Rekstraröryggi upplýsingakerfa

Innra eftirlit

RÍKISENDURSKOÐUN

Október 1998

Efnisyfirlit

Inngangur

Verkefni Ríkisendurskoðunar felast yfirleitt í skoðun á liðnum tilvikum eða ástandi. Við fjárhagsendurskoðun vottar hún reikningsskil tiltekins tímabils en við stjórnsýsluendurskoðun kannar hún hvort gætt hafi verið hagkvæmni og skilvirkni við meðferð og nýtingu ríkisfjár. Önnur aðferðafræði og vandmeðfarnari felst í að nálgast viðfangsefnið áður en tjón hefur átt sér stað. Slík fyrirbyggjandi skoðun getur átt við í tilvikum eins og þegar um er að ræða vandamál tengd tölvuvinnslu ártalsins 2000. Að mati stofnunarinnar er ekki síður gagnlegt fyrir ríkisaðila að Ríkisendurskoðun nálgist viðfangsefni sín með slíkum hætti.

Tilgangur greinargerðar þessarar er sá að aðstoða forstöðumenn ríkisaðila við að efla þann hluta innra eftirlits sem snýr að upplýsingakerfum þeirra og draga þar með úr líkum á verulegri röskun á starfsemi ef rekstrartruflanir verða í kerfunum. Greinargerðin er tekin saman í framhaldi af greinargerð stofnunarinnar um ártalið 2000 sem kom út á síðasta ári. Í þeirri greinargerð voru ríkisaðilar hvattir til þess að leiðrétta kerfi sín áður en það yrði um seinan. Þar var einnig lögð áhersla á nauðsyn þess að gera neyðaráætlanir til þess að grípa til ef þær leiðréttingar sem gerðar væru dygðu ekki og til rekstrartruflana kæmi. Í greinargerðinni var ekki gerð ítarleg grein fyrir gerð neyðaráætlana og er þessari greinargerð því ætlað að bæta úr því.

Starfsemi ríkisaðila byggir nú að miklu leyti á notkun upplýsingakerfa. Oftast er ekki hægt eða óviðunandi að grípa til eldri vinnubragða ef truflanir verða í rekstri kerfanna. Slíkar truflanir geta haft veruleg áhrif á hæfni viðkomandi ríkisaðila til þess að sinna hlutverki sínu. Tölvuöryggismál teljast því ekki lengur einkamál tölvudeilda, heldur meðal brýnustu viðfangsefna forstöðumanna stofnana og fyrirtækja ríkisins.

Þó að hætta af völdum náttúruhamfara sé nokkur hér á landi eru hegðun starfsmanna og aðgangur óviðkomandi aðila að upplýsingakerfum ríkisaðila stærstu áhættuþættirnir með tilliti til rekstrartruflana. Ártalið 2000 verður og stór áhættuþáttur á næstu 14 mánuðum. Búast má við því að þeir ríkisaðilar, sem sjá ekki fyrir endann á leiðréttingum í kerfum sínum vegna þess, séu að verða of seinir til þess að leysa þau, án þess að til einhverra rekstrartruflana komi.

Með greinargerðinni vonast Ríkisendurskoðun til þess að vekja forstöðumenn til umhugsunar um mikilvægi upplýsingakerfa fyrir þann rekstur sem þeir veita forstöðu og þá ábyrgð sem á þeim hvílir við að tryggja öryggi þeirra. Einnig er greinargerðinni ætlað að auka skilning þeirra á helstu áhættuþáttum sem ógnað geta öryggi kerfanna. Lögð er áhersla á nauðsyn áhættumats, mótun öryggisstefnu, val á öryggisráðstöfunum og stöðugt endurmat öryggismála. Allir þessir þættir eru í raun liðir í því innra eftirliti sem Ríkisendurskoðun telur að til staðar ætti að vera hjá hverjum ríkisaðila.

