STAÐA OG ÞEKKINGARUPPBYGGING Í NETÖRYGGISMÁLUM Á ÍSLANDI

Dagur upplýsinga-tækninnar

1. des 2016

Svavar Ingi Hermannsson
CISSP, CISA, CISM

ÖRYGGISÚTTEKT Á ÖRYGGI OPINBERRA VEFJA - 2105

ÖRYGGISÚTTEKT Á ÖRYGGI OPINBERRA VEFJA – UMFANG

- Unnið fyrir Innanríkisráðuneytið
- 256 vefir (Ríki og sveitarfélög)
- 1. júlí - 30. október 2015
- Skýrslur sendar til allra tengiliða
- Heildar niðurstöður verða ekki birtar

ÖRYGGISÚTTEKT OPINBERRA VEFJA – HELSTU NIÐURSTÖÐUR

- Stærri aðilar með meira fjármagn sem meðhöndla viðkvæmar upplýsingar líklegri til að vera með öryggismál í lagi.
- Minni aðilar með minna fjármagn sem meðhöndla upplýsingar sem teljast ekki viðkvæmar líklegri til að vera með öryggismál í ólagi.
- Ekki algilt.
  - Sumir minni aðilar með allt sitt á hreinu.
  - Sumir stærri aðilar sem þurfa að bæta sig.

ÖRYGGISÚTTEKT OPINBERRA VEFJA – VIÐBRÖGÐ

- Mjög jákvæð viðbrögð frá tengiliðum og þjónustuaðilum.
- Fjöldi funda haldnir í framhaldi af UT deginum í fyrra.
- Strax farið að vinna að úrbótum
  - Mikill fjöldi vefkerfa sem hafa verið uppfærð í nýjustu/nýja útgáfu þar sem búið var að laga öryggisveikleika sem fundust.
  - Búið að fjárfesta í rafrænum skilríkjum til þess að dulkóða samskipti (t.d. þegar verið er að senda notandanafn og lykilorð eða aðrar viðkvæmar upplýsingar).

ÖRYGGISÚTTEKT OPINBERRA VEFJA – LÆRDÓMUR (FRÁ ÞVÍ Í FYRRA)

- Ábyrgðarmaður vefs þarf að gera öryggiskröfur í samningum og veita eftirfylgni.
- Hugbúnaðarhús þurfa að axla ábyrgð og bjóða upp á öruggar uppsetningar og öryggisuppfærslur.
- Hýsingar-/þjónustu- aðilar þurfa að axla ábyrgð og bjóða upp á örugga hýsingu með því að setja reglulega inn öryggisuppfærslur og viðhalda kerfunum sínum.
- Hægt er að bæta öryggi mikið með einföldum aðgerðum (t.d. að sækja reglulega öryggisuppfærslur)

ÖRYGGISÚTTEKT OPINBERRA VEFJA – HVAÐ VAR GERT?

- Leitað eftir þekktum öryggisveikleikum með tilliti til OWASP top 10:
  - Vefumsjónarkerfi
  - Vefmiðlari
  - Stýrikerfi

ÖRYGGISÚTTEKT OPINBERRA VEFJA – LÆRDÓMUR (FRÁ ÞVÍ Í FYRRA)

- Ábyrgðarmaður vefs þarf að gera öryggiskröfur í samningum og veita eftirfylgni.
- Hugbúnaðarhús þurfa að axla ábyrgð og bjóða upp á öruggar uppsetningar og öryggisuppfærslur.
- Hýsingar-/þjónustu- aðilar þurfa að axla ábyrgð og bjóða upp á örugga hýsingu með því að setja reglulega inn öryggisuppfærslur og viðhalda kerfunum sínum.
- Hægt er að bæta öryggi mikið með einföldum aðgerðum (t.d. að sækja reglulega öryggisuppfærslur)

HVERNIG ER HÆGT AÐ STYÐJA VIÐ OPINBERA AÐILA?

- Samningsviðauki útgefin til umsagnar
  - http://www.ut.is/utgafa/

STEFNUMÓT VIÐ ÖRUGGA FRAMTÍÐ – ÓGNIR, TÆKIFÆRI OG ÁSKORANIR

UMRÆÐUSKJAL - SAMNINGSVIÐAUKI

- Öryggisstefna
- Áhættumat
- Stjórnun aðgangs
- Öryggisuppfærslur
- Veikleikagreiningar og innbrotsprófanir
- Innbrotsvöktunarkerfi (IDS/IPS)
- Frávikaskráning
- Innra eftirlit

UMRÆÐUSKJAL - SAMNINGSVIÐAUKI (FRAMHALD)

