CyberSecurityHub.cz

TLP:CLEAR

PROGRAM SEMINÁŘE

Právní okénko - *Mgr. Petr Pernica*

- Odpovědnost vedení obce či města nejen z pohledu stávající legislativy.
- Přichází nová legislativa NIS2 (NIS2 a obce či příspěvkové organizace).
- NIS2 v termínech.
- Nová reálná odpovědnost vrcholového vedení dle NIS2.

Úvod do kybernetické bezpečnosti - *Ing. Jiří Sedláček*

- Proč nemůže Vaše IT oddělení odpovídat za kybernetickou bezpečnost.
- Proč je nutné oddělit provozní činnosti a kompetence od činností a kompetencí bezpečnostních.
- Kdo můžou být správné osoby do bezpečnostních rolí.
- Ochrana informací a zajištění kontinuity činností.

Kybernetická bezpečnost prakticky - *Ing. Robert Schindler, MSc.*

- Pragmatický přístup ke kybernetické bezpečnosti.
- Jak řešit kybernetickou bezpečnost, když odborníci chybí.
- Nezbytné minimum aneb jaká organizačních pravidla a jaká technická opatření, které musí být nastavena.
- Jak chránit informace a zajistit kontinuitu činností obce či organizace, aneb krizové řízení je obtížné outsourcovat.

CyberSecurityHub.cz

TLP:CLEAR

MOTTO

CyberSecurityHub.cz

KYBERNETICKOU BEZPEČNOST POTŘEBUJETE ŘEŠIT, PROTOŽE JSTE DOBRÝMI HOSPODÁŘI, CHRÁNÍTE INFORMACE A ZAJIŠŤUJETE KONTINUITU ČINNOSTÍ VAŠÍ OBCE. ZÁKON JE POUZE RÁMCEM PRO ŘEŠENÍ.

TLP:CLEAR

MÝTY

CyberSecurityHub.cz

1. Kybernetickou bezpečnost řeší IT.
2. Nákup bezpečnostních technologií vyřeší všechny Vaše problémy, GDPR a NIS2 nevyjímaje.
3. Obchodník s teplou vodou:

- „posoudíme soulad vaší organizace s NIS2“…
- „zavedeme vám NIS2 na klíč“…

TLP:CLEAR

CyberSecurityHub.cz

Právní okénko - *Mgr. Petr Pernica*

- Přichází nová legislativa NIS2 (NIS2 a obce či příspěvkové organizace).
- Odpovědnost vedení obce či města nejen z pohledu stávající legislativy.
- Nová reálná odpovědnost vrcholového vedení dle NIS2.
- NIS2 v termínech.

TLP:CLEAR

CO JE NIS2?

Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii

CyberSecurityHub.cz

Na co se NIS2 zaměřuje?

- oblast zajišťování kybernetické bezpečnosti

Jaké jsou cíle NIS2?

zavedení / zvýšení odolnosti subjektu proti kybernetickým útokům

- stanovuje povinná opatření
- rozšíření počtu povinných osob
- kategorie subjektů

zlepšení připravenosti členských států na kybernetické útoky

- členský stát – tým CSIRT -> oznamovací povinnost subjektů

jednotná úroveň bezpečnosti v celé EU

- přísnější bezpečnostní požadavky
- finanční sankce

TLP:CLEAR

NOVÝ ZÁKON O KYBERNETICKÉ BEZPEČNOSTI

CyberSecurityHub.cz

Zákon o kybernetické bezpečnosti

Vyhláška o regulovaných službách

- Upravuje kritéria pro identifikaci regulovaných služeb, stanovení režimů poskytovatelů regulovaných služeb, pokud byla jejich regulovaná služba identifikována podle vyhlášky a také specifická kritéria pro identifikaci strategicky významných služeb.

Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností

- Vymezuje jak obsah a rozsah bezpečnostních opatření (která dělí na organizační a technická), ale také lokalizaci informací a dat při jejich zpracování v zahraničí.

Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností

- Obsahuje obsah a rozsah bezpečnostních opatření, přičemž na rozdíl od předchozí uvedené vyhlášky neobsahuje lokalizaci informací a dat, ale naopak zahrnuje způsob stanovení významnosti dopadu kybernetického bezpečnostního incidentu.

Vyhláška o Portálu NÚKIB

- Obsahuje zejména druhy a způsoby hlášení údajů poskytovatelů regulované služby a kybernetických bezpečnostních incidentů.

Vyhláška o nepominutelných funkcích stanoveného rozsahu

- Uvádí kritické funkce rozsahu aktiv, na které se vztahuje řízení kybernetické bezpečnosti podle zákona.

Vyhláška o kritériích rizikovosti dodavatele

- Navazuje na mechanismus posuzování dodavatelů a uvádí kritéria rizikovosti dodavatele a způsob jejich vyhodnocení.

Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti

TLP:CLEAR

NEJVÝZNAMNĚJŠÍ ZMĚNY DOPADAJÍCÍ NA SUBJEKTY

CyberSecurityHub.cz

Článek 2 – oblast působnosti

- rozšiřuje počet povinných subjektů
- NÚKIB – přes 6000 nových subjektů, na které úprava dopadá

Článek 20 – řízení kybernetických bezpečnostních rizik

- odpovědnost managmentu za zajištění kybernetické bezpečnosti
- povinné vzdělávání vrcholového vedení organizace

Článek 30 – dobrovolné oznamování relevantních informací

- hlášení relevantních incidentů, událostí, hrozeb a zranitelností

Článek 34 – ukládání pokut

- významné zvýšení pokut za nedodržení uložených povinností

TLP:CLEAR

ROZDĚLENÍ POVINNÝCH SUBJEKTŮ DLE NIS2

CyberSecurityHub.cz

Článek 3 – **základní a důležité subjekty**

Obě kategorie musí dodržovat stanovené bezpečnostní opatření.

Rozdílná míra rizika při narušení – zohlednění při zavádění požadavků k řízení kyberbezpečnostních rizik.

Rozdílný způsob kontroly.

TLP:CLEAR

ROZDĚLENÍ POVINNÝCH SUBJEKTŮ DLE NOVÉHO ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI

CyberSecurityHub.cz

PRINCIP DVOURYCHLOSTNÍ KYBERNETICKÉ BEZPEČNOSTI (VIZ. NIS2)

Režim vyšších povinností

- základní subjekt

Režim nižších povinností

- důležitý subjekt
- zjednodušený režim povinností

POVINNÝ SUBJEKT

- Povinný subjekt dle zákona
  - „poskytovatel regulované služby“
- Jedna organizace (vymezená IČO) -> jeden režim poskytovatele regulované služby

TLP:CLEAR

OBCE JAKO POVINNÉ OSOBY

Čl. 2 odst. 2. NIS2

- Bez ohledu na jejich velikost se tato směrnice vztahuje také na subjekty, jejichž druh je uveden v příloze I nebo II, pro něž platí, že:

(…)

- f) subjekt je subjektem veřejné správy:
  - i) ústřední vlády, jak je vymezena členským státem podle vnitrostátního práva; nebo
  - ii) na regionální úrovni, jak je vymezena členským státem podle vnitrostátního práva, a na základě posouzení rizik poskytuje služby, jejichž narušení by mohlo mít významný dopad na kritické společenské nebo hospodářské činnosti.

➢ **OBCE S ROZŠÍŘENOU PŮSOBNOSTÍ**

TLP:CLEAR

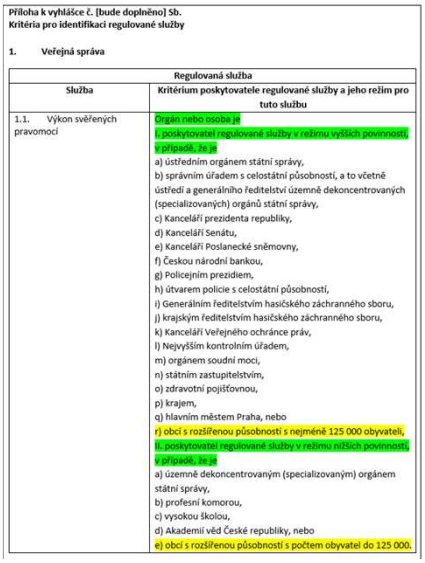
OBCE JAKO POVINNÉ OSOBY

Z důvodové zprávy k návrhu zákona o kybernetické bezpečnosti:

- *„Obce s rozšířenou působností dlouhodobě pod regulaci zákona o kybernetické bezpečnosti nespadaly z důvodu výslovné výjimky. Současné trendy a zkušenosti z České republiky a zahraničí nicméně ukazují, že jejich postavení nelze podceňovat – jak ukazují neblahé zkušenosti některých obcí s kybernetickými bezpečnostními incidenty, které se ani jim nevyhýbají.* ***V případě obcí s rozšířenou působností počítá návrh zákona s jejich zařazením zpravidla do režimu nižších povinností.*** *Lze však také očekávat jejich nižší úroveň kybernetické bezpečnosti obecně. Z toho se dá odhadnout, že náklady na jejich zabezpečení budou v zásadě srovnatelné s výpočtem uvedeným výše.“*

TLP:CLEAR

VYHLÁŠKA O REGULOVANÝCH SLUŽBÁCH TÝKAJÍCÍ SE OBCÍ



Příloha k vyhlášce č. (bude doplněno) Sb.
Kritéria pro identifikaci regulované služby

1. Veřejná správa

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby a jeho režim pro tuto službu
1.1. Výkon svěřených pravomocí	Orgán nebo osoba je i. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je a) ústředním orgánem státní správy, b) správním úřadem s celostátní působností, a to včetně ústředí a generálního ředitelství územně dekoncentrovaných (specializovaných) orgánů státní správy, c) Kanceláří prezidenta republiky, d) Kanceláří Senátu, e) Kanceláří Poslanecké sněmovny, f) Českou národní bankou, g) Policejním prezidiem, h) útvarem policie s celostátní působností, i) Generálním ředitelstvím hasičského záchranného sboru, j) krajským ředitelstvím hasičského záchranného sboru, k) Kanceláří Veřejného ochránce práv, l) Nejvyšším kontrolním úřadem, m) orgánem soudní moci, n) státním zastupitelstvím, o) zdravotní pojišťovnou, p) krajem, q) hlavním městem Praha, nebo r) obcí s rozšířenou působností s nejméně 125 000 obyvateli, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je a) územně dekoncentrovaným (specializovaným) orgánem státní správy, b) profesní komorou, c) vysokou školou, d) Akademií věd České republiky, nebo e) obcí s rozšířenou působností s počtem obyvatel do 125 000.

