Jak zvládnout nZKB:

Zkušenosti, rady a role manažera kybernetické bezpečnosti

Webinář Manpower IT | 7. 11. 2024

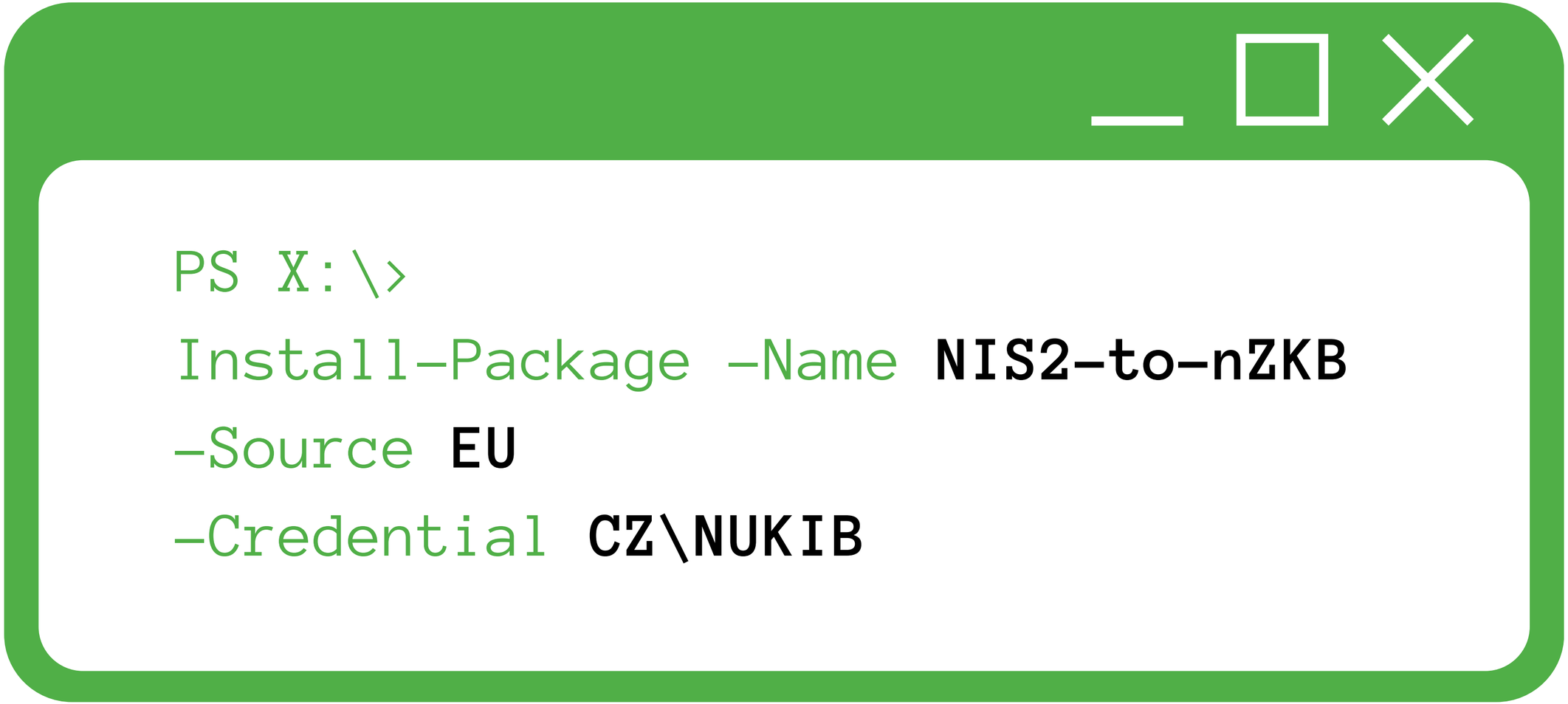
Ing. Martin Konečný, MBA, CISM
www.GUARDIANS.cz

GUARDIANS cz

Agenda.exe

- NIS2 a nZKB
- Dopad regulace na firmy
  - Povinnosti
- MKB / MKBaaS
- Závěrečné rady

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

NIS 2

NIS 2 = Směrnice EU, která nahrazuje předchůdce – Směrnici NIS (1)

Nedopadá na firmy, ale na státy EU! Definuje oblasti, které mají mít členské státy pokryty ve svých zákonech.