Ríkisendurskoðun, 30. október 1998

Helstu niðurstöður

- **Afritataka tölvugagna**

  Langmikilvægasta atriðið til þess að tryggja rekstraröryggi upplýsingakerfa ríkisaðila er að ætíð séu til fullnægjandi afrit af gögnum og hugbúnaði. Nauðsynlegt er að setja skýrar verklagsreglur um afritatöku, meðferð, prófun, geymslu og eyðingu afrita.

- **Prófanir vegna ártalsins 2000**

  Hjá flestum ríkisaðilum er starfsemi í lágmarki í vikunni á milli jóla og nýjárs. Ríkisendurskoðun vill því benda á þann möguleika að ríkisaðilar noti þá viku í desember n.k. til þess að prófa hvort leiðréttingar sem þegar hafa verið gerðar á upplýsingakerfum vegna ártalsins 2000 virki eins og til er ætlast.

- **Hegðun starfsmanna**

  Í öryggismálum upplýsingakerfa þurfa ráðstafanir að beinast bæði að utanaðkomandi aðilum og starfsmönnum viðkomandi. Líklega er í mörgum tilvikum meira hugað að öryggisráðstöfunum sem koma eiga í veg fyrir aðgang utanaðkomandi að upplýsingakerfum en að hegðun eigin starfsmanna, en hún er ein af stærstu ógnunum við öryggi upplýsingakerfa.

- **Áhrif rekstrartruflana**

  Starfsemi ríkisaðila byggir nú að miklu leyti á notkun upplýsingakerfa. Oftast er ekki hægt eða óviðunandi að grípa til eldri vinnubragða ef truflanir verða í rekstri kerfanna. Slíkar truflanir geta haft veruleg áhrif á hæfni viðkomandi ríkisaðila til þess að sinna hlutverki sínu. Tölvuöryggismál teljast því ekki lengur einkamál tölvudeilda, heldur meðal brýnustu viðfangsefna forstöðumanna stofnana og fyrirtækja ríkisins.

- **Verðmæti upplýsinga**

  Forstöðumenn ríkisaðila ættu ætíð að hafa í huga að upplýsingar og gögn eru bæði mikilvæg verðmæti og nauðsynleg fyrir viðkomandi rekstur. Af þessum sökum verður að vernda þau með sérstökum öryggisráðstöfunum.

- Ábyrgð forstöðumanna

Vegna mikilvægis upplýsingakerfa fyrir rekstur stofnana og fyrirtækja ríkisins ætti eitt af hlutverkum forstöðumanna þeirra að vera að taka endanlegar ákvarðanir um umfang þeirra öryggisráðstafana, sem beita á, til þess að vernda eigið upplýsingakerfi ásamt þeim gögnum og upplýsingum sem það geymir. Þetta þýðir með öðrum orðum að forstöðumenn bera ábyrgð á rekstraröryggi upplýsingakerfis stofnunar sinnar eða fyrirtækis á sama hátt og þeir bera ábyrgð á öðrum þáttum rekstrarins. Því er eðlilegt að þeir meti hvaða gögn og upplýsingar eru nauðsynlegar til þess að reksturinn gangi sem eðlilegast fyrir sig, hverjar afleiðingarnar eru ef gögn eru ekki í lagi, gagnaleynd er rofin eða gögn eru ekki aðgengileg.

- Öryggisstefna

Hver stofnun og fyrirtæki ríkisins þarf að móta sérstaka öryggisstefnu vegna upplýsingakerfa sinna. Í öryggisstefnu eiga að birtast þau meginmarkmið sem viðkomandi ríkisaðili stefnir að því að ná með öryggisráðstöfunum sínum.

- Viðunandi ráðstafanir

Ríkisendurskoðun telur að stofnanir og fyrirtæki ríkisins þurfi að huga vandlega að því að samræmi sé á milli öryggisráðstafana í upplýsingakerfum og þeirra hagsmuna sem þær eiga að gæta.

