cesnet

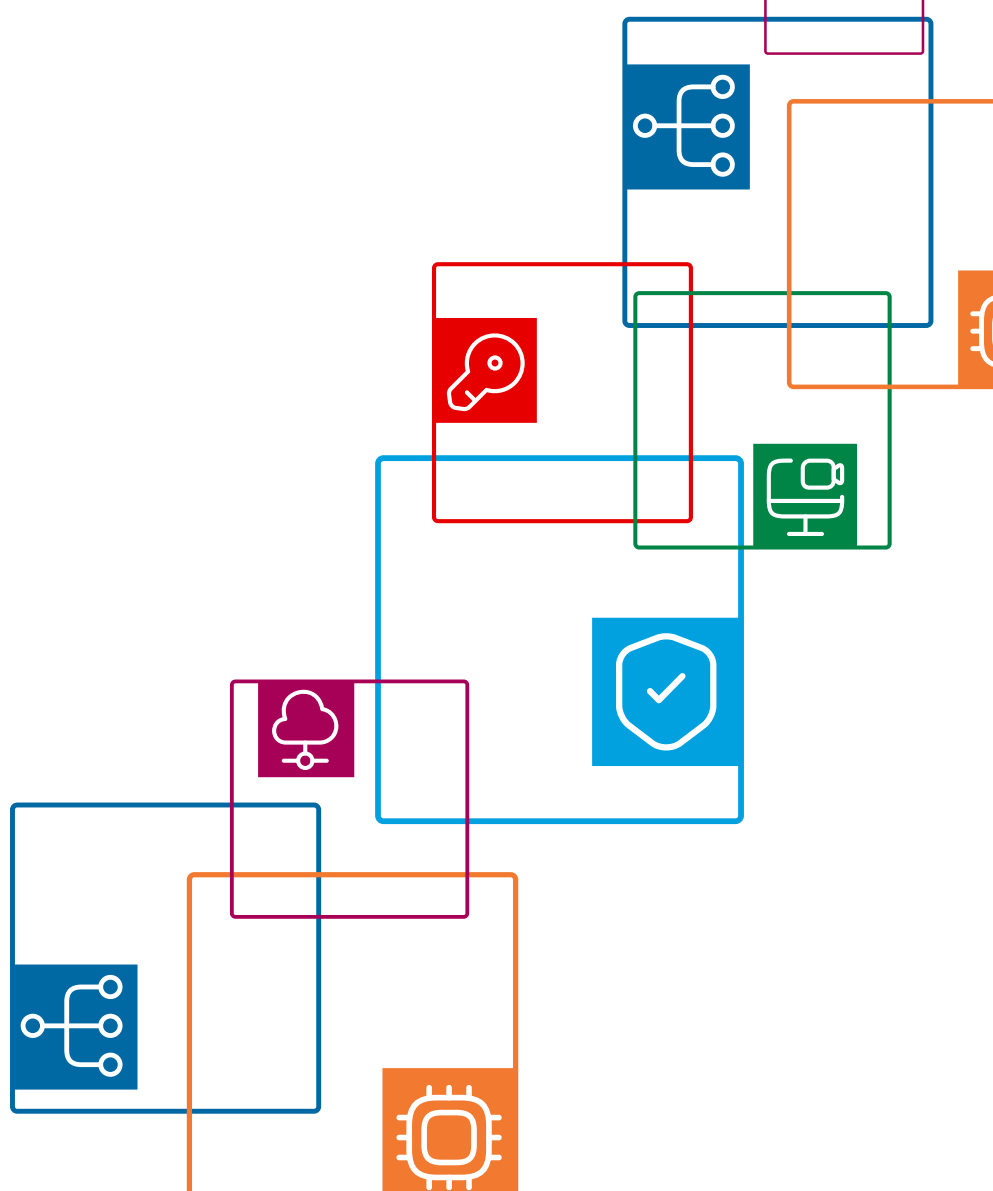
Teorie a praxe nZKB

Analýza rizik

Andrea Kropáčová

TLP: AMBER

18. 6. 2026, Praha

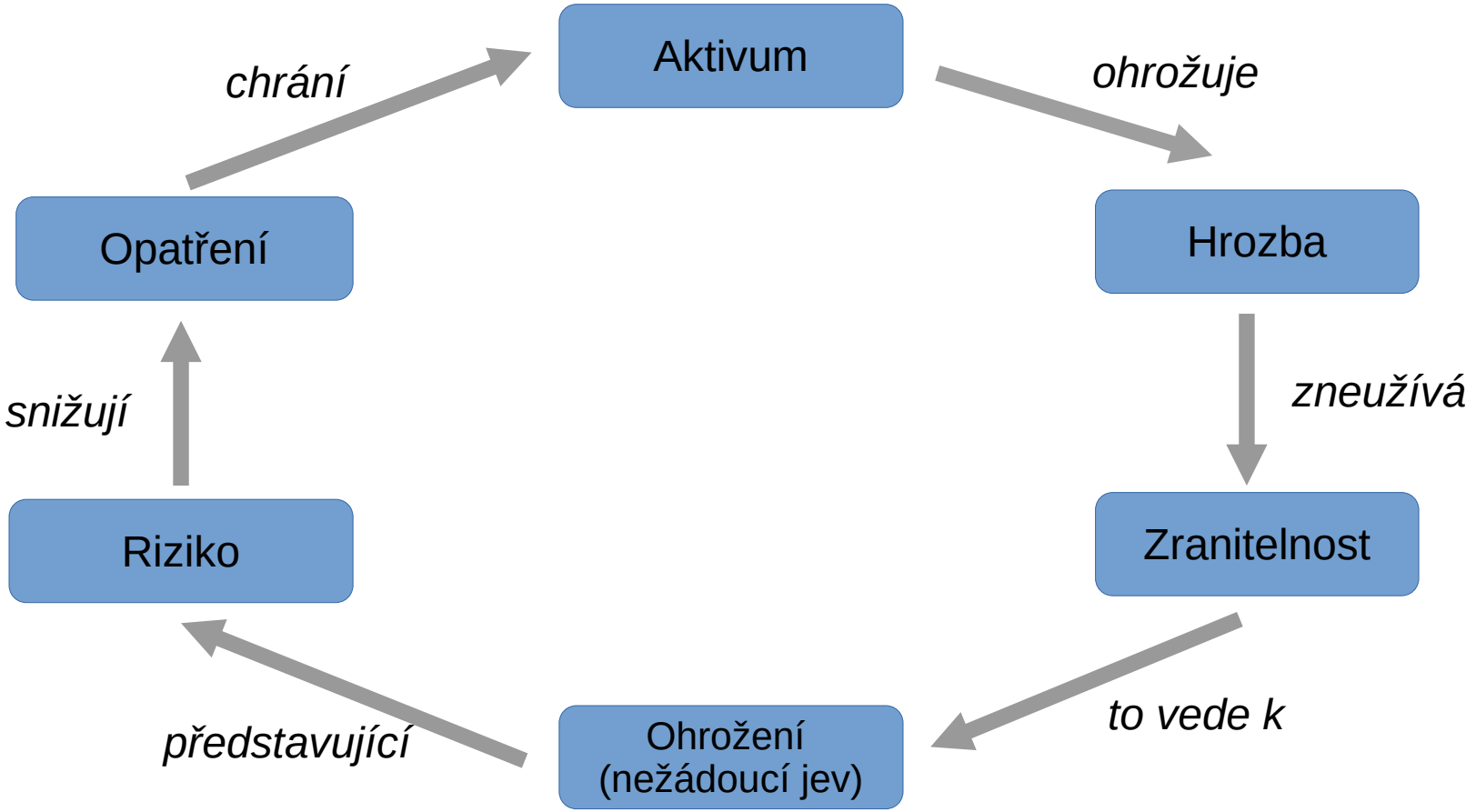


Analýza rizik

- Systematický proces identifikace, hodnocení a stanovení priorit rizik, která mohou negativně ovlivnit cíle, aktiva, proces apod. 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
  - Odhad 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.

Základní pojmy

- **Riziko** = něco, co nechci, aby se stalo mému aktivu (nežádoucí jev)
- **Riziko** = míra pravděpodobnosti, že nastane určitá bezpečnostní hrozba, a velikost následného dopadu, který by tato událost měla na chráněná informační aktiva
- **Nežádoucí jev** = uplatnění hrozby, obecně narušení DDI (dostupnosti, důvěrnosti a nebo integrity aktiva)
- **Hrozba:** Potenciální akce nebo událost, která může zneužít zranitelnost a ohrozit systém nebo data (aktivum).
- **Zranitelnost:** Slabé místo v systému nebo procesech, které může být zneužito.
- **Dopad:** Projev uplatnění hrozby na aktivum za zneužití zranitelnosti
- **Opatření:** Bezpečnostní opatření nebo kontroly, které se implementují k prevenci, zmírnění nebo eliminaci rizik.
- **Dostupnost** – bezpečnostní atribut zajišťující, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby.
- **Důvěrnost** – bezpečnostní atribut zajišťující, že informace jsou přístupné pouze oprávněným uživatelům.
- **Integrita** – bezpečnostní atribut zajišťující správnost a úplnost zpracování informací.


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

Pomůcky

- Seznam aktiv (vím, co chráním)
- Katalog hrozeb (vím, čemu čelím)
- Katalog zranitelností (vím, co jsou typické slabiny)
- Stupnice pro hodnocení (abych získal „čísla“)
  - dopadů
  - hrozeb (pravděpodobnosti, že se hrozba uplatní)
  - zranitelností (pravděpodobnosti, že se hrozba na aktivum uplatní s využitím konkrétní zranitelnosti)
  - hodnoty rizika
- Matematické vyjádření – vzorek pro výpočet „rizika“
  - **riziko = hodnota * hrozba * zranitelnost**

Analýza rizik – vzorce

- **Pro výpočet RIZIKA – je více metod, vzorců a přístupů, např.:**
  - **RIZIKO = HODNOTA * HROZBA * ZRANITELNOST**
  - **RIZIKO = HODNOTA * HROZBA**
  - **RIZIKO = DOPAD * HROZBA**

Analýza rizik – vzorce

- **Pro výpočet RIZIKA – je více metod, vzorců a přístupů, např.:**
  - **RIZIKO = HODNOTA * HROZBA * ZRANITELNOST**
  - **RIZIKO = HODNOTA * HROZBA**
  - **RIZIKO = DOPAD * HROZBA**
  - **RIZIKO = DOPAD * HROZBA * ZRANITELNOST**

Používá CESNET

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

Stupnice pro hodnocení: dopadů

Úroveň	Popis	Měřítko
Nízká	Reputace služby není poškozena. Rozsah případných škod nepřesahuje X Kč. Výpadek služby není větší než Y minut v pracovní době. Nedošlo k narušení bezpečnosti dat a informací ...	$x \leq 1$
Střední	Reputace služby je mírně poškozena a bude potřeba vyvinout úsilí k nápravě. Rozsah případných škod je v rozsahu od A Kč do B Kč. Výpadek služby po dobu více než YY minut v pracovní době. Omezení provozu služby méně než Z hodiny ... Nedošlo k narušení bezpečnosti dat a informací ...	$1 < x <= 3$
