ZoKB a praktické splnění organizačních opatření

Virtuální konference - Řešení technických požadavků NIS2/ZoKB | 19. 2. 2025

Ing. Martin Konečný, MBA, CISM
www.GUARDIANS.cz

GUARDIANS.cz

Představení speakera

Martin Konečný.jpg

kontakty.vcf

Ing. Martin Konečný, MBA, CISM
GSM: +420 736 709 865
martin.konecny@guardians.cz
www.GUARDIANS.cz

GUARDIANS cz

Newsletter

Buďte informováni o novinkách v oblasti kybernetického zákona a dostávejte tipy, jak na implementaci.

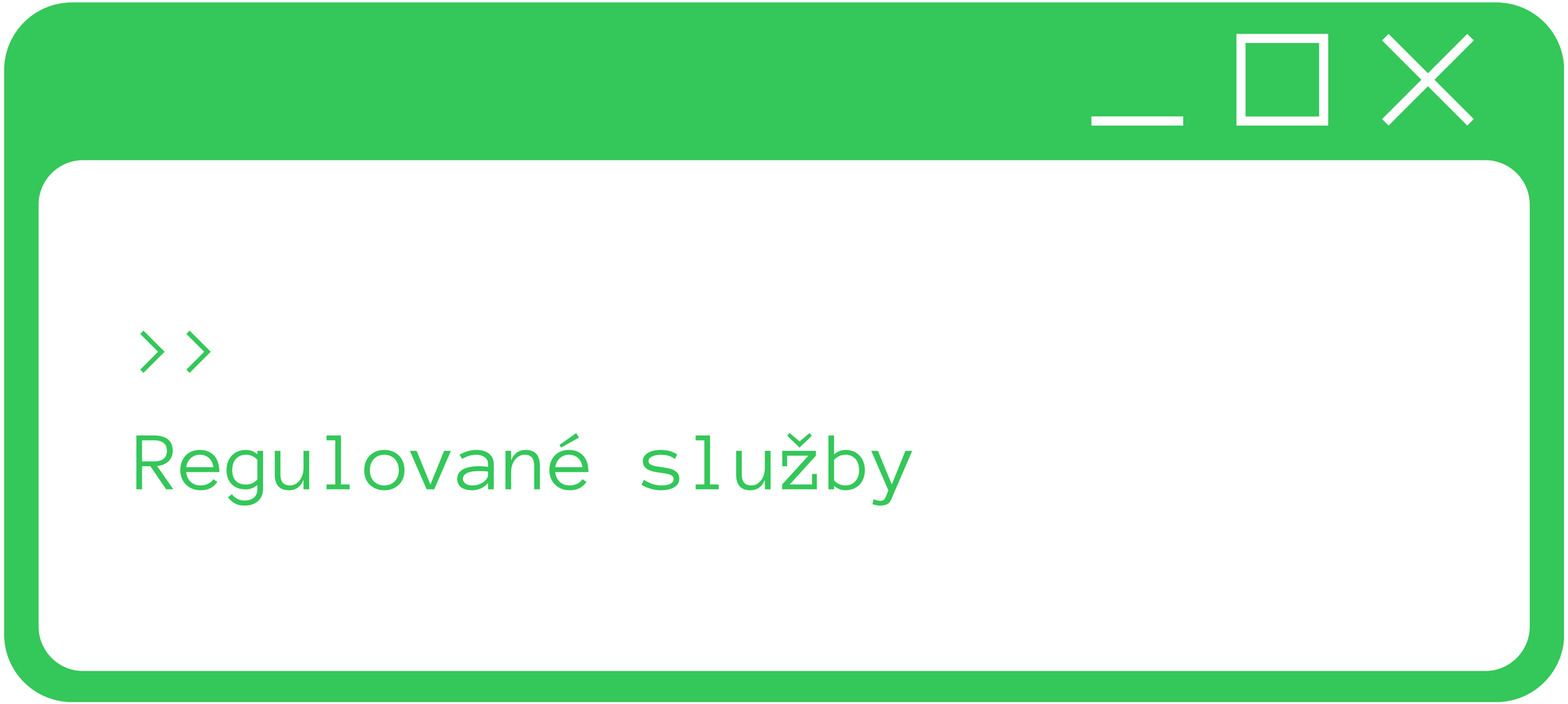
newsletter.guardians.cz

GUARDIANS CZ

Základní otázky k plnění NIS2 / nZKB (agenda)

Z hlediska zástupce firmy, na kterou dopadá NIS2 / nZKB si kladu otázky:

- [ ] **Kdo jsem?** (Typ regulované služby)
- [ ] **Co musím plnit?** (Požadavky dle typu regulované služby)
- [ ] **V jakém rozsahu?** (Stanovení aktiv, která je nutné chránit)
- [ ] **Jaký je můj současný stav řízení kybernetické bezpečnosti?** (Gap analýza, compliance mapování, ...)
- [ ] **Co mi zbývá "dodělat"?** (Zajištění shody s nZKB)
    - Kdo to bude dělat? (Bezpečnostní role)
    - Jaké procesy a technologie implementovat (RfP, PoC, ...)
- [ ] **Jak to vyhodnocovat?** (Metriky, testování, audity)


>>
Regulované služby

nZKB - vyhláška o regulovaných službách

Veřejná správa
Energetika – Elektřina
Energetika – Ropa a ropné produkty
Energetika – Plynárenství
Energetika – Teplárenství
Energetika – Vodík
Výrobní průmysl
Potravinářský průmysl
Chemický průmysl
Vodní hospodářství
Odpadové hospodářství

