



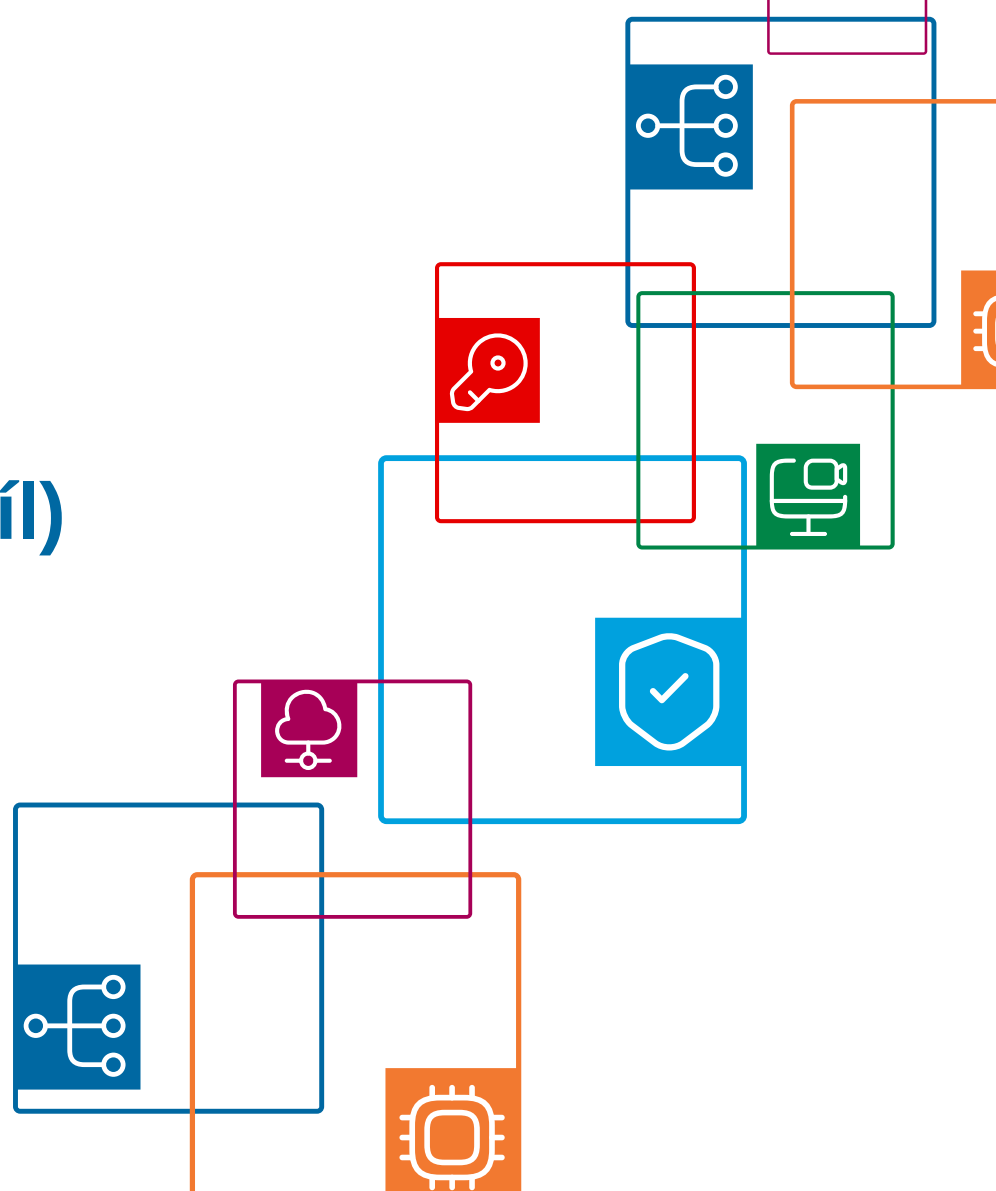
Teorie a praxe nZKB (8. díl)