Vysoká	Reputace služby je významně poškozena, bude potřeba vyvinout významné úsilí a nemalé náklady na její nápravu. Rozsah případných škod je v rozsahu od ... Kč do ... Kč. Omezení provozu služby po dobu déle než 3 hodiny v pracovní době..., opakovaně, ... Došlo k narušení důvěrnosti nebo integrity dat a informací.	$3 < x <= 30$
Kritická	Funkcionalita a reputace služby je nenávratně poškozena, uživatelé nejsou ochotni nebo nemohou službu používat. Rozsah případných škod překračuje ... Kč. Kompletní nedostupnost služby více než ... hodin ... Došlo k narušení důvěrnosti nebo integrity dat a informací, služeb a provozu sítě, včetně osobních údajů uživatelů a citlivých informací.	$30 < x \leq 100$

Stupnice pro hodnocení: pravděpodobnost uplatnění hrozby

Úroveň	Popis	Měřítko
Nízká	Hrozba neexistuje nebo je málo **pravděpodobná**. Předpokládaná realizace hrozby není častější než jednou za 5 let.	0 %≤ x ≤25 %
Střední	Hrozba je málo pravděpodobná až **pravděpodobná**. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.	25 %< x ≤50 %
Vysoká	Hrozba je pravděpodobná až velmi **pravděpodobná**. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.	50 %< x ≤75 %
Kritická	Hrozba je velmi **pravděpodobná** až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.	75 %< x ≤100 %

Stupnice pro hodnocení: pravděpodobnost zneužití zranitelnosti

Úroveň	Popis	Měřítko
Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo **pravděpodobné**. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.	0 %≤x ≤25 %
Střední	Zneužití zranitelnosti je málo pravděpodobné až **pravděpodobné**. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.	25 %<x ≤50 %
Vysoká	Zneužití zranitelnosti je pravděpodobné až velmi **pravděpodobné**. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.	50 %< x ≤75 %
Kritická	Zneužití zranitelnosti je velmi **pravděpodobné** až víceméně jisté. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.	75 %< x ≤100 %

Stupnice pro hodnocení: rizika

Úroveň	Popis	Měřítko
Nízká	Riziko je považováno za akceptovatelné.	x ≤ 1
Střední	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.	
Vysoká	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.	
Kritická	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.	30 < x ≤ 100

Akceptační mez – z metodiky CESNET

- Akceptovatelným rizikem je riziko, které je pro organizace přijatelné a není nutné jej zvládat pomocí dalších bezpečnostních opatření.
- Akceptovatelná rizika jsou ta, která při hodnocení rizik nepřekročí akceptační mez.
- **Mezní kategorií** pro akceptaci rizik je **kategorie střední**.
- Rizika v kategorii **nízká** jsou rizika **zanedbatelná** (pro organizaci akceptovatelná), tj. nejsou ošetřována pomocí dalších bezpečnostních opatření.
- **Rizika kategorie střední mohou být pro organizaci akceptovatelná, rozhodnutí provádí MKB ve spolupráci s garantem aktiva (a případně VKB, ředitelem).**
- Rizika, která nebudou určena jako akceptovatelná, musí vždy být ošetřena pomocí dalších bezpečnostních opatření.
- Rizika kategorie **vysoká a kritická nejsou akceptovatelná** a musí vždy být ošetřena pomocí dalších bezpečnostních opatření.