Letecká doprava
Drážní doprava
Vodní doprava
Silniční doprava
Digitální infrastruktura a služby
Finanční trh
Zdravotnictví
Věda, výzkum a vzdělávání
Poštovní a kurýrní služby
Vojenský průmysl
Vesmírný průmysl

vyšší režim

strategicky významné služby

bezpečnost dodavatelského řetězce, ...

povinnosti pro digitální infrastrukturu a služby podle nařízení EU

nižší režim

GUARDIANS CZ

nZKB - dopad na regulované subjekty - workflow

Digi - MSSP	Poskytovatel řízené bezpečnostní služby, který je poskytovatelem řízené služby a v rámci podnikatelských vztahů poskytuje službu související s řízením rizik nebo zajištěním bezpečnosti informací, je I. poskytovatel regulované služby **v režimu vyšších povinností, v případě, že je velkým podnikem**, II. poskytovatel regulované služby **v režimu nižších povinností, v případě, že je středním podnikem**.
Výrobní průmysl - Výroba elektrických zařízení	Výrobce elektrických zařízení ve smyslu oddílu 27 klasifikace CZ-NACE, který je velkým nebo středním podnikem, je poskytovatel regulované služby v režimu nižších povinností.

** Při počítání velikosti podniku se postupuje v souladu s doporučením EU 2003/361/ES o definici mikropodniků, malých a středních podniků. Více na: https://portal.nukib.gov.cz/storage/uploads/2024/09/06/Factsheet_na_koho_regulace_dopadne_v1.2-VARIANTA2.1-2_uid_66daf1616fa7c.pdf


>>
Povinnosti

Přehled základních povinností

- Registrace poskytovatele regulované služby (hlášení údajů).
- **Stanovení rozsahu.**
- **Plnění bezpečnostních opatření (=> nižší/vyšší režim povinností nebo nařízení EU pro digitální infra a služby).**
- Hlášení a zvládání kybernetických bezpečnostních incidentů.
- Informační povinnost poskytovatele regulované služby.
- **Zohledňování a plnění tzv. Protiopatření (historicky např. varování vůči některým technologiím z Číny, opatření k zabezpečení emailové infrastruktury atp.).**
- U omezeného rozsahu regulovaných subjektů také:
  - Zabezpečení dostupnosti strategicky významné služby (SVS).
  - Aplikace požadavků plynoucích z tzv. Mechanismu prověřování bezpečnosti dodavatelského řetězce.

Vyšší režim / zjednodušeně nižší režim - Bezpečnostní opatření a nástroje

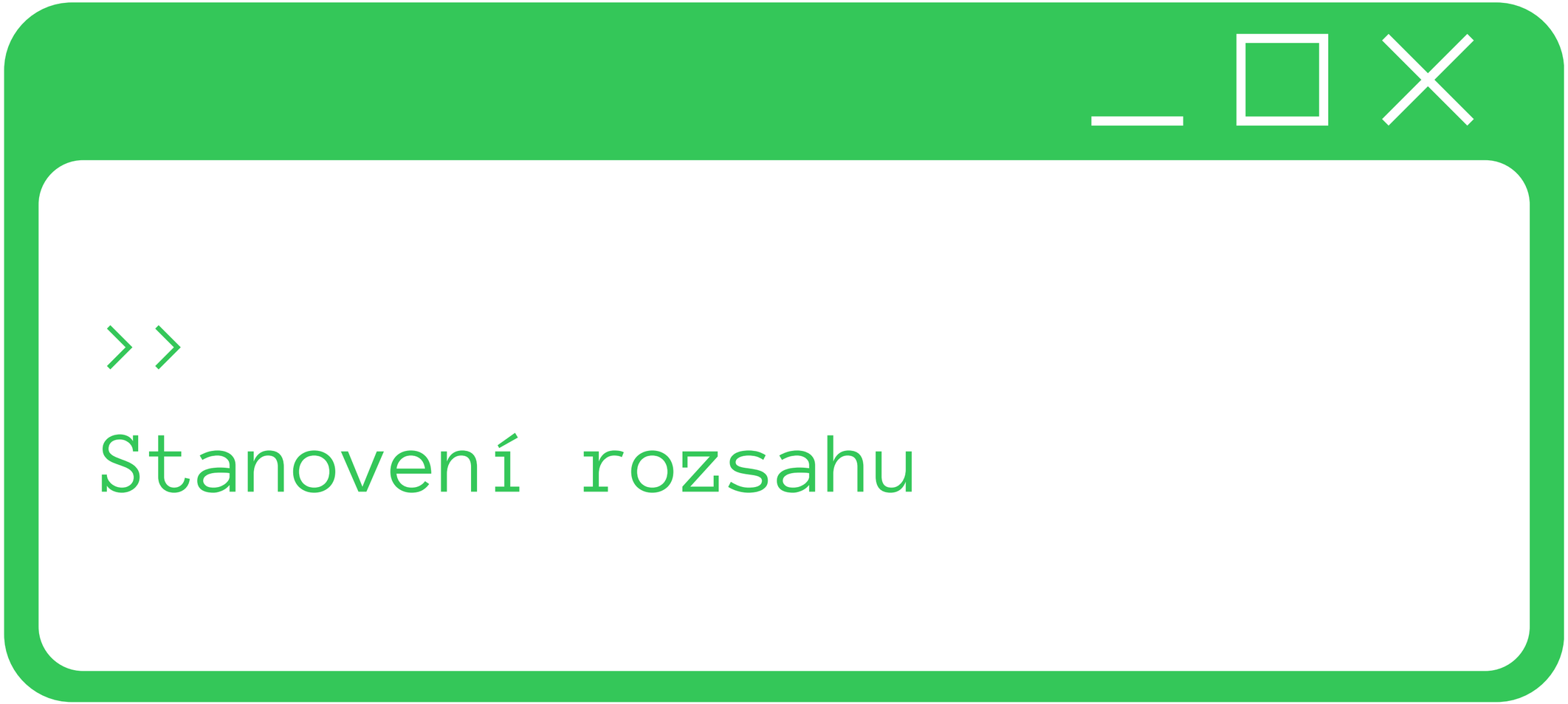
Organizační opatření	Technická opatření	Nástroje / principy (pozor - jde jen o příklady)
Systém řízení bezpečnosti informací		GRC, politiky, metriky
Povinnosti vrcholového vedení		metriky, reporting, manažerské nástroje (leadership, alokace zdrojů, definice pravomocí atd.), edu nástroje a školení
Bezpečnostní role		RACI, kompetence, pracovní smlouvy, smlouvy s dodavateli
Řízení bezpečnostní politiky a dokumentace		GRC, document management system
	Fyzická bezpečnost	prostředky fyz. bezpečnosti (CCTV, turnikety, čtečky, perimetry,...)
	Kryptografické prostředky	PKI, Vulnerability Management, CA, secrets management, hardening
Řízení aktiv		GRC, CMDB
Řízení rizik		GRC, RM tool, metriky, BCMS (z hlediska návaznosti)
Řízení dodavatelů		GRC, SCM nástroje / TPRM, právní služby, CTI, zákaznické audity
Bezpečnost lidských zdrojů		awareness aplikace, gamifikace, nástroje pro testování sociálního inženýrství
	Bezpečnost komunikačních sítí	802.1X, segmentace, FW, VPN, security architecture, SDN, ZTNA
Řízení změn		ticket/change management tool, LM, CMDB
Akvizice, vývoj a údržba	Aplikační bezpečnost	Security by default/design, vulnerability management, penetrační testy, red teaming, hardening, AppFW, WAF, SSDLC
Řízení přístupu	Řízení přístupových oprávnění Správa a ověřování identit	IDM, PAM, Tier model
Zvládání kybernetických bezpečnostních událostí a incidentů	Detekce kybernetických bezpečnostních událostí Zaznamenávání bezpečnostních a relevantních provozních událostí Vyhodnocování kybernetických bezpečnostních událostí	Log management, end-point protection (např. XDR), IDS, IPS, SIEM/SOAR, IRP testing, red teaming, TTX cvičení
Řízení kontinuity činností	Zajišťování dostupnosti regulované služby	BCP, BIA, HA clusters, backups, DRP, testing
	Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv	security architecture, vulnerability and patch management, fyzická bezpečnost, bezp. sítě, segmentace
Audit kybernetické bezpečnosti		GRC, Audit Findings evidence, zákaznické audity, důkazy a metriky

