VIAVIS střežíme podstatné

Technická opatření kyber bezpečnosti

Kybernetická a informační bezpečnost I

Vladimír Lazecký

vladimir.lazecky@viavis.cz

Cíl přednášky

- **Základní přehled technických opatření**
- **Proč?**
  - Zabránit incidentům
  - Detekovat incidenty
  - Udržet stanovenou míru bezpečnosti

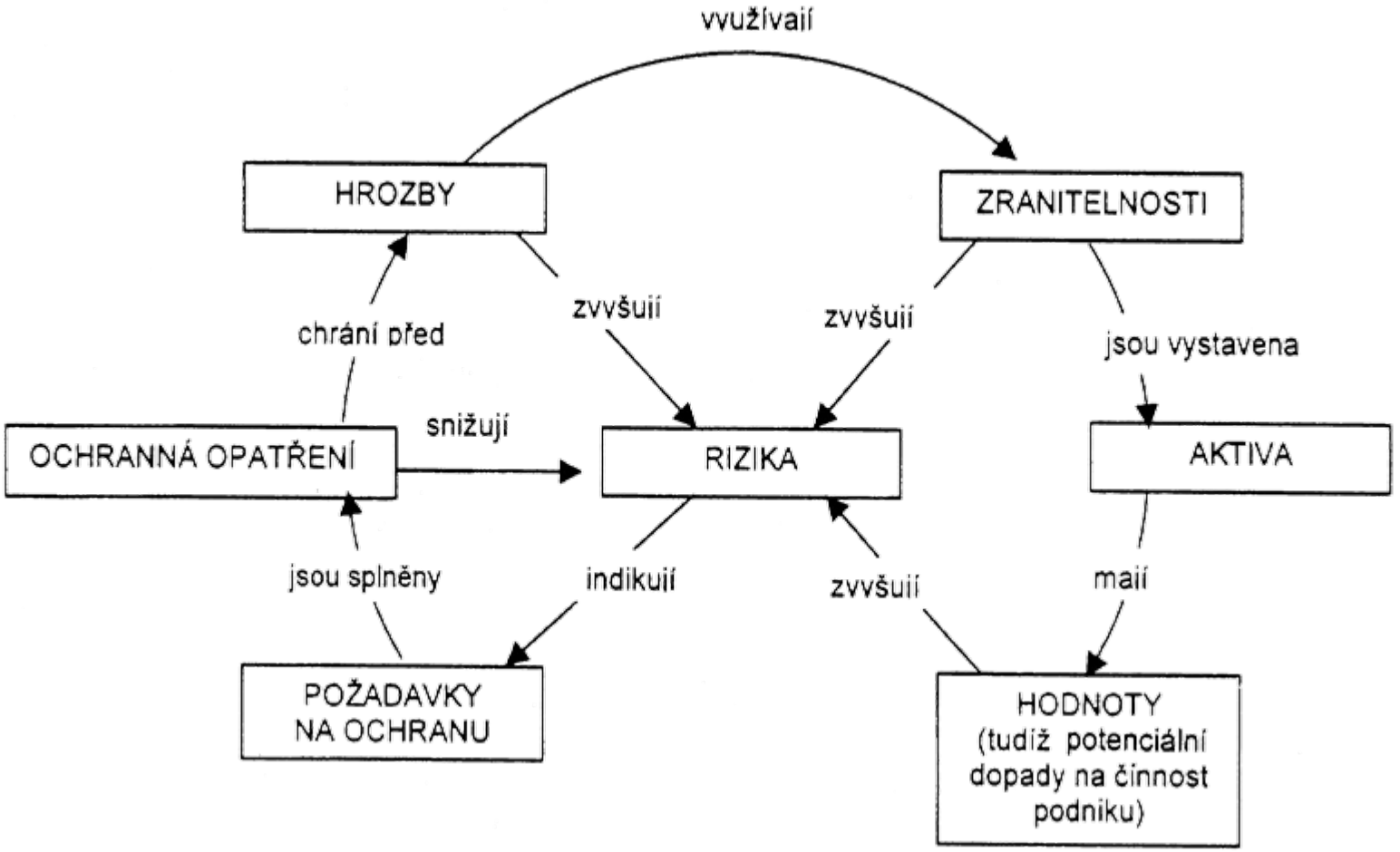
Zopakujeme – základní pojmy analýzy rizik

