Efling varna gegn Netvá

Leiðbeiningar frá Stjórnarráðinu

Guðmundur H. Kjærnested

Framkvæmdastjóri Rekstrarfélags Stjórnarráðsins

Rekstrarfélag Stjórnarráðsbygginga

- Miðlæg þjónustueining innan Stjórnarráðsins sem heyrir undir fjármálaráðuneytið
- Sameiginleg stjórn frá hluta ráðuneyta
- Þjónustar öll ráðuneyti nema utanríkisráðuneyti
- Þjónustar nokkrar ríkisstofnanir, s.s. Fjársýslan.
- Helstu þjónustuþættir eru: Rekstur og viðhald fasteigna, ræsting, öryggisgæsla, rekstur mötuneytis, rekstur ráðherrabifreiða, tölvuþjónusta, rekstur miðlægra tölvukerfa

Skipulag og samræming öryggismála Stjr

Eining	Hlutverk
Ríkislögreglustjóri	Yfirstjórn, stefnumótun og eftirlit með öryggismálum stjórnarráðsins
Lögreglan í Reykjavík	Vettvangs- og aðgerðastjórnun
Forsætisráðuneytið	Yfirstjórn húsnæðismála ráðuneyta, eftirlit með stjórnun öryggismála.
Ráðuneyti	Ábyrgð, stjórnun og eftirlit með öryggismálum ráðuneytis
Rekstrarfélag Stjr	Umsjón og framkvæmd á ákveðnum þáttum öryggismála

Aðilar í ráðuneyti	Hlutverk
Ráðuneytisstjóri	Ábyrgð og stjórnun öryggismála ráðuneytis
Yfirmaður öryggismála	Umsjón með öryggismálum og úrlausn verkefna
Öryggisfulltrúi	Staðgengill yfirmanns öryggismála

Almennt um öryggismál

- Öryggismál eru málaflokkur sem vægi eykst á hverju ári.
- Mótmælin eftir hrunið orsökuðu heildarendur-skoðun öryggismála, ýmsum verklagsreglum var breytt og búin var til sérstök viðbragðsáætlun
- Í fyrra átti sér stað önnur endurskoðun öryggismála – ógnir vegna tölvuárása voru taldar vera verulegar.

Áhættumat – er ógnin raunveruleg ?

- Hún er til staðar og er því miður ansi raunveruleg.
- Við upplifum minni háttar árásir reglulega, greinanlegur vöxtur í slíkum árásum.
- Á síðasta ári áttu sér stað stórar netárásir. Dæmin eru þekkt, t.d. CCP, Sony, ...
- Ógnin er mun margþættari en áður.

Áhættumat – hverjir eru þetta ?

Greining Capacent

- Þjóðir
- Hryðjuverkamenn/öfgahópar
- Hacktivists
- Glæpasamtök og skiplögð starfsemi/þjónusta
- Script kiddies/Kjánar

Áhættumat – Dæmi um árásarfleti

- Net ráðuneytis/stofnunar – markmiðið gæti verið að sökkva viðkomandi neti og á sama tíma framkvæma innbrot
- Tölvur starfsmanna – ná yfirráðum og nota tölvuna til þess að ná yfirráðum yfir öðrum tölvum og mögulega miðlurum (e. servers).
  - Ná yfirráðum með því komast inn í gegnum forrit á tölvu starfsmanns (Facebook, IE, Twitter, Skype, Adobe, ...)
  - Ná yfirráðum með því „plata“ starfsmanninn.

Að plata starfsmanninn

- Gert með ýmsum móti
  - Gefa hluti sem innihalda leyniforrit (USB lykill, tölvumús, ...)
  - Fá notandann til samþykkja innlestur leyniforrita
    - Beiðni í tölvupósti um þáttöku í könnun, könnun inniheldur leyniforrit sem fer inn eftir að notandi hefur samþykkt tiltekna aðgerð í könnuninni
    - Vinningur í tölvupósti

Áhættumat – hvað getur gerst ?