Nařízení EU pro digitální infrastrukturu a služby - Bezpečnostní opatření

1. Politika bezpečnosti sítí a informačních systémů	Politika bezpečnosti sítí a informačních systémů, Úkoly, odpovědnosti a pravomoci
2. Politika řízení rizik	Rámec pro řízení rizik, Sledování souladu
3. **Řešení incidentů** (pozn.: pozor na významnosti incidentů)	Politika řešení incidentů, Monitorování a vedení protokolů, Oznamování událostí, **Hodnocení a klasifikace událostí**, Reakce na incident, Přezkumy po incidentu
4. Kontinuita podnikání a krizové řízení	Plán kontinuity provozu a obnovy provozu po havárii, Krizové řízení
5. Bezpečnost dodavatelského řetězce	Politika bezpečnosti dodavatelského řetězce, Seznam dodavatelů a poskytovatelů služeb
6. Zabezpečení pořizování, vývoje a údržby sítí a informačních systémů	Zabezpečení pořizování služeb IKT nebo produktů IKT, Životní cyklus bezpečného vývoje, **Správa konfigurace**, Řízení změn, opravy a údržba, Testování bezpečnosti, Řízení bezpečnostních záplat, Bezpečnost sítí, Segmentace sítě, Ochrana před škodlivým a neautorizovaným softwarem
7. Politiky a postupy za účelem posouzení účinnosti opatření k řízení kybernetických bezpečnostních rizik	
8. Základní postupy v oblasti kybernetické hygieny a bezpečnostní školení	Zvyšování povědomí a základní postupy v oblasti kybernetické hygieny, Bezpečnostní školení
9. Kryptografie	Politika a postupy v oblasti kryptografie
10. Bezpečnost lidských zdrojů	Bezpečnost lidských zdrojů, **Ověření spolehlivosti**, Postup při ukončení nebo změně pracovního poměru, Disciplinární řízení
11. Kontrola přístupu	Postup kontroly přístupu, Správa přístupových práv, Administrátorské účty a účty pro správu systému, Systémy správy, Identifikace, Ověření, Vícefaktorová autentizace
12. Správa aktiv	Klasifikace aktiv, Zacházení s aktivy, Politika týkající se vyměnitelných médií, Soupis aktiv, Uložení, vrácení nebo smazání aktiv po ukončení pracovního poměru
13. Environmentální a fyzická bezpečnost	Podpůrné služby, Ochrana před fyzickými a environmentálními hrozbami

Více na: https://newsletter.guardians.cz/p/jak-nis2-dopada-na-digitalni-sluzby

GUARDIANS CZ


>>
Stanovení rozsahu

Stanovení rozsahu podle ZKB

- Rozsah podle ZKB vymezují (primární) aktiva.
- **ŘÍZENÍ AKTIV** JE TEDY **JEDNÍM ZE ZÁKLADNÍCH PROCESŮ**
  - **Pokud nevím co vše a s jakou hodnotou mám, jak to mohu adekvátně provozovat, natož chránit?**

- Aktiva
  - **Primární** (zpracovávané informace nebo poskytované služby)
  - **Podpůrná** (aktiva zajišťující fungování primárních aktiv, zejména - zaměstnanci, dodavatelé, technická aktiva jako HW, SW, objekty, apod.)

