EMM

CHRÁNIME VAŠE HODNOTY

IT bezpečnosť vo fiktívnej firme

Pavol Dovičovič, Sulamit Bukovinská, Daša Krátka

2/ Agenda

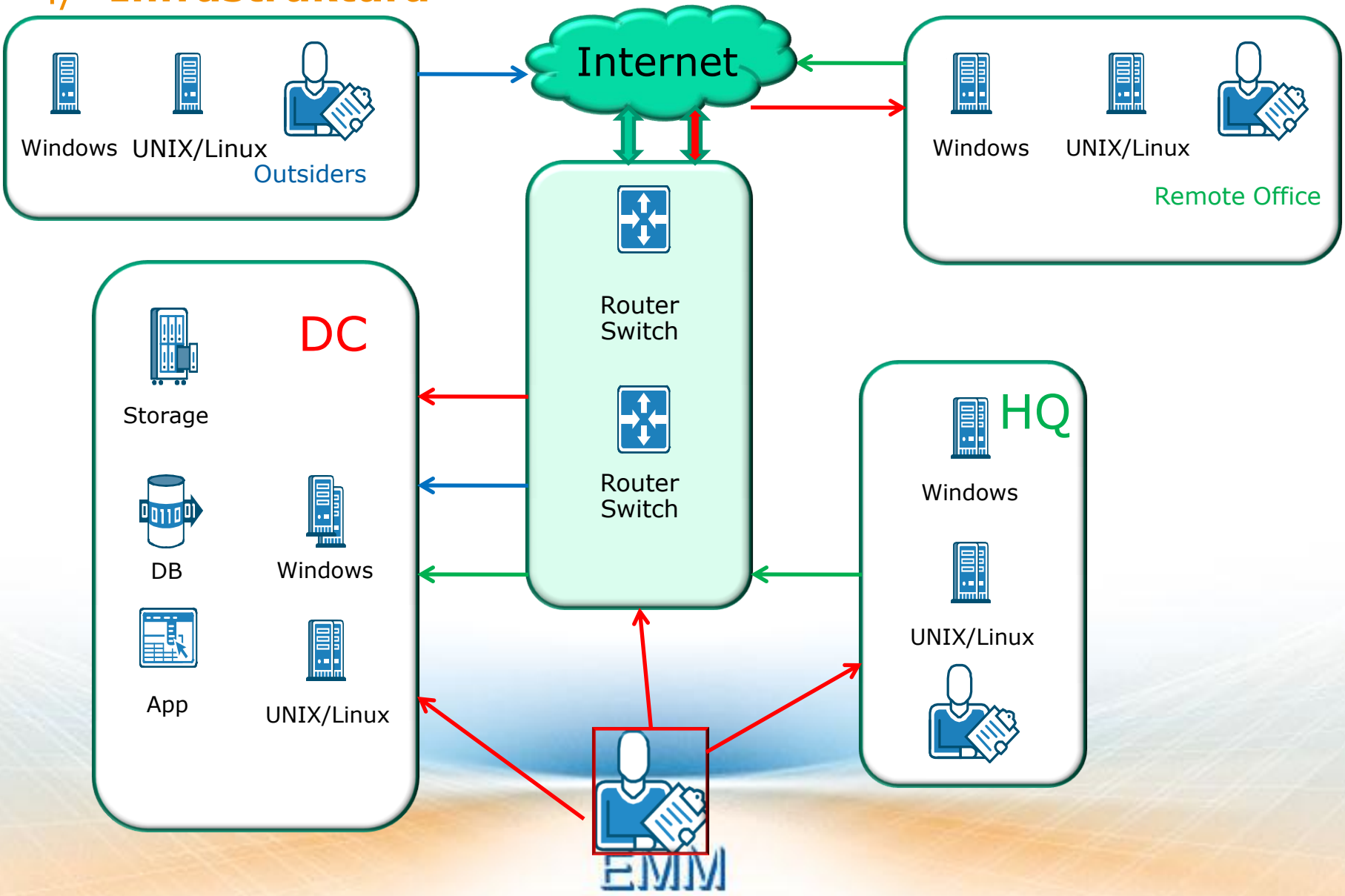
- Predstavenie firmy
- Popis komponentov infraštruktúry
- Definovanie možných hrozieb
- Analýza rizikových bodov
- Nasadenie technických prostriedkov a opatrení.
- Riadiace dokumenty bezpečnosti

EMM

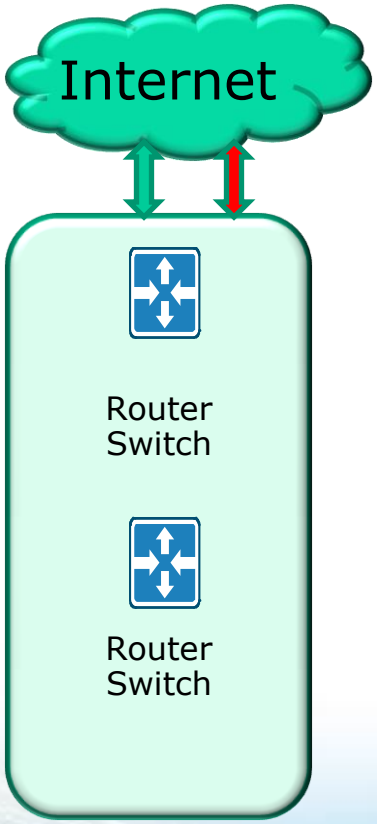
3/ Spoločnosť

- Nadnárodná spoločnosť
- Centrála a pobočky (HQ a Remote Office)
- Datacentrum v centrále spoločnosti
- Práca s mimoriadne citlivými dátami
- Prístup k dátam pre interných zamestnancov
- Prístup pre externých dodávateľov - „Outsiders“
- Vyžadovaný pravidelný audit
- Kompromitované dáta = ... (radšej nemyslieť) ..

