VIAVIS střežíme podstatné

Standardy, regulace, best practices

Kybernetická a informační bezpečnost I

Vladimír Lazecký

vladimir.lazecky@viavis.cz

Cíl přednášky

- **Přehled standardů pro informační a kybernetickou bezpečnost**
- **Proč?**
  - Nevymýšlet vymyšlené
  - Vychází z nich zákonná úprava

Základní pojmy – řízení x management

- Řízení
  - Ekonomické řízení
  - Procesní řízení
  - Projektové řízení
- Systém managementu – management ve smyslu „zvládání“
  - Risk management
  - Oblast personální, HR
  - Systém managementu bezpečnosti (objektová, personální, požární, …)
  - ITIL (IT service management, ISO 20000)
  - ISMS (ISO 27000)

ITIL /ISO 20000

- Procesy určují požadavky na IT služby, které pak slouží k zajištění chodu procesů
- Podniková strategie určuje podobu procesů
  - *Jak tomu rozumíte?*

ITIL / ISO 20000

- **ITSM (IT Service Management) = řízení služeb informačních technologií**
  - Definice a popis služby poskytovaných ICT
  - Pravidla pro užívání služeb
  - Řízení služeb na operativní, taktické a strategické úrovni
- **ITIL (Information Technology Infrastructure Library)**
  - Soubor prověřených postupů, které umožňují plánovat, využívat a zkvalitňovat využití ICT
  - Metodika založená na procesním řízení
- **ISO 20000**
  - Mezinárodní norma definující požadavky a řízení služeb IT
  - Část 1 – specifikace, část 2 – soubor postupů

ITIL - Information Technology Infrastructure Library

- **Části ITIL:**
  - Podnikatelský pohled (Business Perspectives)
  - Správa aplikací IT (Application Management)
  - Dodávka IT služeb (IT Services Delivery) => ITSM
  - Podpora IT služeb (IT Services Support) => Správa IT infrastruktury (IT Infrastructure Management)
  - Řízení IT projektů (IT Project Management)

ITIL

- **ITIL obsahuje 26 procesů, z nichž klíčové jsou následující:**
  - Incident management
  - Event management
  - Request fulfilment
  - Access management
  - Problem management
  - Service asset and configuration management
  - Change management
  - Release and deployment management
  - IT service continuity management
  - Capacity management
  - Availability management
  - Service level management
  - Service catalogue management
  - Financial management for IT services

ITIL

- **Service Desk -** účelem je poskytnout u jedno místo pro adresování požadavků
- **Configuration Management** - proces, jehož výstupem je model infrastruktury pomocí identifikace, řízení, správy a verifikace všech konfiguračních položek
- **Incident management -** proces pro co nejrychlejší obnovení služby a minimalizaci důsledků výpadků
- **Problem Management -** proces zjišťování příčin incidentů
- **Change Management -** proces efektivního a rychlého řízení změn
- **Release Management -** proces zajišťující distribuci a nasazení změny do ICT architektury

ITIL

- **Service Level Management** - plánování, koordinace, návrh, uzavírání a vyhodnocování smluv o poskytování servisní podpory (SLA)
- **Capacity Management** - zajištění trvale dostatečné kapacity infrastruktury
- **Availability Management** - dosažení stanovené úrovně dostupnosti IT služeb
- **IT Service Continuity Management** - řízení schopnosti poskytování definované úrovně služeb při výpadku
- **Financial Management for IT Services** – evidence a řízení nákladů na IT služby

ISO 20000

- Mezinárodní norma definující požadavky a řízení služeb IT
  - Část 1 – specifikace
  - Část 2 – soubor postupů
  - Norma definuje celkem 19 procesů, z nichž se skládá systém řízení služeb

ISO 20000

- Systém řízení služeb:
  1. Ustanovení systému řízení služeb a jeho zlepšování
  2. Řízení dokumentace
  3. Řízení zdrojů
  4. Plánování nových nebo změněných služeb
  5. Návrh a vývoj nových nebo změněných služeb
  6. Přechod na novou nebo změněnou službu
  7. Management incidentů
  8. Management problémů
  9. Management konfigurací
  10. Management změn

ISO 20000

- Systém řízení služeb:
  11. Proces uvolnění
  12. Management kontinuity a dostupnosti služeb
  13. Management kapacit
  14. Management úrovně služeb
  15. Rozpočtování a účtování pro IT služby
  16. Management bezpečnosti informací
  17. Management vztahů s byznysem
  18. Management vztahů s dodavateli
  19. Výkazy o službách

ISMS - Information Security Management System

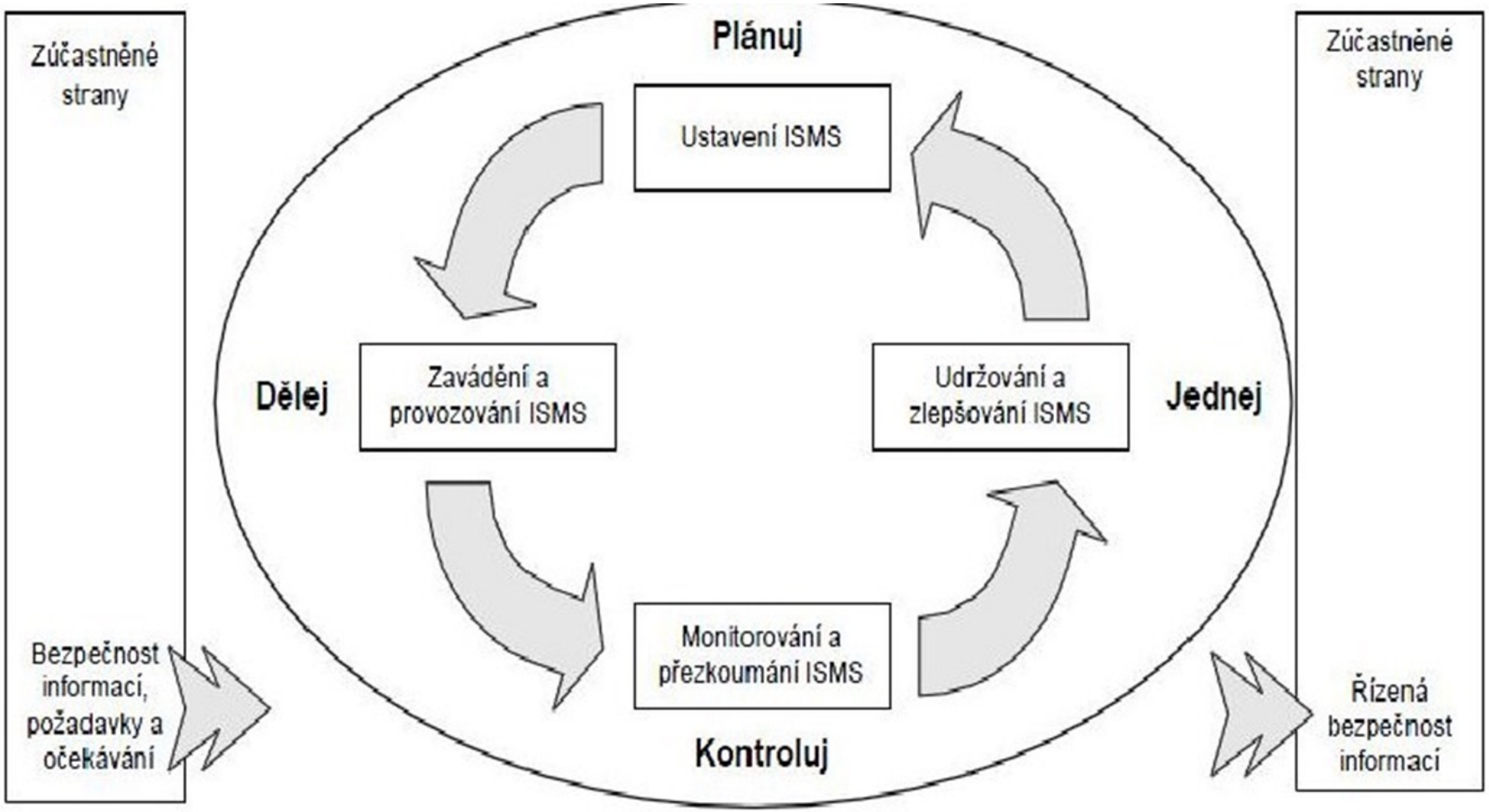
- Důvody pro ISMS
  - ISMS - Systém managementu bezpečnosti informací
  - Management bezpečnosti informací – zvládání, spíše než řízení
- ISMS:
  - Soustava organizačních a technických opatření k eliminaci rizik
  - Rizika spojená se zachováním důvěrnosti, integrity a dostupnosti informací
  - Pokrytí hrozeb s vyšší mírou rizika vhodnými protiopatřeními

