# Jak splnit požadavky nZKB, regulace plynoucí z NIS2

Virtuální konference Security as a Service | 16. 5. 2024

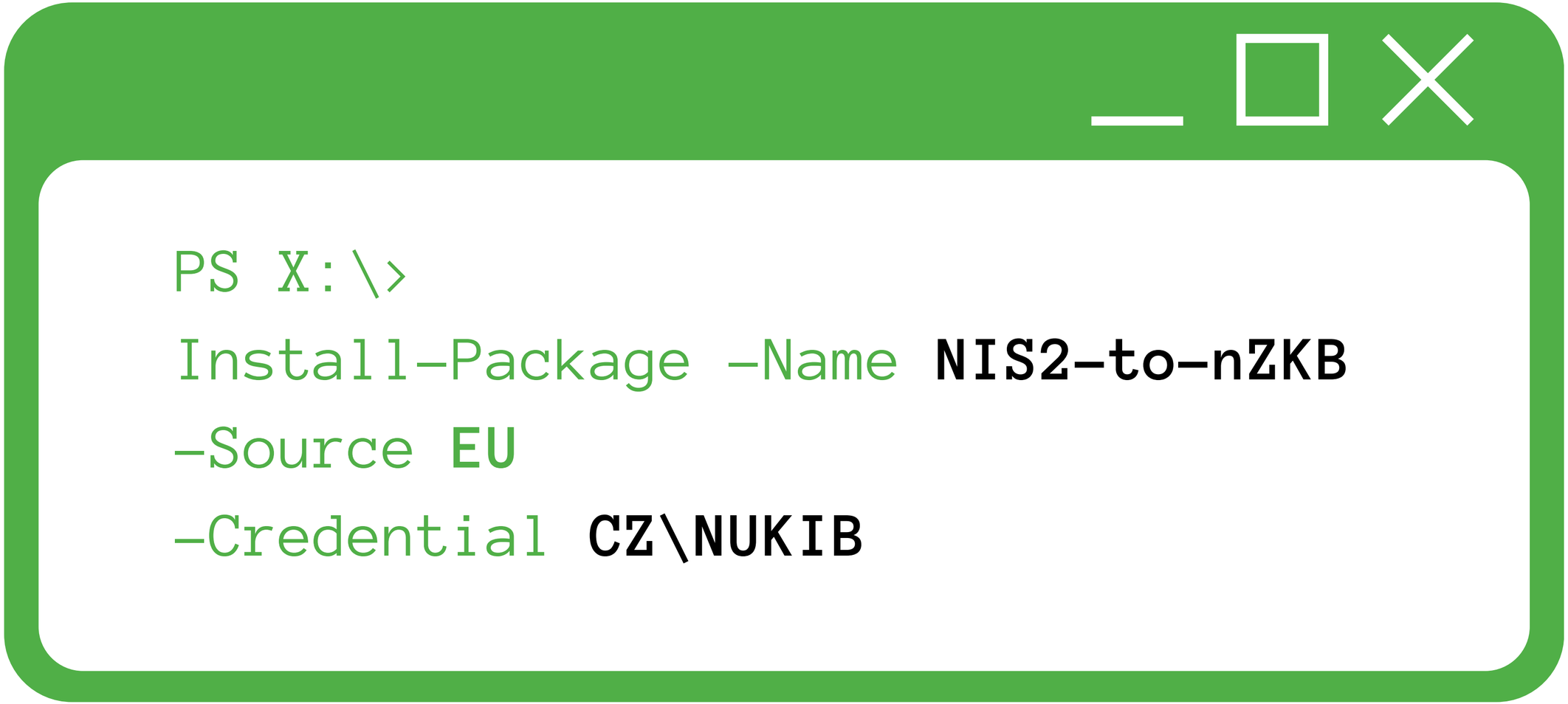
**Ing. Martin Konečný, MBA, CISM**
www.GUARDIANS.cz

GUARDIANS.cz

## Agenda.exe

- Intro k NIS2 a nZKB
  - Dopad regulace na firmy
  - Povinnosti
- Gap analýzy
- MKB / MKBaaS
- Zkušenosti z pohledu konzultanta
- Shrnutí

*Vnímejte prosím informace v této prezentaci tak, že jde o názor autora, na základě jeho zkušeností, neberte tyto informace však jako dogma - možných přístupů a řešení je samozřejmě více.*


PS X:\>
Install-Package -Name NIS2-to-nZKB
-Source EU
-Credential CZ\NUKIB

# NIS2

- Směrnice EU, která nahrazuje předchůdce – Směrnici NIS (1)
- Směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v EU
- Nejedná se o nařízení, jako např. u GDPR - každý z členských států ji zapracovává odlišně do svých zákonů
  - **Nedopadá na firmy, ale na státy EU!**
  - NIS2 definuje oblasti, které mají mít členské státy pokryty ve svých zákonech
- Cílem je, mimo jiné, sjednotit typy regulovaných subjektů v rámci států EU
  - NIS2 definuje regulovaná odvětví a typy subjektů v odvětvích dle důležitosti
    - Essential
    - Important

# NIS2 - Article 21

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

.....