Akceptační mez

Úroveň	Popis	Měřítko
Nízká	Riziko je považováno za akceptovatelné.	$x \leq 1$
Střední	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.	
Vysoká	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.	
Kritická	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.	$30 < x \leq 100$

Analýza rizik – vzorce

- **Pro výpočet RIZIKA – je více metod, vzorců a přístupů, např.:**
  - **RIZIKO = HODNOTA * HROZBA * ZRANITELNOST**
  - **RIZIKO = HODNOTA * HROZBA**
  - **RIZIKO = DOPAD * HROZBA**
  - **RIZIKO = DOPAD * HROZBA * ZRANITELNOST**

Používá CESNET

Dopadová analýza

- Je důležitá pro analýzu rizik i pro BIA (Business Impact Analysis)
- Modelujeme *Co se stane, když ...*
  - ... dojde k narušení dostupnosti aktiva (typu „služba“)
    - služba (DNS, mail, personální systém ...) nefunguje, uživatelé nemohou službu používat
    - nelze realizovat navazující procesy, zaměstnanci nemohou pracovat
  - ... dojde k narušení důvěrnosti aktiva (typu „služba“)
    - útočník zneužil zranitelnost a získal root (admin) oprávnění
    - útočník má přístup ke všem informacím, může je měnit, mazat ...
  - ... dojde k narušení integrity aktiva (typu „služba“)
    - útočník zneužil zranitelnost a získal root (admin) oprávnění a mění fungování aktiva
    - informace byly změněny (a zveřejněny)

Dopadová analýza

- Je důležitá pro analýzu rizik i pro BIA (Business Impact Analysis)
- Modelujeme *Co se stane, když ...*
  - ... dojde k narušení dostupnosti aktiva (typu „služba“)
    - ... systém ...) nefunguje, uživatelé nemohou službu používat
    - ... zaměstnanci nemohou pracovat
  - ... aktiva (typu „služba“)
    - ... (admin) oprávnění
    - ..., může je měnit, mazat ...
  - ... aktiva (typu „služba“)
    - ... získal root (admin) oprávnění a mění fungování aktiva
    - informace byly změněny (a zveřejněny)

Je potřeba se oprostit
od již aplikovaných opatření,
které by vedly k náhledu
„to se nemůže stát“.

Dopadová analýza

- Je důležitá pro analýzu rizik i pro BIA (Business Impact Analysis)
- Modelujeme *Co se stane, když ...*
  - ... dojde k narušení dostupnosti aktiva (typu „služba“)
    - ... systém ...) nefunguje
    - ... zaměstnan
    - ... iva (
    - ... (
    - ... n, mu
    - ... va (typu „
    - ... získal root (admin) op
    - informace byly změněny (a zveřejněny)

Je potřeba se oprostit od již aplikovaných opatření, které by vedly k náhledu „to se nemůže stát“.

Je potřeba hovořit také s garanty navazujících (závislých) aktiv a uživatel

Dopadová analýza

- Co se stane, když ... dojde k narušení DDI ... a dále
  - odvozené:
    - narušení DDI osobních údajů, dat uživatelů, těch, které si u nás uložili,
    - zneužití služby (zařízení) pro další útoky, další průnik do infastruktury
    - nesprávné fungování závislé služby
  - právní a smluvní
    - porušení právních předpisů (GDPR)
    - nedodržení SLA, nedodržení dobré praxe (očekávání ze strany uživatelů)
    - vypovězení kontraktu ze strany zákazníka
    - nedodržení povinností vyplývajících z projektových závazků
  - nakonec
    - ztráta důvěry ve službu ze strany uživatelů, odchod uživatelů
    - poškození renomé služby a organizace
    - finanční postih – pokuta, krácení financí v projektu

Analýza rizik - obecně

RIZIKO = DOPAD * HROZBA * ZRANITELNOST

- Každé aktivum musíme podrobit zkoumání, jak na něj působí hrozba za přítomnosti (zneužití) zranitelnosti
  - na některá aktiva některé hrozby nepůsobí

- Průběh analýzy rizik
  - krok 1. = zkoumáme a určujeme **dopad** narušení dostupnosti, důvěrnosti a integrity na aktivum
  - krok 2. = vybereme pro aktivum **relevantní hrozby** a zjišťujeme **pravděpodobnost**, že se **hrozba** na aktivum **uplatní**
  - krok 3. = uvažujeme, **jaké relevantní zranitelnosti** připadají v úvahu pro dané aktivum a danou hrozbu, především tedy jaká je pravděpodobnost, že bude daná zranitelnost(i) zneužita

Analýza rizik - obecně

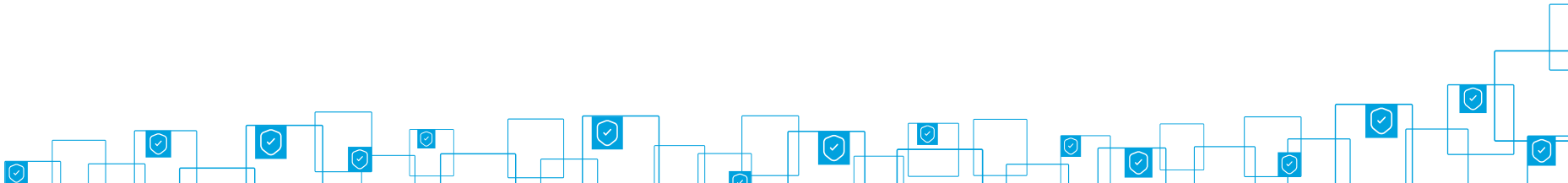
- Na aktivum zkoumáme působení **relevantní hrozby**
  - aktivum ***Místnost s listinnými dokumenty (archiv)***
    - hrozby: požár, voda, znečištění ... **ANO**, relevantní hrozba
    - hrozby: škodlivý SW, DDoS útok ... **NE**, NErelevantní hrozba
  - aktivum ***Personální systém*** *(tj. IT služba)*
    - hrozby: požár, voda, znečištění ... **NE**, NErelevantní hrozba
    - hrozby: škodlivý SW, DDoS útok ... **ANO**, relevantní hrozba
- K hrozbě zvažujeme **relevantní zranitelnosti**
  - hrozba: voda
    - zranitelnost: vodovodní potrubí pod stropem místnosti ... **ANO, relevantní zranitelnost**
    - zranitelnost: absence ochrany proti škodlivému SW ... **NE, NErelevantní zranitelnost**
  - hrozba: škodlivý SW
    - zranitelnost: vodovodní potrubí pod stropem místnosti ... **NE, NErelevantní zranitelnost**
    - zranitelnost: absence ochrany proti škodlivému SW ... **ANO, relevantní zranitelnost**

