VIAVIS střežíme podstatné

Regulace – NIS2

Kybernetická a informační bezpečnost II

Vladimír Lazecký

vladimir.lazecky@viavis.cz

Malé opakování

- Co je to bezpečnost?
- Jak rozumíte pojmu kybernetická bezpečnost?
- Jaký je rozdíl mezi informační a kybernetickou bezpečností?
- O co se kybernetická bezpečnost opírá?
- Co je to informace? Data?

Co je a není bezpečnost

- Bezpečnost je schopnost aktiva odolávat hrozbám
  - Aktivum – vše, co má hodnotu
  - Primární aktivum - ERP systém, dobré jméno…
  - Podpůrná aktiva – lidé, servery, SW…
- POZOR – bezpečnost není stav
  - Hluboký omyl

Informační x kybernetická bezpečnost

- Informační bezpečnost:
  - Zajištění stanovené úrovně bezpečnosti informací
  - Bezpečnost informací = důvěrnost, dostupnost, integrita
- Kybernetická bezpečnost – podmnožina informační bezpečnosti – bezpečnost v kyber prostoru
- Neexistuje oddělená bezpečnost

Motivy, proč informační bezpečnost řešit

- Hodnota aktiva:
  - Stanovení hodnot – analýza rizik
  - Bezcenné aktivum nemá smysl chránit
- Motivy:
  - Osobní bezpečnost
  - Bezpečnost organizace
  - Bezpečnost státu, mezinárodního společenství

Téma dne – jak kybernetickou bezpečnost vynutit

- *Jak byste vynutili KB v:*
  - *Soukromých společnostech*
  - *Státních institucích*
  - *Soukromých osobách*

Regulace na úrovni státu

- Informační/kybernetická bezpečnost v právním řádu:
  - ZÁKON 412/2005 Sb. ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti
  - Navazující vyhlášky – kryptografická ochrana
  - Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
  - Nová vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti

Regulace na úrovni státu

- Informační/kybernetická bezpečnost v právním řádu – nepřímo a zjednodušeně:
  - ZÁKON 412/2005 Sb. ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti
  - 89/2012 Sb. občanský zákoník
  - Obecné nařízení o ochraně osobních údajů (GDPR) 2016/679
  - Zákon č. 110/2019 Sb. o zpracování osobních údajů
  - Trestní zákoník …

Aktuálně – NIS2

- NIS2 – nová směrnice EU o kybernetické bezpečnosti
  - Konečné znění bylo zveřejněno 27.12.2022 ve věstníku EU
  - NIS2 stanovuje cíl, který musí členské země splnit
  - Způsob splnění je na členských zemích
  - V ČR – návrh nového zákona o kybernetické bezpečnosti
  - Transpoziční lhůta do 16.10.2024

NIS2 – přehled stavu

Návrh směrnice NIS2
(prosinec 2020)

Finální znění směrnice NIS2
(27. prosince 2022)

Změny zákona
a nové povinnosti v ČR
(od poloviny roku 2024)

VIAVIS

Hlavní požadavky NIS 2

- Podle čl. 7:
  - **Přijetí národní strategie kybernetické bezpečnosti a kybernetických bezpečnostních politik** pro vybrané oblasti (např. bezpečnost dodavatelského řetězce, koordinované zveřejňování informací o zranitelnostech, zvláštní potřeby malých a středních podniků);
  - Strategie dále stanovuje:
    - Strategické cíle
    - Zdroje k dosažení cílů
    - Politiky a regulační opatření

Hlavní požadavky NIS 2

- Podle čl. 12:
  - Zveřejňování informací o zranitelnostech a zřízení Evropské databáze zranitelností
  - každý členský stát určí jeden ze svých týmů CSIRT (CERT) jakožto koordinátora zveřejňování zranitelností
    - *KB I – přednáška hackerem snad a rychle, OSINT, databáze zranitelností*

Hlavní požadavky NIS 2

- Podle čl. 13:
  - Spolupráce s vnitrostátními úřady a organizacemi a koordinace dozorových činností u organizací, kterým plyne povinnost zajišťovat kybernetickou bezpečnost z více právních předpisů (např. v odvětvích energetiky, letectví nebo ochrany osobních údajů)

Rozumíte tomu?

Hlavní požadavky NIS 2

- Podle čl. 14, 15, 16:
  - Spolupráce s členskými státy v oblastech kybernetického krizového řízení, řešení rozsáhlých kybernetických bezpečnostních incidentů a sdílení strategických informací a dobré praxe

A tomu rozumíte?

Hlavní požadavky NIS 2

- Podle čl. 37:
  - Hlubší spolupráce s dozorovými orgány ostatních členských států na provádění kontrol a vymáhání dodržování uložených povinností
  - Cílem ustanovení nazvaného jako tzv. vzájemná pomoc je nastavit pravidla kontroly takovým způsobem, aby po obdržení odůvodněné žádosti poskytnul úřad vykonávající kontroly kybernetické bezpečnosti v jednom členském státě pomoc druhému úřadu z jiného členského státu, aby bylo možné účinně, účelně a důsledně provést kontrolu, respektive opatření v oblasti dohledu nebo vymáhání

Hlavní požadavky NIS 2

- Podle čl. 21 a 23:
  - Větší zapojení Evropské komise do sjednocení regulace v členských státech (např. formou jednotných metodik pro zavádění bezpečnostních opatření nebo jednotných formulářů pro hlášení incidentů)
  - Komise může přijmout prováděcí akty, kterými stanoví technické, metodické a případně odvětvově specifické požadavky

Hlavní požadavky NIS 2

- Podle čl. 2:
  - **Rozšíření počtu povinných osob** (odhady hovoří o nejméně 6 000 soukromých i státních organizacích), a to jednak rozšířením regulovaných odvětví (např. odvětví odpadového hospodářství), dále rozšířením stávajících regulovaných odvětví o nové regulované služby (např. stávající odvětví digitální infrastruktury o nové regulované služby cloud computingu nebo poskytovatele služeb a sítí elektronických komunikací) a nebo změnou způsobu identifikace povinných osob (kdy primárním kritériem pro zařazení do regulace bude velikost organizace);

Hlavní požadavky NIS 2

- Podle čl. 20:
  - **povinné vzdělávání vrcholového vedení organizace** a větší odpovědnost managementu za zajišťování kybernetické bezpečnosti v organizaci
  - členové řídících orgánů povinných osob musí absolvovat školení, aby tak získali dostatečné znalosti a dovednosti, aby mohli identifikovat rizika a posoudit postupy řízení kybernetických bezpečnostních rizik a jejich dopad na poskytované služby
- Podle čl. 30 dobrovolné hlášení relevantních incidentů, událostí, hrozeb a zranitelností

Hlavní požadavky NIS 2

- Podle čl. 27 a 28 podrobnější požadavky na vedení registru internetových domén nejvyšší úrovně a činnost registrátorů

- Podle čl. 29 větší důraz na sdílení informací mezi povinnými organizacemi

Hlavní požadavky NIS 2

- Podle čl. 34 významné zvýšení pokut za nedodržení uložených povinností:
  - v případě porušení povinností tzv. „essential entity“ (česky základními subjekty), pokuty, jejichž horní hranice sazby bude stanovena na **nejméně 10 milionů EUR** nebo na **alespoň 2 %** celkového celosvětového ročního obratu v předchozím rozpočtovém roce, podle toho, co je vyšší
  - v případě porušení povinností tzv. „important entity“ (česky důležitými subjekty) pokuty, jejichž horní hranice sazby bude stanovena na **nejméně 7 milionů EUR** nebo na **alespoň 1,4 %** celkového celosvětového ročního obratu v předchozím rozpočtovém roce, podle toho, co je vyšší
- ***Pamatujete GDPR hysterii?***
- ***Je efektivní cestou strašení pokutami?***

Nový návrh zákona o kybernetické bezpečnosti

Poskytovatel regulované služby:

- Musí naplňovat kritéria stanovená navrhovanou vyhláškou o regulovaných službách
- Pomocí samoidentifikace zjistí, pro jakou službu nebo služby je regulován
- Následně se musí NÚKIB sám nahlásit (registrovat) a je zapsán do evidence

Nový návrh zákona o kybernetické bezpečnosti

- **Režim povinností poskytovatele regulované služby:**
  - Režim vyšších povinností
  - Režim nižších povinností

Nový návrh zákona o kybernetické bezpečnosti

- **Povinnosti poskytovatele regulované služby:**
  - Registrace NÚKIB
  - Stanovit rozsah řízení kybernetické bezpečnosti
  - Zavádět bezpečnostní opatření
  - Hlásit kybernetické bezpečnostní incidenty
  - Informovat zákazníky o incidentech a hrozbách
  - Provádět protiopatření

Nový návrh zákona o kybernetické bezpečnosti

- **Povinnosti poskytovatele regulované služby:**
  - Uplatnit pravidla lokalizace dat
  - Plnit povinnosti mechanismu řízení bezpečnosti dodavatelského řetězce
  - Podřídit se výkonu kontroly inspektorem
- ***Diskuse – kde vidíte problémy?***

Poskytovatelé regulovaných služeb

TLP: CLEAR

Národní úřad pro kybernetickou a informační bezpečnost NÚKIB

SLUŽBY UVEDENÉ V PŘÍLOZE I

Subjekty poskytující služby uvedené v příloze I níže a splňující podmínku „velký podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány vždy v režimu „essential".