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

- **policies on risk analysis and information system security;**
- **incident handling;**
- **business continuity, such as backup management and disaster recovery, and crisis management;**
- **supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;**
- **security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;**
- **policies and procedures to assess the effectiveness of cybersecurity risk-management measures;**
- **basic cyber hygiene practices and cybersecurity training;**
- **policies and procedures regarding the use of cryptography and, where appropriate, encryption;**
- **human resources security, access control policies and asset management;**
- **the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.**

# Nový kybernetický zákon (nZKB)

**Stav**

- Návrh nZKB v legislativním procesu, na základě jednání legislativní rady vlády dochází k drobným změnám textace návrhu
- Očekávaná platnost nZKB - jaro 2025
- **Poté ale půjdou do legislativního procesu ještě vyhlášky! (tedy i požadavky na bezpečnostní opatření)**

**Struktura**

- **Zákon**
  - Vyhláška **o regulovaných službách** (zde zjistím, zda moje firma pod regulaci spadá)
  - Vyhláška s **bezpečnostními opatřeními** pro **vyšší režim** regulace
  - Vyhláška s **bezpečnostními opařeními** pro **nižší režim** regulace
  - Ostatní vyhlášky

**Pozor na možné změny!**

# nZKB - změny

- Dopad na podstatně větší objem organizací, než dosud ze strany současného ZKB
- Přísnější sankce
- Zjednodušení v “určování“ a v typech regulovaných subjektů (nově 1 typ ve 2 režimech)
  - samoidentifikace
  - 2 režimy - vyšší a nižší režim regulace
- Úpravy v požadavcích na bezpečnostní opatření
- Nové instituty - strategicky významné služby, prověřování bezpečnosti dodavatelského řetězce atd.

```
PS X:\>
Get-ADGroupMember
-Identity "nZKB-regulovane-subjekty"
```

# 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, ...

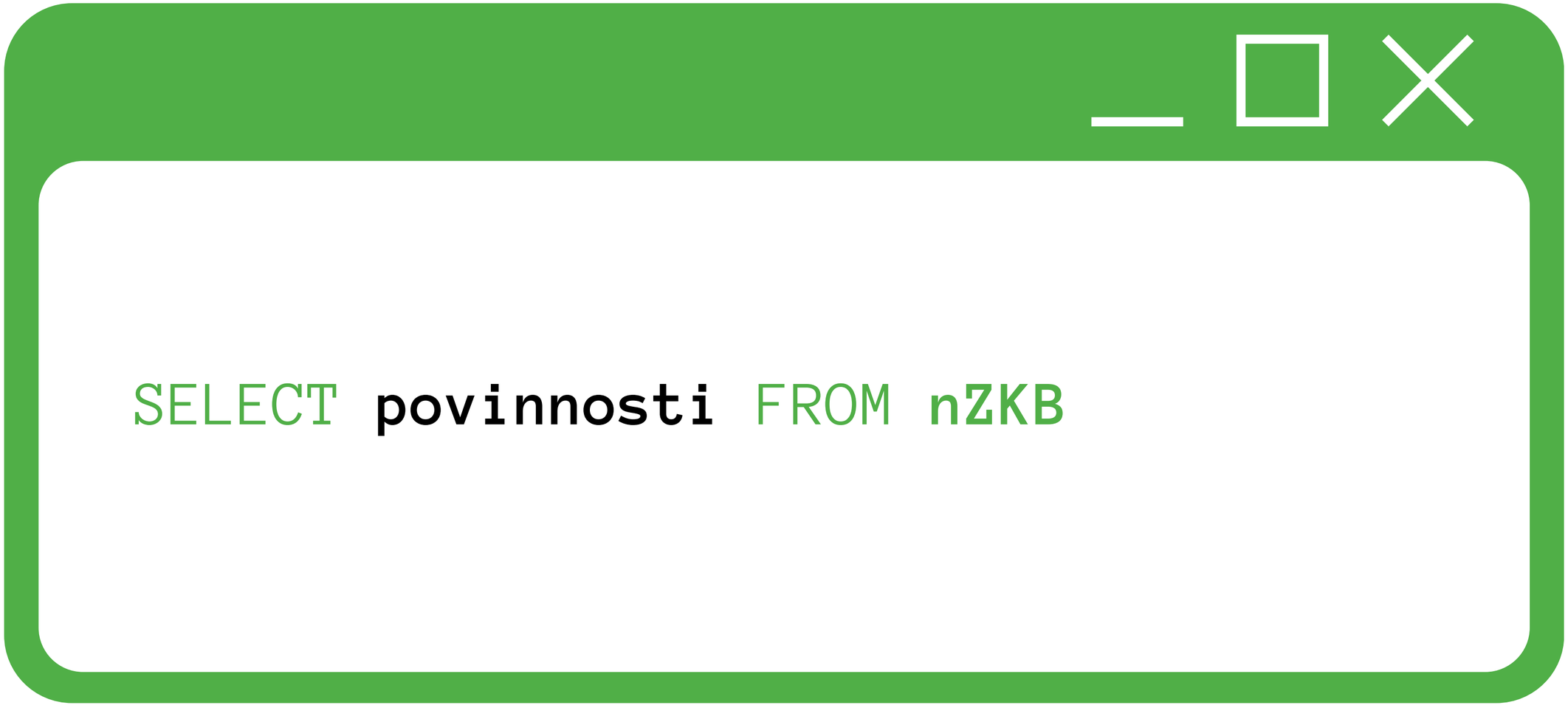
**nižší režim**

***Pozor na nejasnosti u některých definic - MSSP, cloudy atp. a to až na úrovni EU!***

# nZKB - dopad - 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<br>I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je velkým podnikem,<br>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. |


