30.11.2016

Leiðbeiningar um gerð áhættumats og öryggisráðstafanir

Markmið

Markmið áhættumats er að skapa forsendur fyrir vali á öryggisráðstöfunum. Fyrst eru upplýsingaeignir viðkomandi skipulagsheildar/stofnunar/sveitarfélags kortlagðar. Síðan eru áhættuþættir kortlagðir og í framhaldi af því er hægt að bregðast við þeim með viðeigandi hætti, með því að gera ýmsar öryggisráðstafanir.

Mikilvægt er að þeir sem koma að því að kortleggja upplýsingaeignir hafi reynslu og skilning á rekstri viðkomandi skipulagsheildar.

Einnig er mikilvægt að þeir sem koma að sjálfu áhættumatinu við að meta ógnir, líkur og áhrif, hafi reynslu og skilning á viðkomandi rekstri.

Þegar skipulagsheild vinnur persónuupplýsingar s.s. um viðskiptavini, starfsmenn, birgja eða aðra í samræmi við lög nr. 77/2000, um persónuvernd og meðferð persónuupplýsinga, ber að skjalfesta upplýsingaöryggi, þ.m.t. framkvæma áhættumat, í samræmi við reglur nr. 299/2001, um öryggi persónuupplýsinga.

Kortlagning eigna / upplýsingaeigna

Fyrsta skrefið við framkvæmd áhættumats er að kortleggja helstu eignir sem skipta máli fyrir rekstur viðkomandi rekstrareiningar. Hér þarf að hafa í huga að við þurfum ekki að kortleggja fjölda skrifborða, stóla, penna, blýanta eða annarra hluta, nema að við gerum ráð fyrir því að það kunni að hafa áhrif á rekstur eða verndun viðkvæmra upplýsinga.

Fyrir hverja eign þarf að skjala eftirfarandi þætti:

- Nafn á upplýsingaeign
- Lýsing á upplýsingaeign
- Eigandi upplýsingaeignar
- Ábyrgðaraðili upplýsingaeignar

Athugið að hægt er að draga saman fjölda eigna í einn eignaflokk. Þannig að í staðinn fyrir að vera með 10 vefmiðlara skráða hvern á fætur öðrum þá væri hægt að skrá eina eign “Vefmiðlarar” og láta fjölda vefmiðlara fylgja með í lýsingu fyrir umrædda eign.

Æskilegt er að miða við að 5 til 25 mikilvægustu upplýsingaeignirnar / eignaflokkarnir séu teknir saman í fyrsta áhættumati.

Áhættumat

Fyrir hverja upplýsingaeign viljum við kortleggja helstu ógnir/hættur sem steðja að hverri eign fyrir sig, m.a. athuga umfang og afleiðingar ógnarinnar/hættunnar með tilliti til sérhverrar upplýsingaeignar fyrir sig auk þess að minnast á veikleika sem varða viðkomandi eign, t.d. með því að tilgreina hvað geti farið úrskeiðis, hvaða áhrif slíkt geti haft á öryggi og hvaða líkur séu á slíku.

Dæmi:

Eign: Vefmiðlari
Ógn: Einhver gæti brotist inn á vefmiðlarann.
Veikleiki: Öryggisuppfærslur hafa ekki verið settar upp á vefmiðlaranum í fjóra mánuði vegna veikinda.

Eign: Skrifstofuhúsnæði
Ógn: Einhver gæti brotist inn í skrifstofuhúsnæðið.
Veikleiki: Pumpan á hurðinni í bílageymslunni er biluð og lokast ekki alveg sjálfkrafa, því gæti síðasti maður gleymt að loka hurðinni almennilega og óprúttinn aðili gæti komist þannig inn.

Líkur

Fyrir hverja ógn þurfum við að meta líkur á því að hún eigi sér stað/öryggisatvik eigi sér stað. Í okkar tilfelli þá munum við nota skalann 1 til 5:
1 – Sjaldnar en einu sinni á ári.
2 – Einu sinni á ári.
3 – Einu sinni í mánuði.
4 – Einu sinni í viku.
5 – Einu sinni eða oftar á dag.

