Jak NIS2 dopadá na poskytovatele digitálních služeb

Webinář | 29. 5. 2025

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

GUARDIANS.cz

Představení GUARDIANS.cz a 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

Agenda.exe

- Úvod - právní souvislosti
  - Regulované služby
  - Specifika pro digitální služby
- Časová osa
- Povinnosti
  - Požadavky podle nařízení EU k NIS2
  - Zaměření na některé z požadavků + příspěvek hosta
- Přímý a nepřímý dopad
- Výzvy a příležitosti pro digi služby
- Závěr
- Otázky a odpovědi

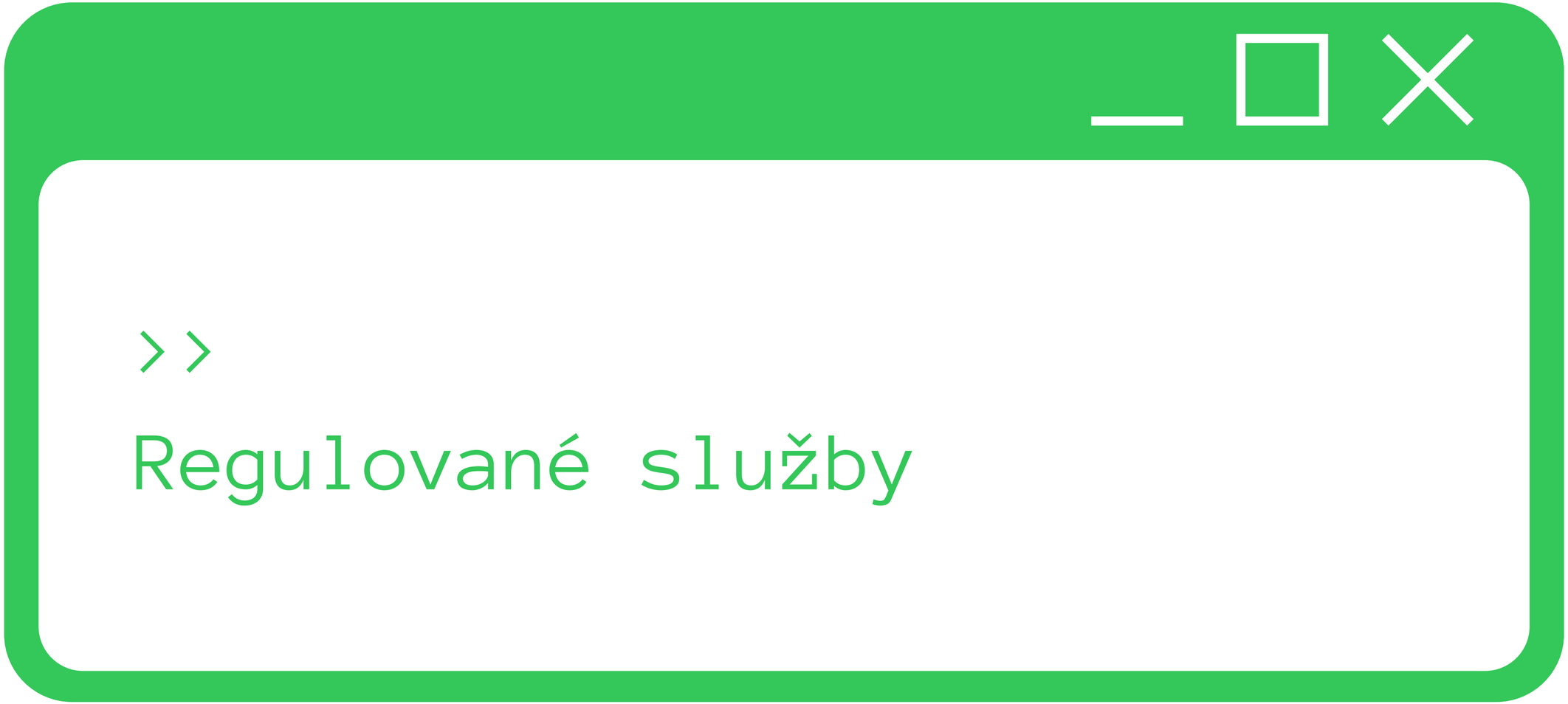
Vnímejte prosím informace v této prezentaci tak, že jde o názor autora, na základě jeho zkušeností a zkušeností Guardians.cz týmu. Neberte tyto informace však jako dogma - možných přístupů a řešení je samozřejmě více. Zároveň prosím vnímejte, že národní předpisy zatím v ČR nebyly schváleny. Schválen je nyní jen akt EU k NIS2 pro digitální služby.

Newsletter

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

newsletter.guardians.cz

GUARDIANS CZ


>>
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

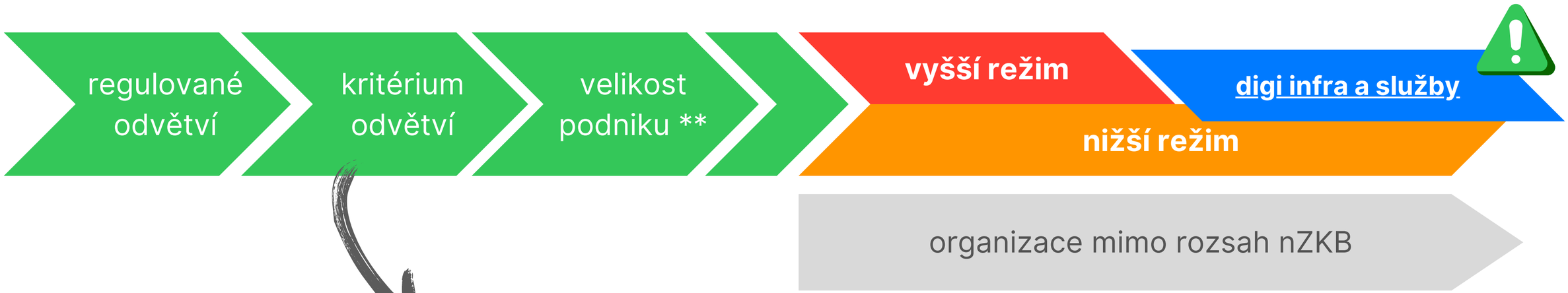
strategicky významné služby

bezpečnost dodavatelského řetězce, ...

Povinnosti pro vybrané digitální služby podle nařízení EU k NIS2

nižší režim

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

Proč je dnešní webinář věnován jen digitálním službám?

Co říká nZKB - § 13

Bezpečnostní opatření

(1) Bezpečnostními opatřeními jsou organizační a technická opatření, jejichž účelem je zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv.

(2) Poskytovatel regulované služby je povinen v rámci stanoveného rozsahu zavádět a provádět bezpečnostní opatření podle § 14 v míře nezbytné pro zajištění kybernetické bezpečnosti regulované služby.

(3) Obsah bezpečnostních opatření a způsob jejich zavádění a provádění stanoví Úřad vyhláškou.

...

Zdroj: nZKB - Senátní tisk č. 109

Co říká nZKB - § 18

→ SPECIFIKA PRO UVEDENÉ DIGI SL.

→ PROVÁDĚCÍ PŘEDPIS PRO DIGI

Zvláštní ustanovení o povinnostech poskytovatelů regulovaných služeb v odvětví digitální infrastruktury a služeb

(1) ***Poskytovatel*** *regulované služby, který je poskytovatelem regulované služby* ***systému překladu doménových jmen***, ***služby vytvářející důvěru*** *podle přímo použitelného předpisu EU, služby* ***správy a provozu registru domény nejvyšší úrovně***, *služby* ***cloud computingu***, *služby* ***datového centra***, *služby* ***sítě pro doručování obsahu***, *služby* ***on-line tržiště***, *služby* ***internetového vyhledávače*** *podle přímo použitelného předpisu EU, služby* ***platformy sociální sítě***, ***řízené služby*** *nebo* ***řízené bezpečnostní služby***, *je ve vztahu k těmto regulovaným službám* ***povinen v rámci stanoveného rozsahu zavádět a provádět vhodná a přiměřená bezpečnostní opatření zahrnující alespoň řízení rizik, řízení bezpečnostní politiky a bezpečnostní dokumentace, zvládání kybernetických bezpečnostních incidentů, řízení kontinuity činností, řízení dodavatelů, bezpečnou akvizici, vývoj a údržbu, aplikační bezpečnost, bezpečnost lidských zdrojů, kryptografické algoritmy, řízení přístupu a správu a ověřování identit***, *a to v míře a způsobem* ***stanoveným prováděcím předpisem Evropské komise, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2022/2555 (dále jen „prováděcí předpis Komise“), pokud jde o technické a metodické požadavky opatření, která jsou uvedení poskytovatelé regulovaných služeb povinni přijímat***;

§ 13 odst. 2 se ve vztahu k těmto regulovaným službám nepoužije.

...

Zdroj: nZKB - Senátní tisk č. 109

Co říká nZKB - § 18

→ INCIDENTY

→ REPORTING STEJNÝ

Zvláštní ustanovení o povinnostech poskytovatelů regulovaných služeb v odvětví digitální infrastruktury a služeb

...

(2) Poskytovatel regulované služby, který je poskytovatelem regulované služby uvedené v odstavci 1, s výjimkou služby vytvářející důvěru podle přímo použitelného předpisu Evropské unie, je ve vztahu k této regulované službě povinen v rámci stanoveného rozsahu ***hlásit všechny kybernetické bezpečnostní incidenty s významným dopadem na poskytování regulované služby****;*

§ 15 odst. 1 a 2 se ve věci vymezení incidentů, které je potřeba hlásit, ve vztahu k této regulované službě nepoužijí*.*

Způsob stanovení významnosti dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby stanoví prováděcí předpis Komise*. Ve věci způsobu hlášení kybernetických bezpečnostních incidentů* ***se uplatní obecná úprava v § 15 a 16, pokud prováděcí předpis Komise nestanoví zvláštní postup****.*

...

Zdroj: nZKB - Senátní tisk č. 109

GUARDIANS CZ

Co říká nZKB - § 18

→ HLAVNÍ PROVOZOVNY

→ ROZHODNUTÍ, OOP

Zvláštní ustanovení o povinnostech poskytovatelů regulovaných služeb v odvětví digitální infrastruktury a služeb

...

