KPMG

cutting through complexity

Hvert er þroskastig netöryggismála á Íslandi?

OWASP Iceland – apríl 2014
Svavar Ingi Hermannsson
KPMG, Ráðgjafarsvið

Dagskrá

- **Kynning**
- **Tilgangur**
- **Heildarmynd**
  - Almennar forsendur
- **Netið skoðað**
  - Aðferðir
  - Niðurstöður
- **Varnarþættir**
  - Eftirlitsþættir
- **Yfirlit**

Hver er ég?

Svavar Ingi Hermannsson hefur sérhæft sig í tölvuöryggi síðustu 15 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 Reykjavik, auk þess að hafa haldið námskeið fyrir viðskiptavini KPMG.

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

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

Tilgangur rannsóknarinnar?

KPMG hafði áhuga á að vita þroskastig upplýsinga og netöryggismála á íslandi.

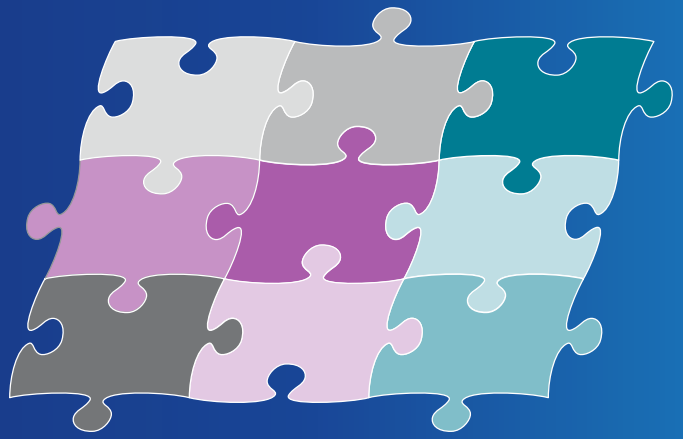
Spurning; Hvernig er netöryggi á Íslandi háttað?

Við fundum engar rannsóknir sem gáfu heildaryfirlit yfir núverandi stöðu mála.

Takmarkað af upplýsingum til staðar.