- Požadavky vychází z:
  - nZKB § 12 Stanovení rozsahu řízení kybernetické bezpečnosti
  - vyhlášky pro vyšší režim regulace - § 8 Řízení aktiv
  - vyhlášky pro nižší režim regulace - § 4 Systém zajišťování minimální kybernetické bezpečnosti, odst. 5

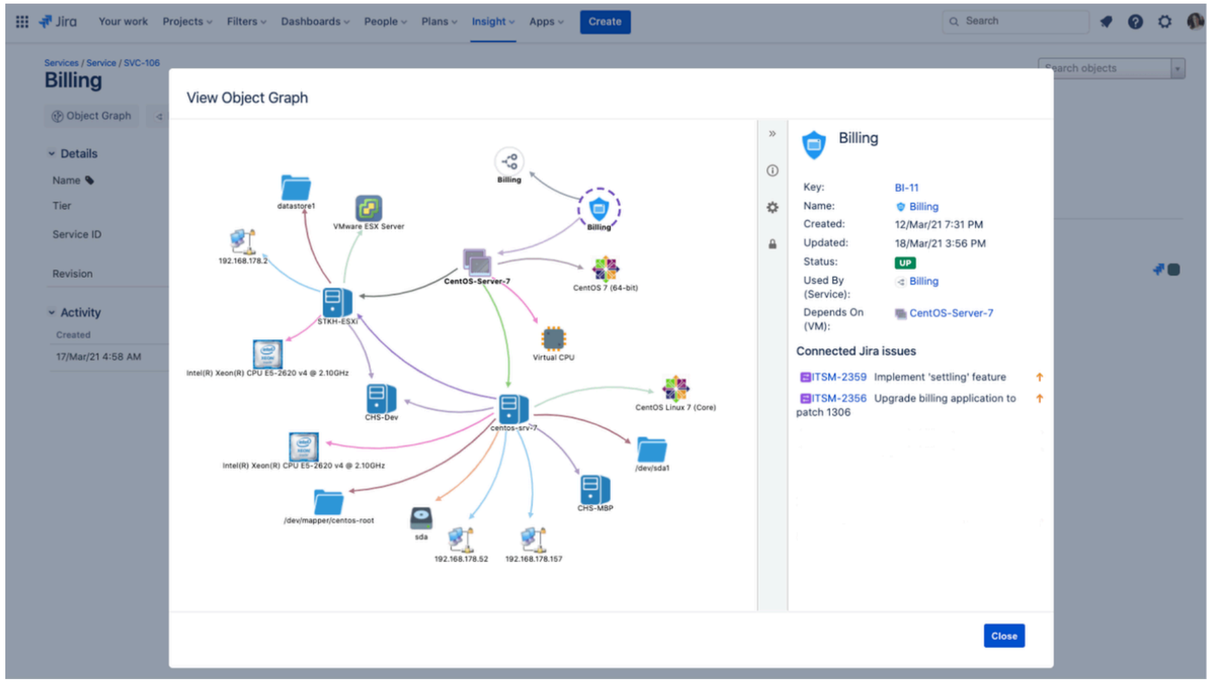
Jak na správné vymezení rozsahu

1. Jako prerekvizitu potřebujete přehled regulovaných služeb organizace (pokud je neznáte, pomůže vám nejlépe právník).
2. U regulované služby si pokládáme otázky:
    a. Z jakých klíčových procesů a služeb se regulovaná služba skládá?
    b. Jaké informace a data se v rámci regulované služby zpracovávají?
3. Dostáváme přehled primárních aktiv, které by měly být v rozsahu (k těmto aktivům je nutné v evidenci doplnit **příznak "v rozsahu"** nebo obdobný + odůvodnění, že aktivum zajišťuje regulovanou službu).
4. Nutno však **doplnit seznam o garanty aktiv a o ostatní primární aktiva**, tedy o všechny ostatní klíčové procesy a služby a související data a informace. Pro úplnost evidence aktiv je nutné u aktiv mimo rozsah doplnit **příznak "mimo rozsah"** + odůvodnění, že aktivum se nepodílí na zajišťování regulovaných služeb.
5. Pozor na to, že seznam musí být auditovatelný, měly by v něm jít vidět jednotlivé změny a atributy související se zahrnutím/vyjmutím z rozsahu (moderní CMDB vám tyto požadavky hravě pokryje).
6. Stanovený rozsah je nutné pravidelně přezkoumávat.

Jak na správné vymezení rozsahu

Pokračujeme dále řízením aktiv

1. Dále si pokládáme otázky, jaké k regulované službě potřebujeme:
    a. zaměstnance
    b. dodavatele
    c. technická aktiva jako HW, SW
    d. objekty
2. Tím získáváme přehled podpůrných aktiv.
3. Určíme garanty podpůrných aktiv.
4. Mapujeme vazby mezi aktivy
    a. potřebujeme tak mimo jiné identifikovat i SPoF
5. Hodnotíme aktiva.
6. ...