- Almennar öryggiskröfur

Í samkomulagi fjármálaráðherra og Skýrr hf. frá 17. febrúar 1997 er í kaflanum um almennar kröfur til landskerfa m.a. fjallað um þær öryggiskröfur sem gerðar eru til landskerfa sem vistuð eru hjá Skýrr hf. Ríkisendurskoðun telur að gera eigi jafnstrangar öryggiskröfur til annarra kerfa þó svo að þau séu vistuð hjá öðrum aðilum en Skýrr hf.

- Aðgangs- og lykilorð

Ríkisendurskoðun telur að ríkisaðilar eigi að hafa reglur Skýrr hf. til viðmiðunar þegar þeir gera kröfur vegna aðgangs- og lykilorða í upplýsingakerfum sínum.

- Tölvuveirur

Tölvuveirur geta valdið verulegum rekstrartruflunum í upplýsingakerfum ríkisaðila. Mikilvægt er því að ríkisaðilar grípi til viðeigandi ráðstafana gegn þeim.

- Dagbækur tölvukerfa

Mikilvægt öryggisatriði í tölvukerfi er að halda víðtæka dagbók, („log-skrá“) yfir það sem gerist í kerfinu, m.a. um óreglulega atburði og aðgangsmál. Nauðsynlegt er að dagbókarfærslurnar nái til tölvukerfisins alls, þ.e. einnig til beina, gátta og annars tengibúnaðar. Ef slíkar dagbækur eru ekki haldnar og skoðaðar reglulega vita menn t.d. ekki hvort brotist hefur verið inn í tölvukerfi þeirra. Tölvudagbók gegnir mikilvægu hlutverki við rannsókn á tölvubrotum.

- Neyðaráætlanir

Stofnanir og fyrirtæki ríkisins þurfa að útbúa skriflegar neyðaráætlanir sem hægt er að grípa til við náttúruhamfarir, bruna og önnur óhöpp. Sérstakur hluti neyðaráætlunar skal vera vegna upplýsingakerfis viðkomandi ríkisaðila og skal hann ná til allra upplýsingakerfa hans.

- Eftirlit og endurmat

Meta þarf hvort starfsmenn virða þær öryggisráðstafanir sem forstöðumaður hefur ákveðið. Öryggisráðstafanir sem þykja góðar í dag geta verið úreltar á morgun. Reglulega þarf því að endurmeta öryggisráðstafanir á sama hátt og endurmeta þarf áhættu og öryggisstefnu viðkomandi ríkisaðila.

- Varðveisla tölvugagna

Ljóst er að skjalalaus viðskipti aukast sífellt og um leið fjölgar þeim ríkisaðilum sem nota upplýsingakerfi er geyma gögn um slík samskipti, sbr. t.d. málaskrárkerfi ráðuneytanna. Telja verður brýnt að Þjóðskjalasafni verði gert kleift að sinna því lögboðna hlutverki sínu að varðveita tölvugögn svo koma megi í veg fyrir að upplýsingar á slíku formi glatist.

- Tilkynningar tölvuinnbrota

Ríkisendurskoðun hvetur ríkisaðila eindregið til þess að tilkynna tölvuinnbrot til lögreglu jafnvel þó ekki sé tilefni til kæru. Ástæðan er sú að hún býr e.t.v. yfir vitneskju um að sami aðili hafi brotist víða annars staðar inn án þess að kæra hafi komið fram. Tilkynningar geta þar með aukið líkur á því að tölvuþrjótur náist.

1. Umfang úttektarinnar

Eins og fram kemur í inngangi greinargerðar þessarar er tilgangur hennar sá að aðstoða forstöðumenn ríkisaðila við að efla innra eftirlit vegna upplýsingakerfa stofnana sinna eða fyrirtækja og draga þar með úr líkum á því að rekstrartruflanir í kerfunum valdi röskun á starfseminni.

Flestir ríkisaðilar eru svo háðir upplýsingakerfum sínum að ef þau eru ekki í rekstrarhæfu ástandi er starfsemi viðkomandi oftast meira og minna lömuð. Aðaltilgangur öryggisráðstafana vegna upplýsingakerfa á því að felast í því að tryggja rekstrarhæfi þeirra.