(3) ***Poskytovatel*** *regulované služby, který je poskytovatelem regulované služby uvedené v odstavci 1, s výjimkou služby vytvářející důvěru podle přímo použitelného předpisu EU, a* ***který má umístěnu hlavní provozovnu v jiném členském státě EU nebo ve smluvním státě Dohody o Evropském hospodářském prostoru*** *(dále jen „jiný členský stát“)* ***nebo má v jiném členském státě ustanoveného zástupce, je povinen ve vztahu k této regulované službě plnit povinnosti stanovené tímto zákonem pouze v rozsahu odstavce 1****.* ***Povinnosti uložené rozhodnutím nebo opatřením obecné povahy Úřadu na základě tohoto zákona jsou pro poskytovatele regulované služby podle věty první závazné pouze v případě, že tak Úřad v rozhodnutí nebo opatření obecné povahy výslovně stanoví.***

(4) Poskytovatel regulované služby uvedené v odstavci 1, který je v režimu vyšších povinností, je povinen řídit se ustanoveními prováděcího předpisu Komise podle odstavců 1 a 2 platnými pro osoby zařazené do kategorie základních subjektů. Poskytovatel regulované služby uvedené v odstavci 1, který je v režimu nižších povinností, je povinen řídit se ustanoveními prováděcího předpisu Komise podle odstavců 1 a 2 platnými pro osoby zařazené do kategorie důležitých subjektů.

...

Zdroj: nZKB - Senátní tisk č. 109

GUARDIANS CZ

Co říká nZKB - § 18

→ OSTATNÍ DIGI SL. DLE NÁRODNÍCH PŘEDPISŮ

Zvláštní ustanovení o povinnostech poskytovatelů regulovaných služeb v odvětví digitální infrastruktury a služeb

...

(5) Plnění povinností poskytovatele regulované služby uvedené v odstavci 1 vůči regulovaným službám neuvedeným v odstavci 1 není použitím tohoto ustanovení dotčeno.

Zdroj: nZKB - Senátní tisk č. 109

Co říká Vyhláška o regulovaných službách?

Pozor: Vyhláška je nyní v MPŘ, tedy může se ještě měnit!

Služba	Podmínky významnosti poskytovatele regulované služby a jeho režim
16.1 Poskytování veřejně dostupné služby elektronických komunikací podle ZoEK	Osoba poskytující veřejně dostupnou službu elektronických komunikací podle zákona o elektronických komunikacích je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že a) je velkým nebo středním podnikem, b) je poskytovatelem veřejně dostupné služby elektronických komunikací skrze nejméně 350 000 aktivních mobilních SIM karet na území České republiky, nebo c) je poskytovatelem nejméně 100 000 aktivních pevných internetových přípojek na území České republiky, nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je malým podnikem, nebo mikropodnikem podle doporučení Komise 2003/361/ES o definici mikropodniků a malých a středních podniků).
16.2 Zajišťování veřejné komunikační sítě podle ZoEK	Osoba zajišťující veřejnou komunikační síť podle zákona o elektronických komunikacích je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že je a) velkým nebo středním podnikem, b) poskytovatelem veřejně dostupné služby elektronických komunikací skrze nejméně 350 000 aktivních mobilních SIM karet na území České republiky, nebo c) poskytovatelem nejméně 100 000 aktivních pevných internetových přípojek na území České republiky, nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je malým podnikem, nebo mikropodnikem.
16.3 Poskytování služby výměnného uzlu internetu	Poskytovatel služby výměnného uzlu internetu je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že a) je velkým podnikem, nebo b) umožňuje propojení nejméně 100 nezávislých sítí s datovým tokem alespoň 1 Tbps, nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je středním podnikem.
16.4 Poskytování služby systému překladu doménových jmen s výjimkou služby poskytované jako součást 16.1	Poskytovatel služeb systému překladu doménových jmen, s výjimkou poskytovatele, který tuto službu poskytuje jako součást regulované služby podle bodu 16.1, je poskytovatelem regulované služby v režimu vyšších povinností v případě, že a) aktivně poskytuje veřejně dostupné služby pro rekurzivní překlad doménových jmen koncovým uživatelům internetu, nebo b) poskytuje služby pro autoritativní překlad doménových jmen pro použití třetí stranou pro více než 10 000 domén druhého řádu.
16.5 Poskytování služby registrace a správy doménových jmen	Osoba poskytující služby registrace doménových jmen s přístupem k Centrálnímu registru doménových jmen pro více než 100 000 doménových jmen druhého řádu v doméně .cz, je poskytovatelem regulované služby v režimu nižších povinností.
16.6 Správa a provoz registru domény nejvyšší úrovně	Osoba spravující a provozující registr domény nejvyšší úrovně je poskytovatelem regulované služby v režimu vyšších povinností.
16.7 Správa a provoz domény gov.cz	Osoba spravující a provozující doménu gov.cz je poskytovatelem regulované služby v režimu vyšších povinností.

Zdroj: Vyhláška k nZKB o regulovaných službách - oficiální podklady v MPŘ

Co říká Vyhláška o regulovaných službách?

Pozor: Vyhláška je nyní v MPŘ, tedy může se ještě měnit!

Služba	Podmínky významnosti poskytovatele regulované služby a jeho režim
16.8 Poskytování služby cloud computingu	Poskytovatel služby cloud computingu je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že je a) velkým podnikem, nebo b) poskytovatelem státního cloud computingu podle zákona o informačních systémech veřejné správy), nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je středním podnikem.
16.9 Poskytování služby datového centra	Poskytovatel služby datového centra, s výjimkou poskytovatele, který tuto službu poskytuje jako součást regulované služby podle bodu 16.8, je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že je velkým podnikem, nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je středním podnikem.
16.10 Poskytování služby sítě pro doručování obsahu (CDN)	Poskytovatel služby sítě pro doručování obsahu (CDN) je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že je velkým podnikem, nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je středním podnikem.
16.11 Správa kvalifikovaného systému elektronické identifikace podle zákona o elektronické identifikaci	Kvalifikovaný správce systému elektronické identifikace podle zákona o elektronické identifikaci je poskytovatelem regulované služby v režimu vyšších povinností.
16.12 Poskytování služby vytvářející důvěru podle přímo použitelného předpisu EU	Poskytovatel služby vytvářející důvěru podle přímo použitelného předpisu Evropské unie) je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že je a) kvalifikovaným poskytovatelem služby vytvářející důvěru, nebo b) nekvalifikovaným poskytovatelem služby vytvářející důvěru a zároveň velkým podnikem, nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je nekvalifikovaným poskytovatelem a zároveň středním podnikem, malým podnikem, nebo mikropodnikem.
16.13 Poskytování řízené služby s výjimkou služby uvedené v bodu 16.14	Poskytovatel řízené služby, s výjimkou služby uvedené v bodu 16.14, poskytující tuto službu zákazníkům, kteří nejsou spotřebiteli **(jen B2B)** je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že je velkým podnikem, nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je středním podnikem.
16.14 Poskytování řízené bezpečnostní služby	Poskytovatel řízené bezpečnostní služby poskytující tuto službu zákazníkům, kteří nejsou spotřebiteli **(jen B2B)** je I. poskytovatelem regulované služby v režimu vyšších povinností v případě, že je velkým podnikem, nebo II. poskytovatelem regulované služby v režimu nižších povinností v případě, že je středním podnikem.

Zdroj: Vyhláška k nZKB o regulovaných službách - oficiální podklady v MPŘ

Co říká Vyhláška o regulovaných službách?

Pozor: Vyhláška je nyní v MPŘ, tedy může se ještě měnit!

Služba	Podmínky významnosti poskytovatele regulované služby a jeho režim
16.15 Poskytování služby on-line tržiště podle zákona upravujícího ochranu spotřebitele)	Poskytovatel služby on-line tržiště podle zákona upravujícího ochranu spotřebitele je poskytovatelem regulované služby v režimu nižších povinností v případě, že je velkým nebo středním podnikem.
16.16 Poskytování služby internetového vyhledávače podle přímo použitelného právního předpisu Evropské unie)	Poskytovatel služby internetového vyhledávače podle přímo použitelného právního předpisu Evropské unie) je poskytovatelem regulované služby v režimu nižších povinností v případě, že je velkým nebo středním podnikem.
16.17 Poskytování platformy sociální sítě	Poskytovatel platformy sociální sítě je poskytovatelem regulované služby v režimu nižších povinností v případě, že je velkým nebo středním podnikem.
16.18 Provozování Národního CERT	Provozovatel Národního CERT je poskytovatelem regulované služby v režimu vyšších povinností.