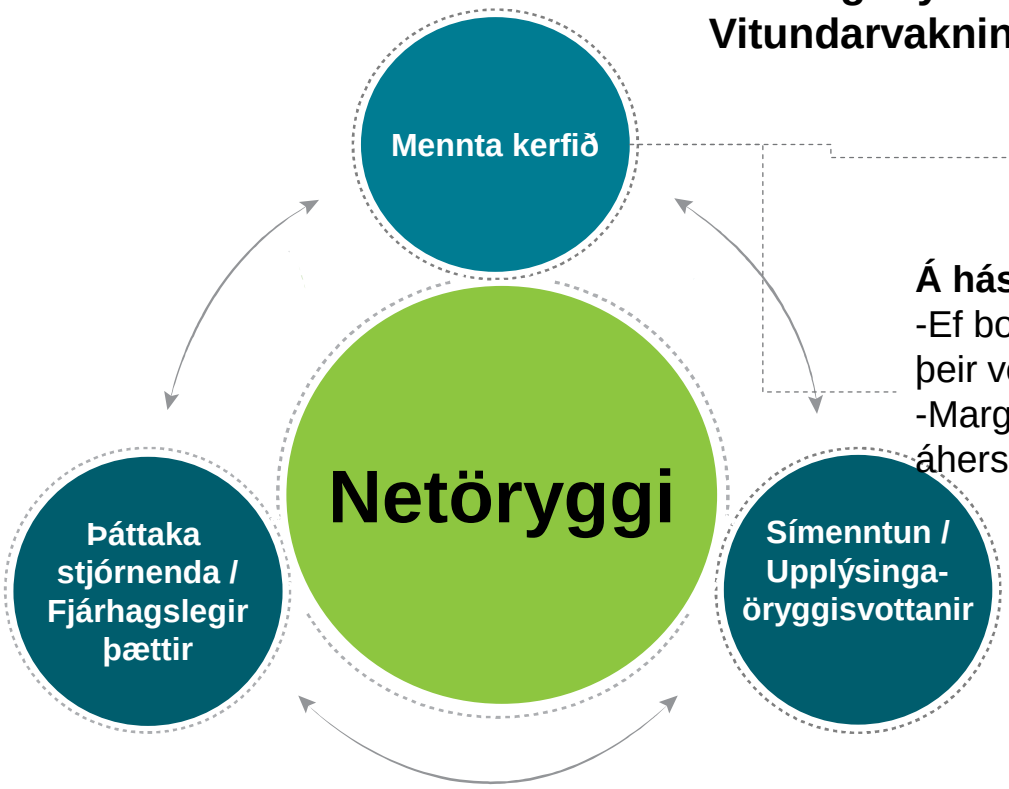
Margar spurningar, fá svör

Púslum raðað saman



Rannsókn – Almennar forsendur – Menntun / Vitund

Ýmsir þættir sem hafa áhrif á netöryggi: Menntun / Vitund



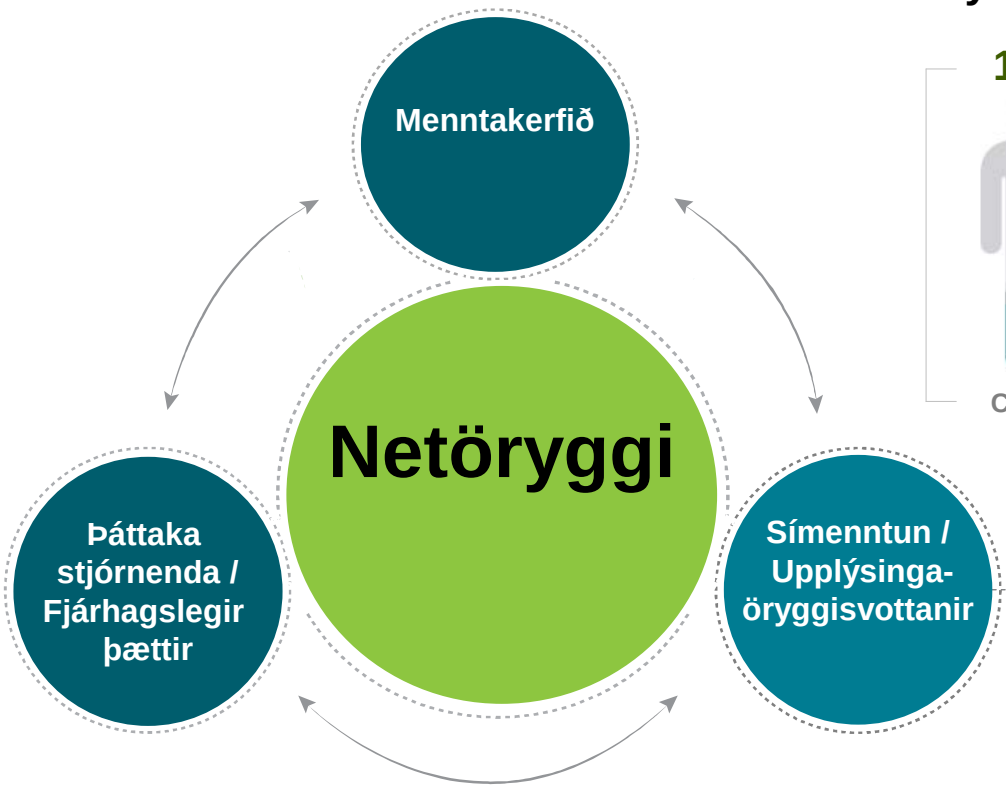
Hvernig styður núverandi menntakerfi við Vitundarvakningu í upplýsingaöryggi?

Á grunnskóla / gagnfræðiskólastigi?
- Það eru tækifæri til að byrja þar
- Öryggisvitund snemma

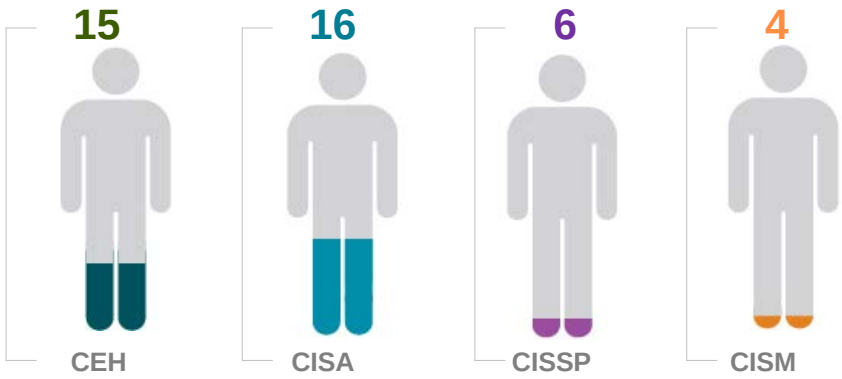
Á háskóla stigi:
-Ef boðið hefur verið upp á kúrsa í tölvuöryggi þá hafa þeir verið valkúrsar.
-Margir tölvuöryggiskúrsar í gegnum tíðina hafa lagt áherslu á dulkóðun.

Rannsókn – Almennar forsendur – Upplýsingaöryggisgráður

Ýmsir þættir sem hafa áhrif á netöryggi: Upplýsingaöryggisgráður



What security certifications is the industry using?



Source: (https://www.isaca.org/)
Source: (https://www.eccouncil.org)
Source: (https://www.isc2.org)

Rannsókn – Almennar forsendur – Aðgengilegar upplýsingar

Fjöldi ISO/IEC 27001 vottaðra fyrirtækja á Íslandi

Fjöldi tilkynntra afskræmdra vefsíðna á íslenskum lénum fyrir árið 2013, dagsetning 10.09.2013 (zone-h.org)

#fjöldi skráðra .is léna	45.201
# tilkynntar afskræmingar	823

Það er tilhneiging að gera lítið úr afhausunum vefsíðna

Það sem þau halda að það sé!
Það sem við vitum að það er!

