

# ÖRYGGI GAGNA Í STJÓRNSÝSLUNNI

Málstofa um rafræna stjórnsýslu hjá ríki og  
sveitarfélögum - maí 2014

Svavar Ingi Hermannsson

# DAGSKRÁ

- KYNNING
  - STAÐA NETÖRYGGISMÁLA Á ÍSLANDI
  - ÁHÆTTUMEÐVITUND STJÓRNENDA
  - VINNA INNANRÍKISRÁÐUNEYTISINS
- 

# KYNNING

## - HVER ER ÉG?

Svavar Ingi Hermannsson hefur sérhæft sig í tölvuöryggi síðustu 20 ár og hefur gengt ýmsum störfum tengt forritun og ráðgjöf í tölvuöryggi (innbrotsprófanir, veikleikagreiningar, kóðarýni, stjórnun upplýsingaöryggis (þar á meðal ISO/IEC 27001 og PCI DSS)).

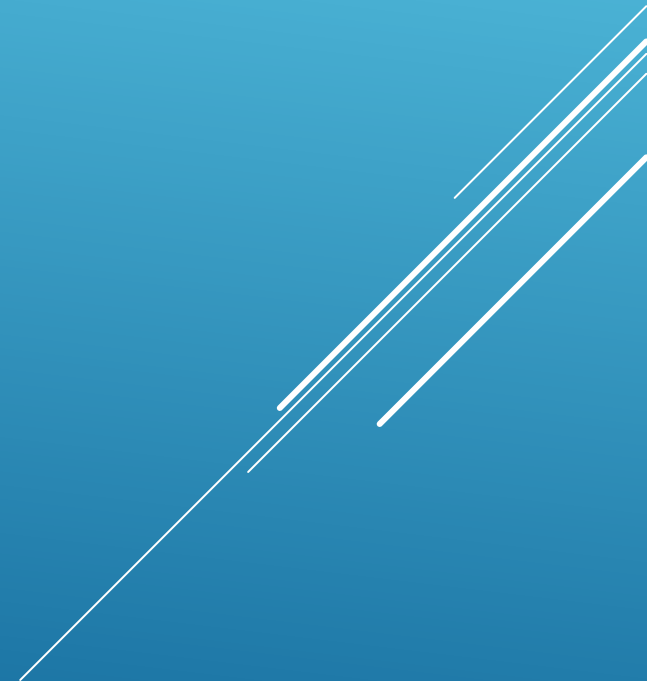
Svavar hefur kennt við Háskóla Íslands og Háskólann í Reykjavík, auk þess að hafa haldið fyrirlestra og námskeið bæði á Íslandi og í útlöndum.

Svavar var formaður faghóps um öryggismál hjá Skýrslutæknifélaginu frá 2007 til 2012.

Svavar er með ýmsar gráður, meðal annars: CISSP, CISA, CISM.



# STAÐA NETÖRYGGISMÁLA Á ÍSLANDI



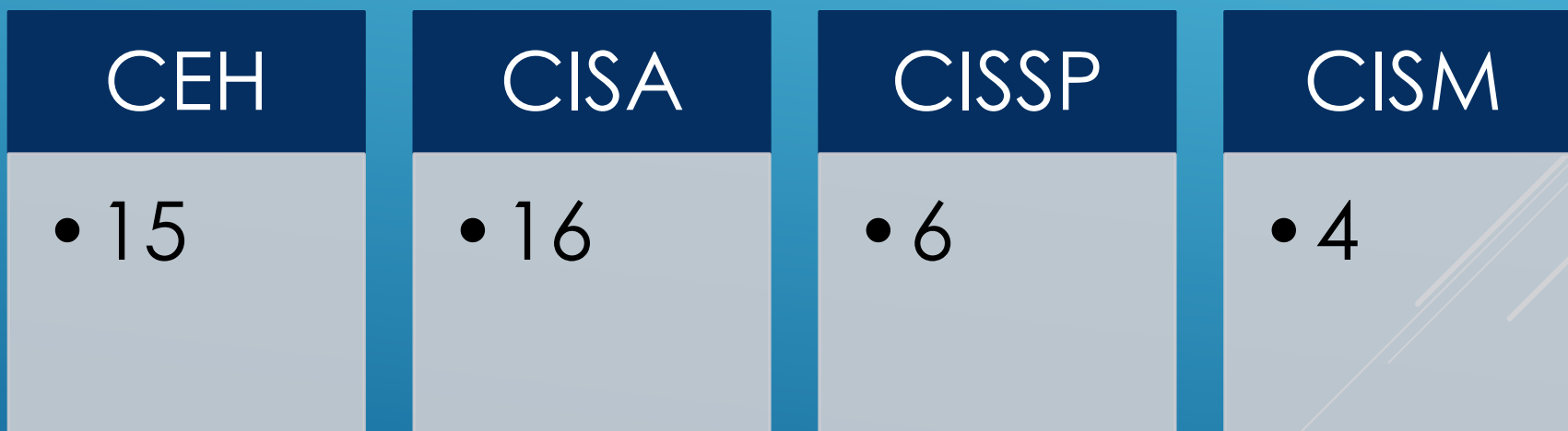
# UPPLÝSINGAÖRYGGISGRÁÐUR

- ÞÆTTIR SEM HAFA ÁHRIF Á NETÖRYGGI: UPPLÝSINGAÖRYGGISGRÁÐUR

- Hverjar eru helstu gráðurnar í upplýsingaöryggi?