ENERGETIKA

Provozovatelé distribuční a přenosové soustavy, výrobci a prodejci elektrické energie, nominovaní organizátoři trhu s elektřinou, provozovatelé dobíjecích stanic spolu s poskytovateli elektromobility.

Subjekty poskytující službu dálkového vytápění nebo chlazení.

Provozovatelé ropovodů, zařízení na těžbu, rafinaci a zpracování ropy, skladovacích a přenosových zařízení, ústřední správci zásob.

Obchodníci s plynem, distributoři plynu, přepravci plynu, výrobci plynu a poskytovatelé uskladňování plynu.

Provozovatelé výroby, skladování a přepravy vodíku. Doposud však není implementováno do českého právního řádu.

DOPRAVA

Komerční letečtí dopravci, řídicí orgány letišť a subjekty provozující pomocná zařízení v rámci letišť, provozovatelé kontroly řízení provozu.

Provozovatel dráhy celostátní nebo regionální anebo veřejné přístupné vlečky a dopravce provozující na těchto drahách drážní dopravu.

Předmětné předpisy se vztahují na námořní přístavy a pro Českou republiku tedy nejsou relevantní.

Silniční orgány odpovědné za plánování, kontrolu a správu silnic spadajících do jejich územní působnosti, poskytovatelé služeb ITS.

BANKOVNICTVÍ

Sektor bankovnictví je regulován nařízením DORA.

INFRASTRUKTURA FIN. TRHŮ

Sektor infrastruktura finančních trhů je regulován nařízením DORA.

ZDRAVOTNICTVÍ

Poskytovatelé zdravotní péče (nemocnice a další), subjekty provádějící výzkum a vývoj léčivých výrobků a přípravků, výrobci základních farmaceutických přípravků.

PITNÁ VODA

Dodavatelé a distributoři vody určené k lidské spotřebě, avšak kromě těch, pro které je to vedlejší činnost k jejich hlavní činnosti zabývající se distribucí jiných komodit a zboží.

ODPADNÍ VODA

Subjekty shromažďující, vypouštějící nebo upravující městské nebo průmyslové odpadní vody nebo splašky, avšak kromě těch, pro které se jedná pouze o vedlejší činnost k jejich hlavní činnosti.

DIGITÁLNÍ INFRASTRUKTURA

Poskytovatelé: výměnných uzlů internetu (IXP), cloud computingu, datového centra, služeb vytvářejících důvěru, elektronických komunikací, CDN služeb, registrů TLD, služeb systému doménových jmen (DNS), s výjimkou poskytovatelů root name serverů .

POSKYTOVATELÉ ŘÍZENÝCH ICT SLUŽEB

Poskytovatelé řízených ICT služeb a poskytovatelé řízených ICT bezpečnostních služeb. Subjekty, pro zákazníky provozující či spravující ICT služby a nástroje, typicky na základě smlouvy o úrovni služeb (SLA).

VEŘEJNÁ SPRÁVA

Ústřední orgány státní správy, veřejná správa na regionální úrovni, soudy a státní zastupitelství a další instituce významné pro chod státu.

VESMÍR

V České republice nejsou umístěny žádné subjekty pozemní infrastruktury, pro Českou republiku tedy nerelevantní.

SLUŽBY UVEDENÉ V PŘÍLOZE II

Subjekty poskytující služby uvedené v příloze I a splňující podmínku „střední podnik" a subjekty poskytující služby uvedené v příloze II a splňující podmínku „velký podnik" a „střední podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány v režimu „important" (nižší nároky z hlediska bezpečnostních opatření), pokud nebude stanoveno speciálními kritérii jinak.

POŠTOVNÍ SLUŽBY

Subjekty, poskytující poštovní služby, tzn. výběr, třídění, přepravu a dodání poštovních zásilek, včetně provozovatelů kurýrních služeb.

ODPADNÍ HOSPODÁŘSTVÍ

Subjekty, poskytující službu nakládání s odpady, tzn. zařízení určená pro nakládání s odpady, obchodníci, zprostředkovatelé, dopravci podle zákona č. 541/2020 Sb., kromě těch, pro které nakládání s odpady není jejich hlavní ekonomickou činností.

CHEMICKÝ PRŮMYSL

Subjekty, poskytující služby v chemickém průmyslu, tzn. výrobci, distributoři, včetně maloobchodníka, který skladuje a uvádí na trh chemickou látku nebo předmět.

POTRAVINÁŘSTVÍ

Potravinářské subjekty, které se zabývají velkoobchodní distribucí a průmyslovou výrobou nebo zpracováním.

VÝROBA

Výroba: zdravotnických a diagnostických zdravotnických prostředků, počítačů, elektronických a optických přístrojů, elektrických zařízení, strojů a zařízení, motorových vozidel (kromě motocyklů), přívěsů a návěsů, ostatních dopravních prostředků a zařízení.

POSKYTOVATELÉ DIGI SLUŽEB

Poskytovatelé on-line tržišť, internetových vyhledávačů, platforem služeb sociálních sítí.

VÝZKUM

Výzkumné organizace, s výjimkou vzdělávacích institucí, jejichž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj s ohledem na využití výsledků tohoto výzkumu pro komerční účely.

SUBJEKTY, KTERÝM PLYNOU POVINNOSTI Z NIS2, ALE NESPADAJÍ DO REŽIMU ESSENTIAL, ANI IMPORTANT

Subjekty shromažďující a udržující přesnou a úplnou registraci názvu domén.

verze 1.0, platná ke dni 16.08.20

Poskytovatelé regulovaných služeb

Příloha k vyhlášce č. XX/XXXX Sb.
Kritéria pro identifikaci regulované služby

1. Veřejná správa

Regulovaná služba	
Služba	Kritérium poskytovatele regulované služby
1.1. Výkon svěřených pravomocí	Orgán nebo osoba je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je a) ústředním orgánem státní správy, b) správním úřadem s celostátní působností, a to včetně ústředí a generálního ředitelství územně dekoncentrovaných (specializovaných) orgánů státní správy, c) Kanceláří prezidenta republiky, d) Kanceláří Senátu, e) Kanceláří Poslanecké sněmovny, f) Kanceláří Veřejného ochránce práv, g) Českou národní bankou, h) Nejvyšším kontrolním úřadem, i) Policejním prezidiem, j) útvarem policie s celostátní působností, k) orgánem soudní moci

Režim vyšších povinností

- **Systém řízení bezpečnosti informací – ISMS**:
  - Cíle ISMS k zajištění bezpečnosti regulované služby
  - Na základě cílů, bezpečnostních potřeb, hodnocení rizik zavede přiměřená bezpečnostní opatření
  - Řídí rizika
  - Vytvoří a schválí bezpečnostní politiku
  - Zajistí provedení auditu kybernetické bezpečnosti
  - Zajistí vyhodnocení účinnosti systému řízení bezpečnosti informací alespoň jednou ročně

Režim vyšších povinností

Systém řízení bezpečnosti informací – ISMS

- Na základě vyhodnocení účinnosti systému řízení bezpečnosti informací zpracuje zprávu o přezkoumání systému řízení bezpečnosti informací
- Průběžně identifikuje a řídí významné změny
- Aktualizuje systém řízení bezpečnosti informací a příslušnou dokumentaci
- Řídí provoz a zdroje systému řízení bezpečnosti informací a zaznamenává činnosti
- Stanoví proces řízení výjimek z pravidel