Analýza rizik - obecně

- Jak vyhodnotit (kvantifikovat) **pravděpodobnost**, že se **hrozba** na aktivum **uplatní?**
  - **Na základě zkušeností**
    - Stalo se někdy? Jak často se nám děje – 1x za rok, 1x za 5 let?
      - Od toho se odvíjí „pravděpodobnost uplatnění hrozby na aktivum“, když „se nikdy nestalo“, říkám, že pravděpodobnost uplatnění hrozby je „nízká“, když se stává např. 1x za rok, tak „střední“, apod. - **postupuji v souladu s dopadovou stupnicí**
  - **Na základě trendů (zohledňuji trendy)**
    - Nám se sice nestalo/neděje (prostě máme štěstí), výsledek předchozího přístupu je „nízká pravděpodobnost“), ale obecný trend uplatňování dané hrozby je rostoucí, zvyšuji proto na hodnotu „střední“
  - **Na základě odchylky od standardu (a požadavků – např. nZKB!!!)**
    - Eliminuji „že máme prostě štěstí, že se nám daná hrozba nikdy neuplatnila“
    - Příklad: máme slabou heslovou politiku, ale nemáme žádné kompromitované přístupové údaje, přesto je to špatně (protože o tom také třeba jenom nevíme) a musíme ji posílit (nehledě na to, že to je také jedno z opatření nZKB)

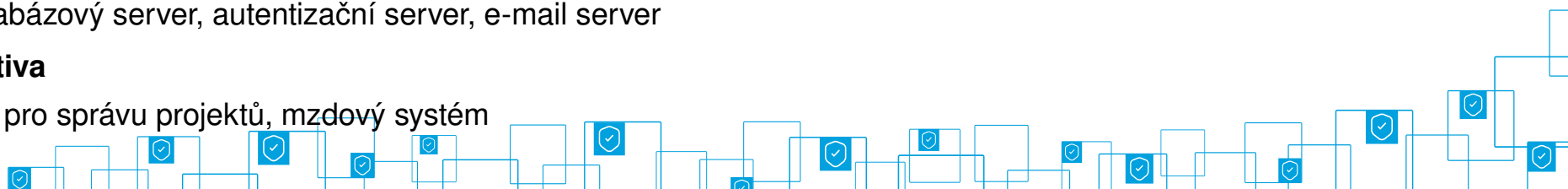
cesnet

Use-case: Analýza rizik pro aktivum “Personální systém”



Aktivum – personální systém

- **Název aktiva:** Personální systém
- **Garant aktiva:** vedoucí oddělení 333
- **Typ aktiva:** služba
- **Popis aktiva:** Systém, který
  - slouží ke správě a řízení veškerých dat a procesů spojených se zaměstnanci
  - obsahuje informace o zaměstnancích (osobní údaje, kontaktní, smlouvy, pracovní pozice, mzdy ...)
  - realizuje životní cyklus zaměstnance, od náboru (uchazeč), přes zaškolení (onboarding), až po rozvoj, školení a ukončení pracovního poměru
  - umožňuje správu agend typu – dovolená, směny, pracovní výkaz uživatelem
  - má webové rozhraní, prostřednictvím kterého si zaměstnanci mohou – aktualizovat některé OÚ, žádat o dovolenou, prohlédnout výplatní pásku ...
  - má tato schémata oprávnění: zaměstnanec, vedoucí, administrátor
  - je provozován na virtalizační platformě, na aplikaci ABC, v režimovém pracovišti XY
- **Podpůrná aktiva:**
  - síť, databázový server, autentizační server, e-mail server
- **Závislá aktiva**
  - systém pro správu projektů, mzdový systém



Aktivum – personální systém

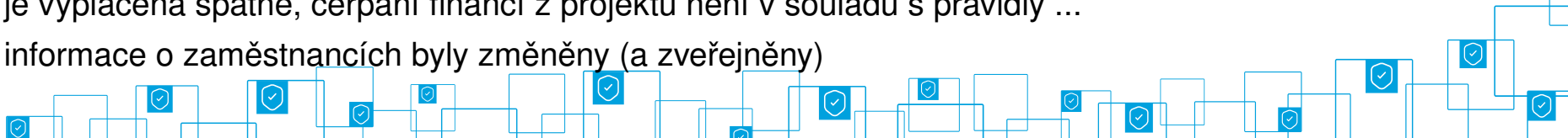
- **Požadavky na zajištění dostupnosti:**
  - hodnota je **vysoká**: zdůvodnění – organizace akceptuje výpadek 2h týdně, ale jsou kritická období, kdy je žádoucí nepřetržitý provoz
- **Požadavky na zajištění důvěrnosti:**
  - hodnota je **kritická**: zdůvodnění – systém obsahuje citlivé informace, včetně osobních údajů
- **Požadavky na zajištění integrity:**
  - hodnota je **kritická**: zdůvodnění – systém je prerekvizitou pro správné zpracování procesů typu výpočet mzdy, žádost o dovolenou, daňové přiznání ...
- **Hodnota aktiva** je **vysoká**
  - zdůvodnění – aktivum je klíčové pro zajištění základních zaměstnaneckých agend, které nejsou jednoduše realizovatelné náhradním řešením, v případě nefunkčnosti vznikají nežádoucí vícepráce, nelze realizovat některé z procesů životního cyklu zaměstnanec, může dojít k prodlení při vyplácení mzdy, reportování k poskytovatelům podpory, obsahuje osobní údaje uživatelů ...