Režim vyšších povinností

- Obce s rozšířenou působností s nejméně 125 000 obyvateli
- Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností

Režim nižších povinností

- Obce s rozšířenou působností do 125 000 obyvatel
- Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností

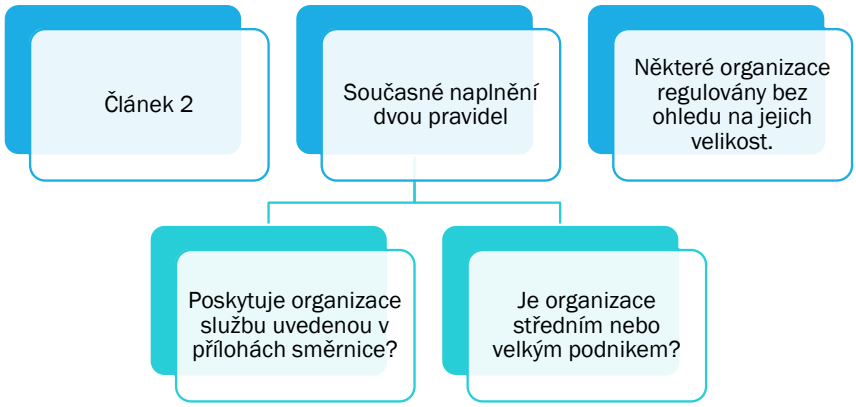
TLP:CLEAR

SEZNAM BEZPEČNOSTNÍCH OPATŘENÍ

Režim nižších povinností	Režim vyšších povinností – organizační opatření	Režim vyšších povinností – technická opatření
• zajišťování minimální úrovně kybernetické bezpečnosti, • **povinnosti vrcholného vedení,** • řízení rizik, • bezpečnost lidských zdrojů, • řízení kontinuity činností, • řízení přístupu, • řízení identit a jejich oprávnění, • detekce a zaznamenávání kybernetických bezpečnostních událostí, • řešení kybernetických bezpečnostních incidentů, • bezpečnost komunikačních sítí, • aplikační bezpečnost, • kryptografické algoritmy	• systém řízení bezpečnosti informací, • **povinnosti vrcholného 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	• 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

TLP:CLEAR

SPADÁ POD REGULACI SMĚRNICE PŘÍSPĚVKOVÁ ORGANIZACE OBCE?



TLP:CLEAR

POSKYTUJE ORGANIZACE SLUŽBU UVEDENOU V PŘÍLOHÁCH SMĚRNICE?

- **Příloha I – vysoce kritická odvětví**
  1. Energetika
  2. Doprava
  3. Bankovnictví
  4. Infrastruktura finančních trhů
  5. Zdravotnictví
  6. Pitná voda
  7. Odpadní voda
  8. Digitální infrastruktura
  9. Řízení služeb IKT
  10. **Veřejná správa**
     - i. ústřední subjekty
     - ii. **regionální subjekty - obce s rozšířenou působností**
  11. Vesmír

- **Příloha II – další kritická odvětví**
  1. Poštovní a kurýrní služby
  2. Nakládání s odpady
  3. Výroba, produkce a distribuce chemických látek
  4. Výroba, zpracování a distribuce potravin
  5. Výroba zdravotnických prostředků, elektronických přístrojů a zařízení, strojů, dopravních prostředků
  6. Digitální poskytovatelé – internetové vyhledávače, on-line tržiště
  7. Výzkum

TLP:CLEAR

JE ORGANIZACE STŘEDNÍM NEBO VELKÝM PODNIKEM?

CyberSecurityHub.cz

Prahové hodnoty *(čl. 2)*

Kategorie podniku	Počet zaměst-nanců: roční pracovní jednotka (RPJ)	Roční obrat	nebo	Bilanční suma roční rozvahy
Střední podnik	< 250	≤ 50 milionů EUR	nebo	≤ 43 milionů EUR
Malý podnik	< 50	≤ 10 milionů EUR	nebo	≤ 10 milionů EUR
Mikropodnik	< 10	≤ 2 miliony EUR	nebo	≤ 2 miliony EUR

TLP:CLEAR

NÁVRH VYHLÁŠKY O REGULOVANÝCH SLUŽBÁCH

CyberSecurityHub.cz

- § 2 odst. 4

„Odchylně od pravidel doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků pro účely této vyhlášky platí, že **pokud je zřizovatelem nebo zakladatelem posuzované organizace územní samosprávný celek, nezohledňuje se tento územní samosprávní celek při určování velikosti podniku**, pokud je tento poskytovatel regulované služby nezávislý z hlediska sítě a informačních systémů, které používá při poskytování svých služeb, a pokud jde o služby, které tento subjekt poskytuje.“

TLP:CLEAR

ODPOVĚDNOST VRCHOLOVÉHO VEDENÍ

CyberSecurityHub.cz

Původní směrnice NIS – pouze obecný rámec - povinné osoby mají zajistit vhodná a přiměřená technická organizační opatření k ošetření rizik a zabránění incidentům.

Důvodová zpráva ke KybeZ: *„Návrh zákona musí zohlednit požadavky směrnice NIS2 na větší odpovědnost vrcholného vedení za zajišťování kybernetické bezpečnosti.“*

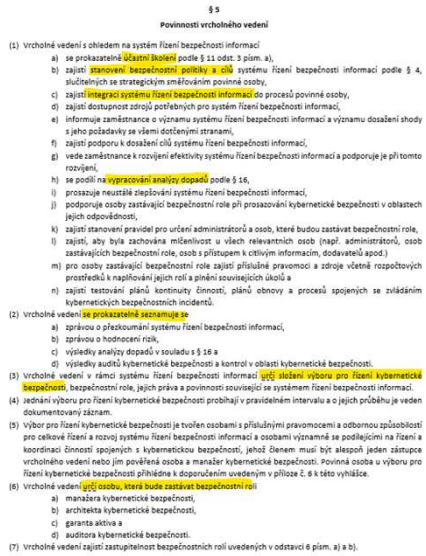
NIS2 - Článek 20 a 21

- Organizace, na které se směrnice NIS2 vztahuje, mají povinnost zavádět a provádět bezpečnostní opatření.
- Odpovědnost vedení organizací za schválení a zavádění bezpečnostních opatření ke snížení rizik pro kybernetickou bezpečnost.
- Vedení organizací má povinnost osobně absolvovat školení na téma kybernetické bezpečnosti a podporovat v těchto školeních také své zaměstnance.
- Cílem směrnice je zavádění preventivních opatření k posílení kybernetické bezpečnosti subjektu.

TLP:CLEAR

ODPOVĚDNOST VRCHOLOVÉHO VEDENÍ V REŽIMU VYŠŠÍCH POVINNOSTÍ

CyberSecurityHub.cz



§ 5

Povinnosti vrcholného vedení

(1) Vrcholné vedení s ohledem na systém řízení bezpečnosti informací
- a) se prokazatelně účastní školení podle § 11 odst. 3 písm. a),
- b) zajistí stanovení bezpečnostní politiky a cílů systému řízení bezpečnosti informací podle § 4, slučitelných se strategickým směřováním povinné osoby,
- c) zajistí integraci systému řízení bezpečnosti informací do procesů povinné osoby,
- d) zajistí dostupnost zdrojů potřebných pro systém řízení bezpečnosti informací,
- e) informuje zaměstnance o významu systému řízení bezpečnosti informací a významu dosažení shody s jeho požadavky se všemi dotčenými stranami,
- f) zajistí podporu k dosažení cílů systému řízení bezpečnosti informací,
- g) vede zaměstnance k rozvíjení efektivity systému řízení bezpečnosti informací a podporuje je při tomto rozvíjení,
- h) se podílí na vypracování analýzy dopadů podle § 16,
- i) prosazuje neustálé zlepšování systému řízení bezpečnosti informací,
- j) podporuje osoby zastávající bezpečnostní role při prosazování kybernetické bezpečnosti v oblastech jejich odpovědnosti,
- k) zajistí stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role,
- l) zajistí, aby byla zachována mlčenlivost u všech relevantních osob (např. administrátorů, osob zastávajících bezpečnostní role, osob s přístupem k citlivým informacím, dodavatelů apod.)
- m) pro osoby zastávající bezpečnostní role zajistí příslušné pravomoci a zdroje včetně rozpočtových prostředků k naplňování jejich rolí a plnění souvisejících úkolů a
- n) zajistí testování plánů kontinuity činností, plánů obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů.

(2) Vrcholné vedení se prokazatelně seznamuje se
- a) zprávou o přezkoumání systému řízení bezpečnosti informací,
- b) zprávou o hodnocení rizik,
- c) výsledky analýzy dopadů v souladu s § 16 a
- d) výsledky auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti.

(3) Vrcholné vedení v rámci systému řízení bezpečnosti informací určí složení výboru pro řízení kybernetické bezpečnosti, bezpečnostní role, jejich práva a povinnosti související se systémem řízení bezpečnosti informací.

(4) Jednání výboru pro řízení kybernetické bezpečnosti probíhají v pravidelném intervalu a o jejich průběhu je veden dokumentovaný záznam.

(5) Výbor pro řízení kybernetické bezpečnosti je tvořen osobami s příslušnými pravomocemi a odbornou způsobilostí pro celkové řízení a rozvoj systému řízení bezpečnosti informací a osobami významně se podílejícími na řízení a koordinaci činností spojených s kybernetickou bezpečností, jehož členem musí být alespoň jeden zástupce vrcholného vedení nebo jím pověřená osoba a manažer kybernetické bezpečnosti. Povinná osoba u výboru pro řízení kybernetické bezpečnosti přihlédne k doporučením uvedeným v příloze č. 6 k této vyhlášce.

(6) Vrcholné vedení určí osobu, která bude zastávat bezpečnostní roli
- a) manažera kybernetické bezpečnosti,
- b) architekta kybernetické bezpečnosti,
- c) garanta aktiva a
- d) auditora kybernetické bezpečnosti.

(7) Vrcholné vedení zajistí zastupitelnost bezpečnostních rolí uvedených v odstavci 6 písm. a) a b).

