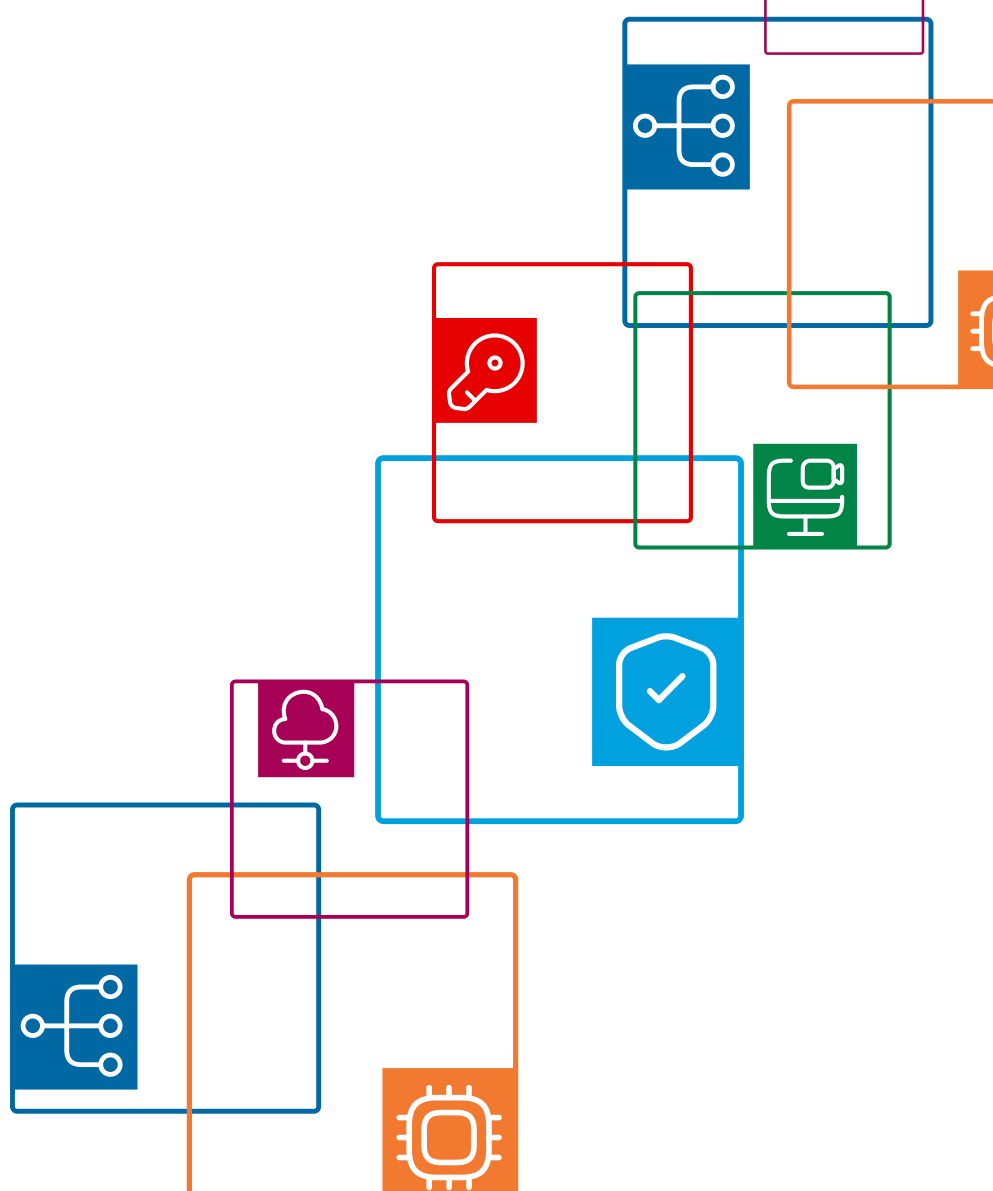
cesnet

Analýza rizik

Andrea Kropáčová

9. 9. 2026, DTU, Pardubice



Úvod

- O čem tato prezentace nebude
  - nebude to kompletní výklad toho, jak se analýza rizik dělá
- O čem bude
  - vybrané postřehy a doporučení
- Proč
  - důležitý prvek řízení (kybernetické bezpečnosti)
  - zákon č. 264/2025 Sb., o kybernetické bezpečnosti (dále nZKB)