Řízení dodavatelů

Andrea Kropáčová

TLP: **AMBER**

23. 9. 2026, Praha



- ... ze Cyber Con 2026, z diskuse od odboru kontroly
- Vyjde podpůrný materiál „Jak nastavit rozsah“
- DB aktiv
 - vyloučení aktiv z rozsahu (regulované služby)
 - zdůvodnění stačí jednoduché - aktivum „Databáze ABC“ – není podpůrné aktivum pro reg. službu „Cloudová služba v odvětví Digitální infra“, protože databáze není v prostředí cloudové služby využita.
- DB aktiv nebo DB majetku?
 - Aktivum „Sít'ové prvky“
 - Aktivum „Sít'ové prvky – na páteři“
 - Aktivum „Sít'ové prvky – v LAN“
 - Aktivum „Sít'ové prvky – v datacentru“

CYBER_CON
2026

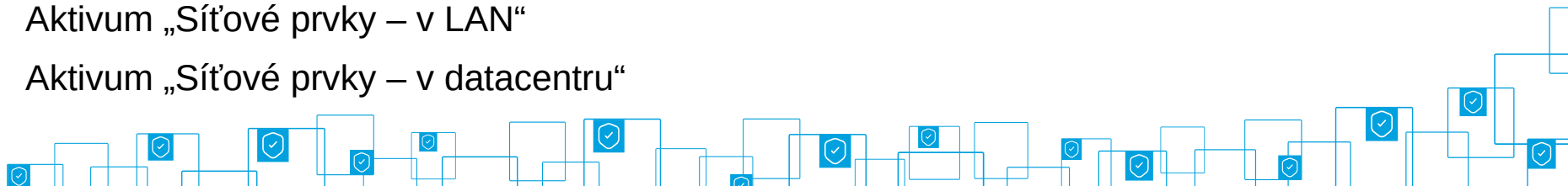
9.–10. ZÁŘÍ 2026

Vystavěná Rno – Rotunda

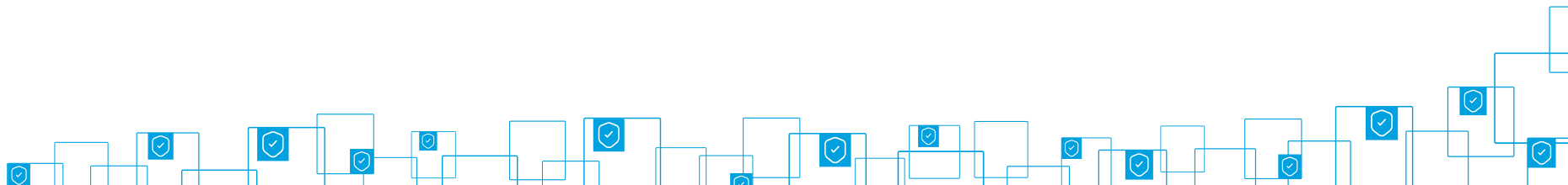
DĚKUJEME, ŽE JSTE BYLI SOUČÁSTÍ

Dva dny plné odborných diskusí, inspirace a sdílení zkušeností jsou za námi. Děkujeme všem účastníkům, řečníkům a partnerům za skvělou atmosféru.

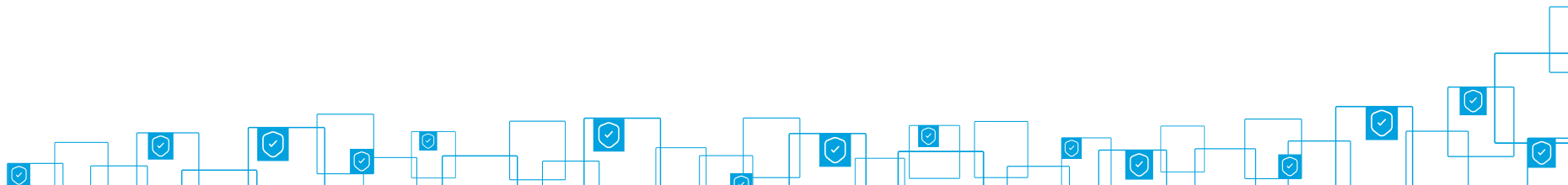
Fotografie a další vstupy z konference zveřejníme již brzy.



