www.pwc.com

Dopad legislativních změn v informační bezpečnosti na interní audit

Tomáš Pluhařík

pwc

IT v interním auditu

Úrovně poznání

1

- Politiky
- Dokumentace a evidence

2

- Reálně implementované procesy
- Logy a provozní záznamy

3

- Implementovaná infrastruktura
- Incidenty

4

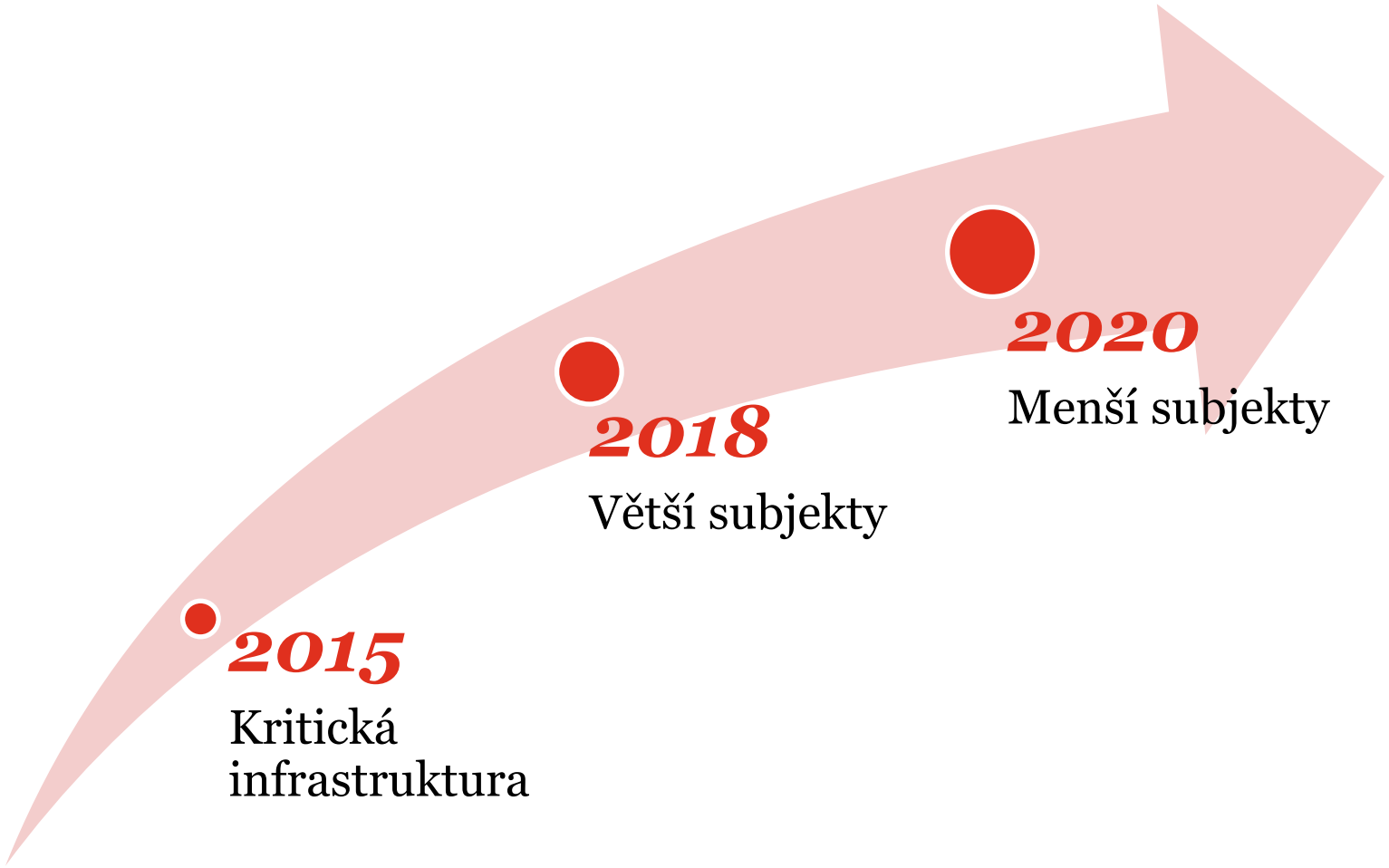
- Reálný provoz na infrastruktuře

Otázka za miliardu …

Je to problém?

- Bezprecedentní přesun odpovědností
- Odpovědnost za škody způsobené
- Masivní regulace všech sektorů
- Nárůst zneužití infrastruktur pro napadání jiných subjektů

Otázka za miliardu …



Aktuální legislativa a rozhodnutí

- *Zákon o kybernetické bezpečnosti (2014) č. 181/2014 sb.*
- *Zákon o ochraně osobních údajů č. 101/2000 sb.*
- *EU Data protection directive > General data protection regulation (GDPR)*
- *EU Network Information Security (NIS) Directive*
- *Electronic identification and trust services (eIDAS)*
- *Industry specific standards and laws*