Pozor, pokud poskytujete regulované služby i v jiných státech EU, doporučuji sledovat národní specifika a zvolit si jednotný celo-korporátní rámec pro řízení KB.

NIS 2 - Article 21

...

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)

- Návrh nZKB v legislativním procesu (viz Sněmovní tisk 759: https://www.psp.cz/sqw/historie.sqw?o=9&t=759).
  - Schvalování nZKB je doprovázeno spoustou nepřesných a klamavých informací, vyvolaných zejména kolem mechanismu řízení bezpečnosti dodavatelského řetězce, který se však má v praxi dotknout jen minima strategických subjektů.
    - Doporučuji shlédnout starší díly newsletteru na: newsletter.guardians.cz
    - A pro pochopení historie také přečíst: https://pagenotfound.cz/clanek/kauza-huawei-cina-vydirala-ceskou-republiku.
  - Zároveň doporučuji projít si samotná bezpečnostní opatření - v nižším režimu byste neměli narazit na nic, co byste již nyní neměli dělat za tím cílem, aby byl Váš business odolný vůči hrozbám v kyberprostoru.
  - **Očekávaná účinnost nZKB - 1. 7. 2025.**
- **Pozn.: U vyhlášek bude samostatný legislativní proces (tzn. připomínky, schvalování atp.)!** (bude zahájen asi po skončení 2. čtení nZKB)