- **ISMS nemusí být cílem certifikovat, je ale dobrým východiskem, jak informační bezpečnost řídit (management) systematicky a efektivně**

PDCA cyklus

- **P(lan), D(o), C(heck), A(ct)**
- Kolbův cyklus učení (zkušenost-reflexe-pojem-experimentální ověření)
  - W. Edwards Deming, Walter A. Shewhart
  - Demingův (Hemmingsův) PDCA model
- Jednoduchá metoda zlepšování s univerzálním použitím
- Plánovat, realizovat, přezkoumat, reagovat
- Total (nejen) Quality Management

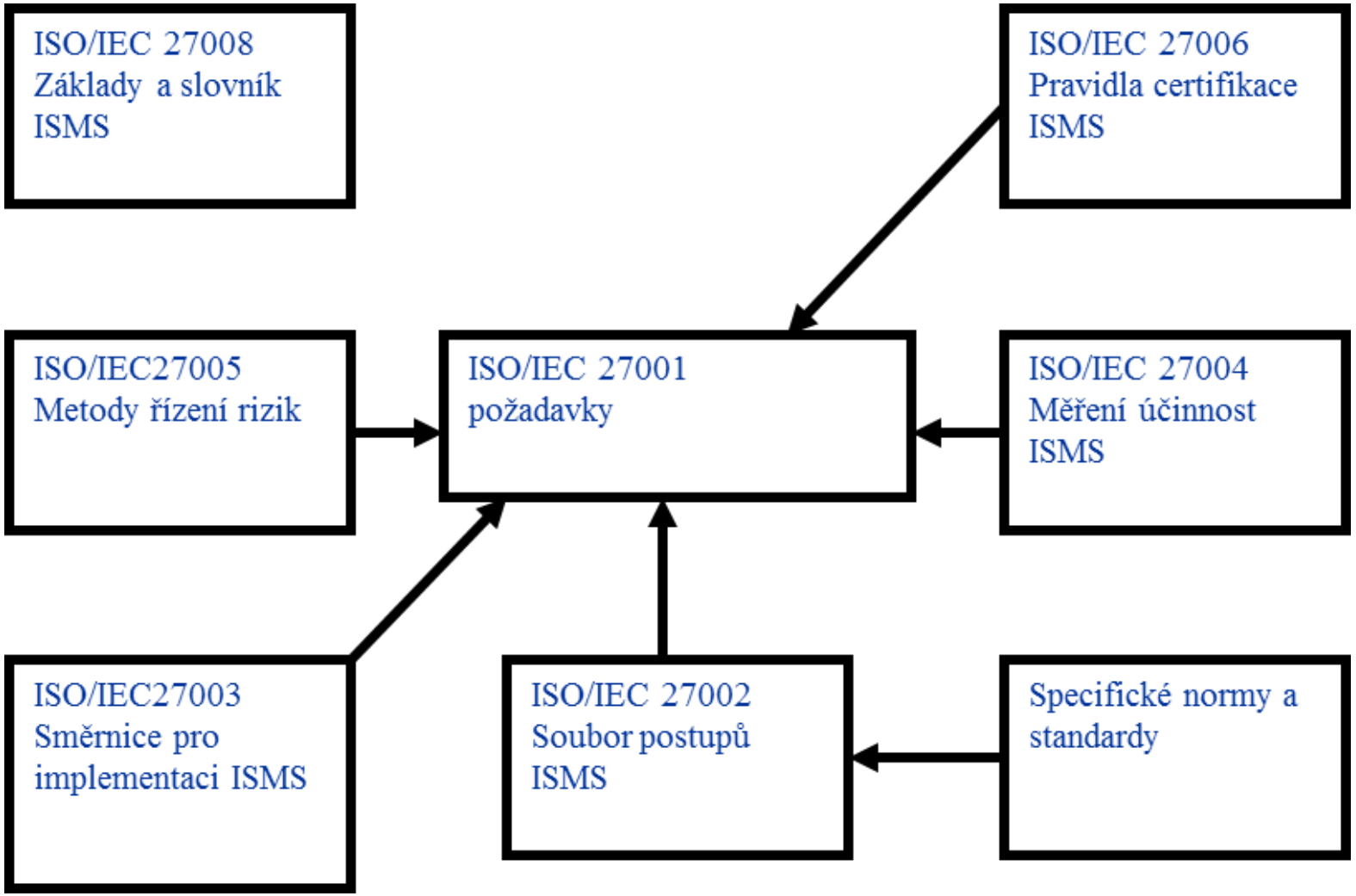
PDCA cyklus


Zúčastněné strany
Bezpečnost informací, požadavky a očekávání
Plánuj
Ustavení ISMS
Dělej
Zavádění a provozování ISMS
Udržování a zlepšování ISMS
Jednej
Monitorování a přezkoumání ISMS
Kontroluj
Zúčastněné strany
Řízená bezpečnost informací