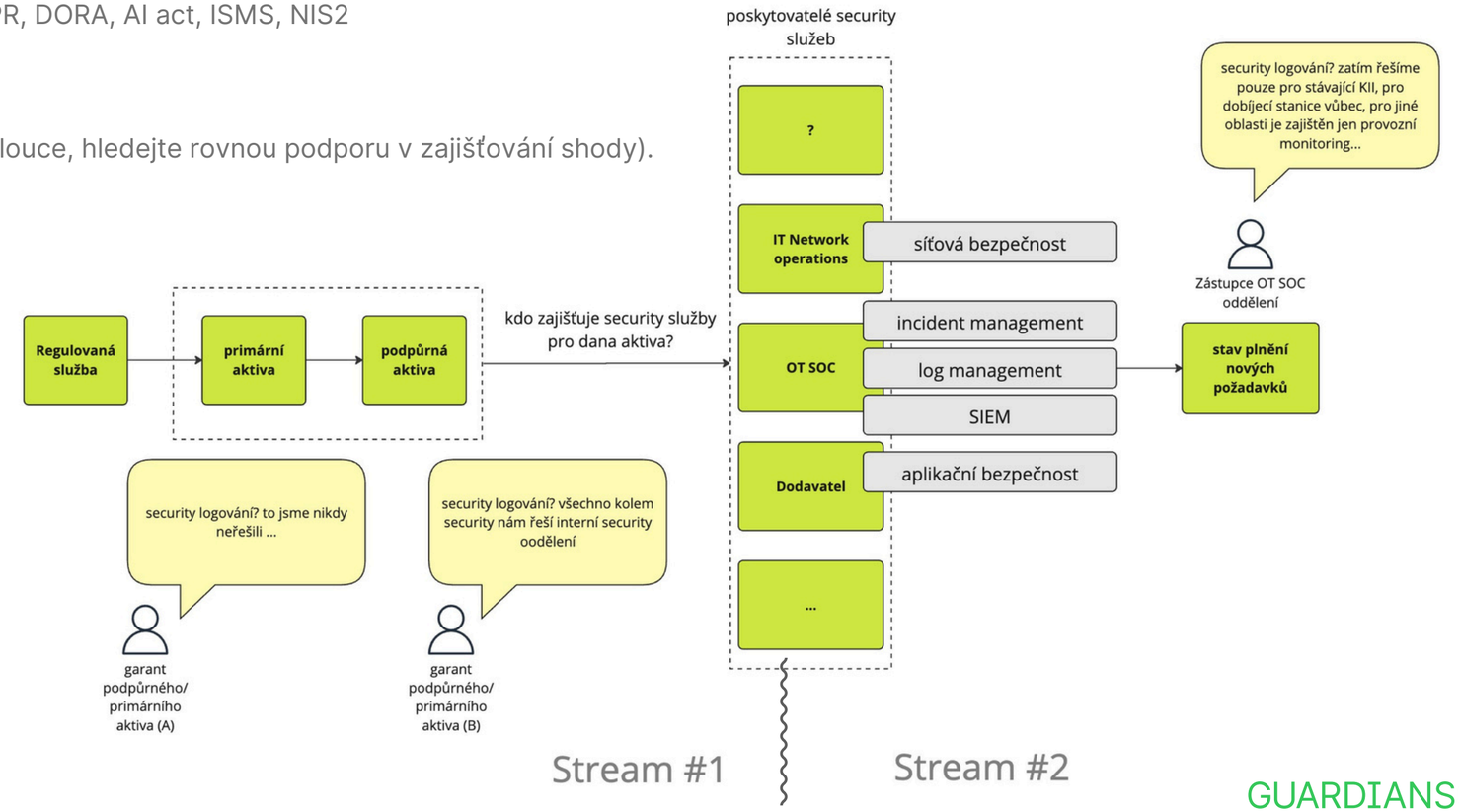
Zdroj: Atlassian.com


>>
Současný stav

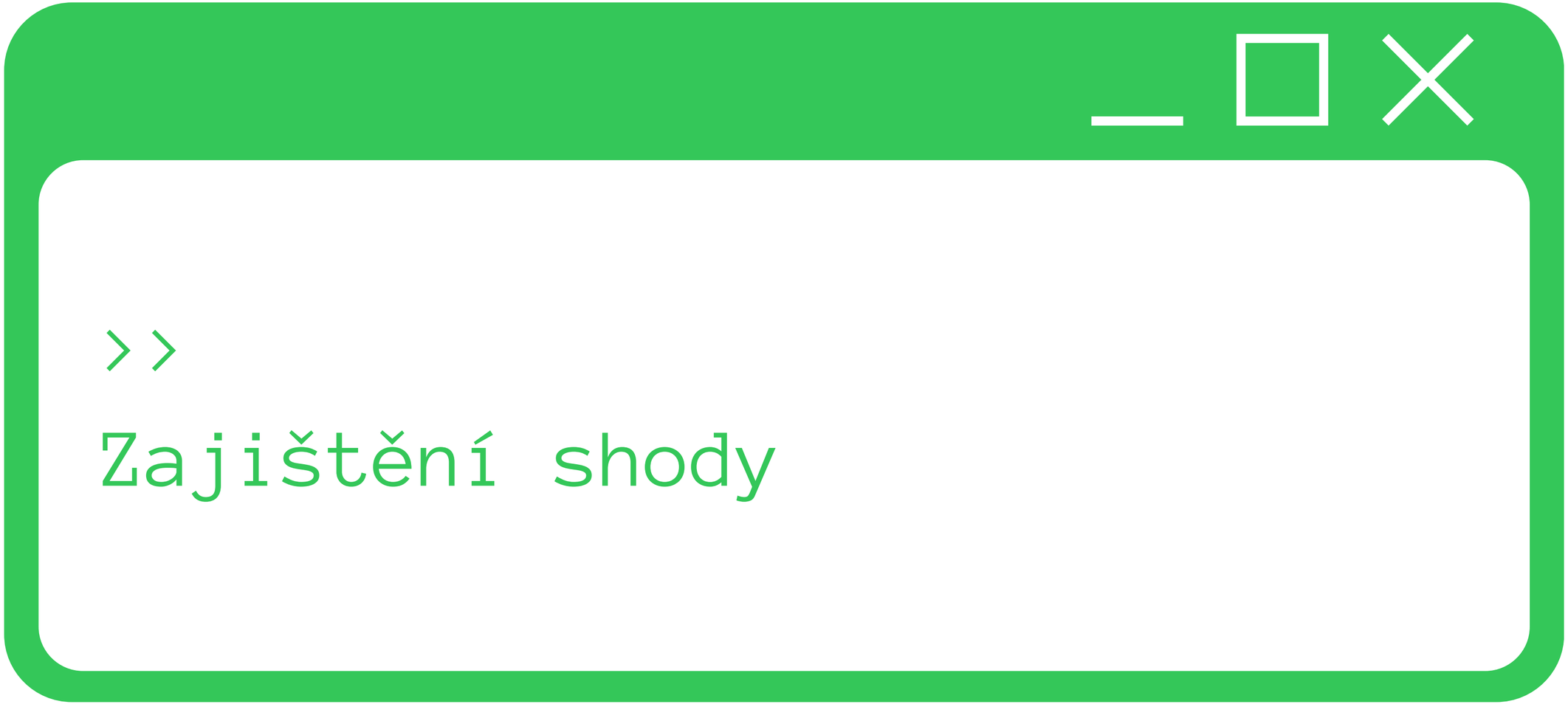
Současný stav řízení kybernetické bezpečnosti