Netið skoðað

Netið skoðað – Allir vinir í skóginum

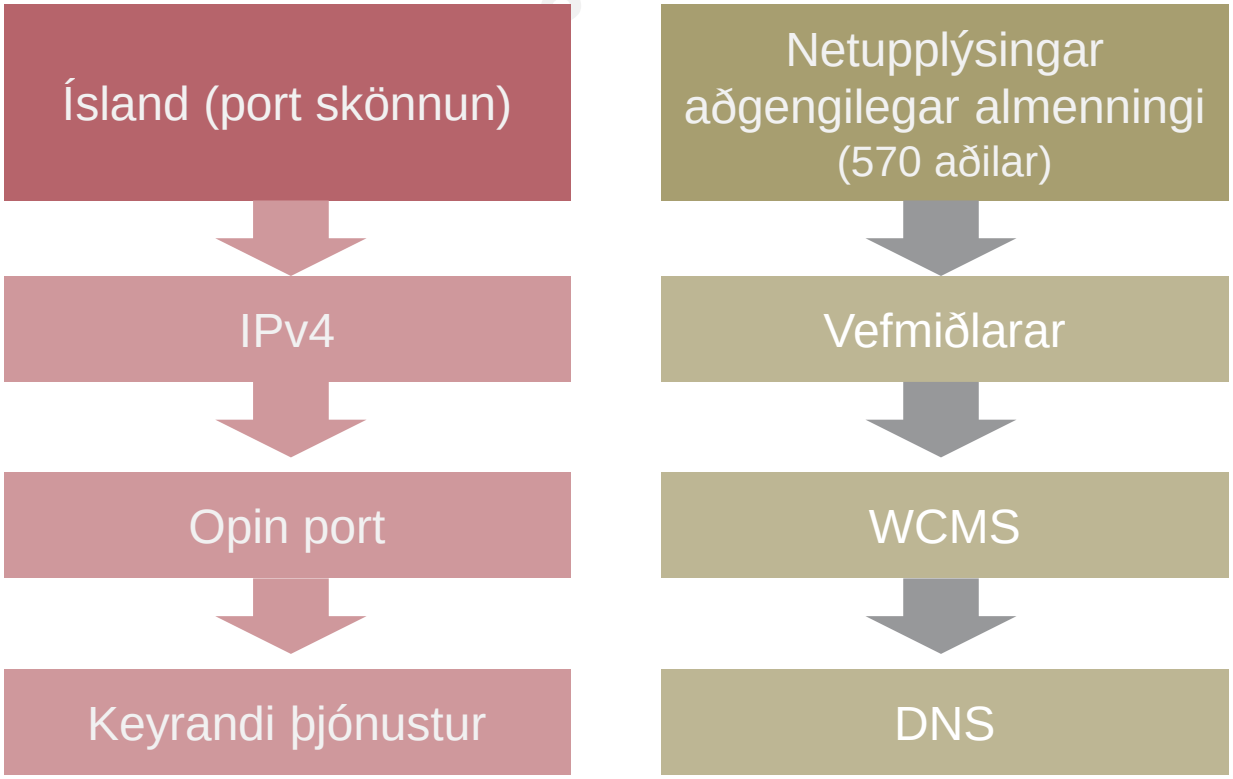
Við vildum prófa allt… hinsvegar

Við framkvæmdum ekki veikleikagreiningu á netunum sem við skönnuðum.

Áhættan var talin of mikil!

Hvað var skoðað?

Tveir stærstu þættir rannsóknarinnar



Aðferðir?

Allar IPv4 úthlutaðar til Íslands skannaðar, 770.000 IP tölur í heildina

Rannsóknin spannaði júní – ágúst 2013.

Notast við
- **ADSL tengingu**
- **Port skanna**
- **Sérsniðin skönnunar og greiningar tól**
- **Landið skannað: 100 port**