- Heildrænt samstarf á sviði netöryggismála
- Ráðningar starfsmanna og verktaka
- Trúnaðaryfirlýsingar
- Þjálfun starfsmanna og verktaka
- Starfslok
- Skýrslugjöf
- Eftirlit

UMRÆÐUSKJAL - SAMNINGSVIÐAUKI (FRAMHALD)

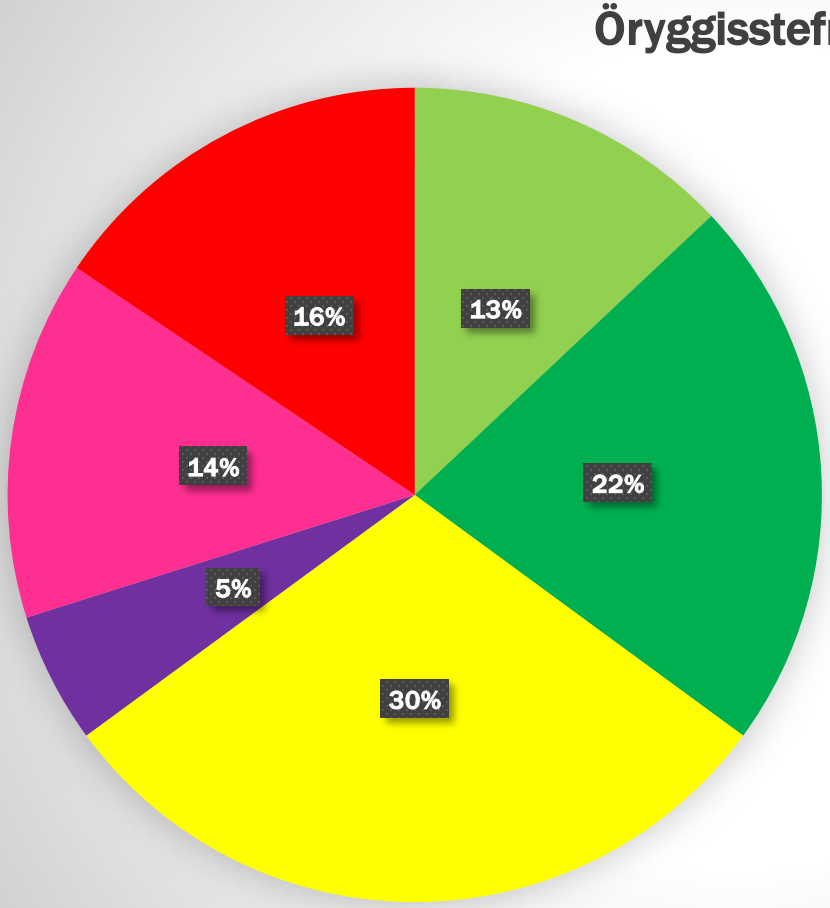
- REKSTUR
  - Breytingastjórnun
  - Öryggisafritunartaka
  - Áætlun um samfelldan rekstur
  - Viðbragðsáætlun fyrir öryggisatvik
- Hugbúnaðarþróun
  - Hugbúnaðarþróunarferli
  - Breytingastjórnun í hugbúnaðarþróun
  - Tilkynning á öryggisveikleikum sem finnast

UMRÆÐUSKJAL - SAMNINGSVIÐAUKI (FRAMHALD)

- Persónuvernd
  - Vinnslusamningur
  - Öryggi persónuupplýsinga
  - Fyrirhugaðar lagabreytingar