SELECT povinnosti FROM nZKB

| Organizační opatření | |
|---|---|
| **Vyhláška pro režim vyšších povinností** | **Vyhláška pro režim nižších povinností** |
| Systém řízení bezpečnosti informací | Zajišťování kybernetické bezpečnosti |
| Povinnosti vrcholného vedení | |
| Bezpečnostní role |  Bezpečnost lidských zdrojů |
| Řízení bezpečnostní politiky a dokumentace | *požadováno přes přílohu* |
| Řízení aktiv | |
| Řízení rizik  | |
| Řízení dodavatelů | *požadováno přes přílohu* |
| Bezpečnost lidských zdrojů | *požadováno přes přílohu* |
| Řízení změn | - |
| Akvizice, vývoj a údržba | - |
| Řízení přístupu | |
| Zvládání kybernetických bezpečnostních událostí a incidentů | Řešení kybernetických bezpečnostních incidentů + stanovení významnosti incidentů |
| Řízení kontinuity činností | Řízení kontinuity činností |
| Audit kybernetické bezpečnosti | - |

| Technická opatření | |
|---|---|
| **Vyhláška pro režim vyšších povinností** | **Vyhláška pro režim nižších povinností** |
| Fyzická bezpečnost | - |
| Bezpečnost komunikačních sítí | |
| Správa a ověřování identit | - |
| Řízení přístupových oprávnění | Řízení identit a jejich oprávnění |
| Detekce kybernetických bezpečnostních událostí | Detekce a zaznamenávání 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 | - |

# Vyšší režim - opatření a nástroje

| Organizační opatření | Technická opatření | Nástroje / principy (př.) |
|---|---|---|
| Systém řízení bezpečnosti informací | | GRC, politiky, metriky |
| Povinnosti vrcholového vedení | | metriky, reporting, manažerské nástroje, 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 |
| Řízení aktiv | | GRC, CMDB |
| Řízení rizik | | GRC, RM tool, metriky, BCMS (z hlediska návaznosti) |
| Řízení dodavatelů | | GRC, SCM nástroje, právní služby |
| 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 |
| Akvizice, vývoj a údržba | Aplikační bezpečnost | Security by default/design, penetrační testy, red teaming, hardening, AppFW, WAF |
| Řízení přístupu | Řízení přístupových oprávnění<br>Správa a ověřování identit | IDM, PAM, Tier model |
| Zvládání kybernetických bezpečnostních událostí a incidentů | Detekce kybernetických bezpečnostních událostí<br>Zaznamenávání bezpečnostních a relevantních provozních událostí<br>Vyhodnocování kybernetických bezpečnostních událostí | log management, end-point protection (např. XDR), IDS, IPS, SIEM/SOAR, IRP testing |
| 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 |

Plnění nZKB není jen o jednom člověku / specializaci / dodavateli, ani o jedné technologii!

# Povinnosti - do kdy plnit?

- Bezpečnostní opatření musí být plněna **nejpozději do 1 roku od zápisu do evidence poskytovatelů regulovaných služeb**
- Zdá se vám to dostatečně dlouhá doba?
  - úskalí:
    - výběrová řízení
    - doba návrhu řešení, volby vhodného vendora, integrátora a samotná implementace u některých řešení může být delší
    - lidské a finanční zdroje
    - ...

```
PS X:\> Start-Process
-FilePath "C:\NIS2-gap-analysis.exe”
```

# Na co si dát pozor

## Warning.exe

- Gap analýza není záležitostí 1 MD
- Gap analýza firem se nedělá vůči NIS2!!
- Bavíme li se o nZKB, pak by gap analýze mělo předcházet právní poradenství - určení zda firma vůbec naplňuje stanovenou regulovanou službu
- Pokud se v rámci gap analýzy rovnou zaměříte na plnění požadovaných bezpečnostních opatření, bez identifikace aktiv, bude vám chybět kontext a analýza bude příliš obecná
- Nelze vynechat business vlastníky klíčových procesů a služeb (garanty aktiv)
- Pozor na možné změny znění nZKB / nVKB!
- Výstupem by měl být: Popis současného stavu, vyhodnocení, doporučení, odhady zdrojů atd.

# Gap analýza k nZKB

**Kde NEmá smysl dělat gap analýzu?**

zelená louka, nulová cybersecurity maturita
*(prostě nedělám gap analýzu, ale navrhuju plán realizace a začínám zavádět...)*

