



Ólafur Róbert Rafnsson

Stjórnkerfi upplýsingaöryggis

Hvernig göngum við um mikilvægar upplýsingar?

Við dagleg störf höfum við aðgang að miklu magni upplýsinga. Við erum áreitt með upplýsingum sem til okkar streyma og eigum auðvelt með að taka saman rafræn gögn og senda frá okkur, til dæmis skjöl viðhengd tölvupósti. Við þessar aðstæður er auðvelt að miðla röngum upplýsingum eða gera mistök og senda skjöl sem ætluð voru öðrum en viðtakanda, svo dæmi séu tekin. Einnig er nauðsynlegt að verja upplýsingar fyrir utanaðkomandi aðilum enda geta brot á upplýsingaöryggi valdið miklum fjárhagslegum skaða eða öðru tjóni. Þannig er mat á orðsporsáhættu gjarnan nátengt mati á öryggi þeirra upplýsinga sem liggja hjá viðkomandi aðila. Við þessar aðstæður hafa þróast sífellt skýrari kröfur um gegnsæi, skýra ferla og ábyrgð. Þær eru settar fram af aðilum sem hafa hagsmuna að gæta varðandi ábyrga meðferð upplýsinga, svo sem stjórnendum viðkomandi fyrirtækja eða stofnana, viðskiptavinum, samtarfs- eða eftirlitsaðilum. Kaupendur vöru og þjónusta setja í auknum mæli skilyrði í útboðum að bjóðendur séu með stjórnkerfi vottuð af óháðum aðila ef

gera á tilboð í verk. Einnig eru dæmi um að ríkisstjórnir séu farnar að setja það í stefnuskrá hjá sér að stofnanir hafi vottuð stjórnkerfi til þess að auka trúverðuleika þeirra.

Stjórnkerfi fyrir upplýsingaöryggi

Í þessari grein er fjallað um stjórnkerfi upplýsingaöryggis sem snýst í raun um hvernig fyrirtæki og stofnanir koma sér upp skipulögðum vinnubrögðum við umgengni um mikilvægar upplýsingar. Alþjóðlega staðlastofnunin ISO hefur þróað staðla fyrir helstu stjórnkerfi sem í notkun eru hjá fyrirtækjum og stofnunum, þeirra á meðal staðalinn ISO 27001 Stjórnkerfi fyrir upplýsingaöryggi. Sem dæmi um aðra þekktu ISO staðla má nefna ISO 9001:2008 Gæðastjórnunarkerfi og ISO 14001 Umhverfisstjórnunarkerfi.

Stjórnkerfi fyrir upplýsingaöryggi hafa víða verið innleidd hjá íslenskum fyrirtækjum. Fjármálaeftirlitið gerir kröfur um að fjármála-fyrirtæki innleiði verklag hjá sér sem byggir á leiðbeinandi tilmælum um rekstur upplýsingakerfa, en þær kröfur byggja á ISO 27001. Samskipti við FME og Persónuvernd

eru auðveldari hjá fyrirtækjum sem eru með vottað stjórnkerfi. Ýmis tæknifyrirtæki sækjast til dæmis eftir vottun til að auka samkeppnisstöðu sína jafnt hérlendis sem erlendis. Vottað stjórnkerfi auðveldar einnig fjármálastofnunum og fyrirtækjum þar sem lánshæfi er metið af Standard & Poors. Aðferðafræði Capacent við áhættugreiningu er einn af hornsteinum Stjórnkerfis upplýsingaöryggis og hefur mælst vel fyrir hjá Standard & Poors.

Vel skipulagt stjórnkerfi:

- Auðveldar fyrirtækinu að koma auga á veikleika í kerfum eða ferlum.
- Gerir stjórnendum kleift að hafa betri yfirsýn yfir rekstur upplýsingakerfa og öryggismála.
- Eykur öryggismeðvitund.
- Eflir skilvirkni á skjölun á helstu kerfum og verklagi og þar með aukið rekstraröryggi.

Því miður eru fjölmörg dæmi þess að innleiðing á Stjórnkerfi upplýsingaöryggis hefur haft þær afleiðingar að hægja mikið á ferlum og rekstrarkostnaður getur hækkað verulega. Í tilfelli þjónustufyrirtækja getur slíkt birtist í lakari þjónustu við viðskiptavininn auk þess að hann gæti þurft að greiða hærra verð.

Það er lítill ávinningur af því að vera með dýrt stjórnkerfi sem veldur því að viðskiptavinir hafa ekki ráð á að kaupa þjónustu fyrirtækisins. Við innleiðingu á Stjórnkerfi upplýsingaöryggis er markmiðið að skerpa verklag við rekstur með betri skjölun, bæta öryggi almennt og lágmarka áhættu, jafnt í rekstri sem þjónustu.

