HVAÐ ÞARF VEFSTJÓRINN AÐ VITA UM ÖRYGGISMÁL?

Staða öryggismála á opinberum vefjum

Hádegisfundur Skýrslutæknifélagsins
21. október 2015

Guðbjörg Sigurðardóttir

Vinnuhópur um umbætur á opinberum vefjum

- Guðbjörg Sigurðardóttir, innanríkisráðuneyti
- Elísabet Jónasdóttir, innanríkisráðuneyti
- Anna Guðrún Björnsdóttir, Sambandi íslenskra sveitarfélaga
- Björn Sigurðsson, forsætisráðuneyti
- Halla Björg Baldursdóttir, Þjóðskrá Íslands
- Sigurður Davíðsson, velferðarráðuneyti

Verkefnið: Umbætur á opinberum vefjum 2005-

Það felur í sér:

- reglulegar endurbætur og viðbætur á **vefhandbók** (sjá ut.is)
- **námskeið** fyrir vefstjóra opinberra vefja (ríkis og sveitarfélaga)
- **beina aðstoð** við vefstjóra (vefstjórar heimsóttir) og
- **mat/úttekt** á öllum helstu opinberu vefjunum annað hvert ár (um 270 vefir).

Verkefnið er fjármagnað af verkefnafé stefnunnar um upplýsingasamfélagið – ***Vöxtur í krafti netsins***.

Verkefni útvíkkað – öryggginu bætt við

- Árið 2014 var verkefnið útvíkkað – nær nú til öryggis vefja.
- **Markmiðið** er að auka öryggi opinberra vefja vegna vaxandi ógna á netinu.
- **Hvað þarf að gera?**
  - Fræðsluefni
  - Námskeið
  - Stuðningur við vefstjóra
  - „Mæla/meta“ öryggi vefjanna.
- Vandasamt verkefni – gerðar eru **auknar kröfur** til vefja og ábyrgðarmanna þeirra.
- Vefstjórar þurfa þó ekki að vera **„tæknilegir“ sérfræðingar**

Fræðsluefni um öryggi opinberra vefja

- Nýtt efni í handbók um opinbera vefi á ut.is
- Leiðbeinandi texti og gátlistar um öryggismál á opinberum vefjum (sjá ut.is)

Námskeið fyrir vefstjóra opinberra vefja

- Haldin eru s**érstök öryggisnámskeið** fyrir vefstjóra – síðast 1. júní 2015
- Fyrirhugað að halda einnig öryggisnámskeið fyrir starfsmenn tölvudeilda þ.e. fyrir þá sem sjá um net, hugbúnað og vélbúnað stofnana og sveitarfélaga.

Stuðningur við vefstjóra

- Á árnunum 2012-2013 fengu ríflega 50 stofnanir beina aðstoð frá sérfræðingi í vefmálum þ.e. við að auka gæði vefjanna og laga að viðmiðum í vefhandbókinni.
- **Skoðað verður** í kjölfar öryggisúttektar **hvort og hvernig** hægt sé að styðja vefstjóra í öryggismálum, einkum í tengslum við þá vefi sem koma verst út úr öryggismatinu.

Mat/úttekt á öryggi opinberra vefja

- Í fyrsta skipti er nú verið að meta **öryggi vefjanna** (aðgreint verkefni).
- Allir vefir (263) verða skannaðir með forritum til að leita að öryggisveikleikum.
- Tengiliðir vefjanna (vefstjórar) svara stuttum spurningarlista.
- Tæplega 40 vefir verða skoðaðir ítarlegar af öryggissérfræðingi.

Dæmi

um stuttar skýrslur sem sendar eru til stofnana og sveitarfélaga þegar búið er að framkvæma öryggisúttekt á vef þeirra.

Efni: Niðurstöður öryggisúttektar á vefnum http://www.xxxx.is/

Í tengslum við könnunina *Hvað er spunnið í opinbera vefi 2015* var í fyrsta sinn gerð úttekt á öryggi 263 opinberra vefja ríkis og sveitarfélaga. 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. Í mörgum tilfellum er um að ræða atriði sem auðvelt er að ráða bót á þegar vitneskjan um þau liggur fyrir. Upplýsingar um öryggi einstakra vefja verða ekki birtar opinberlega, þær verða einungis aðgengilegar þeim sem vinna að úttektinni og forsvarsmanni/vefstjóra viðkomandi ráðuneytis, stofnunar eða sveitarfélags.