Struktura předpisů

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

Pozor! Průběžně sledujte možné změny!

```
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

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


SELECT povinnosti FROM nZKB

Povinnosti

1. Registrace poskytovatele regulované služby (hlášení údajů).
2. **Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby.**
3. **Plnění bezpečnostních opatření (=> nižší/vyšší režim povinností nebo nařízení EU pro digitální infra a služby).**
4. Hlášení a zvládání kybernetických bezpečnostních incidentů.
5. Informační povinnost poskytovatele regulované služby.
6. Zohledňování a plnění tzv. Protiopatření (historicky např. varování vůči některým technologiím z Číny, opatření k zabezpečení emailové infrastruktury atp.).
7. Zabezpečení dostupnosti strategicky významné služby (týká se omezeného rozsahu regulovaných subjektů).
8. Aplikace požadavků plynoucích z tzv. Mechanismu prověřování bezpečnosti dodavatelského řetězce (týká se omezeného rozsahu regulovaných subjektů).
9. ...

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

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

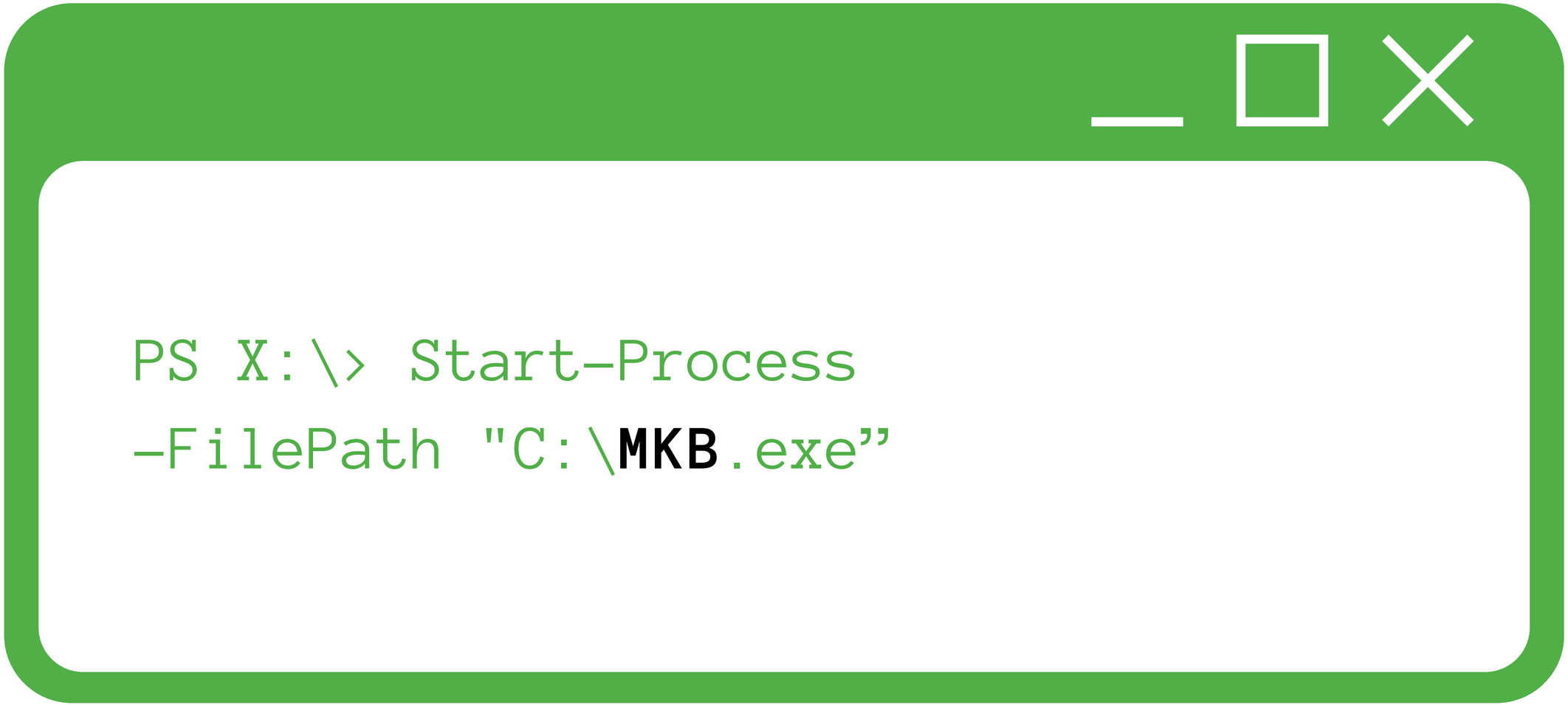
Do kdy plnit bezpečnostní opatření?

- Od účinnosti nZKB má běžet “administrativní” lhůta na “samoidentifikaci” (hlášení kontaktních údajů přes Portál NÚKIB).
- Bezpečnostní opatření musí být plněna **nejpozději do 1 roku od registrace do evidence poskytovatelů regulovaných služeb.**
- Zdá se vám to dostatečně dlouhá doba?
  - Možná úskalí, na která je třeba myslet (zejm. u vyššího režimu):
    - alokace financí,
    - hledání vhodných lidských zdrojů / outsourcing rolí,
    - doba návrhu řešení, volby vhodného vendora / systémového integrátora + reálná doba implementace,
    - výběrová řízení na technologie,
    - ...

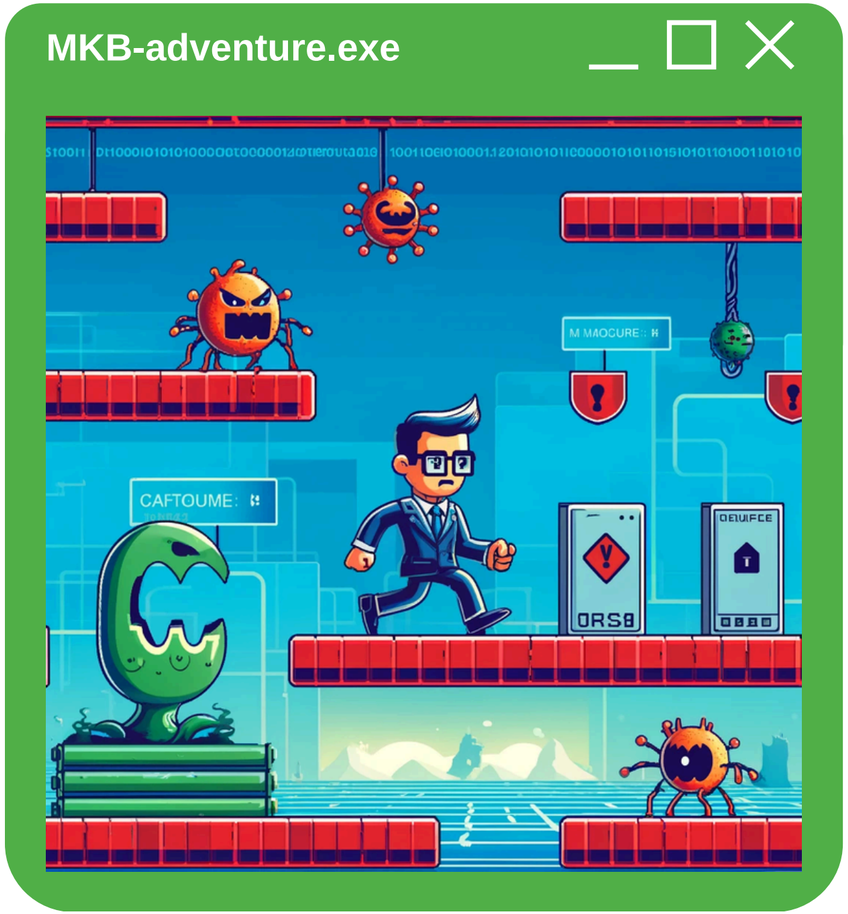
Novinka v povinnostech

Povinnosti vrcholného vedení

- **Pro již regulované subjekty se jedná snad o jedinou zásadní novinku v bezpečnostních opatřeních.**
- Vrcholné vedení:
  - prokazatelně **absolvuje školení**,