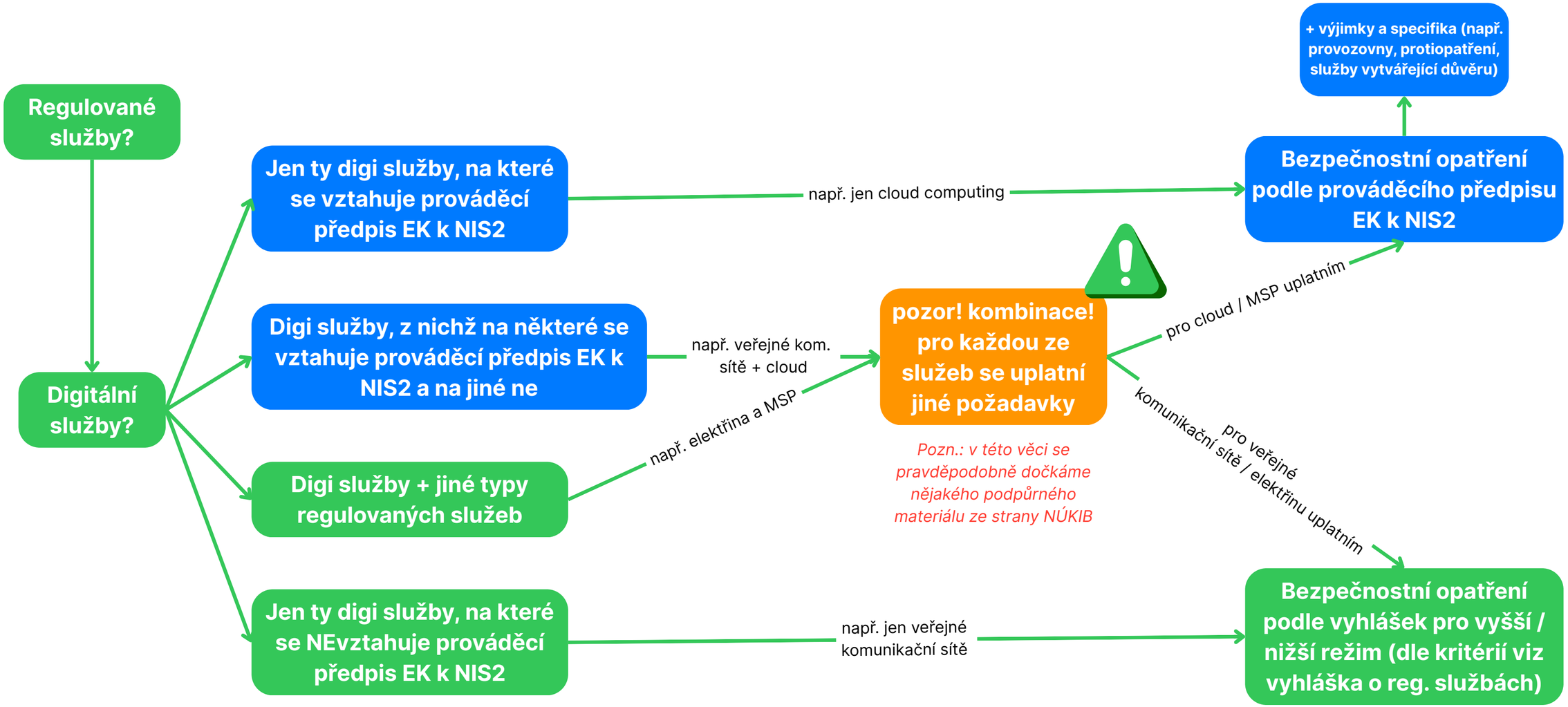
Zdroj: Vyhláška k nZKB o regulovaných službách - oficiální podklady v MPŘ

aby se v tom vyznal...
aneb jak tedy NIS2 dopadá na poskytovatele digi služeb?

služby	režim regulace podle nZKB	bezpečnostní opatření podle	další specifika
veřejně dostupné služby elektronických komunikací	mikropodniky + malé podniky - nižší povinnosti ostatní vyšší povinnosti	vyhláška k nZKB pro daný režim	N/A
veřejné komunikační sítě	mikropodniky + malé podniky - nižší povinnosti ostatní vyšší povinnosti		
služby výměnného uzlu internetu	vyšší povinnosti		
poskytování služby registrace a správy doménových jmen	max. nižší režim		
správa a provoz domény gov.cz	vyšší povinnosti		
Správa kvalifikovaného systému elektronické identifikace podle zákona o elektronické identifikaci	vyšší povinnosti		
DNS	N/A	**Evropské nařízení pro digitální služby K NIS2**	Evropské nařízení pro digitální služby dále upřesňuje případy, v nichž se kyberbezpečnostní incident považuje za významný (pozor! vyjma poskytovatelů služeb vytvářejících důvěru)
registry domén nejvyšší úrovně			
poskytovatelé služeb cloud computingu			
poskytovatelé služeb datových center			
poskytovatelé sítí pro doručování obsahu (CDN)			
poskytovatelé řízených služeb (MSP)			
poskytovatelé řízených bezpečnostních služeb (MSSP)			
poskytovatelé on-line tržišť			
poskytovatelé internetových vyhledávačů a služeb platforem sociálních sítí			
poskytovatelé služeb vytvářejících důvěru			

GUARDIANS CZ

Co z toho všeho plyne?



GUARDIANS CZ

U vybraných digitálních služeb nyní čekáme jen na nZKB a vyhlášku o regulovaných službách.

Bezpečnostní opatření jsou dána prováděcím předpisem EU.

>>

Časová osa

Časová osa pohledem organizací, na které nový kybernetický zákon dopadne

čas

1. **účinnost nového zákona o kybernetické bezpečnosti** [ČR] - sledujte oficiální zdroje, např. https://portal.nukib.gov.cz/.
2. ohlášení regulované služby (“samoidentifikace”) **[povinný subjekt]** - nejpozději do 60 dní od bodu 1.
3. rozhodnutí o registraci [NÚKIB] - cca do 30 dní od bodu 2.
4. hlášení kontaktních údajů **[povinný subjekt]** - nejpozději do 30 dní od bodu 3.
5. povinnost hlásit bezpečnostní incidenty a mít zavedená bezpečnostní opatření **[povinný subjekt]** - nejpozději do 1 roku od bodu 3.


>>
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** (Pozor na případná specifika pro digi. sl. | historicky např. varování vůči některým technologiím z Číny, opatření k zabezpečení emailové infrastruktury atp.).
- U omezeného rozsahu regulovaných subjektů také (v závislosti na předpisu vydaném Vládou ČR):
  - Zabezpečení dostupnosti strategicky významné služby (SVS).
  - Aplikace požadavků plynoucích z tzv. Mechanismu prověřování bezpečnosti dodavatelského řetězce.

Katalog povinností | **Bezpečnostní opatření a nástroje** - Vyšší režim / zjednodušeně nižší režim

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, screening
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, integrace dat (bezpečnostní nástroje, existující systémy atp.)
Řízení rizik		GRC, RM tool, metriky, BCMS (z hlediska návaznosti)
Řízení dodavatelů		GRC, SCM nástroje / TPRM, právní služby, CTI, zákaznické audity, screening
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, automatizace/integrace, zákaznické audity, důkazy a metriky

Katalog povinností | Bezpečnostní opatření podle nařízení EU k NIS2 pro digitální infrastrukturu a služby

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 (background-check)**, 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 Zdroj: Prováděcí předpis Komise pro digitální služby - Oficiální znění (EUR LEX)

GUARDIANS CZ

Náhled do nařízení EU k NIS2 pro digitální infrastrukturu a služby

Zdroj: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=OJ:L_202402690

>>

Vybrané pasáže z nařízení EU k NIS2 pro digitální infrastrukturu a služby

Významnosti incidentů

Článek 3 - Významné incidenty

1. Incident se považuje za významný pro účely čl. 23 odst. 3 směrnice (EU) 2022/2555, pokud jde o příslušné subjekty, je-li splněno jedno nebo více z těchto kritérií:

- *a) incident způsobil nebo může způsobit příslušnému subjektu přímou finanční ztrátu, která přesahuje 500 000 EUR nebo 5 % celkového ročního obratu příslušného subjektu za předchozí účetní období, podle toho, která částka je nižší;*
- *b) incident způsobil nebo může způsobit únik obchodního tajemství příslušného subjektu podle čl. 2 bodu 1 směrnice (EU) 2016/943;*
- *c) incident způsobil nebo může způsobit úmrtí fyzické osoby;*
- *d) incident způsobil nebo může způsobit značnou újmu na zdraví fyzické osoby;*
- *e) došlo k úspěšnému podezřelému zlovolnému a neoprávněnému přístupu do sítě a informačních systémů, který může způsobit vážné narušení provozu;*
- *f) incident splňuje kritéria stanovená v článku 4; [viz následující slajd]*
- *g) incident splňuje jedno nebo více kritérií uvedených v článcích 5 až 14. [viz další slajdy]*

2. Za významné incidenty se nepovažují plánovaná přerušení provozu a plánované důsledky plánovaných operací údržby prováděných příslušnými subjekty nebo jejich jménem.

3. Při stanovení počtu uživatelů dotčených incidentem pro účely článku 7 a článků 9 až 14 příslušné subjekty zohlední všechny tyto položky:

- *a) počet zákazníků, kteří mají s příslušným subjektem uzavřenou smlouvu, která jim umožňuje přístup k síti a informačním systémům příslušného subjektu nebo ke službám, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné;*
- *b) počet fyzických a právnických osob spojených s podnikovými zákazníky, kteří využívají sítě a informační systémy subjektů nebo služby, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné.*

Zdroj: Prováděcí předpis Komise pro digitální služby - Oficiální znění (EUR LEX)

Významnosti incidentů

Článek 4 - Opakující se incidenty

Incidenty, které nejsou jednotlivě považovány za významný incident ve smyslu článku 3, se považují společně za jeden významný incident, pokud splňují ***všechna tato kritéria****:*

- *a) došlo k nim nejméně dvakrát během šesti měsíců;*
- *b) mají stejnou příčinu;*
- *c) společně splňují kritéria stanovená v čl. 3 odst. 1 písm. a).*

Zdroj: Prováděcí předpis Komise pro digitální služby - Oficiální znění (EUR LEX)

Významnosti incidentů

služby	kriteria význ. incidentu
DNS	a) rekurzivní nebo autoritativní služba pro překlad doménových jmen je zcela **nedostupná po dobu delší než 30 minut**; b) **průměrná doba odezvy** rekurzivní nebo autoritativní služby pro překlad doménových jmen na požadavky DNS **je déle než jednu hodinu delší než 10 sekund**; c) je **narušena integrita, důvěrnost nebo autenticita** uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním služby DNS, s výjimkou případů, kdy z důvodu chybné konfigurace nejsou správné údaje méně než 1 000 doménových jmen spravovaných provozovatelem DNS, které představují nejvýše 1 % doménových jmen spravovaných provozovatelem DNS.
registry domén nejvyšší úrovně	a) autoritativní služba pro překlad doménových jmen je **zcela nedostupná**; b) **průměrná doba odezvy** autoritativní služby pro překlad doménových jmen na požadavky DNS **je déle než jednu hodinu delší než 10 sekund**; c) je **narušena integrita, důvěrnost nebo autenticita** uchovávaných, předávaných nebo zpracovávaných dat souvisejících s doménou nejvyšší úrovně.
poskytovatelé služeb cloud computingu	a) služba cloud computingu je zcela **nedostupná po dobu delší než 30 minut**; b) **déle než jednu hodinu je omezena dostupnost služby** cloud computingu poskytovatele pro více než 5 % uživatelů dané služby cloud computingu v Unii nebo pro více než 1 milion uživatelů dané služby cloud computingu v Unii, podle toho, který počet je nižší; c) v důsledku podezřelého zlovolného jednání je **narušena integrita, důvěrnost nebo autenticita** uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním služeb cloud comp.; d) **je narušena integrita, důvěrnost nebo autenticita** uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním služby cloud computingu a toto narušení má dopad na více než 5 % uživatelů dané služby cloud computingu v Unii nebo na více než 1 milion uživatelů dané služby cloud computingu v Unii, podle toho, který počet je nižší.
poskytovatelé služeb datových center	a) služba datového centra provozovaného poskytovatelem je **zcela nedostupná**; b) **dostupnost** služby datového centra provozovaného poskytovatelem je **déle než jednu hodinu omezena**; c) v důsledku podezřelého zlovolného jednání je **narušena integrita, důvěrnost nebo autenticita** uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním služby datového centra; d) je **ohrožen fyzický přístup k datovému centru** provozovanému poskytovatelem.
poskytovatelé sítí pro doručování obsahu (CDN)	a) síť pro doručování obsahu je zcela **nedostupná po dobu delší než 30 minut**; b) **déle než jednu hodinu je omezena dostupnost** sítě pro doručování obsahu poskytovatele **pro více než 5 % uživatelů** dané sítě pro doručování obsahu v Unii **nebo pro více než 1 milion uživatelů** dané sítě pro doručování obsahu v Unii, podle toho, který počet je nižší; c) v důsledku podezřelého zlovolného jednání je **narušena integrita, důvěrnost nebo autenticita** uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním sítě pro doručování obsahu; d) je **narušena integrita, důvěrnost nebo autenticita** uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním sítě pro doručování obsahu a toto narušení má dopad na více než 5 % uživatelů dané sítě pro doručování obsahu v Unii nebo na více než 1 milion uživatelů dané sítě pro doručování obsahu v Unii, podle toho, který počet je nižší.

