HVAÐ ER SPUNNIÐ Í OPINBERA VEFI 2017?

ÚTTEKT Á ÖRYGGI OPINBERRA VEFJA

Svavar Ingi Hermannsson, CISSP, CISM, CISA

Úttekt á öryggi opinberra vefja

- Upplýsingar um úttekt
  https://www.stjornarradid.is/verkefni/upplysingasamfelagid/opinberir-vefir/uttektir-a-opinberum-vefjum/
- Sjálfsmat
- Tæknileg úttekt á vefjum

Sjálfsmat - Niðurstaða

- Sjálfsmat – spurningalisti og einkunnagjöf
  - https://www.stjornarradid.is/lisalib/getfile.aspx?itemid=7c7dcbee-5504-11e7-941a-005056bc530c

- Áhættuflokkar
  - Lítil áhætta 15 - 35 stig
  - Miðlungs áhætta 36 - 58 stig
  - Mikil áhætta 59 stig +

Sjálfsmat – Upplýsingar um vefinn

- Hvaða upplýsingar eru hýstar á vefnum?
  - Eingöngu almennar og opinberar upplýsingar sem allir hafa aðgang að?
  - Almennar upplýsingar en einnig upplýsingar um einstaklinga, s.s. nöfn, netföng eða aðrar upplýsingar, t.d. áskrifendur að fréttum?
  - Almennar upplýsingar en einnig viðkvæmar upplýsingar eins og greiðslukortanúmer, kennitölur, heilsufarsupplýsingar eða aðrar viðkvæmar persónuupplýsingar?

Sjálfsmat – Upplýsingar um vefinn

- Hvaða þjónusta er veitt á vefnum?
  - Einfaldur vefur, almenn upplýsingaveita.
  - Er birt efni sem sótt er á aðra vefi, svo sem RSS-fréttastraumar, efni frá Datamarket eða samfélagsmiðlum?
  - Geta notendur skráð sig á námskeið, sent inn beiðnir eða greitt fyrir þjónustu?

Sjálfsmat – Upplýsingar um vefinn

- Hvernig er miðlun upplýsinga háttað?
  - Í gegnum vef eingöngu
  - Í gegnum vef og snjallforrit (öpp).

Sjálfsmat – Upplýsingar um vefinn

- Hversu oft er efni vefs uppfært?
  - Mánaðarlega eða sjaldnar.
  - Vikulega.
  - Oftar en einu sinni í viku eða nokkrum sinnum í viku.
  - Daglega.

Sjálfsmat – Upplýsingar um vefinn

- Hversu margir hafa aðgang að vefumsjónarkefinu?
  - 1 til 5.
  - 6 til 10.
  - 11 til 20.
  - Fleiri en 20

Sjálfsmat – Upplýsingar um vefinn

- Hversu lengi getur stofnun starfað án vefjarins án þess að það hafi meiri háttar áhrif eða óþægindi á starfsemi stofnunarinnar?
  - Lengri tíma en viku.
  - Viku eða skemmri tíma.
  - Þrjá daga eða skemmri tíma.
  - Einn dag eða skemmri tíma.

Sjálfsmat – Tæknilegar upplýsingar

- Hvernig er hýsingu á vefnum háttað?
  - Stofnunin sér sjálf um hýsingu og rekstur á vefnum.
  - Vefurinn er hýstur hjá þjónustuaðila en stofnunin sér um að setja inn uppfærslur á vefkerfinu o.s.frv.
  - Vefurinn er hýstur hjá stofnun en þjónustuaðilinn sér um að setja inn uppfærslur á vefkerfinu o.s.frv.
  - Hýsingu og rekstri er útvistað að öllu leyti.

Sjálfsmat – Tæknilegar upplýsingar

- Hvernig er vefumsjónarkerfið?
  - Kerfið er þekkt lausn sem margir aðilar nota, t.d. Eplica eða Lisa.
  - Um er að ræða opinn hugbúnað eins og WordPress eða Drupal.
  - Um er að ræða sérsmíðaða lausn fyrir viðkomandi stofnun.
  - Blanda af ofangreindu.

Sjálfsmat – Tæknilegar upplýsingar

- Hvernig er innskráningu í vefumsjónarkerfi háttað (þetta má kanna hjá vefþjónustuaðila)?
  - Notandanafn og krafa um sterkt lykilorð þar sem lykilorð er dulkóðað.
  - Notandanafn og krafa um sterkt lykilorð þar sem lykilorð er ekki dulkóðað.
  - Notandanafn og einfalt lykilorð.

