ÚTTEKT Á ÖRYGGI OPINBERRA VEFJA

Svavar Ingi Hermannsson, CISSP, CISM, CISA

ÚTTEKT Á ÖRYGGI OPINBERRA VEFJA

- Unnið fyrir Innanríkisráðuneytið.
- 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 (256 vefir)
- Tímabil: 1. júlí – 30. október
- Skýrslur sendar til tengiliða

Hvað var gert?

HVERNIG VAR ÚTTEKTIN FRAMKVÆMD?

Tæknileg úttekt – Hvað var skoðað?

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

Tæknileg úttekt – Viðbrögð

- Mjög jákvæð viðbrögð frá tengiliðum og þjónustuaðilum.
- Fjöldi spurninga.
- Strax farið að vinna að úrbótum.
- Samskipti við þjónustuaðila og hugbúnaðarhús.

Hver ber ábyrgð á hverju?

ÁBYRGÐ Á ÖRYGGISMÁLUM

Ábyrgð á öryggismálum

- Ábyrgðarmaður vefs (vefstjóri og forstöðumaður)
  - Samningsmál og eftirfylgni
- Hugbúnaðarhús
  - Tilkynna öryggisveikleika og bjóða upp á öryggisuppfærslur um leið og þær verða til.

Ábyrgð á öryggismálum

- Þjónustuaðilar
  - Vakta kerfi sem verið er að þjónusta, tilkynna um öryggisveikleika sem finnast og bjóða upp á öryggisuppfærslur um leið og þær verða til.
- Hýsingaraðilar
  - Vakta stýrikerfi og vefmiðlara, setja inn öryggisuppfærslur.

VEIKLEIKAR OG ÚRBÆTUR

Tegundir veikleika sem fundust

- SQL Injection veikleikar
  - Fá framleiðanda til að laga öryggisveikleika.
- XSS veikleikar
  - Fá framleiðanda til að laga öryggisveikleika.

Tegundir veikleika sem fundust

- Vefumsjónarkerfi með þekktum öryggisveikleikum
  - Biðja hýsingar-/þjónustu- aðila um að setja inn nýjustu öryggisuppfærslur frá framleiðanda.
- Vefmiðlari með þekktum öryggisveikleikum
  - Biðja hýsingar-/þjónustu- aðila um að setja inn nýjustu öryggisuppfærslu frá framleiðanda.

Tegundir veikleika sem fundust

- Stýrikerfi með þekktum öryggisveikleikum
  - Biðja hýsingar-/þjónustu- aðila um að setja inn nýjustu öryggisuppfærslu frá framleiðanda.
- Innskráning í vefumsjónarkerfi fer fram yfir ódulkóðuð samskipti.
  - Í samráði við framleiðanda, hýsingar-/þjónustu- aðila: stilla innskráningu þannig að hún fari yfir TLS(HTTPS) samskipti (getur kostað skilríki).

Tegundir veikleika sem fundust

- TLS ekki samkvæmt bestu starfsvenjum
  - Fara fram á það við hýsingaraðila að stilla vefmiðlara þannig að hann uppfylli bestu starfsvenjur. Þær er hægt að finna hér: https://www.ssllabs.com/projects/best-practices/

Lærdómur

- Ábyrgðarmaður vefs þarf að gera öryggiskröfur í samningum og veita eftirfylgni.
- Hugbúnaðarhús þurfa að axla ábyrgð og bjóða upp á öruggar uppsetningar og öryggisuppfærslur.
- Hýsingar-/þjónustu- aðilar þurfa að axla ábyrgð og bjóða upp á örugga hýsingu með því að setja reglulega inn öryggisuppfærslur og viðhalda kerfunum sínum.

Takk Fyrir!

- Einhverjar spurningar?
  - svavar@security.is