NIÐURSTÖÐUR ÚTTEKTAR Á ÖRYGGI OPINBERRA VEFJA 2017

UT Dagurinn 2017

30. Nóvember 2017

Svavar Ingi Hermannsson
CISSP, CISA, CISM

ÚTTEKT Á ÖRYGGI OPINBERRA VEFJA

- Unnið fyrir samgöngu og sveitarstjórnarráðuneytið
- Markmiðið er að stuðla að auknu öryggi á opinberum vefjum með því að afla upplýsinga um öryggi þeirra og koma ábendingum til ábyrgðarmanna og vefstjóra einstakra vefja
- Umfang: Ríki og sveitarfélög
- Tímabil: 15. júlí – 30. október
- Skýrslur sendar til tengiliða

HVERNIG VAR ÚTTEKTIN FRAMKVÆMD?

Hvað var gert?

TÆKNILEG ÖRYGGISÚTTEKT

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

TÆKNILEG ÖRYGGISÚTTEKT

- Tegundir öryggisveikleika sem fundust
  - SQL Injection veikleikar
  - XSS veikleikar
  - Öryggisveikleikar og gamlar/óstuddar útgáfur af vefumsjónarkerfum, vefmiðlurum og vefumsjónarkerfum
  - Viðkvæm gögn send ódulkóðuð (t.d. innskráning í vefumsjónarkerfi)
  - TLS stillingar ekki samkvæmt bestu starfsvenjum - https://www.ssllabs.com/projects/best-practices/

ÁRANGUR OG LÆRDÓMUR

Hvað hefur verið gert vel og hvað má betur fara?

ÁRANGUR OG LÆRDÓMUR

- Stórar jákvæðar breytingar frá því úttektin var framkvæmd síðast fyrir 2 árum:
  - Ábyrgðaraðilar 68 vefja sem höfðu greinst með “Alvarlega öryggisveikleika” brugðust við öllum ábendingunum og í ár fundust engir þekktir öryggisveikleikar.

ÁRANGUR OG LÆRDÓMUR

- Í einhverjum tilfellum fundust engir veikleikar fyrir 2 árum síðan en í dag er t.d. stýrikerfi, vefmiðlari eða vefumsjónarkerfi ekki lengur stutt af framleiðanda.
- Nýtt vefumsjónarkerfi sett upp en gleymst að setja upp TLS/SSL.
- Brugðist við ábendingum fyrir 2 árum síðan en ekki viðhaldið.
- Skipt um þjónustuaðila / vefumsjónarkerfi.

ÁRANGUR OG LÆRDÓMUR

- Ábyrgðaraðilar vefja þurfa að gera öryggiskröfur í samningum og veita eftirfylgni.

ÁRANGUR OG LÆRDÓMUR

- Skjöl sem hafa verið búin til og hægt er að nýta:
  - Samningsviðauki vegna upplýsingaöryggis - https://www.stjornarradid.is/media/forsaetisraduneyti-media/media/utvefur/samningsvidauki-v-upploryggis.pdf
  - Leiðbeiningar við gerð áhættumats - https://www.stjornarradid.is/media/forsaetisraduneyti-media/media/utvefur/ahaettumat-oryggisradstafanir.pdf
  - Eyðublað fyrir áhættumat - https://www.stjornarradid.is/media/forsaetisraduneyti-media/media/utvefur/ahaettumat-eydublad2016.xlsx

TAKK FYRIR!

- Spurningar?

svavar@security.is

http://www.security.is/