§ 5 Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností

Vrcholné vedení - osoba nebo skupina osob, které řídí povinnou osobu, nebo statutární orgán povinné osoby

TLP:CLEAR

ODPOVĚDNOST VRCHOLOVÉHO VEDENÍ V REŽIMU NIŽŠÍCH POVINNOSTÍ

§ 5 Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností

Vrcholné vedení

- je prokazatelně poučeno o jeho povinnostech a rozsahu odpovědností,
- zajistí dostupnost zdrojů potřebných pro zajišťování kybernetické bezpečnosti
- se prokazatelně seznamuje s plněním přehledu bezpečnostních opatření
- a další …

CyberSecurityHub.cz

TLP:CLEAR

ODPOVĚDNOST VRCHOLOVÉHO VEDENÍ ZA ŠKODU

- dle občanského zákoníku
- dle zákoníku práce

- postavení starosty obce
- postavění členů rady, zastupitelstva obce

CyberSecurityHub.cz

TLP:CLEAR

KYBERNETICKÁ BEZPEČNOST A VEŘEJNÉ ZAKÁZKY

CyberSecurityHub.cz

§ 24
Řízení dodavatelů a vztah k zadávání veřejných zakázek

(1) Poskytovatel regulované služby je povinen zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro svůj stanovený rozsah.
(2) Tam, kde je to možné, je poskytovatel regulované služby povinen zohlednit požadavky vyplývající z bezpečnostních opatření ve smlouvách se svými dodavateli.
(3) Zohlednění požadavků vyplývajících z bezpečnostních opatření při výběru dodavatele v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

TLP:CLEAR

KYBERNETICKÁ BEZPEČNOST A VEŘEJNÉ ZAKÁZKY

CyberSecurityHub.cz

§ 25
Speciální úprava předání informací a dat od významného dodavatele

(1) Úřad může **v případě hrozícího kybernetického bezpečnostního incidentu** na podnět poskytovatele regulované služby **v režimu vyšších povinností**, který marně vyzval významného dodavatele ke splnění smluvního závazku předat informace a data, rozhodnutím **uložit významnému dodavateli povinnost předat poskytovateli regulované služby v režimu vyšších povinností informace a data související s provozem aktiv sloužících k poskytování regulované služby.** Pokud významný dodavatel informacemi nebo daty souvisejícími s provozem aktiv sloužících k poskytování regulované služby nedisponuje nebo vzhledem ke skutkovým okolnostem není účelné po něm požadovat jejich opatření a vydání, může Úřad povinnost podle předchozí věty uložit i jinému orgánu nebo osobě, která požadovanými informacemi a daty disponuje. Úřad může v rozhodnutí určit formát, rozsah, způsob a lhůtu předání a stanovit povinnost po provedení předání tyto informace a data a jejich kopie bezpečně zlikvidovat.
(2) Podnět podle odstavce 1 musí obsahovat odůvodnění požadavku s ohledem na hrozící kybernetický bezpečnostní incident, podrobný popis předchozího jednání mezi významným dodavatelem a poskytovatelem regulované služby v režimu vyšších povinností zejména s ohledem na nesplnění smluvního závazku významného dodavatele a možné následky, pokud nedojde k předání požadovaných informací a dat.
(3) Rozhodnutí o uložení povinnosti předat informace a data podle odstavce 1 může být prvním úkonem v řízení. Rozklad proti rozhodnutí podle věty první nemá odkladný účinek.
(4) Jednání o úhradě vynaložených nákladů na předání informací a dat nesmí být překážkou řádného splnění povinnosti předat informace a data.

TLP:CLEAR

SANKČNÍ PROSTŘEDKY PŘI NEPLNĚNÍ POVINNOSTÍ

- Princip – účinnost a přiměřenost sankcí
- Zohlednění okolností - závažnost, způsobená škoda, doba trvání, úmyslné či nedbalostní jednání
- Sankce nesmí být likvidační.
- Primárně uložení nápravných opatření navazujících na kontroly (§ 56 a 57 KybeZ).
  - kontroly v režimu vyšších povinností - NÚKIB
  - kontroly v režimu nižších povinností - inspektoři - soukromé společnosti/osoby, které provedou audit
- Přestupky a ukládání pokut (§ 58 KybeZ)
  - Pouze horní limit, není spodní limit
  - Rozdělení na vyšší/nižší režim, maximální výše vychází z NIS2 – až 250 miliónů korun nebo 2 % čistého celosvětového ročního obratu
- Nejzazší sankční prostředek – pozastavení výkonu řídicí funkce fyzické osobě (§ 61 KybeZ)

TLP:CLEAR

POZASTAVENÍ VÝKONU ŘÍDICÍ FUNKCE

§ 61
Pozastavení výkonu řídicí funkce

(1) Soud může na návrh Úřadu rozhodnout, že člen statutárního orgánu právnické osoby, vedoucí odštěpného závodu, prokurista nebo podnikající fyzická osoba, která v přímé souvislosti s plněním rozhodnutí Úřadu, kterým byla poskytovateli regulované služby v režimu vyšších povinností uložena povinnost odstranit nedostatky zjištěné při kontrole, opakovaně nebo závažně porušila své povinnosti při výkonu své řídicí funkce, v důsledku čehož bylo zmařeno řádné splnění rozhodnutí Úřadu, nesmí až do doby odstranění nedostatků zjištěných při kontrole, nejméně však po dobu 6 měsíců vykonávat tuto řídicí funkci.

(2) Návrh lze podat pouze vůči osobě vykonávající řídicí funkci u poskytovatele regulované služby v režimu vyšších povinností a pouze ve vztahu k řídicí funkci, která není veřejnou funkcí vymezenou funkčním nebo časovým obdobím a obsazovanou na základě přímé nebo nepřímé volby nebo jmenováním podle zvláštních právních předpisů.

(3) Ustanovení zákona o obchodních korporacích upravující vyloučení člena statutárního orgánu z výkonu funkce se v částech právních účinků pravomocného rozhodnutí o vyloučení člena statutárního orgánu, informování rejstříkového soudu a odpovědnosti za porušení dočasného zákazu výkonu funkce použijí obdobně.

(4) Informaci o pravomocném rozhodnutí o pozastavení výkonu řídicí funkce Úřad zveřejní na svých internetových stránkách.

(5) Úřad, nejdříve však po uplynutí lhůty podle odstavce 1, provede kontrolu splnění povinnosti odstranit nedostatky zjištěné při kontrole a v případě, že zjistí, že nedostatky byly odstraněny, Úřad o tomto vydá osvědčení, které je podkladem pro výmaz údaje o pozastavení řídicí funkce z obchodního rejstříku podle zákona o veřejných rejstřících právnických a fyzických osob.

TLP:CLEAR

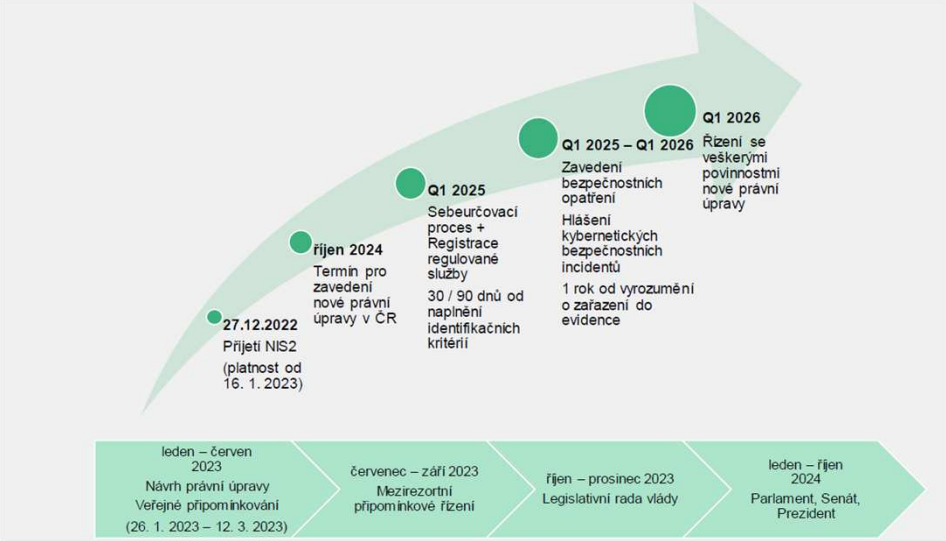
POZASTAVENÍ VÝKONU ŘÍDICÍ FUNKCE

Z důvodové zprávy k § 61:

- *„Pozastavení výkonu řídicí funkce je jedním ze dvou zcela nových správních trestů, jehož zakotvení v právním řádu vyžaduje směrnice NIS 2, konkrétně její čl. 32 odst. 5. … Uvedený článek má za cíl dále posílit účinnost a odrazující účinek opatření v oblasti vymáhání, jež jsou uplatňována v případě porušení směrnice . Citovaný článek je také součástí komplexu opatření pro posílení odpovědnosti vedení základního subjektu za zajišťování kybernetické bezpečnosti, na kterou klade směrnice NIS 2 zvláštní důraz. Doplňuje tak např. články o povinném vzdělávání managementu nebo o odpovědnosti osob oprávněných jednat jménem regulovaného subjektu za plnění povinností spočívajících v zajištění dodržování směrnice.“*

TLP:CLEAR

NIS2 A NOVÝ ZÁKON O KYBERNETICKÉ BEZPEČNOSTI V TERMÍNECH



TLP:CLEAR

NIS2 A NOVÝ ZÁKON O KYBERNETICKÉ BEZPEČNOSTI V TERMÍNECH

CyberSecurityHub.cz

TLP:CLEAR

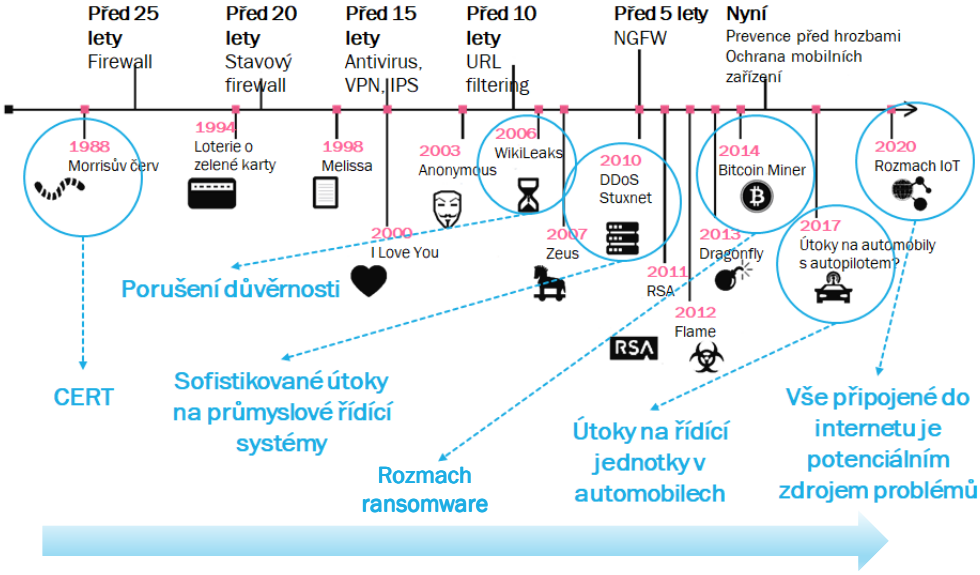
CyberSecurityHub.cz

Úvod do kybernetické bezpečnosti - *Ing. Jiří Sedláček*

- Proč nemůže Vaše IT oddělení odpovídat za kybernetickou bezpečnost.
- Proč je nutné oddělit provozní činnosti a kompetence od činností a kompetencí bezpečnostních.
- Kdo můžou být správné osoby do bezpečnostních rolí.
- Ochrana informací a zajištění kontinuity činností.