PDCA v ISMS

- **Plánuj (ustavení ISMS)**
  - Ustavení politiky ISMS, cílů, procesů
  - Ustavení managementu rizik
  - Ustavení navazujících částí – BCP, IcM, CHM
- **Dělej (zavádění a provozování ISMS)**
  - Zavedení a využívání politiky ISMS, opatření, procesů a postupů.
- **Kontroluj (monitorování a přezkoumání ISMS)**
  - Měření výkonu vůči politice ISMS, cílům
- **Jednej (udržování a zlepšování ISMS)**
  - Přijetí opatření k nápravě a preventivních opatření

ISMS standardy



ISMS standardy

- 27000 – Definice pojmů a terminologický slovník
- 27001 - Systém řízení bezpečnosti informací (ISMS)
- 27002 – Soubor postupů pro řízení bezpečnosti informací
- 27003 - Směrnice pro implementaci systému řízení bezpečnosti informací
- 27004 - Řízení bezpečnosti informací – Měření
- 27005 - Řízení rizik bezpečnosti informací
- 27006 - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací
- 27007 – Směrnice pro audit systémů řízení bezpečnosti informací

Ustavení ISMS

- **Určení rozsahu a hranice ISMS (scope)**
- Definice politiky ISMS
- **Stanovení přístupu k hodnocení rizik:**
  - **Identifikace rizik**
  - Analýza a hodnocení rizik
  - Identifikace a hodnocení variant pro zvládání rizik
  - Výběr cílů a opatření pro zvládání rizik
  - Získání souhlasu vedení s navrhovanými zbytkovými riziky
- **Získání povolení ze strany vedení k zavedení a provozu ISMS**
- **Prohlášení o aplikovatelnosti**

Zavádění a provozování ISMS

- Formulace plánu zvládání rizik
- Zavedení plánu zvládání rizik v život
- Zavedení vybraných bezpečnostní opatření
- Určení způsobu měření účinnosti vybraných opatření
- Programy školení a programy zvyšování informovanosti

- Řízení provozu ISMS
- Řízení zdrojů ISMS
- Zavedení postupů pro rychlou detekci a reakci na bezpečnostní incidenty

Monitorování a přezkoumání ISMS

- Kontinuální monitorování
- Pravidelné přezkoumání účinnosti ISMS
- Měření účinnosti zavedených opatření
- V plánovaných intervalech hodnocení rizik a přezkoumání zbytkových rizika a úroveň akceptovatelného rizika

Udržování a zlepšování ISMS

- Zavádění identifikovaných zlepšení ISMS
- Nápravné a preventivní činnosti
- Návrhy na zlepšení na požadované úrovni detailu se všemi zainteresovanými stranam
- Analýza zlepšení – musí vést k předpokládaným cílům

Struktura dokumentace ISMS

- Rozsah a hranice ISMS
- Politika ISMS
- Definice a popis přístupu k hodnocení rizik
- Identifikace rizik
- Analýza a vyhodnocení rizik
- Identifikace a varianty pro zvládání rizik
- Cíle opatření a bezpečnostní opatření pro zvládání rizik (viz příloha A)
- Akceptace rizik
- Získání povolení k provozování ISMS v rámci organizace
- Prohlášení o aplikovatelnosti

Struktura dokumentace ISMS

- Bezpečnostní strategie
- Bezpečnostní politika
- Metodické dokumenty
    - Metodika Risk Managementu
- Akty interního řízení
- Směrnice (vazba na ITIL):
    - Pro uživatele
    - Pro řízení provozu
    - Pro řízení přístupu
    - Pro zálohování
    - ...

Bezpečnostní strategie

- Základní dokument bezpečnosti celku

- Všechny oblasti bezpečnosti
- Cíle
- Strategie
- Význam bezpečnosti pro fungování celku
- Souhlas a podpora vedení
- Často součást statutu, podnikatelského záměru, strategického plánu apod.

Politika informační bezpečnosti

- **Základní dokument informační bezpečnosti:**
  - Cíle
  - Strategie
  - Organizační aspekty
  - Role
  - Management bezpečnosti
  - Procesy
  - Řízení rizik
  - Správa systémů a aplikací
  - Helpdesk
  - Vývoj a údržba aplikací
  - Řízení změn
  - Vztahy mezi politikami
  - Vydávání a revize politik

Risk management

- Důvody pro RM (ochrana aktiv, OOÚ, OT, přiměřenost personálních opatření, …)
- Ochrana osob a majetku může být funkční pouze tehdy, pokud jsou známy:
  - Hodnoty - aktiva
  - Hrozby - před čím je třeba chránit - analýza rizik,
  - Protiopatření – jak chránit
  - Náklady – optimalizace nákladů
- Risk management – nejen v informační bezpečnosti
  - PO, BOZP, finanční rizika, personální rizika …
  - RM v oblasti finančních rizik, strategických rizik
  - RM: možnosti zobecnění
- **Nástrojem RM je analýza rizik**

Analýza rizik, řízení rizik

- **AR odpovídá na otázky:**
  - Co vlastním a jakou to má hodnotu?
  - Jak o tuto hodnotu mohu přijít?
- **Aktiva:**
  - Zjištění hodnoty aktiva
  - Identifikace a hodnocení hrozeb:
    - Zásahy vyšší moci
    - Organizační nedostatky
    - Technická selhání
    - Lidská selhání
    - Úmyslná škodlivá činnost

Analýza rizik, řízení rizik

- **Hodnocení míry zranitelnosti:**
  - Účinnost stávajících ochranných opatření
  - Hodnocení frekvence hrozeb
  - Hodnocení účinnosti navržených protiopatření

Základní pojmy analýzy rizik

- Aktivum
- Hodnota
- Hrozba
- Zranitelnost
- Četnost
- Dopad hrozby
- Riziko
- Ochranné opatření
- Účinnost

Aktivum

- **Aktivum - všechno, co má hodnotu**
  - Informační aktivum – samotná informace
  - Hmotná aktiva
  - Nehmotná aktiva (např. programy, data, morálka pracovníků, pověst ...)
  - Systémy aktiv - spojují jak hmotné, tak nehmotné prvky – lidé, informační systémy
- **Primární aktiva**
  - Informace, nebo služby kterou zpracovává nebo poskytuje IS
  - Př: řízení výroby, personální systém…
- **Podpůrná aktiva** – aktiva potřebná pro provoz primárních aktiv- lidé, HW, SW…

Hodnota aktiva

- Základní charakteristika aktiva
- Bez hodnoty nemá smysl ochrana
- Hodnota aktiva:
  - Objektivní vyjádření ceny
  - Subjektivním ocenění důležitosti (kritičnosti) aktiva
  - Kombinaci obou přístupů
  - Hodnota aktiva je relativní v závislosti na úhlu pohledu hodnocení
  - Hodnota by měla být vyjádřena cenou (výhoda pro hodnocená nákladů protiopatření)
  - ***Jaká je hodnota aktiva – lidského života?***