nevím, zda firma spadá pod nZKB, možná ne,...
*(nejprve hledám právní pomoc)*

**Kde dává smysl?**

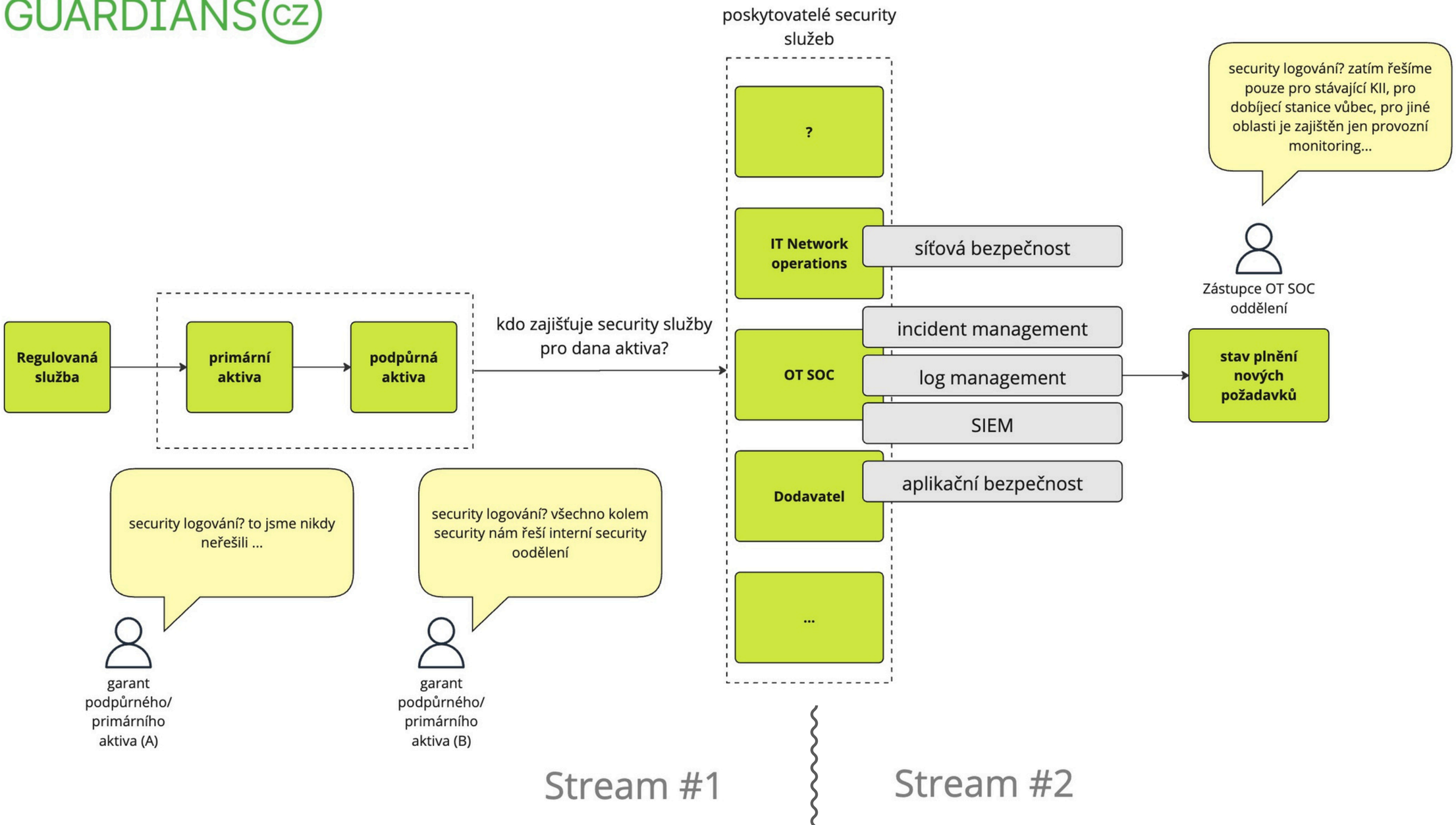
tam, kde už se kybernetický zákon řeší, nebo tam, kde se řeší obdobná regulace např. s přesahem do zahraničního businessu

tam, kde dodávám z hlediska bezpečnosti významné služby v budoucnu jednoznačně regulovaným subjektům, ale stále je nutné zohlednit stávající maturitu