Í grunninn byggja öll stjórnkerfi á sömu grunnkröfum, að skipulagi sé komið á kerfið, haldið sé utan um skjöl og skrár, rekjanleiki sé til staðar, kerfið sé reglulega tekið út, ábyrgðir og hlutverk séu skýr og unnið sé að stöðugum umbótum á kerfinu. Nánari nálgun á einstök stjórnkerfi fer eftir því með hvaða gleraugum við viljum skoða fyrirtækið eða stofnunina. Viljum við einbeita okkur að upplýsingaörygginu, umhverfinu, gæðunum eða einhverju öðru. Hvernig á að gera þetta? Í grunninn byggist Stjórnkerfi upplýsingaöryggis á þrem megin þáttum sem eru:



- » Leynd (Confidentiality)
Koma í veg fyrir að gögn birtist í heimildarleysi hvort sem er fyrir mistök eða af ásetningi
- » Réttleiki (Integrity)
Koma í veg fyrir óleyfilegar breytingar á gögnum
- » Tiltækileiki (Availability)
Tryggir öruggan og skilvísan aðgang að gögnum

Leið sem líkleg er til árangurs gæti verið í eftirtalinni röð;

1. Ákvörðun tekin um innleiðingu staðalsins
2. Ábyrgð stjórnenda skilgreind og verkefnisstjóri tilnefndur
3. Öryggisstefna útfærð (fyrsta útgáfa)
4. Umfang stjórnkerfisins skilgreint
5. Áhættugreining
6. Ákveðið með hvaða hætti skuli meðhöndla áhættu
7. Velja ráðstafanir úr staðlinum til að lágmarka áhættu
8. Innleiða ráðstafanir / nýtt verklag
9. Útbúa stöðumatskýrslu / yfirlit yfir hvaða kröfur stjórnkerfið uppfyllir
10. Ákvörðun um vottun

Oft hefjast innleiðingar á Stjórnkerfi upplýsingaöryggis á því að útbúin er öryggisstefna og útfra henni eru einstök verkefni skilgreind. Mikilvægt er að hafa í huga að hægt er að velja leið sem hentar flestum fyrirtækjum og tekur til helstu reglna og krafna sem fyrirtækið ætlar að uppfylla þó markmiðið sé ekki að votta stjórnkerfið. Einnig eru fyrirtæki mjög ólík og sumar kröfur þar af leiðandi óþarfar.

Vinnu við uppbyggingu stjórnkerfis má skipta í fjóra fasa: Skipuleggja – Framkvæma – Gáta – Aðhafast.

Skipuleggja

Þegar búið er að skilgreina kröfur og væntingar fyrirtækisins varðandi innleiðingu á Stjórnkerfi upplýsingaöryggis er næsta skref að skipuleggja með hvaða hætti skuli koma því upp. Í því felast markmið, ferlar og verklagsreglur sem máli skipta við stjórnun áhættu. Umbætur á upplýsingaöryggi almennt sem ætlað er til þess að skila fyrirtækinu árangri sem samræmist stefnu þess og markmiðum.

Framkvæma

Eftir að búið er að skilgreina helstu reglur og stefnur er komið að því að innleiða þær og starfrækja. Skýrar reglur þurfa að gilda um það með hvaða hætti veittur er aðgangur að húsnæði og kerfum fyrirtækisins svo dæmi sé tekið. Lögð er áhersla á að fella verklag sem miðar að því að halda til haga með hvaða hætti aðgangur er veittur inn í þá ferla sem fyrir eru til að tryggja rekjanleika og flýta fyrir verklagi sem eykur öryggi. Ekki síður er mikilvægt að vera með vel skilgreint verklag þegar loka þarf fyrir aðgang sem er því miður oftast en ekki látið mæta afgangi. Gríðalega mikilvægt getur verið að tryggja að einungis þeir aðilar hafi aðgang að upplýsingakerfum og aðstöðu fyrirtækisins sem þurfi þess nauðsynlega starfs síns vegna.

Gáta

Mikilvægt er að meta hvort breytt verklag við veitingu aðgangs og frágangs skili tilætluðum árangri. Stjórnendur ættu að fá niðurstöður til að rýna hvort breytingar á tilteknu verklagi hafi skilað árangri. Þessi hluti miðar almennt að því að vakta og rýna stjórnkerfið.