Zdroj: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=OJ:L_202402690

Významnosti incidentů

služby	kriteria význ. incidentu
MSP **MSSP**	a) MSP/MSSP je **zcela nedostupná po dobu delší než 30 minut**; b) **déle než jednu hodinu je omezena dostupnost** MSP/MSSP **pro více než 5 % uživatelů** dané služby v Unii nebo **pro více než 1 milion uživatelů** dané služby v Unii, podle toho, který počet je nižší; c) v důsledku podezřelého zlovolného jednání je **narušena integrita, důvěrnost nebo autenticita** uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním MSP/MSSP; d) je narušena integrita, důvěrnost nebo autenticita uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním MSP/MSSP a toto narušení má dopad na více než 5 % uživatelů dané MSP/MSSP v Unii nebo na více než 1 milion uživatelů dané služby v Unii, podle toho, který počet je nižší.
poskytovatelé on-line tržišť	a) on-line tržiště je **zcela nedostupné pro více než 5 % uživatelů** on-line tržiště v Unii **nebo pro více než 1 milion uživatelů** on-line tržiště v Unii, podle toho, který počet je nižší; b) **omezenou dostupností** on-line tržiště je dotčeno **více než 5 % uživatelů** on-line tržiště v Unii **nebo více než 1 milion uživatelů** on-line tržiště v Unii, podle toho, který počet je nižší; c) v důsledku podezřelého zlovolného jednání je **narušena integrita, důvěrnost nebo autenticita** uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním on-line tržiště; d) je **narušena integrita, důvěrnost nebo autenticita** uchovávaných, předávaných nebo zpracovávaných údajů souvisejících s poskytováním on-line tržiště **a toto narušení má dopad na více než 5 % uživatelů** daného on-line tržiště v Unii **nebo na více než 1 milion uživatelů** daného on-line tržiště v Unii, podle toho, který počet je nižší.
poskytovatelé internetových vyhledávačů	a) internetový vyhledávač je **zcela nedostupný pro více než 5 % uživatelů** daného internetového vyhledávače v Unii **nebo pro více než 1 milion uživatelů** daného internetového vyhledávače v Unii, podle toho, který počet je nižší; b) **omezenou dostupností** internetového vyhledávače je dotčeno více než 5 % uživatelů internetového vyhledávače v Unii nebo více než 1 milion uživatelů daného internetového vyhledávače v Unii, podle toho, který počet je nižší; c) v důsledku podezřelého zlovolného jednání je **narušena integrita, důvěrnost nebo autenticita** uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním internetového vyhledávače; d) je narušena integrita, důvěrnost nebo autenticita uchovávaných, předávaných nebo zpracovávaných údajů souvisejících s poskytováním internetového vyhledávače a toto narušení má **dopad na více než 5 % uživatelů** daného internetového vyhledávače v Unii nebo na **více než 1 milion uživatelů** daného internetového vyhledávače v Unii, podle toho, který počet je nižší.
poskytovatelé služeb platforem sociálních sítí	a) platforma sociální sítě je **zcela nedostupná pro více než 5 % uživatelů dané platformy** sociálních sítích v Unii **nebo pro více než 1 milion uživatelů platformy** sociálních sítí v Unii, podle toho, které číslo je nižší; b) **omezenou dostupností platformy** sociálních sítí je **dotčeno více než 5 % uživatelů** platformy sociálních sítí v Unii **nebo více než 1 milion uživatelů** dané platformy sociálních sítí v Unii, podle toho, který počet je nižší; c) v důsledku podezřelého zlovolného jednání je narušena **integrita, důvěrnost nebo autenticita** uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním platformy sociálních sítí; d) je narušena integrita, důvěrnost nebo autenticita uchovávaných, předávaných nebo zpracovávaných údajů souvisejících s poskytováním platformy sociálních sítí a toto narušení má dopad na více než 5 % uživatelů dané platformy sociálních sítí v Unii nebo na více než 1 milion uživatelů dané platformy sociálních sítí v Unii, podle toho, který počet je nižší.
poskytovatelé služeb vytvářejících důvěru	a) služba je **zcela nedostupná po dobu delší než 20 minut**; b) služba je **pro uživatele nebo spoléhající se strany nedostupná déle než jednu hodinu, počítanou na základě kalendářního týdne**; c) **omezenou dostupností služby** je dotčeno více než 1 % uživatelů nebo spoléhajících se stran v Unii nebo více než 200 000 uživatelů nebo spoléhajících se stran v Unii, podle toho, který počet je nižší; d) je **narušen fyzický přístup** do oblasti, kde jsou umístěny sítě a informační systémy a kam mají přístup pouze důvěryhodní pracovníci poskytovatele služby, nebo je narušena ochrana takového fyzického přístupu; e) je **narušena integrita, důvěrnost nebo autenticita** uchovávaných, předávaných nebo zpracovávaných dat souvisejících s poskytováním služby vytvářející důvěru a toto narušení má dopad na více než 0,1 % uživatelů dané služby vytvářející důvěru nebo spoléhajících se stran v Unii nebo na více než 100 uživatelů dané služby vytvářející důvěru nebo spoléhajících se stran v Unii, podle toho, který počet je nižší.

GUARDIANS CZ

Zdroj: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=OJ:L_202402690

Významnosti incidentů - shrnutí

- Požadavky na významnost incidentů v zásadě pojmou vše s ohledem na narušení “integrity, důvěrnosti nebo autenticity”, samozřejmě s určitou přiměřeností
  - **Ale pak jsou tu další kritéria, která tu přiměřenost specifikují - např. doby nedostupnosti služby, opakované nevýznamné incidenty atp., kdy je jasně dané, co se musí hlásit regulátorovi!!!!**

Zdroj: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=OJ:L_202402690

Compliance mapování

ISO 27k, EU akt k NIS2 pro digi. sl., nZKB - vyšší režim,... → relativně shodné požadavky, které ale mají odlišnou terminologii → proto mapování

nové požadavky (to, co již ve firmě mám mapuji na nové požadavky) — *mapované požadavky (vyhláška nZKB - vyšší režim) (pozn.: může být i ISO 27k a jiné - co již firma má)*

Podkategorie	tagy	Požadavek 1. úroveň	Požadavek 2. úroveň	Poznámka	Stav (nezdě...	ext_opatreni_vyssi	ext-stav...	ext-opatreni-vyssi-1uroven	ext-opatreni-vyssi-2uroven
6.4. Řízení změn, opravy a údržba	changes	6.4.3. V případě, že nebylo možné dodržet standardní postupy řízení změn z důvodu mimořádné události, příslušné subjekty zdokumentují výsledek změny a vysvětlení, proč nebylo možné postupy dodržet.				§4, odst. 1, k	shoda	Povinná osoba v rámci systému řízení bezpečnosti informací	stanoví proces řízení výjimek z pravidel stanovených podle p
6.4. Řízení změn, opravy a údržba	changes	6.4.4. Příslušné subjekty postupy přezkoumávají a v případě potřeby aktualizují v plánovaných intervalech a při významných incidentech nebo významných změnách operací či rizik.				§4, odst. 1, f7 §4, odst. 2, c1	částečně pl... neshoda	Povinná osoba v rámci systému řízení bezpečnosti informací Povinná osoba v případě neplnění povinnosti řízení rizik podle odstavce 1 písm. c)	zajistí vyhodnocení účinnosti systému řízení bezpečnosti infc obsahuje zohlední v plánu zvládání rizik
6.5. Testování bezpečnosti	audit appsec	6.5.1. Příslušné subjekty stanoví, zavedou a uplatňují politiku a postupy pro testování bezpečnosti.				§ 25, odst.4 § 25, odst.4 § 25, odst.6 § 25, odst.6 § 25, odst.6	shoda shoda shoda shoda shoda	Povinná osoba provádí pravidelné skenování zranitelnosti technických aktiv regulované služby Povinná osoba provádí pravidelné skenování zranitelnosti technických aktiv regulované služby Povinná osoba provádí penetrační testování technických aktiv s ohledem na hodnocení těchto aktiv a hodnocení rizik Povinná osoba provádí penetrační testování technických aktiv s ohledem na hodnocení těchto aktiv a hodnocení rizik Povinná osoba provádí penetrační testování technických aktiv s ohledem na hodnocení těchto aktiv a hodnocení rizik	z interní a externí komunikační sítě a alespoň jednou ročně. z interní a externí komunikační sítě, před jejich uvedením do provozu a v souvislosti s významnou změnou podle § 12 odst. 3.
6.5. Testování bezpečnosti	audit appsec	6.5.2. Příslušné subjekty:	a) na základě posouzení rizik provedeného podle bodu 2.1 stanoví potřebu, rozsah, četnost a typ bezpečnostních testů;		NEshoda				
6.5. Testování bezpečnosti	ISMS audit risk appsec	6.5.2. Příslušné subjekty:	b) provádějí bezpečnostní testy podle zdokumentované metodiky testování, která se vztahuje na složky identifikované v analýze rizik jako důležité pro bezpečný provoz;		NEshoda				
6.5. Testování bezpečnosti	audit appsec	6.5.2. Příslušné subjekty:	c) dokumentují typ, rozsah, čas a výsledky testů, včetně posouzení kritičnosti a zmírňujících opatření pro každé zjištění;		Shoda				

pokud není zděděno (tedy promapováno)

