IBM Security

Trendy v informačnej bezpečnosti - ochrana údajov: ako EÚ ovplyvní konanie firiem?

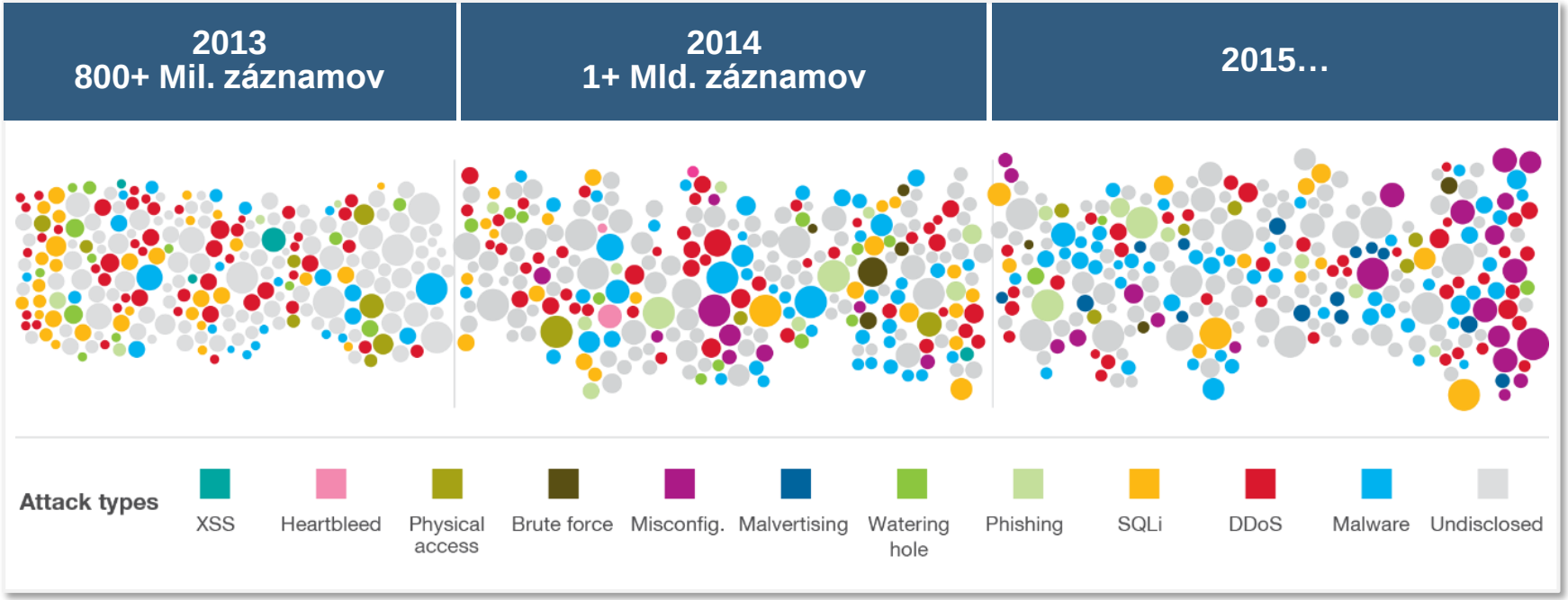
JARNÁ ITAPA 2017

Ivan Makatura

23. Máj 2017 Hotel Bôrik Bratislava

IBM

Nárast počtu, objemu a komplexnosti útokov je nespochybniteľný…



Priemerná doba detekcie pokročilého útoku

201 dní

Medziročný nárast počtu incidentov

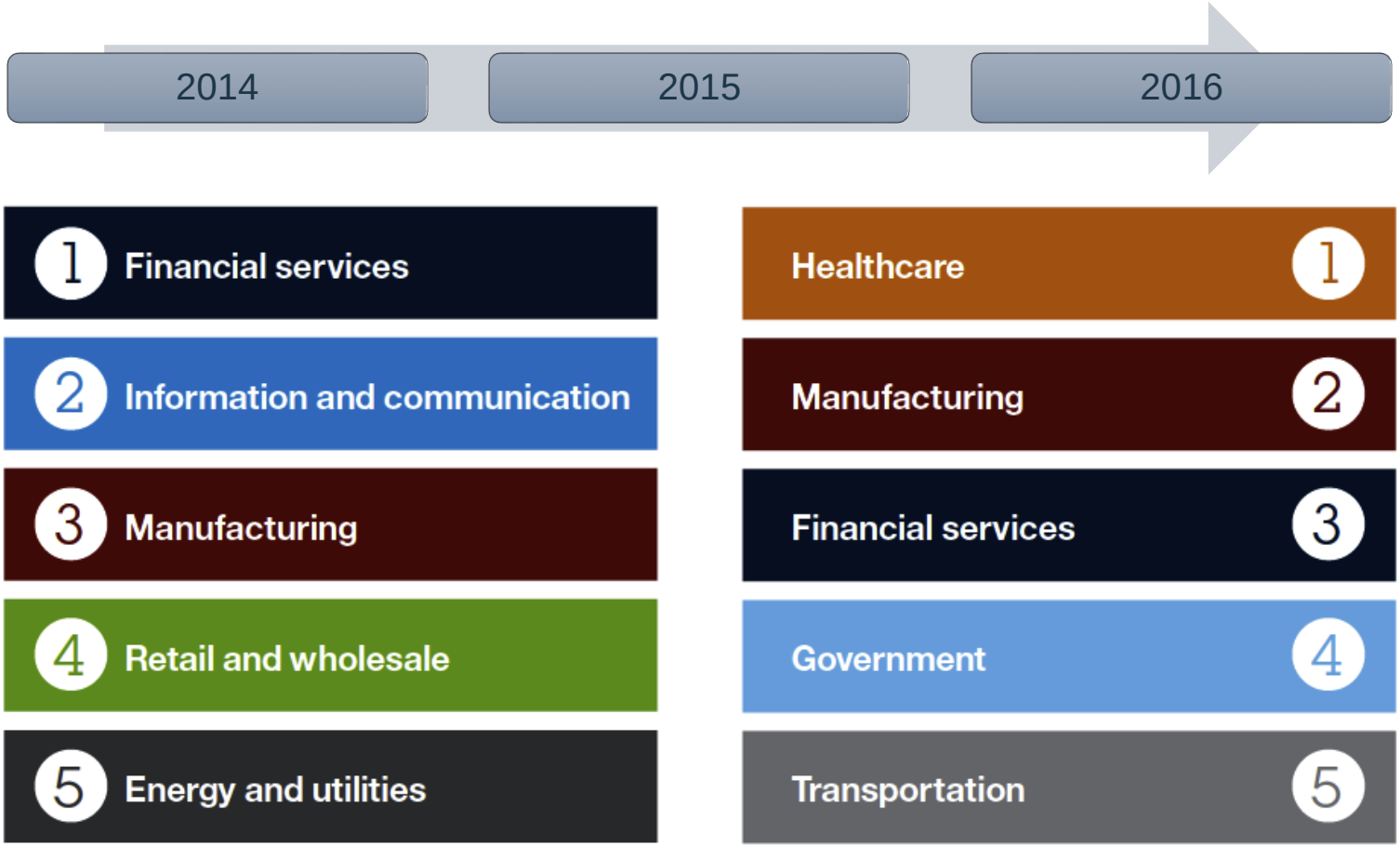
23%

Priemerné náklady incidentu v USA

3,79 Mil. USD

Zdroj: IBM X-Force Threat Intelligence Report - 2016

