BESPOKE COUNSELS

ROWAN LEGAL

ZÁKON O KYBERNETICKÉ BEZPEČNOSTI A NAVAZUJÍCÍ PROVÁDĚCÍ PŘEDPISY

JUDr. Josef Donát, LLM,
ROWAN LEGAL, advokátní kancelář s.r.o.

Řízení informatiky v soukromém a veřejném sektoru, 23.1. 2015, Praha

MEMBER OF MULTILAW

KYBERNETICKÁ BEZPEČNOST

- Kybernetický prostor (§2 písm. a) ZKB):

digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací

MEMBER OF MULTILAW

ZÁKON O KYBERNETICKÉ BEZPEČNOSTI

- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- Schválen Senátem, podpis prezidenta 13.8.2014
- Účinnost od 1. 1. 2015

MEMBER OF MULTILAW

PROVÁDĚCÍ PŘEDPISY

- Nařízení vlády, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
- Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
- Vyhláška o významných informačních systémech a jejich určujících kritériích
- Publikováno ve Sbírce zákonů: 19.12.2014

MEMBER OF MULTILAW

CÍLE

- Ochrana jednotlivců
- Ochrana státu
- Závazky vůči zahraničí (EU Cybersecurity Directive)

MEMBER OF MULTILAW

PRINCIPY A NÁSTROJE

- Dva CERTy (Cybersecurity emergency response team)
  - – Národní CERT
  - – Vládní CERT (NBÚ)
- Registrace
- Oznamování
- Bezpečnostní standardy
- Ukládání protiopatření

MEMBER OF MULTILAW

POVINNÉ SUBJEKTY

- Poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací
- Subjekty zajišťující významné sítě
- Správci **významných informačních systémů**
- Správci **komunikačních systémů** zaražených do **kritické informační infrastruktury**
- Správci **informačních systémů** zaražených do **kritické informační infrastruktury**

ROWAN LEGAL
MEMBER OF MULTILAW

ELEKTRONICKÉ KOMUNIKACE

- Poskytovatelé služeb a subjekty zajišťující sítě
- Povinnosti
  – Hlásit kontaktní údaje národnímu CERT
- Ve stavu kybernetického nebezpečí
  – Provádět reaktivní protiopatření NBÚ

MEMBER OF MULTILAW

VÝZNAMNÉ SÍTĚ

- Přímé zahraniční propojení nebo přímé připojení ke kritické informační infrastruktuře
- Povinnosti
  - Hlásit kontaktní údaje národnímu CERT
  - Detekovat a reportovat bezpečnostní incidenty národnímu CERT
- Ve stavu kybernetického nebezpečí
  - Provádět reaktivní protiopatření NBÚ

ROWAN LEGAL
MEMBER OF MULTILAW

VÝZNAMNÉ INFORMAČNÍ SYSTÉMY

- Informační systémy orgánů veřejné moci, u kterých narušení bezpečnosti informací může ohrozit nebo výrazně omezit výkon činnosti veřejné správy
- Povinnosti
  - Hlásit kontaktní údaje NBÚ
  - Zpracovávat bezpečnostní dokumentaci
  - Zavádět bezpečnostní opatření
  - Detekovat a reportovat bezpečnostní incidenty NBÚ
  - Provádět protiopatření NBÚ

ROWAN LEGAL

MEMBER OF MULTILAW

KRITICKÁ INFORMAČNÍ INFRASTRUKTURA

- Prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy podle zákona o krizovém řízení
- Povinnosti
  - Hlásit kontaktní údaje NBÚ
  - Zpracovávat bezpečnostní dokumentaci
  - Zavádět bezpečnostní opatření
  - Detekovat a reportovat bezpečnostní incidenty NBÚ
  - Provádět protiopatření NBÚ

ROWAN LEGAL

MEMBER OF MULTILAW

STAV KYBERNETICKÉHO NEBEZPEČÍ

- Ohrožení systémů, sítí či zájmů ČR
- Předseda vlády na návrh ředitele NBÚ
- Možnost ukládat protiopatření všem provozovatelům sítí a poskytovatelům služeb elektronických komunikací

ROWAN LEGAL

MEMBER OF MULTILAW

APLIKACE V RÁMCI PČR

- Významné informační systémy
  - Vyhláška NBÚ a MV o významných informačních systémech
  - Konkrétní výčet + obecná kritéria
  - Nezbytné pro výkon rozhodujících činností orgánu veřejné moci
  - Ohrožení nebo omezení činnosti s negativní dopadem na veřejné zájmy
  - **Výběr informačních systémů provede správce na základě svého posouzení**
- Kritická infastruktura (sítě/systémy)
  - Nařízení vlády o kritériích pro určení prvku kritické infrastruktury - odvětví kybernetická bezpečnost
  - určení usnesením vlády či opatřením obecné povahy NBU

MEMBER OF MULTILAW

KONKRÉTNÍ POVINNOSTI

- Nahlásit kontaktní údaje NBÚ
- Zavést bezpečnostní opatření
- Zpracovat bezpečnostní dokumentaci
- Detekovat a oznamovat bezpečnostních incidenty NBÚ
- Provádět protiopatření NBÚ

ROWAN LEGAL

MEMBER OF MULTILAW

KONTAKTNÍ ÚDAJE

- Do 31. 1. 2015 či do 30 dnů od vzniku povinnosti oznámit NBÚ
- Údaje orgánu
  – Název, adresa sídla, identifikátor orgánu veřejné moci/IČO
- Údaje o fyzické osobě, která je za orgán oprávněna jednat ve věcech ZKB
  – Jméno, příjmení, telefonní číslo a adresa elektronické pošty.
- Formulář stanoven vyhláškou
- Listinným hlášením/datovou schránkou

