ČVUT

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

NIS2 a Kybernetická bezpečnost – obce a města

Kybernetická bezpečnost 2023 - 2025

Odbor Bezpečnosti RČVUT

Hynek Vlas ŘOB

Jiří Svačinka MKB

NIS 2

Zpřísnění pravidel pro řízení kybernetické bezpečnosti

NIS2 zavádí jeden typ povinné osoby = **poskytovatel regulované služby** jako náhrada stávající samostatně definované povinné osoby

Poskytovatelem regulované služby je kdokoliv, kdo poskytuje alespoň jednu regulovanou službu, tedy službu, jejíž narušení by mohlo mít významný dopad na zabezpečení důležitých společenských nebo ekonomických činností.

Významným dodavatelem je každý, kdo s poskytovatelem regulované služby vstupuje do právního vztahu, který je významný z hlediska stanoveného rozsahu řízení kybernetické bezpečnosti.

NIS 2

Zpřísnění pravidel pro řízení kybernetické bezpečnosti

- **Identifikace všech primárních** aktiv v rámci celé organizace (včetně jejich evidence)

- Určení, která **primární aktiva souvisejí s poskytováním regulované služby**, a určení jejich podpůrných aktiv
- Řízení přístupu k aktivům
- Stanovení rozsahu systému řízení bezpečnosti

- **Tvorba/aktualizace bezpečnostních politik** a bezpečnostní dokumentace

- Komplexnější přístup k řízení rizik, povinnost identifikovat rizika, vyhodnocovat a přijímat opatření ke snížení rizik, posuzovat naplňování plánu zvládání rizik
- Zabezpečení pořizování, vývoje a údržby sítí a informačních systémů

- **Důraz na bezpečnost lidských zdrojů**, pravidelná školení a kybernetická hygiena
- Prosazování politik a postupů týkajících se používání kryptografie, případně šifrování
- **Využívání vícefaktorového ověření identity**

- Zajištění provedení **auditu kybernetické bezpečnosti**

NIS 2

Zpřísnění pravidel pro řízení kybernetické bezpečnosti

- **Hlášení registračních, kontaktních a dalších doplňujících údajů NÚKIBu**

- **Hlášení kybernetických bezpečnostních incidentů** (prvotní hlášení do 24 hodin)

- **Informování uživatelů regulované služby** (v případě kybernetického informačního incidentu)

- **Vzájemné sdílení podstatných informací** o kybernetické bezpečnosti včetně informací týkajících se kybernetických hrozeb, zranitelností, indikátorů narušení, taktiky, technik a postupů, varování při ohrožení kybernetické bezpečnosti a konfiguračních nástrojů

NIS 2

Essential Entities

- Méně povinností a jednodušších než KII –> jednodušší VKB
- Hlášení incidentů a plnění mimořádných opatření
- Periodický externí audit ISMS, namátková kontrola NÚKIB

Important Entities

- Minimální bezpečnostní standard
  - Seznam požadavků, které mají zavést
- Jednoduchá analýza rizik (spíše bezpečnostních potřeb)
- Pravidelný externí audit za určitou periodu / Self asessment
- Omezené hlášení incidentů a plnění mimořádných opatření
- Možnost kontroly NÚKIB v případě podezření na neplnění
- Omezené služby NÚKIB

NIS 2 – určující kritéria

Digitální infrastruktura

- Výměnné uzly internetu, DNS, TLD, Cloud computing, Datová centra, Sítě pro doručování obsahu, Služby vytvářející důvěru, Veřejné sítě a služby elektronických komunikací

Veřejná správa

- Ústřední subjekty veřejné správy
- Subjekty veřejné správy územních jednotek úrovně NUTS 1 a NUTS 2

NIS 2 – Dopady do národní regulace

V současné době je v regulaci NIS 1 - ZKB cca 350 subjektů v kategorii KII, PZS a VIS.

