Leiðbeiningar við að nota eyðublöð fyrir áhættugreiningu

Inngangur

Áhættugreining snýst um að greina mögulegar ógnir, varnarleysi gagnvart ógnum og líkur á að ógnir eigi sér stað. Auk þess eru afleiðingar metnar með tilliti til hættu á missi trúnaðar, heilindum og aðgengis.

Eyðublöð og dæmi sem Samband íslenskra sveitarfélaga hefur fengið að láni frá KL í Danmörku fyrir vinnuna við áhættumat:

- Áhrifamat
    - Mat á áhrifum - eyðublað
    - Tegundir afleiðinga
- Varnarleysismat (líkindamat)
    - Mat á varnarleysi - eyðublað
    - Dæmi um ógnir
- Áhættuskrá

Sniðugt getur verið að prenta eyðublöðin eða hafa opin á tölvuskjá meðan leiðbeiningunum er fylgt eftir í þessu skjali.

Áður en hægt er að hefja áhættumatið þarf að skapa yfirsýn yfir mikilvæga viðskiptaferla, upplýsingakerfi og innviði sem taka þarf með í áhættumatinu. Þessir hlutir eru einnig kallaðir eignir. Auk þess að ákvarða eigendur eignanna þar sem þeir leggja sitt af mörkum við mat á áhrifum og varnarleysi.

Til dæmis:

Tegund	Eign	Eigandi
Ferli	Launagreiðsla	Fjármálastjóri
Viðskiptaferli	Opus	Fjármálastjóri
Viðskiptaferli	Tímaskráningakerfi	Mannauðsstjóri
stuðningskerfi	Netþjónar	Tæknideild
stuðningskerfi	Net	Tæknideild

Skýring hugtaka

- **Viðskiptaferli**
  Ferli sem hægt er að nota til að leysa kjarnaverkefni sveitarfélagsins . Mikilvægt viðskiptaferli getur verið ferli sem nauðsynlegt er fyrir sveitarfélagið til að uppfylla reglur. Til dæmis greiðslu á bótum í reiðufé.
- **Innviðir**
  Innviðir ná yfir tæknilega hluti sem er undirstaða upplýsingatækniþjónustu. Þetta geta verið netþjónar, spjaldtölvur, tölvur, net osfrv.
- **Eign**
  Notað fyrir meðal annars viðskiptaferla, upplýsingakerfi, netþjóna, netkerfi, tölvur o.s.frv.
- **Áhrifamat**
  Lýsir áhrifum trúnaðarmissis, heilindum eða aðgengis sem getur haft á sveitarfélagið og íbúa.
- **Tegundir afleiðinga**
  Brot á trúnaði, heilindum eða aðgengi getur haft mismunandi afleiðingar. Sumar tegundir geta haft áhrif á líf, heiður og velferð, aðrar á orðspor/traust sveitarfélagsins o.s.frv. Sveitarfélagið ákveður sjálft hvers konar afleiðingar það vill leggja mat á.
- **Varnarleysismat**
  Veitir yfirsýn yfir varnarleysi eigna sem eykur líkur á ógnum. Einnig oft kallað líkindamat.
- **Trúnaður**
  Þegar óviðkomandi aðilar hafa aðgang að gögnum sem þeir ættu ekki að hafa aðgang að.
- **Heilindi**
  Segir til um hvort hægt sé að treysta á gögn, þ.e. að gögnin sem eru til dæmis í kerfi séu þau réttu og að það sé óhætt að taka ákvarðanir út frá því.
- **Aðgengi**
  Hvort kerfi og gögn séu ávalt aðgengileg.
- **Áhættuskrá**
  Notað til að skrásetja áhættur sem og aðgerðir/ráðstafanir til að draga úr áhættunni.
- **Áhættugildi**
  Áhættugildið er fundið með því að margfalda afleiðinguna (út frá áhrifamati) með líkunum á að varnarleysi vegna ógnar eigi sér stað (varnarleysismat).

Áhrifamat

Áhrifamat veitir yfirsýn yfir viðskiptalegar afleiðingar ef brotið er á trúnaði, heilindum eða aðgengi. Ekki er hægt að framkvæma matið án þátttöku eiganda viðskiptaferlisins.