MEMBER OF MULTILAW

BEZPEČNOSTNÍ OPATŘENÍ

- Jiný rozsah u
  - – Kritické infrastruktury
  - – Významných IS (menší požadavky)
- Organizační opatření
- Technická opatření
- Možnost prokázat provedení certifikátem ISO 27001
- **Zavést do 1. 1. 2016 resp. do 12 měsíců od vzniku povinnosti**

MEMBER OF MULTILAW

ORGANIZAČNÍ OPATŘENÍ

- Systém řízení bezpečnosti informací
- Řízení rizik
- Bezpečnostní politika
- Organizační bezpečnost
- **Kontrola a audit**

MEMBER OF MULTILAW

ORGANIZAČNÍ BEZPEČNOST

- Bezpečnostní role (kritická infrastruktura)
  - Manažer kybernetické bezpečnosti a architekt kybernetické bezpečnosti
  - Řádně vyškoleni + praxe nejméně 3 roky s řízením bezpečnosti informací nebo s navrhováním bezpečnostní architektury
  - Auditor kybernetické bezpečnosti (nesmí být totožný)
  - Řádně vyškolen + praxe nejméně 3 roky s prováděním auditů systému řízení bezpečnosti informací
  - Garant aktiva a výbor pro řízení kybernetické bezpečnosti

ROWAN LEGAL
MEMBER OF MULTILAW

TECHNICKÁ OPATŘENÍ

- Fyzická bezpečnost
- Řízení přístupových oprávnění
- Aplikační bezpečnost
- Kryptografické prostředky

MEMBER OF MULTILAW

BEZPEČNOSTNÍ DOKUMENTACE

- **Elektronicky**
- Metodika pro identifikaci a hodnocení rizik
- Zpráva o hodnocení rizik
- Plán zvládání rizik
- Systém zvládání kybernetických bezpečnostních incidentů

ROWAN LEGAL

MEMBER OF MULTILAW

KYBERNETICKÝ BEZPEČNOSTNÍ INCIDENT

- Fyzické poškození
- Selhání infrastruktury
- Události způsobené škodlivým softwarem (viry)
- Technické útoky
- Porušení organizačních opatření

MEMBER OF MULTILAW

DETEKCE A OZNAMOVÁNÍ BEZPEČNOSTNÍCH INCIDENTŮ

- Detekovat
- Určit kategorii (I až III dle závažnosti)
- Hlásit bezodkladně po detekci
  - Elektronickým formulářem na http://hlaseni.nckb.nbu.cz
  - Emailem na adresu hlaseni@nckb.nbu.cz
  - Datovou zprávou
  - **Automatizovaným hlášení prostřednictvím určeného rozhraní**
  - Listinným hlášením
- **Od 1. 1. 2016 resp. do 12 měsíců od vzniku povinnosti**

ROWAN LEGAL

MEMBER OF MULTILAW

(PROTI)OPATŘENÍ

- Varování
- Ochranné opatření
  - Opatření obecné povahy
  - **Zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací**
  - **Na základě analýzy již vyřešeného kybernetického bezpečnostního incidentu**

ROWAN LEGAL

MEMBER OF MULTILAW

(PROTI)OPATŘENÍ II.

- Reaktivní opatření
  - Rozhodnutí/opatření obecné povahy
  - **K řešení kybernetického bezpečnostního incidentu** anebo k **zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací před kybernetickým bezpečnostním incidentem**
  - **Povinnost oznámit provedení**
  - Změna nebo rozšíření zavedených organizačních opatření
  - Změna nebo rozšíření zavedených technických opatření

MEMBER OF MULTILAW

KONTROLA A SANKCE

- NBÚ
- **Nápravná opatření** při nedostatcích
  - Ve stanovené lhůtě odstranit, popřípadě jakým způsobem
  - U bezprostředně ohrožených významných IS a KI možnost **zakázat používání systému nebo části do doby, než bude zjištěný nedostatek odstraněn**
- **Správní delikty** (pokuta až 100 000 Kč)
  - Neprovádění bezpečnostní opatření anebo nevedení bezpečnostní dokumentaci
  - Neohlášení kybernetického bezpečnostního incidentu

  …

MEMBER OF MULTILAW

ZÁKON NENÍ VŠELÉK

- Podstatou je prevence a sdílení informací
- **Nezajišťuje zneškodnění útočníka**
- Zdánlivě nejsnadnější obranou je odpojení
- Odpojen může být útočník i „nevinné oběti“

MEMBER OF MULTILAW

PROTIÚTOKY

- Pasivní versus aktivní obrana
- Záleží na interpretaci pojmu reaktivní opatření
  - Extenzivně vs. restriktivně
- Otázky
  - Kdo by měl rozhodnout?
  - Kdo by měl provést?
  - Kdo odpovídá?

MEMBER OF MULTILAW

STÍHÁNÍ KYBERZLOČINCŮ

- Není cílem zákona
- Jde o prevenci resp. zmírnění škod
- Nevytváří kriminalistické nástroje
- Povinná mlčenlivost CERTů

MEMBER OF MULTILAW

JUDr. Josef Donát, LLM
donat@rowanlegal.com

cz.linkedin.com/in/josefdonat/

ROWAN LEGAL, advokátní kancelář s.r.o.
+420 224 216 212

MEMBER OF MULTILAW