Více v newsletteru: Compliance mapování, konsolidace auditů a analýz

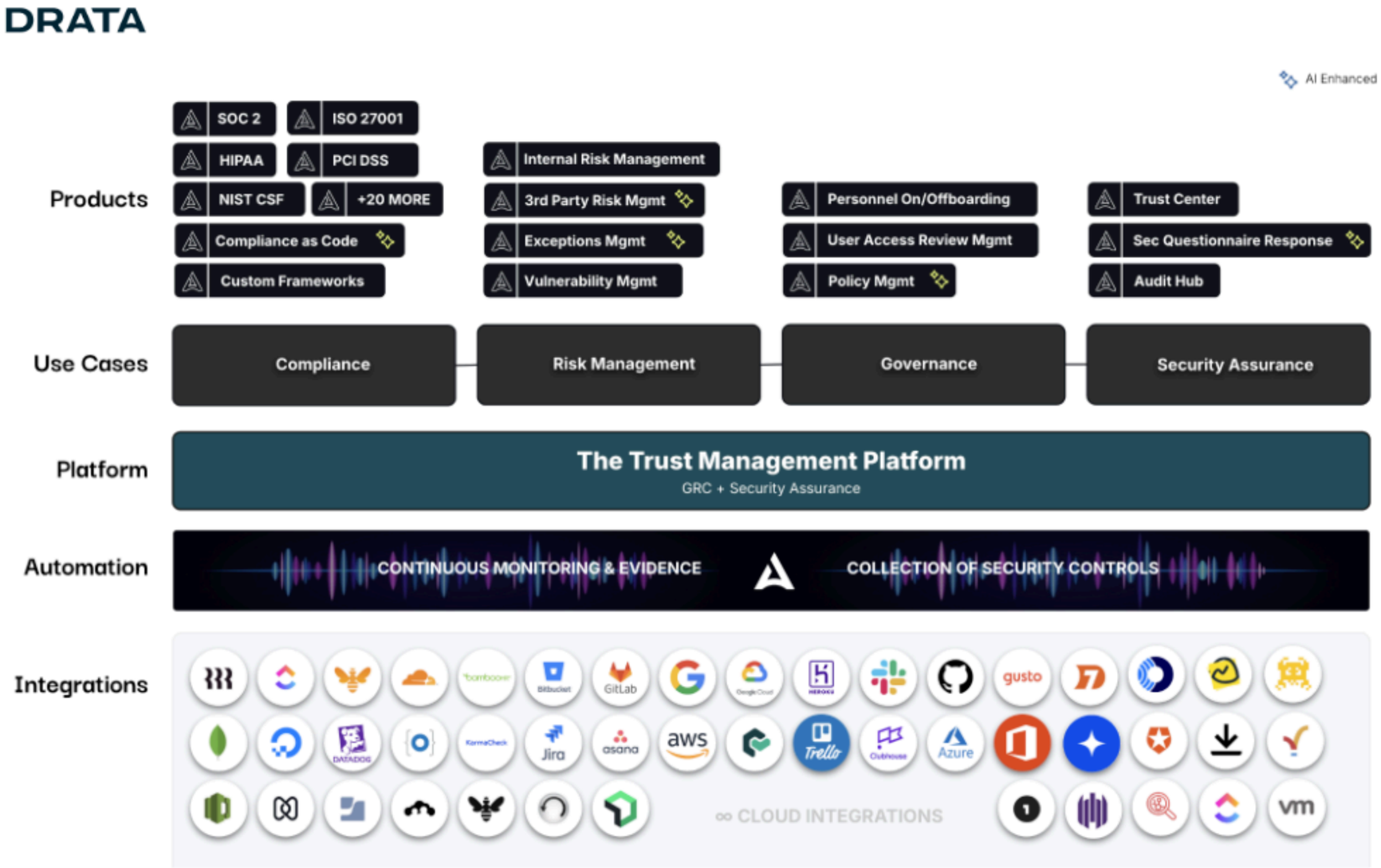
GUARDIANS CZ

GRC (=Governance, Risk & Compliance)

Kdy se poskytovatelům digitálních služeb vyplácí GRC nástroj?

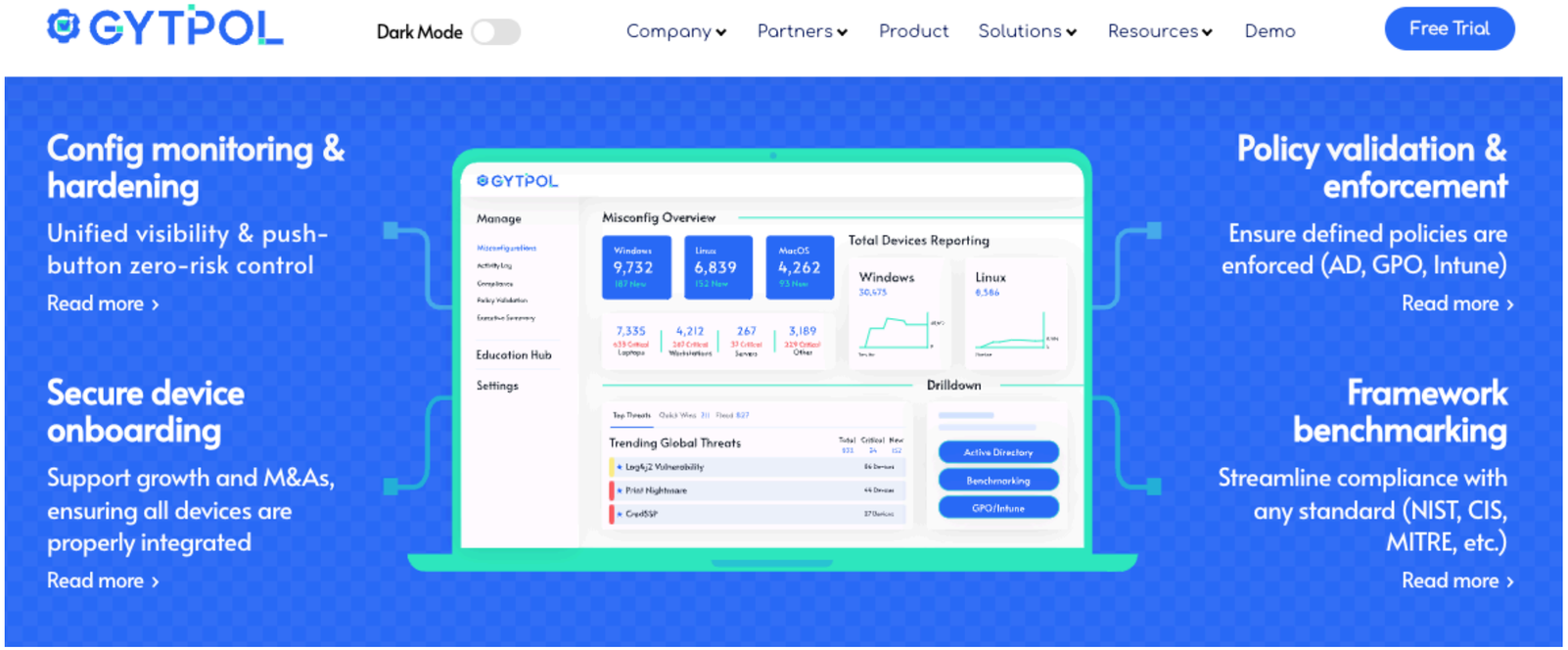
- Výhody
  - mapování - u požadavků podle ISO 27k, SOC2, PCI DSS již namapováno
  - automatizace, integrace, automatizovatelný sběr důkazů
  - aktuálnost standardů a podporované regulace v ceně nástroje
  - ...
- Nevýhody
  - CZ regulace většinou tyto nástroje nemají a je nutné je doplnit, což ale nemusí být vůbec problém (nebojte se toho)
  - když se vám z nástroje stane cíl
  - ...
- K posouzení, zda výhoda/nevýhoda
  - Náklady - je nutné individuálně porovnat Váš use case
  - Nezávislé na změně konzultanta, ale chce to dělat zálohy / exporty jako backup
  - Konkrétní nástroje - volte i s ohledem na to, jaké standardy a regulace chcete řešit, jací jsou vaši současní zákazníci vč. zemí atd.