Pro NIS 2:

- Nárůst počtu subjektů se předpokládá **sedmnáctinásobný**.
- Regulace by se neměla týkat jednotlivých systémů, ale celých organizací.
- K určování ES a IE nebude využíváno dopadových kritérií. Postačí poskytování služeb ve vymezením odvětví a velikost organizace.
- Vzhledem k množství a diverzitě jednotlivých předpokládaných povinných osob nelze všem uložit stejné povinnosti (vyplývá i z NIS2).
- NÚKIB by měl zřizovat/koordinovat komunity kybernetické bezpečnosti a zajišťovat výměnu informací o zranitelnostech. (alternativa k NEWEBu)

NIS 2 – určující kritéria

NIS 1 - ZoKB

- § 3 - Systém řízení bezpečnosti informací
- § 4 - Řízení aktiv
- § 5 - Řízení rizik
- § 6 - Organizační bezpečnost
- § 7 - Bezpečnostní role
- § 8 - Řízení dodavatelů
- § 9 - Bezpečnost lidských zdrojů
- § 10 - Řízení provozu a komunikací
- § 11 - Řízení změn
- § 12 - Řízení přístupu
- § 13 - Akvizice, vývoj a údržba
- § 14 - Zvládání kybernetických bezpečnostních událostí a incidentů
- § 15 - Řízení kontinuity činností
- § 16 - Audit kybernetické bezpečnosti

NIS 2 - Novela ZoKB

- i) systém řízení bezpečnosti informací,
- ii) povinnosti vrcholového vedení,
- iii) bezpečnostní role,
- iv) řízení bezpečnostní politiky a bezpečnostní dokumentace,
- v) řízení aktiv,
- vi) řízení rizik,
- vii) řízení dodavatelů,
- viii) bezpečnost lidských zdrojů,
- ix) řízení změn,
- x) akvizice, vývoj a údržba,
- xi) řízení přístupu,
- xii) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
- xiii) řízení kontinuity činností a
- xiv) audit kybernetické bezpečnosti.

Obce s rozšířenou působností nad 125tis.

Vaše organizace je zařazena do režimu VYŠŠÍCH povinností, kde spadají následující bezpečnostní opatření.

Před zaváděním bezpečnostních opatření je nutné stanovit v organizaci tzv. Rozsah řízení kybernetické bezpečnosti.

Organizační opatření

- Systém řízení bezpečnosti informací
- Povinnosti vrcholného vedení
- Bezpečnostní role
- Řízení bezpečnostní politiky a bezpečnostní dokumentace
- Řízení aktiv
- Řízení rizik
- Řízení dodavatelů
- Bezpečnost lidských zdrojů
- Řízení změn
- Akvizice, vývoj a údržba
- Řízení přístupu
- Zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů
- Řízení kontinuity činností
- Audit kybernetické bezpečnosti

Technické opatření

- Fyzická bezpečnost
- Bezpečnost komunikačních sítí
- Správa a ověřování identit
- Řízení přístupových oprávnění
- Detekce kybernetických bezpečnostních událostí
- Zaznamenávání bezpečnostních a relevantních provozních událostí
- Vyhodnocování kybernetických bezpečnostních událostí
- Aplikační bezpečnost
- Kryptografické algoritmy
- Zajišťování dostupnosti regulované služby a
- Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

Obce s rozšířenou působností do 125tis.

Vaše organizace je zařazena do režimu NIŽŠÍCH povinností, kde spadají následující bezpečnostní opatření.

Před zaváděním bezpečnostních opatření je nutné stanovit v organizaci tzv. Rozsah řízení kybernetické bezpečnosti.