Rekstraröryggi upplýsingakerfa byggir á því að:

❶ Upplýsingakerfi sé aðgengilegt.
❷ Upplýsingakerfi sé nothæft.

Viðfangsefni þessarar greinargerðar er rekstrarhæfi upplýsingakerfa. Meginmál greinargerðarinnar snýst um helstu áhættuþætti með tilliti til rekstraröryggis upplýsingakerfa, framkvæmd áhættumats, mótun öryggisstefnu og öryggisráðstafanir. Einnig er fjallað um þörfina á stöðugu eftirliti og endurmati öryggismála vegna kerfanna.

Áreiðanleiki og gagnaleynd flokkast í raun utan efnis greinargerðar þessarar. Þrátt fyrir það er í henni stutt umfjöllun um þessi atriði vegna þess hve nátengd þau eru rekstrarhæfi upplýsingakerfa.

Það er grundvallaratriði að ríkisaðilar gefi réttar upplýsingar eða afgreiði mál á réttum forsendum. Því skulu öryggisráðstafanir einnig beinast að því að tryggja áreiðanleika gagna.

Áreiðanleiki gagna byggir á því að:

❶ Gögn séu rétt færð inn.
❷ Gögn séu heildstæð, þ.e. öll gögn færð inn.
❸ Gögn séu gild en ekki úrelt.

Einnig er mikilvægt að gagnaleynd sé tryggð. Ríkisaðilar vinna reyndar oft með upplýsingar sem almenningur á rétt á aðgangi að samkvæmt upplýsingalögum en frá þessu eru þó mikilvægar undantekningar.

Gagnaleynd getur t.d. byggst á:

❶ Lögum nr. 121/1989 um skráningu og meðferð persónuupplýsinga.
❷ Upplýsingalögum nr. 50/1996, sbr. 3. grein.
❸ Almannahagsmunum, sbr. 17. gr. stjórnsýslulaga, nr. 37/1993.
❹ Eignar- eða höfundarréttarsjónarmiðum.
❺ Samkeppnissjónarmiðum, sbr. samkeppnislög, nr. 8/1993.

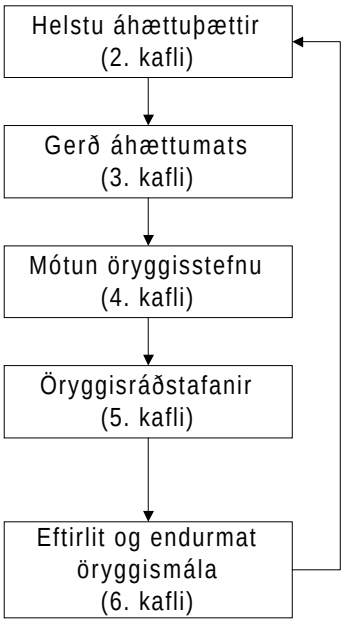
Bandaríska ríkisendurskoðunin gerði nýlega úttekt á því á hvaða þætti einkafyrirtæki, sem talin eru standa framarlega í öryggismálum, legðu áherslu á vegna öryggis upplýsingakerfa sinna. Í framhaldi af úttektinni gerði hún skýrslu[1] með

[1] Information Security Management, Learning from Leading Organizations, maí 1998.

ábendingum til þarlendra ríkisaðila um þau atriði sem hún telur að þeir eigi að leggja aðaláherslu á vegna öryggis upplýsingakerfa sinna.

Ríkisendurskoðun telur áhersluatriði í áðurnefndri skýrslu góðar viðmiðanir og gerir margar þeirra að sínum í greinargerð þessari. Hér er helst að nefna þá megináherslu sem lögð er á verðmæti gagna og það sjónarmið að forstöðumenn stofnana beri ábyrgð á öryggi upplýsingakerfa sinna og því eigi þeir að taka endanlegar ákvarðanir um þær öryggisráðstafanir sem viðhafa skal þeim til verndar.

Myndin hér á eftir sýnir í grófum dráttum uppbyggingu greinargerðarinnar.