Áhrif

Fyrir hverja ógn þá metum við einnig möguleg áhrif hennar(öryggisatviksins) á rekstur skipulagsheildarinnar. Við munum einnig nota skalann 1 til 5.
1 – Engin áhrif á rekstraröryggi.
2 – Lítil áhrif á rekstraröryggi.
3 – Einhver áhrif á rekstraröryggi.
4 – Mikil áhrif á rekstraröryggi.
5 – Gífurlega mikil áhrif á rekstraröryggi. Gæti leitt til rekstrarstöðvunar.

Áhætta

Áhætta er í kjölfarið reiknuð út með því að margfalda líkur á því að ógn eigi sér stað (öryggisatvik eigi sér stað) með viðeigandi áhrifum. Þannig fáum við „áhættustuðul“ á bilinu 1 til 25, þar sem 1 er lægsta mögulega áhætta og 25 er hæsta mögulega áhætta.

Öryggisáhætta = Líkur á ógn x Áhrif ógnar

- Ásættanleg áhætta er á bilinu 1 til og með 3.
- Miðlungs áhætta er á bilinu 4 til og með 9.
- Mikil áhætta er á bilinu 10 til og með 25.

	Áhrif				
Líkur	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Öryggisráðstafanir

Eftir að búið er að framkvæma áhættumat þá þarf að bregðast við þeim áhættum sem finnast og eru utan ásættanlegra marka skipulagsheildarinnar. Hægt er að bregðast við áhættu á ferna vegu:

1. Hægt er að innleiða öryggisráðstafanir.
2. Hægt er að færa áhættu til (t.d. með því að kaupa tryggingar).
3. Hægt er að forðast og/eða útiloka áhættu.
4. Hægt er að sætta sig við áhættu af ásetningi.

Ef unnið er að áhættumati vegna vinnslu persónuupplýsinga ber ábyrgðaraðila að setja fram skriflega lýsingu á öryggisráðstöfunum sbr. 3. tölul. 3. gr. reglna nr. 299/2001, um öryggi persónuupplýsinga. Öryggisráðstafanir skal endurskoða reglulega.

Viðbrögð við mikilli áhættu

Ábyrgðaraðili eignar ber ábyrgð á að bregðast við þeim ógnum sem tengjast viðkomandi upplýsingaeign með viðunandi hætti. Mikilvægt er að velja og grípa til öryggisráðstafana fyrir allar alvarlegar áhættur sem fyrst, þ.e.a.s. fyrir þær áhættur sem fá áhættustuðul á bilinu 13 til og með 25.

Áhættumeðferðaráætlun

Fyrir hverja áhættu þarf að skrá eftirfarandi þætti:

1. Áhættumeðferðaráætlun: Lýsir því hvort og þá hvernig bregðast skuli við áhættunni, t.d. með því að innleiða öryggisráðstafanir, kaupa tryggingar eða sætta sig við viðkomandi áhættu.
2. Áætluð lok: Lýsir því hvenær ráðgert sé að innleiða öryggisráðstöfun / ljúka áhættumeðferð.
3. Ábyrgðaraðili: Hver ber ábyrgð á að öryggisráðstafanir séu innleiddar.
4. Framkvæmdaraðili: Hver mun framkvæma öryggisráðstafanirnar.

Samþykki æðstu stjórnenda

Eftir að áhættumat hefur verið framkvæmt skal það kynnt æðstu stjórnendum til samþykkis. Mikilvægt er að samþykki þeirra sé veitt á formlegan og sannanlegan hátt s.s. með undirritun eða bókun í fundargerð.

Að sama skapi skal áhættumeðferðaráætlun kynnt æðstu stjórnendum til samþykkis. SLíkt samþykki skal einnig vera veitt á formlegan og sannanlegan hátt.