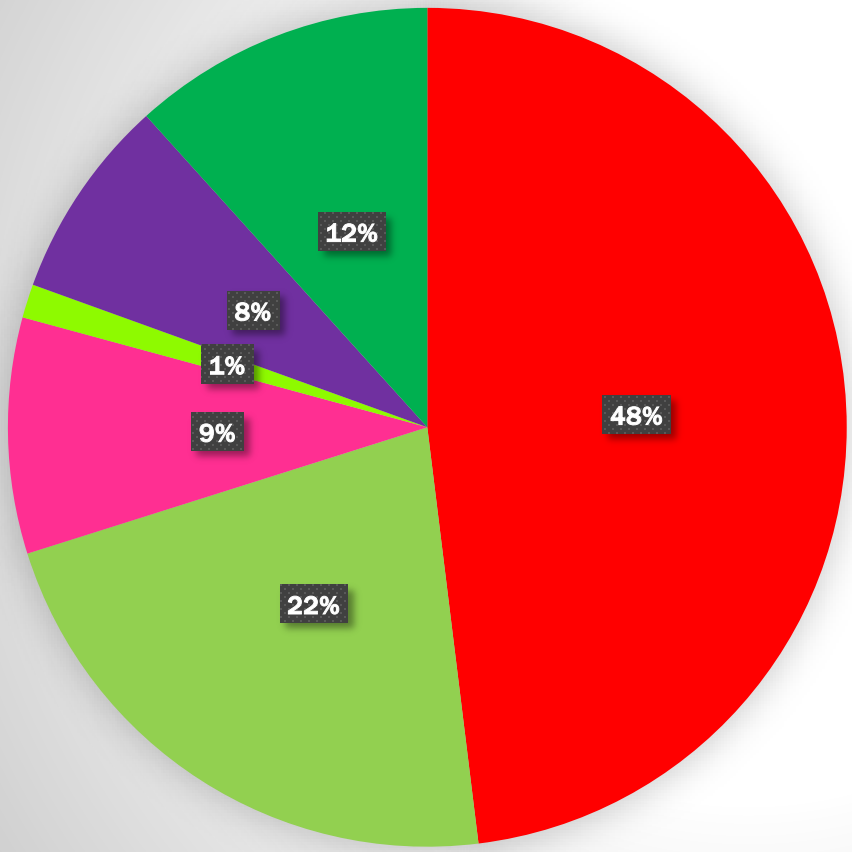
KÖNNUN Á STÖÐU STJÓRNUNARLEGS UPPLÝSIGNAÖRRYGGIS

KÖNNUN Á STÖÐU STJÓRNUNARLEGS UPPLÝSIGNAÖRRYGIS – NIÐURSTÖÐUR



- Búið er að skjalfesta formlega öryggisstefnu en hún hefur ekki ennþá verið samþykkt af æðstu stjórnendum.
- Búið er að skjalfesta formlega öryggisstefnu, sem hefur verið samþykkt af æðstu stjórnendum og er rýnd að lágmarki einu sinni á tveggja ára fresti á rekjanlegan hátt.
- Starfsmenn eru almennt meðvitaðir um öryggismál en formleg öryggisstefna hefur ekki verið skjalfest.
- Veit það ekki.
- Það er ekki búið að móta öryggisstefnu en áætlað er að móta hana á næstunni.
- Það er ekki búið að móta öryggisstefnu og ekki áætlað að gera það á næstunni.

KÖNNUN Á STÖÐU STJÓRNUNARLEGS UPPLÝSIGNAÖRRYGIS – NIÐURSTÖÐUR



- Áhættumat hefur ekki verið framkvæmt á síðustu 2 árum og ekki er til skjalfest verklag fyrir framkvæmd áhættumats.
- Áhættumat hefur verið framkvæmt á síðustu 2 árum en það var ekki gert samkvæmt skjalfestu verklagi.
- Búið er að skjalfesta verklag um framkvæmd áhættumats en það hefur ekki verið framkvæmt síðustu 2 ár.
- Búið er að skjalfesta verklag um framkvæmd áhættumats og er það framkvæmt að lágmarki einu sinni á ári. Verklagið hefur ekki verið formlega samþykkt af æðstu stjórnendum.
- Veit það ekki.
- Verklag um framkvæmd áhættumats hefur verið skjalfest og áhættumat framkvæmt samkvæmt því að lágmarki einu sinni á ári. Áhættumatið sjálft er formlega samþykkt af æðstu stjórnendum á rekjanlegan hátt.

HVERNIG ER HÆGT AÐ STYÐJA VIÐ OPINBERA AÐILA?

- Dæmi um öryggisstefnu?
- Leiðbeiningar um framkvæmd áhættumats
- Eyðublað sem hægt er að nota við framkvæmd áhættumats

- Allt aðgengilegt frá UT vefnum:
  - http://www.ut.is/utgafa/

ÁHÆTTUMAT - EYÐUBLAÐ

Áhættumat						Áhættumeðferæaráætlun			
Upplýsingaeign	Ógn	Veikleiki	Líkur	Áhrif	Áhætta	Áhættumeðferð	Áætluð lok	Ábyrgðaraðili	Framkvæmdaraðili

KÖNNUN Á STÖÐU STJÓRNUNARLEGS UPPLÝSIGNAÖRRYGIS - VIÐBRÖGÐ

- Hvernig er hægt að styðja við ykkur?
  - Fræðsluefni
  - Námskeið
  - Bein aðstoð

- Ef þið hafið spurningar, ábendingar eða viljið óska eftir aðstoð, þá getið þið sent tölvupóst á netfangið: oryggi@irr.is

VERKEFNI FRAMUNDAN

HELSTU VERKEFNI FRAMUNDAN

- Umræðuskjal - samningsviðauki
- Öryggisstefna
- Áhættumat

TAKK FYRIR

- Einhverjar spurningar?
  - svavar@security.is