Příklady, jak jej zmapovat:

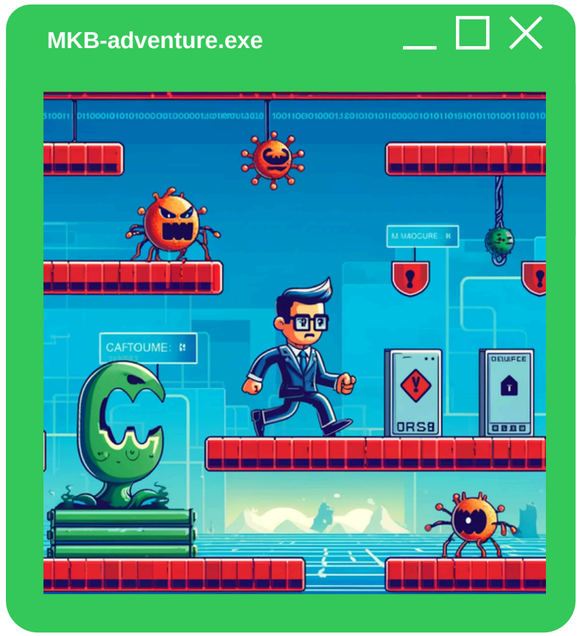
- **Compliance mapování**
  - Když na vás dopadá více regulací/standardů - nejčastěji GDPR, DORA, AI act, ISMS, NIS2
- **Gap analýza**
  - Nedělejte gap analýzu, pokud to není nutné (jste li na zelené louce, hledejte rovnou podporu v zajišťování shody).
- **Audity**
- **Testy**
- **Cvičení**
- **...**



GUARDIANS CZ


>>
Zajištění shody

Manažer kybernetické bezpečnosti (MKB)



Pozn.: Pro nižší režim povinností není povinná role MKB, hovoří se tu o osobě odpovědné za KB (obecně).

Úkoly MKB

1. Porozumění kontextu organizace a jejím strategickým a obchodním cílům.
2. Podpora při stanovení rozsahu, hodnocení aktiv a jejich vazeb na ostatní aktiva a poskytování regulovaných služeb.
3. Mapování současného stavu řízení kybernetické bezpečnosti organizace.
4. Zajištění procesu řízení rizik a podpora s identifikací a hodnocením rizik.
5. S ohledem na rizika, sestavení plánu zvládání rizik (RTP) a prohlášení o aplikovatelnosti (SoA) (přehled bezpečnostních opatření).
6. V návaznosti na předchozí kroky, sestavení/aktualizace bezpečnostní strategie kybernetické bezpečnosti.
7. Odpovědnost za projekt zavádění jednotlivých bezpečnostních opatření.
    a. Podpora při výběru vhodných technologických partnerů, dodavatelů bezpečnostních řešení (end-point protection, ZTNA, log management, SIEM/SOAR atd.).
8. U vyššího režimu regulace, spolupráce s architektem kybernetické bezpečnosti na definici cílové bezpečnostní architektury organizace.
9. Spolupráce na zavádění a testování bezpečnostních procesů (např. incident management, řízení přístupů atd.).
10. Komunikace s NÚKIB a příslušným CERT týmem ve věcech regulace.
11. Podpora při zajišťování kyber-bezpečnostních školení a zvyšování úrovně bezpečnostního povědomí.
12. Reporting směrem k vedení organizace.
13. Koordinace schůzek výboru pro řízení KB (vyšší režim).
14. ...

Klíčová je komunikace s garanty

- **Kdo je garant aktiva?**
  - Záleží na úhlu pohledu a granularitě řízení aktiv, co je ale nutné říct – chybou je, když v tomto ohledu zapomenete na toho **nejvýznamnějšího garanta - vrcholný management**.