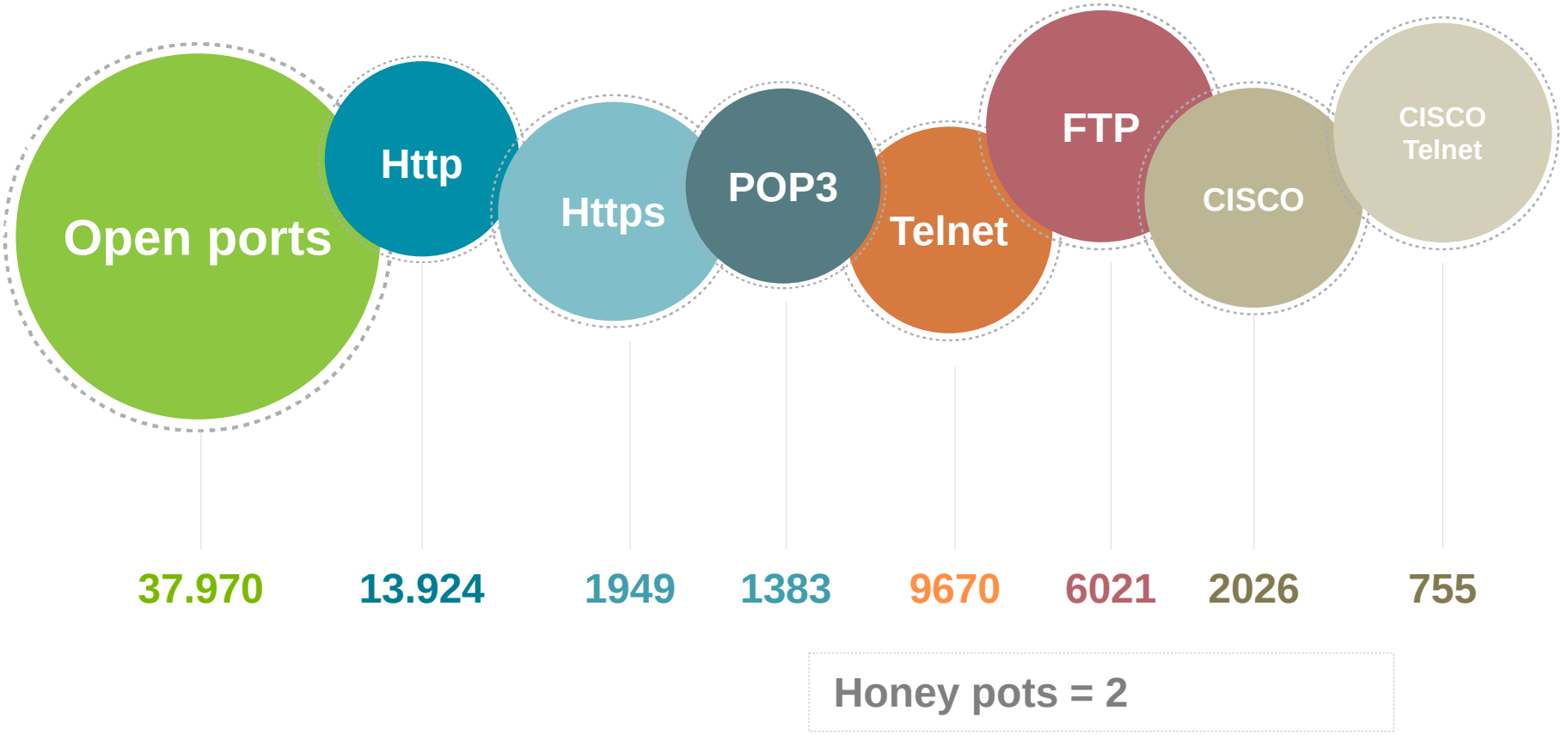
Reykjavik Internet Exchange – RIX
This is a list of Autonomous System Numbers that are, to the best of our knowledge, registered to Icelandic entities and are in use in Iceland. From the networks originated by these AS numbers we derive a list of IP networks in use in Iceland.

Please note that this is not a geo-location service, as there are always networks in use in Iceland that are originated by external AS numbers or by AS numbers registered to foreign or international service providers. Some networks, registered to Icelandic entities, are in use abroad, partially or totally. When we refer to Icelandic AS-numbers or networks, please bear this in mind.

Source: (http://www.rix.is/english/is-as-nets-en.html)

Rannsókn – Skönnun á IP tölum Íslands

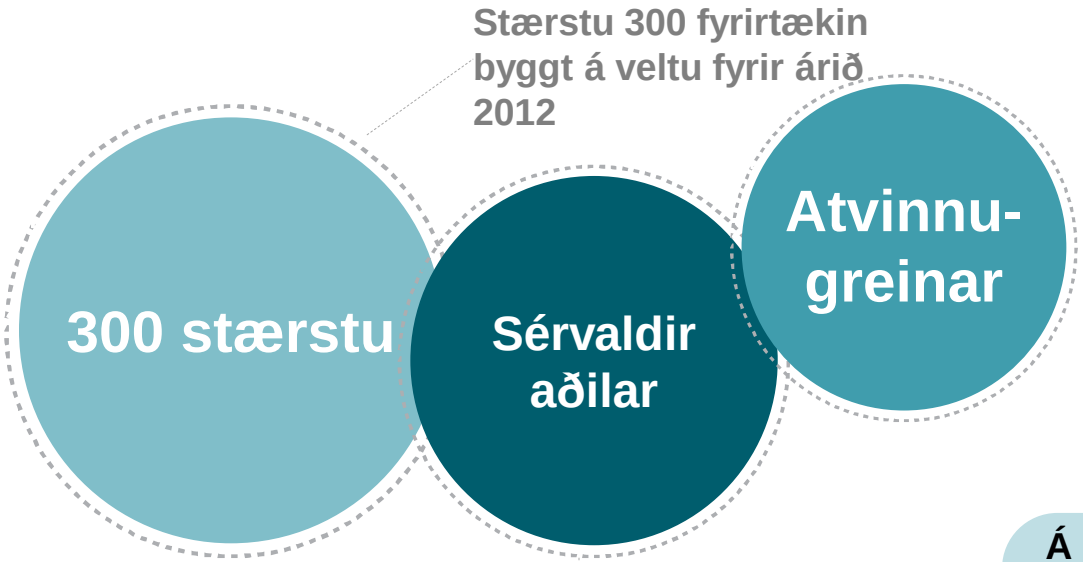
Skönnun á öllum IPv4 sem tilheyra Íslandi, Í heildina 770.000 IP tölur



Lénin skoðuð

Rannsókn – Lénin

Uppbygging rannsóknarinnar og umfang fyrir íslensku lénin.