Zdroj pro tuto prezentaci

- Zavádění ISMS podle ISO27000 v CESNET (rozhodnutí 2014)
- CESNET je povinný subjekt zákona o kybernetické bezpečnosti
- Certifikace, kontroly, audity (vlastní, zakázkové)
- Konzultace

Zdroj pro tuto prezentaci

- Zavádění ISMS podle ISO27000 v CESNET (rozhodnutí 2014)
- CESNET je povinný subjekt zákona o kybernetické bezpečnosti
- Certifikace, kontroly, audity (vlastní, zakázkové)
- Konzultace
- Semináře Teorie a praxe nového zákona o kybernetické bezpečnosti

Zdroj pro tuto prezentaci

- Zavádění ISMS podle ISO27000 v CESNET (rozhodnutí 2014)
- CESNET je povinný subjekt zákona o kybernetické bezpečnosti
- Certifikace, kontroly, audity (vlastní, zakázkové)
- Konzultace
- Semináře Teorie a praxe nového zákona o kybernetické bezpečnosti
- **Proces, kdy CESNET je zákazníkem označen za významného dodavatele**
- **Proces, kdy se zákazník snaží CESNET označit za významného dodavatele**

Zdroj pro tuto prezentaci

- Zavádění ISMS podle ISO27000 v CESNET (rozhodnutí 2014)
- CESNET je povinný subjekt zákona o kybernetické bezpečnosti
- Certifikace, kontroly, audity (vlastní, zakázkové)
- Konzultace
- Semináře Teorie a praxe nového zákona o kybernetické bezpečnosti
- **Proces, kdy CESNET je zákazníkem označen za významného dodavatele**
- **Proces, kdy se zákazník snaží CESNET označit za významného dodavatele**
- **Proces, kdy se zákazník snaží, aby se CESNET směrem k němu sám identifikoval jako významný dodavatel a zdůvodnil tuto roli ;-)**

- Dva formální rámce
  - ČSN EN ISO/IEC 27001:2023
    - 2015 – rozhodnutí o zavedení ISMS
    - 2018 – certifikace
  - zákon o kybernetické bezpečnosti (od 1. 11. 2025 zákon č. 264/2025 Sb.)
    - 2015 – povinný subjekt
    - 2022 – prvek KII
    - 2026 – provozovatel regulovaných služeb
      - 16.8 **Poskytování služby cloud computingu** (odvětví: Digitální infrastruktura a služby)
      - 19.1 **Výzkum a vývoj** (odvětví: Věda, výzkum a vzdělávání)

Analýza rizik

- Riziko, je nebezpečí vzniku události, která může negativně ovlivnit dosažení stanovených cílů nebo plnění úkolů.
- Systematický proces identifikace, hodnocení a stanovení priorit rizik, která mohou negativně ovlivnit cíle, aktiva, procesy (obecně zájmy) organizace.
- Slouží jako podklad pro řízení rizik.
- Základní kroky:
  - Identifikace rizik – určení potenciálních hrozeb a zranitelností
  - Hodnocení pravděpodobnosti – jak často nebo s jakou pravděpodobností může riziko nastat
  - Identifikace dopadů – jaké následky by mělo riziko na organizaci (finanční, reputační, provozní atd.).
  - Stanovení úrovně rizika – kombinace pravděpodobnosti a dopadu.
  - Prioritizace rizik – seřazení podle závažnosti pro účely řízení.