GRC - DRATA


DRATA
AI Enhanced
Products
SOC 2
ISO 27001
HIPAA
PCI DSS
NIST CSF
+20 MORE
Compliance as Code
Custom Frameworks
Internal Risk Management
3rd Party Risk Mgmt
Exceptions Mgmt
Vulnerability Mgmt
Personnel On/Offboarding
User Access Review Mgmt
Policy Mgmt
Trust Center
Sec Questionnaire Response
Audit Hub
Use Cases
Compliance
Risk Management
Governance
Security Assurance
Platform
The Trust Management Platform
GRC + Security Assurance
Automation
CONTINUOUS MONITORING & EVIDENCE
COLLECTION OF SECURITY CONTROLS
Integrations
∞ CLOUD INTEGRATIONS

Správa konfigurací

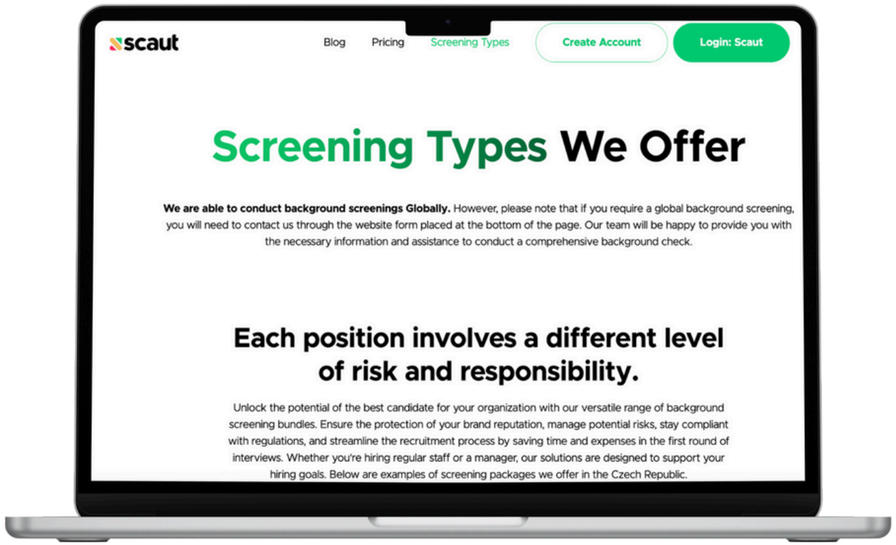
- Možná řešení
  - CIS benchmarky
  - nástroj jako GYTPOL
  - Ubuntu Pro - CIS
  - Ansible, Puppet, Terraform …
  - Microsoft Endpoint Configuration Manager (MECM), Microsoft Intune, …



https://gytpol.com/solutions

Background-checky

[vstup hosta - Petr Moroz, CEO | scaut.com]



https://scaut.com/en/screening-types

10.2. Ověření spolehlivosti

- *10.2.1. Příslušné subjekty v proveditelném rozsahu zajistí, aby se u jejich **zaměstnanců a v příslušných případech u přímých dodavatelů a poskytovatelů služeb provádělo ověřování spolehlivosti** v souladu s bodem 5.1.4 (prověřování spolehlivosti zaměstnanců dodavatele, u rizikových dodavatelů), pokud to vyžadují jejich úkoly, povinnosti a oprávnění.*

- *10.2.2. Pro účely bodu 10.2.1 příslušné subjekty:*
  - *a) zavedou kritéria, která stanoví, které úkoly, odpovědnosti a pravomoci mohou vykonávat pouze osoby, jejichž spolehlivost byla ověřena;*
  - *b) zajistí, aby ověření spolehlivosti těchto osob uvedené v bodě 10.2.1, které vezme v potaz platné zákony, předpisy a etické zásady úměrně k obchodním požadavkům, ke klasifikaci aktiv podle bodu 12.1, k sítím a informačním systémům, k nimž mají mít přístup, a vnímaným rizikům bylo provedeno před tím, než tyto osoby začnou vykonávat dané úkoly, odpovědnosti a pravomoci.*

- *10.2.3. Příslušné subjekty tuto politiku v plánovaných intervalech přezkoumávají a v případě potřeby aktualizují a v případě potřeby ji aktualizují.*

>>

Přímý a nepřímý dopad nZKB a proč je to důležité téměř pro jakékoliv poskytovatele digi služeb

Přímý vs. nepřímý dopad + kombo

Přímý dopad nZKB

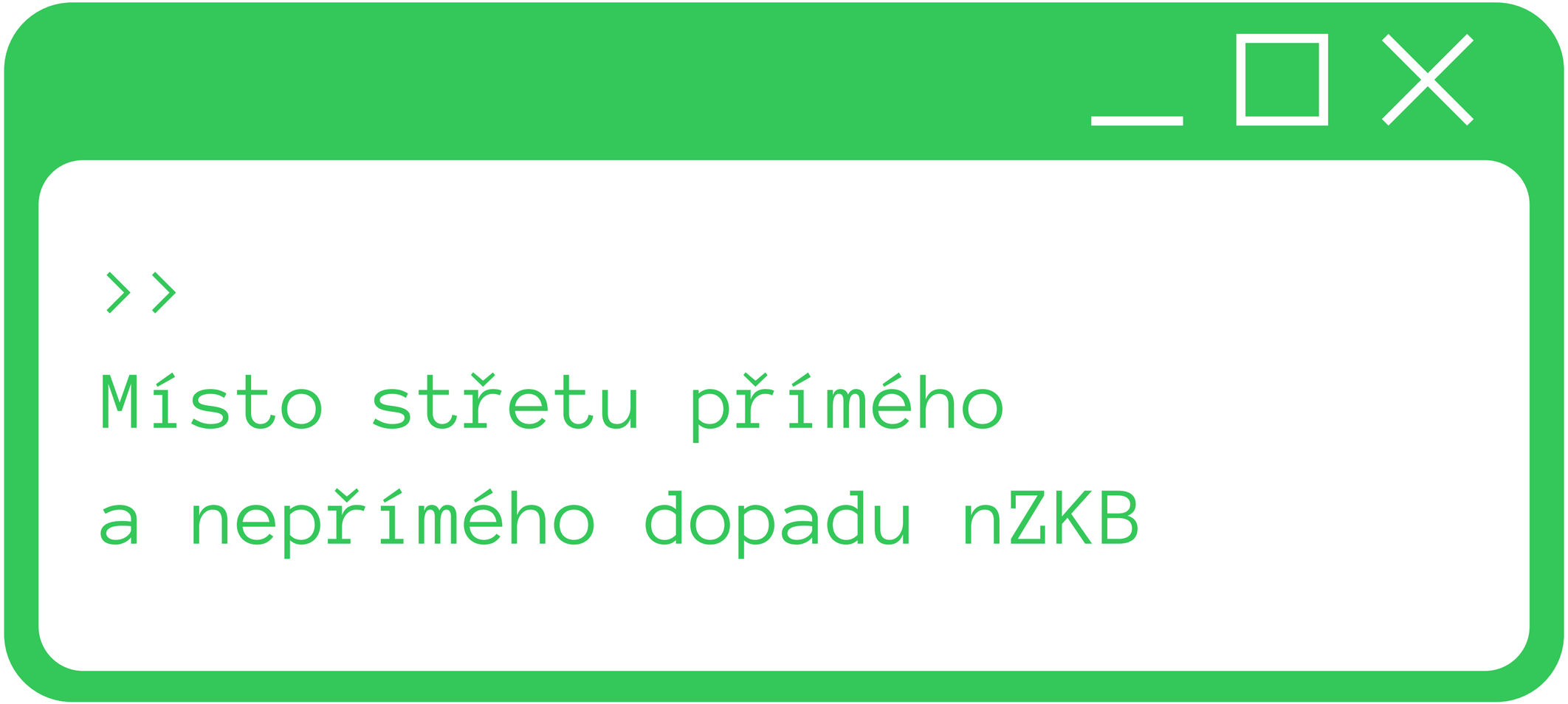
- Poskytovatel poskytuje regulované služby (je povinnou osobou podle nZKB).

Nepřímý dopad nZKB

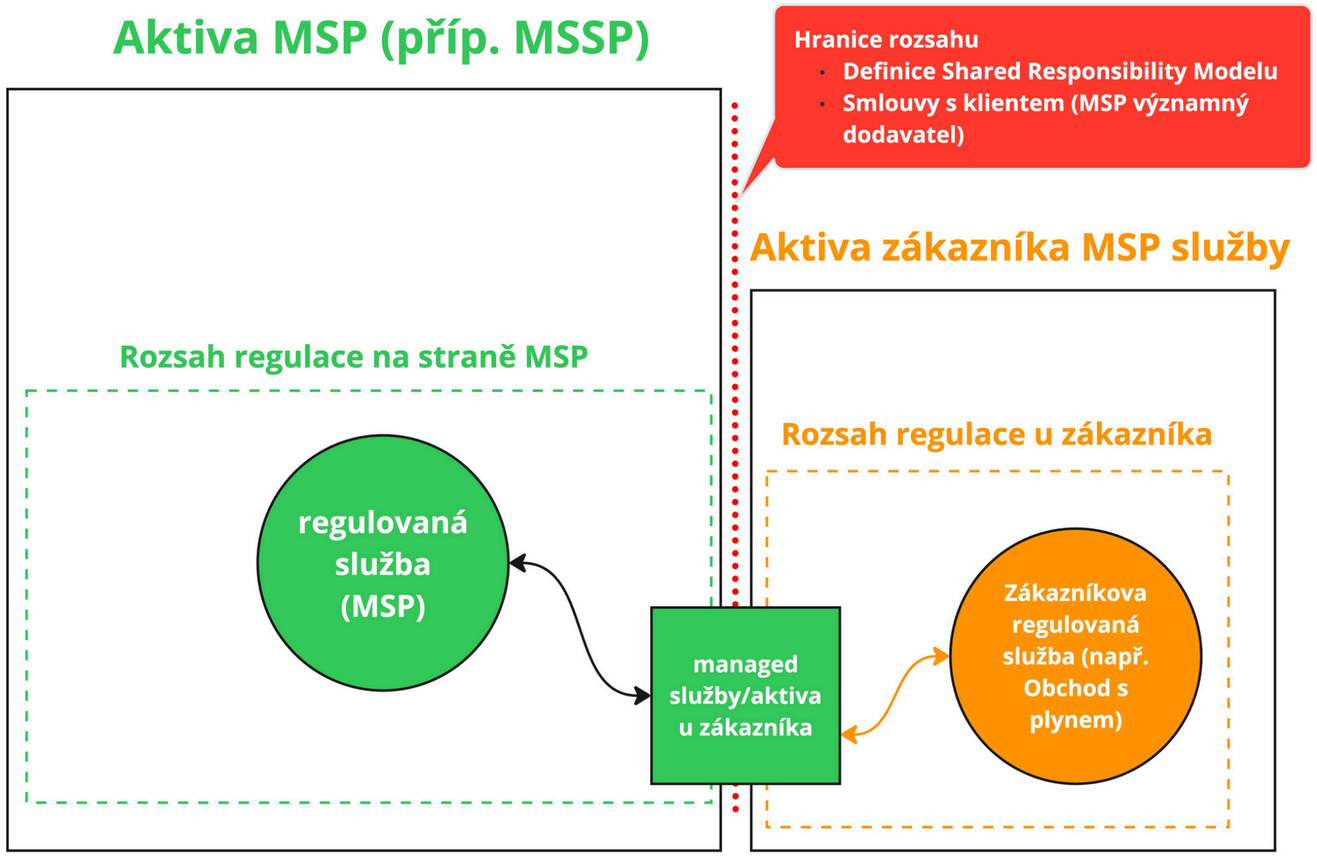
- Poskytovatel NEposkytuje regulované služby (NENÍ povinnou osobou podle nZKB), ale jejím zákazníkem jsou jiné povinné organizace, které skrz řízení dodavatelů kladou bezpečnostní požadavky na poskytovatele. Poskytovatel je významným dodavatelem pro jinou povinnou osobu.
- Poskytovatel je “nucen” plnit určitá bezpečnostní opatření v rámci smluvního vztahu (aby nepřišel o zakázku).