GUARDIANS CZ

# Workflow

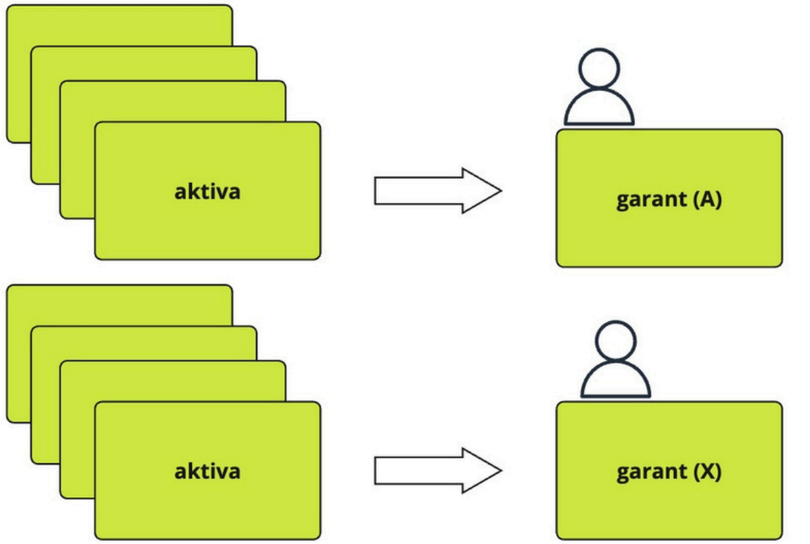
GUARDIANS CZ



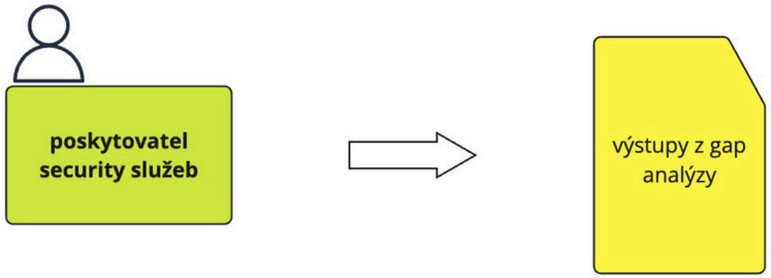

Stream #1

Stream #2

# Workflow




**Odborný pohled potřebný k detailní gap analýze**




**§ 25 Aplikační bezpečnost**

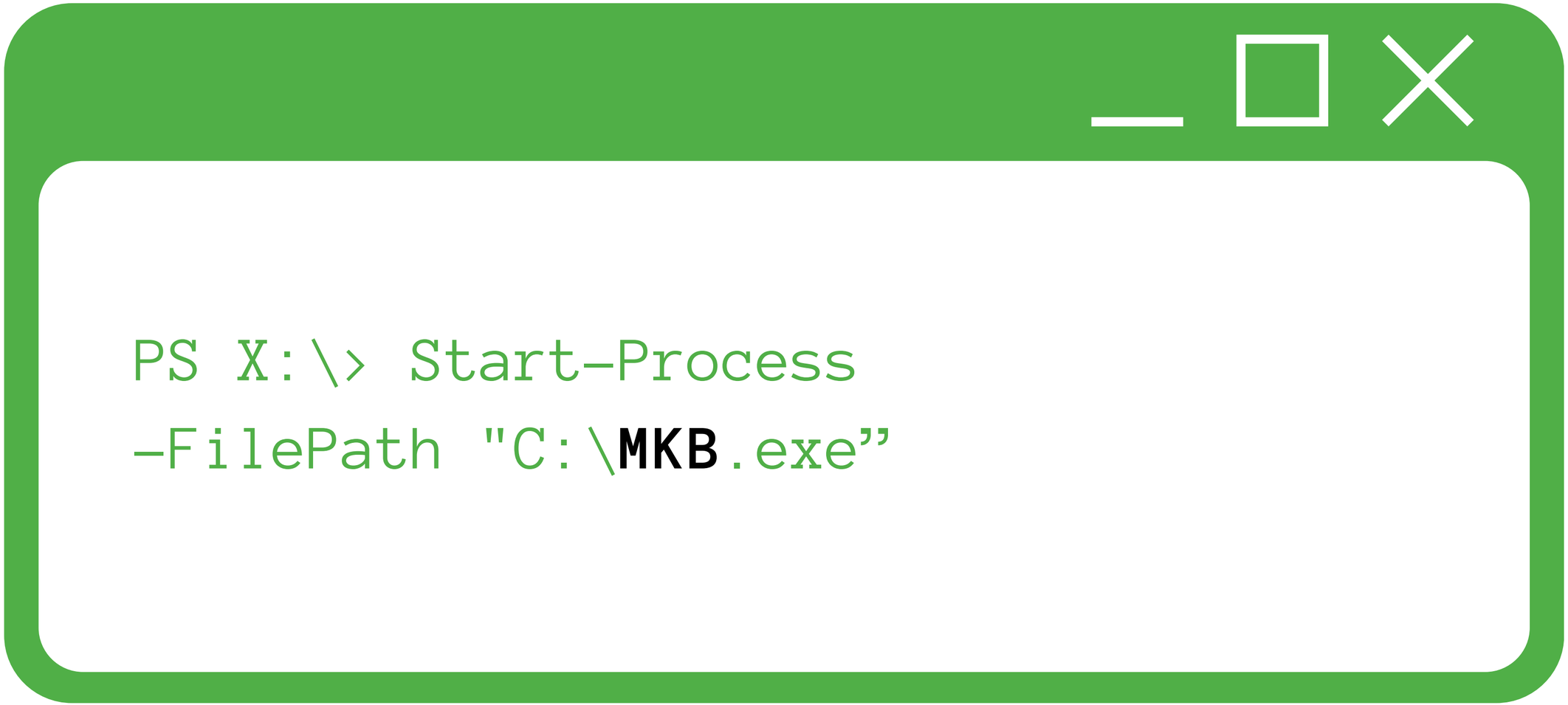
1. aktuální a podporovaný HW, SW
    a. řízení bezpečnostních výjimek
2. ochrana aplikací
3. každoroční skenování zranitelností z interní a externí komunikační sítě
    a. nápravná opatření
4. s ohledem na hodnotu aktiv, provádění penetračního testování z interní a externí komunikační sítě, v případě jejich uvádění do provozu, nebo při významných změnách, minimálně však jednou za 2 roky
    a. nápravná opatření
    b. re-test
5. ...

GUARDIANS.cz

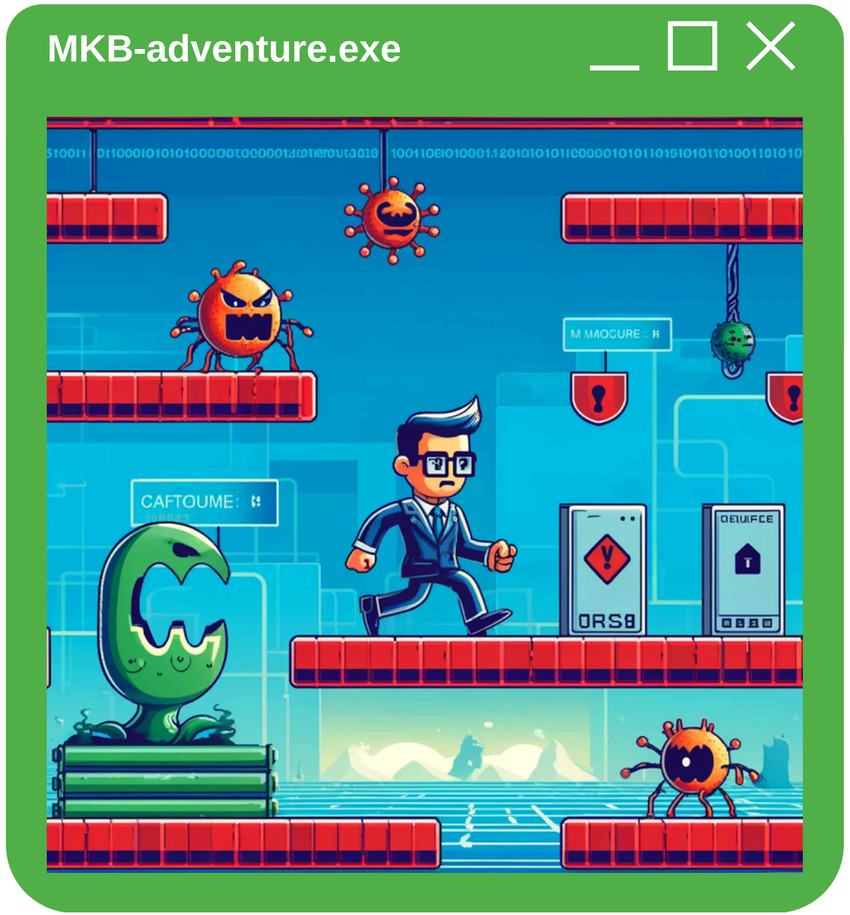
# Co po gap analýze?

