Deloitte.

Soulad se zákonem o kybernetické bezpečnosti

Prevence a potlačování bezpečnostních hrozeb a kybernetických útoků patří mezi strategické zájmy současné společnosti.

Útoky se přesouvají do oblasti organizované kybernetické průmyslové špionáže a kybernetického terorismu. Útočníci se stále více zaměřují na prvky kritické infrastruktury, jako jsou energetické systémy, produktovody, zdravotnické informační systémy a informační systémy veřejné správy.

Proto je v celém světě a nejen v České republice současným trendem oblast bezpečnosti a ochrany informačních technologií před zásahy, které mohou ohrozit jejich fungování, důvěrnost, dostupnost a integritu dat.

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti si klade za cíl zvýšit bezpečnost kybernetického prostoru, nastavit mechanismus aktivní spolupráce mezi soukromým sektorem a veřejnou správou za účelem vyšší efektivity při řešení kybernetických bezpečnostních událostí a v této souvislosti zavádí do praxe soubor oprávnění a povinností.

V souladu s požadavky zákona o kybernetické bezpečnosti musí organizace aplikovat sadu bezpečnostních opatření, které se významně shodují s požadavky na certifikaci dle ISO/IEC 27001.

Koho se zákon týká?

1. Poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací
2. Orgán nebo osoba zajišťující významnou síť
3. Správce informačního systému kritické informační infrastruktury,
4. Správce komunikačního systému kritické informační infrastruktury
5. Správce významného informačního systému.

Jaké jsou základní povinnosti?

1. Oznámit kontaktní údaje
2. Detekovat kybernetické bezpečností události
3. Hlásit kybernetické bezpečnostní incidenty
4. Zavést bezpečnostní opatření
5. Provádět opatření vydaná NBÚ a ve stanovené lhůtě oznámit výsledek opatření.

Kompetence Deloitte:

- Deloitte CyberSOC - tým profesionálů, kteří celosvětově poskytují provoz bezpečnostního monitoringu na bázi služby SaaS v provozním módu 24x7.
- Systémový přístup k řízení bezpečnosti informací a naplnění požadavků zákona o kybernetické bezpečnosti.
- Realizované mezinárodní i vnitrostátní projekty z oblasti systému řízení bezpečnosti informací podle standardu ISO/IEC 27001 a 27002.
- Odborníci s rozsáhlými zkušenostmi z oblasti veřejného sektoru, financí, energetiky a IT.
- Právní poradenství v oblasti IT s využitím vlastní renomované právnické kanceláře Ambruz & Dark Deloitte Legal s.r.o.
- Kontinuální vzdělávání konzultantů v oblasti informační bezpečnosti – certifikace CISA, CISM, CRISC, CISSP, CGEIT a další.
- Zajištění podpory řízení IT projektů a jejich kvality Odborníci s rozsáhlými zkušenostmi s projektovým řízením, kteří ovládají řadu metodik a nástrojů pro podporu řízení projektů, a to jak vlastních (např. Project Management Metod - PMM), tak i specificky zaměřených na konkrétní případy

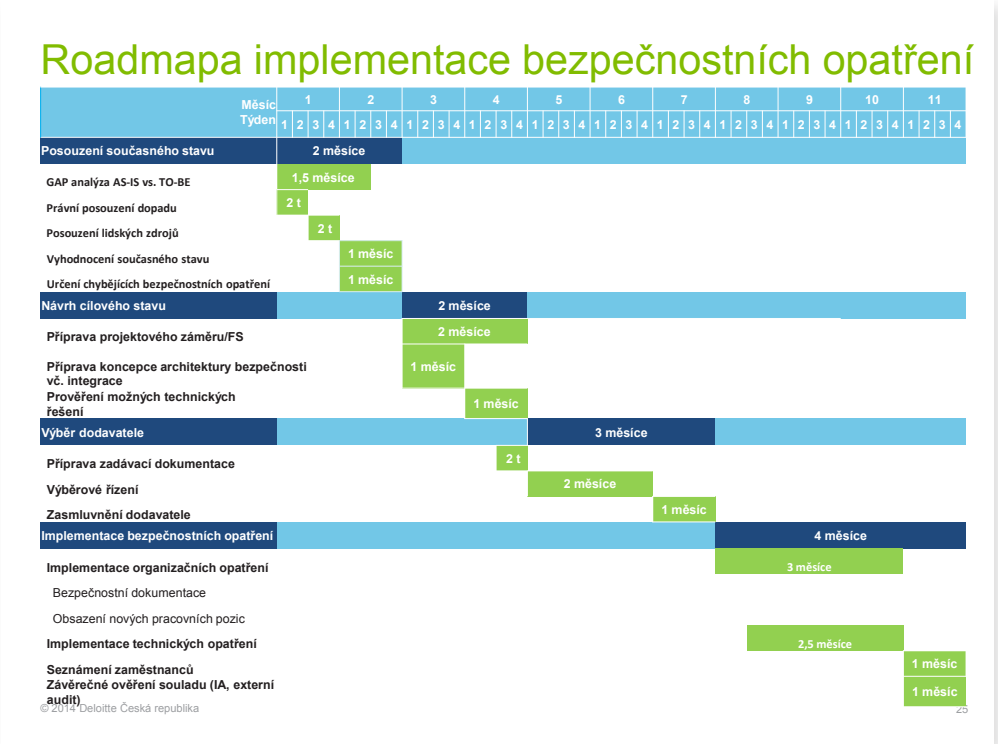
Odpovědnost a sankce v případě nesplnění požadavků daných zákonem