Analýza rizik – k aktivu „Personální systém“

- Průběh analýzy rizik
  - krok 1. = určujeme **dopad** narušení dostupnosti, důvěrnosti a integrity na aktivum

Analýza rizik – k aktivu „Personální systém“

- Co se stane, když ...
  - ... **dojde k narušení dostupnosti aktiva (personálního systému)**
    - zaměstnanec nemůže aktualizovat informace o sobě, nemůže požádat o dovolenou, neuzavře pracovní výkaz, neodešle včas žádost o roční zúčtování daně ...
    - nedochází k přenosu informací do navazujících služeb – systém pro řízení projektů, mzdový systém
  - ... **dojde k narušení důvěrnosti aktiva (personálního systému)**
    - kompromitované přístupové údaje zaměstnance: dopad je lokalizovaný na data a procesy spojené s dotčeným zaměstnancem
    - kompromitované přístupové údaje vedoucího: dopad na více zaměstnaneckých účtů, modifikace dat
    - kompromitované přístupové údaje administrátora: dopad na celý systém, vyzrazení informací o zaměstnancích
  - ... **dojde k narušení integrity aktiva (personálního systému)**
    - útočník zneužil zranitelnost a získal root (admin) oprávnění a mění fungování aktiva, navazující systémy (mzdový, projektový) pracují s nesprávnými podvrženými daty, zaměstnancům není vyplacena mzda, nebo je vyplacena špatně, čerpání financí z projektů není v souladu s pravidly ...
    - informace o zaměstnancích byly změněny (a zveřejněny)



Analýza rizik – k aktivu „Personální systém“

- Co se stane, když ... dojde k narušení DDI u aktiva (personální systém)
  - rozšířené dopady:
    - narušení DDI osobních údajů
    - zneužití služby (zařízení) pro další útoky, další průnik do infastruktury – na další aktiva (služby)
    - nesprávné fungování závislého systému – „projektový IS“, „mzdový systém“
  - právní a smluvní dopady:
    - porušení právních předpisů (GDPR), zákoníku práce
    - nedodržení povinností vyplývajících z projektových závazků
  - odvozené dopady:
    - ztráta důvěry ve službu ze strany uživatelů
    - finanční postih – pokuta, krácení financí v projektu
    - audit ze strany dozorového orgánu

  ==> Hodnota dopadu = **KRITICKÁ**

Analýza rizik – k aktivu „Personální systém“

RIZIKO = KRITICKÁ * HROZBA * ZRANITELNOST

- Krok 2: ***Pravděpodobnost uplatnění hrozby***
  - hrozby: selhání nebo narušení komunikační sítě, škodlivý SW, nesprávné použití a správa zařízení a systémů, zneužití identity ...
  - Jak často dochází k:
    - nedostupnosti služby (narušení dostupnosti) — *Nevím, neměříme, nelogujeme...*
    - narušení důvěrnosti a integrity dat (a proč?) — *Nikdy se nestalo, zatím ...*
    - kompromitaci uživatelské identity — *Nikdy se nestalo, zatím ...*
    - bezpečnostním incidentům a jakým — *Za poslední rok 1x DdoS.*
    - chybnému pracování dat — *Nikdy se nestalo ...*
    - jaké řešíte uživatelské problémy — *Občas někdo zapomene heslo...*

==> Pravděpodobnost uplatnění hrozby ==> **NÍZKÁ? STŘEDNÍ?**

Analýza rizik – k aktivu „Personální systém“

RIZIKO = KRITICKÁ * HROZBA * ZRANITELNOST

- Krok 2: ***Pravděpodobnost uplatnění hrozby***
  - hrozby: selhání nebo narušení komunikační sítě, škodlivý SW, nesprávné použití a správa zařízení a systémů, zneužití identity ...
  - Jak často dochází k:
    - nedostupnosti služby (narušení dostupnosti) — *Nevím, neměříme, nelogujeme...*
    - narušení důvěrnosti a integrity dat (a proč?) — *Nikdy se nestalo, zatím ...*
    - kompromitaci uživatelské identity — *Nikdy se nestalo, zatím ...*
    - bezpečnostním incidentům a jakým — *Za poslední rok 1x DdoS.*
    - chybnému pracování dat — *Nikdy se nestalo ...*
    - jaké řešíte uživatelské problémy — *Občas někdo zapomene heslo...*
  - Odchylka od standardu (a ne-aplikace opatření = požadavků ZKB)
    - jaká je heslová politika? 8 znaků? — *To je ale slabé!*
    - je zaveden 2-faktor? — *Není.*
    - je aplikován pravidelný patchmanagement? — *Není, aktualizuje se dle lidských kapacit.*
  - Jaké jsou trendy?
    - phishing je na vzestupu, cílených útoků na uživatelovy přihlašovací údaje přibývá
    - objevuje se více zranitelností v SW
    - ...

==> Pravděpodobnost uplatnění hrozby ==> **VYSOKÁ**

Analýza rizik – k aktivu „Personální systém“

RIZIKO = KRITICKÁ * VYSOKÁ * ZRANITELNOST

- Průběh analýzy rizik
  - krok 1. = určujeme **dopad** narušení dostupnosti, důvěrnosti a integrity aktiva
  - krok 2. = vybereme pro aktivum relevantní hrozby a zjišťujeme **pravděpodobnost**, že se **hrozba** na aktivum **uplatní**
  - krok 3. = určujeme, jaké **zranitelnosti** připadají v úvahu pro dané aktivum a danou hrozbu, především tedy jaká je pravděpodobnost, že bude daná zranitelnost(i) zneužita
    - zkoumáme, jaká technická opatření jsou aplikována, a která chybí
    - pravděpodobnost uplatnění zranitelnosti = má dané aktivum nějaké v relevanci k hrozbě? Např. když zkoumám možnost uplatnění hrozby „škodlivý kód“, tak zjišťuji, jestli a jak je spravován OS daného aktiva, jestli jsou aplikovány anti* obranné mechanismy, dále mechanismy pravidelného patchmanagementu, scanování na zranitelnosti, správy state-of-the-art ...

Analýza rizik – k aktivu „Personální systém“

RIZIKO = KRITICKÁ * VYSOKÁ * ZRANITELNOST

- Krok 3. **Pravděpodobnost uplatnění zranitelnosti**
  - hrozby: selhání nebo narušení komunikační sítě, škodlivý SW, nesprávné použití a správa zařízení a systémů, zneužití identity ...
  - zranitelnosti (relevantní k hrozbám): slabá heslová politika, absence aplikace antimalware ochrany, absence řízení přístupových oprávnění, absence aplikace FW, absence HA režimu ...
  - co dělám pro to, abych minimalizoval zranitelnosti a vektory uplatnění hrozby?
    - aktualizuji dle kapacit
    - je to za VPN
    - pravidelně testuji, monitoruji, vyhodnocuji
    - školím uživatele a administrátory ...
  - jaké zranitelnosti jsou přítomny
    - slabá heslová politika,
    - nemáme zaveden 2-faktor
    - nelogujeme, nezaznamenáváme problémy
    - nemáme HA režim

  ==> Pravděpodobnost zneužití zranitelnosti ==> VYSOKÁ

Analýza rizik – k aktivu „Personální systém“

- Aktivum: Personální systém
  - systém, který slouží ke správě a řízení veškerých dat a procesů spojených se zaměstnanci

- DOPAD ==> **KRITICKÝ**
- PRAVDĚPODOBNOST UPLATNĚNÍ HROZBY ==> **VYSOKÁ**
- PRAVDĚPODOBNOST ZNEUŽITÍ ZRANITELNOSTI ==> **VYSOKÁ**