  - zajistí stanovení bezpečnostní politiky a **cílů ISMS, slučitelných se strategickým směřováním firmy**, zajistí **integraci ISMS do procesů firmy**, zároveň zajistí podporu k dosažení cílů systému řízení bezpečnosti informací a vede zaměstnance k rozvíjení efektivity (vyšší režim),
  - se **podílí na vypracování analýzy dopadů a zajistí testování IRP, BCP, DRP** (vyšší režim),
  - podporuje osoby zastávající bezpečnostní role při prosazování kybernetické bezpečnosti v oblastech jejich odpovědnosti, **zajistí jim pravomoci potřebné pro naplňování jejich rolí a zdroje včetně rozpočtových prostředků** k naplňování jejich rolí a plnění souvisejících úkolů (vyšší režim),
  - zajistí dostupnost zdrojů potřebných pro zajišťování kybernetické bezpečnosti,
  - zajistí stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role (vyšší režim),
  - se prokazatelně seznamuje se stavem KB organizace,
  - **zajistí zastupitelnost bezpečnostních rolí (vyšší režim).**


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.

Doporučení:

- U kandidátů prověřujte reference a reálné schopnosti, ale také bezpečnostní aspekty.

Úkoly MKB

1. Porozumění kontextu organizace a jejím strategickým a obchodním cílům.
2. Podpora při stanovení přehledu všech aktiv organizace, 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 s ohledem na typ organizace, ideálně s podporou dat, které jsou dostupné v bezpečnostních nástrojích, v MITRE ATT&CK a jiných relevantních znalostních bázích.
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 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 výborů pro řízení KB (vyšší režim).
14. ...

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

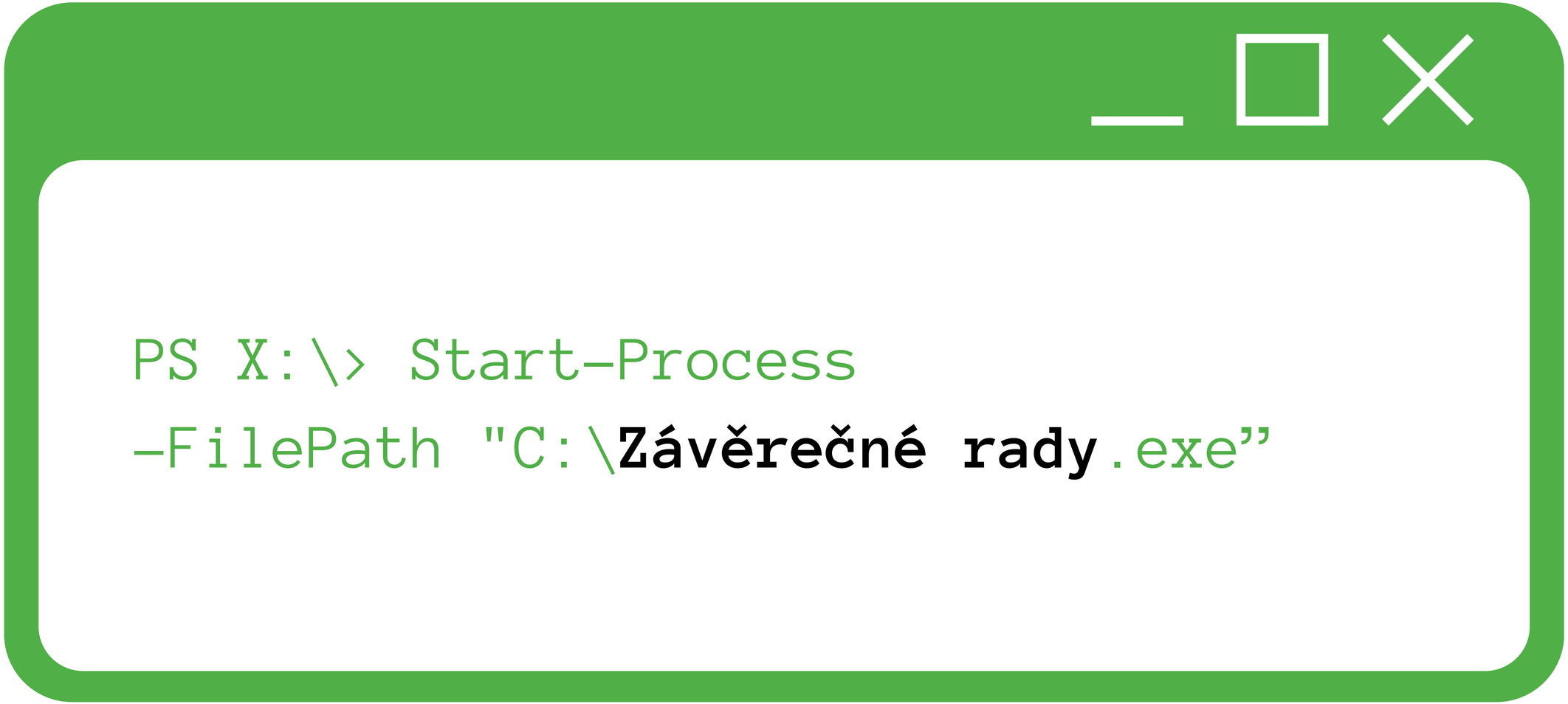
MKBaaS

- Obecně je vhodné zopakovat, že nZKB klade jisté nároky (nejen) na lidské zdroje:
    - manažer kybernetické bezpečnosti (MKB),
    - architekt kybernetické bezpečnosti,
    - auditor kybernetické bezpečnosti,
    - nebo obecně na osobu odpovědnou za kybernetickou bezpečnost 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) - toto ale platí i když se rozhodnete pro vlastního zaměstnance v roli MKB.

- Po poskytovateli MKBaaS vyžadujte:
  - **Zastupitelnost + pohotovost.**