## Next-steps.exe

- Revize výstupů
- Získání potřebných zdrojů
  - lidské, finanční a jiné
- Plán / projekt pro nápravu gapů
- Revize existujících procesů a služeb
- Revize existujících bezpečnostních opatření
  - úpravy směrnic a procesů
  - úpravy konfigurací nástrojů
  - ...
- Design nových řešení
- Pořízení a implementace nových nástrojů
- Testování
- Audity
- ...


PS X:\> Start-Process
-FilePath "C:\MKB.exe”

# Manažer kybernetické bezpečnosti (MKB)




**Znalosti**:

- Normy řady ISO/IEC 27000 (ISMS) a obdobné normy z oblasti bezpečnosti a ICT
- Přehled v oblasti ICT (operační systémy, databáze, aplikace, datové sítě) s důrazem na bezpečnost
- Řízení rizik, řízení kontinuity činností
- Relevantní právní a regulatorní požadavky, zejména zákon
- Kontext povinné osoby

**Zkušenosti**:

- Prosazování ISMS
- Porozumění definicím rizik a rizikovým scénářům, řízení rizik
- Schopnost interpretovat výsledky řízení rizik a koordinovat zvládání rizik.

**Vzdělání a praxe**:

- min. 3 roky praxe v oboru informační nebo kybernetické bezpečnosti, nebo VŠ a alespoň 1 rok praxe v oboru informační nebo kybernetické bezpečnosti

**Relevantní certifikace**:

- CISM, CRISC, CISSP a obdobné

# Úkoly MKB

1. Porozumění kontextu organizace a jejím obchodním cílům
2. Podpora při stanovení přehledu všech aktiv organizace, hodnocení aktiv a jejich souvislosti s poskytováním regulovaných služeb organizace
3. Mapování současného stavu řízení kybernetické bezpečnosti organizace
4. Zajištění procesu řízení rizik a podpora s identifikací a hodnocením rizik s ohledem na typ organizace, ideálně s podporou dat, které jsou dostupné v bezpečnostních nástrojích, v MITRE ATT&CK a jiných relevantních datových zdrojích
5. S ohledem na rizika sestaví plán zvládání rizik (RTP) a prohlášení o aplikovatelnosti (SoA) (přehled bezpečnostních opatření)
6. V návaznosti na předchozí kroky pomůže sestavit bezpečnostní strategii kybernetické bezpečnosti
7. Sestaví projekt zavádění jednotlivých bezpečnostních opatření
8. U vyššího režimu regulace, společně s architektem kybernetické bezpečnosti, definuje cílovou bezpečnostní architekturu organizace
9. Společně pracuje na zavádění a testování bezpečnostních procesů (např. incident management, řízení přístupů atd.)
10. Podporuje organizaci při výběru vhodných technologických partnerů, dodavatelů bezpečnostních řešení (end-point protection, ZTNA, log management, SIEM/SOAR atd.)
11. Komunikuje s NÚKIB a příslušným CERT týmem ve věcech regulace
12. Pomáhá zajišťovat kyberbezpečnostní školení
13. Reportuje a zodpovídá se vedení organizace
14. ...


PS X:\> Start-Process
-FilePath "C:\MKBaaS.exe”

# MKB(aaS) - intro

- Obecně je vhodné zopakovat:
  - nZKB klade jisté nároky (nejen) na lidské zdroje
    - manažer kybernetické bezpečnosti (MKB)
    - architekt kybernetické bezpečnosti
    - auditor kybernetické bezpečnosti
    - nebo obecně na osobu odpovědnou za kyberbezpečnost organizace
  - Firmy mají nedostatek lidských zdrojů v oblasti KB
  - Pokud mají zaměstnance, kterému by některou z rolí přiřadili, tak často nesplňují kvalifikační / znalostní předpoklady
    - to je důvod k hledání externí podpory - např. MKBaaS

Pozor na to, že zapojením MKBaaS

  - se firma nezbavuje odpovědnosti, tu přenést nelze
  - to neznamená, že na své straně nebudete muset rezervovat další zdroje (HR, finance, nástroje atd.) a že se o “nic” už nemusíte starat (viz odpovědnosti výše)
  - ...

# MKBaaS

- Co chtít po MKB(aaS):
  - **Reference, kompetence!**
  - Systém řízení bezpečnosti informací (+ SOA)
    - podpora při řízení aktiv
    - podpora při řízení rizik (+ RTP)
  - Strategie a plán pro řízení kybernetické bezpečnosti organizace
  - Podpora při výběru vhodných bezpečnostních nástrojů
  - Pravidelný reporting a komunikace směrem k vrcholnému vedení (+ výbor)
  - Security by default / by design (v procesech organizace)
  - Komunikace s NÚKIB a s příslušným CERT týmem a regulátorem
  - Podílení se na řízení bezpečnostních incidentů
  - Další povinnosti z vyhlášky o KB
  - **Zastupitelnost + pohotovost**
  - **Transparentnost a podporu při exit strategii!**
  - ...