Mynd 1. Uppbygging greinargerðarinnar

2. Helstu áhættuþættir

Í þessum kafla er fjallað um helstu áhættuþætti sem geta haft áhrif á rekstur upplýsingakerfa stofnana og ríkisfyrirtækja. Með öðrum orðum má segja að verið sé að fjalla um þær ógnanir sem steðjað geta að rekstri áðurnefndra kerfa.

Á síðasta ári braust fyrrverandi starfsmaður ríkisfyrirtækis hér á landi inn í tölvuherbergi þess og hafði áður en hann var handtekinn náð að eyðileggja nokkuð af tölvubúnaði fyrirtækisins. Þó svo að umrætt atvik hafi ekki haft áhrif á getu þess til þess að sinna hlutverki sínu, má telja líklegt að svipaðar kringumstæður hefðu getað haft í för með sér verulegar truflanir í rekstri einhvers annars ríkisaðila, t.d. lokun í nokkra daga á meðan tölvubúnaður væri endurnýjaður og afrit sett inn af hugbúnaði og gögnum. Lengd rekstrarstöðvunar er í tilviki sem þessu m.a. háð því að til séu réttar útgáfur hugbúnaðar og ný afrit af gögnum.

Dæmið hér á undan sýnir glöggt að horfa þarf til fleiri þátta en náttúruhamfara og eldsvoða þegar hugað er að rekstraröryggi ríkisaðila.

2.1 Ártalið 2000

Sá áhættuþáttur sem brýnast er að tekið sé á nú er að tölvuvinnsla ártalsins 2000 valdi ekki rekstrartruflunum hjá ríkisaðilum. Ef þeir eru ekki þegar farnir að huga að lausn þessa vandamáls er í mörgum tilvikum að verða of seint að leysa það í tíma. Treysti þeir á upplýsingatækni þurfa þeir að búa sig undir truflanir á rekstri sínum. Allir ríkisaðilar þurfa að búa sig undir hugsanlegar rekstrartruflanir í kerfum þeirra sem þeir eiga samskipti við og áhrif þeirra á rekstur sinn.

Í skýrslu sem Ríkisendurskoðun gaf út í júlí 1997 var gerð grein fyrir vandamálum tengdum tölvuvinnslu á ártalinu 2000. Því verður ekki rakið nánar hér hve alvarlegum rekstrartruflunum þetta vandamál getur valdið. Í skýrslunni kom fram að stofnunin teldi að stefna þyrfti að því að leysa þau vandamál sem tengjast vinnslum á þessu og síðari ártölum fyrir árslok 1998. Stofnunin ítrekar þessa skoðun sína þar sem mörg kerfi vinna með ártöl fram í tímann og verða því e.t.v. ónothæf áður en árið 2000 gengur í garð.

Mikið er í húfi að vel takist til við úrlausn á þeim vandamálum sem tengjast ártalinu 2000 svo að ekki komi til verulegra rekstrartruflana hjá ríkisaðilum og fleirum. Ef sú verður raunin, er ekki í öllum tilvikum hægt að benda á hver beri kostnað vegna þeirra. Í svari forsætisráðherra við fyrirspurn Hjörleifs Guttormssonar um þetta mál á síðasta þingi, sjá þingskjal 990, kom fram að líklega munu dómstólar í einhverjum tilvikum þurfa að skera úr um það.

Ýmislegt hefur verið gert vegna ártalsins 2000 frá því að áðurnefnd skýrsla var gefin út. Haldnar hafa verið nokkrar ráðstefnur um málið og hafa Ríkiskaup sérstaklega beitt sér í því, sjá t.d. heimasíðu þeirra **http://www.rikiskaup.is/**.