- Zajišťování minimální úrovně kybernetické bezpečnosti
- Povinnosti vrcholného vedení
- Řízení rizik
- Bezpečnost lidských zdrojů
- Řízení kontinuity činností
- Řízení přístupu
- Řízení identit a jejich oprávnění
- Detekce a zaznamenávání kybernetických bezpečnostních událostí
- Řešení kybernetických bezpečnostních incidentů
- Bezpečnost komunikačních sítí
- Aplikační bezpečnost
- Kryptografické algoritmy

Obce obecně – příprava na NIS2

Analýza stávajícího stavu kybernetické bezpečnosti v rámci organizace.

Zjistit, které služby organizace poskytuje, jaká aktiva (informace a návazně technologie, zaměstnance, dodavatele…) pro jejich poskytování potřebuje a jak by narušení dostupnosti, důvěrnosti či integrity mohlo organizaci a zejména jí poskytované služby ovlivnit.

Posouzení opatření, která jsou již zavedena

Začít s řešením největších problémů, které v dané obci jsou a stanovit si plán do budoucna. Šlpůení relevantních osob – uživatelů či vedoucích pracovníků;

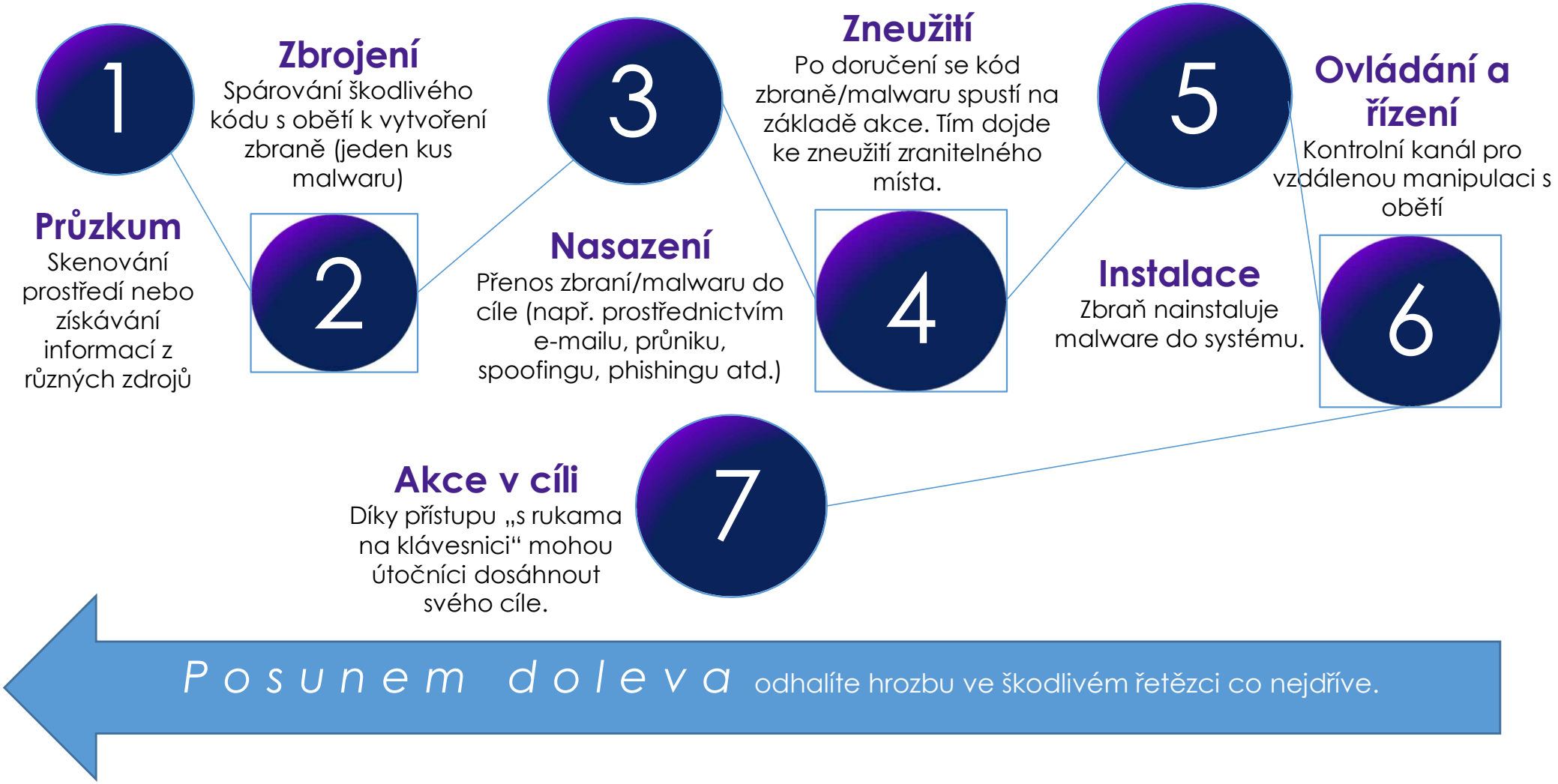
Zálohování potřebných dat, firewally a antivirové řešení.

