
Hvað er mikilvægast frá sjónarhóli einkafyrirtækja?

“Nú vantar stefnuna!” – faghópur Ský um öryggismál

Orri Hauksson
21. maí 2014

Hlíting gagnvart eftirlitsaðilum

Síminn hlítir ýmsum reglugerðum og lögum, meðal annars:

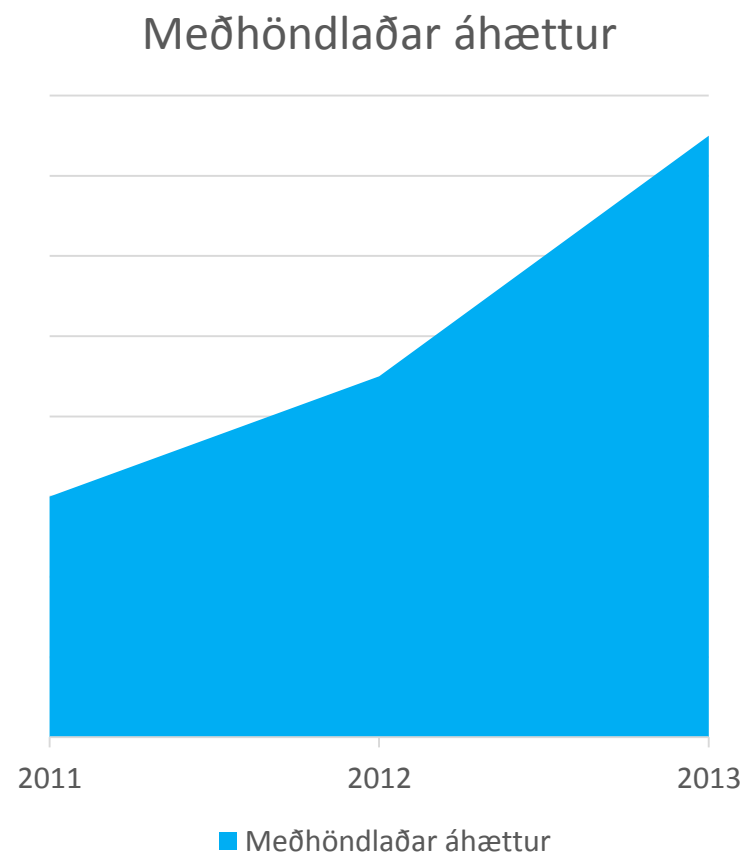
- Persónuverndarlög nr. 77/2003 ásamt reglugerðum PV
- Fjarskiptalög nr. 81/2003 ásamt reglugerðum PFS
- Tilmæli Fjármálaeftirlitsins nr. 2/2014
- Samkeppnislög nr. 44/2005
- Hlíting við PCI-DSS
- Hlíting við ISO 27001:2005

Samstarf með viðbragðsaðilum

- Síminn hefur starfað með CERT-ÍS frá stofnun og lítur á það sem mikilvægan þátt í sinni starfsemi
- Síminn var þátttakandi í fyrsta áfanga samevrópsku netöryggisæfingar á vegum ENISA og CERT-ÍS nú í lok apríl
- Síminn er hluti af viðbragðsáætlunum Almannavarna
- Birgjar Símans gegna veigamiklu og skilgreindu hlutverki í viðbragðsáætlunum Símans

Stjórn upplýsingaöryggis hjá Símanum

- Síminn byggir sitt stjórnkerfi upplýsingaöryggis á ISO 27001:2005 og framkvæmir reglulega áhættumat, innri og ytri úttektir, veikleikaskimanir og innbrotatilraunir (e. penetration testing)
- Fjöldi þeirra áhætta sem koma fram í mati og þarfnast meðhöndlunar fer vaxandi
- Fjöldi og alvarleiki veikleika sem er tilkynnt um virðist einnig fara vaxandi t.a.m. Hjartablóð, IE og aðrir „zero day“ veikleikar
- Uppljóstrarir Snowden - NSA



Hvernig aðstoðar Síminn viðskiptavinum?