Öryggisúttektina vann Svavar Ingi Hermannsson upplýsingaöryggissérfræðingur á tímabilinu 1. júlí til 30. október 2015. Vefirnir 263 voru skannaðir með forritum sem leita að veikleikum í öryggi þeirra. Þeir vefir sem taldir eru innihalda sérstaklega viðkvæmar upplýsingar voru skoðaðir ítarlegar, meðal annars með hliðsjón af þekktri aðferðafræði sem lýst er í Vefhandbókinni á ut.is (OWASP top 10), sjá: http://www.ut.is/vefhandbok/yfirlit/oryggi/ og http://www.ut.is/vefhandbok/yfirlit/oryggi/veflausnir.

Ekki voru framkvæmdar innbrotsprófanir heldur einungis leitað eftir öryggisveikleikum. Sjá útskýringar á framkvæmd öryggisúttektarinnar á UT-vefnum, á slóðinni http://www.ut.is/konnun2015/framkvaemd/.

Aðferð við mat á veikleikum

Mat á veikleikum er byggt á svokölluðum CVSS-gildum (Common Vulnerability Scoring System) þegar þau eru til. Ef þau eru ekki til er byggt á huglægu mati. Heildarmat á veikleikum vefs tekur mið af „veikasta hlekknum“ sem finnst á vefnum eða með öðrum orðum stærsta öryggisveikleikanum sem finnst. Flokkunin sem stuðst er við í þessari skýrslu fylgir eftirfarandi viðmiðum:

CVSS-gildi	Mat á veikleikum
7 - 10	**Alvarlegir veikleikar**
0.1 - 6.9	**Veikleikar fundust**
0	**Ekki fundust veikleikar**

Fyrirvari

Hvort sem veikleikar fundust við úttektina á öryggi vefsins eða ekki, er alls ekki tryggt að aðrir öryggisveikleikar séu ekki til staðar. Öryggisúttekt sem þessi er bundin við umfang, tíma, útgáfu viðkomandi vefkerfis, vefmiðlara og stýrikerfi á þeim tíma og þeim aðgangi sem prófunaraðili hafði að vefnum. Það er mikilvægt að halda áfram öryggisúttektum í framtíðinni, sérstaklega þegar meiriháttar breytingar eru gerðar á vefkerfinu eða þegar nýrri virkni er bætt við eða breytt. Æskilegt er að stofnun þín óski eftir skýrslum frá þjónustu-/hýsingar- og rekstraraðilum vegna innbrotsprófana og öryggisúttekta að lágmarki einu sinni á ári á því umhverfi er tengist vefnum.

TRÚNAÐARMÁL

Öryggisúttekt á vefnum http://www.xxxxx.is/
Neðangreindar upplýsingar lúta aðeins að þeim vef sem tilgreindur er hér að ofan. Þær eru tæknilegs eðlis og tölvudeild, tæknimaður eða fyrirtæki sem þjónustar vefinn þarf að fá þær til að geta brugðist við ábendingunum og þannig bætt öryggi vefsins.

NIÐURSTÖÐUR (sértækar niðurstöður fyrir hvern vef fyrir sig):

Heildarmat á öryggi vefsins: **Alvarlegir veikleikar**
Skoðaðir voru þekktir öryggisveikleikar á vefmiðlara, vefumsjónarkerfi og stýrikerfi. Matið byggist á svokallaðri CVSS-einkunnagjöf þar sem niðurstaðan endurspeglast í alvarlegasta veikleikanum. Sjá sundurliðun matsþátta hér að neðan.

Vefumsjónarkerfi: Ekki fundust veikleikar
Ekki fundust upplýsingar um útgáfu af vefumsjónarkerfi. Ekki er vitað um þekkta öryggisveikleika.
Vefmiðlari: Ekki fundust veikleikar
Ekki er vitað um þekkta öryggisveikleika.
Stýrikerfi: Ekki fundust veikleikar
Ekki er vitað um þekkta öryggisveikleika.

Aðrir veikleikar:
Innskráning í vefumsjónarkerfi (http://www.xxxxx.is/yyy/) fer fram með ódulkóðuðum samskiptum: Alvarlegir veikleikar
Notandanafn og lykilorð er sent ódulkóðað. Þegar notendanöfn og lykilorð eru send er mikilvægt að það sé gert á öruggan hátt og yfir dulkóðuð samskipti. Sjá nánari upplýsingar í **OWASP top 10 - A2**.