Pomůcky a prerekvizity

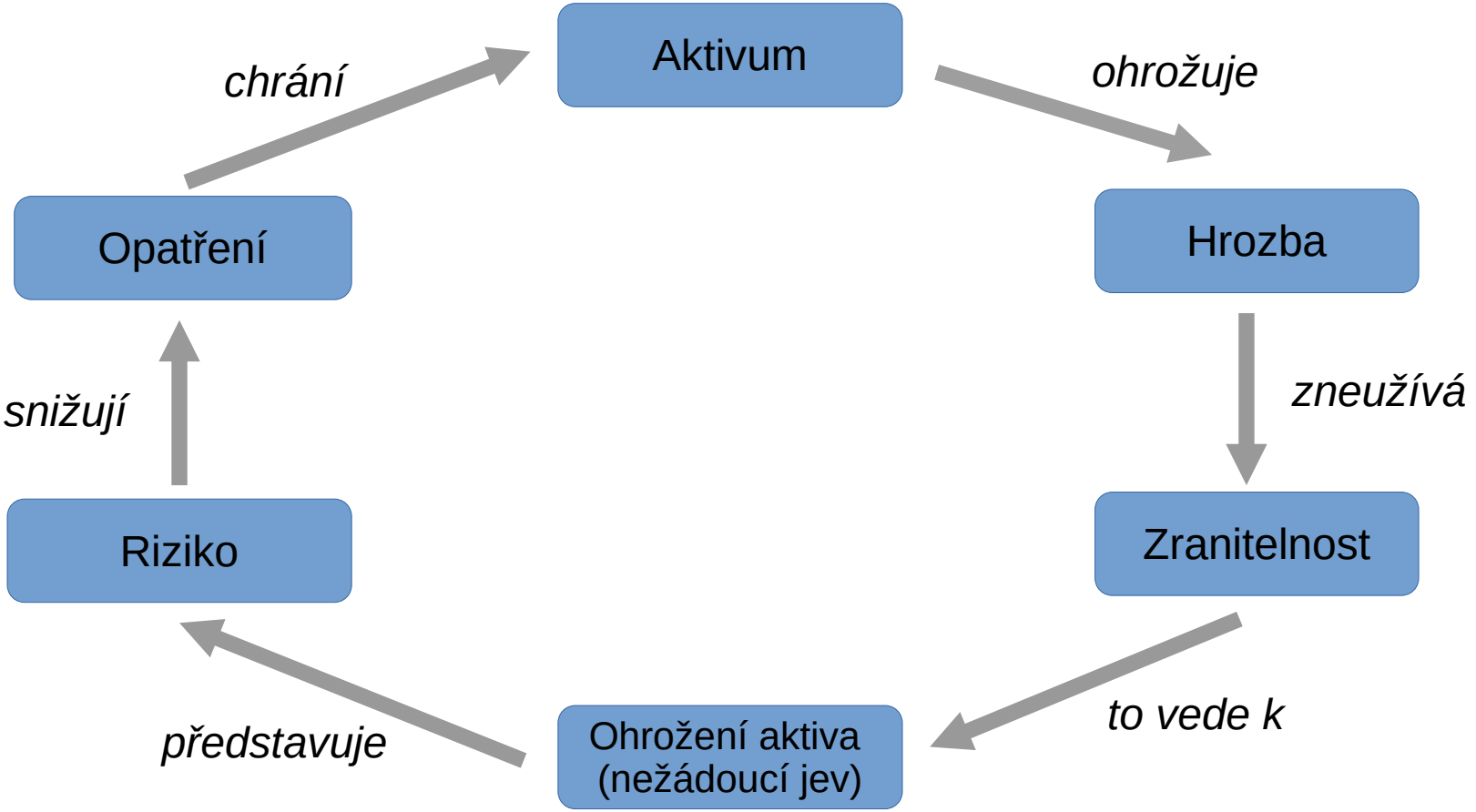
- Seznam aktiv (vím, co chráním)
- Katalog hrozeb (vím, čemu čelím)
- Katalog zranitelností (vím, co jsou typické slabiny)
- Metodiky
  - pro hodnocení aktiv
  - **pro hodnocení rizik**
- Matematický aparát, který míru rizika dokáže „vyčíslit“