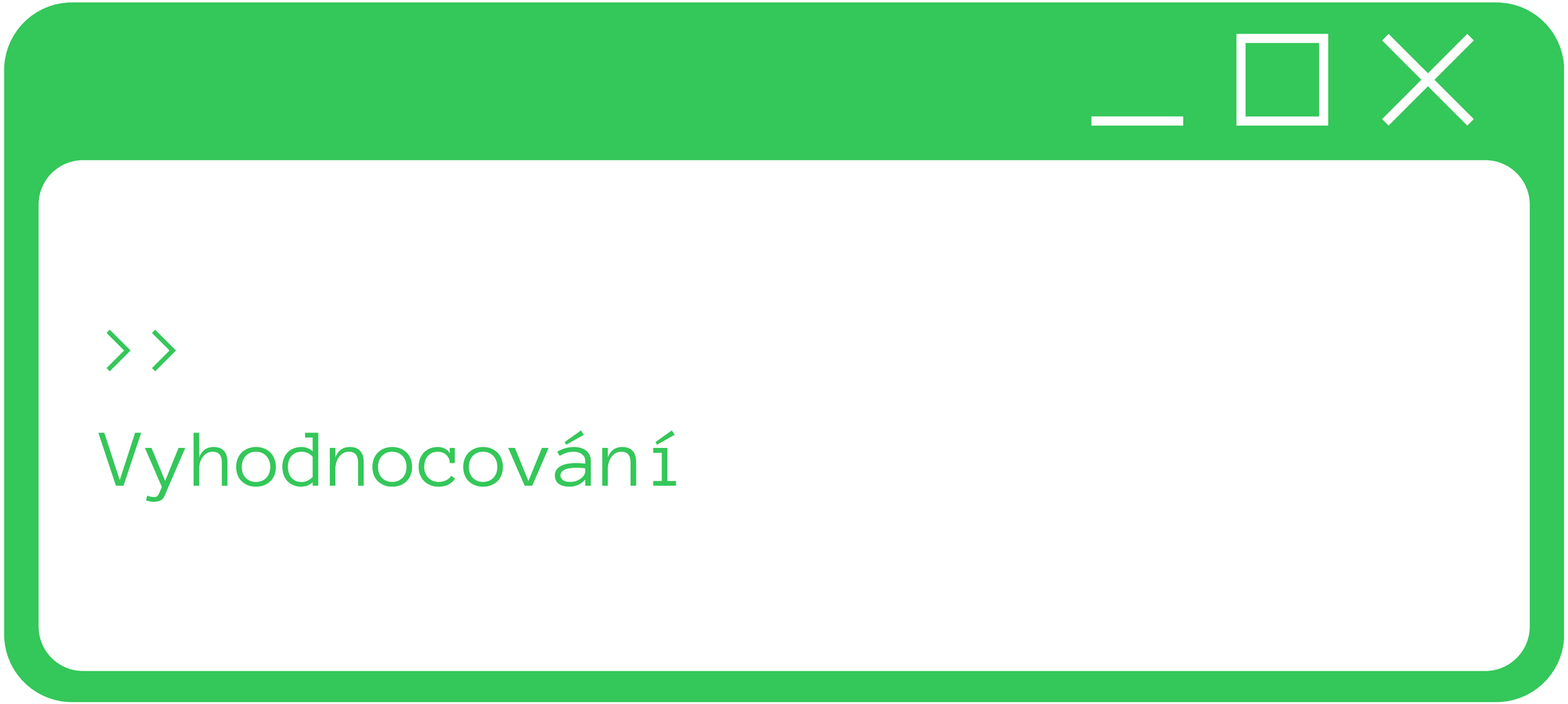
- **Proč je komunikace s garanty klíčová?**
  - Garant aktiva, mimo jiné, pomáhá s tím, aby vaše bezpečnostní opatření byly implementovány v souladu s business potřebami a aby podporovaly business cíle!

- **Výzva je, docílit toho, že máte od garantů průběžně aktualizované informace:**
  - **CMDB, rizika, priority atp.**

Řízení rizik - jak na to (a jak ne)