Hrozba

- **Hrozba** - síla, událost nebo aktivita, která může způsobit škodu na aktivech
- Hrozby - např. požár, přírodní katastrofa, krádež zařízení, získání přístupu k informacím neoprávněnou osobou, chyba obsluhy apod.
- **Dopad hrozby** - škoda, kterou způsobí hrozba při jednom působení na aktivum
  - Lze jej odvodit od ztrát, do kterých jsou zahrnuty náklady na znovuobnovení činnosti aktiva nebo
  - Náklady na odstranění následků škod způsobených hrozbou
- Základní charakteristikou hrozby je její úroveň

Zranitelnost

- **Zranitelnost** - nedostatek, slabina nebo stav aktiva, který využívá hrozba
  - Je vlastností aktiva
  - Vyjadřuje, jak citlivé je aktivum na působení dané hrozby
  - Zranitelnost vznikne všude tam, kde dochází k interakci mezi hrozbou a aktivem
- Základní charakteristikou zranitelnosti je úroveň
- **Úroveň zranitelnosti aktiva** se hodnotí podle citlivosti (náchylnost aktiva být poškozeno danou hrozbou) a kritičnosti (důležitost aktiva pro organizaci)

Riziko

- **Riziko** - míra ohrožení aktiva, míra nebezpečí, že se uplatní hrozba a dojde ke vzniku škody. Velikost rizika je vyjádřena jeho úrovní.
  - Úroveň rizika je určena hodnotou aktiva, zranitelností aktiva a úrovní hrozby
  - **Pouze protiopatření úroveň rizika snižuje**

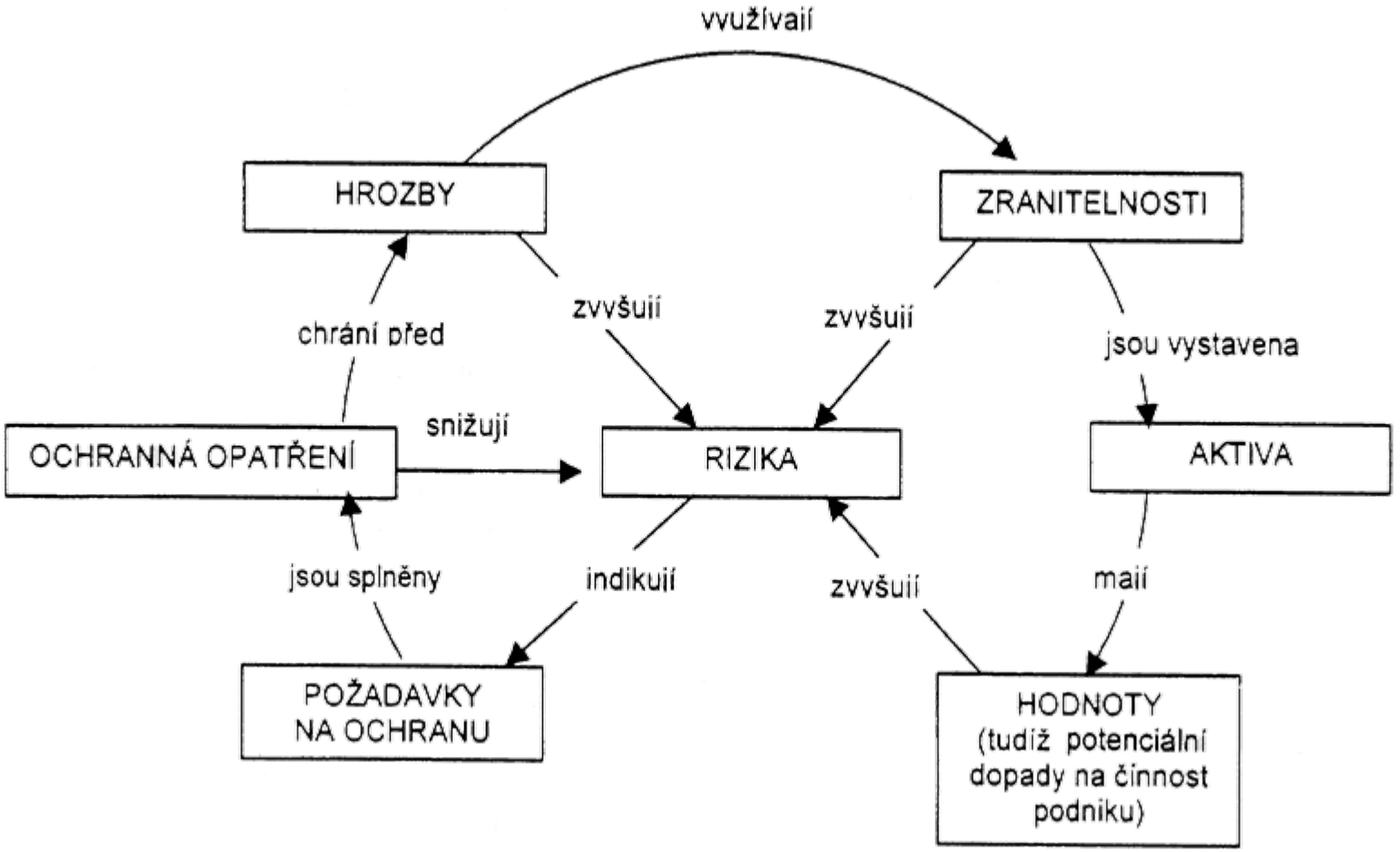
- **Zbytkové riziko** – malé riziko, je pro systém přijatelné a není nutné podnikat další protiopatření k jeho snížení

Protiopatření

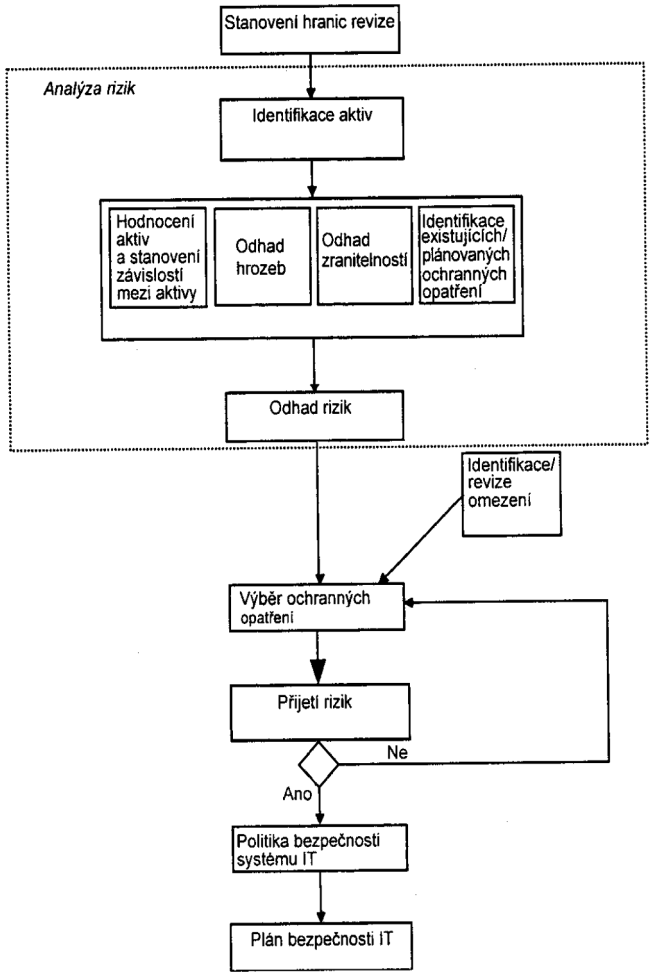
- **Protiopatření** - proces, procedura, technický či právní prostředek nebo cokoliv jiného vedoucí ke
  - Zmírnění působení hrozby
  - Eliminaci hrozby
  - Snížení zranitelnosti nebo dopadu hrozby
- Protiopatření se měří efektivitou a náklady
  - Efektivita - jak sníží účinek hrozby
  - Náklady – cena za protiopatření – v relaci s hodnotou aktiva