Kombinace - např.

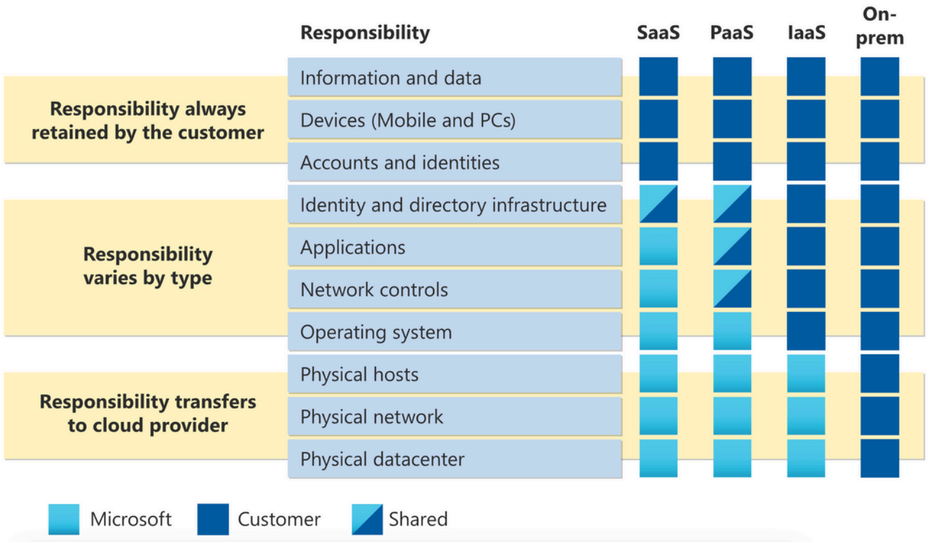
  - Cloud service provider, který je velkým podnikem
  - Interní kompetenční centrum (MSP, MSSP) v energetice, logistice atp.


>>
Místo střetu přímého
a nepřímého dopadu nZKB

Místo střetu přímého a nepřímého dopadu nZKB



Př. Shared Responsibility Model - MS Azure



Zdroj: https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

>>

Situace, kdy organizace spadá i do jiného odvětví regulovaných služeb

Příklad - holding v energetice s MSP/MSSP

- Holding primárně poskytující služby v odvětví energetiky.
  - Spadá do regulovaných služeb, do vyššího režimu.
  - Poskytuje ale i služby typu MSP/MSSP, neboť má vlastní kompetenční centrum. Odtud poskytuje služby MSP/MSSP v rámci holdingu.
- Holding usiluje o centralizaci procesů a služeb (ostatně i proto kompetenční centrum vzniká).
- Z hlediska požadovaných bezpečnostních opatření se uplatní kombinace, tedy:
  - **U regulovaných služeb v energetice se aplikují požadavky na vyšší režim.**
  - **U MSP/MSSP se musí opatření zavádět dle nařízení EU pro digi služby.**
  - **Vzhledem k centralizaci je nezbytné využít compliance mapování, ideálně s podporou moderního GRC nástroje.**


>>
Výzvy a příležitosti

Výzvy

- “Soulad se všemi těmi regulacemi” .... GDPR, AI Act, SOC2 Type II, ISO 27001, ISO 27017, ISO 27018, NIS2, ...
  →Compliance mapování
- Být věrohodným, bezpečným poskytovatelem digi služeb pro významné klienty
- Obstát u zákaznických auditů a kontrol ze strany regulátorů
- Dobře využívaný GRC nástroj usnadní správu compliance a v dlouhodobém horizontu ušetří nemalé finance (automatizace, integrace dat, interní HR - nižší nároky na kompetence, ...)
- Shared Responsibility Modely
- Odbavování bezpečnostních dotazníků a security požadavků ze strany klientů
- Zajistit metriky související s událostmi tak, aby bylo možné vyhodnocovat významnost incidentů
- Zajistit reporting incidentů bez API / integrace na straně regulátora

Příležitosti

- Registrace do eGC => poskytování služeb “státu”
- Je vhodné vnímat, že už jen z principu nárůstu počtu povinných osob ze současných 500 organizací na asi 10.000+ organizací, logicky vzroste počet organizací, které se budou muset spoléhat na profesionální služby v oblasti digitálních služeb => nárůst počtu potenciálních zákazníků.
- Sázka na poskytování bezpečných služeb => bezpečnostní sektor obecně roste a kybernetická bezpečnost v něm hraje velice významnou roli.
- ...

Když chcete poskytovat služby veřejné správě → eGC (eGovernment Cloud)

Pravidla pro zápis do eGC katalogu specifikuje vyhláška č. 316/2021 Sb. (nyní v MPŘ) a jsou závislé na bezpečnostní úrovni, do které se chcete zapsat. Nejčastěji ale budete potřebovat:

- certifikaci podle ISO/IEC 27001 s rozšířením o ISO/IEC 27017, ISO/IEC 27018
- příp. SOC2 Type II
- pravidelné skeny zranitelností zapsaných cloud. služeb
- penetrační testy zapsaných cloud. služeb
- podmínky služeb + smluvní podmínky (vč. shared responsibility modelů)
- atd.

Návrh vyhlášky o některých požadavcích pro zápis do katalogu cloud computingu (MPŘ):
https://odok.gov.cz/portal/veklep/material/KORNDGWN9B86/

Trust Portal

- Jako poskytovatelé pravděpodobně již nyní čelíte řadě dotazů na bezpečnost od svých zákazníků, kteří např. musí plnit DORA, současný nZKB, nebo jsou z odvětví, kde kyberbezpečnost hraje významnou roli - např. zbrojní průmysl, R&D, stát.
  - Jak by to ale vypadalo, když pro většinu zákazníků budete vyplňovat separátní dotazníky, kdy každý je jiný? Zvládnete to? Najmete na to člověka?
    - Řešením může být něco jako “Trust Portál” (obdobně k tomu přistupují velcí hráči jako MS, AWS a další)
- Trust portál
  - Řízený přístup k vybraným certifikacím a častým otázkám vašich klientů (pozn.: některé GRC mají v sobě)
- Inspirace - jak to dělají velcí hráči:
  - MS Service Trust Portal - https://servicetrust.microsoft.com/
  - AWS - https://aws.amazon.com/compliance/soc-faqs/

Trust Portal pomocí GRC

SafeBase Features Spotlight

Trust Center Content

Content Library, custom cards, direct subprocessor links, PDF view, automated doc watermarking, SOC bridge letters

Trust Center Updates

Proactively share impact and remediation after an incident. Share subprocessor additions, deletions, and usage updates.

Trust Center Customization

Connect security and your brand with custom branding, custom URLs, and website integrations.

Multiple Products

Showcase your trust posture and make it easy for buyers to self-serve security documentation across your product portfolio.

Trust Center Access and Governance

Robust permissioning and access controls like auto bulk invite, SCIM, expiration dates, and more.

Automated NDA

Allow buyers to securely self-serve required documentation via integrated NDA signing in SafeBase.

Permission Profiles

Designate different access levels with highly configurable permission profiles, like assigning access by buyer role, company segment, ARR, or industry.

Custom Rules Engine

Give access to the right people for the right reason in real time based on attributes in Salesforce like revenue, customer type, and NDA status.

Knowledge Base

Maintain your FAQ content library giving self-serve access to internal and external stakeholders via your Trust Center.

AI Questionnaire Assistance

Save up to 80% of time answering questionnaires with auto-approval, auto-mapping, multi-language support, document parsing, and more.

Chrome Extension

Provide questionnaire responses directly in your buyer's TPRM portal.

Collaboration

Assign questions to SMEs or groups, bulk assign tasks, send email, Slack, and Teams notifications, add due dates and more.

Hubspot Integration

Automate access, approvals, and NDA workflows based on Hubspot CRM data.

Advanced Analytics Dashboard

Communicate security program ROI and focus areas with revenue dashboards fueled by CRM data.