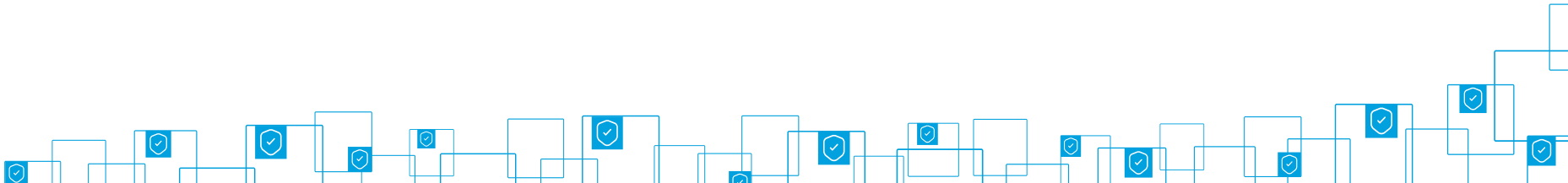
- **RIZIKO = DOPAD * HROZBA * ZRANITELNOST**
- **RIZIKO = KRITICKÝ * VYSOKÁ * VYSOKÁ**
- **RIZIKO = KRITICKÉ**

Analýza rizik – k aktivu „Personální systém“

- Navržená základní opatření:
  - Zavedení 2-faktoru, zesílení heslové politiky
  - HA režim
  - Zavedení logování a vyhodnocování logů
  - Zavedení pravidel na maintenance
  - Zavedení zaznamenávání událostí typu „ztráta hesla“, „nedostupnost“, „špatné autorizační oprávnění“ ...
    - Když nemám čísla a neměřím, jsem „slepý“
      - nevím, jestli se zlepšuji/zhoršuji

ZÁZNAMY!!!

Předávám slovo Marcele ...



Kdy provádíme analýzu rizik?

- Zavádění a údržbě ISMS (nZKB)
- Reakci na Varování vydané NÚKIB
  - „Huawei“
  - „DeepSeek“
  - „Čína“
- Při zadávacích řízeních
- Při KBI
- ...

Varování „Huawei“

- Vydáno 17. prosince 2018

VAROVÁNÍ

Národní úřad pro kybernetickou a informační bezpečnost, se sídlem Mučednická 1125/31, 616 00 Brno, podle § 12 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů vydává toto

v a r o v á n í :

Použití technických nebo programových prostředků následujících společností, včetně jejich dceřiných společností, představuje hrozbu v oblasti kybernetické bezpečnosti:

- **Huawei Technologies Co., Ltd., Šen-čen, Čínská lidová republika**
- **ZTE Corporation, Šen-čen, Čínská lidová republika**

Varování „Huawei“

1) Na základě skutečností zjištěných při výkonu své působnosti dospěl Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) k tomu, že použití technických nebo programových prostředků výše vyjmenovaných společností představuje hrozbu v oblasti kybernetické bezpečnosti, a proto podle § 12 odst. 1 zákona o kybernetické bezpečnosti vydává toto varování.

Varování „Huawei“

1) Na základě skutečností zjištěných při výkonu své působnosti dospěl Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) k tomu, že použití technických nebo programových prostředků výše vyjmenovaných společností představuje hrozbu v oblasti kyb
tot

4) Právní a politické prostředí Čínské lidové republiky („ČLR“), ve kterém uvedené společnosti primárně působí, a jejímiž zákony jsou povinny se řídit, vyžaduje po soukromých společnostech součinnost při naplňování zájmů ČLR, včetně podílu na zpravodajských aktivitách aj. Tyto společnosti se zároveň takové spolupráci se státem povětšinou nebrání; úsilí chránit zájmy zákazníků na úkor zájmům ČLR je v tomto prostředí značně sníženo. Podle dostupných informací existuje organizační a personální propojení mezi těmito společnostmi a státem. Uvedené tedy vytváří obavy, že zájmy ČLR mohou být stavěny nad zájmy uživatelů technologií uvedených společností.

Varování „Huawei“

1) Na základě skutečností zjištěných při výkonu své působnosti dospěl Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) k tomu, že použití technických nebo programových prostředků výše vyjmenovaných společností představuje hrozbu v oblasti kyb
tot

4) Právní a politické prostředí Čínské lidové republiky („ČLR“), ve kterém uvedené společnosti primárně působí, a jejímiž zákony jsou povinny se řídit, vyžaduje po soukromých společnostech součinnost při naplňování zájmů ČLR, včetně podílu na zpravodajských aktivitách aj. Tyto společnosti se zároveň takové spolupráci se státem povětšinou nebrání; úsilí chránit zájmy zákazníků na úkor zájmům ČLR je v tomto prostředí značně sníženo. Podle dostupných informací existuje organizační a personální propojení mezi těmito společnostmi a státem. Uvedené tedy vytváří o
společnos

7) Technické a programové prostředky uvedených společností jsou dodávány do informačních a komunikačních systémů, které mají či mohou mít z hlediska bezpečnosti státu strategický význam. Narušení bezpečnosti informací, tedy narušení dostupnosti, integrity nebo důvěrnosti informací v takových informačních a komunikačních systémech může mít zásadní dopad na bezpečnost České republiky a její zájmy.

Varování „Huawei“

1) Na základě skutečností zjištěných při výkonu své působnosti dospěl Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) k tomu, že použití technických nebo programových prostředků výše vyjmenovaných společností představuje hrozbu v oblasti kyb
tot

4) Právní a politické prostředí Čínské lidové republiky („ČLR“), ve kterém uvedené společnosti primárně působí, a jejímiž zákony jsou povinny se řídit, vyžaduje po soukromých společnostech součinnost při naplňování zájmů ČLR, včetně podílu na zpravodajských aktivitách aj. Tyto společnosti se zároveň takové spolupráci se státem povětšinou nebrání; úsilí chránit zájmy zákazníků na úkor zájmům ČLR je v tomto prostředí značně sníženo. Podle dostupných informací existuje organizační a personální propojení mezi těmito společnostmi a státem. Uvedené tedy vytváří o
společnos

7) Technické a programové prostředky uvedených společností jsou dodávány do informačních a komunikačních systémů, které mají či mohou mít z hlediska bezpečnosti státu strategický význam. Narušení bezpečnosti informací, tedy narušení dostupnosti, integrity nebo důvěrnosti inform
na be

8) Tyto skutečnosti ve svém souhrnu vedou k důvodné obavě z možných bezpečnostních rizik při používání technologií těchto společností. Míra potenciálního rizika vzhledem k možnému dopadu narušení bezpečnosti informací u informačních a komunikačních systémů důležitých pro stát je nezanedbatelná.

