Það er val um auðkenningarleiðir
Nýr staðall til að meta áhættu

„Er þetta heilbrigt“, hádegisfundur Ský, Grand hóteli, 15. apríl 2015

Hörður Helgi Helgason
@HHelgi

LANDSLÖG

Borgartúni 26
105 Reykjavík
Talsími: 520 2900
Bréfasími: 520 2901
www.landslog.is

Hver er ég og hvernig veist þú það?

Spurningar?
#ErThettaHeilbrigt

Auðkenning er lykillinn – að öllu

- Daglegt líf, samskipti við vini, fjölskyldu og annað fólk
- Aðgangur að húsnæði, farartækjum, svæðum og aðstöðu

- -> Auðkenning með föstum kerfum og ferlum sem eru flest okkur lítt meðvituð og ósjálfráð

Spurningar?
#ErThettaHeilbrigt

Okkar stafræna líf

- Við erum samofin upplýsingatækni, eigum okkur annað líf, stafrænt
- Margt í því lífi speglar og samræmist vel lífi okkar í kjötheimum, en annað síður
- Eitt af því sem okkur gengur illa með þar – raunar verr og verr: Auðkenning
- Aðgangsstýringar: Auðkenning (sannvotun) og aðgangsheimildir

Spurningar?
#ErThettaHeilbrigt

Hverjar eru auðkenningarleiðirnar?

- Þekking, vörslur og eigindi
  - Þekking: Aðgangs-/lykilorð, PIN, öryggisspurningar
  - Vörslur: Aðgangskort, handsími eða annar farsími, rafræn eða hlutbundin skilríki
  - Eigindi: Eiginhandarundirritun; einnig lífkenni, svo sem sjáaldursmynstur, fingraför, andlitsfall, kjarnsýrusamsetning eða raddmynstur
- Ýmist farin ein leið eða fleiri þættir fléttaðir saman

Spurningar?
#ErThettaHeilbrigt

Í daglegu lífi erum við vön hinni fjölbreyttu flóru auðkenningar en í stafrænu lífi okkar erum við alltaf að leita hini einu réttu auðkenningarleið.

Hún er ekki til

Spurningar?
#ErThettaHeilbrigt

Val á auðkenningarleiðum

- Engin ein leið er rétt
- Þarf að byggjast á mati á þörfinni
  - of veik auðkenning: hætta á óheimilum aðgangi
  - of sterk auðkenning: hætta á skerðingu á nauðsynlegu aðgengi, óvarkárri meðferð eininda

- Góður staðall gæti hjálpað mikið til …

Spurningar?
#ErThettaHeilbrigt

ISO 29115:2013

- Information technology -- Security techniques -- Entity authentication assurance framework
- Tækninefnd FUT um dreifilyklaskipulag hefur til umsagnar frumvarp að íslenskum staðli, frÍST ISO 29115:2013 Upplýsingatækni - Öryggistækni – Umgjörð um fullvissu sannvottunar eininda

Spurningar?
#ErThettaHeilbrigt

Fyrir hvern er staðallinn?

- Nýtist útgefendum sannvottunaraðferða sem þurfa að meta fullvissustig þeirra
- Nýtist þjónustuveitendum sem þurfa að
  - meta þörf fyrir fullvissustig við veitingu þjónustu
  - velja sannvottunaraðferðir
- Nýtist einnig öðrum, t.d. eftirlitsaðilum, sem þurfa að meta sannvottunaraðferðir eða þörf fyrir fullvissustig

Spurningar?
#ErThettaHeilbrigt

Mat á þörf fyrir fullvissustig þjónustu

- Hefbundin áhættugreining, 4 fullv.stig (LoA)
  1. Lágmarks traust á auðkenningunni en nokkur vissa um að ávallt sé um sama aðila að ræða, t.d. sjálfvalið user/pass eða MAC addressa.
  2. Nokkur vissa um auðkenningu, einþátta í lagi.
  3. Mikil vissa, fjölþátta auðkenning og dulkóðun.
  4. Mjög mikil vissa. LoA3 + sanna auðkenni einsaklinga í eigin persónu og örugg geymsla dulkóðunarlykla og gagna.

Spurningar?
#ErThettaHeilbrigt

Val á fullvissustigi

Possible consequences of authentication failure	Possib. impact of authent. failure by LoA*			
	1	2	3	4
Inconv., distress or damage to standing or reputation	Min	Mod	Sub	High
Financial loss or agency liability	Min	Mod	Sub	High
Harm to the entity, its programs, or public interests	N/A	Min	Mod	High
Unauthorized release of sensitive information	N/A	Mod	Sub	High
Personal safety	N/A	N/A	Min Mod	Sub High
Civil or criminal violations	N/A	Min	Sub	High

* Min=Minimum; Mod=Moderate; Sub=Substantial; High=High

Spurningar?
#ErThettaHeilbrigt

Mat á fullvissustigi sannvottunaraðferða

- Raunhæft mat á fullvissustigi hverrar aðferðar er nauðsynlegt til að tryggja rétt val
- Nokkur þekkt íslensk dæmi:

Fullvissustig	Meginkröfur ISO 29115	Dæmi um sannvottunaraðferð sem talið er að uppfylli fullvissustigið
1	Einfalt lykilorð	Veflykill skattsins Lykilorð banka (án Auðkennislykils)
2	Flókið lykilorð, traust skráning og afhending	Íslykill
3	Tveggja þátta aðferð, t.d. lykilorð með styrkingu	Styrktur Íslykill (með SMS) Lykilorð banka+Auðkennislykill
4	Fullgild rafræn skilríki	Fullgild Íslandsrótarskilríki frá Auðkenni

(heimild: Þorvarður Kári Ólafsson, Þjóðskrá Íslands)

Spurningar?
#ErThettaHeilbrigt

Niðurstöður

- Auðkenning gegnsýrir allt okkar líf
- Þörf fyrir auðkenningu eru margar og mismunandi – einnig í okkar stafræna lífi
- Nýlegur staðall, sem liggur nú fyrir í frumvarpi að íslenskum staðli, getur hjálpað til við val á auðkenningarleiðum
- Mikilvægt að val á leiðum byggi á raunhæfu mati á þörf fyrir auðkenningu

Spurningar?
#ErThettaHeilbrigt

Spurningar?
#ErThettaHeilbrigt

hhh@landslog.is
www.landslog.is
@HHelgi