RIZIKO = DOPAD * HROZBA * ZRANITELNOST

- Stupnice pro hodnocení
  - dopadů
  - pravděpodobnosti, že se hrozba uplatní
  - pravděpodobnosti, že se hrozba uplatní s využitím konkrétní zranitelnosti
  - hodnoty rizika, akceptační mez

Kdy provádíme analýzu rizik? V kyber ...

- Zavádění a údržbě ISMS
- Při adaptaci (dosahování souladu) s nZKB
- V reakci na Varování vydané NÚKIB – „Huawei“, „DeepSeek“, „Čína“
- Při řízení dodavatelů
  - a při zadávacích řízeních
- Při zvládání kybernetických bezpečnostních událostí
- ...


Aktivum
ohrožuje
Hrozba
zneužívá
Zranitelnost
to vede k
Ohrožení aktiva
(nežádoucí jev)
představuje
Riziko
snižují
Opatření
chrání

Proč analýzu dělat?

- **Pomáhá pochopit, co je pro organizaci skutečně důležité.**
- Spojuje kybernetické hrozby s dopady na aktiva, procesy a “business”.
- Dává základ pro volbu a priorizaci (bezpečnostních opatření).
- Umožňuje zdůvodnit, proč něco chráníme více a něco méně.
- Vytváří podklad pro řízení rizik v ISMS (nZKB) a pro průběžné zlepšování.

Analýza rizik = nástroj pro rozhodování, ne cíl sám o sobě.

Největší přidaná hodnota - dopady

- Samotná hrozba neříká, jak vážný problém organizaci způsobí.
- Klíčová otázka je: **„Co se stane, když…?“**
- Dopad může být technický, bezpečnostní, provozní, finanční, právní, reputační...
- Stejný technický incident může mít pro různé systémy, služby a procesy úplně jinou závažnost.

Nejzajímavější informace často nepochází z IT, ale u lidí, kteří aktivum (službu) používají.

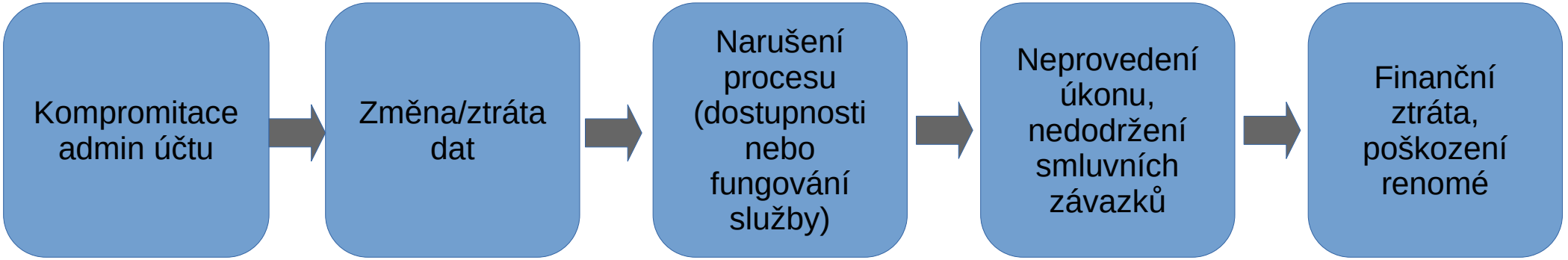
Ptejte se různých lidí

- **Bezpečáka:** Jaké scénáře, hrozby a zranitelnosti připadají v úvahu?
- **IT administrátora:** Co se může technicky stát?
- **Uživatel / vlastník procesu (služby):** Co to udělá s každodenní prací?
- **Business owner:** Co to udělá se závazky vůči zákazníkovi/partnerovi?
- **Vedení:** Co jsou naše priority? Jak velké riziko jsme ochotni přijmout?

