

Vybrané riziká informačnej bezpečnosti – spôsob prevencie a mitigácie hrozieb v oblasti fyzickej bezpečnosti

Ing. Stanislav Kmet', PhD.

- CEO, GI-BÓN s.r.o. Žilina
- Konzultant pre IT a IMS:
 - ISMS – ISO/IEC 27001
 - eIDAS
 - SMS – ISO/IEC 20000-1
 - BCM – ISO 22301
 - GDPR
- Audítor kybernetickej bezpečnosti
- Externý audítor pre IMS
- Člen TK 37

Riziká fyzickej bezpečnosti

Cieľ fyzickej bezpečnosti a bezpečnosti prostredia:

Zabrániť neautorizovanému fyzickému prístupu, zničeniu alebo zasahovaniu do informácií organizácie alebo zariadení spracúvajúcich informácie.

Hodnota aktív

- Klasifikácia informácií
- Kategorizácia sietí a informačných systémov

Hrozby, zraniteľnosti, riziká a opatrenia informačnej bezpečnosti pre oblasť fyzickej bezpečnosti.



Požiadavky na fyzickú bezpečnosť

- **Legislatívne, regulačné a sektorové požiadavky**
 - Zákon č. 18/2018 Z.z. o ochrane osobných údajov
 - Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti
 - Zákon č. 272/2016 Z.z. o dôveryhodných službách
 - Zákon č. 483/2001 Z.z. o bankách
 - Zákon č. 351/2011 Z.z. o elektronických komunikáciách
 - TISAX – automobilový priemysel
- **Normatívne požiadavky**
 - ISO/IEC 27001 a ISO/IEC 27002
 - NIST, SOC 2, RESILIA ...