4/ Infraštruktúra

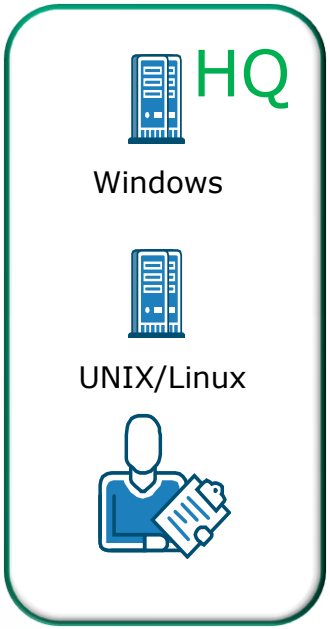


5/ Network



- Firewall
- Antivir
- Content filtering
- DLP
- Detekcia anomálií

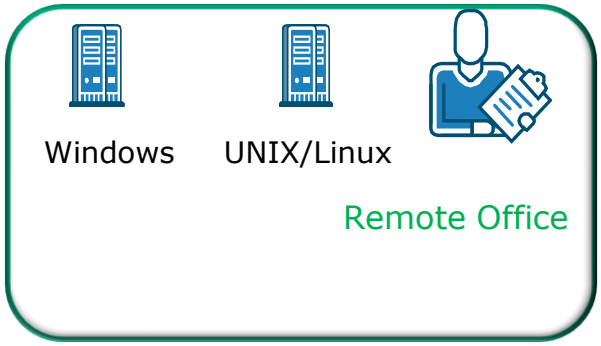
6/ Lokálne PC



- Antivir
- Endpoint Protection
- LDAP
- Užívateľské práva
- Activity Monitoring

EMM

7/ Remote office



- Antivir
- Endpoint Protection
- LDAP
- Užívateľské práva
- Activity Monitoring
- VPN
- Šifrovanie

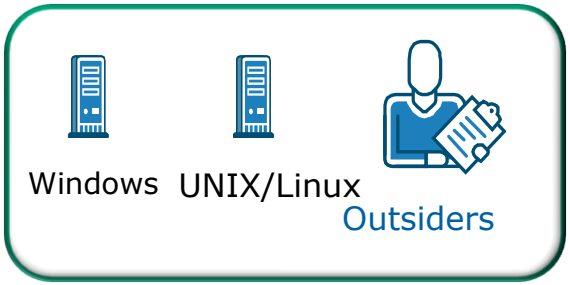
EMM

8/ Mobilní používatelia

- Šifrovanie
- Endpoint Protection
- Vzdialená správa
- Profily
- Activity Monitoring

EMM

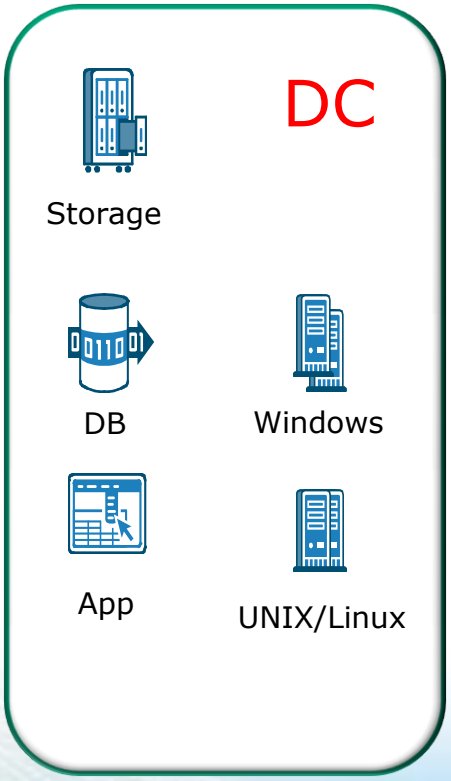
9/ Outsiders



- Užívateľské práva
- Activity Monitoring
- VPN
- Šifrovanie

EMM

10/ Datacentrum



- Firewall
- Zónovanie
- Antivir
- Endpoint Protection
- LDAP
- Užívateľské práva
- Activity Monitoring
- Vulnerability Scanner
- Šifrovanie

EMM

11/ Používatelia

Úmysel – nedokážete kontrolovať ľudské umysly

- Človek je komplexný biologický systém

Prostriedky – nedokážete kontrolovať všetky prostriedky, ktoré používajú „iní“ ľudia.

- „Iní“ ľudia budú stále vyvíjať ďalšie prostriedky a nástroje
- Môžete sa snažiť tento proces eliminovať, ale neuspejete pri zastavení tohto procesu

Príležitosti – jediný aspekt, ktorý dokážete ovplyvniť.

- Môžete implementovať bezpečnostné mechanizmy na elimináciu/zníženie príležitostí na kompromitáciu dát.