# MKB(aaS)


**Bez kontextu to nejde**

**Bez součinnosti to nejde**

**Bez spolupráce s vedením to nejde**

**MKBaaS není totéž, co vlastní MKB**

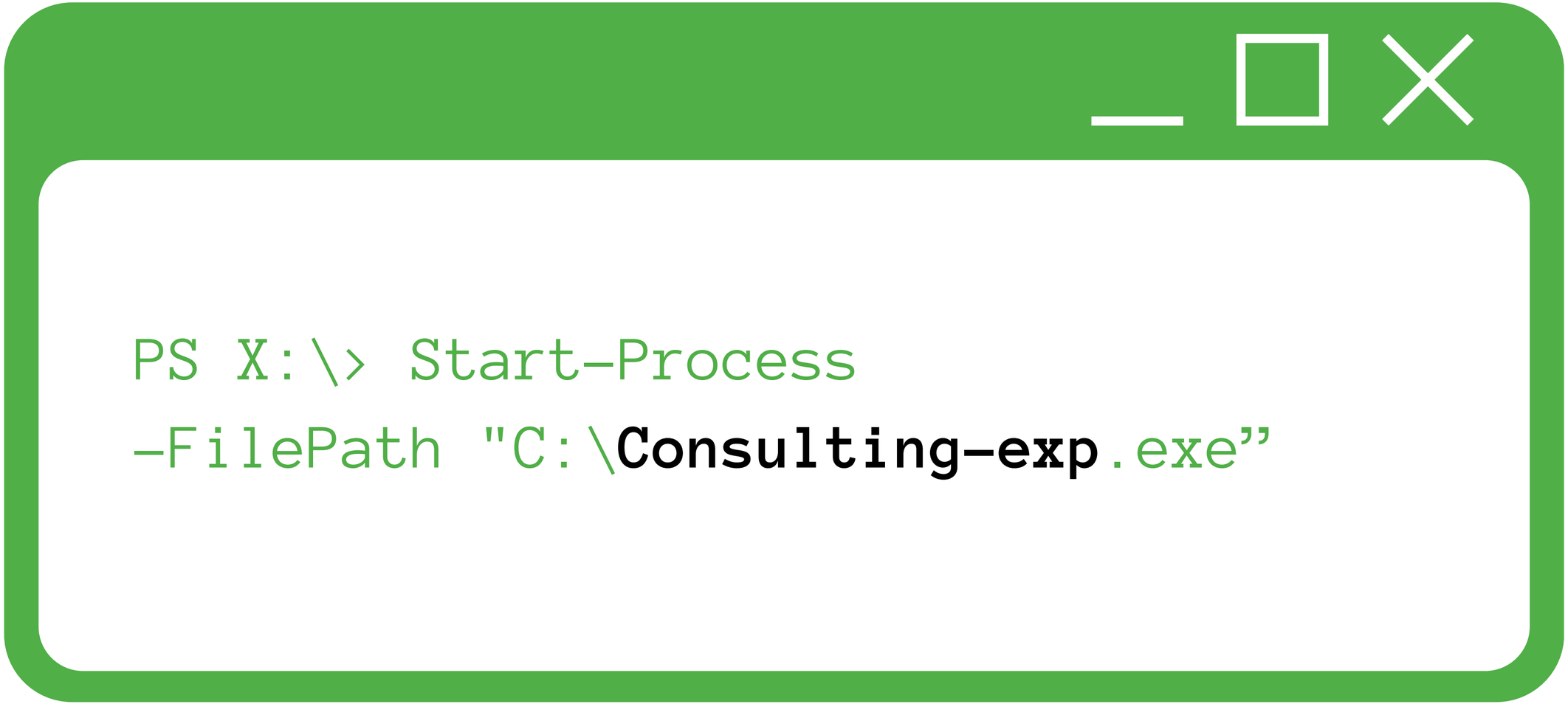
**Data-driven security RM**

**Náklady na MKBaaS nejsou rovny celkovým nákladům na bezpečnost!**

**Papír vs. praxe - co má přednost?**

# Security-as-a-Service

- Obecně je třeba vnímat určité rozdíly u Security-as-a-Service oproti “tradičnímu” řešení
  - Využití Security-as-a-Service neznamená, že nepotřebujete další vlastní zdroje
    - usnadnění v oblasti provozních záležitostí
    - využití zkušeností dodavatele
    - nutné ale zajistit správnou implementaci
  - Interní zaměstnanec v roli MKB vs. MKBaaS
  - Interní log management nástroj + infrastrukturní technologie + infra tým + security tým vs. LMaaS
  - Uplatnění jiných typů nákladů CAPEX vs. OPEX (Security-as-a-Service)
  - Nezapomenout na bezpečnost dodavatelského řetězce i v rámci Security-as-a-Service


PS X:\> Start-Process
-FilePath "C:\Consulting-exp.exe”