  - **Transparentnost a podporu při exit strategii! (např. pokud budete přecházet z outsourcingu k vlastnímu zaměstnanci)**


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

V řízení KB je klíčová 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.**

Bezpečnost neřešíte pro regulátora

Nezaměřujme se “jen” na compliance, zaměřme se na praxi!

Berme nZKB jako jistý impuls (něco co nás donutí) k tomu začít pro zajišťování své kyberbezpečnosti opravdu něco dělat, ale...

...kybernetickou bezpečnost řešíte pro svojí firmu (pro svojí konkurenceschopnost, udržitelnost podnikání, důvěryhodnost vůči klientům apod.), nikoli pro regulátora!

VS.

Rozdíly v přístupu

Domény podle NIST	nZKB řeším “jen” pro regulátora (většinou nízká maturita)	Kybernetickou bezpečnost zajišťuji primárně pro své podnikání (vyšší maturita)
Govern, Identify	• Stanoveny politiky tak, jak je požaduje NÚKIB, v pořadí, jaké uvádí vyhláška. Prakticky však politiky neodpovídají reálné situaci firmy. • Řízení aktiv a rizik je řešeno doplněním dat do šablon NÚKIBu. Prakticky tomu ale moc nerozumíme a nevíme, co nám to má reálně přinést.	• Máme stanovené reálné bezpečnostní cíle, metriky a politiky tak, že odpovídají potřebám firmy a zohledňují compliance požadavky. • Pro řízení aktiv ve firmě využíváme firemní CMDB, kde jsou konfigurační položky doplněné o atributy, které vyžaduje nZKB. Řízení aktiv je součástí každodenní operativy. • Máme přehled o tom, co je náš skutečný “threat landscape”, máme popsány scénáře rizik a možné dopady, pracujeme s pravděpodobností dopadů, abychom určili výši rizika.
Protect	• Bezpečnostní opatření zavádíme pouze “slepě” tak, jak je po nás požadováno ve vyhlášce.	• Bezpečnostní opatření zavádíme s ohledem na identifikovaná reálná rizika (nikoliv rizika z katalogu). • Tam, kde se vyhláškou stanovené opatření z hlediska rizikovosti nevyplatí nasazovat, uvedu do SoA a pravidelně vyhodnocuju změny.