EMM

12/ Používatelia

Udržať „zlých" ľudí mimo

Perimeter

Reakcie na útoky

„Hardenning"

Detekcia hrozieb

Povoliť prístup „dobrým"

Identity

Prístupové práva

Monitoring

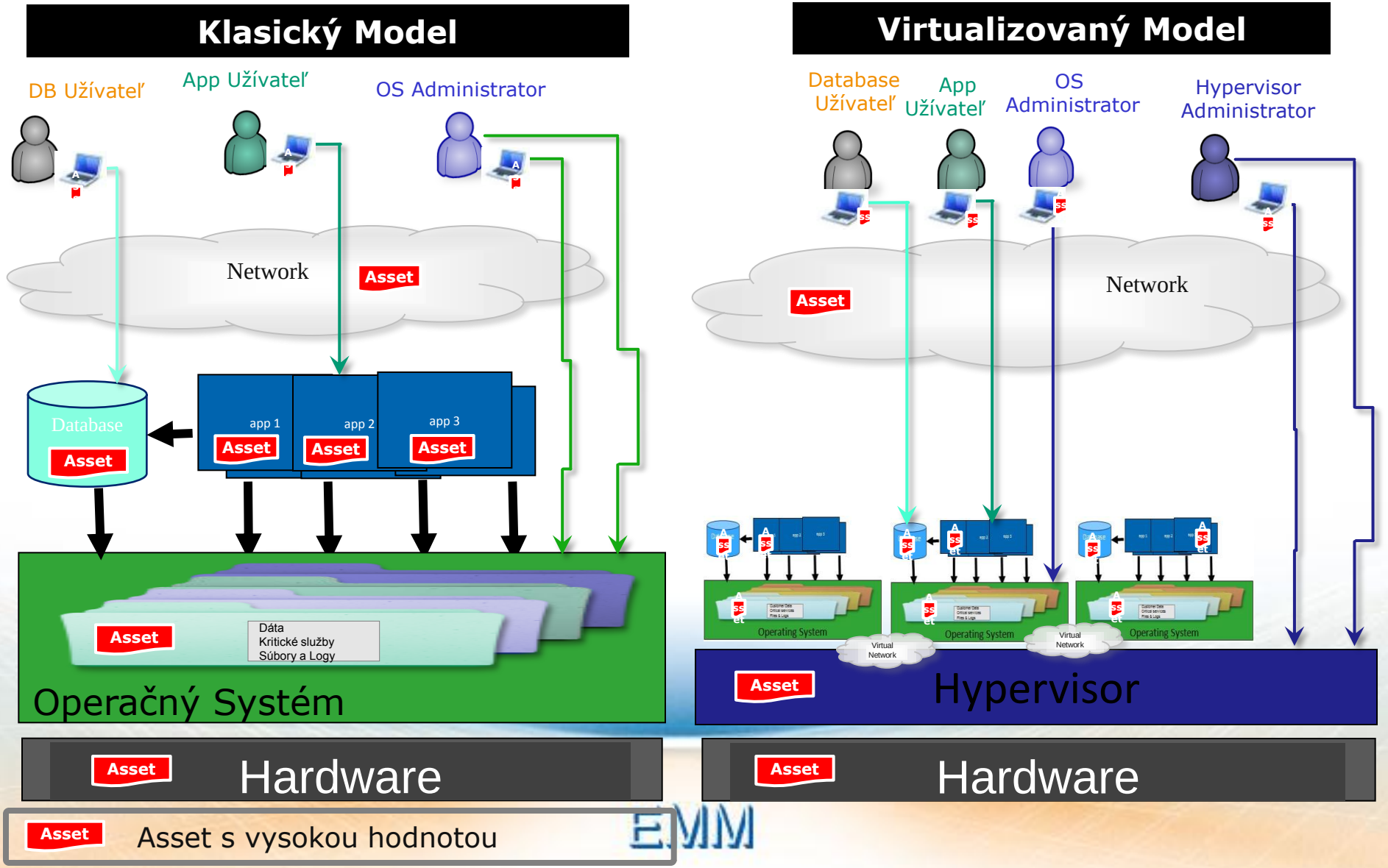
Definovanie úloh

Prevencia

Povolenia

EMM

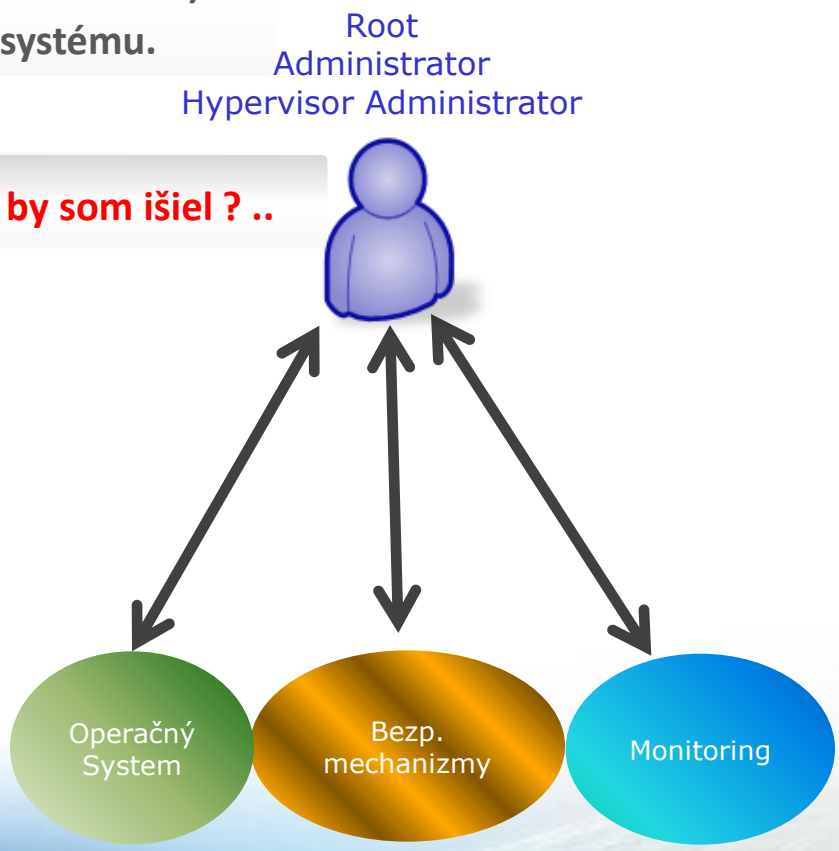
13/ Používatelia



14/ Používatelia

Jedna entita (Root/OS Administrator/Hypervisor Administrator) má úplnú kontrolu nad 3 životne dôležitými časťami systému.