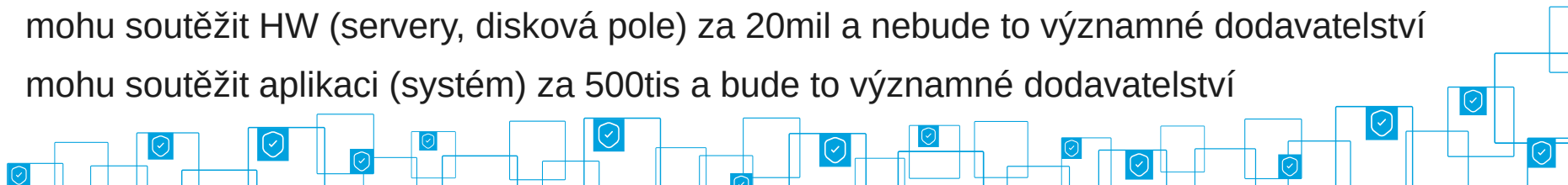
- Cílem je zajištění (zvýšení) kyberbezpečnosti
- Očekává se „živý proces“, ne „papír pro papír“
 - s výsledky analýzy rizik se pracuje
 - existuje plán zvládání rizik
 - garant opatření, termín, stav
 - PoA zohledňuje stav kyberbezpečnosti v organizaci a stav plnění povinností
 - neočekává se (při kontrole), že všechno bude „zelené“, ale musí být vidět rozvaha, jak povinnosti aplikovat



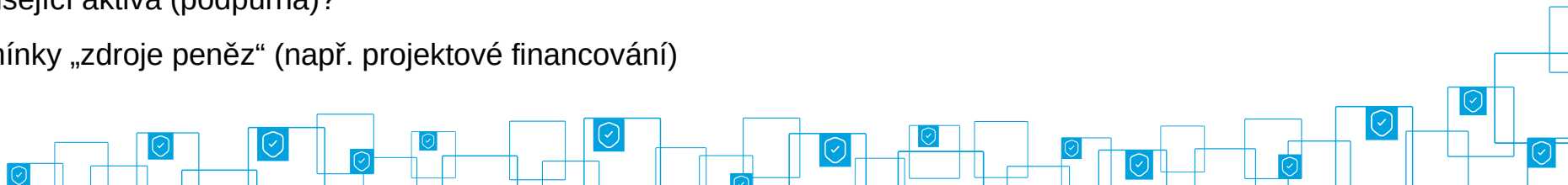
„Nákupy“



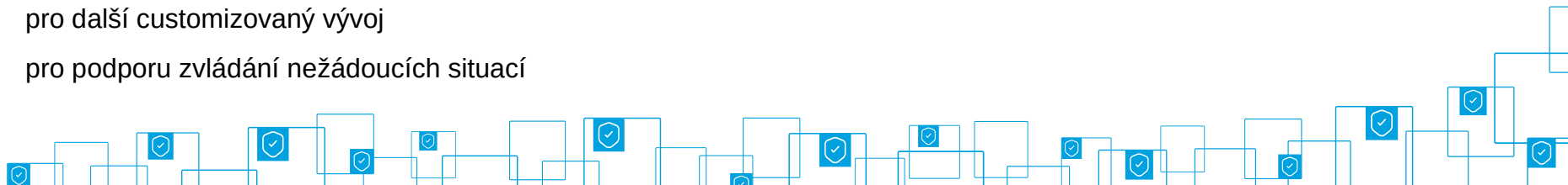
- Analýzu rizik děláme pro všechny „nákupy“ (s různou mírou „papírování“)
- Výsledky analýzy rizik zohledňujeme do podmínek nákupu (zadávacího řízení)
 - pořizují notebook (obecně mobilní zařízení)
 - opatření: servis NBD, vadný disk nevracíme (nebo povinně šifrujeme) --> do směrnice
 - opatření: nepořizovat „čínský výrobek“ (výsledek AR k varování NÚKIB) --> pokyn k vedoucím
- Vyjde-li nám z analýzy rizik, že dodavatel nově realizované zakázky bude **významný**, dáváme tuto informaci do zadávacího řízení (spolu s opatřeními – požadavky na dodavatele – plnění)
- **Významnost není o (finančním) objemu zakázky!!!**
 - klíčem pro rozhodování je VLIV na oblast kybernetické bezpečnosti
 - mohu soutěžit HW (servery, disková pole) za 20mil a nebude to významné dodavatelství
 - mohu soutěžit aplikaci (systém) za 500tis a bude to významné dodavatelství