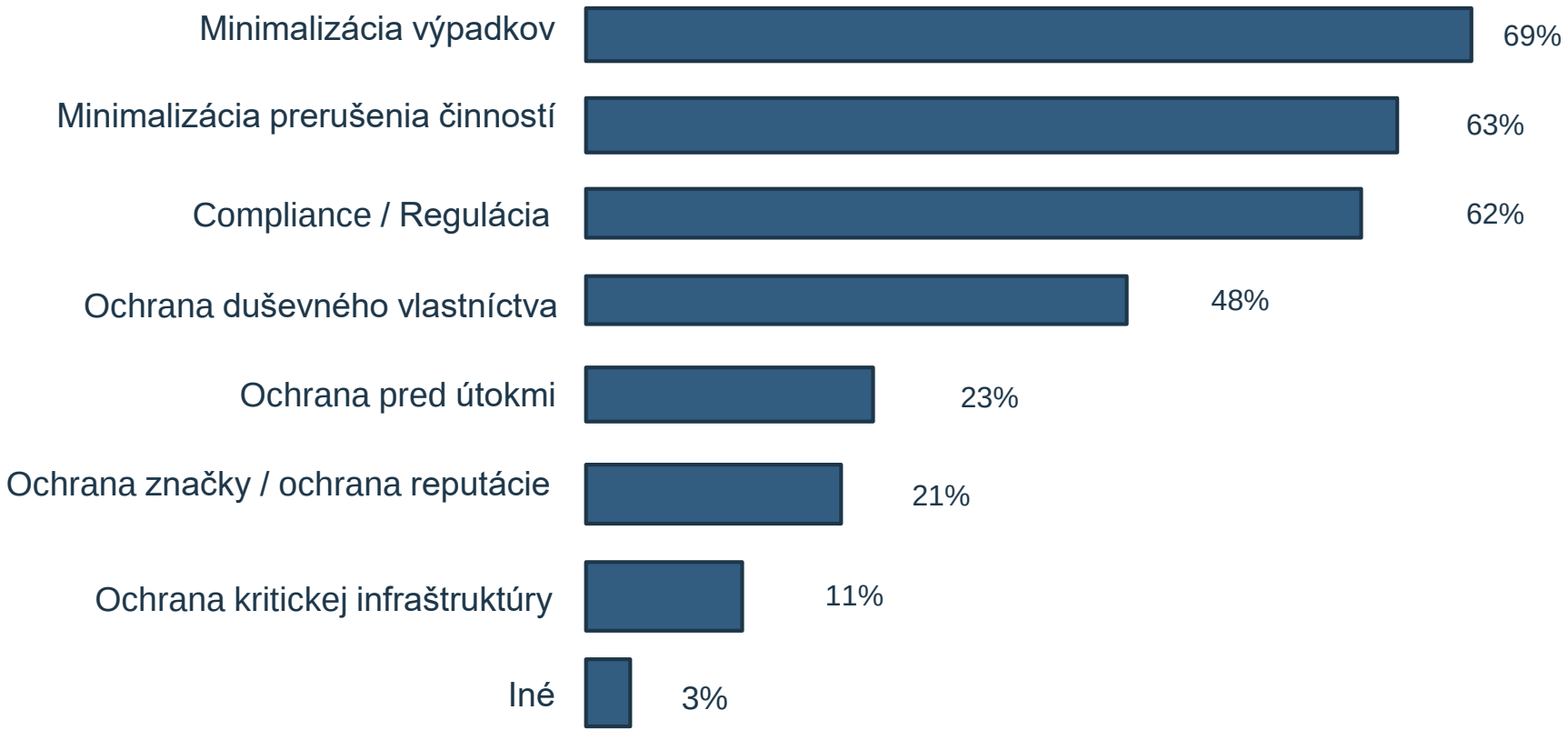
Distribúcia bezpečnostného rizika podľa odvetví



Zdroj: IBM X-Force Threat Intelligence Report - 2016

Je regulácia potrebná?

Typické objektívne dôvody pre riadenie bezpečnostného rizika…



Zdroj: Ponemon's 2016 Application Security Risk Study

Čo reálne poháňa bezpečnosť? (typické subjektívne dôvody)

Požiadavky na ochranu informačných aktív v slovenskej legislatíve

- Zákon č. 122/2013 Z. z. **o ochrane osobných údajov**
- Zákon č. 483/2001 Z. z. **o bankách**
- Zákon č. 272/2016 Z. z. **o dôveryhodných službách pre elektronické transakcie** na vnútornom trhu
- Zákon č. 351/2011 Z.z. **o elektronických komunikáciách**
- Zákon č. 215/2004 Z. z. **o o ochrane utajovaných skutočností**
- Zákon č. 45/2011 Z. z. **o kritickej infraštruktúre**
- Zákon č. 300/2005 Z. z. **trestný zákon**
- Zákon č. 275/2006 Z. z. **o informačných systémoch verejnej správy**
- Zákon č. 319/2002 Z. z. **o obrane SR**
- Výnos č. 55/2014 Z. z. **o štandardoch pre informačné systémy verejnej správy**

... v znení neskorších predpisov...