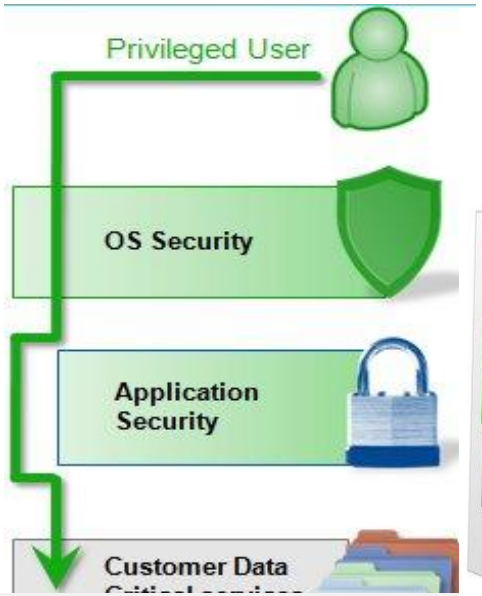
Čiže, ak by som bol „zlý chlapec“, po ktorom účte by som išiel ? ..

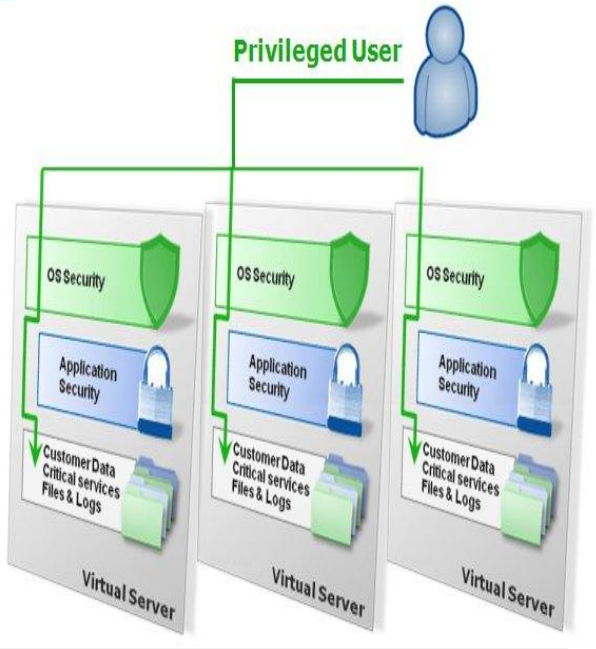


15/ Používatelia

> Root / Administrator

- Môže obísť aplikačnú bezp.
- Môže vidieť a modifikovať app. logy.
- Môže zmeniť systémové súbory
- Môže zmeniť systémovú konfiguráciu





2 scenáre:

- „Dobrý chlapec" sa stane zlým
- „Zlý chlapec" získa identitu dobrého chlapca

Pamätajte !! Každý dobrý chlapec sa môže stať zlým, či už zo svojej vôle, alebo proti nej !!

Používatelia

17/ Monitoring

- Security Operation Center
- SIEM
- Ticketing
- Auditing

EMM

Zhrnutie

- Zabezpečenie perimetra – FW, AV, CF, DLP, ADS, Ext. scanner,..
- Zabezpečenie DC – FW, AV, Zone Restrict, Vuln. Scanner, SoD,..
- Zabezpečenie pracovných staníc „HQ" – AV, End. Protection, User rights,..
- Zabezpečenie „Remote office" – FW, VPN a „HR",..
- Zabezpečenie „Outsiders" – VPN,..
- SIEM, Audit, Ticketing, Riadiace dokumenty bezpečnosti,..

19/ Urobili sme všetko na ochranu IT ???

EMM

Otázky:

Je zabezpečenie dostatočné?