- Východiska pro analýzu rizik (aneb co od garanta potřebuje MKB (a právník) vědět)
 - Co jdeme pořizovat? (identifikace aktiva, nové aktivum --> rovnou zaevidujeme)
 - Kdo to bude provozovat? My nebo dodavatel nebo oboje?
 - Jaká bude role dodavatele? Bude se podílet na – správě?, údržbě?, vývoji?, bude mít přístup k aktivům? ▲
 - Povolíme subdodávky?
 - Kde bude aktivum fyzicky umístěno?
 - Jaká služba (y) na něm budou realizovány? ▲
 - Jaká data a informace na něm budou uložena? Jaký k nim bude režim přístupu? Kdo k nim bude mít přístup? ▲
 - Jaké budou požadavky na dostupnost?
 - Jaká je představa o exit strategii „služby“?
 - Mezní situace – narušení bezpečnosti DDI, výměna vadné HW komponenty (např. paměťového média)? ▲
 - Související aktiva (podpůrná)?
 - Podmínky „zdroje peněz“ (např. projektové financování)
 - ...



- Východiska
 - systém bude provozován na prostředcích CESNET (bude ve fyzickém perimetru CESNET)
 - správa systému bude zajišťována modelem
 - CESNET: síť, HW, umístění, instalace a údržba OS
 - dodavatel: instalace, provoz a údržba aplikace
 - data uložená v systému
 - osobní údaje zaměstnanců, citlivé osobní údaje zaměstnanců, personální informace, mzdové schéma
 - přístup do systému
 - různá oprávnění: zaměstnanec, vedoucí pracovník, personální, administrátor
 - dodavatel bude mít přístup do systému (administrátorská práva)
 - z důvodu úvodního deploymentu
 - pro další customizovaný vývoj
 - pro podporu zvládnání nežádoucích situací



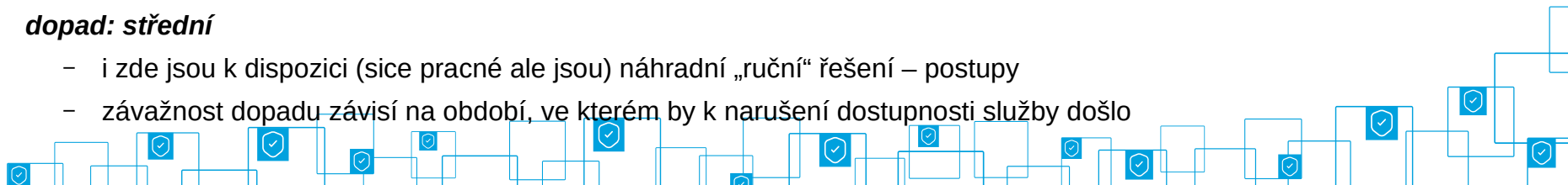
- **Narušení dostupnosti**

- z pohledu uživatelů (zaměstnanců)

- se systémem nelze pracovat, zaměstnanci nemohou využívat agendy, které systém zajišťuje (např. zadání dovolenek a volných dní, náhled na přehledová data, výkazy, uzavření docházky ...)
 - **dopad: nízký – střední**
 - z hlediska funkcionalit pro zaměstnance tyto jsou nahraditelné jiným způsobem (ústní dohoda, el. podepsaný e-mail, listinné sdělení)