Jedno aktivum ≠ jeden pohled na riziko.

Garant (vlastník) aktiva nemusí být ten, kdo je schopen nejlépe určit dopad.

Od technického incidentu ... k business dopadu

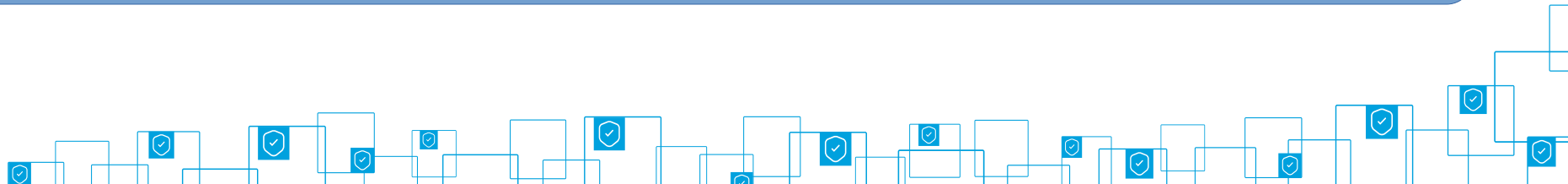


Dobrá analýza rizik umí vysvětlit celý řetězec, ne jen první technický článek.

Co vlastně analyzujeme?

- **Aktiva:** informace, systémy, služby, procesy, know-how, lidé, závislosti…
- **Hrozby:** co může způsobit nežádoucí událost?
- **Zranitelnosti:** co umožňuje, aby se hrozba uplatnila?
- **Scénáře:** jak může konkrétní událost proběhnout?
- **Dopady:** co bude výsledkem pro organizaci?

Praktické pravidlo: neanalyzujte jen „co máme“, ale hlavně „co by se stalo, kdyby to přestalo fungovat nebo se tomu přestalo věřit“.



Hodnocení: pozor na snahu o přesnost

- Škály 1–5 nebo podobné jsou užitečné hlavně pro konzistentní porovnávání.
- Číslo nemusí být objektivní měření reality.
- Důležitější než složitý výpočet je srozumitelná a stabilní metodika a popis celého "příběhu" – *událost -> technický dopad -> narušení procesu -> "business" dopad*.
- Ujasněte si, co přesně znamená „nízké", „střední" a „vysoké" riziko.
- Nezapomeňte oddělovat inherentní a reziduální riziko.

Když neumíme vysvětlit, proč riziko dostalo dané hodnocení, samotné číslo nám moc nepomůže.

Nejčastější úskalí

- Analýza „od stolu“ pouze bezpečnostním nebo IT týmem.
- Příliš obecné scénáře typu „kybernetický útok“.
- Zaměření na technická aktiva bez pochopení procesů, souvislostí a závislostí.
- Falešná přesnost čísel a barevné heatmapy bez kontextu.
- Příliš mnoho rizik, která nikdo neřídí.
- Jednorázový dokument, který je po schválení zapomenut.
- Akceptace rizika bez určení skutečného vlastníka.
- Opatření, jejichž cena převyšuje to, co chráníme.
- Mylná představa, že rizika eliminujeme. Rizika snižujeme!

Z praxe ...

- Z analýzy rizik aktiva „Personální systém“
- Aktéři: MKB, administrátor aktiva „Personální systém“, personalista
- Modelace hrozeb (situací)
  - nedostupnost systému -> zam. si nezadá dovolenou --> nebude vyplacena mzda
  - kompromitace přístupových údajů --> narušení integrity dat
  - ztráta dat, špatné fungování systému, narušení OOÚ
  - „přestupní stanice“
  - ....