- Návrh zákona **o kybernetickej bezpečnosti**
- Návrh zákona **o výkone správy v oblasti informačných technológií verejnej správy (ITVS)**
- Pripravovaný zákon **o ochrane osobných údajov**

7

Požiadavky na ochranu informačných aktív v európskej legislatíve

- Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zaistenie vysokej spoločnej úrovne bezpečnosti sietí a informácií v Únii

  (The Network and Information Security Directive , ďalej len „**NIS**“)

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov

  (The General Data Protection Regulation, ďalej len „**GDPR**“)

- Smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu Únii

  (Payment Services Directive 2, ďalej len „**PSD2**“)

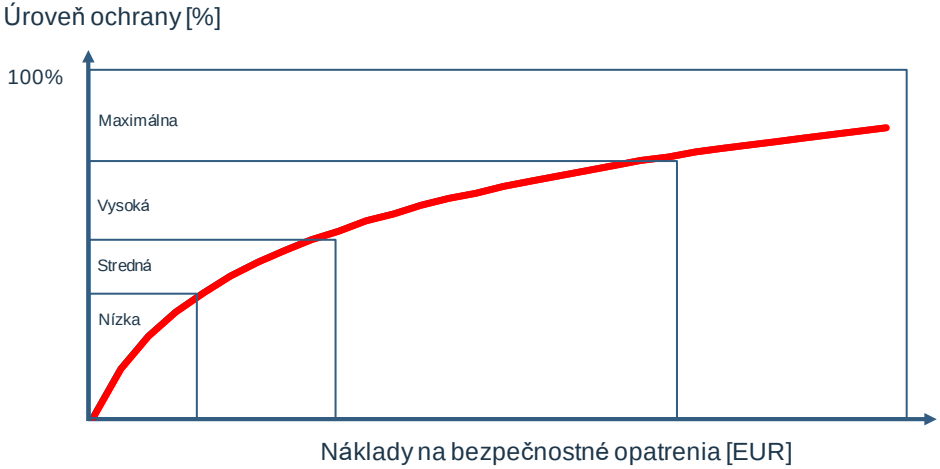
- Nariadenie Európskeho parlamentu a Rady (EÚ) 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu

  (Regulation on Electronic identification and trust services for electronic transactions

  ďalej len „**eIDAS**“)

