ÖRYGGISKRÖFUR SEM GERÐAR ERU TIL SKJALAVEITNA VEGNA SAMSKIPTA VIÐ PÓSTHÓLF

Í þessum gátlista má finna atriði sem vefþjónusta skjalaveitna (SkjalaveitaAPI) þarf að uppfylla áður en tenging við Pósthólf Ísland.is getur átt sér stað. Nánar um útfærslu á þjónustu skjalaveitna má sjá hér.

Tilgangurinn með gátlistanum er að koma í veg fyrir mögulegar öryggisholur þegar vefþjónustur eru útfærðar af skjalaveitum.

GÁTLISTI

1. Flutningslag

Öll samskipti eiga að vera dulkóðuð, notast þar við https (TLS 1.2 +). Skilríki á vefþjón ættu að vera útgefin af vottuðum skilríkja-útgefanda (ekki self signed).

☐ Samskipti eru dulkóðuð á þjóni sem styður TLS 1.2+.

☐ Skilríki á þjóni eru útgefin af vottuðum skilríkja-útgefanda.

2. Hýsingarumhverfi

Hýsa skal vefþjónustu skjalaveitna í eins öruggu hýsingarumhverfi og mögulegt er. Leitast skal við að hýsa ekki vefþjónustu skjalaveitna í Samhýstu umhverfi.

☐ Aðrir vefir eða vefþjónustur skulu ekki vera hýstar á vefþjón vefþjónustu skjalaveitna

3. Auðkenning

Vefþjónusta ætti að vera útfærð með skilríkja auðkenningu á samskiptalagi (krefjast client certificate auðkenningar). Þjónustan ætti ekki að vera aðgengileg með öðrum hætti.

☐ Vefþjónustan er einungis aðgengileg með skilríkjaauðkenningu.

4. Skilríkjatraust

Í raunumhverfi skjalaveitu ætti einungis að treysta skilríki sem Ísland.is notar til auðkenningar í raunumhverfi Pósthólfsins. Prófunarumhverfi Pósthólfsins notast við annað skilríki sem ætti aldrei að vera treyst í raunumhverfi.

☐ Raunumhverfi treystir einungis skilríkjum raunumhverfið Pósthólfsins á Ísland.is

5. Aðgangstakmarkanir

Vefþjónustan ætti einungis að vera lokuð á netlagi. Þ.e. hún ætti einungis að vera aðgengileg þeim IP tölum sem Pósthólfið á ísland.is notar þegar kallað er í þjónustuna.

☐ Vefþjónustan er einungis aðgengileg IP tölum sem Pósthólfið á ísland.is notar.

6. Sannreyna inntaksform

Inntak ætti að sannreyna með tilliti til innspýtingar (e. Injection) ásamt því að tryggja rétt snið (e. format).

☐ Vefþjónustan skilar villu ef inntak er tómt (þ.e. annað hvort kennitala eða skjalId er tómt).

☐ Vefþjónustan skilar villu ef kennitala er ekki á réttu sniði.

☐ Vefþjónustan skilar villu ef einkenni skjals (skjalId) er ekki á réttu sniði. Sniðið má ekki vera "giskanlegt" t.d. stigvaxandi tala..

☐ Vefþjónustan er varin fyrir innspýtingu (e. Injection).
https://www.owasp.org/index.php/Top_10-2017_A1-Injection

7. Sannreyna inntaksgögn

Þegar Pósthólfið á Ísland.is sækir skjöl frá skjalaveitum er sent par af kennitölu og einkenni skjal (SkjalId). Skjalaveitan ætti alltaf að sannreyna að skjalið sem vísað er í (skjalId) sé í eigu gefinnar kennitölu. M.ö.o. er skjalinu ekki skilað eingöngu út frá gefnu einkenni skjals (skjalId).

☐ Vefþjónustan ber saman kennitölu og einkenni skjals áður en skjali er skilað.

8. Atburðarskráning

Þegar kallað er í þjónustuna ætti skrá öll köll í atburðarskráningu. Þar ætti að koma fram kennitala og einkenni skjals sem var sótt (eða reynt að sækja).

☐ Aðgerðir eru skráðar í atburðarskráningu.

Þessi gátlisti var unnin af Advania og yfirfarinn af Syndis. Eigandi þjónustu er Verkefnastofa um stafrænt Ísland, Fjármála -og efnahagsráðuneytið.