- 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…

Základní vztahy



VIAVIS

ISMS – systém managementu informační bezpečnosti

- Organizační opatření:
  - ISMS, ZKB, Vyhláška ZKB (nejen)
  - Definice pravidel hry
  - Politiky, směrnice, role, odpovědnost, pravomoc
  - Řízení dodavatelů…
  - Procesy – PDCA cyklus

- **Technická opatření**

Technická opatření – inspirace vyhláška č. 82/2018

- **Fyzická bezpečnost**
  - Co je fyzická bezpečnost?
  - Definice perimetru
    - Zabránění neoprávněnému přístupu
    - Ochrana před poškozením a zcizením
    - Ochrana systémů a lidských zdrojů

Technická opatření

- **Bezpečnost komunikačních sítí**
  - Perimetr a segmentace
  - Řízení provozu
  - Vzdálené přístupy, zajištění dostupnosti, důvěrnosti a integrity
  - Blokování nežádoucího provozu
- Technologie:
  - Firewall, IDS (Intrusion Detection System), FlowMon, VPN…
- Problémy:
  - Technologické systémy
  - Vzorce chování a detekce anomálií

Technická opatření

- **Správa a ověřování identit**
  - Centrální x decentralizovaná správa identit
  - Vysoká míra jistoty u ověření identity
  - Podpora více faktorové autentizace
  - Single Sign On
- Identity Management System (AD…)
- Řízení přístupových oprávnění – náročný a komplikovaný proces
- Autorizace uživatelů

Technická opatření

- **Ochrana před škodlivým kódem**
  - ***Co je škodlivý kód?***
  - Antiviry
  - Jaké jsou jejich limity?
  - Spyware, malware, Trojan Horse, Back Door…

Technická opatření

- **Zaznamenávání a detekce událostí**
  - Uživatelé, správci, záznam aktivit
  - Detekce anomálií, jejich hodnocení
  - Incidenty – detekované události představující bezpečnostní hrozbu
  - Klíčové otázky:
    - Jakou zvolit hloubku
    - Jak efektivně vyhodnocovat
  - Metadata dražší dat

Technická bezpečnost

- **Aplikační bezpečnost**
  - Zranitelnosti a slabiny aplikací
  - Ověřování integrity dat
  - Útoky na data – WEB, mailová komunikace
- *Jak navrhnete požadavky na bezpečnost aplikace?*
- *Co vše do aplikační bezpečnosti patří?*

(samostatný předmět)

VIAVIS

Pojďme si opět hrát

Naše stará známá Soukromá s.r.o.

Soukromá s.r.o. je středně velká soukromá společnost zaměřená na strojírenskou zakázkovou výrobu s 300 stálými zaměstnanci a úzkou spolupráci s dalšími firmami (kooperace). Původně šlo o malou nástrojárnu, která postupně rostla. Dnes generuje tržby kolem 700 mil/rok, je stabilní, trvale v zisku. Struktura vlastníků jsou 3 společníci, fyzické osoby.

Hlavní činnost spočívá převážně v návrhu, programování robotů a jejich kompletací a testování z výroby a nasazením u zákazníků. Zákazníci jsou světově známé výrobní korporace, kde Soukromá s.r.o. vykryla niku trhu, je schopna rychle reagovat na atypické požadavky v jednotlivých kusech. Část výrobních kooperací probíhá u dodavatelů v Číně a v zemích EU.