Aðhafast

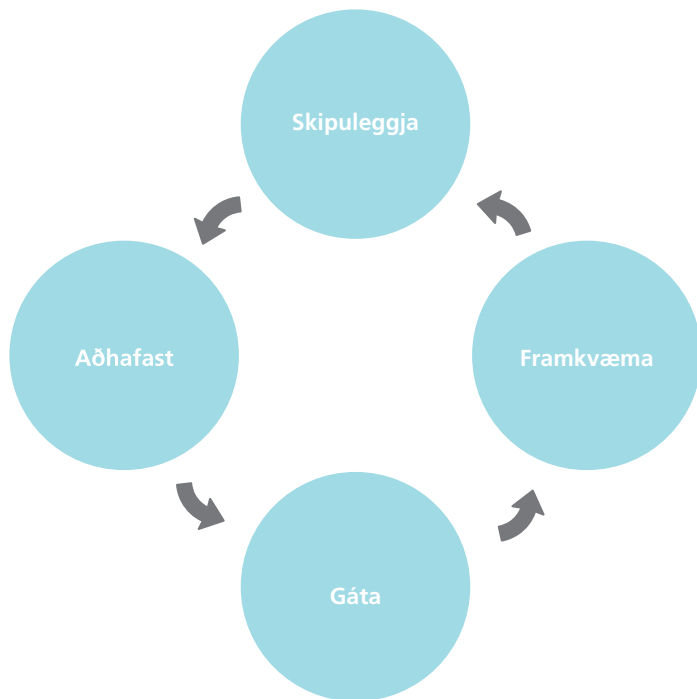
Þegar niðurstöður úr rýni tiltekins verklags eins og þess sem getið er hér að ofan liggja fyrir er líklegt að gera þurfi úrbætur á því. Það þarf stöðugt að gera úrbætur sem byggja á niðurstöðum úttekta á stjórnkerfinu og það má ekki gera ráð fyrir því að allt verklag, stefnur, skjölun o.s.frv. verði komið í endanlegt horf strax í fyrstu tilraun. Gera verður ráð fyrir því frá upphafi að innleiðing á breyttu verklagi þurfi að endurskoða reglulega með það að markmiði að það samræmist stefnu fyrirtækisins og skili tilætluðum árangri.

Aðferðafræði PDCA módel

Þessi aðferðafræði byggist á módelinu PDCA eða Plan Do Check Act. Ítarlegar leiðbeiningar um þessa aðferð er að finna í ISO27003.

Virk þátttaka stjórnenda nauðsynleg

Oft hefjast innleiðingar á Stjórnkerfi upplýsingaöryggis á því að útbúin er öryggisstefna og útfrá henni eru einstök verkefni skilgreind. Mikilvægt er að hafa í huga að hægt er að velja leið sem hentar flestum fyrirtækjum og tekur til helstu reglna og krafna sem fyrirtækið ætlar að uppfylla þó markmiðið sé ekki að fá vottun á stjórnkerfinu. Einnig eru fyrirtæki mjög ólík og



sumar kröfur þ.a.l. óþarfar.

Að byggja upp stjórnkerfi er ekki gert á einni nóttu og þarfnast góðs undirbúnings. Gríðarlega mikilvægt er að æðstu stjórnendur beri ábyrgð á að innleiðingin sé markviss og árangursrík en það er best tryggt með virkri þáttöku þeirra við innleiðingu.

Innleiðing stjórnkerfisins varðar alla starfsmenn og tengda aðila sem veita fyrirtækinu þjónustu sem og viðskiptavinum. Markviss innleiðing ætti að auka öryggi upplýsinga viðskiptavina, starfsmanna og þjónustuaðila og þar með bæta ímynd fyrirtækisins. Einnig ætti hún að bæta starfsánægju og efla vitund viðskiptavina og starfsmanna á öryggismálum almennt.

Það eru til fjölmörg kerfi, tæki og tól sem ætluð eru til að bæta öryggi kerfa og starfsmanna en oft er besta vörnin vel upplýstur starfsmaður og góðir ferlar.

Ólafur Róbert Rafnsson er ráðgjafi í upplýsingatækni hjá Capacent. Sérsvið hans eru gagnavernd, upplýsingaöryggi og rekstur og stjórnun upplýsingakerfa. Ólafur er kerfisfræðingur frá Rafiðnaðarskólanum. Hann er með MCSE gráðu frá Microsoft og hefur auk þess lokið ýmsum námskeiðum á sviði öryggismála, SharePoint og í almennum rekstri. Ólafur hefur starfað hjá Capacent frá árinu 1998 og hefur gegnt starfi forstöðumanns upplýsingatæknimála KPMG, ráðgjafa í öryggismálum með áherslu á stjórnkerfi upplýsingaverndar (ISO27001), sem úthýstur öryggisstjóri hjá Tryggingamiðstöðinni 2006, framkvæmdastjóri hjá Capacent IT Services 2006-2008, CIO hjá Capacent International.