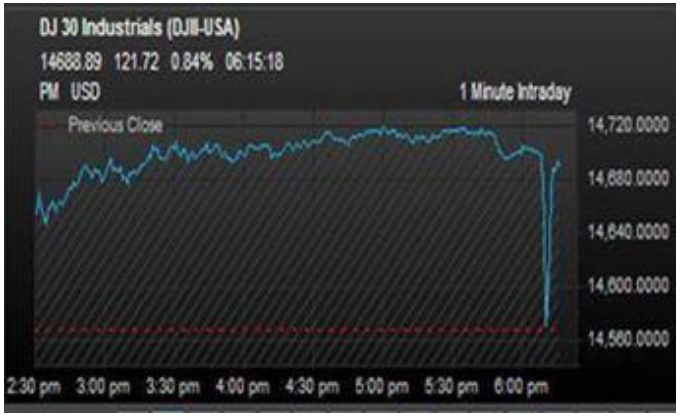
Zákon o kybernetické bezpečnosti č. 181/2014 Sb.

Building a better working world

Kybernetická bezpečnost - sci-fi nebo realita?

Official AP account on Twitter:



"Breaking: Dvě explose v Bílém domě, Obama je raněn

Za kolik se dá útok dnes koupit

- Konzultace spojené s útokem typu botnet $350-$400
- Infekce a její rozšíření ~$100 za 1 tisíc instalací
- Další služby:
  - Direct Denial of Service (DDoS) $535 za 5 hodin denně v trvání jednoho týdne,
  - email spam $40 / 20 tisíc emailů) and Web spam ($2 za 30 umístění)

Source: http://resources.infosecinstitute.com/cybercrime-and-the-underground-market/

Zákon o kybernetické bezpečnosti č. 181/2014 Sb.

- Zásady zákona:
  - Minimalizace zásahů do práv soukromoprávních subjektů
  - Individuální zodpovědnost za bezpečnost vlastních informačních systémů
- Povinné osoby
  - Kritická infrastruktura
  - Významná infrastruktura
- Základní úkoly:
  - Bezpečnostní opatření postavené na normě ISO 27001 – standardizované (ISMS)
  - Technologicky a procesně nezávislé
  - Hlášení bezpečnostních incidentů
  - Reakce na incidenty – protiopatření
- www.govcert.cz

Důsledky pro IA

- Dopady pro vnitřní kontrolní systém
  - Je-li vybudován a pravidelně auditován funkční ISMS, pak je nutné doplnit stávající plán auditu na oblasti vzešlé z KI nebo VI:
    - Výkon povinností týkajících se informačních aktiv
    - Řízení souvisejících rizik a jejich dopadu na aktiva
    - Detekce a hlášení incidentů
    - Funkčnost CERT týmu organizace a jeho řešení mimořádných událostí
- Aktivní role IA:
  - Ujištění o stavu implementace souladu s ZKB
  - Komunikovat nově zjištěná rizika managementu
  - Zapracovat do auditních plánů

Příloha