TLP:CLEAR

VÝVOJ MALWARE



TLP:CLEAR

KYBERNETICKÁ BEZPEČNOST

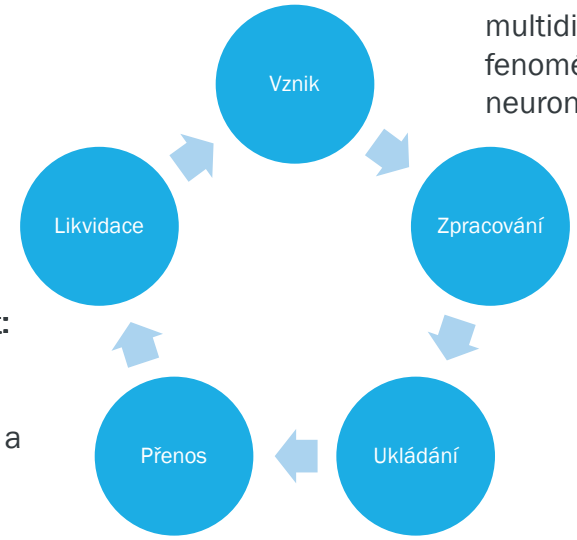
CyberSecurityHub.cz

Souhrn právních, organizačních, technických a vzdělávacích prostředků k zajištění ochrany kybernetického prostoru.

TLP:CLEAR

INFORMAČNÍ **BEZPEČNOST**

Informace je složitý multidimenzionální fenomén podobající se neuronu (prof. Peter Staněk).



Informační bezpečnost: Ochrana informací ve všech formách (elektronické, papírové) a po jejich celý životní cyklus.

CyberSecurityHub.cz

TLP:CLEAR

KYBERNETICKÝ **PROSTOR**

Digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací . *(ZoKB - §2 pís a)*

CyberSecurityHub.cz

TLP:CLEAR

KYBERNETICKÝ **PROSTOR - VRSTVY**

CyberSecurityHub.cz

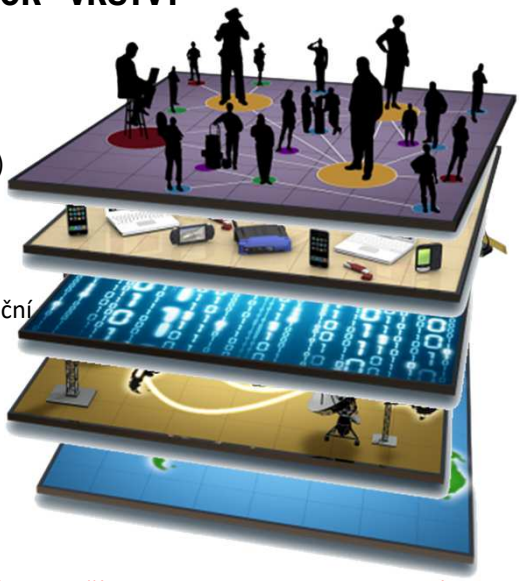
Personální
(osoby, identity)

Rozhraní

Datová/informační

Fyzická

Geografická



iCloud Google Drive OneDrive

Pro výkon suverenity se uvažuje fyzická vrstva infrastruktury, tedy geografická lokalita „železa“

TLP:CLEAR

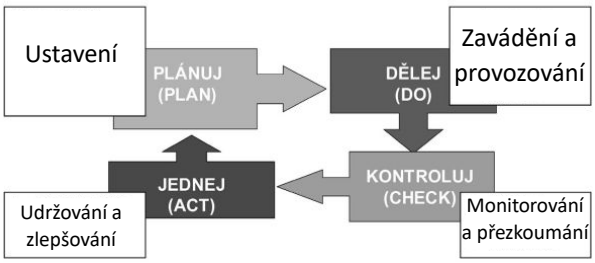
Vaši identitu může mít a zneužít kdokoli, kdekoli v kybernetickém prostoru…

JAK NAPLNIT **POTŘEBY/POŽADAVKY Z OBLASTI KB?**

CyberSecurityHub.cz

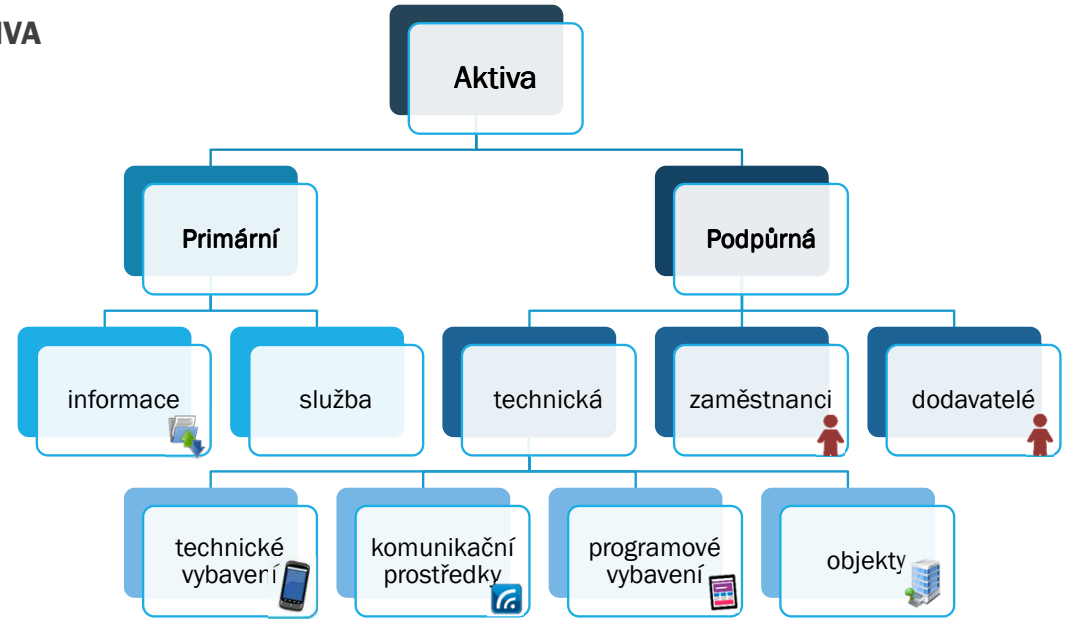
- Ujasnit si, jestli SŘBI/ISMS zavádím z důvodu zákonné povinnosti či dobrovolně a **jaký tedy mám stanovený bezpečnostní rámec.**
- Zavést SŘBI/ISMS **v souladu** s tímto bezpečnostním rámcem.

Demingův cyklus (PDCA)



TLP:CLEAR

AKTIVA



CyberSecurityHub.cz

TLP:CLEAR

REGISTR AKTIV

SŘBI JE ŘÍZENÝM A DOKUMENTOVANÝM...
Registr aktiv bude aktualizován průběžně a opakovaně validován v každé iteraci revize analýzy rizik organizace, jakož i v případě změny podmínek, jež platná analýza ošetřuje.

CyberSecurityHub.cz

- ID Aktiva
- Název aktiva
- Popis aktiva
- Nadřízené aktivum
- Typ aktiva
- Kategorizace aktiva
- Hodnocení dostupnosti (A)
- Hodnocení důvěrnosti (C)
- Hodnocení integrity (I)
- Celkové hodnocení aktiva
- Garant aktiva
- Lokalizace aktiva
- Datum identifikace aktiva

TLP:CLEAR

ORGANIZACE - PŘÍSTUP Z POHLEDU TEORIE ŘÍZENÍ

CyberSecurityHub.cz

Lidé
Zkušení profesionálové.

Procesy
Optimalizované procesy šetřící čas a náklady.

Technologie
Moderní technologie nezbytné pro chod společnosti.

Organizace je v podstatě směs tří základních prvků: lidí, procesů a technologií.

TLP:CLEAR

PŘÍSTUP Z POHLEDU KYBERNETICKÉ BEZPEČNOSTI

CyberSecurityHub.cz

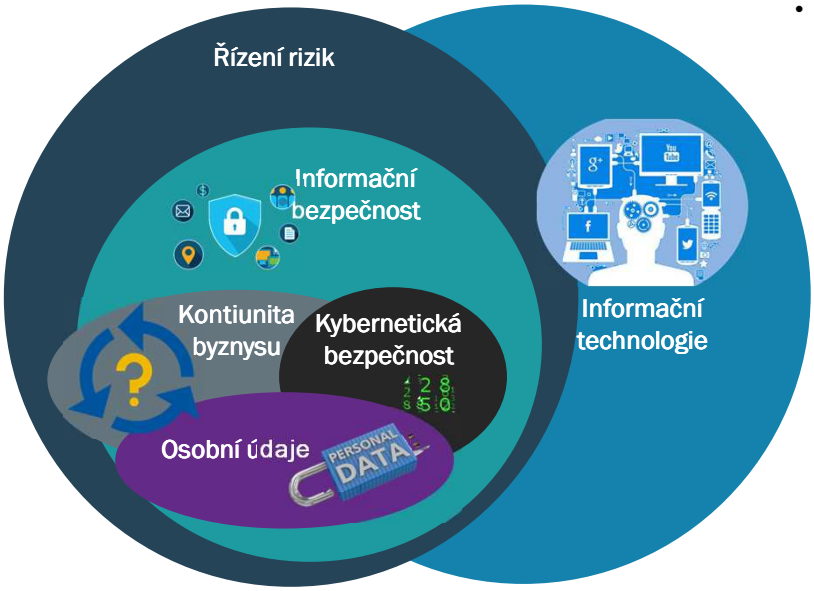
- Systémy detekcí kybernetických událostí a incidentů.
- Systémy zjišťování zranitelností.
- Systémy chránící informace – nutná klasifikace informací.

- Role v souladu se ZoKB.
- Expertní CSIRT tým.
- Ostatní týmy a osoby.

- Procesy řízení kybernetických bezpečnostních událostí a incidentů.
- Procesy zajištění kontinuity.
- Procesy koordinace provozovatelů a dodavatelů.