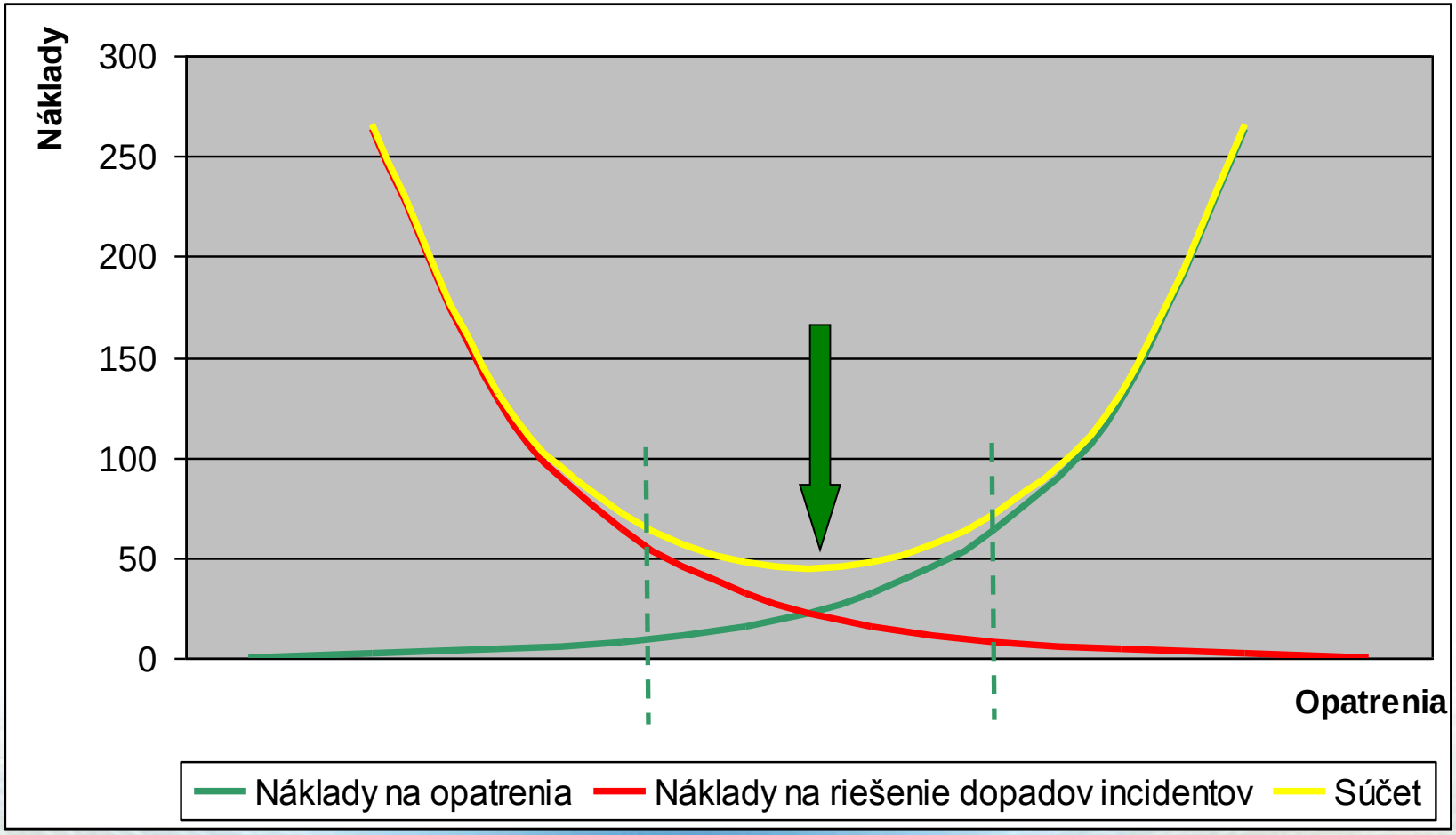
Čo je to dostatočné?

Je a má byť všade zabezpečenie (použité bezpečnostné opatrenia) rovnaké?

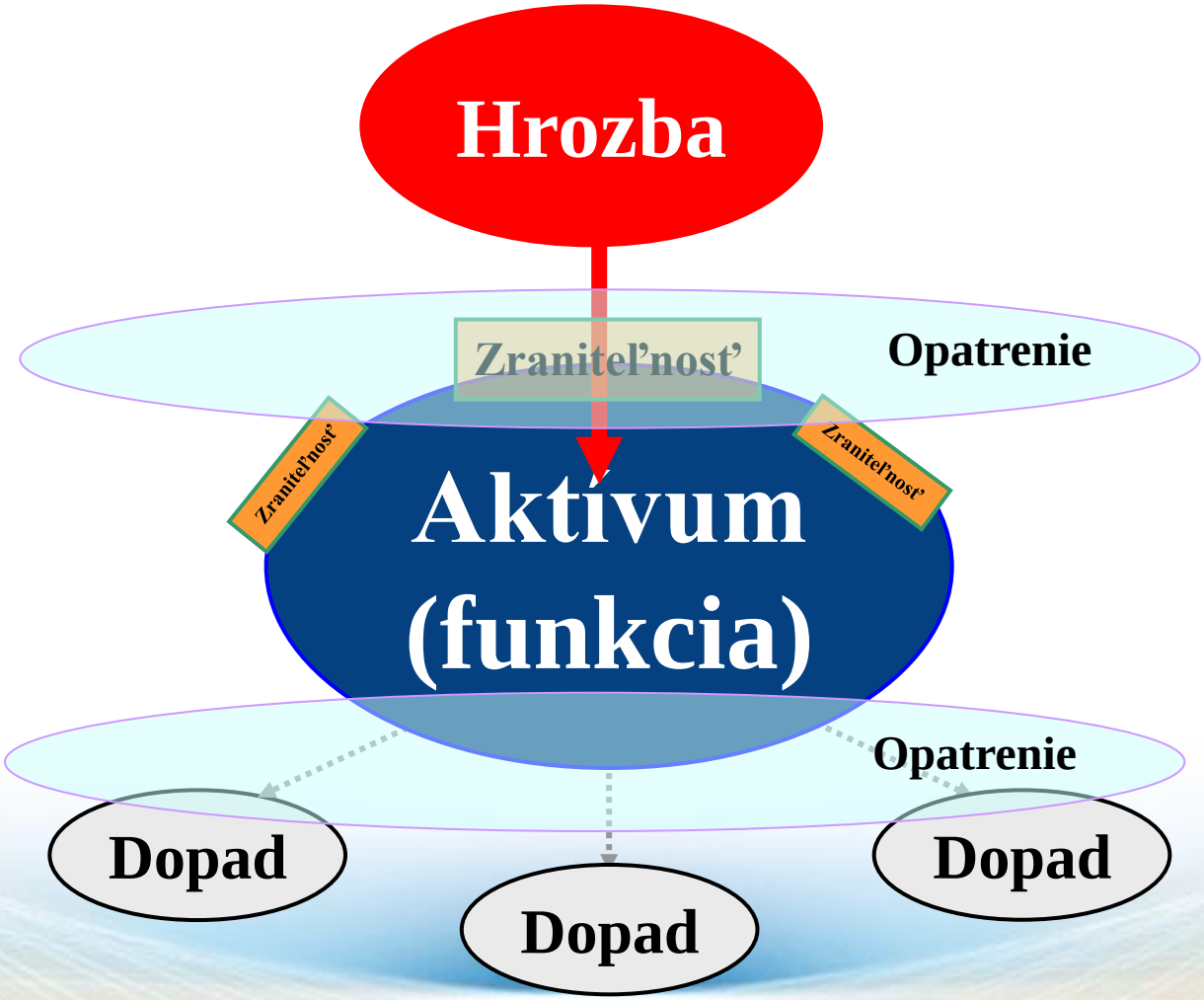
Ak nie, kto povie kde má byť aké?