- **Výběr vhodného protiopatření spočívá v optimalizaci, kdy se hledají nejúčinnější protiopatření, jejichž realizace přinese co nejmenší náklady**

Základní vztahy



Procesy risk managementu



Provedení analýzy rizik my

- I. Krok:
  - Hranice posuzování (scope)
  - Nelze provádět analýzu rizik v neomezeném rozsahu
  - Časový snímek – čím delší expozice, tím rozmazanější
  - Čím větší rozsah, tím nepřesnější výsledky
  - Čím menší rozsah , tím vrůstá riziko „bílých míst“ (neodhalených slabin)
  - Volba metody (strategie):
    - Neformální přístup
    - Vysoce formalizovaný přístup
    - Kombinovaný přístup
    - Metodika (CRAMM, RANIT…)

Provedení analýzy rizik

- **II. krok - Identifikace aktiv**
  - Model Informačního systému (NE POUZE IT systému)
  - Aktivům jsou přiřazeni jejich vlastníci
  - BIA – Business Impact Analysis - analýza dopadů incidentu
    - Jaká bude škoda, když dojde:
      - Prolomení důvěrnosti komponenty
      - Dostupnosti komponenty
      - Integrity komponenty
      - Vše s parametry (nedostupnost 1 hodinu, 4 hodiny, 24 hodin…)

Provádění analýzy rizik

- **III. krok RM (AR) – Identifikace a ocenění aktiv**
  - Identifikace aktiv, jejich příslušnost ke komponentám a jejich vlastníků
  - Hodnota aktiv je stanovována v relativní stupnici nebo finančním rozsahu
- **IV. krok RM (AR) – Odhad hrozeb**
  - Hrozby jsou vybírány katalogu, který závisí na charakteru aktiva
  - Aktivum – data registru obyvatel x administrátor databáze
  - Katalog hrozeb je navržen v technických standardech

Provádění analýzy rizik

- **V. krok RM (AR)** – Odhad frekvence hrozeb
  - Jak často se hrozba může uplatnit

- **VI. krok RM (AR)** – Odhad zranitelnosti
  - Jak je aktivum vůči dané hrozbě citlivé?

Provádění analýzy rizik

- **VII. krok RM (AR)** – Identifikace stávajících protiopatření
  - Jaká protiopatření jsou již implementována
  - Jak jsou účinná
  - Katalog protiopatření je navržen ve standardu ČSN ISO/IEC 27001.
  - Protiopatření jsou kontextově závislá na typu aktiva, jeho ceně a typu hrozby

Provádění analýzy rizik

- **VIII. krok RM (AR) –** Hodnocení míry rizika
  - Míra rizika je stanovena pro jednotlivé hrozby
  - Hrubá míra rizika –bez zohlednění účinnosti protiopatření
  - Aktuální míra rizika –se zohledněním účinnosti stávajících protiopatření
  - Míra rizika modelovaná –se zohledněním účinnosti uvažovaných protiopatření
- **IX. krok RM - Kritéria pro akceptaci rizik**
  - Rozhodnutí o kritériích pro akceptaci rizik stanovuje svým rozhodnutím management
  - Hlediska – náklady, neexistující protiopatření, nízká míra rizika

Provádění analýzy rizik

- **X. krok RM – Varianty pro zvládání rizik**
  - Aplikování vhodných opatření – technických, procesních, smluvních…
  - Vědomé a objektivní akceptování rizik
  - Vyhnutí se rizikům
  - Přenesení rizik na třetí strany, např. na pojišťovny, dodavatele

Bezpečnostní politika

- **Technická a organizační bezpečnostní opatření, ISO/IEC 27002**
  - Organizace bezpečnosti informací
  - Personální zabezpečení
  - Řízení priorit
  - Řízení přístupu
  - Kryptografie
  - Fyzikální a environmentální bezpečnost
  - Bezpečnost provozu

Bezpečnostní politika

- **Technická a organizační bezpečnostní opatření, ISO/IEC 27002**
  - Bezpečnost komunikace
  - Systém akvizicí, vývoj a údržba
  - Dodavatelské vztahy
  - Řízení incidentů informační bezpečnosti
  - Informačně bezpečnostní aspekty kontinuity podnikání
  - Shoda

Audit

- **Zjištění shody požadovaného a skutečného stavu (co je a co není audit)**
  - Obvykle dle ČSN ISO/IEC 27001
  - Interní audit
  - Audit třetí stranou
  - Audit akreditovaným certifikačním orgánem
- Technický audit
- Penetrační testování
- Socio inženýrství

Bezpečnostní role

- **Manažer informační bezpečnosti**
- **Správce informační bezpečnosti**
- **Auditor – interní/externí**
- **Řídící výbor informační bezpečnosti**
- Požadavky:
  - Separace rolí, zamezení koncentraci pravomocí bez možnosti kontroly
  - Výkonné role v oblasti funkčnosti x výkonné role ve správě bezpečnosti
  - Správce systému x správce bezpečnosti
  - Metodická role x auditor
  - Manažer bezpečnosti x auditor
  - Socio inženýrství

Zákon o kybernetické bezpečnosti č. 161/2014 Sb.

- **Motivace:**
  - Jak postihnout subjekt za to, že nepoužívá bezpečnostní opatření
  - Jak vynutit realizaci bezpečnostních opatření
- Kybernetická bezpečnosti státu x individuální informační bezpečnost
- Kybernetická bezpečnost - ochranu národního kyberprostoru
- Vynutitelnost řešení bezpečnostních incidentů

Zákon o kybernetické bezpečnosti č. 161/2014 Sb.