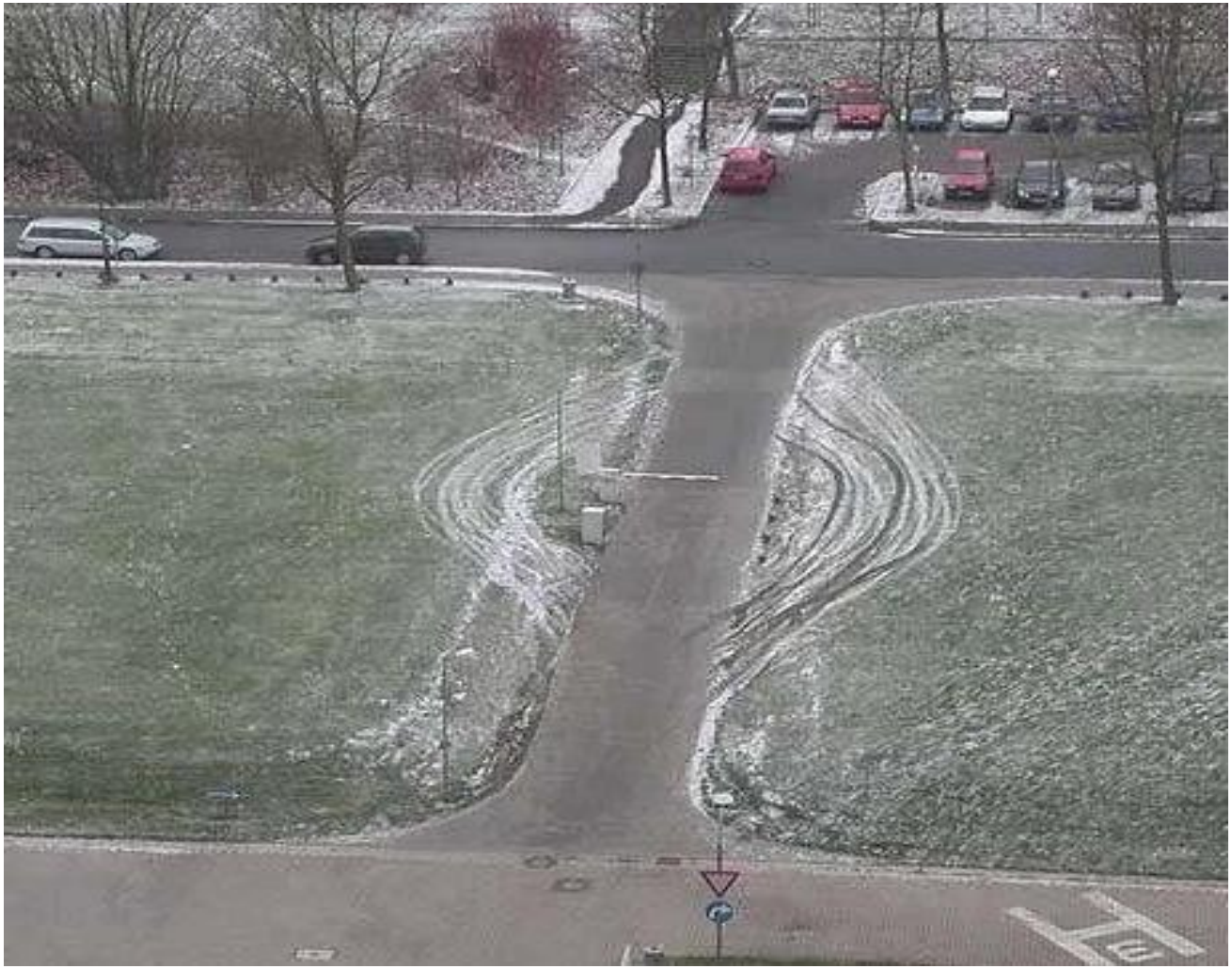
Greining Capacent

- Hæfur aðili gæti brotist inn í tölvukerfi allra fyrirtækja á Íslandi
- ...gæti valdið miklu tjóni
- Hvaða tjóni?
  - Komist í flest gögn og kerfi
  - Tölvupóst allra
  - Gæti breytt eða skoðað upplýsingar í fjármálakerfum/launakerfum/osfrv.
  - Borgað “reikninga”
  - Eyðilagt gögn eða t.d. allar tölvur á netkerfi
- Erfitt að koma í veg fyrir innbrot
- Öflugt eftirlit er besta vörnin
- Innbrot af þessu tagi gæti tekið einn dag eða vikur/mánuði eftir flækjustigi

Varnaraðgerðir

- Mikilvæg staðreynd er að tölvuöryggismál er óaðskiljanlegur hluti af heildaröryggismálum
- Eina sem er öruggt er að enginn er öruggur – aðilar þurfa að skilgreina lágmarksöryggi og reyna að ná því og viðhalda.
- Finna þarf jafnvægi milli notagildis og öryggis. Kostnaður aðgerða skiptir hér sjálfsögðu miklu máli.
- Hættulegt er að halda að til séu galdralausnir sem kaupa öryggi
- Öryggismál verða að vera skoðuð með heildstæðum hætti – besta leiðin er að innleiða öryggisstjórnunarkerfi

