IBM Security

Manažment bezpečnostných rizík (aj) vo verejnej správe

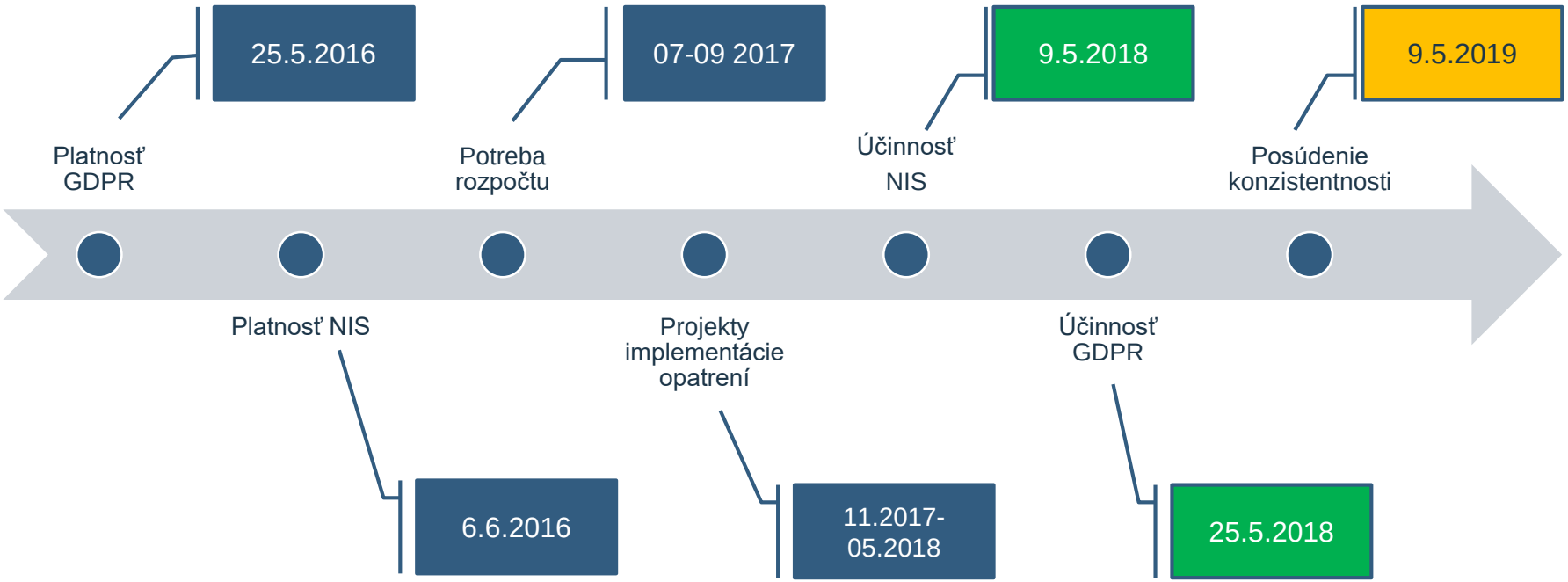
ITAPA 2018

Ivan Makatura
IBM Slovensko, s.r.o.

20. Marec 2018 Poprad

IBM

Lehoty, ktoré stoja za pripomenutie…



Ochrana údajov...? Informačná bezpečnosť...? Kybernetická bezpečnosť...?

Typické subjektívne dôvody pre ochranu informačných aktív

OCHRANA KRITICKEJ INFRAŠTRUKTÚRY
11%

OCHRANA ZNAČKY OCHRANA REPUTÁCIE
21%

PREVENCIA INCIDENTOV
34%

SÚLAD S REGULÁCIOU
62%

MINIMALIZÁCIA VÝPADKOV PRODUKCIE
69%

Zdroj: Ponemon's 2016 Application Security Risk Study

Zodpovednosť Prevádzkovateľa podľa GDPR

- Prevádzkovateľ prijme vhodné technické a organizačné opatrenia, aby:
  - **zabezpečil**, že spracúvanie sa vykonáva v súlade s Nariadením
  - **bol schopný preukázať**, že spracúvanie vykonáva v súlade s Nariadením
- Opatrenia majú byť prijaté s ohľadom na:
  - povahu, rozsah, kontext a účely spracúvania,
  - riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb
- Uvedené opatrenia sa podľa potreby **preskúmajú** a aktualizujú

Riadenie rizík

Komponenty kybernetickej bezpečnosti

Odolnosť voči hrozbám je kombináciou viacerých disciplín

Organizácia	Technologické prostredie
Ochrana údajov	Klasifikácia informácií
Riadenie IT rizík	Manažment zrnaniteľností
Havarijné plánovanie	Security Governance
IT architektúra	Riadenie aktív
Riadenie prístupov	Riadenie zmien a konfigurácií
Riešenie incidentov	Service Level Management
Vzťahy a komunikácia	Biznis architektúra
Ekosystém partnerov	Vzdelávanie a povedomie

GDPR vs. NIS? Nájdite dva rozdiely...

NIS / ZoKB:	GDPR / ZOOÚ:
• Orientovaná najmä na zaručenie odolnosti voči technickým zraniteľnostiam	• Orientovaná na zaručenie práv dotknutých osôb
• Prostredníctvom požiadavky aby prevádzkovateľ základnej služby prijal dodržiaval bezpečnostné opatrenia	• Prostredníctvom požiadavky aby prevádzkovateľ prijal vhodné technické a organizačné opatrenia
• **kybernetický bezpečnostný incident** = akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, negatívny vplyv na kybernetickú bezpečnosť	• **porušenie ochrany** = porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu spracúvaných osobných údajov

Bezpečnosť informácií = stav, v ktorom sú informácie považované za zabezpečené voči hrozbám

Porušenie ochrany osobných údajov = bezpečnostný incident

Ochrana údajov = informačná bezpečnosť.

Riadenie bezpečnosti je udržiavanie akceptovateľnej miery identifikovaného rizika