaných stran
  - Komunikace nejvýznamnějších rizik
  - Příprava a předkládání všech reportů a doporučení v oblasti bezpečnosti informací

- **Zlepšování:**
  - Zajištění implementace všech nápravných opatření
  - Ověření účinnosti nápravných opatření a odstranění příčiny neshod

Manažer kybernetické bezpečnosti - IV.

- **Řízení aktiv:**
  - Údržba a aktualizace registru aktiv
  - Návrh postupů likvidace dat a jejich nosičů

- **Vztahy s dodavateli:**
  - Analýza rizik outsourcovaných procesů
  - Vyhodnocování systému bezpečnosti informací u dodavatelů
  - Definice bezpečnostních doložek ke smlouvám s dodavateli

- **Komunikace:**
  - Definice přijatelných typů komunikačních kanálů
  - Příprava komunikačního prostředí pro případy nouze/katastrofy

Manažer kybernetické bezpečnosti - V.

- **Řízení incidentů:**
  - Příjem hlášení bezpečnostních událostí a incidentů
  - Koordinace reakcí na bezpečnostní události a incidenty
  - Příprava důkazů pro právní kroky po vyřešení incidentu
  - Analýza bezpečnostních událostí a incidentů, řízení implementace nápravných opatření

- **Řízení kontinuity podnikání:**
  - Koordinace tvorby analýzy dopadu nepředvídaných událostí a plánů odezvy
  - Koordinace cvičení a testování plánů
  - Provedení kontroly a aktualizace plánů po incidentu

Manažer kybernetické bezpečnosti - VI.

- **Technická opatření:**
  - Vypracování metody a způsobu ochrany mobilních zařízení, počítačových sítí a dalších komunikačních kanálů
  - Vypracování metod autentizace uživatelů, vynucování politiky hesel, metod šifrování atd.
  - Vypracování pravidel pro bezpečnou práci z domova
  - Definice požadovaných funkcí a zabezpečení internetových služeb
  - Definice zásad bezpečného rozvoje informačních systémů
  - Kontrola protokolů o aktivitách uživatelů a administrátorů

Hlavním úkolem manažera kybernetické bezpečnosti je rozvoj kultury zabezpečení informací založené na riziku, které organizace podstupuje. Manažer kybernetické bezpečnosti si musí být vědom skutečnosti, že každá aktivita organizace sebou nese bezpečnostní rizika a že takováto rizika musí být souborem opatření zmírněna na přijatelnou úroveň.

Otázky a odpovědi

novicom

CYBER SECURITY & NETWORK MANAGEMENT
HAS NEVER BEEN EASIER

ADDNET BVS CCM ACADEMY APPLIANCE