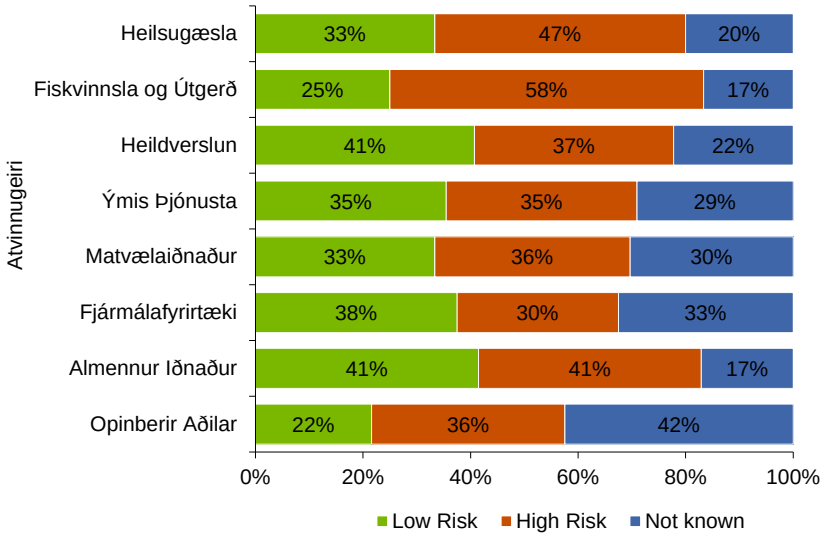


Á þessari kynningu munum við einbeita okkur að heildinni auk þess sem eftirfarandi þrjár atvinnugreinar eru skoðaðar: Public – Financial - Healthcare

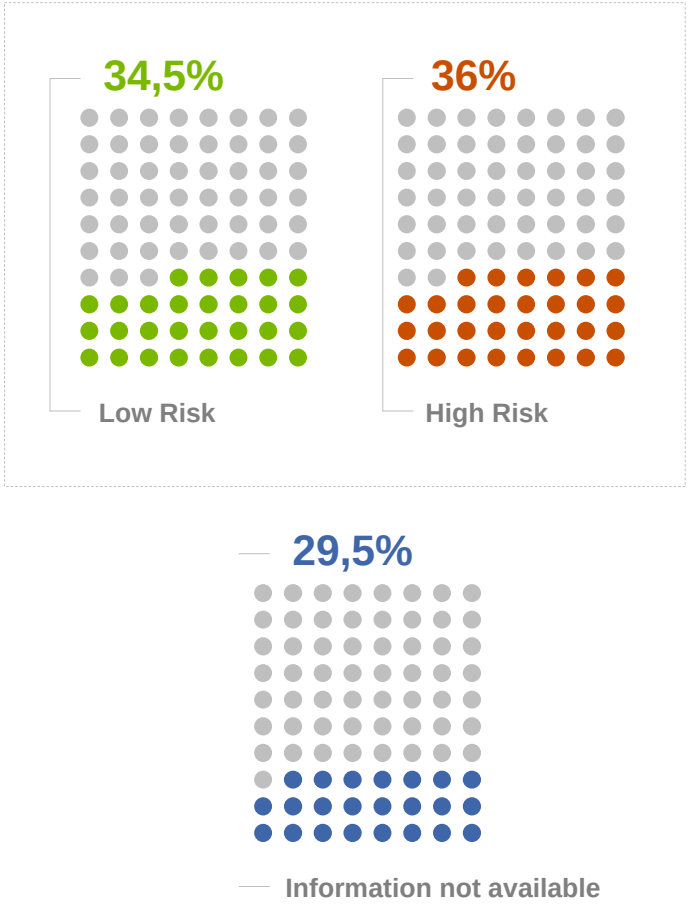
Niðurstöður – Vefmiðlarar

- **Rannsóknin skoðaði vefmiðlarana sem hýstu 570 lénin**
- **Áhætta er skilgreind sem mikil eða lítil**