A na základe čoho to povie?

Analýza rizík – prečo?



Analýza rizík – čo?



Analýza rizík – čo potrebujeme?

- Zoznam aktív (údaje, SW, HW, priestory, ľudia...)
- Hodnotenie aktív – ich dôležitosť pre fungovanie spoločnosti (možné následky v prípade narušenia ich dostupnosti, dôvernosti, integrity) – na základe dotazníkov, rozhovorov, pozorovania...
- Existujúce opatrenia – aktuálny stav

Príklad – poisťovňa ZDRAVIA

Analýza rizík – ako? - príklad

Aktívum	Hrozba		Zraniteľnost		Dopad	Riziko miera
	popis	hod	popis	hod		
Priestory serverovňa	Záplava	3	v záplavovej oblasti, na spodnom podlaží, bez BCP, bez NCS	3	3	27
	Poruchy dodávky el. energie	2	nedostatočná kapacita UPS	3	3	12
	Negatívne vplyvy prostredia	1	klima, antistat. podlahy,	1	2	2
	Krádež	2	riadený prístup SKV, mreže na oknách, PSN, EPS,	1	3	6
servery IS NEMOC	zničenie údajov a konfigurácií	1	zálohy, aj externe uložené, podľa plánu	1	3	3
	poruchy a chyby zariadení	2	starý server,	3	3	12
APV NEMOC	Chyby SW	1	riadený vývoj , testy,	1	2	2
administrátori	chyby personálu	2	dobre zaškolení, vysoké bezpečnostné povedomie,	1	2	4
	neautorizovaná činnosť	2	nestanovené pravidlá	3	3	12

Analýza rizík – čo z toho?

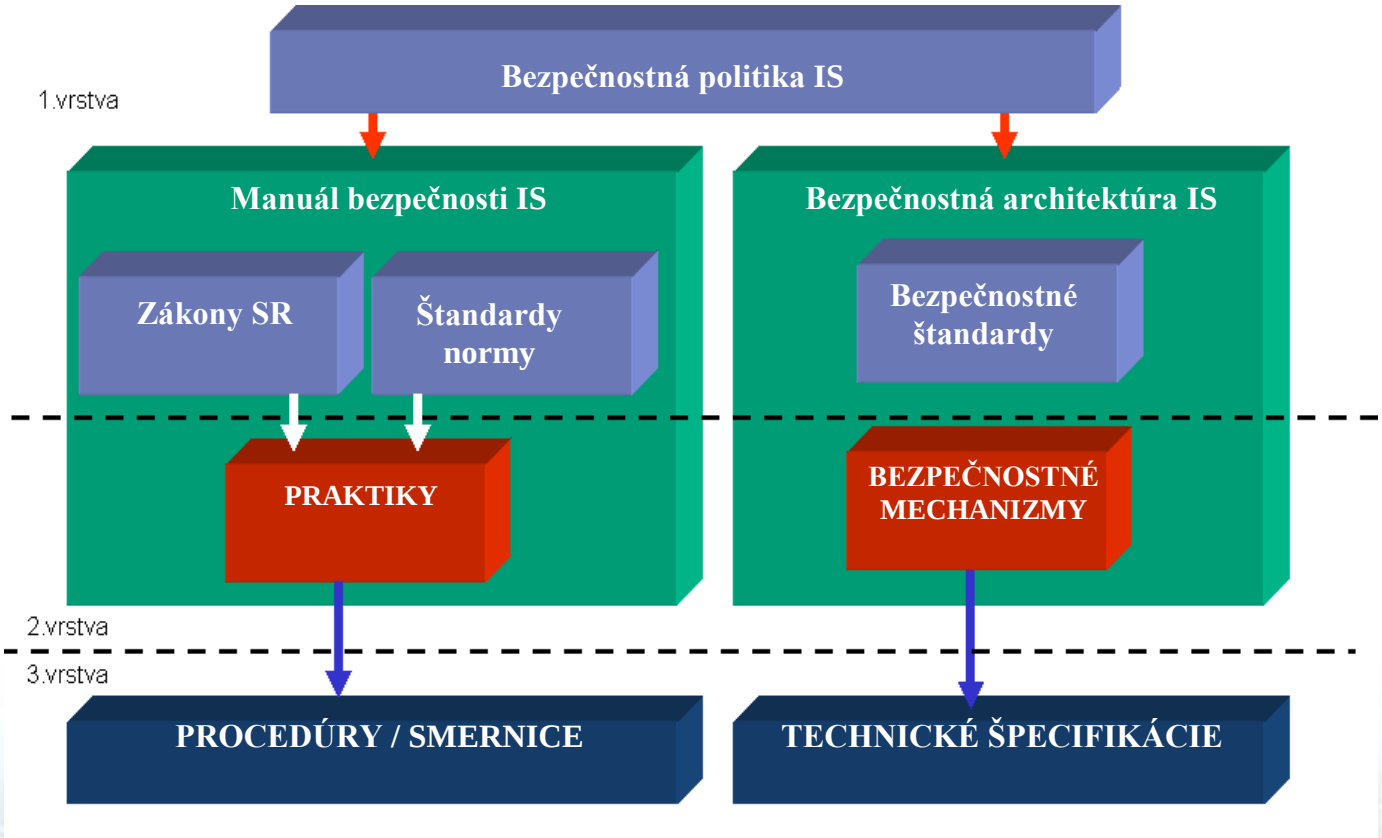
Riziká – treba prijať opatrenia na zníženie na akceptovateľnú úroveň.