Režim vyšších povinností

- **Povinnosti vrcholového vedení**:
  - Vrcholové vedení se prokazatelně účastní školení
  - Zajistí stanovení bezpečnostní politiky a cílů systému řízení bezpečnosti informací
  - Zajistí integraci systému řízení bezpečnosti informací do procesů povinné osoby
  - Zajistí dostupnost zdrojů potřebných pro systém řízení bezpečnosti informací
  - Informuje zaměstnance o významu systému řízení bezpečnosti informací
  - Zajistí podporu k dosažení cílů systému řízení bezpečnosti informací
  - Vede zaměstnance k rozvíjení efektivity systému řízení bezpečnosti informací
  - Podílí se na vypracování analýzy dopadů (BIA)

Režim vyšších povinností

- **Povinnosti vrcholového vedení:**
  - Prosazuje neustálé zlepšování systému řízení bezpečnosti informací
  - Podporuje osoby zastávající bezpečnostní role
  - Zajistí stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role
  - Zajistí, aby byla zachována mlčenlivost administrátorů a osob zastávajících bezpečnostní role
  - Pro osoby zastávající bezpečnostní role zajistí příslušné pravomoci a zdroje
  - Zajistí testování plánů kontinuity činností, plánů obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů

Režim vyšších povinností

- Vrcholové vedení se prokazatelně seznamuje se:
  - Zprávou o přezkoumání systému řízení bezpečnosti informací
  - Zprávou o hodnocení rizik
  - Výsledky analýzy dopadů
  - Výsledky auditů kybernetické bezpečnosti a kontrol v oblasti kybernetické bezpečnosti

Režim vyšších povinností

- Vrcholové vedení určí:
  - Složení výboru pro řízení kybernetické bezpečnosti
  - Bezpečnostní role, jejich práva a povinnosti
    - Manažera kybernetické bezpečnosti
    - Architekta kybernetické bezpečnosti
    - Garanta aktiva
    - Auditora kybernetické bezpečnosti

Řízení dodavatelů

- Pravidla pro dodavatele, která zohledňují požadavky ISMS
- Seznámení dodavatelů s pravidly

- Další povinnosti:
  - Identifikace a evidence významných dodavatelů
  - Prokazatelně písemně informuje své významné dodavatele o jejich evidenci
  - Řídí rizika spojená s dodavateli
  - Smlouvy uzavírané s významnými dodavateli musí obsahovat relevantní oblasti uvedené v příloze č. 7 k vyhlášce
  - Pravidelně přezkoumává plnění smluv s významnými dodavateli z hlediska ISMS

Řízení dodavatelů

- Povinná osoba u významných dodavatelů:
  - V rámci výběrového řízení a před uzavřením smlouvy provádí hodnocení rizik
  - Stanoví způsoby a úrovně realizace bezpečnostních opatření a určí obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření
  - Provádí pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany
  - V reakci na rizika a zjištěné nedostatky zajistí jejich řešení

- ***Máte představu o konkrétním řešení?***

Bezpečnost lidských zdrojů

- Stanoví plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí včetně formy, obsahu a rozsahu poučení a školení:
  - Poučení vrcholového vedení o jeho povinnostech, o bezpečnostní politice zejména v oblastech systému řízení bezpečnosti informací a řízení rizik
  - Poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice
  - Potřebná teoretická i praktická školení uživatelů, administrátorů a osob zastávajících bezpečnostní role
  - Pravidla tvorby bezpečných hesel
  - Relevantní témata uvedená v příloze č. 8 této vyhlášky

Řízení změn

- Povinná osoba v rámci řízení změn u aktiv
  - Identifikuje změny, které mají nebo mohou mít vliv na kybernetickou bezpečnost
  - Stanoví pravidla, postupy a kritéria pro určení významných změn
  - Dokumentuje řízení významných změn
  - Provádí hodnocení rizik
  - Přijímá bezpečnostní opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami
  - Aktualizuje bezpečnostní a provozní dokumentaci
  - Zajistí jejich testování před uvedením do provozu
  - Zajistí možnost navrácení do původního stavu

Akvizice, vývoj údržba

- Povinná osoba:
  - Řídí rizika
  - Řídí významné změny
  - Stanoví bezpečnostní požadavky v souladu s touto vyhláškou a vlastními bezpečnostními potřebami
  - Zahrne bezpečnostní požadavky do projektu akvizice, vývoje a údržby
  - Dodržuje a vymáhá dodržování požadavků
  - Zajistí oddělení provozního, zálohovacího, vývojového, testovacího a jiných specifických prostředí, a zajistí ochranu informací a dat se v nich vyskytujících
  - Je-li cílem provedení akvizice nebo vývoje technické aktivum využívající autentizační mechanizmus, zejména za účelem ověření identity uživatelů nebo administrátorů
  - Je-li cílem provedení akvizice nebo vývoje technické aktivum užívající kryptografické algoritmy, plní požadavky podle § 26 odst. 1 písm. a) a odst. 3 písm.

Řízení přístupu

- Povinná osoba na základě bezpečnostních a provozních potřeb řídí přístup k aktivům a přijímá bezpečnostní opatření, která slouží k zajištění ochrany přístupových a autentizačních údajů
- Řídí přístup na základě skupin a rolí
- Přidělí každému uživateli a administrátorovi přistupujícímu k aktivům přístupová práva a oprávnění a jedinečný identifikátor
- Řídí identifikátory, přístupová práva a oprávnění účtů technických aktiv
- Zavádí bezpečnostní opatření pro řízení přístupu technických aktiv k jiným aktivům
- Zavádí bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení a jiných obdobných technických aktiv, popřípadě i bezpečnostní opatření spojená s využitím technických aktiv, která povinná osoba nemá ve své správě

Řízení přístupu

- Omezí přidělování administrátorských a privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce
- Omezí a kontroluje používání programových prostředků a vybavení, které mohou být schopné překonat systémové nebo aplikační kontroly
- Prosazuje, aby byla při používání privátních autentizačních informací a mechanismů dodržována stanovená pravidla a postupy
- Přiděluje a odebírá přístupová oprávnění v souladu s politikou řízení přístupu
- Provádí pravidelné přezkoumání veškerých přístupových oprávnění včetně rozdělení do skupin a rolí
- Zajistí bezodkladné odebrání nebo změnu přístupových oprávnění při změně pozice nebo zařazení na základě skupin a rolí

Řízení přístupu

- Zajistí bezodkladné odebrání nebo změnu přístupových oprávnění při ukončení nebo změně smluvního vztahu
- Dokumentuje přidělování a odebírání přístupových oprávnění
- Využívá nástroj pro správu a ověřování identity podle § 20 a nástroj pro řízení přístupových oprávnění

Zvládání incidentů

- Zavede procesy, pravidla a postupy pro detekci, zaznamenávání a vyhodnocování kybernetických bezpečnostních událostí
- Přidělí odpovědnosti pro:
  - Detekci, zaznamenávání a vyhodnocování kybernetických bezpečnostních událostí
  - Koordinaci a zvládání kybernetických bezpečnostních incidentů
- Definuje a dodržuje pravidla a postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu
- Zajistí detekci kybernetických bezpečnostních událostí
- Zajistí, že uživatelé, administrátoři, osoby zastávající bezpečnostní role, další zaměstnanci a dodavatelé budou oznamovat neobvyklé chování technických aktiv a podezření na jakékoliv zranitelnosti

Zvládání incidentů

- Zajistí posuzování kybernetických bezpečnostních událostí, při kterém musí být rozhodnuto, zda mají být klasifikovány jako kybernetické bezpečnostní incidenty
- Zajistí zvládání kybernetických bezpečnostních incidentů podle stanovených postupů
- Přijímá bezpečnostní opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu
- Hlásí kybernetické bezpečnostní incidenty
- Vede záznamy o kybernetických bezpečnostních incidentech a o jejich zvládání
- Prošetří a určí příčiny kybernetického bezpečnostního incidentu
- Vyhodnotí účinnost řešení kybernetického bezpečnostního incidentu a na základě vyhodnocení stanoví nutná bezpečnostní opatření, popřípadě aktualizuje stávající bezpečnostní opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu.