Webserver niðurstöður eftir atvinnugeirum



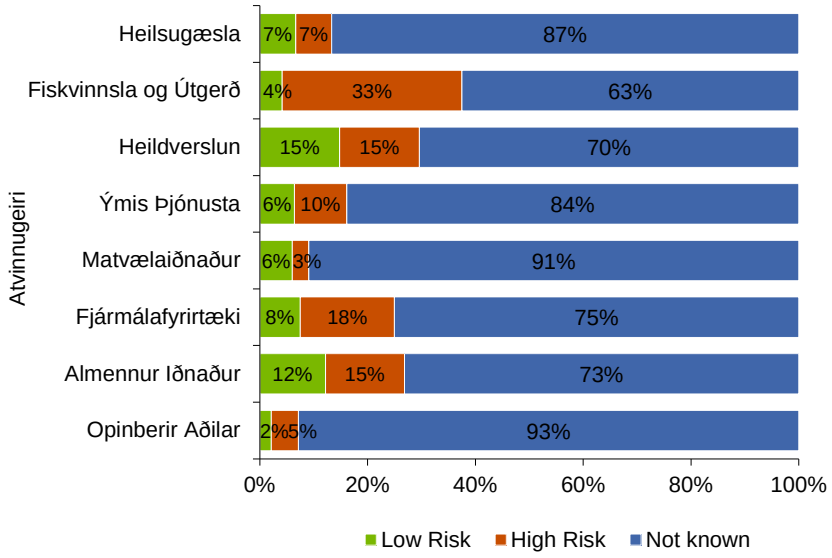
Heildar niðurstöður



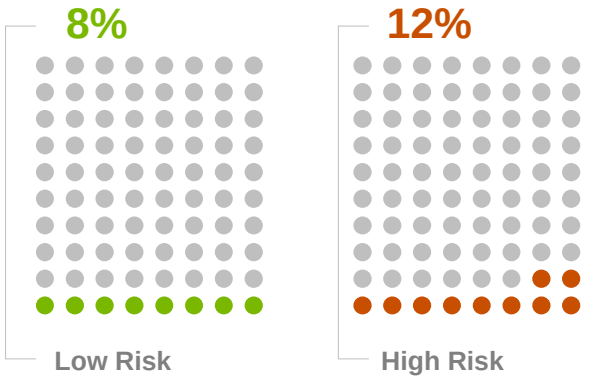
Niðurstöður – Web Content Management Systems (WCMS)

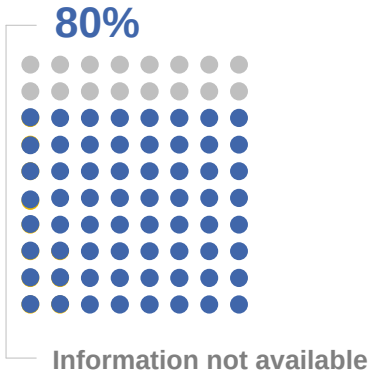
- **Rannsóknin skoðaði WCMS í notkun hjá 570 lénunum.**
- **Áhætta er skilgreind sem mikil eða lág.**

WebCMS niðurstöður eftir atvinnugeirum



Heildar niðurstöður



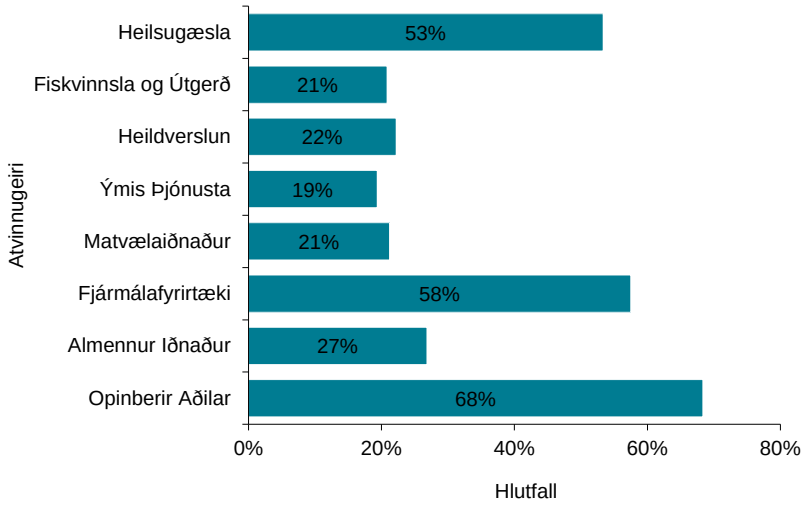


Niðurstöður – Web Content Management Systems (WCMS) - framhald

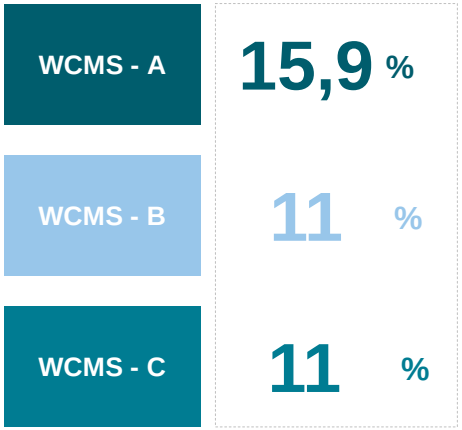
- **Hversu mörg óþekkt WCMS voru Íslensk af þessum 570?**

Íslensk WCMS: 40,7%

Hlutfall íslenskra vefja eftir atvinnugeirum



Dreifing WCMS



Niðurstöður – DNS

- **Hvernig er dreifingin á DNS skráningu?**
- **Fjöldi DNS miðlara fyrir 570 lénin: 309**