Excel skjalið Áhrifamat.xlsx inniheldur eyðublað fyrir mat á áhrifum og dæmi um tegundir áhrifa.

Mat á áhrifum - eyðublað

Eyðublaðið er notað til að skrá afleiðingar brots á **t**rúnaði, **h**eilindum og **a**ðgengi (THA) fyrir viðskiptaferli (eign). Afleiðingarnar eru metnar með hliðsjón af flipanum „Tegundir afleiðinga“ í Excel skjalinu.

Að auki kemur fram hvaða persónuupplýsingar ferlið notar og hvaða aðrar eignir (t.d. upplýsingakerfi). Þær eignir eru síðar teknar með í varnarleysismatinu.

Tegundir afleiðinga

Sniðmátið inniheldur dæmi um tegundir afleiðinga. Til dæmis, hvaða áhrif mun brot á trúnaði, heilindum eða aðgengi hafa á líf, heiður og velferð, á orðspor/traust o.s.frv. Hægt er að aðlaga blaðið í samræmi við þær afleiðingar sem sveitarfélagið vill leggja mat á áhrif vegna.

Varnarleysismat

Varnarleysismatið sýnir yfirlit yfir veikleika eigna eða stjórnunar sem gæti orðið fyrir einni eða fleiri ógnum. Varnarleysi er ekki hættulegt í sjálfu sér, fyrr en það verður fyrir ógn.
Varnarleysismatið er hægt að framkvæma með viðtölum/vinnustofum með fagfólki, kerfiseigendum og upplýsingatæknideild.

Dæmi um ógnir

Áður en varnarleysismatið hefst þarf sveitarfélagið að hafa byggt upp þá ógnakrá sem það vill nota til að meta veikleika í tengslum við.
Fyrir þessa notkun er að finna hugmyndir um ógnir í flipanum „Dæmi um ógnir“ í Excel skjalinu Varnarleysismat.xlsx.

Mat á varnarleysi - eyðublað

Eyðublaðið fyrir varnarleysismatið er notað til að meta varnarleysi eigna (t.d. upplýsingakerfa).

Varnarleysismat á eignum ætti að vera gert í tengslum við áhrifamatið. Sveitarfélagið setur inn í eyðublaðið þær ógnir sem er kosið að leggja mat á. Við mat á líkum á að ógn geti orðið á veikleika skal hafa eftirfarandi í huga:

- Hversu líklegt er að ógnin muni gerast? Í fyrsta lagi ætti að leggja mikla áherslu á söguleg gögn – hvaða ógnir hafa raunverulega komið fram í formi öryggisatvika? Hefur sveitarfélagið orðið fyrir tölvuþrjótaárás, vefveiðum(e. phishing) eða hefur verið krafist lausnargjalds (e. ransomware), þjófnaði á persónuupplýsingum, sendingu persónuupplýsinga til rangs viðtakanda eða hafa starfsmenn hlaðið upp persónuupplýsingum í einkaskýjaþjónustu?
- Hversu vel hefur sveitarfélagið innleitt aðgerðir til að verjast ógninni? Öryggisráðstafanir hafa vissulega þegar verið gerðar sem draga úr áhrifum í tengslum við sumar af þeim ógnum sem taldar eru upp í ógnarskránni. Til dæmis ógnir vegna netþjóna, netkerfi, biðlara o.s.frv. hefur yfirleitt verið áhættumetin og meðhöndluð af upplýsingatæknideild. Tilgreina þarf fyrirliggjandi öryggisráðstafanir ásamt framlagi þeirra til að draga úr líkum og afleiðingum.

Eyðublaðið inniheldur þrjá dálka sem hægt er að nota til að ákvarða hvort ógnin geti haft áhrif á trúnað, heilindi og aðgengi. Þetta er aðeins ætlað til að auðvelda mat á varnarleysi.