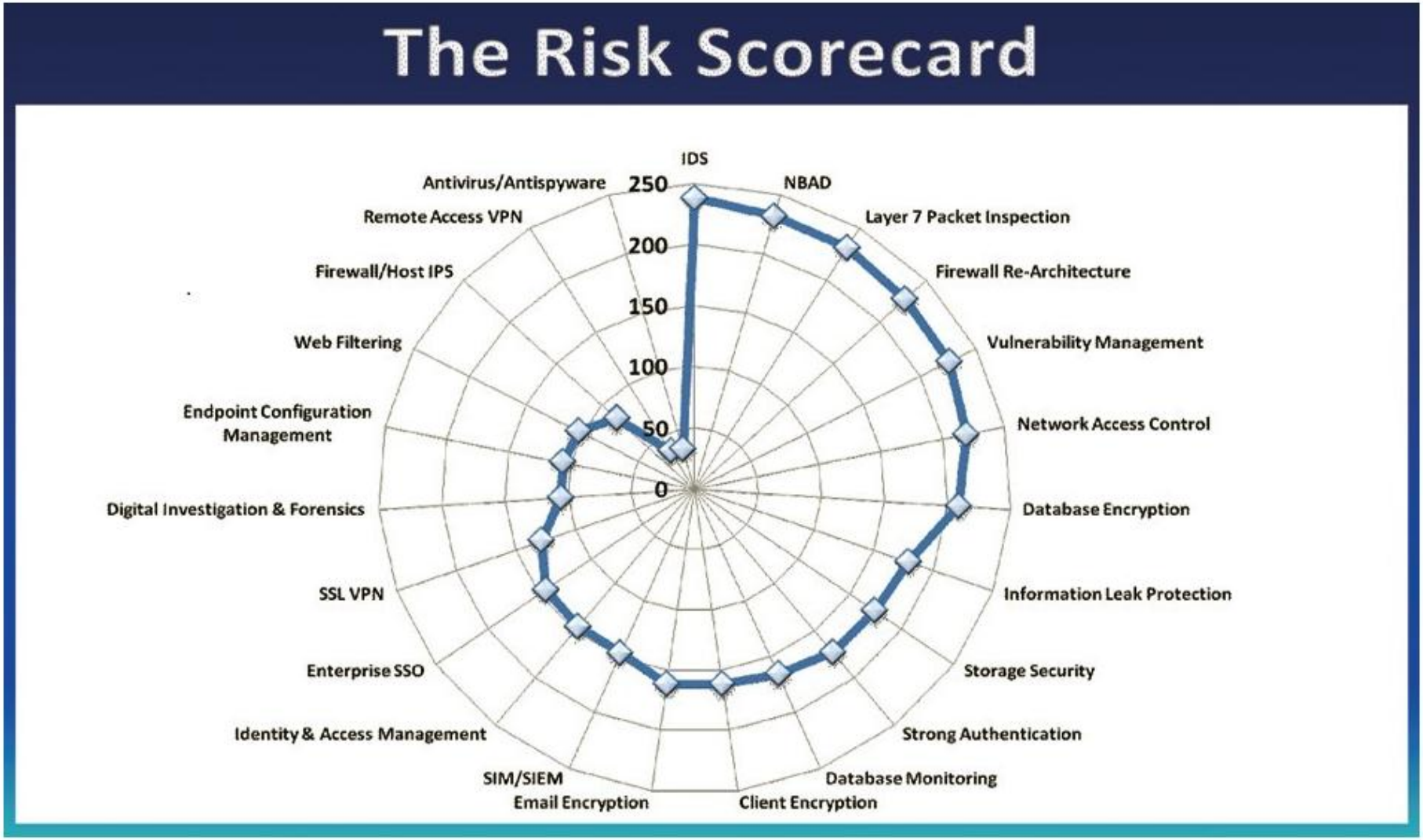
Veikir hlekkir í öryggiskeðjunni



Innleiðing öryggisstjórnunarkerfis – leitin að veiku hlekkjunum

- Eignagreining
- Áhættumat
- Aðgerðir
- Vottun
- Reglulegt endurmat og aðgerðir í kjölfarið

Ýmsir þættir í tölvuöryggi



Varnaraðgerðir – Atriði sem skoða skal

- Raunlægt öryggi tölvusala
- Auðkennis- og aðgangsstjórnun
- Eftirlit og eftirlit og eftirlit og síðan meira eftirlit, samræmd eftirlit (SIEM)
- Endurskoðun á eldveggjastillingum. Fara yfir allar tengingar við ytra net, millinet. Gáfaðir eldveggir (e. content aware)
- Reglulegar veikleikaprófanir (Skimun – Ytri úttekt – Innri úttekt)
- Innbrotsvarnakerfi
- Gagnalekar (e. information leak)
- Öruggt VPN með tveggja þátta auðkenningu
- Uppfærslur á stýrikerfum miðlara

Varnaraðgerðir – Atriði sem skoða skal fr.h.

- Uppfærslur á hugbúnaði
- Uppfærslur og eftirlit með netbúnaði
- Réttindi á útstöðvum
- Meðhöndlun útstöðva og gesta
- Skilgreining á leyfðum hugbúnaði, verkferlar við uppsetningu á hugbúnaði
- Lokanir á vefsíður
- Öflugt vírus- og óværu varnarkerfi
- Öryggisúttektir á mikilvægum kerfum, t.d. kerfum með snertingu við ytra net
- Rannsóknarkerfi (e. forensic)
- Fræðsla til notenda

Takk fyrir mig !

Takk fyrir mig !