Z praxe ...

- Z analýzy rizik aktiva „Personální systém“
- Aktéři: MKB, administrátor aktiva „Personální systém“, personalista
- Modelace hrozeb (situací)
  - nedostupnost systému -> zam ena mzda
  - kompromitace přístupových úd
  - ztráta dat, špatné fungování sy
  - „přestupní stanice“
  - ....

Opatření:

- Zavést MFA
- Dáme za FW, aplikujeme anti DdoS ochranu
- Údržba nebude prováděna prvních 6 dní v měsíci
- Zálohování
- ....

Z praxe ...

- Z analýzy rizik aktiv
- Aktéři: MKB,
- Modelace
  - nedostup
  - kompromita
  - ztráta dat, špatné fungování sy
  - „přestupní stanice“
  - ....

Napadá Tě garante ještě něco? Co ještě vidíš jako riziko, co tady dosud nezaznělo?

“, personalista

na mzda

ujeme anti

chranu

- Udržba nebude prováděna prvních 6 dní v měsíci
- Zálohování
- ....

Z praxe ...

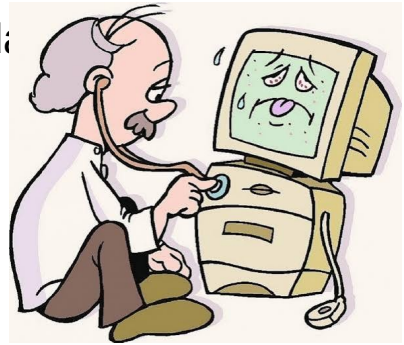
- Z analýzy rizik aktiv
- Aktéři: MKB, “, personalista
- Modelace
  - nedostup
  - kompromita
  - ztráta dat, špatné fungování sy
  - „přestupní stanice“
  -

Napadá Tě garante ještě něco? Co ještě vidíš jako riziko, co tady dosud nezaznělo?

na mzda

ujeme anti
chranu

- Udržba nebude prováděna prvních 6 dní v měsíci



Že to celý běží na 12 let starym křápu, kterej už dávno není v záruce, pro disky chodím do bazaru, protože jinde už se nedají sehnat ... a když už 10 let říkám vedení, že je potřeba koupit novou mašinu, tak se jen zeptají – jede to? No, jede, no, ale ... Tak proč chceš novou mašinu?

Zranitelnosti

1. nedostatečná údržba aktiv
2. zastaralost aktiv
3. nedostatečná ochrana perimetru
4. nedostatečné bezpečnostní povědomí uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení
5. nedostatečné zálohování
6. nevhodné nastavení přístupových oprávnění
7. nedostatečné postupy a procesy pro detekování kybernetických bezpečnostních událostí a identifikování kybernetických bezpečnostních incidentů
8. nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit činnost, která může mít vliv na bezpečnost regulované služby
9. nedostatečné stanovení bezpečnostních pravidel a postupů, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení
10. nedostatečná ochrana aktiv
11. nevhodně navržená bezpečná architektura
12. nedostatečná míra nezávislé kontroly
13. neschopnost včasného odhalení pochybení ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení
14. nedostatek zaměstnanců s potřebnou odbornou úrovní znalostí
15. umístění aktiva mimo fyzickou kontrolu (například na území cizího státu)