Řízení kontinuity činností

- Stanoví metodiku pro provedení analýzy dopadů
- Pomocí analýzy dopadů vyhodnotí a dokumentuje možné dopady kybernetických bezpečnostních incidentů a zohlední hodnocení rizik, v rámci kterého posoudí možná rizika související s ohrožením kontinuity činností
- Na základě výstupů analýzy dopadů a hodnocení rizik stanoví cíle řízení kontinuity činností:
  - Minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu regulované služby
  - Doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb regulované služby
  - Bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání

Řízení kontinuity činností

- Stanoví politiku řízení kontinuity činností, která obsahuje naplnění cílů a stanoví práva a povinnosti administrátorů a osob zastávajících bezpečnostní role
- Vypracuje, aktualizuje a pravidelně testuje plány kontinuity činností a plány obnovy související s poskytováním regulované služby
- Realizuje bezpečnostní opatření pro zvýšení odolnosti

Audit kybernetické bezpečnosti

- Plán provádění auditu kybernetické bezpečnosti
- V rámci auditu kybernetické bezpečnosti:
  - Posuzuje zda byly zavedeny bezpečnostní opatření požadované zákonem o kybernetické bezpečnosti a touto vyhláškou
  - Posuzuje soulad zavedených bezpečnostních opatření s právními předpisy, vnitřními předpisy, jinými předpisy, smluvními závazky a nejlepší praxí vztahujícími se k regulované službě
  - Provádí a dokumentuje audit dodržování pravidel a postupů stanovených v bezpečnostní politice, včetně přezkoumání technické shody a dříve stanovených nápravných opatření
- Povinná osoba stanoví případná nápravná opatření

Audit kybernetické bezpečnosti

- Plán provádění auditu kybernetické bezpečnosti
- Provádění auditu:
  - Při významných změnách, v rámci jejich rozsahu
  - V pravidelných intervalech alespoň po 2 letech
  - V souladu s plánem auditu kybernetické bezpečnosti
- Audit kybernetické bezpečnosti musí být prováděn osobou vyhovující podmínkám stanoveným v § 6 odst. 4

Fyzická bezpečnost

- Povinná osoba
  - Předchází poškození, krádeži nebo zneužití aktiv nebo přerušení poskytování regulované služby
  - Stanoví fyzický bezpečnostní perimetr ohraničující oblast, ve které jsou uchovávány nebo zpracovávány informace a data, nebo ve které jsou umístěna technická aktiva regulované služby
  - Dokumentuje jednotlivé fyzické bezpečnostní perimetry podle písmena b) s ohledem na hodnocení umístěných technických aktiv a rozdělí je na jednotlivé úrovně fyzické ochrany

Fyzická bezpečnost

- U každého fyzického bezpečnostního perimetru stanoveného přijme relevantní bezpečnostní opatření fyzické ochrany s ohledem na jeho úroveň fyzické ochrany:
  - K zamezení neoprávněnému vstupu
  - K zamezení poškození a neoprávněným zásahům
  - K zajištění fyzické ochrany na úrovni objektů a v rámci objektů
  - Pro zajištění detekce narušení fyzického bezpečnostního perimetru
  - Eviduje vstupy a přístupy do fyzického bezpečnostního perimetru

Bezpečnost komunikačních sítí

- Povinná osoba pro ochranu bezpečnosti komunikační sítě, a to včetně jejího síťového perimetru:
  - Zajistí segmentaci komunikační sítě, včetně oddělení provozního, zálohovacího, vývojového, testovacího a jiného specifického prostředí
  - Zajistí řízení komunikace v rámci komunikační sítě
  - Zajistí řízení vzdáleného přístupu ke komunikační síti
  - Zajistí řízení vzdálené správy technických aktiv
  - V rámci řízení komunikace, vzdáleného přístupu a vzdálené správy povoluje pouze takovou komunikaci, která je nezbytná pro řádné zajištění regulované služby
  - Pomocí kryptografických algoritmů zajistí důvěrnost a integritu při přenosu informací a dat v rámci komunikační sítě
  - Využívá nástroj, který zajistí ochranu integrity komunikační sítě

Správa a ověřování identit

- Povinná osoba používá nástroj pro správu a ověření identity administrátorů, uživatelů a technických aktiv regulované služby
- Nástroj pro správu a ověření identity administrátorů, uživatelů a technických aktiv zajišťuje:
  - Ověření identity před zahájením jejich aktivit
  - Řízení počtu možných neúspěšných pokusů o přihlášení
  - Odolnost uložených a přenášených autentizačních údajů vůči hrozbám a zranitelnostem, které by mohly narušit jejich důvěrnost nebo integritu
  - Opětovné ověření identity po stanovené době nečinnosti
  - Dodržení důvěrnosti při vytváření výchozích autentizačních údajů při obnově přístupu
  - Centralizovanou správu identit

Správa a ověřování identit

- Povinná osoba pro ověření identity administrátorů, uživatelů a technických aktiv využívá autentizační mechanizmus, který je založený na **vícefaktorové autentizaci** s nejméně dvěma různými typy faktorů
- Povinná osoba do doby splnění požadavků pro ověření identity administrátorů, uživatelů nebo technických aktiv podle odstavce 3 vede evidenci technických aktiv, účtů a autentizačních mechanismů, které tyto požadavky nesplňují, a to včetně odůvodnění
- Povinná osoba do doby splnění požadavku pro ověření identity administrátorů, uživatelů nebo technických aktiv využívající autentizační mechanismus založený na vícefaktorové autentizaci s nejméně dvěma různými typy faktorů využívá autentizaci pomocí kryptografických klíčů nebo certifikátů

Správa a ověřování identit

- Povinná osoba do doby splnění požadavku pro ověření identity administrátorů, uživatelů a technických aktiv využívající autentizační mechanismus založený na autentizaci pomocí kryptografických klíčů nebo certifikátů,
  využívá nástroj pro autentizaci pomocí identifikátoru účtu a hesla a tento nástroj musí vynucovat následující pravidla:
  - Délky hesla alespoň
    12 znaků pro účty uživatelů
    17 znaků pro účty administrátorů
    22 znaků pro účty technických aktiv
  - Umožňující zadat heslo o délce alespoň 64 znakůP
  - Po ověření identity technických aktiv musí být výchozí heslo bezodkladně změněno a nové heslo musí být vytvořeno náhodným řetězcem složeným z malých a velkých písmen, číslic a speciálních znaků

Správa a ověřování identit

- Neomezující použití malých a velkých písmen, číslic a speciálních znaků
- Umožňující uživatelům a administrátorům změnu hesla, přičemž období mezi dvěma změnami hesla nesmí být kratší než 30 minut
- Povinné změny hesla v intervalu maximálně po 18 měsících
- Neumožňující uživatelům a administrátorům:
  1. zvolit si hesla ze slovníku nejčastěji používaných hesel,
  2. tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému nebo obdobným způsobem a
  3. opětovné použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel

Správa a ověřování identit

- Povinná osoba vytváří náhodné výchozí heslo nebo identifikátor sloužící k vytvoření nebo pro obnovení přístupu
- Povinná osoba bezodkladně zneplatní heslo nebo identifikátor sloužící k vytvoření nebo pro obnovení přístupu po jeho prvním použití nebo uplynutím nejvýše 24 hodin od jeho vytvoření
- Povinná osoba u administrátorského účtu určeného zejména pro případ obnovy po kybernetickém bezpečnostním incidentu, musí vynucovat následující pravidla
  - Bezodkladně vynutí změnu výchozí hesla
  - Heslo musí být vytvořeno náhodným řetězcem složeným z malých a velkých písmen, číslic a speciálních znaků
  - Délka hesla musí být alespoň 22 znaků,
  - Heslo musí být uloženo na bezpečném místě

Správa a ověřování identit

- S účtem a jeho heslem mohou manipulovat pouze pověřené osoby a to v nezbytně nutných případech
- Musí být vynucena změna hesla po jeho použití nebo v intervalu maximálně po 18 měsících
- Eviduje manipulaci a pokusy o manipulaci s tímto účtem a jeho heslem.