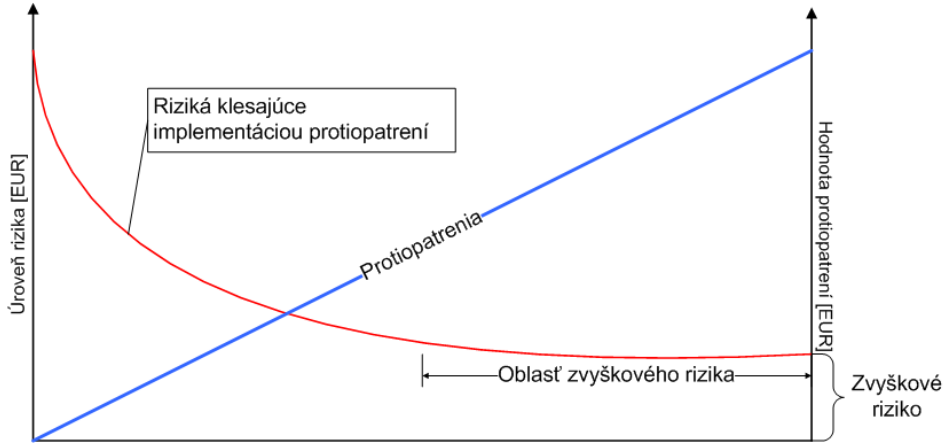
Náklady vyvolané reguláciou

Náklady vs. efektivita v informačnej bezpečnosti



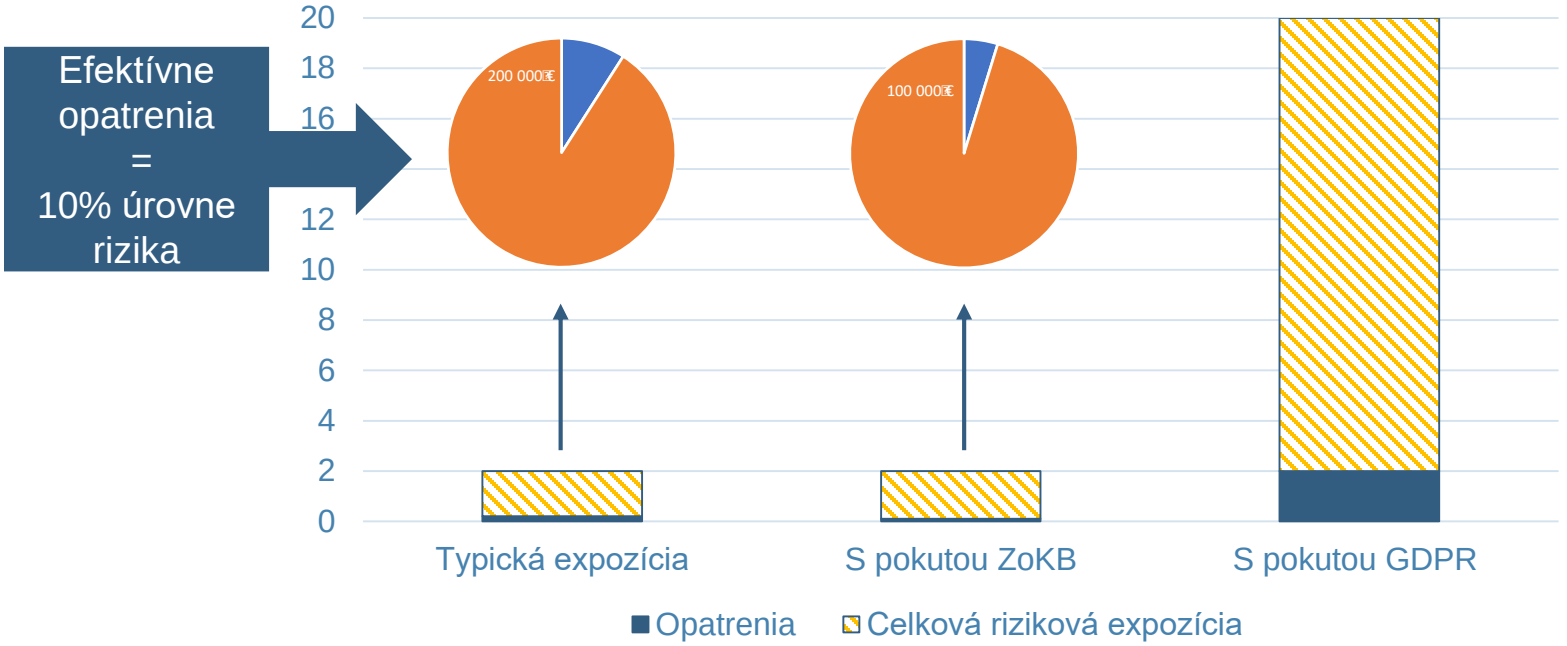
- Absolútna úroveň ochrany nie je dosiahnuteľná ani za predpokladu neobmedzených nákladov
- Je úlohou vlastníka rizík rozhodnúť o efektivite opatrení
- Cieľom regulácie je dosiahnuť žiadúce správanie zúčastnených subjektov

- Nulové riziko nie je dosiahnuteľné ani za predpokladu neobmedzených nákladov
- GDPR vyžaduje tzv. predbežnú konzultáciu zvyškových rizík (aká bude kompetencia ÚOOÚ v riadení rizík?)
- Štát nie je vlastníkom rizík, mal by teda v regulácii dodržiavať doktrínu „laissez-faire“ („nechajte nás konať“)



Zdroj: BSI Standard 100-2 IT-Grundschutz Methodology, v.1.0. Bundesamt für Sicherheit in der Informationstechnik