Hrozby

1. porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení
2. poškození nebo selhání technického anebo programového vybavení
3. zneužití identity
4. užívání programového vybavení v rozporu s licenčními podmínkami
5. škodlivý kód
6. narušení fyzické bezpečnosti
7. přerušení poskytování služeb elektronických komunikací, družicových služeb nebo dodávek elektrické energie nebo jiných důležitých služeb
8. narušení dostupnosti primárních nebo podpůrných aktiv umístěných mimo území České republiky
9. zneužití nebo neoprávněná modifikace informací
10. ztráta, odcizení nebo poškození aktiva
11. nedodržení smluvního závazku ze strany dodavatele
12. pochybení ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení
13. zneužití vnitřních prostředků, sabotáž
14. dlouhodobé přerušení poskytování služeb elektronických komunikací, družicových služeb, dodávky elektrické energie nebo jiných důležitých služeb
15. zaměstnanci s nedostatečnou odbornou úrovní znalostí
16. cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,
17. zneužití vyměnitelných technických nosičů dat
18. napadení (odposlech, modifikace, podvržení) elektronické komunikace, družicových služeb nebo jiných důležitých služeb
19. závislost na dodavateli
20. zneužití cizí státní moci pro přístup k aktivům
21. zpřístupnění nebo předání aktiv na základě žádosti jiného státu

Nejčastější úskalí

- Analýza „od stolu“ pouze bezpečnostním nebo IT týmem.
- Příliš obecné scénáře typu „kybernetický útok“.
- Zaměření na technická aktiva bez pochopení procesů, souvislostí a závislostí.
- Falešná přesnost čísel a barevné heatmapy bez kontextu.
- Příliš mnoho rizik, která nikdo neřídí.
- Jednorázový dokument, který je po schválení zapomenut.
- Akceptace rizika bez určení skutečného vlastníka.
- Opatření, jejichž cena převyšuje to, co chráníme.
- Mylná představa, že rizika eliminujeme. Rizika snižujeme!

Pro začátečníky

- Začněte menším, dobře pochopitelným rozsahem.
- Mluvte s administrátory, uživateli a vlastníky procesů.
- Pochopte související procesy a jejich kritičnost.
- Pracujte s konkrétními scénáři.
- Dopady popisujte tak, aby jim rozuměli všichni.
- Ke každému významnému riziku přiřaďte vlastníka a opatření.
- Vytvořte prostředí, kde na to nebudete sami.

Co se stane když? To je oč tu běží ...

Shrnutí

- Nejde o vytvoření co největšího “registru rizik”.
- Nejde o to mít všechno ohodnocené na škále 1–5.
- Jde o pochopení toho, co se může stát a co to znamená pro organizaci.
- Jde o rozhodnutí, která rizika snížíme, která přijmeme a proč.
- A jde o to, aby se tato rozhodnutí propsala do živého ISMS.

Dobrá analýza rizik nepřináší jistotu a pocit bezpečí.
Přináší podklady pro rozhodnutí.

Shrnutí II

- Analýza rizik (celé ISMS) je multidisciplinární záležitost.
- Ani sebelepší osoba na pozici MKB to nezvládne bez podpory (top) managementu a širší spolupráce.
- Bezpečnost něco stojí ...
- ... ale neměla by stát více, než to, co chráníme.
- Připravte se na to, že ani skvěle provedná analýza rizik vás nepřipraví na všechno, co se může stát.
- Mějte kvalitní zaměstnance a podporujte jejich odborný růst.
- Analýza rizik není jen záležitost kyber.

Promo

- **Mailing list csirt-forum@cesnet.cz, csirt-forum-subscribe@cesnet.cz**
  - reporty o zranitelnostech, https://cyberfeed.cesnet.cz
  - pozvánky na akce – pracovní skupiny a semináře
  - místo, kde je možné se zeptat
  - určen pro (technické) zaměstnance z organizací připojených do e-infrastruktury CESNET
- **Seminář Teorie a praxe nového zákona o kybernetické bezpečnosti (8. díl)**
  - 23. 9. 2026, 09:30 – max 13:00
  - https://events.cesnet.cz/event/75
  - **téma: řízení dodavatelů**
- **Kybernetická bezpečnost v CESNET:** https://www.cesnet.cz/bezpecnost

cesnet

Děkuji za pozornost!

Andrea Kropáčová, CESNET

andrea@cesnet.cz