Obce jsou častým zřizovatelem organizací, které mohou být novou regulací dotčeny rovněž – jedná se například o některé subjekty v odvětví zdravotnictví, vodohospodářství či odpadního hospodářství. Přestože na tyto subjekty bude regulace dopadat samostatně a budou poskytovateli regulovaných služeb sami o sobě, je dobré s takovou situací z pozice zřizovatele počítat a přiměřeně se na ni připravit.

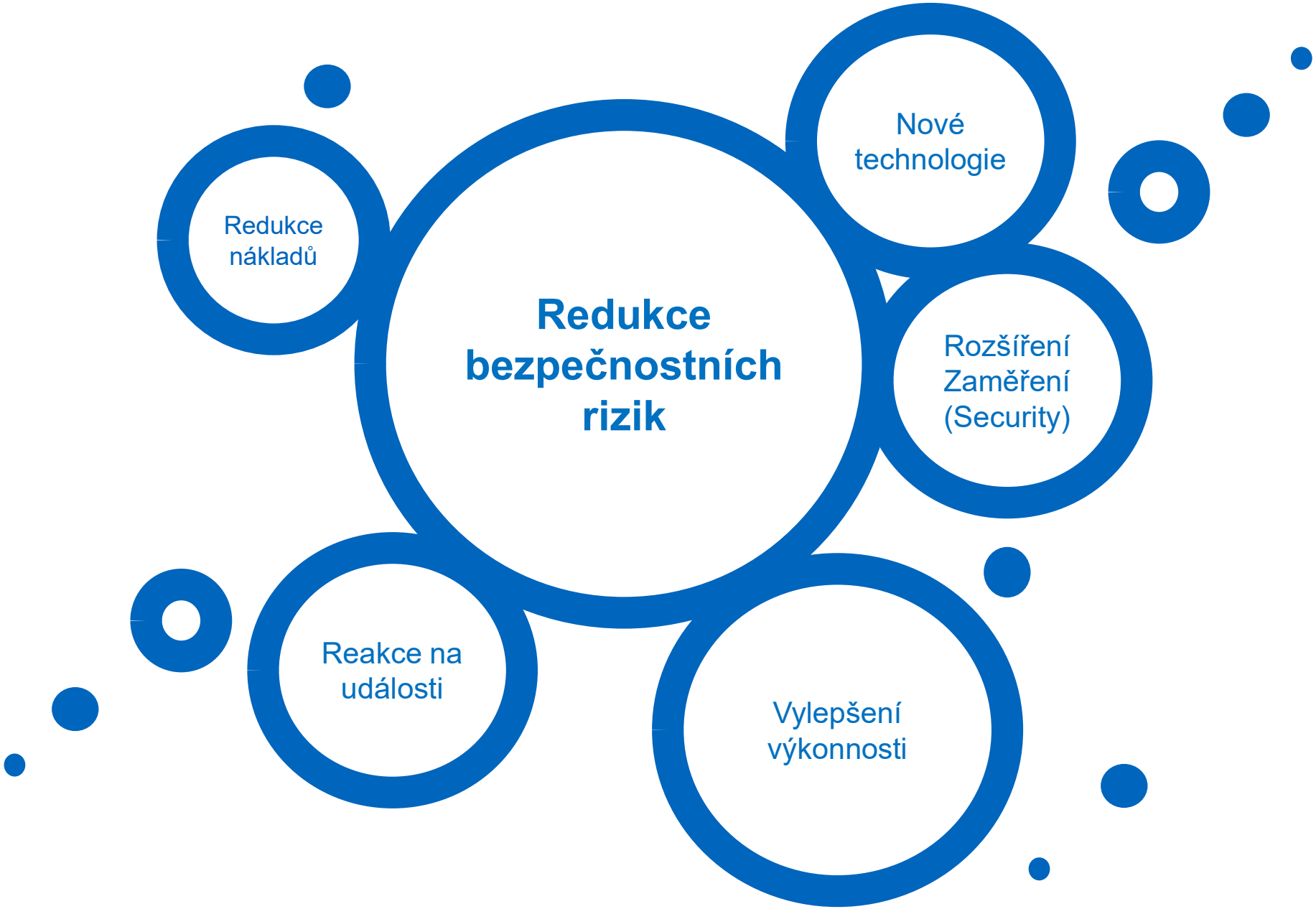
Služby řízení KB pro obce

Správa prostředí externích hrozeb

Zachycení škodlivého řetězce (Kill Chain)



Služby řízení KB pro obce



Služby řízení KB pro obce

Shoda se ZoKB

- Řízení rizik
- Politika kyb. bezpečnosti
- Data Governance - VIS a datové toky = firewall pravidla
- Klasifikace dat a Data retention = GDPR + Spis. služba
- Mapování procesů - BPMN, UML
- Řízení oprávnění
- Řízení dodavatelů

Produkt-Služba dle ZokB

- Evidence účtů a služeb
- Revize oprávnění ke službám
  PIM/PAM, 2FAKAUT
- Penetrační testy
- Skenování zranitelností
- Automatizace bezpečnostních testů
- Bezpečné řízení a deployment změn

Služby řízení KB pro obce

Personál dle ZoKB

- Školení personálu
- Trénink use-case personálu
- Řízení oprávnění dle rolí
- Zlepšení politiky hesel
- Prevence úniku dat

Infrastruktura dle ZokB