Stærstu DNS miðlararnir

Dreifing léna

SP A	16,9 %
SP B	11,5 %
SP C	9 %

DNS útgáfur

Hlutdeild

Bind	32 %
Microsoft	5,2 %
Unknown / hidden	61,5 %

Bind sem lekur upplýsingum um stýrikerfi: 46

Niðurstöður – TLS/SSL

- **Hversu margar einstakar IP tölur voru fyrir 570 lénin? 342 IP tölur**
- **Hversu margar af þessum 342 IP tölum bjóða upp á TLS/SSL? 188 (55%)**

Veikleikar skoðaðir:

Veikleikar sem fundust

Weak Cipher	96,3 %
SSLv2	39,4 %
MD5	4,8 %

Aðrir þættir:

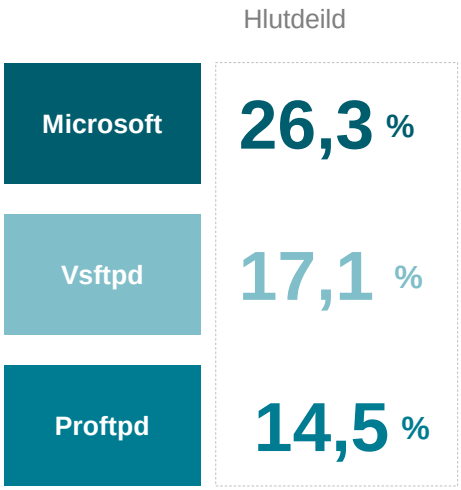
Veikleikar sem fundust

Self signed	16,5 %
Expired	15,4 %

Niðurstöður – FTP

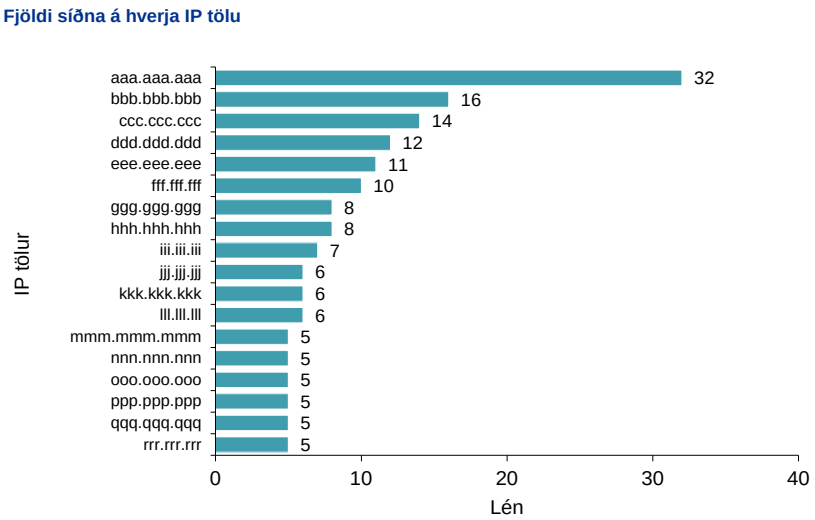
- **Hversu margar af 342 IP tölunum bjóða upp á FTP? 152**
- **Hversu margar af þessum 152 auglýsa TLS/SSL stuðning? 21 (13,8%)**

Dreifing milli tegunda



Niðurstöður – Dreifing á IP tölur

- **Hvernig er dreifingunni háttað fyrir þessar 342 IP tölur með tilliti til 570 l?**
- **Hversu stór hluti léna er á umfangsmestu IP tölurnar?**



Dreifing léna á IP tölur

Teknar eru fyrir 34 stærstu af 342

34 umfangsmestu IP tölur	38 %
Aðrar IP tölur	62 %

Niðurstöður – Dreifing milli þjónustuaðila

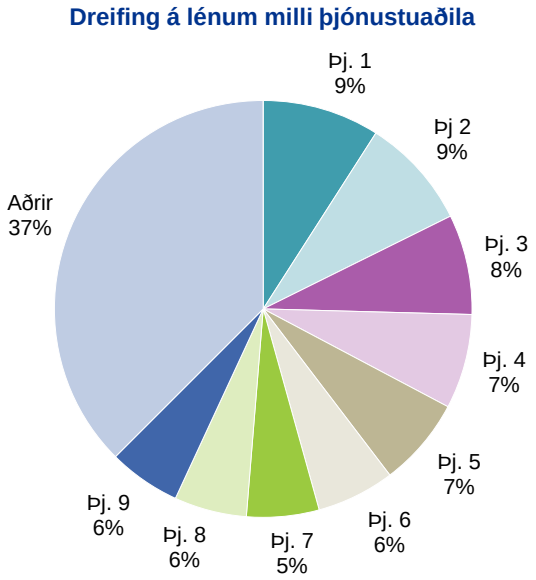
- **Hvernig var dreifingin milli þjónustuaðila fyrir þessi 570 lén?**