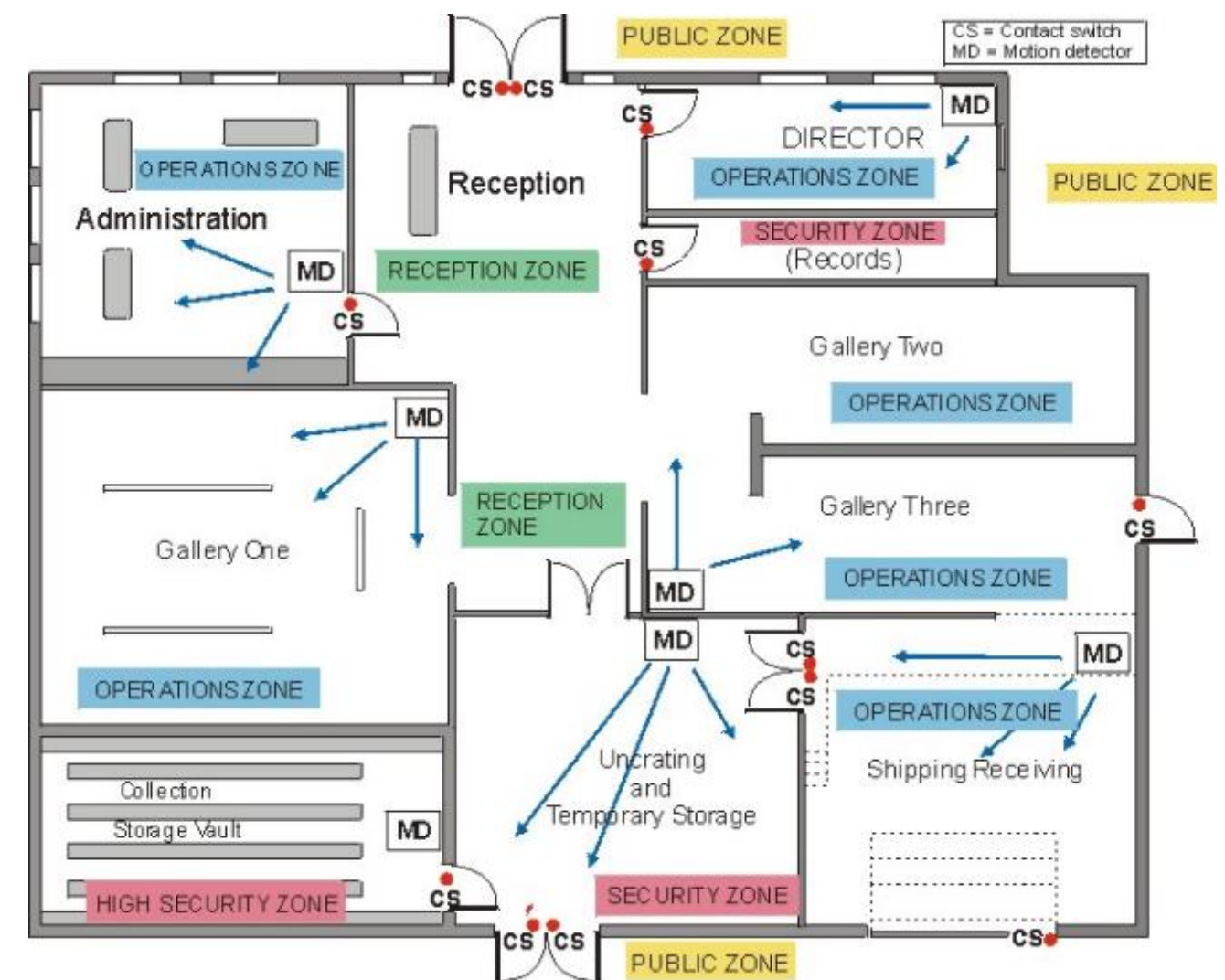
Perimeter fyzickej bezpečnosti

- Perimeter
 - Jasne definovaný, súvislý, s bariérami
 - Riadenie fyzického prístupu – kľúčový a kartový poriadok, externé prístupy
 - Detekcia narušenia – SBS, kamery, PIR, infrazávory, radary, termokamery, vzdialený monitoring (SOC)
 - Externé hrozby a hrozby prostredia



Zóny fyzickej bezpečnosti

- Bezpečnostné zóny
 - Definovanie zón
 - Bariéry a riadenia prístupu pre každú zónu
 - Právomoci a zodpovednosti (napr. NDA)
 - Režimové opatrenia pre prácu v zóne
 - Povedomie – „need to know“



Opatrenia pre zónu D - príklad

- **Mechanické zábranné prostriedky**
 - bezpečnostné protipožiarne dvere, bezpečnostná zárubňa,
 - bezpečnostný zámok a kovanie (vylúčený zo systému generálneho kľúča),
 - samozatvárací mechanizmus na dverách,
 - uprednostňovať miestnosti v zázemí budovy bez okien,
 - ochrana okien – mreže, bezpečnostná fólia, zatemnenie,
 - uprednostňovať miestnosti vybudované z pevných stavebných materiálov
- **Elektronické zabezpečovacie prostriedky**
 - poplachový systém na hlásenie narušenia – samostatný, oddelený od iných priestorov alebo ostatných zón,
 - systém kontroly vstupu – odporúčaný,
 - systémy na sledovanie/identifikovanie hrozieb vyplývajúcich z prostredia (zatečenie vodou, zvýšená vlhkosť, zvýšená teplota).



Riziká fyzickej bezpečnosti I.

Zistenia z auditov informačnej bezpečnosti

- Perimeter – narušenie... alarm... a potom čo?
- Fyzické prístupy pre tretie strany – chýbajúca evidencia a kontrola
- Zabezpečené oblasti – označiť alebo neoznačiť?
- Serverovňa – najchladnejší sklad
- Externé hrozby – pád lietadla?
- Hrozby prostredia – voda a kanalizácia
- Kamerové systémy – označenie a retencia záznamov
- Priestory na nakladanie a vykladanie – nemáme?