- Hvað eru margar slíkar gráður skráðar á Íslandi?

Fjöldi fyrirtækja  
2012 samkvæmt  
hagstofu var  
tæplega 63.000



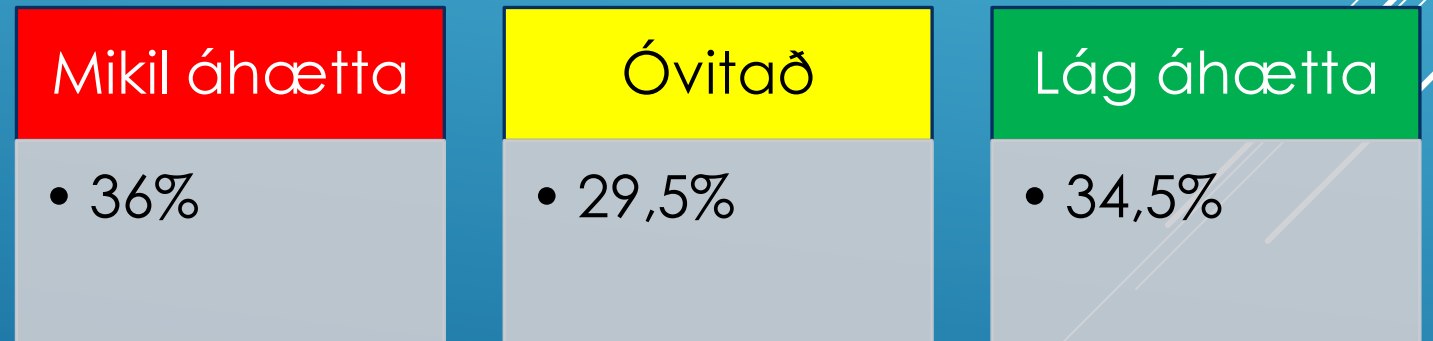
# RANNSÓKN KPMG

## RANNSÓKN KPMG Á STÖÐU NETÖRYGGISMÁLA Á ÍSLANDI

Framkvæmd var ítarleg rannsókn á stöðu netöryggismála síðasta sumar af KPMG. Niðurstöður hafa verið kynntar á ráðstefnum, kynningum og fundum. Eftirfarandi er einn margra þátta sem kom fram:

### STAÐA VEFMIÐLARA UM 570 AÐILA

Skoðaðir voru vefmiðlararar 570 aðila, þar af voru 300 stærstu fyrirtækin samkvæmt veltu árið 2012, opinberir aðilar og fjármálafyrirtæki.



# ÞÆTTIR SEM HAFA ÁHRIF Á NETÖRYGGI

## ISO/IEC 27001 VOTTUN

Fjöldi ISO/IEC 27001 vottaðra fyrirtækja/stofnanna á Íslandi í fyrra: 20

## FJÖLDI TILKYNNTRA AFSKRÆMDRA VEFSÍÐNA Á ÍSLENSKUM LÉNUM FYRIR ÁRIÐ 2013

Fjöldi afskræmda vefsíðna (e. Website defacement) íslenskra léna (.is) á árinu 2013 var í kringum 1.000

Hvað er afskræming vefsíðu?

# ÁHÆTTUVITUND STJÓRNENDA

## HVERNIG GETA STJÓRNENDUR HAFT ÁHRIF Á ÖRYGGI?

Stjórnendur geta óskað eftir upplýsingum og sett fram kröfur um ákveðið öryggisstig.

- Þegar fjórfest er í veflausn er hægt að óska eftir upplýsingum eins og: hefur verið gerð óháð öryggisúttekt á viðkomandi vefkerfi?
- Eru forritarar viðkomandi hugbúnaðarhúss meðvitaðir um helstu öryggisveikleika í vefforritun? Hafa þeir hlotið þjálfun á því sviði? (t.d. OWASP top 10)
- Ábyrgist þjónustuaðili öryggisuppfærslur að kostnaðarlausu?

## ÁHÆTTUÞÆTTIR UPPLÝSINGAKERFA/VEFKERFA

- Er búið að framkvæma veikleikagreiningu á upplýsingatækni hverfinu?
- Er búið að gera öryggisúttekt á lykil upplýsingakerfum?
- Var þetta gert af óháðum þriðja aðila?



# VINNA INNANRÍKISRÁÐUNEYTISINS

## HVERNIG VITA STJÓRNENDUR: HVAÐ BER AÐ VARAST?

Í samstarfi við KPMG hefur verið unnin uppfærsla á vefhandbókinni þar sem tekið er á upplýsingaöryggismálum. Þar eru meðal annars gátlistar við:

- Val á veflausn.
- Val á þjónustuaðila.
- Gátlisti sem hægt er að nota við samningsgerð.
- Gátlisti fyrir örugga uppsetingu grunnkerfa.
- Gátlisti sem hægt er að nýta við öryggisprófanir.



# Vefhandbókin

## HANDBÓK UM OPINBERA VEFI

Mörg sjónarhorn – Veldu þína leið – Efnisflokkar, markhópar, gæðamál



# SPURNINGAR?

svavar@security.is / svavar@upplýsingaöryggi.is

A series of several parallel white lines of varying thicknesses, slanted diagonally from the bottom-left towards the top-right, located in the right half of the image.