Dreifing Þjónustuaðila

Hlutdeild

SP A	7,3 %
SP B	5,3 %
SP C	4,9 %

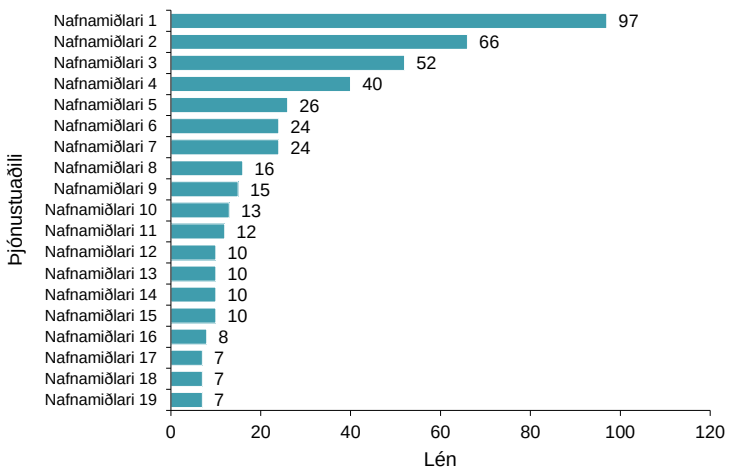
Dreifing þar sem Þjónustuaðilar eru þekktir:



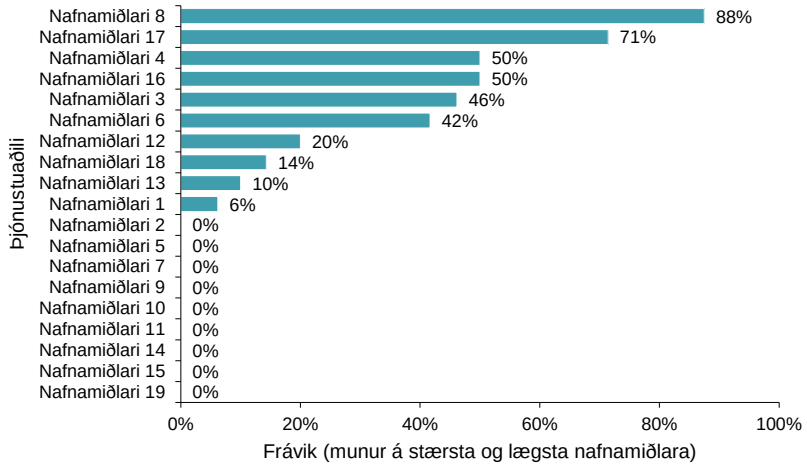
Niðurstöður – Umfang og frávik nafnamiðlara

- **Hverjir eru stærstu nafnamiðlararnir?**
- **Hversu mikið frávik eru á milli stærstu og minnstu nafnamiðlara hjá hverjum þjónustuaðila?**

Umfang nafnamiðlara hjá þjónustuaðila



Frávik á nafnamiðlurum þjónustuaðila



Varnarþættir

Hvaða fyrirbyggjandi stýringar og eftirlitsþættir eru í boði?

Australian Government – Department of Defense

“At least 85% of the targeted cyber intrusions that Defense Signals Directorate (DSD) responds to in 2011 could be prevented by following the Top 4 mitigation strategies listed in our Strategies to Mitigate Targeted Cyber Intrusions”

Helstu 35 eftirlitsþættirnir og stýringarnar

Mitigation Strategy Effectiveness Ranking	Mitigation Strategy	Overall Security Effectiveness	User Resistance	Upfront Cost (Staff, Equipment, Technical Complexity)	Maintenance Cost (Mainly Staff)	Designed to Prevent or Detect an Intrusion	Helps Mitigate Intrusion Stage 1: Code Execution	Helps Mitigate Intrusion Stage 2: Network Propagation	Helps Mitigate Intrusion Stage 3: Data Exfiltration

http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

Helstu 35 eftirlitsþættirnir og stýringarnar

Mitigation Strategy Effectiveness Ranking	Mitigation Strategy	Overall Security Effectiveness	User Resistance	Upfront Cost (Staff, Equipment, Technical Complexity)	Maintenance Cost (Mainly Staff)
1	**Application whitelisting** of permitted/trusted programs, to prevent execution of malicious or unapproved programs	Essential	Medium	High	Medium
2	**Patch applications** e.g. PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate high risk vulnerabilities within two days. Avoid Adobe Reader prior to X.	Essential	Low	High	High
3	**Patch operating system** vulnerabilities. Patch or mitigate high risk vulnerabilities within two days. Avoid running Windows XP or earlier.	Essential	Low	Medium	Medium
4	**Minimise the number of users with domain or local administrative privileges.** Such users should use a separate unprivileged account for email and web browsing.	Essential	Medium	Medium	Low

Stóra spurningin / Yfirlit

Hvert er þroskastig netöryggismála á Íslandi?

KPMG

cutting through complexity

Spurningar?

shermannsson@kpmg.is

kpmg.com/socialmedia