- Revize architektury infrastruktury
- Zodolňování slabých míst infrastruktury
- Snížení útoků na datovou síť a infrastrukturu
- Zlepšení identity & access managementu
- Automatizované testy a opravy
- Princip „infrastructure as code“

Služby řízení KB pro obce

Zajištění odolnosti

- Identifikace kritických komponent a služeb
- Modernizace *Incident response*
- Modernizace zálohování
- Zlepšení log management
- Zlepšení monitoringu a detekce anomálií
- Disaster recovery postupy a plány

Shrnutí

Útočník

- nezajímá legislativa a zákonné regulace.
- organizuje interní motivace k získání profitu.
- zajímá zranitelnost a pravděpodobnost profitu.
- zajímá jakákoliv inovace pro útok.

Obránce

- **musí mít motivaci bránit svěřené prostředí !!!!**
- musí mít organizaci postupů a dril a nástroje k obraně.
- musí mít know-how pro provoz bezpečnostních nástrojů.
- musí mít know-how pro harmonizaci detekční schopnosti nástrojů na stávající a inovované symptomy útoků.

Shrnutí

Monitoring

- log management
- netflow monitoring
- směřování na automatizaci detekce a reakce

Analytika

- **Platforma Threat Intelligence**
- **Reporting o bezpečnosti 1xQ**

ČVUT

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Děkujeme za pozornost

Hynek Vlas ŘOB

Jiří Svačinka MKB