- Zákaz používání systému v případě nedostatků
- Sankce při nesplnění povinností stanovených zákonem až do výše 100 000 Kč i opakovaně
- Občanskoprávní odpovědnost, odpovědnost statutárních orgánů, řídících osob
- Vznik škody třetím subjektům
- Odpovědnost zaměstnanců v oblasti kybernetické bezpečnosti dle pracovněprávních předpisů

Deloitte ČR je připraven pomoci dosáhnout určeným subjektům souladu se zákonem o kybernetické bezpečnosti.

Roadmapa implementace bezpečnostních opatření:

1. **GAP analýza** současného stavu a požadavků kladených zákonem o kybernetické bezpečnosti na základě metodiky společnosti Deloitte včetně právního posouzení dopadu.
2. **Návrh cílového stavu** včetně zpracování Feasibility Study, prověření dostupných technických řešení a případných dodavatelů formou RfI
3. **Implementační plán** prioritizovaných protiopatření naplňujících požadavky zákona o kybernetické bezpečnosti zahrnující i oblast výběrového řízení vč. poskytnutí podpory při výběrovém řízení.
4. **Implementace navržených protiopatření** a nastavení procesů komunikace s ústředními orgány státní správy. Součástí je poskytnutí projektové podpory a QA, tvorba požadované bezpečnostní dokumentace, poskytnutí služby Security As A Service – Security Operations Centre.
5. **Post implementační aktivity** jsou zaměřeny na zvyšování přidané hodnoty procesů řízení informační bezpečnosti v souladu se zákonem o kybernetické bezpečnosti a s životním cyklem ISMS. Součástí je závěrečný bezpečnostní audit.



Bezpečnostní opatření podle zákona

- Systém řízení bezpečnosti informací
- Řízení rizik
- Bezpečnostní politika (ISO 27K)
- Organizační bezpečnost
  - Manažer kybernetické bezpečnosti
  - Architekt kybernetické bezpečnosti
  - Auditor
  - Garant aktiv
- Stanovení bezpečnostních požadavků pro dodavatele
- Řízení aktiv
- Bezpečnost lidských zdrojů
- Řízení provozu a komunikací KII/VIS
- Řízení přístupu ke KII/VIS
- Akvizice, vývoj a údržba KII/VIS
- Zvládání KBU/KBI
- Řízení kontinuity činností
- Kontrola a audit KII a VIS
- Fyzická opatření
- Nástroj pro ochranu integrity komunikačních sítí
- Nástroj pro ověřování identity uživatelů
- Nástroj pro řízení přístupových oprávnění
- Nástroj pro ochranu před škodlivým kódem
- Nástroj pro zaznamenávání činnosti KII a VIS, jejich uživatelů, administrátorů
- Nástroj pro detekci KBU
- Nástroj pro sběr a vyhodnocení KBU
- Aplikační bezpečnost
- Kryprografické prostředky
- Nástroj pro zajišťování úrovně dostupnosti informací
- Bezpečnost průmyslových a řídících systémů

Kontakt

Vlastimil Červený
Senior Manager
+420 737 210 667
vcerveny@deloitteCE.com

Richard Boura
Senior Manager
+420 602 182 778
rboura@deloittece.com

Deloitte označuje jednu či více společností Deloitte Touche Tohmatsu Limited, britské privátní společnosti s ručením omezeným zárukou („DTTL"), jejích členských firem a jejich spřízněných subjektů. Společnost DTTL a každá z jejích členských firem představuje samostatný a nezávislý právní subjekt. Společnost DTTL (rovněž označovaná jako „Deloitte Global") služby klientům neposkytuje. Podrobný popis právní struktury společnosti Deloitte Touche Tohmatsu Limited a jejích členských firem je uveden na adrese www.deloitte.com/cz/onas.

© 2014 Deloitte Česká republika