Nuclear Accident	9	9	27
Terrorist Attacks	9	9	27
Toxic Cloud	9	9	27
War / Civil War	9	9	27
Kidnapping	9	8	26
Earthquake	9	5	23
Explosions	9	5	23

Riziká fyzickej bezpečnosti II.

Zistenia z auditov informačnej bezpečnosti

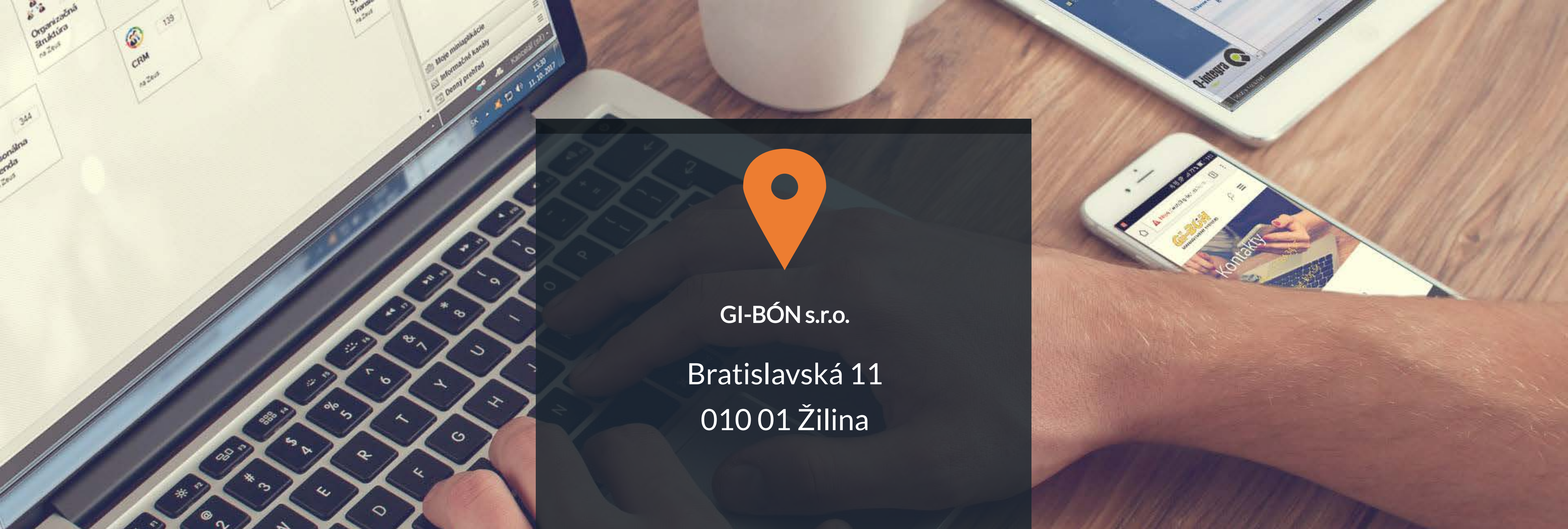
- Bezpečnosť zariadení – zdieľané tlačiarne
- Podporné služby – netestované po zmene kapacity
- Kabeláž – riešime až po prerušení
- Údržba zariadení – plány a záznamy
- Bezpečnosť zariadení mimo organizáciu – šifrovanie, wipe out
- Vyradenie a opätovné používanie – identifikácia
- Neobsluhované zariadenia – ochrana
- Politika čistého stola – kontrola
- Incidenty - spolupráca



Opatrenia pre zvýšenie fyzickej bezpečnosti

- **Business Impact Analysis** – na čo sa sústrediť?
- **Aktívne a pasívne bezpečnostné prvky** - vhodná kombinácia
- **Plány a testy kontinuity** – reálne
- **Incidenty** – odpoveď a spolupráca
- **Povedomie** – školenia, kampane, nácviky, testy





GI-BÓN s.r.o.

Bratislavská 11
010 01 Žilina



skmet@gi-bon.sk



+421905253664



www.gi-bon.sk



Ďakujem za pozornosť