Řízení přístupových oprávnění

- Povinná osoba pro řízení přístupových oprávnění
  - Využívá centralizovaný nástroj s ohledem na vazby mezi aktivy
  - Řídí oprávnění pro přístup k jednotlivým aktivům
  - Řídí oprávnění pro čtení dat, zápis dat a změnu oprávnění

Detekce kybernetických a bezpečnostních událostí

- Povinná osoba používá nástroj pro detekci kybernetických bezpečnostních událostí, který v rámci komunikační sítě zajišťuje:
  - Ověření a kontrolu přenášených dat v rámci komunikační sítě a mezi komunikačními sítěmi
  - Ověření a kontrolu přenášených dat na síťovém perimetru komunikační sítě
  - Blokování nežádoucí komunikace
- Povinná osoba používá centrálně spravovaný nástroj s ohledem na vazby mezi aktivy pro detekci kybernetických bezpečnostních událostí, který u jednotlivých relevantních technických aktiv zajišťuje:
  - Nepřetržitou a automatickou ochranu před škodlivým kódem
  - Řízení a sledování používání vyměnitelných zařízení a datových nosičů
  - Řízení automatického spouštění obsahu vyměnitelných zařízení a datových nosičů

Detekce kybernetických a bezpečnostních událostí

- Řízení oprávnění ke spouštění kódu
- Řízení a sledování komunikace aplikací, jejich služeb a procesů
- Detekci na základě chování technického aktiva, uživatelů a aplikací

- Povinná osoba provádí pravidelnou a bezodkladnou aktualizaci nástroje používaného podle odstavce 1 a 2, a to včetně jeho nastavení a detekčních pravidel.

Zaznamenávání událostí

- Povinná osoba na základě hodnocení aktiv a bezpečnostních potřeb určí technická aktiva, u kterých je zaznamenávání bezpečnostních a relevantních provozních událostí prováděno
- Povinná osoba v souladu s odstavcem 1 zaznamenává bezpečnostní a relevantní provozní události
  - Detekované podle § 22
  - V rámci komunikační sítě
  - Na síťovém perimetru
  - Technických aktiv
- Povinná osoba aktualizuje rozsah technických aktiv v pravidelných intervalech a při významných změnách
- Povinná osoba zajišťuje nepřetržitou synchronizaci jednotného času technických aktiv

Zaznamenávání událostí

- Povinná osoba v rámci zaznamenávání událostí zaznamenává zejména následující informace o události:
  - Datum a čas včetně specifikace časového pásma
  - Typ činnosti
  - Jednoznačnou identifikaci technického aktiva, které činnost zaznamenalo
  - Jednoznačnou identifikaci účtu, pod kterým byla činnost provedena
  - Jednoznačnou identifikaci zařízení původce
  - Úspěšnost nebo neúspěšnost činnosti
- Povinná osoba v rámci zajištění důvěrnosti a integrity informací získaných zajistí jejich ochranu před neoprávněným čtením a jakoukoliv změnou

Zaznamenávání událostí

- Povinná osoba v rámci zaznamenávání událostí zaznamenává
  - Přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů
  - Provedení a neúspěšný pokus o provedení privilegované činnosti
  - Manipulace a neúspěšný pokus o manipulaci s účty, oprávněními a právy
  - Neprovedení činností v důsledku nedostatku přístupových práv nebo oprávnění
  - Zahájení a ukončení činností technických aktiv
  - Kritických a chybových hlášení technických aktiv
  - Přístup a neúspěšný pokus o přístup k záznamům událostí
  - Manipulaci a neúspěšný pokus o manipulaci se záznamy událostí
  - Změnu a neúspěšný pokus o změnu nastavení nástrojů pro zaznamenávání událostí
  - Další činností uživatelů, které mohou mít vliv na bezpečnost regulované služby.
- Povinná osoba používá centrální nástroj s ohledem na vazby mezi aktivy pro sběr a uchovávání záznamů událostí zaznamenaných podle odstavce 2 **(18 měsíců)**

Vyhodnocování kybernetických bezpečnostních událostí

- Povinná osoba používá nástroj pro nepřetržité vyhodnocování kybernetických bezpečnostních událostí detekovaných podle § 22 pro:
  - Sběr, vyhledávání a seskupování souvisejících záznamů za účelem detekce kybernetických bezpečnostních událostí
  - Nepřetržité poskytování informací o detekovaných kybernetických bezpečnostních událostech, včasné varování určených bezpečnostních rolí
  - Vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů

Vyhodnocování kybernetických bezpečnostních událostí

- Povinná osoba v rámci používání nástroje v souladu s odstavcem 1 zajistí:
  - Omezení případů nesprávného či nežádoucího vyhodnocování kybernetických bezpečnostních událostí
  - Pravidelnou aktualizaci nastavení nástroje včetně jeho pravidel pro detekci a vyhodnocování kybernetických bezpečnostních událostí
  - Pravidelnou aktualizaci pravidel pro nepřetržité poskytování informací o detekovaných kybernetických bezpečnostních událostech včetně včasného varování určených bezpečnostních rolí
- Povinná osoba využívá informací získaných nástrojem pro vyhodnocení kybernetických bezpečnostních událostí pro optimální nastavení systému řízení bezpečnosti informací regulované služby a zavádění bezpečnostních opatření.

Aplikační bezpečnost

- Povinná osoba pro zajištění bezpečnosti regulované služby užívá technická aktiva, která jsou výrobcem, dodavatelem nebo jinou osobou podporována a zajistí bezodkladné aplikování bezpečnostních aktualizací vydaných pro tato aktiva
- Povinná osoba do doby plnění odstavce 1 eviduje technická aktiva, která již nejsou výrobcem, dodavatelem nebo jinou osobou podporována a zavede bezpečnostní opatření, která zaručí obdobnou nebo vyšší úroveň bezpečnosti těchto technických aktiv
- Povinná osoba dále v rámci aplikační bezpečnosti zajistí trvalou ochranu aplikací, informací, transakcí a přenášených identifikátorů relací před:
  - Neoprávněnou činností
  - Popřením provedených činností

Aplikační bezpečnost

- Povinná osoba provádí pravidelné skenování zranitelnosti technických aktiv regulované služby
  - Z interní a externí komunikační sítě
  - Alespoň jednou ročně.
- Povinná osoba zohlední výsledky skenů zranitelnosti v rámci řízení rizik podle § 9 a zavádí bezpečnostní opatření na základě zjištěných výsledků
- Povinná osoba provádí penetrační testování technických aktiv s ohledem na hodnocení těchto aktiv a hodnocení rizik:
  - Z interní a externí komunikační sítě
  - Před jejich uvedením do provozu
  - V souvislosti s významnou změnou podle § 12 odst. 3

Aplikační bezpečnost

- Povinná osoba zohlední výsledky penetračního testování v rámci řízení rizik podle § 9 a zavádí bezpečnostní opatření na základě zjištěných výsledků
- Povinná osoba provede opětovné otestování (retest) nálezu zjištěného na základě provedeného skenování zranitelnosti nebo penetračního testování za účelem ověření funkčnosti zavedených bezpečnostních opatření
- Povinná osoba v souladu s odstavcem 6 písm. a) provádí pravidelně penetrační testování a to alespoň jednou za dva roky
- Povinná osoba v odůvodněných případech, pokud nemůže provést penetrační testování v rozsahu nebo intervalu stanoveném v odstavci 9, může rozdělit toto penetrační testování do systematických celků. V takovém případě je nutno provést penetrační testování v rozsahu stanoveném v odstavci 6 nejpozději do 5 let.

Kryptografické algoritmy

- Povinná osoba pro zajištění ochrany technických aktiv a jejich komunikace:
  - Používá aktuálně odolné kryptografické algoritmy
  - Prosazuje bezpečné nakládání s kryptografickými algoritmy
  - Zohledňuje doporučení a metodiky v oblasti kryptografických algoritmů vydané Úřadem, zveřejněné na jeho internetových stránkách
- Povinná osoba v souladu s odstavcem 1 zajišťuje bezpečnou:
  - Hlasovou, audiovizuální a textovou komunikaci, a to včetně e-mailové komunikace
  - Nouzovou komunikaci v rámci organizace

Kryptografické algoritmy

- Povinná osoba v případě využívání kryptografických klíčů a certifikátů pro ochranu technických aktiv a komunikační sítě používá:
  - Pouze aktuálně odolné kryptografických klíče a certifikáty
  - Systém správy klíčů a certifikátů, který
    1. zajistí generování, distribuci, ukládání, změny, omezení platnosti zneplatnění certifikátů a řádnou likvidaci kryptografických klíčů
    2. umožní kontrolu a audit
    3. zajistí důvěrnost a integritu kryptografických klíčů