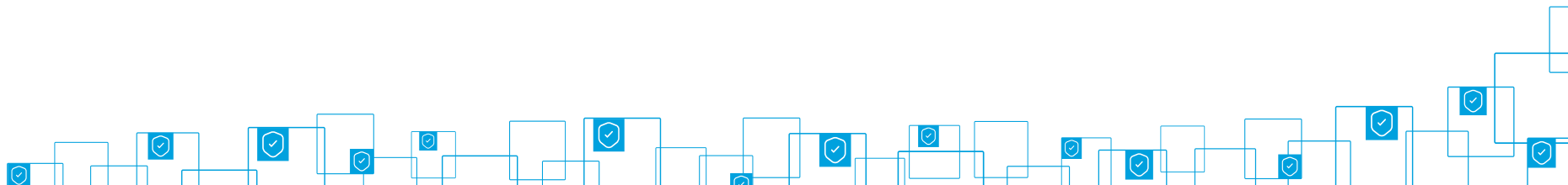
- z pohledu navazujících systémů

- nepřenáší se data do navazujících systémů
 - nemožnost včas (v termínu) vyplatit mzdy
 - nemožnost vytvořit výkazy v projektech (což může mít dopad na plnění povinností v projektech vůči dodavatelům účelových podpor)
 - neplnění povinností vůči státní správě v oblasti zaměstnanosti (reporting)
 - **dopad: střední**
 - i zde jsou k dispozici (sice pracné ale jsou) náhradní „ruční“ řešení – postupy
 - závažnost dopadu závisí na období, ve kterém by k narušení dostupnosti služby došlo



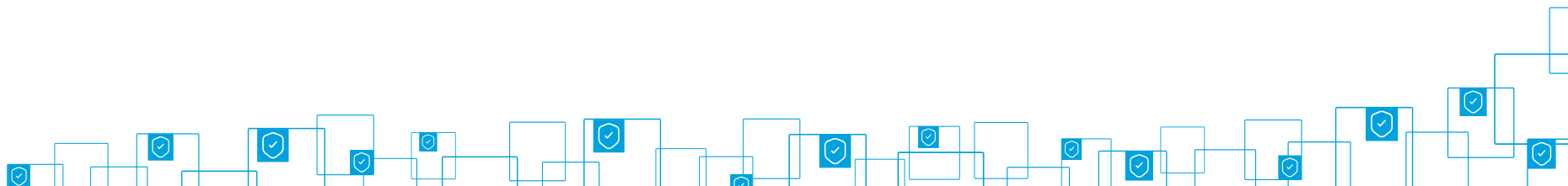
- **Narušení důvěrnosti**

- velký problém - systém obsahuje citlivá data (OÚ) zaměstnanců a bývalých zaměstnanců, takže může dojít k porušení ochrany OÚ (nedodržení povinností vyplývajících z legislativy a k legislativnímu postihu), možnost vzniku újmy zaměstnance
- v případě zveřejnění dat a informací je zde také aspekt poškození renomé, znevýhodnění CESNET při náboru nových zaměstnanců
- **dopad: vysoký**



- **Narušení integrity**

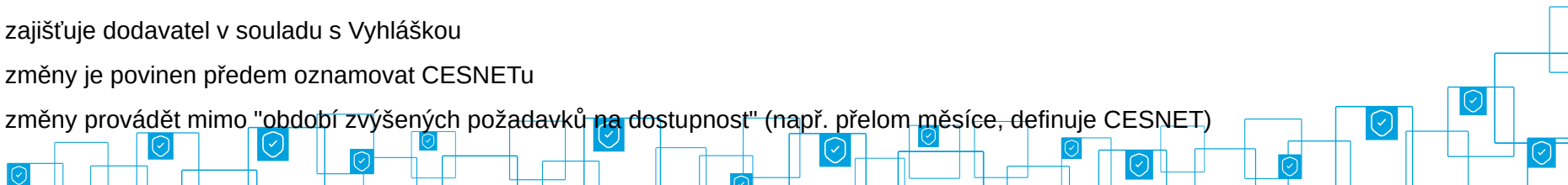
- v případě včas nezjištěné kompromitace systému/dat dojde k nežádoucí manipulaci dat a informací, což bude mít vliv také na navazující agendy a může dále vést např. k:
 - manipulaci s daty typu výpočet mzdy
 - manipulaci s daty typu výkaz do projektu a následně výpočtu mzdy
 - manipulaci s daty důležitými pro daňová přiznání
- **dopad: vysoký**