# Chyby v uvažování zákazníků

*VY DĚLÁTE TU PAPÍROVOU NEBO TECHNICKOU BEZPEČNOST?*

*ŘEKNĚTE MI, ZDA SPADÁM POD REGULACI*

*BUSINESS CONTINUITY JE ZÁLEŽITOSTÍ “SECURITY”*

*INFO/CYBER SECURITY JE JEN JEDNA SPECIALIZACE, KAŽDÝ UMÍ VŠE ...*

*K ŘÍZENÍ DODAVATELŮ MI STAČÍ APLIKOVAT BEZPEČNOSTNÍ DODATKY DO SMLUV*

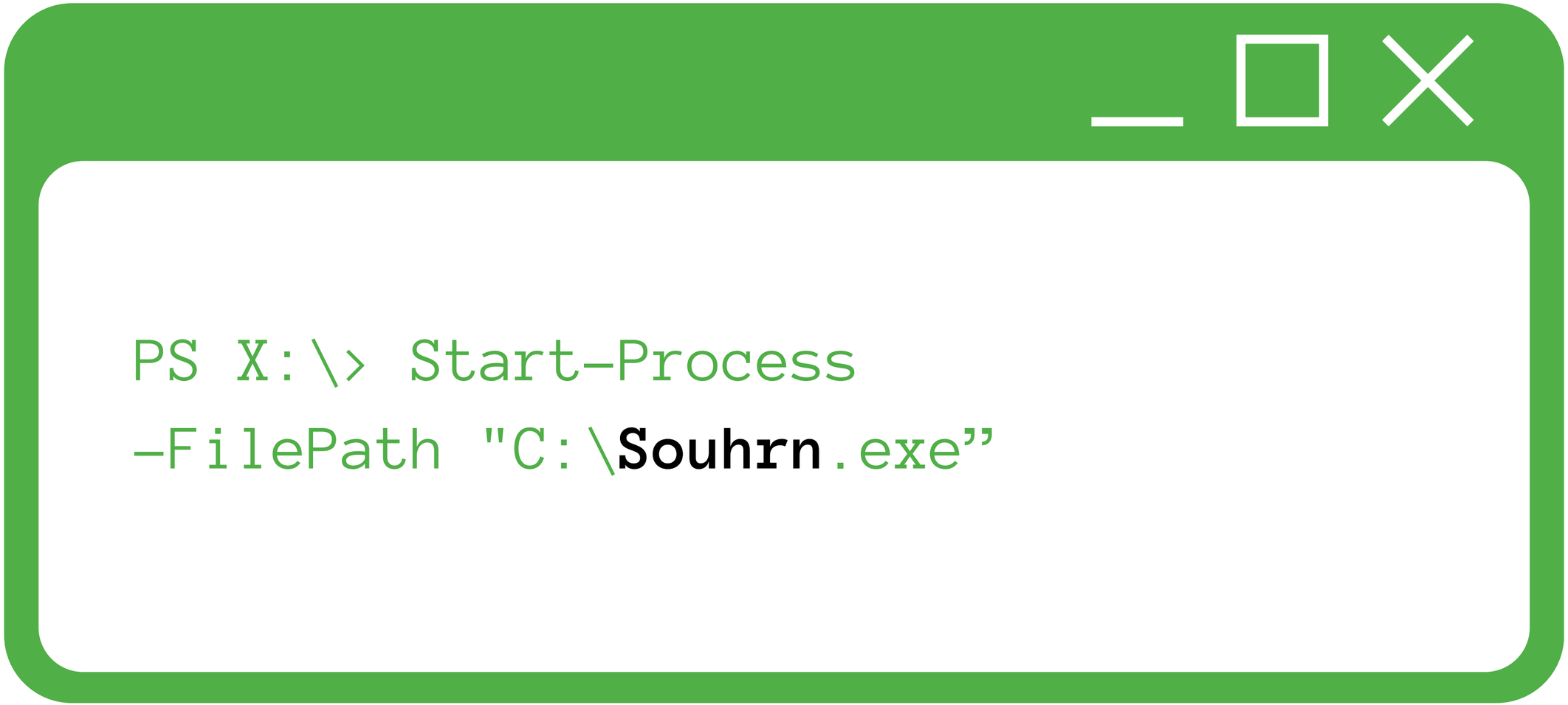
*NAŠE FIRMA NENÍ PRO HACKERY ZAJÍMAVÁ*

*HLAVNĚ, ABY TO BYLO CO NEJLEVNĚJŠÍ A ABY “ABY TO PROŠLO U NUKIBU”....*

GUARDIANS CZ


# Rozdílné Cybersecurity Maturity úrovně

*Zákazníci často požadují službu, ke které je třeba určitých prerekvizit, které však nemají splněny, jejich požadavky tak někdy nejsou pro jejich organizace efektivní, ani smysluplné*


PS X:\> Start-Process
-FilePath "C:\Souhrn.exe”

# Souhrn

- Pokud si nejste jisti s dopadem regulace na vaše společnosti, hledejte právní pomoc
- Nedělejte gap analýzu, pokud to není nutné
- Včas zajistěte lidské zdroje a naplánujte security budgety
- Nesoustřeďujte se jen na papíry ale na skutečnou bezpečnost
- Při aplikaci bezpečnostních opatření vnímejte kontext a zohledňujte rizika
- Pamatujte na to, že odpovědnosti se nedá zbavit skrz dodavatele
- Buďte odolní vůči NIS2 fantomům
- Přistupujte k zajišťování kybernetické bezpečnosti smysluplně!
- ...

# Newsletter

Pokud byste chtěli být informováni o tom, co se děje (nejen) kolem nZKB, zaregistrujte se k odběru mého newsletteru.

https://martinkonecny.substack.com/

GUARDIANS CZ

# nZKB kurz

A pokud byste chtěli jít hlouběji do problematiky, tak mám pro vás jedinečnou možnost využít tento promo kód a registrovat se do 4-měsíčního nZKB kurzu!

**Promo kód: 4M-NZKB-VIP**

https://www.cybersecurityplatform.cz/udalosti/4-mesicni-kurz-k-novemu-kybernetickemu-zakonu

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