Almenn öryggisatriði sem þarf að huga að fyrir alla vefi:

Vefumsjónarkerfi:
Mikilvægt er að tryggja að framleiðandi vefumsjónarkerfis láti vita ef öryggisgallar finnast, hefjist strax handa við að lagfæra þá og bjóði upp á öryggisuppfærslur um leið og þær verða til.

Öryggisuppfærslur og viðhald
Æskilegt er að fara fram á það við hýsingar-/þjónustuaðila að settar séu inn öryggisuppfærslur í tengslum við stýrikerfi, vefmiðlara, vefumsjónarkerfi og aðrar mögulegar þjónustur og íhluti (e. Plug-in) eigi síðar en 30 dögum eftir að þær hafa verið gefnar út. Bent er á að setja slík atriði inn í samninga.

Skýrslur vegna innbrotsprófana og öryggisúttekta
Æskilegt er að óska eftir skýrslum vegna innbrotsprófana og öryggisúttekta á því umhverfi er tengist vefnum að lágmarki einu sinni á ári frá þjónustu-/hýsingar- og rekstraraðilum.

Annað dæmi

Sértæk niðurstaða fyrir annan vef

NIÐURSTÖÐUR:

Heildarmat á öryggi vefsins: **Alvarlegir veikleikar**

Skoðaðir voru þekktir öryggisveikleikar á vefmiðlara, vefumsjónarkerfi og stýrikerfi. Matið byggist á svokallaðri CVSS-einkunnagjöf þar sem niðurstaðan endurspeglast í alvarlegasta veikleikanum. Sjá sundurliðun matsþátta hér að neðan.

Vefumsjónarkerfi: Veikleikar fundust

Ekki fundust upplýsingar um útgáfu af vefumsjónarkerfi. **XSS** galli fannst í vefleit. Hægt er að finna nánari upplýsingar um XSS galla í **OWASP top 10 –A3**. Mikilvægt er að láta framleiðanda vita sem sem fyrst til þess að laga viðkomandi öryggisgalla.

Vefmiðlari: Ekki fundust veikleikar

Ekki er vitað um þekkta öryggisveikleika.

Stýrikerfi: Ekki fundust veikleikar

Ekki er vitað um þekkta öryggisveikleika.

Aðrir veikleikar:

Innskráning í vefumsjónarkerfi (http://www.yyyyy.is/zzzzn/) fer fram með ódulkóðuðum samskiptum: Alvarlegir veikleikar

Notandanafn og lykilorð er sent ódulkóðað. Þegar notendanöfn og lykilorð eru send er mikilvægt að það sé gert á öruggan hátt og yfir dulkóðuð samskipti. Sjá nánari upplýsingar í **OWASP top 10 - A2**.

Dæmi um hvað vefstjórinn finnur þegar hann leitar skýringa

"XSS is the most prevalent web application security flaw. XSS flaws occur when an application includes user supplied data in a page sent to the browser without properly validating or escaping that content. There are three known types of XSS flaws: 1) Stored, 2) Reflected, and 3) DOM based XSS.

Detection of most XSS flaws is fairly easy via testing or code analysis……" o.s.frv..

Þjónustuveitendur/tölvudeildir þurfa að fá niðurstöður öryggisúttektarinnar

Önnur verkefni sem innanríkisráðuneytið vinnur að og snerta net- og upplýsingaöryggi

Stefna um net- og upplýsingaöryggi

- Innanríkisráðuneytið hefur gefið út fyrstu stefnuna um net- og upplýsingaöryggi, sjá: http://www.innanrikisraduneyti.is/frettir/nr/29272/
- Felur í sér að gerðar verða auknar kröfur til opinberra upplýsingakerfa m.a. opinberra vefja.
- Innleiðing stefnunnar er að hefjast.
- Sett hefur verið á fót Netöryggisráð og komið verður á víðtæku samráði.

Frumvarp um eflingu netöryggissveitar

- Til umsagnar eru nú á vef innanríkisráðuneytis drög að lagafrumvarpi um breytingar á lögum um almannavarnir sem fela í sér eflingu netöryggissveitarinnar, CERT-ÍS.
- Netöryggissveit verður flutt frá Póst- og fjarskiptastofnun til ríkislögreglustjóra skv. drögunum.
- Unnt er að senda ráðuneytinu umsögn um frumvarpsdrögin til og með 21. október 2015.

Að lokum

Kröfur til öryggis opinberra vefja fara vaxandi

Fræðsluefni á vefnum ut.is