Dostupnost regulované služby

- Povinná osoba zavede bezpečnostní opatření pro zajišťování dostupnosti regulované služby, kterými zajistí:
  - Dostupnost regulované služby podle cílů stanovených dle § 16
  - Odolnost regulované služby vůči hrozbám a zranitelnostem, které by mohly snížit její dostupnost
  - Redundanci aktiv nezbytných pro zajištění dostupnosti regulované služby
- Povinná osoba pro zajištění dostupnosti regulované služby v souladu s odstavcem 1 vytváří pravidelné zálohy nastavení technických aktiv, informací a dat nezbytných zejména pro účely obnovy regulované služby pro případ kybernetického bezpečnostního incidentu

Dostupnost regulované služby

- Povinná osoba u záloh vytvářených podle odstavce 2 zajistí:
  - Pravidelné testování jejich integrity, dostupnosti a obnovitelnosti
  - Dokumentování výsledků testů provedených podle odstavce 3 písm. a)
  - Ochranu ukládaných záloh a dat v nich obsažených před narušením jejich integrity a důvěrnosti, a to zejména šifrováním těchto záloh v souladu s § 26
  - Ochranu ukládaných záloh a dat v nich obsažených před narušením jejich dostupnosti
- Povinná osoba za účelem omezení šíření kybernetického bezpečnostního incidentu a snížení jeho dopadu odděluje zálohovací prostředí od jiných prostředí podle § 19 písm. a)

Zabezpečení průmyslových aktiv

- Povinná pro zajištění kybernetické bezpečnosti průmyslových, řídicích a obdobných specifických technických aktiv dále využívá nástroje a zavádí bezpečnostní opatření, která zajistí:
  - Omezení fyzického přístupu k průmyslovým, řídicím a obdobným specifickým technickým aktivům
  - Omezení oprávnění k přístupu k průmyslovým, řídicím a obdobným specifickým technickým aktivům
  - Segmentaci komunikačních sítí průmyslových, řídicích a obdobných specifických technických aktiv od jiných prostředí a segmentaci těchto komunikačních sítí podle § 19
  - Omezení vzdálených přístupů a vzdálené správy průmyslových, řídicích a obdobných specifických technických aktiv
  - Ochranu jednotlivých průmyslových, řídicích a obdobných specifických technických aktiv před využitím známých hrozeb a zranitelností
  - Obnovu dostupnosti průmyslových, řídicích a obdobných specifických technických aktiv

Lokalizace dat při zpracování v zahraničí

- Povinná osoba posoudí možný dopad kybernetického bezpečnostního incidentu na informace a data zpracovávaná v rámci stanového rozsahu a o tomto posouzení vyhotoví písemný záznam
- Povinná osoba v rámci stanoveného rozsahu zajistí, že na území České republiky jsou zpracovávány veškeré informace a data, u nichž kybernetický bezpečnostní incident může:
  - Vést ke zranění skupiny více než 2 500 lidí nebo přímému ohrožení nebo ztrátě života skupiny více než 250 lidí
  - Vést k omezení nebo narušení zpracování osobních údajů, které je nezbytné pro zajišťování obranných a bezpečnostních zájmů České republiky
  - Vést k závažnému a dlouhodobému narušení schopnosti vyšetřovat trestnou činnost nebo zpochybnění soudního řízení v rámci orgánů činných v trestním řízení
  - Negativně ovlivnit nebo poškodit diplomatické vztahy České republiky

Lokalizace dat při zpracování v zahraničí

- Vést k finančním ztrátám přesahujícím 10 % běžných výdajů ročního rozpočtu povinné osoby a tyto ztráty odpovídají částce 10 000 000 Kč a vyšší, nebo může způsobit hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo
- Způsobit dotčení prvku kritické infrastruktury provozovaného povinnou osobou a může:
  1. zapříčinit hromadné nepokoje nebo jinak závažně narušit veřejný pořádek s celostátními dopady,
  2. narušit řádné fungování části nebo celé povinné osoby, přičemž může závažně omezit nebo zastavit provádění důležitých činností povinné osoby a narušit řízení, poškodit rozvoj nebo poškodit prosazování cílů a zájmů povinné osoby,
  3. negativně ovlivnit vztahy s jinými organizacemi nebo vztahy s veřejností a negativní následky mohou být dlouhodobě mezinárodní, nebo
  4. dojít k rozsáhlému omezení poskytování nezbytných služeb nebo jinému závažnému zásahu do každodenního života postihujícího více než 125 000 osob.

Lokalizace dat při zpracování v zahraničí

- Povinnost stanovená v odst. 1 se nevztahuje na uchovávání zašifrovaných informací a dat na území členských států Evropské unie, Evropského sdružení volného obchodu, Organizace Severoatlantické smlouvy, Organizace pro ekonomickou spolupráci a rozvoj v případě, že tyto informace a data byly zašifrovány v souladu s § 26 této vyhlášky povinnou osobou
- Povinná osoba v rámci stanoveného rozsahu zajistí, že na území členských států Evropské unie, Evropského sdružení volného obchodu, Organizace Severoatlantické smlouvy nebo Organizace pro ekonomickou spolupráci a rozvoj jsou zpracovávány veškeré informace a data u nichž kybernetický bezpečnostní incident může:
  - Vést ke zranění skupiny více než 100 lidí a nejvíce 2 500 lidí nebo přímému ohrožení nebo ztrátě života jednotlivce nebo skupiny nejvíce 250 lidí
  - Vést k narušení vyšetřování trestné činnosti nebo soudního řízení v rámci orgánů činných v trestním řízení
  - Zapříčinit hromadné nepokoje nebo jinak závažně narušit veřejný pořádek s regionálními dopady

Lokalizace dat při zpracování v zahraničí

- Negativně ovlivnit obraz České republiky ve světě
- Narušit řádné fungování části nebo celé povinné osoby, přičemž může závažně omezit nebo zastavit provádění důležitých činností povinné osoby a narušit řízení, poškodit rozvoj nebo poškodit prosazování cílů a zájmů povinné osoby
- Negativně ovlivnit vztahy s jinými částmi povinné osoby, jinými organizacemi nebo vztahy s veřejností, avšak negativní následky mohou být nejvýše celostátní nebo krátkodobě mezinárodní
- Vést k finančním ztrátám ve výši přesahující 5 % a maximálně 10 % běžných výdajů ročního rozpočtu povinné osoby a tyto ztráty odpovídají částce 1 000 000 Kč a vyšší, nebo může způsobit hospodářské ztráty státu ve výši mezi 0,1 % a 0,5 % hrubého domácího produktu
- Způsobit omezení, narušení nebo nedostupnost služeb pro více než 50 000 osob

Lokalizace dat při zpracování v zahraničí

- Negativně ovlivnit regulovanou službu, která naplňuje dvě a více z níže uvedených kritérií:
  - 1. v rámci regulované služby se zpracovávají zvláštní kategorie osobních údajů nebo údaje vysoce osobní povahy, zejména finanční údaje o stavu majetku, výši finančních prostředků, dluzích nebo půjčkách nebo platební morálce, záznamy o historii soukromých volání subjektů údajů, údaje z \elektronické pošty subjektů údajů a podobně
  - 2. v rámci regulované služby dochází ke zpracování osobních údajů, kterým je dotčeno nebo lze důvodně předpokládat, že bude dotčeno více než 10 000 subjektů údajů
  - 3. v rámci regulované služby dochází k automatizovanému rozhodování, které se dotýká subjektu údajů.

Deprese?