- Síminn býður ISO27001 vottaða þjónustu á fyrirtækjamarkaði
- SPAM- og vírusvarnir á pósti
- Vírusvörn á útstöð - val
- Síun á óæskilegu efni – val
- Stýring á öryggi snjalltækja – val
- Tveggja þátta auðkenning – val
- Læsing gagna (lekavarnir) - val
- Rafrænt skilríki til auðkenningar á SIM korti – val
- Mínar síður – þjónustugátt viðskiptavina



Mikilvægi rafrænna auðkenna

- Rafræn skilríki frá Auðkenni 2008
- Möguleikinn til þess að geyma skilríki á SIM korti nóvember 2013
- Frá því að fyrst kom fram vilji stjórnvalda til þess að styðja við rafræna undirskrift eru liðin 13 ár
- Fyrst núna eru rafræn skilríki aðgengileg
- Fyrirséð flóðbylgja í notkun á rafrænum skilríkjum
- En hvað með Íslykilinn?
- „Skattskil 2016 eingöngu með rafrænum skilríkjum - Áskorun“

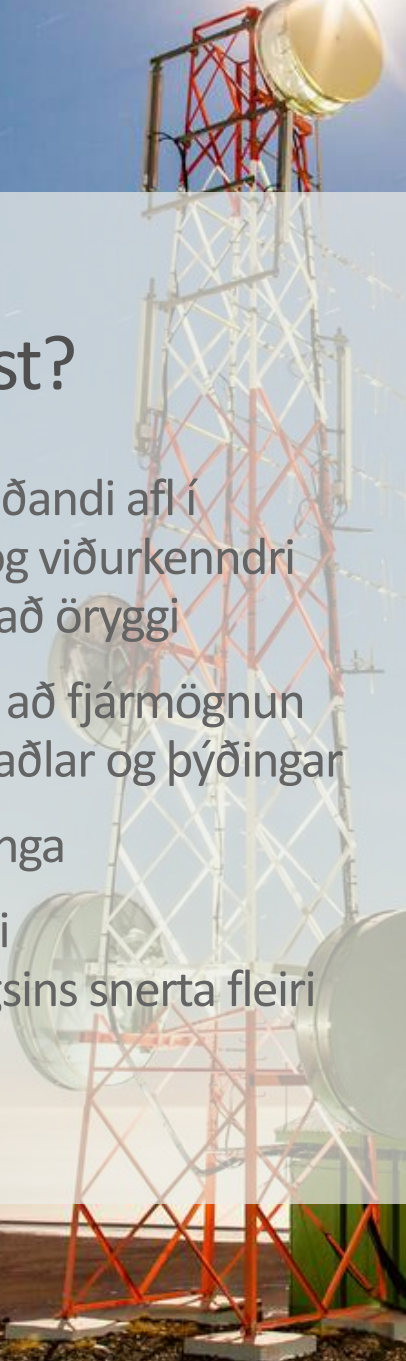
Authentication mechanisms	Threats											
(eIDA method)	1a	1b	1c	2a	2b	2c	3a	3b	4a	4b	4c	
Username/password	5	5	5	3	3	5	5	5	5	5	5	
TAN code list	4	3	5	5	5	5	5	5	5	4	5	
SMS-based OTP	1	1	4	3	2	5	4	5	4	2	5	
Time-based h/w OTP	1	1	3	5	3	5	3	5	4	3	5	
Chal.Resp. h/w OTP	1	1	3	4	2	4	3	4	3	2	5	
Mobile OTP App	1	2	3	3	3	5	3	5	3	3	5	
Token e-Signature	1	1	1	4	2	4	1	3	2	1	3	
Chip card e-Signature	1	1	1	3	1	4	1	3	2	1	3	
Mobile phone e-Signature	1	1	1	3	2	4	1	3	2	1	3	

Table 1 eIDE methods THREATS APPLICABILITY. Threats are described in section 4.1 above. Applicability ranges from 1: Not Applicable to 5: Highly Applicable

Hlutverk stjórnsvalda

– hvað er mikilvægast?

- Stjórnsvald þurfa að vera leiðandi afl í notkun nýrrar tækni jafnt og viðurkenndri aðferðafræði sem stuðlar að öryggi
- Stjórnsvald komi enn frekar að fjármögnun og útgáfu fagefnis t.a.m. staðlar og þýðingar
- Miðlun mikilvægra upplýsinga
- Málefni er varða ómissandi upplýsingainnviði samfélagsins snerta fleiri en fjarskiptafyrirtæki



Hlutverk stjórnsvalda

– hvað er mikilvægast?

- Öryggismál eru langhlaup – hefur tekið 13 ár fyrir rafræn skilríki
- Hver er sýn stjórnsvalda á lögsögu gagna?
- Samræmi í upplýsingaskyldu
- Markaðslausnir drífa framþróun
- Öryggi er aðgreining á markaði



Takk fyrir