Varování „Huawei“

11) NÚKIB dále upozorňuje, že v souladu s § 4 odst. 4 zákona o kybernetické bezpečnosti jsou orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle zákona o kybernetické bezpečnosti nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

Varování „Huawei“

- Čím se tedy máme zabývat?
  - obecně: vlivem (působením) nové hrozby „Huawei“ na aktiva
    - technickými a programovými prostředky, a to:
      - těmi, co už máme
      - těmi, které jdeme pořizovat

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
22. **Huawei**
23. **DeepSeek**
24. **Čína**

Varování „Huawei“

- Metodika k Varování Huawei:
  - https://nukib.gov.cz/download/publikace/podpurne_materialy/2019_01_04_metodika_k_varov%C3%A1n%C3%AD_z_17-12-2018_v1.0.pdf

> Ze skutečností uvedených ve vydaném varování vyplývá, že hrozbu, na kterou varování upozorňuje, je v souladu s tabulkou č. 1 přílohy č. 2 VKB potřeba hodnotit jako velmi pravděpodobnou až více méně jistou. V případě užití jiné stupnice hodnocení hrozby, jak umožňuje § 5 odst. 3 VKB, je nutno tuto hrozbu ohodnotit způsobem odpovídajícím příslušné úrovni podle VKB.

Varování „Huawei“

- Metodika k Varování Huawei:
  - https://nukib.gov.cz/download/publikace/podpurne_materialy/2019_01_04_metodika_k_varov%C3%A1n%C3%AD_z_17-12-2018_v1.0.pdf

> Ze skutečností uvedených ve vydaném varování vyplývá, že hrozbu, na kterou varování upozorňuje, je v souladu s tabulkou č. 1 přílohy č. 2 VKB potřeba hodnotit jako velmi pravděpodobnou až více méně jistou. V případě užití jiné stupnice hodnocení hrozby, jak umožňuje § 5 odst. 3 VKB, je nutno tuto hrozbu ohodnotit způsobem odpovídajícím příslušné úrovni podle VKB.

  - hodnota je KRITICKÁ

- RIZIKO = DOPAD * **HROZBA**
- RIZIKO = DOPAD * **HROZBA** * ZRANITELNOST

Varování „Huawei“

- Z Varování a Metodiky máme:
  - **Hrozbu:** využívání technických a programových produktů Huawei ...
  - **Hodnotu hrozby:** Úřad hrozbu hodnotí na úrovni KRITICKÁ = hrozba je pravděpodobná až jistá

Tab. č. 1: Stupnice pro hodnocení hrozeb

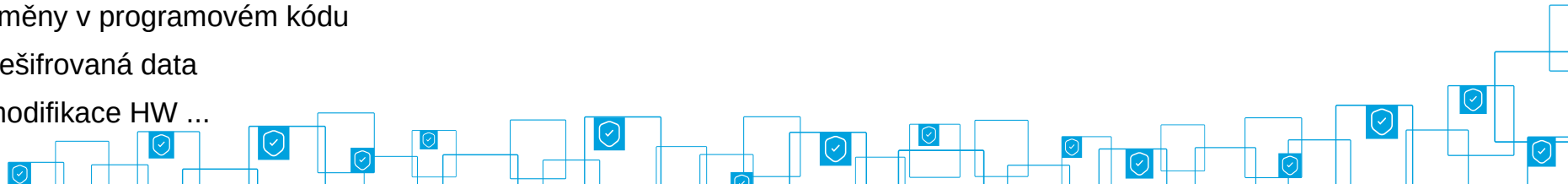
Úroveň	Popis
Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Varování „Huawei“: analýza rizik

- **RIZIKO = DOPAD * KRITICKÁ * ZRANITELNOST**
- **Další kroky:**
  - Identifikace relevantních aktiv
  - Dopady uplatnění hrozby na relevantní aktiva
  - Identifikace a vyhodnocení relevantních zranitelností

Varování „Huawei“: analýza rizik

- **RIZIKO = DOPAD * KRITICKÁ * ZRANITELNOST**
- **Další kroky:**
  - Identifikace relevantních aktiv
    - **Síťová zařízení**
    - Management systémy sítě (tedy SW)
    - Servery, disková pole...
  - Dopady uplatnění hrozby na relevantní aktiva **==> KRITICKÝ**
    - narušení důvěrnosti dat a informací (odposlech komunikace), modifikace přenášených dat
    - deaktivace komunikačních služeb (narušení dostupnosti), odepření služby
    - modifikace přenášených dat, narušení integrity přenášených dat
  - Identifikace a hodnocení relevantních zranitelností **==> VYSOKÝ**
    - změny v programovém kódu
    - nešifrovaná data
    - modifikace HW ...



Varování „Huawei“: analýza rizik

- **RIZIKO = DOPAD * KRITICKÁ * ZRANITELNOST**
- **RIZIKO = KRITICKÝ * KRITICKÁ * VYSOKÝ**
- **Hodnota RIZIKA = KRITICKÉ** (a tedy neakceptovatelné)

Varování „Huawei“: analýza rizik

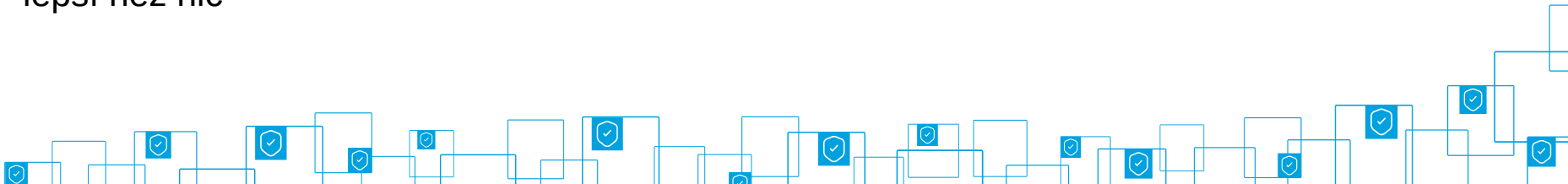
- Opatření ke snížení/eliminaci identifikovaného rizika
  - redundance (např. zdvojení infrastruktury)
  - regulace, síťová izolace (omezení komunikačního perimetru)
  - detailní monitoring
  - *nepoužití zařízení „Huawei“ (tj. jeho deaktivace nebo nepořízení)*

Varování „Huawei“: analýza rizik

- Máme:
  - identifikovaná relevantní aktiva
  - provedenou analýzu rizik
  - máme rámcová opatření
- Jdeme se zabývat:
  - lze opatření (na aktivu X) použít?
  - snižuje opatření riziko (u aktiva X) dostatečně?
  - je realizace opatření ekonomicky únosná?