- *Právo být zapomenut*
- *…*

Zákon o kybernetické bezpečnosti (2014) č. 181/2014 sb. + prováděcí vyhláška

POSITIVE

- ✓ Definuje kritickou infrastrukturu státu a významné systémy státu
- ✓ Definuje národní CERT tým a jeho roli
- ✓ Stát přenáší odpovědnosti a povinnosti na subjekty zákona
- ✓ Zákon definuje struktury, procesy a přístupy, které mají být použity v informační bezpečnosti
- ✓ Zákon definuje role, které mají být zavedeny u subjektů zákona
- ✓ Odpovědnost za škody způsobené v případě prolomení nezabezpečené infrastruktury
- ✓ Zákon zasahuje jak veřejný, tak soukromý sektor

NEGATIVE

- x Stát přenáší odpovědnosti a povinnosti na subjekty zákona
- x Definice dotčených subjektů není jasná a bude upřesňovaná během roku 2015
- x Pokuty jsou velmi nízké a mohou být ignorovány komerčními subjekty
- x NBU a CERT nemají vynucovací pravomoci a kapacitu

Výzvy z pohledu interního auditu a IT

- Nejasné rozdělení dotčených subjektů
- Úplně nová sada pravidel k auditování
- Neustálená prováděcí vyhláška a očekávaná novelizace zákona
- Zákon definuje dobře governance a proces reportování problému a už hůře (spíše vůbec) technická protiopatření

- Pokuty vyplývající ze zákona jsou mizivé, ale větší rizika přináší zákony přidružené
- Současný IT management zákon ještě úplně nebere vážně
- Obecně existuje velmi slabé povědomí o informační bezpečnosti i na IT úrovni

Časté nedostatky

- Absence strategie IT a (informační) bezpečnosti
- Organicky rostlé IT
- Syndrom statického přístupu k bezpečnosti – *„Takhle sme to tady dělali vždycky“*
- Papírové politiky bez reálného dopadu do provozu
- Závislý pohled provozovatele

Co s tím?

- Konzervativně vyhodnotit jestli se mě zákon dotýká i s ohledem na další legislativní změny v horizontu 5 let
- Compliance check (i vůči ostatním zákonům)
- SAM, Data a Infrastructure audit

- Information security audit (pozor toto není compliance check)
- Definice strategie (informační) bezpečnosti
- Implementace náprav
- *Modlit se, že než se to opraví tak na vás NBU nepřijde …*

Zákon o ochraně osobních údajů č. 101/2000 sb.

POSITIVE

- ✓ Definuje problematiku ochrany dat na obecné úrovni
- ✓ Definuje typy dat
- ✓ Definuje pravidla jak data zpracovávat
- ✓ Definuje práva subjektů a vlastníků dat
- ✓ Definuje anonymizaci
- ✓ Výslovně nezakazuje zpracování dat se souhlasem majitele těchto dat

NEGATIVE

- x Definuje problematiku ochrany dat na obecné úrovni
- x Omezuje zavedení cloudových řešení
- x Omezuje zavedení masivnějšího vytěžování dat za účelem další monetizace
- x Komplikuje zavádění některých bezpečnostních/forenzních kroků pokud narazíte na subjekty bez souhlasu o zpracování
- x V horizontu nejbližších 2 let bude nahrazen GDPR

Výzvy z pohledu interního auditu a IT

- IT musí při zavádění nových technologií a procesů brát ohled na to, že některé datové vstupy mohou být považovány za osobní nebo citlivé údaje
- Zpracování citlivých/osobních údajů v případě auditu a nebo forenzním vyšetřování je „na hraně“
- Bezpečnostní vyšetřování může být komplikováno právem vlastníka na informaci o tom jak jsou jeho data zpracovávána

- Pro dodržení paragrafu 13 je důležité studovat detailní reálné implementace a provoz který data zpracovává a ukládá
- Paragraf 13 je také důležitým vodítkem pro opatření překrývající se se Zákonem o kybernetické bezpečnosti
- Jakékoliv předávání dat mimo EU podléhá regulaci paragrafem 27 a bude dále omezováno v rámci GDPR

Časté nedostatky

- Neexistující strategie nakládání s daty
- Syndrom meziúložiště – data jsou často v rámci technologického procesu ukládána mimo systémy na nekontrolovaných meziúložistích s mizivou kontrolou přístupu
- Syndrom univerzálního uživatele

- Syndrom falešné anonimizace
- Data přenášená mimo jurisdikci EU v rámci cloudových řešeni
- Paralelní procesy zaváděné kreativitou operations týmů
- Vynášení dat mimo procesy

Co s tím?

- Konzervativně vyhodnotit **JAK** se mě zákon dotýká v IT i s ohledem na další legislativní změny v horizontu 5 let
- Compliance check (i vůči ostatním zákonům)
- SAM, Data a Infrastructure audit

- Data privacy audit (pozor toto není compliance check)
- Definice strategie (informační) bezpečnosti
- Implementace náprav
- *Modlit se, že než se to opraví tak na vás NBU a UOOU nepřijde …*

Quickwins a náprava

- Zapojení IT/cybersecurity auditorů do interních auditů (reálná možnost zapojení třetích stran)
- Prohloubení auditu IT až na úroveň 3 a 4

- Vytvoření bezpečnostních a data strategií na IT konzultovaných na všech úrovních (včetně compliance checku v rámci interního auditu)

Otázky

Kontakt

Tomáš Pluhařík
manager
Mobil: +420 775013225
E-mail:
tomas.pluharik@cz.pwc.com

Děkuji za pozornost!