Opatrenia – rôzne – z hľadiska:

- „sily“ (napr. heslo, karta, biometriky),
- typu (organizačné, technické, preventívne, minimalizujúce následky)
- finančnej náročnosti.

Výstup z analýzy – „Kde nás najviac tlačí topánka“, čo je prvoradé.

Riadiace dokumenty bezpečnosti - príklad



EMM

Analýza rizík

Normy a štandardy v tejto oblasti:

- ISO 31000 – Risk management – Principles and guidelines
- ISO 31010 – Risk management – Risk assessment techniques
- ISO 27005 Riadenie rizík informačnej bezpečnosti (pôvodne ISO 13335 časti 3 a 4)
- NIST SP 800-30 Risk Management Guide for Information Technology Systems (odporúčania National Institute of Standards and Technology)
- COBIT – Process P09 Assess and Manage Risks

Kto sme?

Nadnárodná spoločnosť (SR, ČR, Poľsko a Maďarsko):

Poisťovňa ZDRAVIA

Sídlo spoločnosti na Slovensku:

Košice, Jenisejská ul. 57

Lokalita a adresa dátového centra:

Košice, Tomášikova ul. 37

Čo robíme?

Poskytovanie nadštandardného zdravotného poistenia

- poistenie pri hospitalizácii:
  - Premium 1
  - Premium 2
  - Premium 3
- poistenie pracovnej neschopnosti spôsobenej chorobou alebo úrazom
- poistenie invalidity spôsobenej chorobou alebo úrazom
- poistenie pracovnej neschopnosti a hospitalizácii pri dopravnej nehode
- *pripoistenie LADY*
- *pripoistenie GENTLEMAN*
- *pripoistenie voľby lekára*

Prežijeme? (nie len v kríze?)

- *Aké sú obchodné ciele organizácie?*
- *Ako chce organizácia svoje obchodné ciele dosiahnuť?*
- *Aké sú produkty/služby organizáciou poskytované?*
- *Aké časové úseky sú dôležité v poskytovaní produktov a služieb?*
- *Kto každý (interné aj externé subjekty) je zahrnutý do procesu, ktorými budú obchodné ciele dosahované?*

Analýza dopadov

Odpovede:

- identifikované kritické procesy / obchodné činnosti
- stanovená kritickosť procesov a následne aplikácií / systémov, ktoré sú nevyhnutné pre dané procesy
- identifikované možné dopady (finančné aj nefinančné) v prípade narušenia uvedených procesov
- identifikované požiadavky na zabezpečenie obnovy procesov na minimálnu požadovanú úroveň

Služby IS / ICT sú podriadené potrebám obchodných / vecných útvarov. *Je potrebné si uvedomiť, že informatika poskytuje svoje služby vecným /obchodným útvarom na dosiahnutie obchodných cieľov organizácie.*

IS ZDRAVIE a pohľad na jeho dostupnosť

Vstup z BIA procesy – pohľad vlastníkov:

Proces poskytovania nadštandardného poistenia / IS ZDRAVIE.

Vlastník IS ZDRAVIE je vedúci úseku Poistenie (office – Budapešť).

- Požiadavky vlastníka procesu na dostupnosť IS ZDRAVIE je 48 hodín.
- Havarijné plány – neexistujú?!? Náhradné postupy – neexistujú.
- Požiadavky vlastníka na zálohovanie a archiváciu údajov – nevedomosť.

Vstup z BIA ICT - pohľad informatikov – aktuálne možnosti:

IS ZDRAVIE je kritickým systémom, ktorý spracúva informácie o výplatách poistného pri pobyte v nemocnici, pracovnej neschopnosti a invalidity. IS bol dodávkou „na kľúč" a o jeho správu a update zabezpečuje dodávateľská organizácia.

- Zálohovanie a archivácia (politika, typy záloh, uloženie médií a manipulácia s nimi).
- Havarijné plány - neexistujú, náhradné postupy – spísané len postupy ukladania / archivácie dát, záložné komponenty – neexistujú.
- aktuálny stav: RTO = !, RPO = 24hod (
- *súvisiaci IS Register: RTO = !, RPO = 24hod (spravovaný interne)*

33/ Prežijeme? (nie len / aj v kríze?)