- ***Váš názor na regulaci?***

Režim nižších povinností – bezpečnostní opatření

- Zajišťování minimální úrovně kybernetické bezpečnosti:
  - Stanoví strategické cíle zajišťování minimální úrovně kybernetické bezpečnosti
  - Na základě strategických cílů zajišťování minimální úrovně kybernetické bezpečnosti a bezpečnostních potřeb zavede bezpečnostní opatření směřující k zajištění bezpečnosti regulované služby
  - Vytvoří a schválí bezpečnostní politiku v oblasti zajišťování minimální úrovně kybernetické bezpečnosti, která obsahuje hlavní zásady, strategické cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení kybernetické bezpečnosti, a na základě bezpečnostních potřeb stanoví bezpečnostní politiku a bezpečnostní dokumentaci v dalších oblastech

Režim nižších povinností – bezpečnostní opatření

- **Zajistí pravidelné vyhodnocení účinnosti zajišťování minimální úrovně kybernetické bezpečnosti, které obsahuje:**
  - **Vyhodnocení strategických cílů zajišťování minimální úrovně kybernetické bezpečnosti stanovených podle písmena a)**
  - **Posouzení naplňování plánu zavádění bezpečnostních opatření zpracovaného podle odstavce 2 písm. a)**
  - **Posouzení výsledků kontrol provedených v oblasti kybernetické bezpečnosti**
  - **Výsledky předchozích vyhodnocení účinnosti zajišťování minimální úrovně kybernetické bezpečnosti provedených podle písmene d)**
  - **Posouzení dopadů kybernetických bezpečnostních incidentů s významným dopadem na poskytované služby podle § 13**
  - **Posouzení změn, které mohou mít negativní dopad na zajišťování minimální úrovně kybernetické bezpečnosti podle § 11**

Režim nižších povinností – bezpečnostní opatření

- Na základě vyhodnocení účinnosti zajišťování minimální úrovně kybernetické bezpečnosti podle písmene d) zpracuje zprávu o přezkoumání zajišťování minimální úrovně kybernetické bezpečnosti
- Aktualizuje zajišťování minimální úrovně kybernetické bezpečnosti a příslušnou dokumentaci na základě:
  - Zjištění z kontrol provedených v oblasti kybernetické bezpečnosti
  - Výsledků vyhodnocení účinnosti zajišťování minimální úrovně kybernetické bezpečnosti
  - Dopadů kybernetických bezpečnostních incidentů s významným dopadem na poskytované služby

Režim nižších povinností – bezpečnostní opatření

- Zpracuje přehled bezpečnostních opatření, který obsahuje přehled všech bezpečnostních opatření požadovaných touto vyhláškou, která:
  - Nebyla aplikována, včetně odůvodnění a přehledu přijatých náhradních bezpečnostních opatření
  - Byla aplikována, včetně způsobu plnění.
- Povinná osoba v souladu se strategickými cíli zajišťování minimální úrovně kybernetické bezpečnosti stanovenými podle odstavce 1 písm. a) a s plánem zavádění bezpečnostních opatření zavádí bezpečnostní opatření.

Režim nižších povinností – bezpečnostní opatření

- Povinnosti vrcholového vedení:
  - Vrcholové vedení povinné osoby s ohledem na zajišťování minimální úrovně kybernetické bezpečnosti:
    - Se prokazatelně účastní školení podle § 10 odst. 2 písm. a)
    - Zajistí stanovení bezpečnostní politiky a strategických cílů zajišťování minimální úrovně kybernetické bezpečnosti
    - Zajistí dostupnost zdrojů potřebných pro zajišťování minimální úrovně kybernetické bezpečnosti v souladu s plánem zavádění bezpečnostních opatření
    - Informuje zaměstnance o významu zajišťování minimální úrovně kybernetické bezpečnosti a významu dosažení shody s jeho požadavky se všemi dotčenými stranami
    - Zajistí podporu k dosažení zamýšlených strategických cílů
    - Se podílí na vypracování analýzy dopadů podle § 14,

Režim nižších povinností – bezpečnostní opatření

- Prosazuje neustálé zlepšování zajišťování minimální úrovně kybernetické bezpečnosti
- Určí osoby zastávající bezpečnostní role a stanoví příslušné pravomoci
- Podporuje bezpečnostní role v oblastech její odpovědnosti
- Přijímá bezpečnostní opatření vedoucí:
  - Ke kontinuálnímu zlepšování zajišťování minimální úrovně kybernetické bezpečnosti a
  - K dosažení stanovených strategických cílů v oblasti kybernetické bezpečnosti
- Vrcholové vedení se prokazatelně seznamuje
  - Se zprávou o přezkoumání zajišťování minimální úrovně kybernetické bezpečnosti
  - S výsledky analýzy dopadů v souladu s § 14
  - S výsledky kontrol provedených v oblasti kybernetické bezpečnosti

Režim nižších povinností – bezpečnostní opatření

- Vrcholové vedení v rámci zajišťování minimální úrovně kybernetické bezpečnosti určí osobu, která bude zastávat bezpečnostní roli:
  - Odpovědnou za kybernetickou bezpečnost včetně stanovení jejích povinností, odpovědností a pravomocí
  - Garanta aktiva
- Vrcholové vedení zajistí zastupitelnost osoby odpovědné za kybernetickou bezpečnost

Režim nižších povinností – bezpečnostní opatření

- Řízení bezpečnostní politiky a bezpečnostní dokumentace:
  - Povinná osoba v rámci řízení bezpečnostní politiky a bezpečnostní dokumentace:
    - Stanoví bezpečnostní politiku a vede bezpečnostní dokumentaci zahrnující oblasti uvedené v příloze č. 3 k této vyhlášce
    - V provozní dokumentaci stanoví pravidla a postupy, které zohledňují relevantní oblasti z bezpečnostní politiky a bezpečnostní dokumentace
  - Povinná osoba dodržuje pravidla a postupy stanovené podle odstavce 1
  - Povinná osoba pravidelně přezkoumává bezpečnostní politiku a bezpečnostní dokumentaci, zajistí jejich aktuálnost a zohlednění jejich relevantních oblastí v provozní dokumentaci
  - Povinná osoba určí osobu odpovědnou za pravidelný přezkum a aktualizaci bezpečnostní politiky a bezpečnostní dokumentace a zohlednění jejich relevantních oblastí v provozní dokumentaci podle odstavce 3

Režim nižších povinností – bezpečnostní opatření

- **Bezpečnostní politika a bezpečnostní dokumentace musí být řízeny tak, aby byly**
  - **Dostupné v elektronické nebo listinné podobě**
  - **Komunikovány v rámci povinné osoby**
  - **Přiměřeně dostupné dotčeným stranám**
  - **Chráněny z pohledu důvěrnosti, integrity a dostupnosti**
  - **Vedeny tak, aby informace v nich obsažené byly úplné, čitelné, správné, snadno identifikovatelné a vyhledatelné**

Režim nižších povinností – bezpečnostní opatření

- Řízení aktiv
  - Povinná osoba v souladu s provedenou identifikací a evidencí aktiv:
  - Stanoví metodiku pro identifikaci a hodnocení aktiv alespoň v rozsahu uvedeném v příloze č. 1 k této vyhlášce, včetně stanovení úrovní aktiv
  - Určí a eviduje garanty aktiv
  - Hodnotí primární aktiva z hlediska důvěrnosti, integrity a dostupnosti a zařadí je do jednotlivých úrovní podle písmene a)
  - V rámci hodnocení primárních aktiv posuzuje relevantní oblasti uvedené v příloze č. 1 k této vyhlášce
  - Identifikuje a eviduje relevantní vazby mezi aktivy
  - Hodnotí podpůrná aktiva a zohledňuje přitom zejména vazby na primární aktiva,

Režim nižších povinností – bezpečnostní opatření

- **Pro jednotlivé úrovně primárních aktiv podle písmene a) stanovuje a zavádí pravidla ochrany nutná pro zabezpečení jejich důvěrnosti, dostupnosti a integrity, které obsahují zejména přípustné způsoby používání aktiv:**
- **Pravidla pro manipulaci s aktivy**
- **Pravidla pro klasifikaci informací**
- **Pravidla pro označování aktiv**
- **Pravidla správy výměnných médií**
- **Pravidla pro bezpečné elektronické sdílení a fyzické přenášení aktiv**
- **Pravidla pro určení způsobu likvidace informací a dat a jejich kopií a likvidace technických aktiv, která jsou nosiči informací a dat s ohledem na úroveň aktiv v souladu s přílohou č. 2 k této vyhlášce.**

Režim nižších povinností – bezpečnostní opatření

- Řízení dodavatelů
  - Povinná osoba při uzavírání smlouvy s dodavateli související se správou nebo dodávkou technických aktiv, která jsou podle hodnocení těchto aktiv významná pro regulovanou službu:
  - Stanoví přiměřená pravidla zohledňující požadavky zajišťování minimální úrovně kybernetické bezpečnosti pro tyto dodavatele na základě zjištěných bezpečnostních potřeb a pravidelně tato pravidla aktualizuje
  - Seznamuje tyto dodavatele s pravidly podle písmene a) a vyžaduje plnění těchto pravidel
  - Identifikuje a eviduje tyto dodavatele