Detect	• **Logujeme a vyhodnocujeme pouze “slepě” to, co požaduje vyhláška a to v plném rozsahu (nákladné). Vendor nám technologie nasadil dle VŘ, ale neumíme s tím pracovat, nástroje nám ale fungují, neustále nám chodí nějaké alerty, ale nemáme nyní člověka, který by s tím pracoval…**	• **S ohledem na identifikovaná rizika, systémovou a bezpečnostní architekturu, nastavené procesy atp., máme definovánu strategii pro logování a vyhodnocování logů a logujeme a vyhodnocujeme primárně kritická aktiva, pro méně kritická aktiva využíváme rozdílné retence, navazující odlišné doby reakce atp. Umíme efektivně pracovat s IOCs a nasazené nástroje nám reálně pomáhají s investigací incidentů …**
Respond	• Proces na zvládání incidentů máme opsaný z vyhlášky, pro incidenty máme speciální workflow v ticketovacím systému, ale vlastně žádné incidenty nemáme. Když ano, tak je pro nás priorita incident nahlásit na NÚKIB a uvidíme, co nám poradí. Proces testujeme jen formálně.	• Máme definovaný a pravidelně testovaný a aktualizovaný proces pro řešení incidentů. Incidenty jsou zakládány i na základě kritických alertů ze security nástrojů. Testujeme celý proces i prakticky.
Recover	• BCP, DRP a plán zálohování je spíše formální a obecné, pravidelně děláme table-top testování.	• BCP, DRP a backup plány odpovídají realitě a jsou definované pro regulovanou službu a podnikové kritické procesy a to tak, že podle nich může postupovat relativně kdokoliv, kdo zná daný proces/technologii. Procesy testujeme a aktualizujeme.

Jak začít?

1. Pokud si nejste jisti s dopadem regulace na Vaši firmu, hledejte nejprve právní pomoc.
2. Zmapujte si současný stav plnění bezpečnostních opatření. Nedělejte gap analýzu, pokud to není nutné (jste li na zelené louce, hledejte rovnou podporu v zajišťování shody).
3. Identifikujte si všechna primární aktiva a s ohledem na regulované služby vymezte rozsah.
4. Zmapujte si detailně rozsah (primární a podpůrná aktiva, vazby, důležitost pro business).
5. Průběžně bezpečnost komunikujte dovnitř businessu (vedení, garanti aktiv, zaměstnanci,...).
6. Začněte provádět analýzy rizik - zvolte takovou metodu a takové informace, které Vám pomohou se o bezpečnosti rozhodovat, ne metodu, která Vám pomůže tak akorát vyplnit excelovou tabulku.
7. Nesoustřeďujte se jen na papíry ale na skutečnou bezpečnost. Rozhodně nedělejte to, že nejprve píšete (nebo si necháte napsat) směrnice a poté aplikujete do praxe.