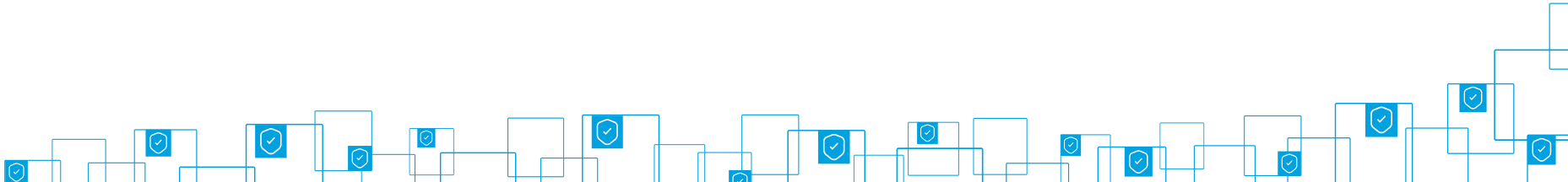
Varování „Huawei“: analýza rizik

- Aktivum „síťové prvky“
- Opatření:
  - redundance
    - řeší jen dostupnost, ale ne důvěrnost a integritu
  - síťová izolace
    - nelze použít u L3 síťových prvků s globálním komunikačním dosahem
    - lze použít u izolovaných (např. laboratorních) sítí
  - detailní monitoring
    - lze všude, ale není preventivní ani dostatečně reaktivní a tedy účinný, ale pro některé případy lepší než nic



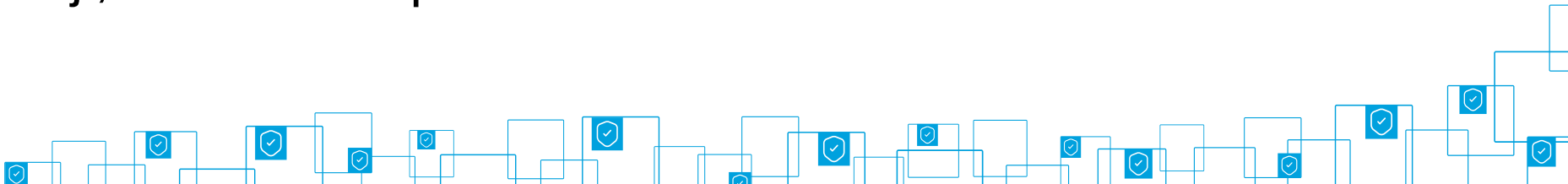
Varování „Huawei“: analýza rizik

- Aktivum „síťové prvky“
- Aplikace opatření:
  - pro již provozované aktiva
    - *okamžitá náhrada - není možná – nejsou finance na nová zařízení, nejsou lidské zdroje na redesign architektury sítě apod.*
    - detailní monitoring, s plánem reakce
    - náhrada bezprostředně po konci životnosti, tj. za 1 rok
  - pro výběrová řízení
    - na L3 prvky – vyloučit
    - na komponenty laboratorních sítí – nevylučovat, izolovat, monitorovat



Varování „Huawei“: resumé

- Varování jsem přečetl a zpracoval
- Identifikoval jsem relevantní aktiva
- Provedl jsem analýzu rizik
- Stanovil jsem
  - protiopatření pro aktiva, která už mám a jsou technologie „Huawei“
  - rámcová opatření pro zadávací řízení
    - která přezkoumávám pro každé jedno zadávací řízení
- Kontroluji, hodnotím a přezkoumávám



Zadávací řízení

- Pozor na následující situaci
  - mám seznam aktiv ...
  - ... a jdu kupovat něco, co v seznamu aktiv nemám
- Doporučení
  - u každého zadávacího řízení (pořizování) vždy provést úvahu, jestli se může jednat o technický nebo programový prostředek, na které je uplatnitelné Varování Huawei
  - u každého zadávacího řízení (pořizování) vždy provést úvahu, jestli se na předmět pořizování nevztahuje některé z vydaných varování
  - když si nejsme jistí, jestli to, co jdeme soutěžit, může být Huawei, děláme AR

Zadávací řízení

- Co od garanta potřebuje MKB (a právník) vědět, aby mohl pro zadávací řízení udělat analýzu rizik?

Zadávací řízení

- Co od garanta potřebuje MKB (a právník) vědět, aby mohl pro zadávací řízení udělat analýzu rizik?
  - Co jdeme pořizovat? (identifikace aktiva, nové aktivum, skupina aktiv)
  - Kdo to bude provozovat?
  - Role dodavatele
    - bude se podílet na – správě?, údržbě?, vývoji?, bude mít přístup k aktivům (a datům?)
  - Povolíme subdodávky?
  - Kde bude aktivum fyzicky umístěno?
  - Jaká služba na něm bude realizována? Jaké budou požadavky na dostupnost?
  - Jaká data a informace na něm budou uložena? Jaký k nim bude režim přístupu? Kdo k nim bude mít přístup?
  - Jaká je představa o exit strategii?
  - Mezní situace ala výměna vadné HW komponenty (např. paměťového média)?
  - Související aktiva (podpůrná)?

Analýza rizik

- ... podle předpisu **riziko = dopad * hrozba * zranitelnost**
- Bezpečnost vyžaduje komplexní přístup
  - modelace pomoci riziko = dopad * hrozba * zranitelnost odhalí
    - která opatření nejsou aplikována (zálohování, logování, silné šifry)
    - obecně – slabiny v základní péči o aktivum
    - když se zadaří, tak souvislosti
  - penetrační testy
    - “kde nechal tesař díru“
    - ... občas i mimo dané aktivum, ale s velkým dopadem na něj
  - interní kontroly
    - kde je rozpor mezi představou (“funguje to takto”, “probíhá to takto”, “stane se toto”) a realitou
  - testování
    - funguje to tak, jak má a jak si myslím?

Analýza rizik – závěrečná moudra

- Řízení rizik je nekončící proces, provádí se průběžně.
- Riziko snižujeme.
- Začněte s menšími celky a škálujte, rozšiřujte šířku i hloubku záběru postupně.
- Oslavujte vítězství – i malé kroky ke zmírnění rizik se počítají.
- Vždy se ptejte – “Co se změnilo?“, „Jaká nová rizika se objevila?“
- Spolupráce je povinná – kybernetická bezpečnost je odpovědností každého.
- Očekávejte (a překonávejte) odpor – nepohodlí znamená, že měníte status quo.
- V případě pochybností předpokládejte to nejhorší – a buďte opatrní ve svých hodnoceních.
- Rizika odhalují priority – proměňují omezené zdroje ve strategické kroky.
- Kyberbezpečnost není novinka – sousta nálezů bude adresovatelná už existujícími zdroji … ale je to i příležitost jak zdroje do kyberbezpečnosti navýšit.
- Garanti aktiv ví všechno ;-).

Co dál?

- **18. června 2026**
  - prezentace pošleme
  - xls soubor s AR pro personální systém
- **23. září 2026**
  - řízení dodavatelů
- **červenec – srpen – opakování některého z téma**
  - jak se neutopit v detailu
  - GAP analýza
  - jak pracovat s vedením
  - jen implantovat nZKB do organizace

Děkuji za pozornost.

Andrea Kropáčová, andrea@cesnet.cz