TLP:CLEAR

JAK NA OCHRANU INFORMACÍ



- Hranice SŘBI/ISMS
- Rozsah SŘBI/ISMS
  - dle ISO 27001
  - dle ZoKB
  - dle jiného zákona či standardu
  - dle MBS NÚKIB
  - ....

CyberSecurityHub.cz

TLP:CLEAR

BEZPEČNOST INFORMACÍ

☞Je nezbytné přijmout taková opatření aby nedošlo k narušení důvěrnosti, integrity a dostupnosti informací. Často **nejsou** v praxi příslušná opatření implementována a to proto, že zpravidla proti sobě stojí dva protichůdné požadavky. Na jedné straně je požadavek na zvyšování kvality poskytovaných služeb, na straně druhé požadavek na snižování nákladů. Zákonitě tak vznikají rizika, která je nutné řídit!

Bezpečností informací rozumíme zajištění důvěrnosti, integrity a dostupnosti informací a dat *(ZoKB §2, pís c)*.

CyberSecurityHub.cz

TLP:CLEAR

KLASIFIKACE INFORMACÍ

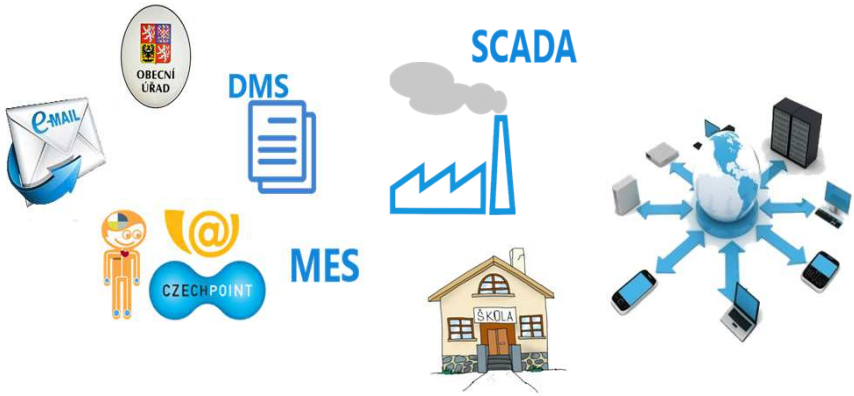
- Pravidla
- Identifikace
- Klasifikace
- Označení
- Zacházení

- **Klasifikace informací:** proces, ve kterém je informaci přiřazen určitý stupeň klasifikace s ohledem na její význam pro organizaci.
- **Klasifikační stupně:** škála, podle které se provádí klasifikace informací.

CyberSecurityHub.cz

TLP:CLEAR

KONTINUITA ČINNOSTÍ



Business Continuity = strategická a taktická způsobilost organizace být připraven a reagovat na incidenty a narušení činností organizace za účelem pokračování na předem stanovené přijatelné úrovni.

CyberSecurityHub.cz

TLP:CLEAR

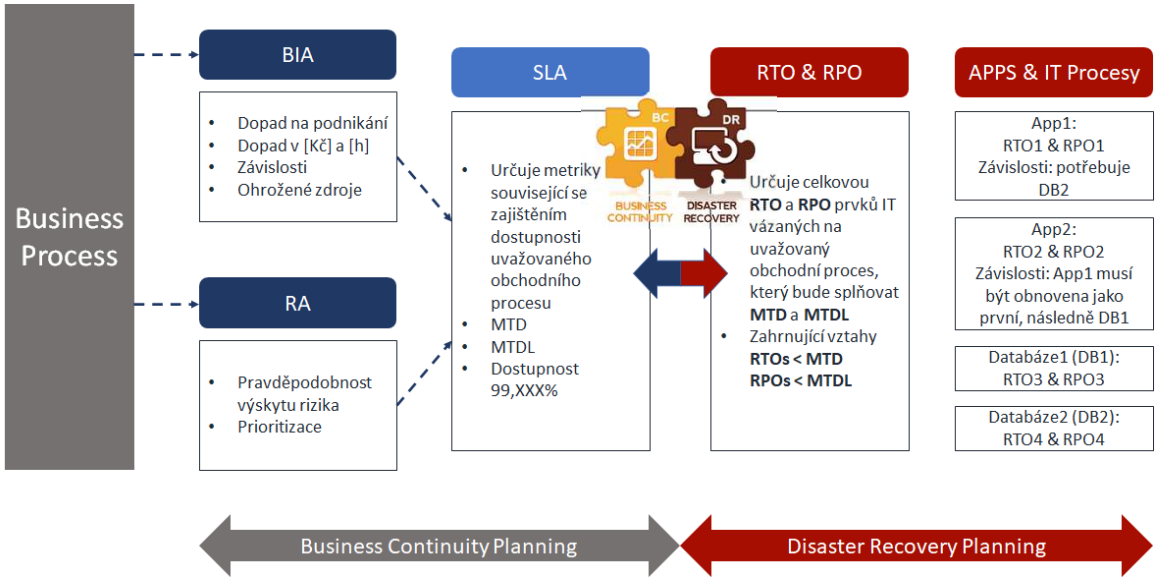
KONTINUITA ČINNOSTÍ

Závěr vyšetřovací komise:

- **nedodržení podmínek**, na které byl plánovaný pokus připraven,
- **obecný nedostatek bezpečnostní kultury,**
- **elektrárenští operátoři nebyli dostatečně vyškoleni a obeznámeni s charakteristikami reaktoru.**

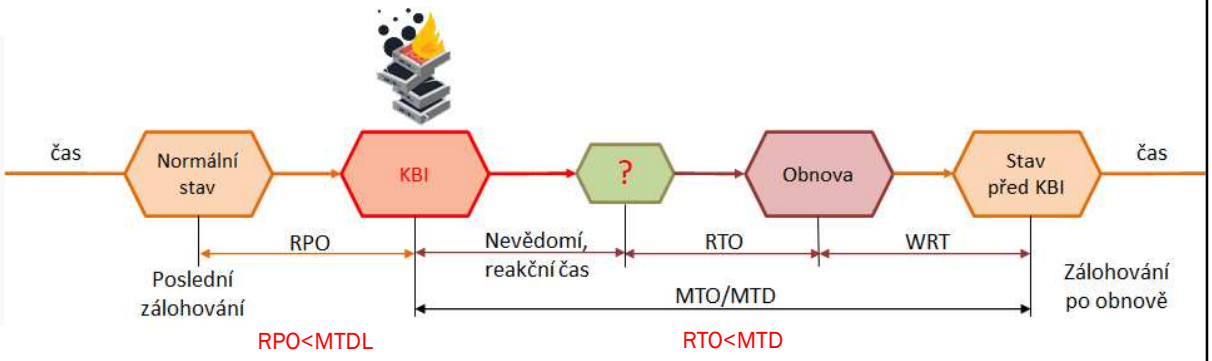
TLP:CLEAR

KONTINUITA ČINNOSTÍ



TLP:CLEAR

KONTINUITA ČINNOSTÍ



CyberSecurityHub.cz

TLP:CLEAR

ŘEŠÍ IT KYBERNETICKOU BEZPEČNOST?

Provozně procesní pohled

- IT oddělení udržuje ICT v chodu – jedná se o provozní, nikoli bezpečnostní oddělení,
  - aplikace nových záplat a aktualizace firmware jsou riskantní…
    => nechuť IT provádět aktualizace.
- IT oddělení je často vnímáno pouze jako podpůrné oddělení, které musí všem vyhovět…
- IT pracovníci nemohou z pohledu své pracovní náplně definovat primární aktiva.

Osobnostní pohled

- IT zaměstnanci jsou často introvertními osobnostmi,
- IT zaměstnanci neradi dokumentují svoje činnosti,
  - z důvodu přetíženosti,
  - z osobních důvodů.

Organizační a finanční pohled

- IT oddělení je často podřízeno finančnímu řediteli organizace.
  - veškerá rozhodnutí o nákupech jsou často blokována,
  - bezpečnostní opatření (zvláště technická) nejsou zadarmo…
  - IT oddělení má v majetku veškeré ICT a je proto vnímáno jako oddělení, kde by se mělo šetřit,
  - IT oddělení se díky úsporám potýká s lidskými zdroji.
- IT oddělení nemůže být zodpovědné za aplikaci bezpečnostních opatření v organizaci, protože by kontrolovalo samo sebe…

CyberSecurityHub.cz

TLP:CLEAR

IT VERSUS KB

Rozdílné požadavky

IT

- Zajištění provozu.

KB

- Chránit informace.
- Zajistit kontinuitu činností.

- **Bezpečnostním opatřením** se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru *(ZoKB, §4, (1))*
- **Bezpečnostními opatřeními** jsou *(ZoKB, §5, (1))*
  - Organizační opatření,
  - Technická opatření.

byznys kontinuita

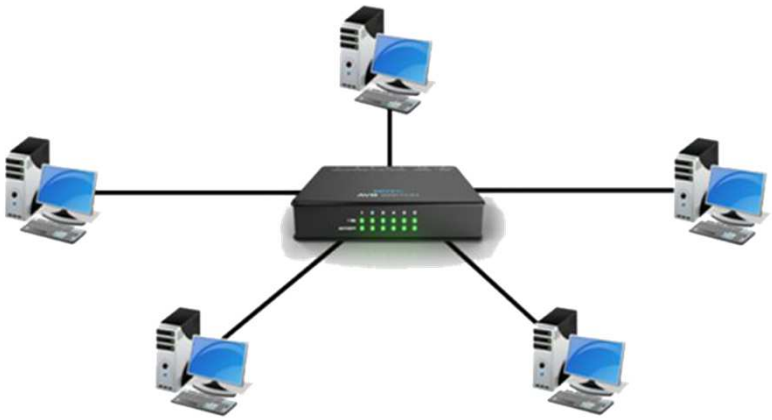
ochrana informací (CIA)

Podstata

- **Provoz „umožňuje“** ve smyslu poskytuje
- **Bezpečnost „omezuje“** ve smyslu chrání

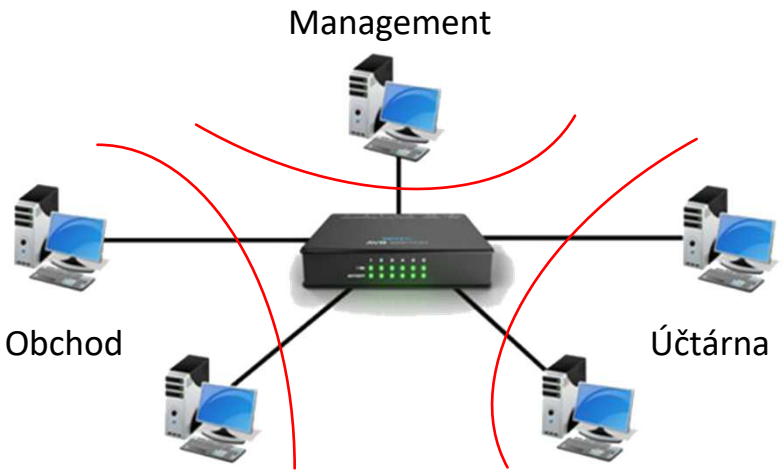
TLP:CLEAR

PŘÍSTUP Z POHLEDU IT



TLP:CLEAR

PŘÍSTUP Z POHLEDU KB



TLP:CLEAR

PŘEKÁŽKY PŘI ŘEŠENÍ IB/KB

Odpor

- Managementu (častá ignorance, zlehčování a nepochopení závažnosti).
- IT (nechuť dokumentovat, být kontrolován).
- Zaměstnanců
  - Každá nová restrikce je často vnímána odmítavě.
  - Lidé nechtějí mít přidělenu další práci a odpovědnost.
- V oblasti OÚ - správce nechce být správcem a zpracovatel zpracovatelem.