- **Opatření (směrem k dodavateli)**

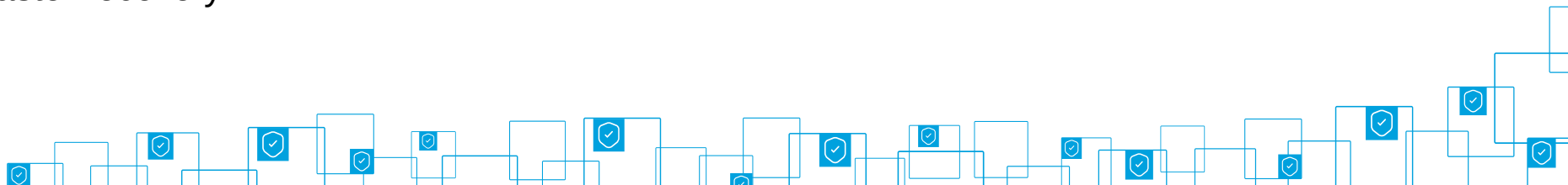


- stanovení pravidel pro řízení přístupu zaměstnanců dodavatele do systému
 - oznámení o ukončení PP --> deaktivace přístupu
- požadavek na proškolení zaměstnanců dodavatele
- stanovení pravidel zásahů dodavatele do systému (aplikace)
 - oznámení, zdůvodnění, dohodnutí času, dodržení principů řízení změn
 - povinnost hlásit provozní/bezpečnostní problémy (které zjistil dodavatel)
 - povinnost provádět zásahy nejdříve na testovací instanci, záznam
- reakční doba v případě zjištěného problému
- DPA
- řízení změn
 - zajišťuje dodavatel v souladu s Vyhláškou
 - změny je povinen předem oznamovat CESNETu
 - změny provádět mimo "období zvýšených požadavků na dostupnost" (např. přelom měsíce, definuje CESNET)

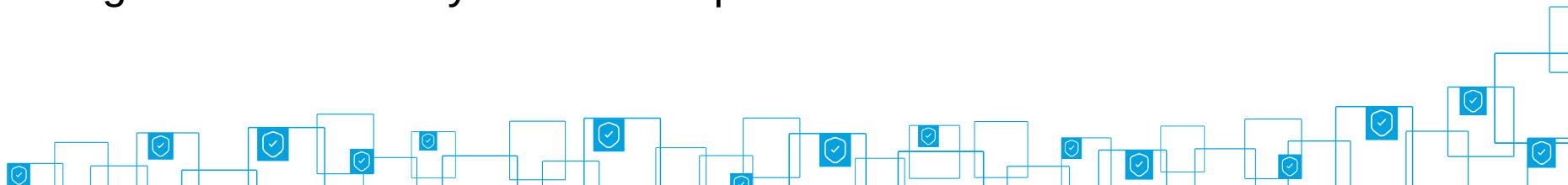


- **Opatření (pro CESNET)**

- zajistit fyzickou bezpečnost umístěním do režimového pracoviště
- zajistit first-hop-security
- zajistit monitoring funkcionality systému (pro včasnou detekci nežádoucích stavů)
- HA režim
- MFA
- uchovávání a zpracování logů na centrálním logmanagement systému CESNET
- evidence a pravidelná kontrola přístupových oprávnění
- zálohování
- disaster recovery



- Významný dodavatel?
 - ANO
 - Zdůvodnění
 - Systém bude obsahovat informace typu (citlivé) osobní údaje zaměstnanců, mzdovou politiku, data pro výkaznictví v projektech.
 - Dodavatel (zaměstnanci dodavatele) budou mít přístup do provozovaného systému (v roli Administrátor systému).
 - Systém bude obsahovat řadu agend pro podporu velkého množství činností sdružení (IDM, projektový systém, systém pro správu cest).
 - Systém kromě vysokých požadavků na důvěrnost a integritu musí garantovat také vysokou dostupnost.