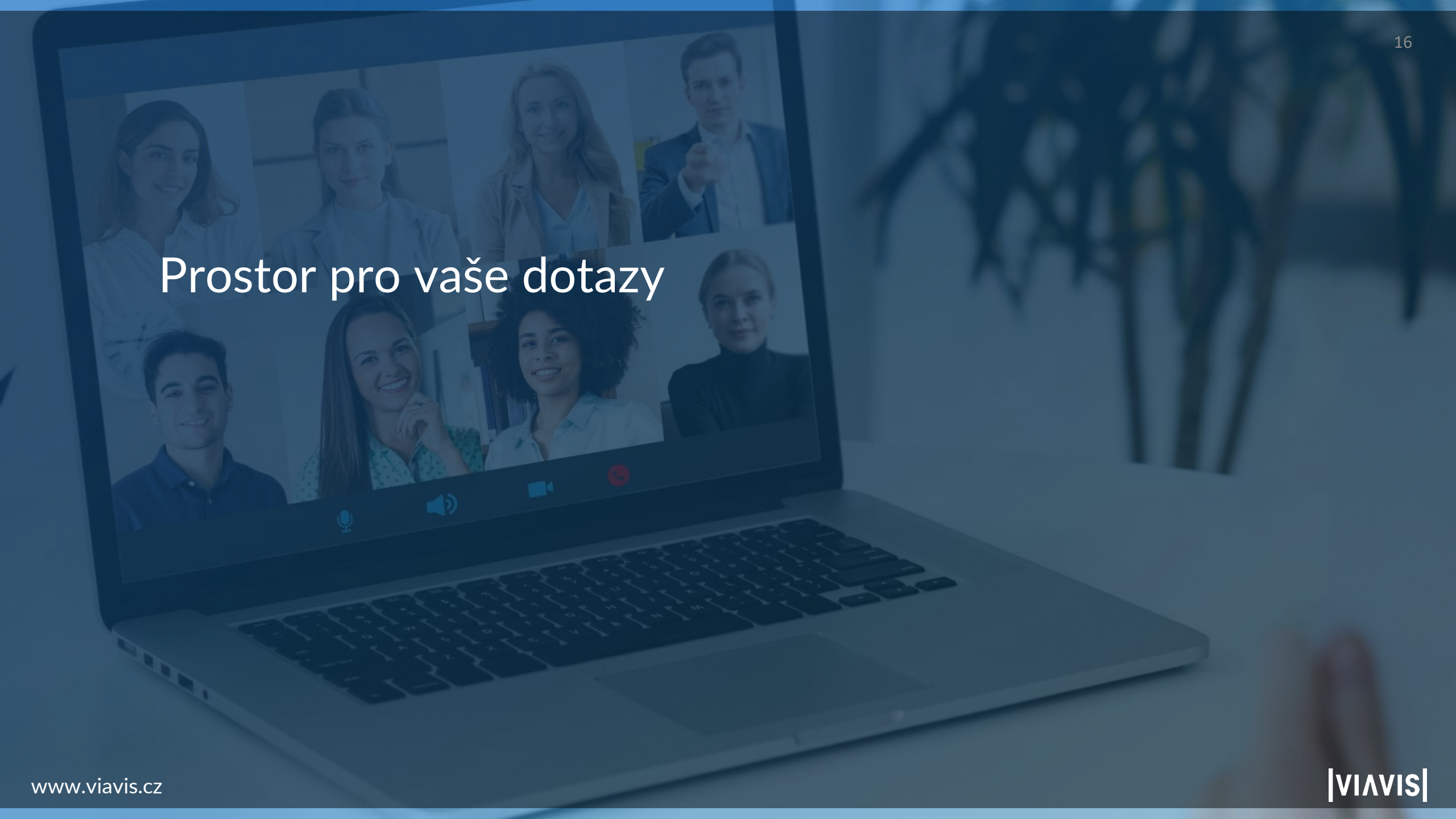
Nastoupil bezpečnostní manažer

- **Společnost je po incidentu**
  - Najala bezpečnostního manažera
  - Jeho cílem je „vyřešit bezpečnost“
  - Co bude dělat? Jak bude postupovat?

Pravidla hry

- **Tým managementu**
  - Ředitel, obchodní, výrobní a ekonomický ředitel
- **Bezpečnostní manažer + IT tým**
- 2 skupiny, každá bude pro tu druhou představovat tým managementu

Prostor pro vaše dotazy



Prostor pro vaše dotazy…

Děkuji za pozornost

Za tým VIAVIS a.s.

- Vladimír Lazecký