SYNDIS
Creative[in]Security

ÞJÓÐSKRÁ ÍSLANDS
REGISTERS ICELAND

Minnisblað v. rafrænnar kjörskrár

1. September 2020

Inngangur

Syndis var beðið um álit á hugsanlegum áhættum fólgnum í innleiðingu á rafrænni kjörskrá. Kjörskráin segir til um hverjir hafa rétt til þess að taka þátt í kosningum, þ.e. hverjir hafa kosningarrétt á kjördag. Þegar kjósandi hefur fengið afhentan kjörseðilinn er merkt við hann í kjörskrá og mun þar af leiðandi leysa af hólmi þær bækur sem notaðar hafa verið í sama tilgangi.

Með rafrænni kjörskrá þarf að hafa í huga öryggi kerfisins, bæði við framkvæmd kosninga og varðveislu ganga. Huga þarf að því að engin komist inn í kerfið eða gögn þess. Tryggja þarf með öllum tiltækum ráðum að gera kerfið eins öruggt og hægt er hverju sinni. Æskilegt er að við hönnun á innviðum kerfisins að flétta inn net- og upplýsingaöryggi og fylgja verkefninu frá upphafi til leiðarenda.

Allt ferli rafrænna gagna er mjög ólíkt gögnum á pappír. Ef átt er við rafræn gögn er mjög erfitt, ef ekki ómögulegt, að komast að því hver var að verki enda gögnin aðgengileg úr mörgum áttum. Þetta er ólíkt, t.d. skráningarbókum kjörskrár þar sem viðkomandi þarf að hafa raunverulegan aðgang að bókinni til að geta átt við gögnin í henni.

1. Útstöðvar

Mikilvægt er að þær útstöðvar sem verða notaðar á kjörstöðum séu með þekkta uppsetningu, ekki er ráðlegt að nota tölvur sem hafa verið í notkun annars staðar þar sem hætta er á að þær hafa að geyma óværur. Tvær leiðir væru líklegast færar í þessum efnum, ein leið sem hægt væri að skoða er að nota sýndarumhverfi þar sem útstöðvar, sem nú þegar eru á kjörstað, eru notaðar til að fá aðgang að sýndarvélum, á lokuðu neti, sem hafa svo aðgang að kjörskránni. Önnur leið væri að úthluta tölvum með þekkta og örugga uppsetningu á kjörstaði. Samhliða þessu eru mikilvægt að eingöngu sú virkni sem notuð er sé aðgengileg og að öll virkni stýrikerfis og/eða vafra sé takmörkuð til að lágmarka líkur á misnotkun útstöðvar.

Syndis mælir með að skoða gaumgæfilega möguleikann á að nota sýndarvélar á lokuðu neti á þann hátt að tölvur á kjörstöðum tengjast sýndarumhverfi og þannig fæst aðgangur að kjörskrá.

2. Vandamál með tenginu

Til að tryggja rekstraröryggi kerfisins, þá er lykilatriði að Internettenging sé stöðug. Ef tengingin verður óvirk, þá verður að vera varaleið, t.d. 4/5G tenging. Líkurnar á að Internet tenging með kapli og 4/5G tenging verði óvirkar á sama tíma verða að teljast harla ólíklegar, en áhættan er til staðar t.d. rafmagnsleysi. Mælt er með að hafa til reiðu viðbragðsáætlun sem grípa skal í skyldi slíkt gerast.

Samþykkja þarf áhættuna á að rafmagnsleysi gæti átt sér stað.

3. Atburðaskráning

Mikilvægt er að geta rakið aðgerðir allra aðila og hverjir voru að störfum á hvaða tíma. Þetta gerir þá kröfu til þeirra sem vinna á kjörstöðum að þurfa að tengjast með eigin auðkenni, rafræn skilríki ættu að vera skylda. Hættan er alltaf sú að þegar að starfsmaður á kjörstað yfirgefur vinnustöð sína, t.d. í matarhléi, og gleymir að skrá sig út og að annar starfsmaður geti þá framkvæmt aðgerðir í nafni þess sem áður hafði skráð sig inn.

Gera má ráð fyrir að starfsmaður gleymi að skrá sig út þegar að útstöðin er yfirgefin, meta þarf þessa hættu miðað við þá hættu sem er við núverandi fyrirkomulag.

4. Rekstur og aðgangur

Ef um er að ræða miðlægan gagnagrunn, þá er alltaf einhver sem hefur aðgang að öllum gögnum á meðan að kjörskráin er til. Mikilvægt er að takmarka þetta aðgengi og hafa ítarlegar skráningar á öllum atburðum. Það eru alltaf líkur á að tenging við þetta mikilvæga kerfi gæti rofnað, hugsanlega einhverjir sem gera álagsárás til að trufla kosningar eða önnur tæknileg vandamál. Viðbragðsáætlun skal vera til fyrir slíka atburði.

Lagt er til að vera með tvöfalda auðkenningu þannig að tveir aðilar þurfa að samþykkja aðgengi að viðkvæmum gögnum.

5. Hugbúnaðar- og netöryggi

Allur hugbúnaður getur innihaldið tæknilega öryggisveikleika og er gríðarlega mikilvægt að þróun kerfis sé í takt við eðlilegar kröfur. Fyrir vefkerfi mælum við með OWASP sem viðmið, þá bæði er varðar þróun og prófanir á kerfinu. Að sama skapi þurfa reglur um stöðugar öryggisuppfærslur að vera til staðar og mælst er til þess að eftirlit sé viðhaft til að tryggja slíkt. Æskilegt er að hafa öryggi að leiðarljósi frá hönnun til vöru, þetta er hægt að gera með því að framkvæma kóðarýni á þróunarferlinu. Þegar kerfið er á lokastigi er mælt með því að framkvæmd sé sértæk, tæknileg öryggisúttekt á bæði hugbúnaðar- og netöryggi áður en kerfið fer í notkun. Gera má ráð fyrir um 10-15 tíma vinnu á mánuði í öryggisráðgjöf á meðan kerfið er hannað og þróað og síðan gæti gróft mat verið um 120 tímar á sértækri tæknilegri úttekt á hugbúnaðarlausninni og netöryggi.