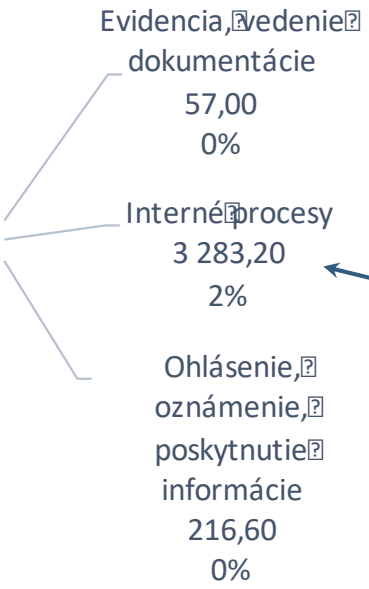
Nadmerné pokuty neprispievajú ku ošetreniu rizík, ale predstavujú nové riziko…



- GDPR namiesto zníženia rizík vytvára úplne nové hrozby, ktoré niekoľkonásobne prekročia hodnotu pôvodných identifikovaných rizík
- To môže spôsobiť zníženie prahu vnímania potreby ochrany údajov

Odhadované finančné dopady Zákona o kybernetickej bezpečnosti

TCO = 1 rok
Počet dotknutých subjektov = cca 160



- Riadenie bezpečnostných rizík
- Bezpečnosť systémov a zariadení
- Riadenie prevádzky IT
- Riadenie kybernetických bezpečnostných incidentov
- Riadenie dostupnosti siete a informačného systému
- Monitorovanie, testovanie bezpečnosti a bezpečnostné audity

- Kalkulačka nákladov Ministerstva hospodárstva SR
- agregovaná kalkulácia nákladov všetkých povinností, ktoré vyplývajú podnikateľom z predkladaného materiálu (založená na metodike „Activity Based Costing“)

Ako môže regulácia pomôcť?

Požiadavky akademickej sféry na právnu úpravu IB

Požiadavka	ZoKB	GDPR
Regulácie nesmú byť v rozpore s teoretickými princípmi informačnej bezpečnosti	✓	✗
Regulácie majú zlepšiť stav vzdelávania v informačnej bezpečnosti	✓	~
V rámci SR sa zvýši odborná spôsobilosť všetkých subjektov v interakcii s IKT	✓	✓
Zavedené certifikačné schémy poslúžia ako metrika kvalifikácie	✓	✗
Regulácie majú zabezpečiť implementáciu informačnej bezpečnosti prostredníctvom sústavy kvalifikácií	~	✗
Zákon má tlačiť na stratégiu v technickej normalizácii v oblasti IB	✓	✗

Požiadavky komerčných subjektov na právnu úpravu IB

Proces / Požiadavka	ZoKB	GDPR
Riadenie rizík		
• V SR vznikne ustálená a unifikovaná schopnosť riadenia bezpečnostných rizík	✓	~
• Manažment rizík sa stane základným a hlavným východiskom pre meranie efektivity protiopatrení	✓	✓
• Požiadavky na proces nesmú byť formálne (papierová bezpečnosť neznižuje úroveň rizík)	✓	✗
• Penalizácie budú primerané	✓	✗
Bezpečnostná architektúra		
• Kritické systémy a siete budú bezpečné a odolné proti všetkým známym narušeniam, náhodným alebo úmyselným	✓	~
Overovanie súladu		
• Požiadavky regulácie musia byť auditovateľné	✓	~
• Musí byť stanovená metrika pre auditing	~	✗
• Musia byť stanovené minimálne kvalifikačné požiadavky pre auditorov	~	~

Požiadavky komerčných subjektov na právnu úpravu IB

Proces / Požiadavka	ZoKB	GDPR
Pravidlá reakcie na bezpečnostné incidenty		
• Pravidlá procesu reakcie na incidenty musia byť prehľadne definované	✓	✗
• Zákon musí prinášať výhody vo forme zlepšenia procesu:		
- systém včasnej reakcie	✓	✗
- koordinácia reakcie (musí byť efektívna a zmysluplná, nie formálna)	✓	✗
Notifikácia incidentov		
• Má byť povinná až od určitej relevantnej hodnoty (threshold)	✓	~
• Musí byť vhodne štatisticky spracovaná a použitá pre budúce zlepšenie stavu IB	✓	✗
• Obnoviť princíp „Single Point of Contact“	~	~

IBM Security

ĎAKUJEM

SLEDUJTE NÁS NA:

ibm.com/security

securityintelligence.com

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions

ivan.makatura@sk.ibm.com

IBM