- **Některé pojmy ZKN:**
- **Kybernetický prostor:**
  - Digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací
- **Kritická informační infrastruktura:**
  - Prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti
- **Bezpečnost informací:**
  - Zajištění důvěrnosti, integrity a dostupnosti informací a dat

Zákon o kybernetické bezpečnosti č. 161/2014 Sb.

Významný informační systém:

- Informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci

Zákon o kybernetické bezpečnosti č. 161/2014 Sb.

- **Významná síť -** síť elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře
- **Základní služba -** služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví:
  - Energetika
  - Doprava
  - Bankovnictví
  - Infrastruktura finančních trhů
  - Zdravotnictví
  - Vodní hospodářství
  - Digitální infrastruktura
  - Chemický průmysl

Zákon o kybernetické bezpečnosti č. 161/2014 Sb.

- **Informační systém základní služby** - informační systém, na jehož fungování je závislé poskytování základní služby

- **Provozovatel základní služby** - orgán nebo osoba, která poskytuje základní službu a která je určena Národním úřadem pro kybernetickou a informační bezpečnost

- **Digitální služba -** služba informační společnosti podle zákona upravujícího některé služby informační společnosti, která spočívá v provozování:
  - On - line tržiště
  - Internetového vyhledávače
  - Cloud computingu
  - Příslušným orgánem orgán vykonávající působnost v oblasti kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti č. 161/2014 Sb.

- **Ukládaná bezpečnostní opatření:**
  - V nezbytném rozsahu
  - Dokumentovaná opatření
  - Organizační opatření
  - Technická opatření

Zákon o kybernetické bezpečnosti č. 161/2014 Sb.

- **Organizační opatření:**
  - systém řízení bezpečnosti informací
  - řízení rizik
  - bezpečnostní politika
  - organizační bezpečnost
  - stanovení bezpečnostních požadavků pro dodavatele
  - řízení aktiv
  - bezpečnost lidských zdrojů
  - řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému

Zákon o kybernetické bezpečnosti č. 161/2014 Sb.

- **Organizační opatření:**
  - řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému
  - akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů
  - zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů
  - řízení kontinuity činností
  - kontrola a audit kritické informační infrastruktury a významných informačních systémů

Zákon o kybernetické bezpečnosti č. 161/2014 Sb.

- **Technická opatření:**
  - fyzická bezpečnost
  - nástroj pro ochranu integrity komunikačních sítí
  - nástroj pro ověřování identity uživatelů
  - nástroj pro řízení přístupových oprávnění
  - nástroj pro ochranu před škodlivým kódem
  - nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů
  - nástroj pro detekci kybernetických bezpečnostních událostí
  - nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Zákon o kybernetické bezpečnosti č. 161/2014 Sb.

- **Technická opatření:**
  - aplikační bezpečnost
  - kryptografické prostředky
  - nástroj pro zajišťování úrovně dostupnosti informací
  - bezpečnost průmyslových a řídících systémů

Vyhláška č. 82/2018 k zákonu kybernetické bezpečnosti

- **Definice pojmů**
- **Systém řízení bezpečnosti informací (ISMS)**
  - Vchází z ISO 27000
  - Používá mírně jiné pojmy
  - Definuje postupy – řízení aktiv, rizik atd.

NIS 2

- ***Co je NIS2?***
  - NIS - The Network and Information Security Directive
  - DIRECTIVE (EU) 2022/... OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), repealing Directive (EU) 2016/1148
    - Finální schválení přelom 2022/2023
    - 21 měsíců transpoziční lhůta
    - 2024 nový právní předpis (zákon + vyhlášky o KB)

NIS 2

Nejvýznamnější změny?

- Rozšíření počtu povinných osob
- Povinné vzdělávání vrcholového vedení organizace a větší odpovědnost managementu za zajišťování kybernetické bezpečnosti v organizaci
- Dobrovolné hlášení relevantních incidentů, událostí, hrozeb a zranitelností
- Podrobnější požadavky na vedení registru internetových domén nejvyšší úrovně a činnost registrátorů
- Důraz na sdílení informací mezi povinnými organizacemi a spolupráci mezi regulátorem a povinnými organizacemi
- Zvýšení pokut za nedodržení uložených povinností (nově se stanovuje úroveň pokut až ve výši 2 % celkového obratu společnosti nebo 10 milionů EUR)

NIS 2

- ***Koho se NIS2 týká?***
  - ZKB/VKB – úzká skupina, předmětem regulace byly identifikované systémy
  - NIS2 – přílohy definují služby důležité pro společnost (60 služeb v 18 odvětvích)
    - organizace poskytuje alespoň jednu službu uvedenou v přílohách směrnice
    - je středním nebo velkým podnikem, tedy zaměstnává 50 a více zaměstnanců, nebo dosahuje ročního obratu nebo bilanční sumy roční rozvahy alespoň 10 milionů EUR (zhruba 250 milionů CZK).

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 vtahují 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 16.08.2022

NIS 2

- ***Koho se NIS2 týká?***
  - Základní Essential entities (režim vyšších povinností) stávající (+-VIS)
    - aktualizovaná VKB
  - Důležitý Important entities (režim nižších povinností) (nové +- VIS)
    - „druhá“ vyhláška o KB

NIS 2

- ***Jaké povinnosti NIS2 ukládá?***
  - Bezpečnostní opatření aktuálního ZKB/VKB rámcově zůstanou zachována
    - Čl. 18 NIS2 – stanovuje okruhy, které mají být rozpracovány
    - okruhy budou pro „essential“ a „important“ přizpůsobeny tak, že povinnosti stanovené organizacím v režimu „important“ budou méně přísné, než v případě režimu „essential“
    - Dvě sady pravidel
      - Režim vyšších povinností
        - Stávající opatření
      - Režim nižších povinností
        - Vybraná opatření (zdůvodnit nevybrání, standard minimálních bezpečnostních požadavků)

Čl. 18 NIS2

- Analýza rizik a politiky bezpečnosti informací
- Zvládání incidentů
- Kontinuita činností (tj. business kontinuita), přičemž směrnice tento okruh ještě rozvádí o příklad zálohování, zotavení (disaster recovery) a krizové řízení
- Bezpečnost v rámci dodavatelského řetězce
- Bezpečnost v rámci pořízení, vývoje a údržby systémů
- Politiky a postupy pro hodnocení účinnosti bezpečnostních opatření (tj. audit)
- Praktiky základní počítačové hygieny a vzdělávání v oblasti kybernetické bezpečnosti
- Politiky a postupy týkající se využívání kryptografie a tam, kde je to vhodné, také šifrování
- Bezpečnost lidských zdrojů, řízení přístupů a aktiv
- Využívání vícefaktorového ověření identity, bezpečných komunikačních nástrojů a nástrojů pro nouzovou komunikaci

NIS 2

- ***Jaké povinnosti NIS2 ukládá?***

  - Důraz na vzdělávání (čl. 17 NIS2)
  - Důraz na zajištění kontinuity činností
  - All hazard approach
  - Risk based approach
  - … za porušení povinností pokuty …