Fyrir hverja ógn eru metnar líkurnar á því að eignin (upplýsingakerfið) verði fyrir barðinu á ógninni. Ef líkurnar á ógn eru miklar á meðan afleiðing brots er mikil verður að flytja ógnina í áhættuskrána. Þetta er merkt í dálknum 'Meðhöndlun'.

Áhættuskrá

Excel skjalið Áhættuskrá.xlsx er notað til að skrásetja áhættur sem og aðgerðir/ráðstafanir til að draga úr áhættunni.
Sniðmátinu er ætlað að skrásetja áhættu í hverju ferli.

Þegar hingað er komið ætti að vera búið að meta afleiðingar brota á trúnaði, heilindum og aðgengi í ferli í áhrifamatinu, og varnarleysi eigna (upplýsingakerfa) sem ferlið notar í varnarleysismatinu.

Áhættugildið er fundið með því að margfalda afleiðingarnar (út frá áhrifamati) með líkum á að varnarleysi verði (varnarleysismat). Sjá mynd með áhættugildum hér að neðan.
Til dæmis, ef stjórnendur sveitarfélagsins hafa ákveðið að samþykkja áhættugildi allt upp að og með 8, þyrfti að færa ógnir (frá varnarleysismatinu) með líkurnar 3 (líklegt) eða 4 (mjög líklegt) inn í áhættuskrá ef afleiðing brots (frá áhrifamati) er samtímis metin 3 (mjög alvarlegt) eða 4 (alvarlegt/ósættanlegt).

Stjórnendur geta einnig valið að setja ógnir í áhættuskrána með t.d. 8 í áhættugildi ef þarf að leggja áherslu á þær. Til dæmis getur þetta verið áhætta þar sem minni líkur eru á að eignin verði fyrir áhrifum af ógninni, en gæti aftur á móti haft alvarlegar/ósættanlegar afleiðingar.

Líkur	**Áhættugildi**			
4. Mjög líklegt	4	8	12	16
3. Líklegt	3	6	9	12
2. Litlar líkur	2	4	6	8
1. Ólíklegt	1	2	3	4
Afleiðing	1. Óveruleg	2. Minna alvarleg	3. Mjög alvarleg	4. Alvarleg

Fyrir hverja eign (upplýsingakerfi) þarf að skrá inn eftirfarandi í áhættuskrána:

- Sérhver ógn sem hefur hærra áhættugildi en það sem stjórnendur hafa ákveðið að sé ásættanlegt.
- Hugsanlegt varnarleysi sem getur orðið fyrir ógn - er skortur á öryggisráðstöfunum eða eftirliti?
- Áhrif (tegundir afleiðinga) frá áhrifamati.
- Afleiðing frá áhrifamati.
- Líkur úr varnarleysismati.
- Aðgerð/ráðstöfun til að draga úr áhættu.
- Nafn eiganda áhættunnar sem getur brugðist við.
- Fjárhagslegar afleiðingar ef áhættan á sér stað. Til dæmis getur það haft fjárhagslegar afleiðingar ef um stórar tölvuþrjótaárásir er að ræða.
- Sent inn/flutt í. Til dæmis getur það verið fyrir ytri lánadrottinn.
- Meðhöndlun
  1. Samþykkja (áhættan er samþykkt og ekki er gripið til frekari aðgerða). Hægt er að taka áhættuna ef kostnaður við að draga úr henni er meiri en afleiðingin.
  2. Færa (áhætta er flutt til þriðja aðila, t.d. ytri birgja).

3. Forðast (forðast áhættuna með því að stöðva eða breyta starfseminni sem veldur áhættunni). Hægt er að velja að forðast áhættuna ef áhættan er of mikil og viðeigandi eftirlitsráðstafanir finnast ekki.
4. Stýra (áhættunni er stjórnað með því að innleiða aðgerðir sem fjarlægja eða draga úr líkum eða afleiðingum).

Byggt á ofangreindu er nú hægt að lýsa afgangs áhættunni:

- Afleiðingar brots eftir að ráðstafanir hafa verið innleiddar.
- Líkur á brotum eftir að ráðstafanir hafa verið innleiddar.
- Niðurstaða - er afgangsáhættan ásættanleg og samþykkt af stjórnendum?