Neschopnost stanovit rozsah a hranice SŘBI/ISMS

- Primární aktiva a jejich ohodnocení, podpůrná aktiva,...

Obecně nedostatek dobré vůle (začíná to u managementu) a finančních zdrojů...

TLP:CLEAR

BEZPEČNOSTNÍ ROLE

https://www.zakonyprolidi.cz/cs/2018-82#p7

Manažer kybernetické bezpečnosti
- Je bezpečnostní role **odpovědná za systém řízení bezpečnosti informací**.
- Nesmí být pověřen výkonem rolí odpovědných za provoz informačního a komunikačního systému.

Architekt kybernetické bezpečnosti
- Je bezpečnostní role **odpovědná za zajištění návrhu implementace bezpečnostních opatření** tak, aby byla zajištěna bezpečná architektura informačního a komunikačního systému.

Auditor kybernetické bezpečnosti
- Je bezpečnostní role **odpovědná za provádění auditu kybernetické bezpečnosti**.
- Nesmí být pověřen výkonem jiných bezpečnostních rolí.

Garant aktiva
- Je bezpečnostní role **odpovědná za zajištění rozvoje, použití a bezpečnost aktiva** (tuto roli nelze outsourcovat).

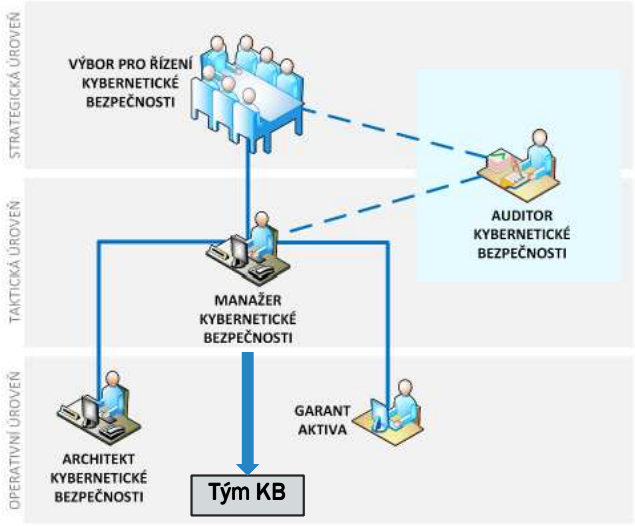
- praxe po dobu nejméně tří let, nebo
- praxe po dobu jednoho roku, pokud absolvoval studium na vysoké škole

Detailní informace k bezpečnostním rolím lze čerpat z Přílohy č. 6 k vyhlášce č. 82/2018 Sb.

CyberSecurityHub.cz

TLP:CLEAR

HIERARCHIE BEZPEČNOSTNÍCH ROLÍ



Obr. 2: Hierarchie bezpečnostních rolí

Role
Jmenování a statuty.

Výbor – jmenování, statut, jednací řád.

Vyváženost práv a povinností.

Manažer KB – odpovědný za SŘBI – mj. právo „vypnout“ organizaci.

CyberSecurityHub.cz

TLP:CLEAR

CyberSecurityHub.cz

Kybernetická bezpečnost prakticky - *Ing. Robert Schindler, MSc.*

- Pragmatický přístup ke kybernetické bezpečnosti.
- Jak řešit kybernetickou bezpečnost, když odborníci chybí.
- Nezbytné minimum aneb jaká organizačních pravidla a jaká technická opatření, které musí být nastavena.
- Jak chránit informace a zajistit kontinuitu činností obce či organizace, aneb krizové řízení je obtížné outsourcovat.

TLP:CLEAR

CyberSecurityHub.cz

KYBERNETICKÁ BEZPEČNOST PRAKTICKY – KDO ?

Ing. Robert Schindler, MSc.

Manažer kybernetické bezpečnosti

2015 – Ministerstvo financí ČR – první MKB
člen meziresortní pracovní skupiny pro vzorové Metodiky KB

Architekt kybernetické bezpečnosti

od 2018 AKB Technické sítě Brno
AKB Statutární město Brno
od 2021 AKB Brněnské komunikace

2021 – 2022 AKB Fakultní nemocnice Brno

TLP:CLEAR

CELOSVĚTOVÉ ROČNÍ NÁKLADY SPOJENÉ S KYBERKRIMINALITOU

5,5 bilionu Eur

5 500 000 000 000 Eur

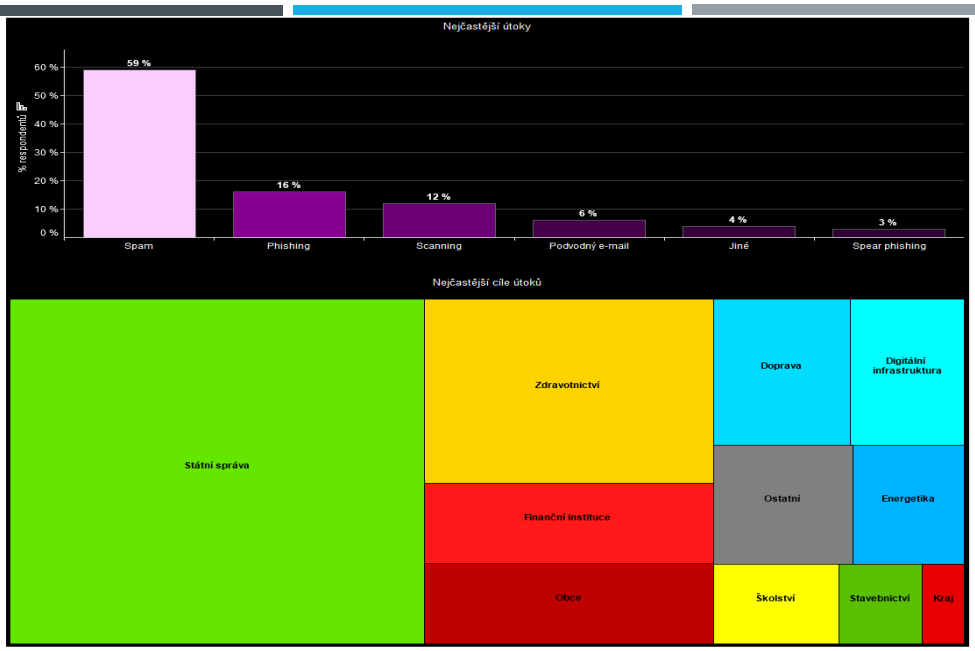
132 000 000 000 000 Kč

Plánovaná cena nové nemocnice ve Zlíně **8 Miliard Kč**
= cca **16 500 nemocnic**

Rusko utratilo za válku do konce 2022 odhadem **1 900 Miliard Kč**.

CyberSecurityHub.cz

TLP:CLEAR



CyberSecurityHub.cz

TLP:CLEAR

PŘEDKOPLÁDANÉ ZAŘAZENÍ OBCE PODLE NIS2

CyberSecurityHub.cz

- Obec se stane poskytovatelem v režimu **nižších povinností**
- Regulovanou službou podle VRS je „**Výkon svěřených pravomocí**“
- Kritériem pro režim nižších povinností je:
  - „Obec s rozšířenou působností s méně než 125 000 obyvateli“

- Obce v režimu vyšších povinností:
  - Brno
  - Ostrava
  - Plzeň

TLP:CLEAR

POČTY OBYVATEL OBCÍ K ZAŘAZENÍ DLE NIS2

CyberSecurityHub.cz

Správní obvod	Počet celkem ve správním obvodu		Obec	Počet obyvatel v obci
Brno	396 101		Brno	396 101
Ostrava	316 149		Ostrava	283 504
Plzeň	201 517		Plzeň	181 240
Olomouc	167 827		Liberec	107 389
České Budějovic	166 778		Olomouc	101 825
Černošice	158 235			
Liberec	149 554			
Hradec Králové	148 986			
Pardubice	134 359			
Kladno	126 779			

TLP:CLEAR

CO S PŘÍPRAVOU NIS2 NA OBCI

CyberSecurityHub.cz

V současnosti je nesmysl provádět jakoukoli rozdílovou analýzu GAP proti NIS2

- Legislativa pro NIS2 není platná a teprve se v meziresortu vypořádávají připomínky
- Není tedy vůči čemu hodnověrně porovnávat

Co s tím ?

- Dá se něco dělat do doby než bude účinná legislativa ?