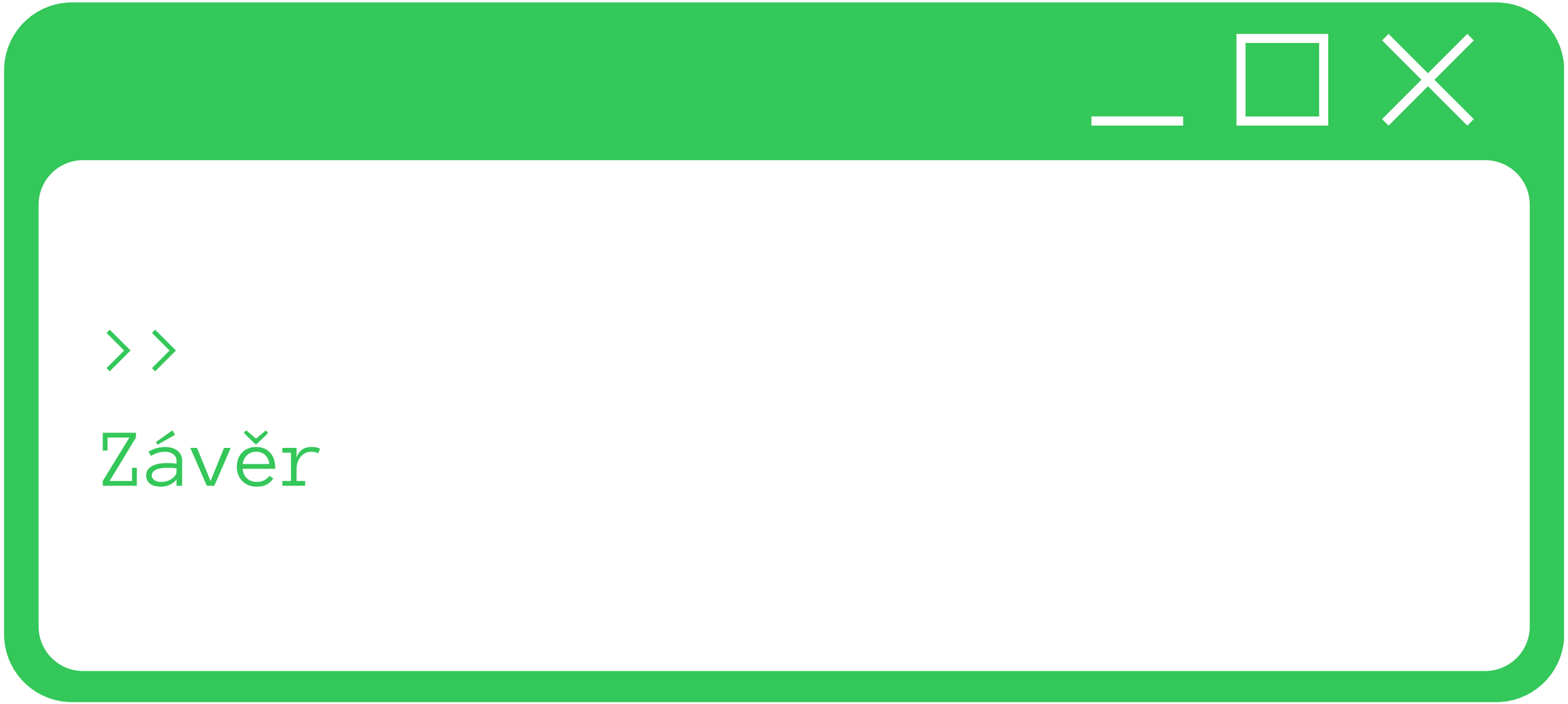
- Nekombinujte “nahodile” různé metodiky dohromady.
  - Zvolte si jeden přístup, **který bude podporovat vaše rozhodování** a tím postupujte.
    - **Doporučuji kvalitní popis scénáře rizika a stanovení jeho výše (ideálně kvantitativně).**
  - Samozřejmě přezkoumávejte jeho účinnost a zlepšujte.
- **Pamatujte - Nástroj není cíl!** (cílem není mít risk management / GRC nástroj, krásně vybarvený a vyplněný, ale mít řízená rizika).
- **Pracujte s reálnými daty!.**
  - Popisujte scénáře rizik, ale reálné - vzhledem ke kontextu.
  - Využijte security nástroje, které vám rizika identifikují (XDR, IDS/IPS, honeypoty, vulnerability skenery ...).
  - Využijte MITRE ATT&CK®.
- Popisujte četnosti možného výskytu a možné dopady (kolik by to firmu stálo).
- Pokud se budete pohybovat v korporátním prostředí, hledejte “parťáky”, kteří již nějaký risk management dělají (např. finanční rizika, strategická/celo-korporátní rizika).
- Neopisujte do rizik “jedna k jedné” výstupy ze security nástrojů a incidentů.
- Současnou metodiku NÚKIB k řízení rizik **NEDOPORUČUJI**.
  - Naopak doporučuji inspirovat se ve starší dopadové tabulce: Metodika | Tabulka.
- **Pracujte s možnými finančními dopady rizik => pak vám bude rozumět business / vrcholné vedení.**
- **Komunikujte rizika!**

1. Zkuste změnit mindset - zajišťujte kybernetickou bezpečnost pro svoji organizaci, ne pro regulátora, bude to jistě trochu dražší, ale alespoň to bude k něčemu…
2. Pamatujte na to, že MKB není superman, že musí spolupracovat s businessem (nezvládne vše sám).
3. Pamatujte na to, že odpovědnosti se nedá zbavit skrz dodavatele.
4. **Nezačínejte směrnicemi!** **Začněte strategií, aplikací primárně technických a poté organizačních opatření, vše dokumentujte a poté doplňte o směrnice. Rozhodně nedělejte to, že nejprve píšete (nebo si necháte napsat) směrnice a poté aplikujete do praxe.**
5. Při aplikaci bezpečnostních opatření vnímejte kontext a zohledňujte rizika.
6. **Usilujte o security by default / by design => Nestavějte kybernetickou bezpečnost jako něco, co je vedle vašeho primárního businessu, nýbrž jako jeho součást!**
7. Balancování mezi krátkodobým ziskem a dlouhodobým udržitelným businessem díky zajištění cyber resilience je výzva pro MKB a vrcholné vedení - nutno “párovat” obchodní a bezpečnostní strategie.
8. **Žádná bezpečnostní technologie nebude dost bezpečná, pokud s ní v čase nemíníme neustále pracovat!**
9. Přistupujte k zajišťování kybernetické bezpečnosti smysluplně!


>>
Vyhodnocování

Vyhodnocování účinnosti

1. Stanovte si metriky, ty pravidelně vyhodnocujte.
2. Provádějte testování a simulace
    a. Penetrační testy
    b. Cvičení
    c. Testování IRP, BCP, DRP
3. Provádějte audity, střídejte při tom auditory!


>>
Závěr

Základní otázky k plnění NIS2 / nZKB - shrnutí

- ☑ **Kdo jsem?** (Typ regulované služby)
- ☑ **Co musím plnit?** (Požadavky dle typu regulované služby)
- ☑ **V jakém rozsahu?** (Stanovení aktiv, která je nutné chránit)
- ☑ **Jaký je můj současný stav řízení kybernetické bezpečnosti?** (Gap analýza, compliance mapování)
- ☑ **Co mi zbývá “dodělat”?** (Zajištění shody s nZKB)
    - Kdo to bude dělat? (Bezpečnostní role)
    - Jaké procesy a technologie implementovat (RfP, PoC, ...)
- ☑ **Jak to vyhodnocovat?** (Metriky, testování, audity, cvičení, ...)

nZKB akademie 2025

Unikátní vzdělávání zaměřené
na nový kybernetický zákon
v souvislostech.

Se slevovým kódem **ALIANCE-ZKB**
za cenu **19.000 Kč bez DPH**

https://www.cybersecurityplatform.cz/akademie

GUARDIANS CZ

Děkuji za pozornost

Martin Konečný.jpg

kontakty.vcf

Ing. Martin Konečný, MBA, CISM
GSM: +420 736 709 865
martin.konecny@guardians.cz
www.GUARDIANS.cz

GUARDIANS cz