Sjálfsmat – Tæknilegar upplýsingar

- Eru innskráningar í vefumsjónarkerfi dulkóðaðar yfir TLS/HTTPS?
  - Já
  - Nei

Sjálfsmat – Tæknilegar upplýsingar

- Er aðgangur að vefumsjónarkerfinu leyfður utanhúss (yfir netið)?
  - Já
  - Nei

Sjálfsmat – Tæknilegar upplýsingar

- Sækir vefurinn sjálfvirkt upplýsingar frá öðrum kerfum, t.d. með uppflettingum í gagnagrunna annarra stofnana?
  - Engar tengingar við kerfi ytri aðila.
  - Tenging til staðar við eitt kerfi hjá ytri aðila, t.d.ef flett er upp á kennitölu í þjóðskrá til að sækja nafn og heimilisfang.
  - Tenging til staðar við fleiri en eitt kerfi hjá ytri aðila.

Sjálfsmat – Tæknilegar upplýsingar

- Tengist vefurinn við upplýsingakerfi stofnunarinnar?
  - Engar tengingar við önnur kerfi.
  - Tenging við kerfi sem innihalda ekki viðkvæmar upplýsingar, t.d. ef dagatöl, listi yfir starfsfólk eða upplýsingar um atburði eru sóttar í sérstakan grunn og birtar á vef.
  - Tenging við kerfi sem innihalda viðkvæmar upplýsingar, t.d. viðskiptamannakerfi, fjárhags- og/eða skjalakerfi. Annað dæmi er ef fyllt er út umsókn á vef og hún rennur beint inn í skjalakerfi stofnunar.

Sjálfsmat – Tæknilegar upplýsingar

- Þurfa notendur að auðkenna sig?
  - Notendur þurfa aldrei að auðkenna sig á vefnum.
  - Notendur geta þurft að auðkenna sig til að nálgast ákveðna þjónustu og auðkenningin fer fram í innskráningu Ísland.is.
  - Notendur geta þurft að auðkenna sig til að nálgast ákveðna þjónustu með notendanafni og lykilorði.
  - Annars konar auðkenning.

Sjálfsmat – Tæknilegar upplýsingar

- Er upplýsingatæknideild til staðar?
  - Já
  - Já, en rekstri upplýsingatæknikerfa er útvistað að hluta.
  - Nei, rekstri upplýsingatæknikerfa er alfarið útvistað.

HVAÐ ER SPUNNIÐ Í OPINBERA VEFI 2017?

TÆKNILEG ÚTTEKT

Tæknileg úttekt

- Vefumsjónarkerfi
- Vefmiðlari
- Stýrikerfi
- Annað
  - 40 vefir skoðaðir nánar með tilliti til OWASP top 10.
  - http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf

Tæknileg úttekt - framhald

- Vefumsjónarkerfi
  - Ekki fundust veikleikar.
  - Ekki fundust upplýsingar um vefumsjónarkerfi.
  - Veikleikar fundust.
  - Alvarlegir veikleikar fundust.
    - Ekki lengur stutt af framleiðanda.
  - XSS / SQL Injection veikleikar.

Tæknileg úttekt - framhald

- Vefmiðlari
  - Ekki fundust veikleikar.
  - Ekki fundust upplýsingar um vefmiðlara
  - Veikleikar fundust.
  - Alvarlegir veikleikar fundust.
    - Ekki lengur stutt af framleiðanda.

Tæknileg úttekt - framhald

- Stýrikerfi
  - Ekki fundust veikleikar.
  - Ekki fundust upplýsingar um stýrikerfi.
  - Veikleikar fundust.
  - Alvarlegir veikleikar fundust.
    - Ekki lengur stutt af framleiðanda.

Tæknileg úttekt - framhald

- Annað
  - TLS (HTTPS) uppfyllir ekki bestu starfsvenjur.
  - Innskráning fer fram með ódulkóðuðum samskiptum.

Hvað getum við gert?

- Umræðuskjal – Samningsviðauki
  - https://www.stjornarradid.is/media/forsaetisraduneyti-media/media/utvefur/samningsvidauki-v-upploryggis.pdf

Hvað getum við gert?

- Dæmi:
  - Öryggisuppfærslur á stýrikerfum
  - Öryggisuppfærslur á vefkerfum og hugbúnaði
  - Veikleikagreiningar / innbrotsprófanir
  - Innbrotsvöktunarkerfi
  - Frávikaskráning og tilkynningar um öryggisfrávik
  - Innra eftirlit
  - O.fl.

Hvað getum við gert?

- Áhættumat, eyðublað fyrir áhættumat og dæmi um öryggisstefnu
  - https://www.stjornarradid.is/efst-a-baugi/frettir/stok-frett/2017/01/06/Upplysingaoryggi-samningsvidauki-leidbeiningar-og-eydublod-fyrir-gerd-ahaettumats/

Takk Fyrir!

- Einhverjar spurningar?
  - svavar@security.is

SECURITY.IS