TLP:CLEAR

POSOUZENÍ DLE BEST-PRACTISE

CyberSecurityHub.cz

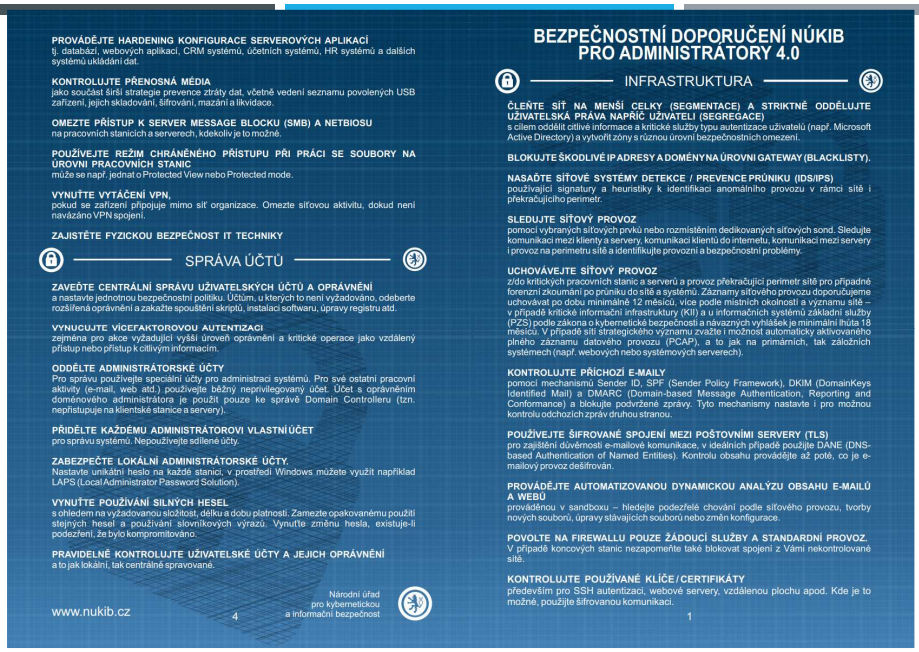
NÚKIB vydal a aktualizuje 2 praktické „kuchařky“ k zabezpečení vlastní infrastruktury

- **Bezpečnostní doporučení NÚKIB pro administrátory X.X**
  - Infrastruktura
  - Uživatelé
  - Stanice & Servery
- **Minimální bezpečnostní standard**
  - Manažerská část (organizační opatření)
  - Technická část

Souhrn praktických bodů a doporučení bez ohledu na to, zda je subjekt zařazený pod zákon o kybernetické bezpečnosti.

„Papírové posouzení“

TLP:CLEAR



PROVÁDĚJTE HARDENING KONFIGURACE SERVEROVÝCH APLIKACÍ
tj. databází, webových aplikací, CRM systémů, účetních systémů, HR systémů a dalších systémů ukládání dat.

KONTROLUJTE PŘENOSNÁ MÉDIA
jako součást širší strategie prevence ztráty dat, včetně vedení seznamu povolených USB zařízení, jejich skladování, šifrování, mazání a likvidace.

OMEZTE PŘÍSTUP K SERVER MESSAGE BLOCKU (SMB) A NETBIOSU
na pracovních stanicích a serverech, kdekoliv je to možné.

POUŽÍVEJTE REŽIM CHRÁNĚNÉHO PŘÍSTUPU PŘI PRÁCI SE SOUBORY NA ÚROVNI PRACOVNÍCH STANIC
může se např. jednat o Protected View nebo Protected mode.

VYNUŤTE VYTÁČENÍ VPN,
pokud se zařízení připojuje mimo síť organizace. Omezte síťovou aktivitu, dokud není navázáno VPN spojení.

ZAJISTĚTE FYZICKOU BEZPEČNOST IT TECHNIKY

SPRÁVA ÚČTŮ

ZAVEĎTE CENTRÁLNÍ SPRÁVU UŽIVATELSKÝCH ÚČTŮ A OPRÁVNĚNÍ
a nastavte jednotnou bezpečnostní politiku. Účtům, u kterých to není vyžadováno, odeberte rozšířená oprávnění a zakažte spouštění skriptů, instalaci softwaru, úpravy registru atd.

VYNUCUJTE VÍCEFAKTOROVOU AUTENTIZACI
zejména pro akce vyžadující vyšší úroveň oprávnění a kritické operace jako vzdálený přístup nebo přístup k citlivým informacím.

ODDĚLTE ADMINISTRÁTORSKÉ ÚČTY
Pro správu používejte speciální účty pro administraci systémů. Pro své ostatní pracovní aktivity (e-mail, web atd.) používejte běžný neprivilegovaný účet. Účet s oprávněním doménového administrátora je použít pouze ke správě Domain Controlleru (tzn. nepřistupuje na klientské stanice a servery).

PŘIDĚLTE KAŽDÉMU ADMINISTRÁTOROVI VLASTNÍ ÚČET
pro správu systémů. Nepoužívejte sdílené účty.

ZABEZPEČTE LOKÁLNÍ ADMINISTRÁTORSKÉ ÚČTY.
Nastavte unikátní heslo na každé stanici, v prostředí Windows můžete využít například LAPS (Local Administrator Password Solution).

VYNUŤTE POUŽÍVÁNÍ SILNÝCH HESEL
s ohledem na vyžadovanou složitost, délku a dobu platnosti. Zamezte opakovanému použití stejných hesel a používání slovníkových výrazů. Vynuťte změnu hesla, existuje-li podezření, že bylo kompromitováno.

PRAVIDELNĚ KONTROLUJTE UŽIVATELSKÉ ÚČTY A JEJICH OPRÁVNĚNÍ
a to jak lokální, tak centrálně spravované.

www.nukib.cz

4

Národní úřad pro kybernetickou a informační bezpečnost

BEZPEČNOSTNÍ DOPORUČENÍ NÚKIB PRO ADMINISTRÁTORY 4.0

INFRASTRUKTURA

ČLEŇTE SÍŤ NA MENŠÍ CELKY (SEGMENTACE) A STRIKTNĚ ODDĚLUJTE UŽIVATELSKÁ PRÁVA NAPŘÍČ UŽIVATELI (SEGREGACE)
s cílem oddělit citlivé informace a kritické služby typu autentizace uživatelů (např. Microsoft Active Directory) a vytvořit zóny s různou úrovní bezpečnostních omezení.

BLOKUJTE ŠKODLIVÉ IP ADRESY A DOMÉNY NA ÚROVNI GATEWAY (BLACKLISTY).

NASAĎTE SÍŤOVÉ SYSTÉMY DETEKCE / PREVENCE PRŮNIKU (IDS/IPS)
používající signatury a heuristiky k identifikaci anomálního provozu v rámci sítě i překračujícího perimetr.

SLEDUJTE SÍŤOVÝ PROVOZ
pomocí vybraných síťových prvků nebo rozmístěním dedikovaných síťových sond. Sledujte komunikaci mezi klienty a servery, komunikaci klientů do internetu, komunikaci mezi servery i provoz na perimetru sítě a identifikujte provozní a bezpečnostní problémy.

UCHOVÁVEJTE SÍŤOVÝ PROVOZ
z/do kritických pracovních stanic a serverů a provoz překračující perimetr sítě pro případné forenzní zkoumání po průniku do sítě a systémů. Záznamy síťového provozu doporučujeme uchovávat po dobu minimálně 12 měsíců, více podle místních okolností a významu sítě – v případě kritické informační infrastruktury (KII) a u informačních systémů základní služby (PZS) podle zákona o kybernetické bezpečnosti a návazných vyhlášek je minimální lhůta 18 měsíců. V případě sítí strategického významu zvažte i možnost automaticky aktivovaného plného záznamu datového provozu (PCAP), a to jak na primárních, tak záložních systémech (např. webových nebo systémových serverech).

KONTROLUJTE PŘÍCHOZÍ E-MAILY
pomocí mechanismů Sender ID, SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) a DMARC (Domain-based Message Authentication, Reporting and Conformance) a blokujte podvržené zprávy. Tyto mechanismy nastavte i pro možnou kontrolu odchozích zpráv druhou stranou.

POUŽÍVEJTE ŠIFROVANÉ SPOJENÍ MEZI POŠTOVNÍMI SERVERY (TLS)
pro zajištění důvěrnosti e-mailové komunikace, v ideálních případě použijte DANE (DNS-based Authentication of Named Entities). Kontrolu obsahu provádějte až poté, co je e-mailový provoz dešifrován.

PROVÁDĚJTE AUTOMATIZOVANOU DYNAMICKOU ANALÝZU OBSAHU E-MAILŮ A WEBŮ
prováděnou v sandboxu – hledejte podezřelé chování podle síťového provozu, tvorby nových souborů, úpravy stávajících souborů nebo změn konfigurace.

POVOLTE NA FIREWALLU POUZE ŽÁDOUCÍ SLUŽBY A STANDARDNÍ PROVOZ.
V případě koncových stanic nezapomeňte také blokovat spojení z Vámi nekontrolované sítě.

KONTROLUJTE POUŽÍVANÉ KLÍČE / CERTIFIKÁTY
především pro SSH autentizaci, webové servery, vzdálenou plochu apod. Kde je to možné, použijte šifrovanou komunikaci.

1

TLP:CLEAR

REÁLNÉ ZJIŠTĚNÍ STAVU ODOLNOSTI – BEZPEČNOSTNÍ TESTY

- **Provedení bezpečnostního posouzení MS Active Directory**
  - Většinou nejslabší část celého ICT
  - Obsahuje uživatelské účty a při kompromitaci účtu vysoké riziko úspěšného kybernetického útoku
- **Provedení testování technických zranitelností**
  - Zapojení testovací sondy do infrastruktury
  - Doba trvání minimálně 2 – 3 týdny
  - Umí zjistit slabě zabezpečené a rizikové systémy
- **Provedení analýzy datových toků**
  - Zapojení síťové sondy do interní infrastruktury
  - Doba trvání minimálně 4 týdny
  - Umí odhalit začínající kybernetický útok