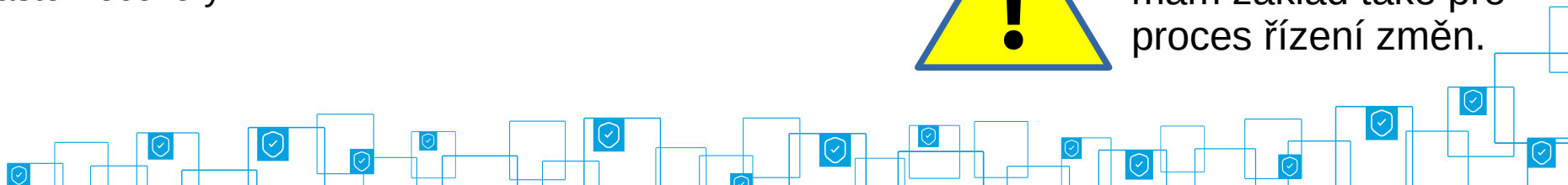


- **Opatření (pro CESNET)**

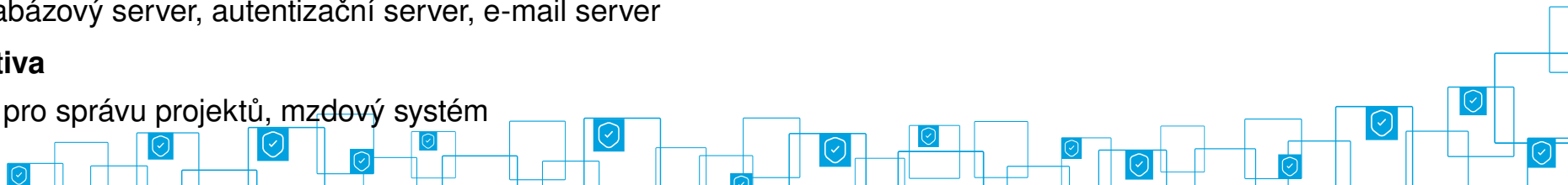
- zajistit fyzickou bezpečnost umístěním do režimového pracoviště
- zajistit first-hop-security
- zajistit monitoring funkcionality systému (pro včasnou detekci nežádoucích stavů)
- HA režim
- MFA
- uchovávání a zpracování logů na centrálním logmanagement systému CESNET
- evidence a pravidelná kontrola přístupových oprávnění
- zálohování
- disaster recovery



V tento moment
mám základ také pro
proces řízení změn.



- **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 nábory (uchazeč), přes zaškolení (onboarding), až po rozvoj, školení a ukončení pracovního poměru
 - umožňuje správu agend typu – dovolená, směny, pracovní výkaz uživatele
 - 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 virtualizační 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



- Analýza rizik
 - limity
 - postřeh z DTU v Pardubicích
- <https://www.cesnet.cz/bezpecnost> - jak zabezpečujeme e-infrastrukturu CESNET
- Due dilligence?
 - byl projeven zájem o přednášku na téma due dilligence

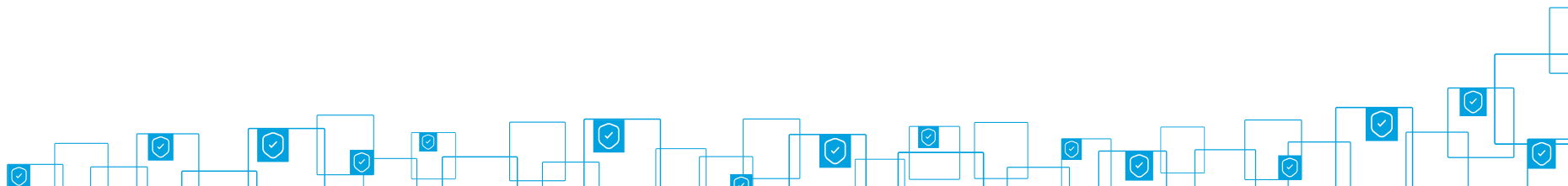


- **Listopad 2026**

- téma: kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty
- včetně předvedení hlášení směrem k NÚKIB
- za spolupráce NÚKIB

- **Rok 2027**

- zopakování některých témat?
- setkání na konkrétní vybraná témata – forma diskusní pracovní skupiny



Děkuji za pozornost.

Andrea Kropáčová, andrea@cesnet.cz