8. Při aplikaci bezpečnostních opatření vnímejte kontext a zohledňujte rizika.
9. Sestavte si přehled současných a chybějících bezpečnostních opatření (bezpečnostních procesů a nástrojů) potřebných k ošetření rizik.
10. Hledejte a nasaďte vhodné chybějící nástroje (RfP, PoC, rozhodnutí, implementace, integrace, ladění).
11. **Usilujte o security by default / by design => Nestavějte kybernetickou bezpečnost jako něco, co je vedle Vašeho primárního businessu, nýbrž jako jeho součást!**
12. Metriky, metriky, metriky - neustále vyhodnocujte účinnost toho, co děláte - měření, skenování, testování (např. penetrační testy).
13. Testujte své schopnosti a zlepšujte se.
14. ...

1. Zkuste změnit mindset - zajišťujte kybernetickou bezpečnost pro sebe, ne pro regulátora, bude to možná 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. 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.
5. Žádná bezpečnostní technologie nebude dost bezpečná, pokud s ní v čase nemíníme neustále pracovat!
6. Všeho moc škodí - nesnažte se zbytečně o nasazení velkého množství bezpečnostních nástrojů, to není správná metrika vypovídající o Vaší bezpečnosti, začněte od naprosto základních bezpečnostních doporučení (pro správce, pro vrcholné vedení, pro zaměstnance), “zkroťte své současné bezpečnostní nástroje a zlepšujte se/je.
7. Přistupujte k zajišťování kybernetické bezpečnosti smysluplně!
8. ...

Newsletter

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

newsletter.guardians.cz

GUARDIANS CZ

nZKB kurz

A pokud byste chtěli jít hlouběji do problematiky, tak mám pro vás jedinečnou možnost využít tento promo kód na 30% slevu a registrovat se do 4-měsíčního nZKB kurzu!

Promo kód pro účastníky konference:

MANPOWERIT-2024

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

GUARDIANS CZ

nZKB webinář na míru

Na 10.12. jsem si pro vás připravil unikátní webinář, který se liší od běžných webinářů tím, že vy sami máte možnost ovlivnit jeho obsah! Během 90 minut se zaměříme na klíčová témata, která vás nejvíce zajímají – konkrétně ta, která uvedete při registraci.

https://www.guardians.cz/unikatni-webinar-nzkb-nis2

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