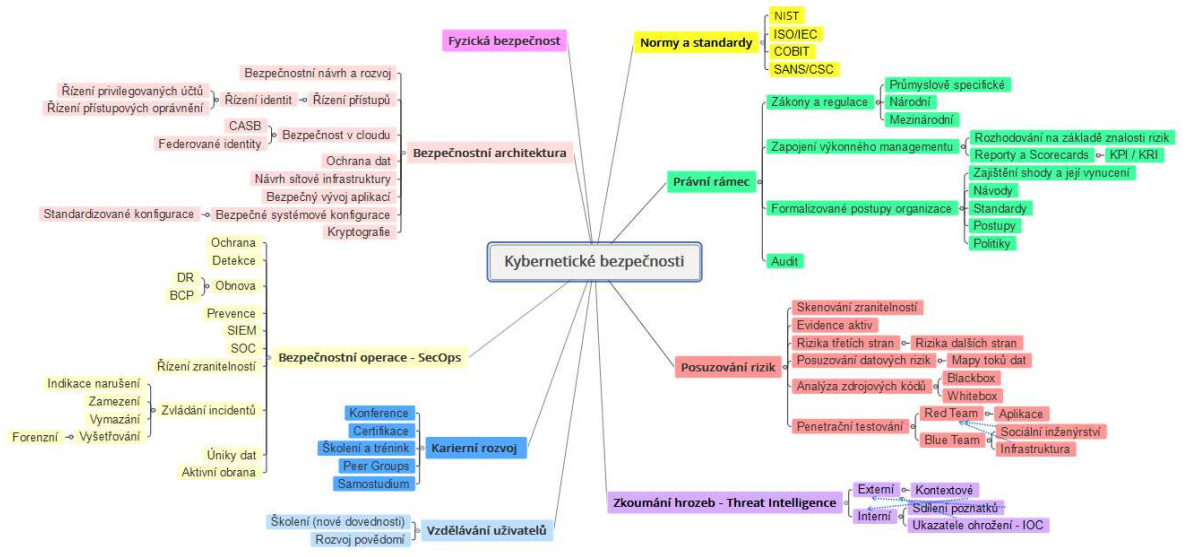
TLP:CLEAR

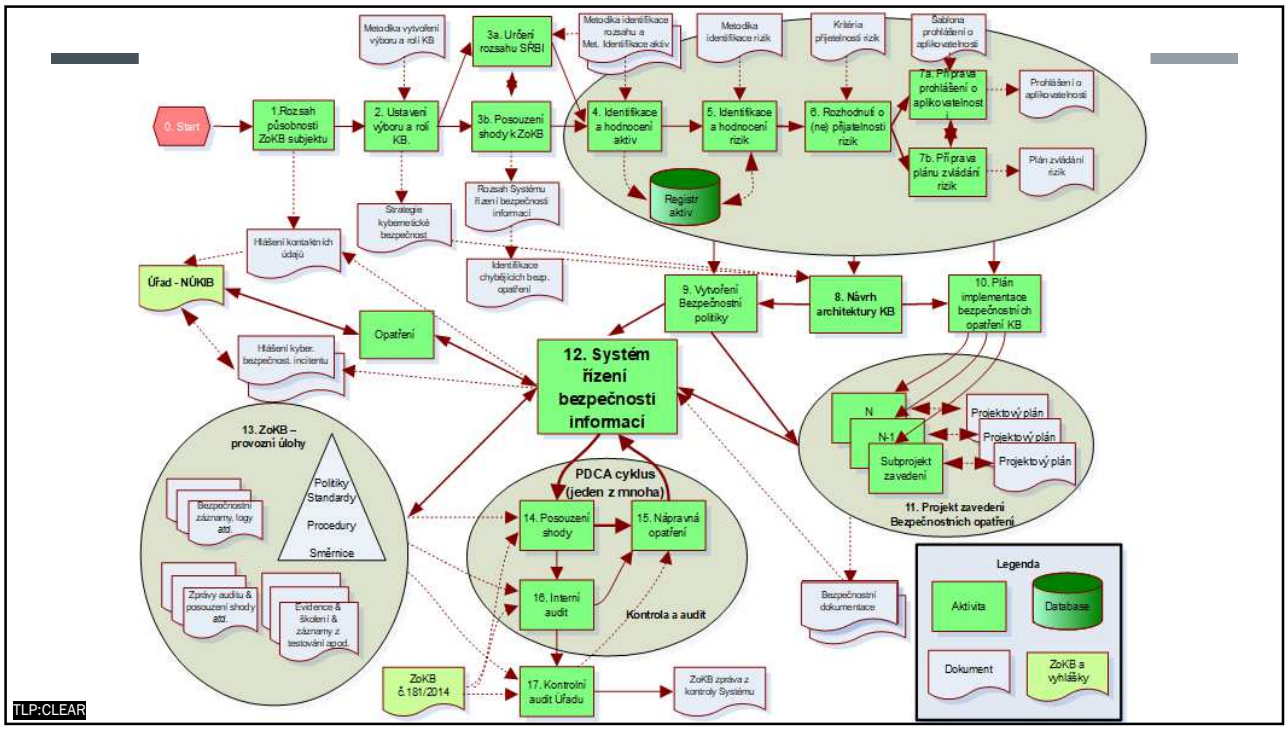
GENERALIZOVANÉ VÝSLEDKY BEZPEČNOSTNÍHO POSOUZENÍ

- **Technické bezpečnostní opatření se pořídila, ale nikdo je nesleduje a nevyhodnocuje**
  - Bez ohledu kolik stála, opatření jsou neúčinná
- **Segmentace sítě, pokud existuje, tak je provozně orientovaná**
  - Nechrání na síťové úrovni a viry se mohou šířit
- **Havarijní nebo krizové plány pro Kybernetickou bezpečnost neexistují**
  - Není jasné co dělat, když už začne kyber. útok nebo incident – Kdo řídí a velí ?
- **Zálohy nebo způsoby obnovy dat se netestují**
  - Poslední záchrana se ukáže nefunkční = poškozené nebo taky zašifrované zálohy (Ransomware)
- **Bezpečnostní testy se nedělaly nebo nedělají**
  - Neví se slabiny, takže se ani neodstraňují

CyberSecurityHub.cz

TLP:CLEAR





OPATŘENÍ NÁVRHU VYHLÁŠKY – REŽIM NIŽŠÍ POVINNOSTI

§ 4	Zajišťování minimální úrovně kybernetické bezpečnosti	Organizační opatření
§ 5	Povinnosti vrcholového vedení	
§ 6	Bezpečnostní role	
§ 7	Řízení bezpečnostní politiky a bezpečnostní dokumentace	
§ 8	Řízení aktiv	
§ 9	Řízení dodavatelů	
§ 10	Bezpečnost lidských zdrojů	
§ 11	Řízení změn, akvizice, vývoje a údržby	
§ 12	Řízení přístupu	
§ 13	Zvládání kybernetických bezpečnostních událostí a incidentů	
§ 14	Řízení kontinuity činností	
§ 15	Fyzická bezpečnost	Technická opatření
§ 16	Bezpečnost komunikačních sítí	
§ 17	Správa a ověřování identit	
§ 18	Řízení přístupových oprávnění	
§ 19	Detekce kybernetických bezpečnostních událostí	
§ 20	Zaznamenávání událostí	
§ 21	Aplikační bezpečnost	
§ 22	Kryptografické algoritmy	
§ 23	Zajišťování dostupnosti regulované služby	
§ 24	Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv	

CyberSecurityHub.cz

TLP:CLEAR

ORGANIZACE - PŘÍSTUP Z POHLEDU TEORIE ŘÍZENÍ

CyberSecurityHub.cz

Lidé
Zkušení profesionálové.

Procesy
Optimalizované procesy šetřící čas a náklady.

Technologie
Moderní technologie nezbytné pro chod společnosti.

Organizace je v podstatě směs tří základních prvků: lidí, procesů a technologií.

TLP:CLEAR

PRVKY BEZPEČNOSTI Z JINÉHO POHLEDU

CyberSecurityHub.cz

Lidé

- Zaměstnanci – nejslabší prvek kybernetické bezpečnosti
- Odborníci na KB – nejobtížněji získatelný prvek KB
  - Chybějící lidé / zaměstnanci v části kybernetické bezpečnosti.

Technologie

- Nejsnadněji získatelné bezpečnostní opatření
- Samy o sobě nejsou samospasitelné
- Bez organizačních opatření = procesů a lidí nejsou dostatečně účinné

Procesy

- Klíčové pro zajištění funkčnosti a hlavně účinnosti bezpečnostních opatření
- Propojují technologie a osoby

TLP:CLEAR

JAK ŘEŠIT KYBERNETICKOU BEZPEČNOST, KDYŽ ODBORNÍCI CHYBÍ.

- Určitě potřebujete vašeho vlastního pracovníka, který bude mít **U VÁS** odpovědnost za kybernetickou bezpečnost.
- Nemusí to být nezbytně nutně odborník na kybernetickou bezpečnost, stačí osoba schopná věci interně řídit a organizovat i v rámci zvládání **krizových situací.**
- Tato osoba se dá postupně vyškolit a vzdělat, jen musí sama chtít. Podmínka NUTNÁ!

- K této interní KB osobě zajistěte aspoň jednoho externího KB odborníka např. v roli Architekta KB, která bude odborně podporovat vaši odpovědnou osobu za KB a současně tento externí KB odborník nebude řešit vlastní dodávky technologií
- Proč hned nepořídit externího Manažera KB ? Krizové řízení lze obtížně zajistit externě službou !
- Více obcí může sdílet jednoho externího KB odborníka.

TLP:CLEAR

STANDARDY KYBER. BEZPEČNOSTI MČ

Pro brněnské městské části jsme vytvořili vodítko co prioritně dělat:
„Minimální standardy kybernetické bezpečnosti“ schváleno RMB

- **Požadavky v oblasti ochrany před škodlivým kódem**
  - Zajištění základní detekce na koncových zařízení
- **Zajištění aktualizací SW**
  - Minimalizace zranitelností prostřednictvím aktualizací
- **Segmentace sítě**
  - Oddělené části sítě včetně podpory Firewallem
- **Požadavky na emailový systém**
  - Aktualizovaná a účinná Antimalwarová ochrana
- **Zálohování a Havarijní plány**
  - Odolný a zkontrolovaný zálohovací systém
  - Primární cíl Ransomware útoků

TLP:CLEAR

PRIORITY ORGANIZAČNÍCH BEZPEČNOSTNÍCH OPATŘENÍ

Zajišťování minimální úrovně kybernetické bezpečnosti	**0**
Povinnosti vrcholového vedení	**1**
Bezpečnostní role	**1**
Řízení bezpečnostní politiky a bezpečnostní dokumentace	**4**
Řízení aktiv	**3**
Řízení dodavatelů	**5**
Bezpečnost lidských zdrojů	**5**
Řízení změn, akvizice, vývoje a údržby	**4**
Řízení přístupu	**3**
Zvládání kybernetických bezpečnostních událostí a incidentů	**2**
Řízení kontinuity činností	**2**

CyberSecurityHub.cz

TLP:CLEAR

JAK VYPADÁ KYBERNETICKÝ ÚTOK RANSOMWARE

1. **Fáze**
   Trvalé automatizované útoky – už nepřestanou
   Zvenku hledání zranitelných míst,
   Zevnitř je hlavně používání **Sociotechnik útoků** - Ženy naletí na „slevy“, muži na falešné investice
2. **Fáze**
   Malware je uvnitř a „šmejdí po síti – to trvá hodiny, dny, týdny
   Zatím neškodí, jen zjišťuje jako zloděj.
   V této fázi se dá detekovat a hlavně zastavit !
3. **Fáze**
   Útočník ví co potřebuje a spouští útok – **útok trvá minuty, nebo desítky**
   Nejdřív ničí zálohy a pak vše ostatní

CyberSecurityHub.cz

TLP:CLEAR

Děkujeme za pozornost

Váš tým KB

CyberSecurityHub.cz

Ing. Jiří Sedláček
Mail: jiri.sedlacek@nsmcluster.com
Mobile: +420 602 129 224

Ing. Robert Schindler, MSc.
Mail: schindler@elat.cz
Mobile: +420 602 625 123

Mgr. Petr Pernica
Mail: advokat@petrpernica.cz
Mobile: +420 728 783 904

TLP:CLEAR