Nadnárodná spoločnosť (SR, ČR, Poľsko a Maďarsko):

Poisťovňa ZDRAVIA

Sídlo spoločnosti na Slovensku:

Košice, Jenisejská ul. 57 – záplavová zóna

Lokalita a adresa dátového centra:

Košice, Tomášikova 37 – záplavová zóna

Neexistencia záložného dátového centra

Biznis-kritický proces poskytovania nadštandardného poistenia / IS ZDRAVIE (IS Register)

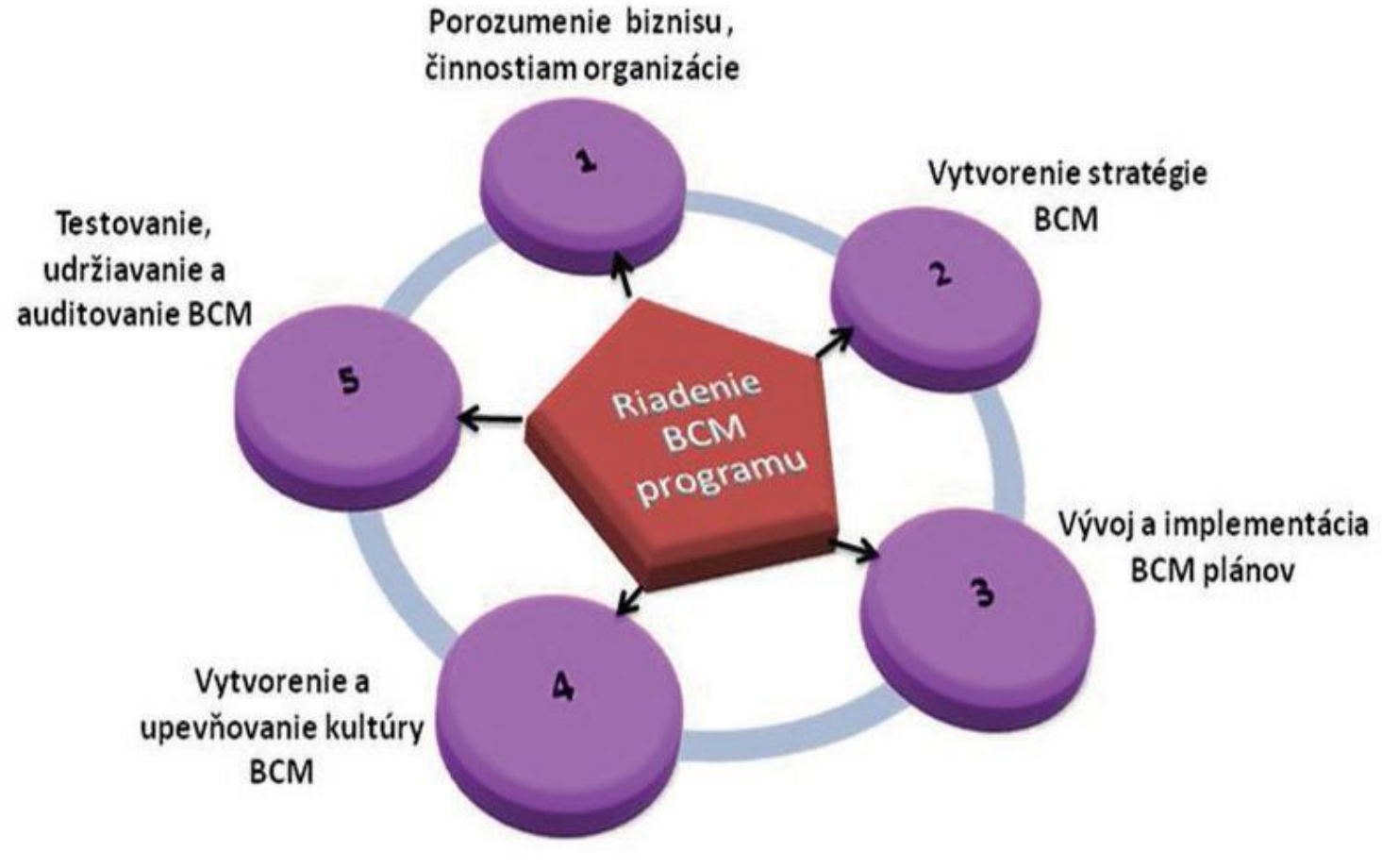
AKO na to?

Výstavba záložného dátového centra / outsourcing dátového centra ???

Dôležité pri výbere / rozhodnutí:

- Finančné a personálne možnosti.
- Lokalita / požiadavky na lokalitu - nachádza sa v lokalite blízko vášho biznisu?, Je mimo záplavovej zóny? Je to oblasť s nízkou pravdepodobnosťou hrozby seizmickej aktivity?
- Požiadavky na budovu - je určená výlučne pre účely dátového centra?
- Energetická efektívnosť (úspora energie pri nových DC až 25 %)
- Požadovaná / garantovaná **dostupnosť a spoľahlivosť** (Podľa metodiky Uptime Institute)
- Požiadavky na fyzickú a objektovú bezpečnosť – je areál dátového centra oddelený oplotením, kontrolovaný bezpečnostnými kamerami a nepretržite zabezpečený bezpečnostnou službou umiestnenou priamo v objekte dátového centra?
- V prípade outsourcingu – je zabezpečený princíp zónovania t.j. oddelenie IT sál od podporných non IT technológií do samostatných priestorov s oddeleným prístupom?

Business Continuity Mangement



Business continuity management

BS 25999:2006 Business continuity management – Part 1: Code of practice

BS 25999:2007 Business continuity management – Part 2: Specification

BS 25777:2008 Information and communications technology continuity management – Code of practice Understanding the ICT requirements for business continuity

BS ISO 22301:2012 Societal security — Business continuity management systems - Requirements

BS ISO 22313:2012 Societal security — Business continuity management systems - Guidance

BIP 2214:2011 - A practical approach to business impact analysis. Understanding the organization through business continuity management

Are you secure? I´m secure!

EMM, spol. s r. o.
Sekurisova ul. č. 16
841 02 Bratislava 42
Tel.: +421 (2) 602 54 111
Fax: +421 (2) 602 54 901
E-mail: emm@emm.sk

WWW.EMM.SK