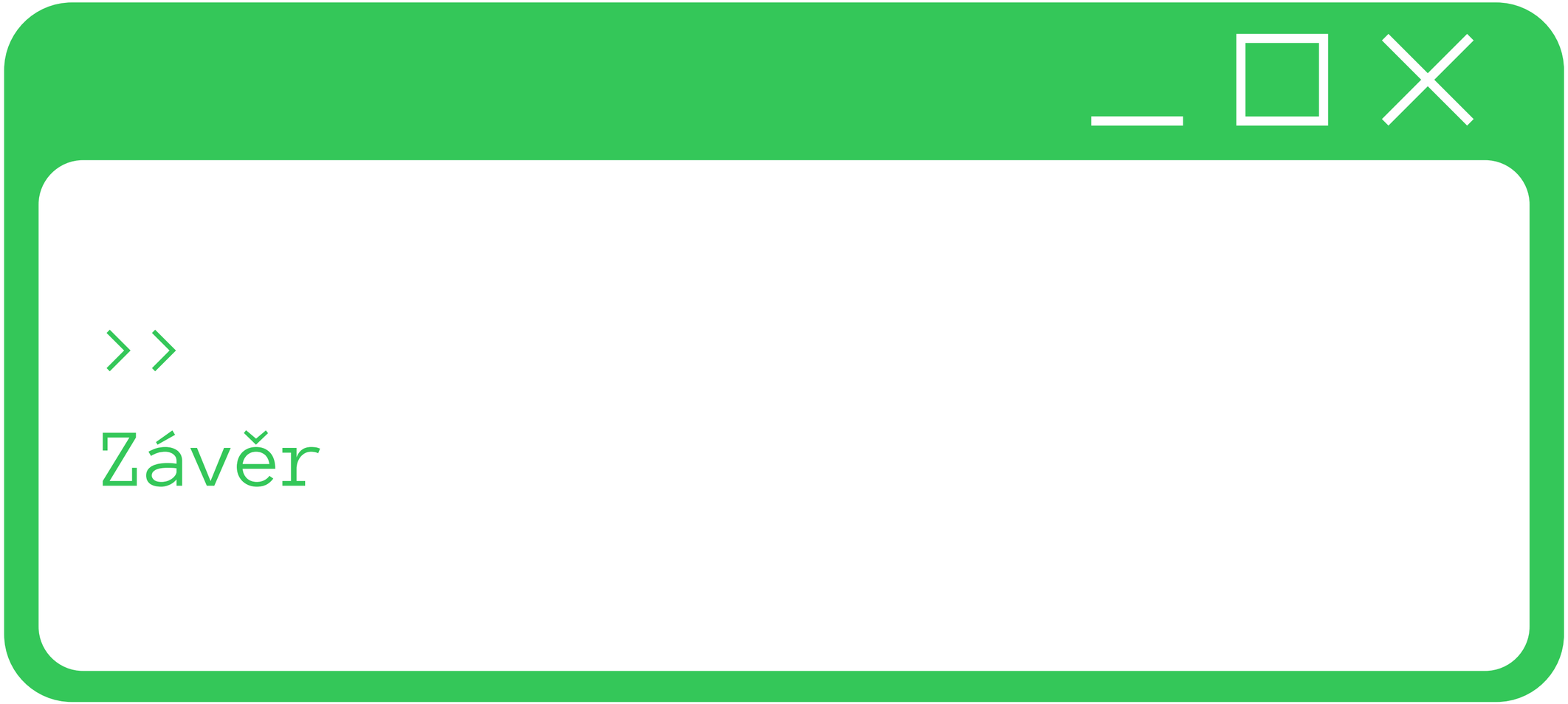
Top Metrics Dashboard

Gain comprehensive, real-time views into key SafeBase metrics, like account activity, usage, and Trust Center engagement.

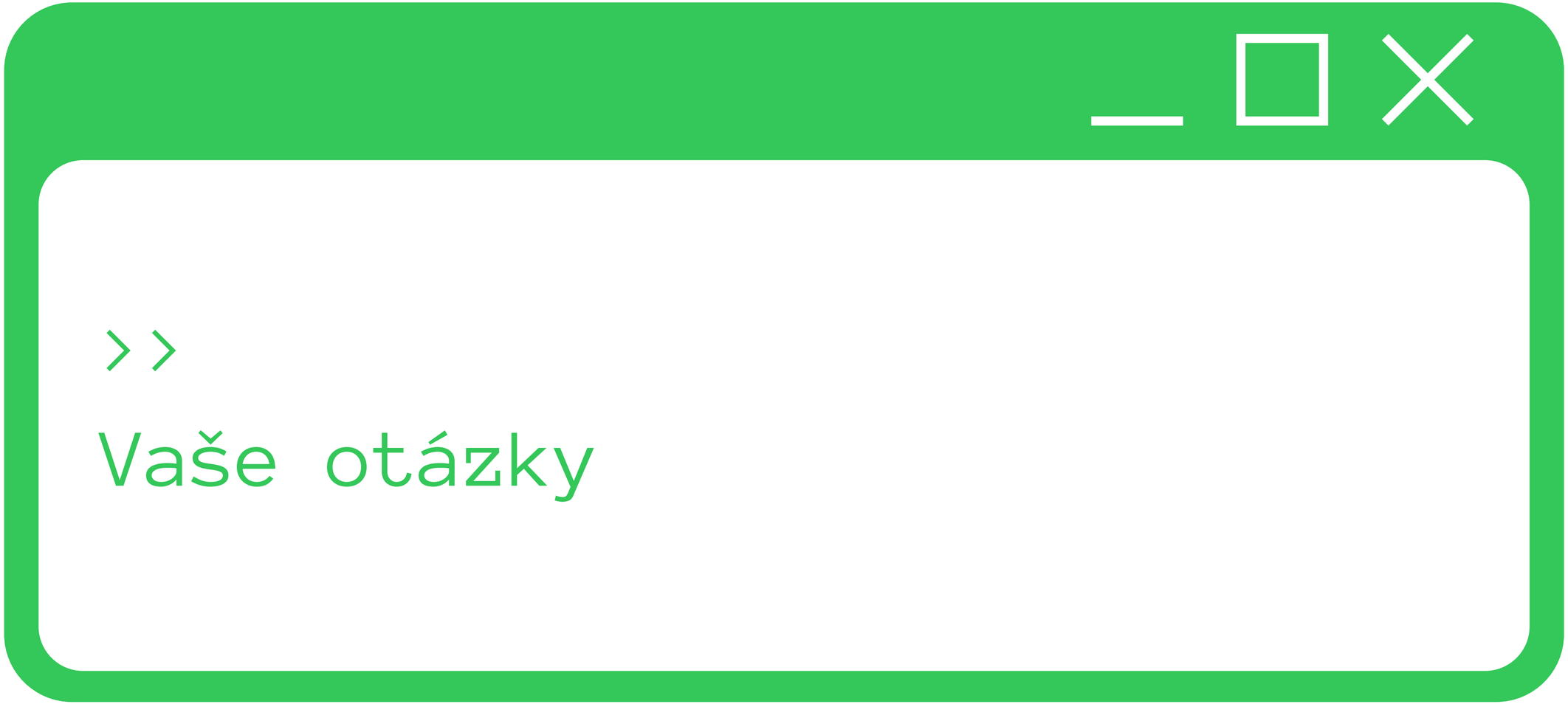
AI Analytics Dashboard

Track and measure the accuracy and time savings achieved by using AI Questionnaire Assistance.

GUARDIANS CZ


>>
Závěr

1. **Pokud již máte certifikaci podle ISO/IEC 27001, nebo ještě lépe máte poctivý SOC2 Type II - vyjděte z toho a do-mapujte si požadavky nové regulace na to, co již máte. Vyplynou Vám z toho jen drobné gapy, na které se zaměřte!**
2. Jste poskytovateli digitálních služeb, tzn. většinou máte spoustu informací v používaných nástrojích / systémech, které stačí správně integrovat a využít pro účely bezpečnosti (VM tooly, logy, threat monitoring, provozní monitoring → rizika, opatření atp.).
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, většinou to nedopadne...**
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 CISO/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!


>>
Vaše otázky

Řízení dodavatelů

V EU aktu je požadováno:

- *definovat politiku řízení dodavatelů*
- *stanovit bezpečnostní kriteria pro výběr dodavatele*
- *hodnotit rizika spojená s dodavateli*
- *aby smlouvy s dodavateli obsahovaly požadovaná ustanovení*
- *vést seznam dodavatelů*
- *...*

+ případná národní specifika (pro určité typy subjektů např. BDŘ?)

Jaké jsou optimální nástroje pro technická opatření?

Na tuto otázku je těžké odpovědět, při volbě bezpečnostních nástrojů hraje roli mnoho aspektů - již využívané technologie a platformy, úroveň bezpečnostních rizik a přístup ke zvládání rizik organizace, dále samozřejmě také rozpočet, další dostupné zdroje atd. Inspirací k typům bezp. nástrojů mohou být přehledové tabulky uvedené v prezentaci dříve.

Jak správně definovat MSP a MSSP? Když poskytuji například fakturační SaaS, jsem MSP?

Viz dříve zmíněná přehledová tabulka s povinnostmi pro cloud (SaaS) a MSP => povinnosti jsou totožné, nemá smysl řešit, zda náhodou SaaS není i MSP. SaaS je podle definic NIS2 cloud.

Co máme splnit a nejlépe i jak, jako poskytovatel Internetu (ISP)?

Zde záleží, zda je ISP pouze v kategorii regulovaných služeb 16.1. nebo 16.2. a na velikosti podniku => nižší/vyšší režim. Pokud ale ISP poskytuje i další z digitálních služeb, pak je nutné si dát pozor na případnou kombinaci bezpečnostních opatření podle vyhlášek k nZKB a podle nařízení EU k NIS2.

S čím vám rádi pomůžeme

- **Získání konkurenční výhody díky SMYSLUPLNĚ zvládnutým požadavkům na kybernetickou bezpečnost ze strany regulace/zákazníků**
- Compliance mapování
- Nasazení GRC nástroje (DRATA, ISMS Online, ...)
- Posouzení dopadu regulace ve spolupráci s partnery (právní služby)
- Gap analýza
- Příprava na ISO/IEC 27001 certifikace vč. případného rozšíření o ISO/IEC 27017 a ISO/IEC 27018
- Příprava pro SOC2 Type I a Type II
- Manažer kybernetické bezpečnosti
- Zajištění shody s nZKB / NIS2 obecně
- Penetrační testy
- Mapování požadavků nové regulace na SOC2 a/nebo ISO/IEC 27k (značná úspora nákladů).
- Registrace do eGC ve spolupráci s partnery (kombinace právních, cyber/info sec. konzultačních služeb a pentestů)

+ více v našem portfoliu na webu **https://www.guardians.cz/cs/**

GUARDIANS CZ

nZKB akademie 2025

Unikátní vzdělávání zaměřené
na nový kybernetický zákon
v souvislostech.

Se slevovým kódem **BENEFIT-25**
se slevou 25%

https://www.cybersecurityplatform.cz/akademie

GUARDIANS CZ

Online školení nZKB pod lupou

Adam Kučínský (NÚKIB) a Martin Konečný (Guardians.cz) vás provedou (18. 6. 2025 | 9:00 - 16:0 jednodenním online školením k nZKB.

Se slevovým kódem **BENEFIT-25**
jen za cenu 3.000 Kč bez DPH

https://www.cybersecurityplatform.cz/udalosti/online-skoleni-novy-kyberneticky-zakon-pod-lupou

GUARDIANS.CZ

Jak zabezpečit AI a zajistit shodu s EU AI Act pomocí AIMS

Jiří Císek (AK Cisek) a Martin Konečný (Guardians.cz) vás 19. 6. 2025 (9:00-11:00) provedou svým webinářem na aktuální, trendy téma - zabezpečení AI pomocí AIMS (ISO 42001) a AI Act.

Účast na webináři je zdarma, registrace nutná.

https://www.guardians.cz/unikatni-webinar-jak-zabezpecit-ai-a-zajistit-shodu-s-ai-act-pomoci-aims

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