NIS 2

- ***Jaké povinnosti NIS2 ukládá?***
  - Všichni musí hlásit KBI
    - Významnost dopadu – posouzení kritérií
      - incident způsobil nebo může způsobit vážné provozní narušení služby nebo finanční ztráty pro dotčený subjekt;
      - incident ovlivnil nebo může ovlivnit jiné fyzické nebo právnické osoby, způsobuje značné materiální i nemateriální ztráty,
    - Prakticky použitelné stanovení zpřesňujících pravidel v národních předpisech členských států, např.
      - Významnost dopadu
        - Významný dopad na regulovanou službu
        - Úmyslné zavinění
      - Important jen ty KBI, které mají původ k kybernetickém prostoru

NIS 2

- ***Jak se na NIS2 připravit?***

  - NIS2 není revolucí v oblasti kybernetické bezpečnosti
  - **Důvodem pro implementaci opatření KB by neměla být obava před pokutami**
  - Základem je ustavit SŘBI jako racionální a propojený systém integrující veškeré požadavky
  - Efektivnost opatření (risk management je základem)
  - Personální aspekty

GDPR

- **NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)**
  - 14.4. 2016 – schváleno
  - 24.5.2016 – platnost
  - Povinnost přizpůsobit se do 25.5.2018
  - Nahrazuje zák. č. 101/2000 Sb. a Směrnici č. 95/46/ES
  - Platnost pro státy EÚ (28) a EFTA (Norsko, Island, Lichtenštejnsko)

GDPR

- Dosavadní lokální právní předpisy jsou nahrazeny jediným souborem předpisů o ochraně údajů, který platí pro celou EU
  - Unifikace pravidel
  - Neumožní dostatečně zohlednit lokální rozdíly
- Nařízení zruší některé povinnosti:
  - Oznamování všech zpracování osobních údajů
- Nařízení zavádí povinnosti nové:
  - Jmenovat zvláštního pověřence ochrany údajů,
  - povinnost zjišťovat, jak se k některým druhům zpracování staví ti, jejichž údaje mají být zpracovávány apod.

GDPR

- Povinnost pro správce/zpracovatele (zaměstnávající více než 250 osob) vést záznamy o činnostech zpracování
- Podnikatelům se výrazně zjednoduší předávání osobních údajů mimo EU - jednotný přístup národních regulátorů
- Evropská komise získá velmi rozsáhlé právo přijímat prováděcí předpisy
- Podnikatelé musí případy závažného narušení ochrany údajů oznamovat vnitrostátnímu orgánu dozoru co nejdříve (pokud možno do 24 hodin)

GDPR

- **Posílení práva fyzických o**sob na přístup k osobním údajům
- **Právo na přenositelnost údajů** - osobní údaje z jednotlivých sociálních sítí bude možné přenášet od jednoho poskytovatele služeb k dalšímu
- **Právo být zapomenut** - bude možné explicitně požadovat vymazání osobních údajů
- Zpracování osobních údajů o dětech mladších 13 let bude možné pouze se souhlasem jejich rodičů
- **Podstatné zvýšení pokut**, které mohou být uděleny za porušení předpisů

GDPR

- **Posílení práva fyzických o**sob na přístup k osobním údajům
- **Právo na přenositelnost údajů** - osobní údaje z jednotlivých sociálních sítí bude možné přenášet od jednoho poskytovatele služeb k dalšímu
- **Právo být zapomenut** - bude možné explicitně požadovat vymazání osobních údajů
- Zpracování osobních údajů o dětech mladších 13 let bude možné pouze se souhlasem jejich rodičů
- **Podstatné zvýšení pokut**, které mohou být uděleny za porušení předpisů

Obchodní tajemství

- **Základní problémy v soukromém sektoru:**
  - Ochrana hodnot (informačních aktiv):
  - Know how
  - Obchodních informací
  - Strategických informací
  - Zdrojů zaměstnavatele

- **Rozumná míra regulace vztahů s dodavateli a státem**

- **Předvídatelnost a stabilita prostředí**

Obchodní tajemství

- **Právní rámec: Zákon č. 89/2012 Sb., občanský zákoník**
  - Část první – Obecná ustanovení
  - Hlava IV – Věci a jejich rozdělení
  - Díl 2 – Rozdělení věcí
  - § 504 – Obchodní tajemství
  - Část čtvrtá – Relativní majetková práva
  - Hlava III – Závazky z deliktů
  - Díl 2 – Zneužití a omezení soutěže
  - Oddíl 2 – Nekalá soutěž
  - § 2988, § 2989 - Ochrana proti nekalé soutěži

Obchodní tajemství

- **Právní rámec: Zákon č. 89/2012 Sb., občanský zákoník**
  - Může jít pouze o skutečnosti uvedené v § 504 občanského zákoníku
  - Jedná se o projev vůle podnikatele, který konkretizuje rozsah skutečností zahrnujících obchodní tajemství
  - Podnikatel musí druhou stranu s předmětem obchodního tajemství seznámit

