Dopady zákona o kybernetické bezpečnosti (ZKB)

Jan Mareš

O čem hovoříme?

- Zákon: 181/2014 Sb.
- Vyhláška č. 316/2014 Sb.
- VIS a KIS: vyhláška č. 317/2014 Sb. a č. 205/2016 Sb.

- Patronace: NBÚ - Národní bezpečnostní úřad

Co přináší do státní správy

- **DOKUMENTACI ICT**
- Zavedení a zrevidování procesů
- Stanovení rolí a zodpovědnosti
- Zvýšení povědomí o IT a bezpečnosti
- Centralizace řízení bezpečnosti na státní úrovni

- (větší vazba mezi organizačními složkami státu)

Co musí mít každá organizace

- Bezpečnostní dokumentaci
- Personální opatření
- Technické opatření

Co musí mít každá organizace

- **Bezpečnostní dokumentaci**
  - pravidla pro řízení bezpečnosti informací (vychází z ISO 27000, ITIL)
  - stanovení důležitosti informací a prostředků (aktiva)
  - stanovující politiky pro jednotlivé oblasti (např. logování, monitoring, pošta, aktualizace, hesla, ...)
  - specifikuje procesy

Co musí mít každá organizace

- **Personální opatření**
  - Výbor pro KB
  - Manažera
    - Řízení bezpečnosti informací (hlídá dodržování pravidel)
  - Architekta
    - Návrh řešení bezpečnostních opatření
  - Auditora
    - Kontrola navrhnutých řešení

Co musí mít každá organizace

- **Technické opatření**
  - log management (SIEM pro KIS)
  - Netflow/IPFIX sondu na vnějším perimetru*
  - nástroj pro pravidelné testování zranitelnosti*

(* do budoucna vyžadováno)

Záludnosti pro státní správu

- Nedostatek kvalifikovaných osob
  - nutno vychovat
  - neschopnost finančního ohodnocení
  - sdílení rolí
- Externě vytvořená bezpečnostní dokumentace nereflektující skutečnost
- Nesprávné stanovení oprávnění rolí
  - snaha mít moc nad všemi
- **Transformace politik bezpečnostní dokumentace**

Dopady ZKB

- Ne vše je nutné soutěžit
- Veškerá komunikace je zaznamenávána
- Stanovení akceptovatelné úrovně šifrování a minimální bezpečnosti
- Omezení práva na informace

Dopady ZKB

- **Ne vše je nutné soutěžit**
  - Dle ustanovení §29, odst. a),c),d) ZVZ (z. č. 134/2016) je možné nesoutěžit či více omezit soutěž z důvodu bezpečnosti

    Zadavatel není povinen zadat veřejnou zakázku v zadávacím řízení,

    a) pokud by provedení zadávacího řízení ohrozilo ochranu základních bezpečnostních zájmů České republiky a současně nelze učinit takové opatření, které by provedení zadávacího řízení umožňovalo,

    c) jde-li o zadávání nebo plnění veřejné zakázky v rámci zvláštních bezpečnostních opatření stanovenými jinými právními předpisy a současně nelze učinit takové opatření, které by provedení zadávacího řízení umožňovalo,

  - Lze technologicky omezit výsledné řešení

Dopady ZKB

- **Veškerá komunikace je zaznamenávána**
  - Ze zákona musí být vždy zaveden log management, někde i SIEM
  - Plán NBÚ/GOVCERT je nasazení NETFLOW sond a sběr dat na centrální místo u nich pro hloubkovou analýzu

Dopady ZKB

- **Stanovení akceptovatelné úrovně šifrování a minimální bezpečnosti**
  - Akceptovatelné šifrování - příloha č. 3 vyhlášky 316/2014
  - Uplatnění bezpečnostní dokumentace na dodavatele i integrátory

Dopady ZKB

- **Omezení práva na informace**
  - Dle ustanovení § 11 odst. 4 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění zákona č. 61/2006 Sb.

    f) údajích vedených v evidenci incidentů podle zákona o kybernetické bezpečnosti, ze kterých bylo možné identifikovat orgán nebo osobu, která kybernetický bezpečnostní incident ohlásila nebo jejichž poskytnutí by ohrozilo účinnost reaktivního nebo ochranného opatření podle zákona o kybernetické bezpečnosti.

  - Jakékoliv informace týkající se IT i osob lze odmítnout zveřejnit

Co nás čeká do budoucnosti

- Rozšíření působnosti zákona
- Státní portál agregující bezpečnostní informace a doporučení
- Pravidelné bezpečnostní polygony
- Státní cloud a schválení využívání cloud. služeb státní správou
- Zákon o elektronické identifikaci

Dotazy

- Hodnocení přednášky

http://a.openalt.cz/3101

Děkuji

jan.mares@manast.eu