Režim nižších povinností – bezpečnostní opatření

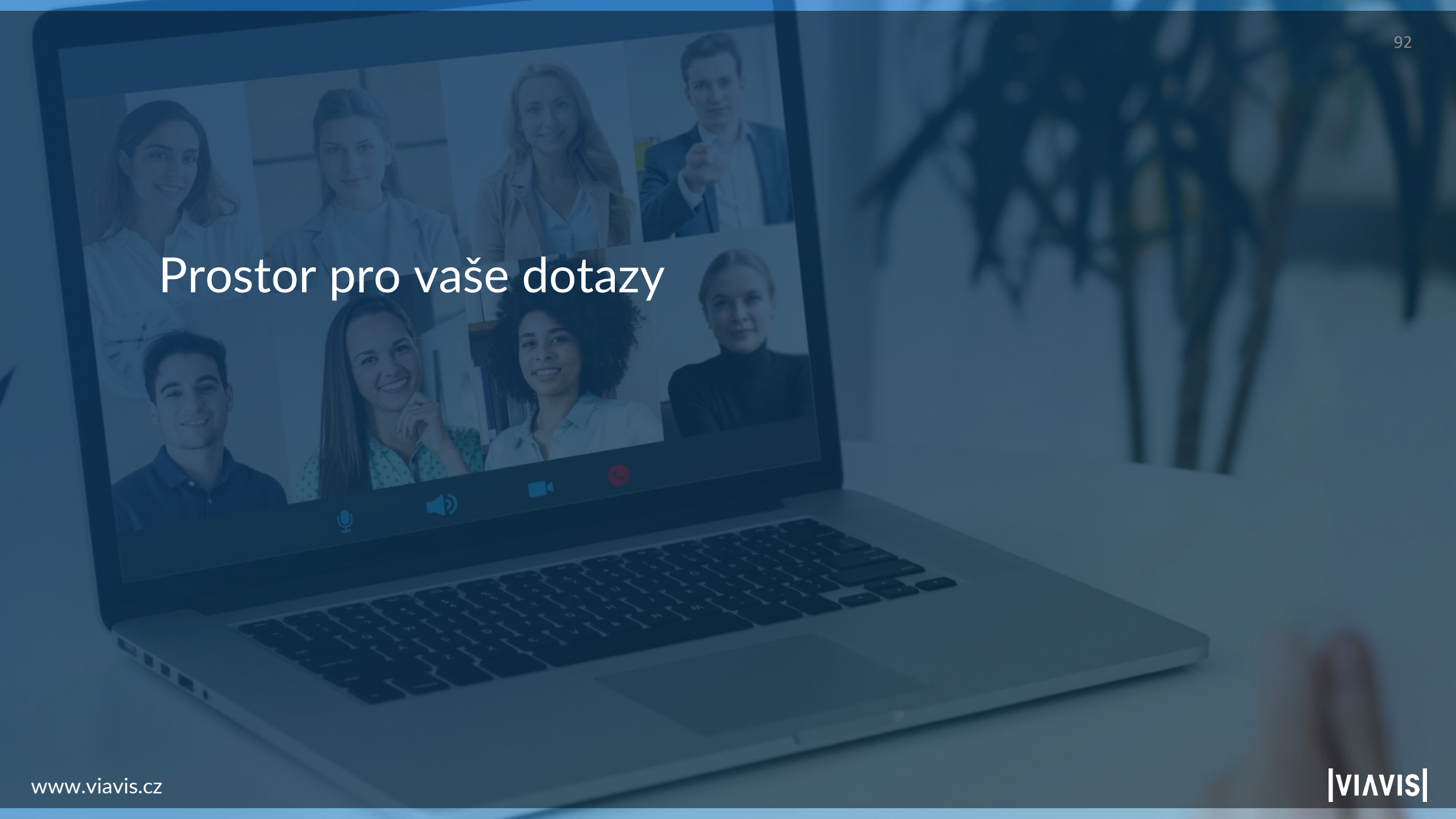
- Zajistí, aby smlouvy s těmito dodavateli obsahovaly zejména relevantní oblasti uvedené v příloze č. 4 k této vyhlášce
- Povinná osoba u dodavatelů podle odstavce 1
  - Provádí pravidelné vyhodnocení a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany
  - Zajistí řešení nedostatků zjištěných podle písmene a).

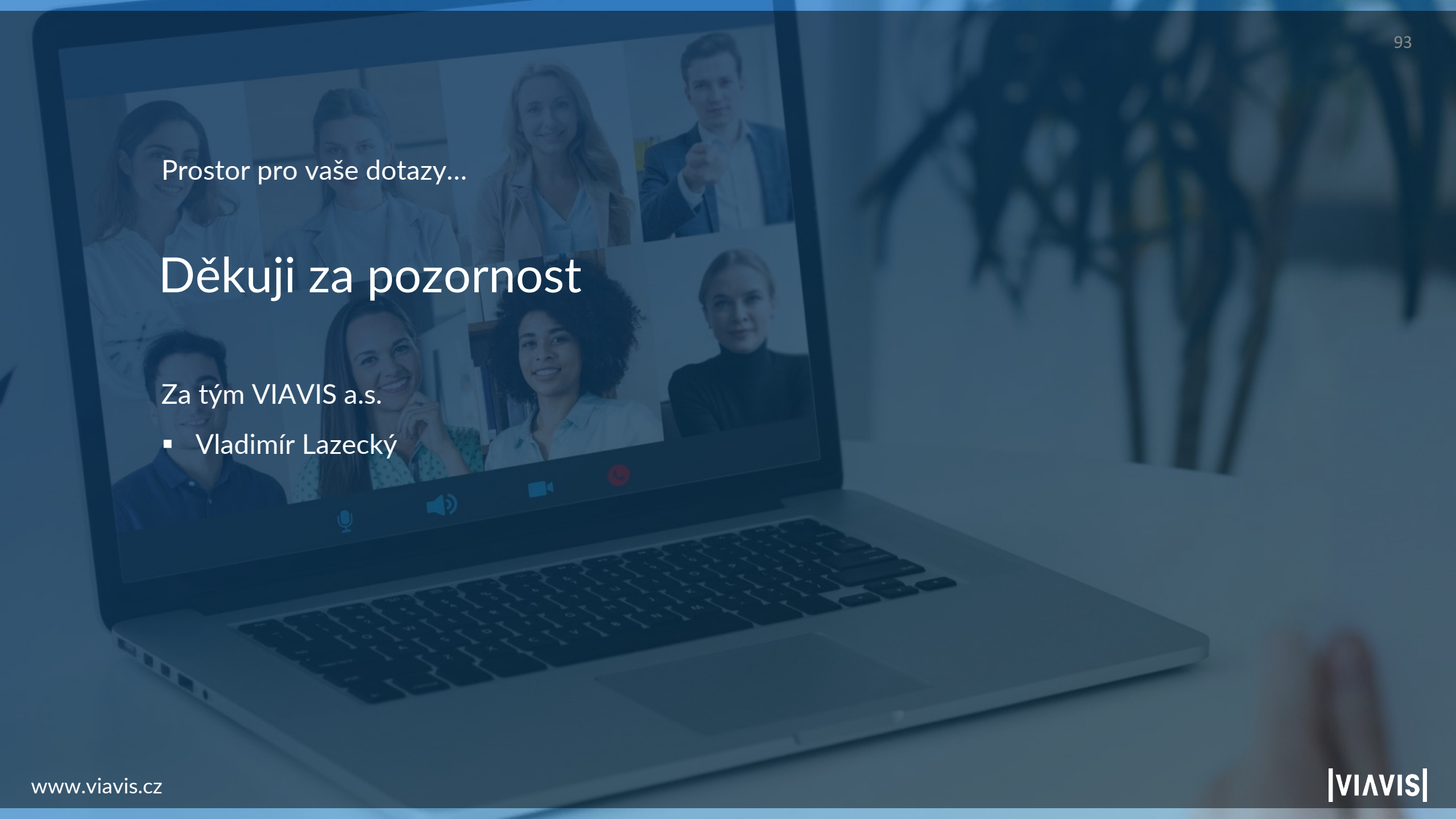
Pojďme si to zkusit

- Soukromá s.r.o.
- Městský úřad
- Vysoká škola

- Navrhněte projekt NIS2 Compliance
  - Jak budete postupovat?

Prostor pro vaše dotazy





Prostor pro vaše dotazy…

Děkuji za pozornost

Za tým VIAVIS a.s.

- Vladimír Lazecký