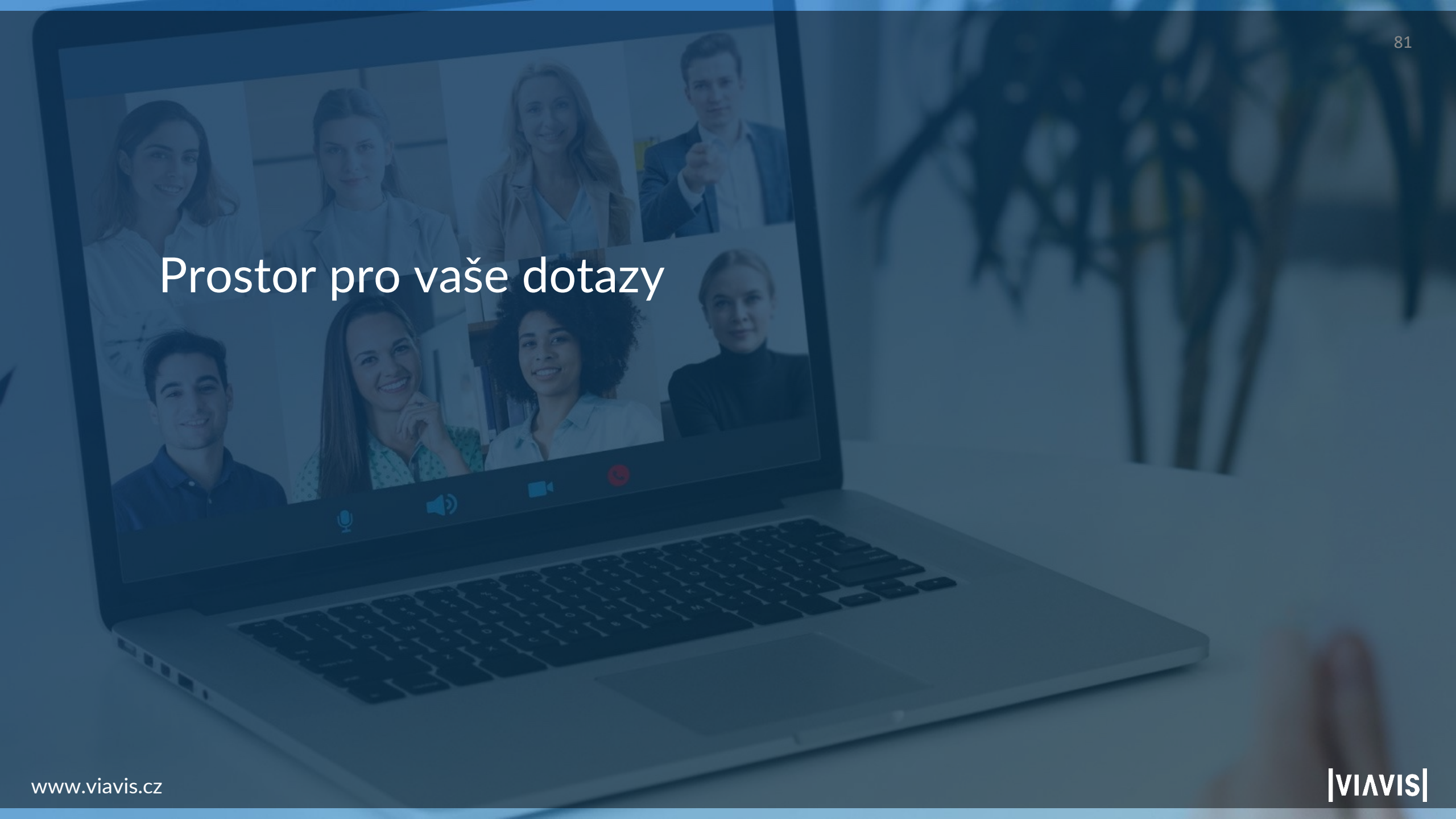
Obchodní tajemství

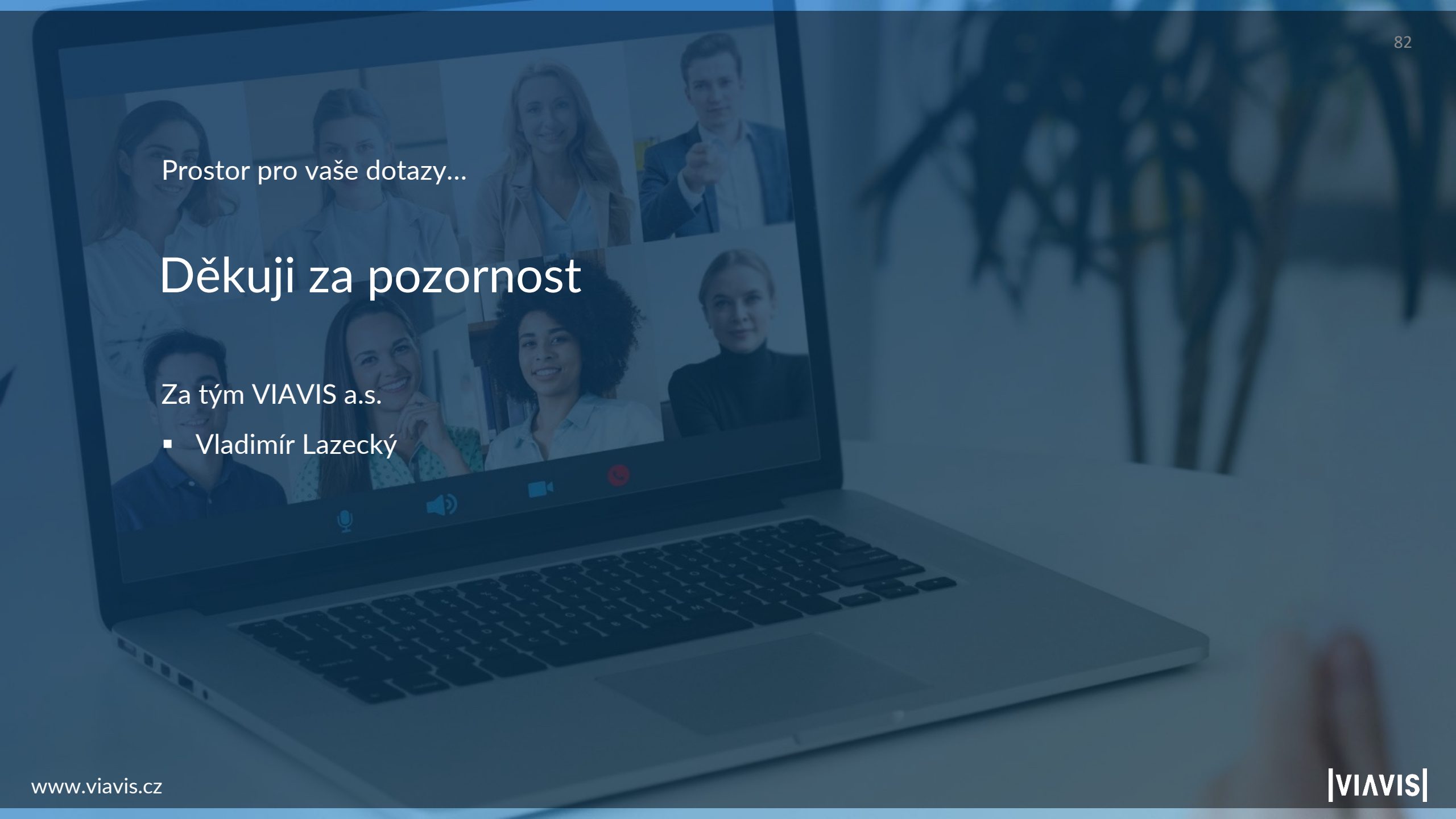
- **Stanovení:**
  - Které skutečnosti tvoří předmět obchodního tajemství
  - Kdo je oprávněn se s těmito skutečnostmi seznamovat
  - Zajištění řádné ochranu dokumentů obsahujících obchodní tajemství (vč. elektronických) před neoprávněným zpřístupněním
  - Se skutečnostmi tvořícími předmět obchodního tajemství seznámit jen nezbytný okruh osob oprávněných
  - Prokazatelné seznámení
  - Prokazatelné poučení o způsobu nakládání a způsobu jejich ochrany

Zkuste si analýzu rizik

- **Vyberte a proveďte:**
  - Informační systém
  - Analýzu rizik
  - Návrh na implementaci protiopatření
  - Zdůvodněte

Prostor pro vaše dotazy





Prostor pro vaše dotazy…

Děkuji za pozornost

Za tým VIAVIS a.s.

- Vladimír Lazecký