SVĚTOVÝ DEN NORMALIZACE 2014

APLIKACE TECHNICKÉ NORMALIZACE NA KYBERNETICKOU BEZPEČNOST VE VZTAHU K ZÁKONU O KYBERNETICKÉ BEZPEČNOSTI

Ing. Aleš Špidla
Vicepresident Českého institutu manažerů informační bezpečnosti
předseda Koordinační skupiny pro kybernetickou bezpečnost
ales.spidla@cimib.cz

Okruhy

- Zákon o kybernetické bezpečnosti – stručně
- Prováděcí předpis
- Cyber Security Coordination Group (CSCG)
- Praxe

Zákon o kybernetické bezpečnosti

ZKB – www.govcert.cz

Zásady:

- minimalizace zásahu do práv soukromoprávních subjektů
- individuální odpovědnost za bezpečnost vlastních informačních systémů

Pilíře:

- bezpečnostní opatření – technologicky neutrální (standardizace),
- hlášení kybernetických bezpečnostních incidentů,
- Protiopatření - reakce na incidenty.

Prováděcí předpis

- DEFINICE POJMŮ
- ORGANIZAČNÍ OPATŘENÍ

Povinnosti vyplývající ze ZKB splní ten, kdo

- stanoví s ohledem na aktiva a organizační bezpečnost rozsah a hranice systému řízení bezpečnosti informací,
- řídí rizika
- vytvoří a schválí bezpečnostní politiku v oblasti systému řízení bezpečnosti informací,
- monitoruje účinnost bezpečnostních opatření,
- vyhodnocuje vhodnost a účinnost bezpečnostní politiky podle
- zajistí provedení auditu kybernetické bezpečnosti
- zajistí vyhodnocení účinnosti systému řízení bezpečnosti informací,
- aktualizuje systém řízení bezpečnosti informací a příslušnou dokumentaci řídí provoz a zdroje systému řízení bezpečnosti informací, zaznamenává činnosti spojené se systémem řízení bezpečnosti informací a řízením rizik.

Prováděcí předpis

- TECHNICKÁ OPATŘENÍ
  - Fyzická bezpečnost
  - 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 činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů
  - Nástroj pro detekci kybernetických bezpečnostních událostí
  - Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
  - Aplikační bezpečnost
  - Kryptografické prostředky
  - Nástroj pro zajišťování úrovně dostupnosti
  - Bezpečnost průmyslových a řídicích systémů

Prováděcí předpis

BEZPEČNOSTNÍ DOKUMENTACE

§28 – Bezpečnostní dokumentace – definovaný obsah

§29 - Prokázání certifikace

Orgán a osoba uvedená v § 3 písm. c) až e) zákona, jejíž informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém je zcela zahrnut do rozsahu systému řízení bezpečnosti informací, který byl certifikován podle příslušné technické normy[)] akreditovaným certifikačním orgánem, a která vede dokumenty obsahující

a. popis rozsahu systému řízení bezpečnosti informací,

b. prohlášení politiky a cílů systému řízení bezpečnosti informací,

c. popis použité metody hodnocení rizik a zprávu o hodnocení rizik,

d. prohlášení o aplikovatelnosti,

e. certifikát systému řízení bezpečnosti informací splňující požadavky příslušné technické normy zabývající se bezpečností informací (ISO/IEC 27001:2013 resp. ČSN ISO/IEC 27001:2014)

f. záznam o přezkoumání systému řízení bezpečnosti informací včetně souvisejících vstupů a výstupů přezkoumání a

g. zprávu z auditů provedených certifikačním orgánem včetně příslušných záznamů o nápravě zjištěných neshod s příslušnou normou,

splňuje požadavky na zavedení bezpečnostních opatření podle zákona a této vyhlášky.

Prováděcí předpis

- KYBERNETICKÝ BEZPEČNOSTNÍ INCIDENT
- REAKTIVNÍ OPATŘENÍ A KONTAKTNÍ ÚDAJE
- PŘÍLOHY
  - Hodnocení a úrovně aktiv
  - Hodnocení rizik
  - Minimální požadavky na kryptografické algoritmy
  - Struktura bezpečnostní dokumentace

Cyber Security Coordination Group (CSCG)

- CSCG působí jako poradní a koordinační orgán rady CEN v technických, politických a strategických otázkách, týkajících se standardizace kybernetické bezpečnosti.

- Cíle CSCG jsou:

- poskytnout strategické poradenství pro technické výbory CEN (European Committee for Standardization, Comité Européen de Normalisation, Europäisches Komitee für Normung, www.cen.eu), CENELEC (European Committee for Electrotechnical Standardization) a ETSI (European Telecommunications Standards Institute)
- provádět analýzu evropských a mezinárodních standardů pro kybernetickou bezpečnost
- definovat společné evropské požadavky pro evropské a mezinárodní standardy kybernetické bezpečnosti
- vytvořit evropský plán na sjednocení kybernetické bezpečnosti
- působit jako kontaktní místo pro všechny instituce EU v otázkách, týkajících se standardizace kybernetické bezpečnosti
- vytvořit návrh společné americké a evropské strategie pro vytvoření rámce mezinárodních standardů v oblasti kybernetické bezpečnosti
- posílit koordinaci evropských aktivit ve výborech ISO a IEC s cílem společné transatlantické strategie

Praxe

- Vůle vedení k budování bezpečnostní kultury instituce.
- Zhodnocení aktiv a analýza rizik
- Řízení dodavatelů
- Řízení celého životního cyklu všech prvků informačního systému
- Personální bezpečnost (osvěta, vzdělání)
- Nastavení procesů pro zvládání incidentů a sdílení a rozvíjení znalostí o hrozbách a zranitelnostech.
- Monitorování a audit
- Zajištění kontinuity činnosti
- Fyzická bezpečnost všech rozhodujících technologií informačního systému
- Definice parametrů bezpečnosti informačního systému,
  - ochrana identit,
  - pravidla pro přístupy do informačního systému,
  - pravidla pro používání mobilních zařízení,
  - pravidla pro BYO (Bring Your Own Device, Network, Aplication) apod.
  - Síťová bezpečnost

Děkuji za pozornost

ales.spidla@gmail.com

ales.spidla@cimib.cz

+420 724 939 876