Í maí sl. skipaði fjármálaráðherra sérstaka nefnd um ártalið 2000. Skipan hennar er mikilvægt skref í þá átt að koma í veg fyrir að íslenskt þjóðfélag verði fyrir verulegum skakkaföllum vegna þeirra vandamála sem tengjast ártalinu 2000 í upplýsingakerfum og tækjabúnaði. Hlutverk nefndarinnar er samkvæmt erindisbréfi að:

> *„vara við, upplýsa og benda á hvernig standa beri að lausn þeirra vandamála sem tengjast ártalinu 2000 í upplýsingakerfum og tækjabúnaði þannig að ekki hljótist skaði af skakkri meðferð ártala á þeim tímamótum.“*

Sjá einnig vefsíðu nefndarinnar http://2000.stjr.is.

Nýjasta framtakið er samstarf Landssímans og fjármálaráðuneytisins um rekstur sérstaks upplýsingasíma, 800-2000, vegna vandamála tengdum tölvuvinnslu ártalsins 2000 þar sem er að finna almennar upplýsingar fyrir stærri sem smærri tölvunotendur.

Hjá flestum ríkisaðilum er starfsemi í lágmarki í vikunni á milli jóla og nýjárs. Ríkisendurskoðun vill því benda á þann möguleika að ríkisaðilar noti þá viku í desember n.k. til þess að prófa hvort leiðréttingar sem þegar hafa verið gerðar á upplýsingakerfum vegna ártalsins 2000 virki eins og til er ætlast.

2.2 Tölvuumhverfi

Í maí 1995 var gerð könnun[2] á meðal endurskoðenda upplýsingakerfa (CISA[3]) á viðhorfi þeirra til tölvuöryggismála. Í könnuninni kemur fram að þeir telja áhættu mismunandi eftir því hvert tölvuumhverfið er, flestir telja að mesta áhættan sé í víðnetstengdu einkatölvukerfi, sjá nánar í töflunni hér á eftir:

Áhætta ef	**Mikil**	**Í meðallagi**	**Lítil**
Víðnetstengt einkatölvuumhverfi	71%	27%	2%
Staðarnetstengt einkatölvuumhverfi	35%	64%	1%
Einkatölva	32%	50%	18%
Miðtölvuumhverfi	17%	75%	8%
Stórtölvuumhverfi	7%	71%	22%

Ljóst er því að mismunandi öryggiskröfur þarf að gera eftir því hvernig umhverfi upplýsingakerfa er háttað.

[2] Perceived Security Threats to Today´s Accounting Information Systems: A Survey of CISA´s
IS Audit & Control Journal, Volume III, 1996.
[3] „Certified Information System Auditor“.

2.3 Hegðun starfsmanna

Tæknin ein og sér er ekki lausn á öllum vandamálum sem upp koma varðandi öryggi upplýsinga. Notendur þurfa að skilja mikilvægi þeirra upplýsinga sem þeir vinna með og bera ábyrgð á öryggi þeirra.

Í öryggismálum upplýsingakerfa þurfa ráðstafanir að beinast bæði að utanaðkomandi aðilum og starfsmönnum viðkomandi. Líklega er í mörgum tilvikum meira hugað að öryggisráðstöfunum sem koma eiga í veg fyrir aðgang utanaðkomandi að upplýsingakerfum en að hegðun eigin starfsmanna, en samkvæmt áðurnefndri könnun er hún ein af stærstu ógnunum við öryggi upplýsingakerfa. Hér er bæði átt við umsjónarmenn upplýsingakerfa og almenna starfsmenn.

Í áðurnefndri könnun á meðal endurskoðenda upplýsingakerfa voru þeir m.a. spurðir að því hverjar þeir teldu vera þrjár helstu ógnanir sem steðjuðu að tölvuvæddum fjárhagskerfum. Afar athyglisvert er að sjá hve þessir sérfræðingar telja hegðun starfsmanna mikla ógnun við öryggi upplýsingakerfa, sérstaklega þegar um einka- eða miðtölvur er að ræða, en þar eru áhættuþættir tengdir starfsmönnum í öllum þremur efstu sætunum. Í stórtölvuumhverfi eru þeir í fyrsta og þriðja sæti. Það er aðeins í nettölvuumhverfi sem áhætta tengd starfsmönnum er eingöngu í þriðja sæti en aðrir þættir lenda í því fyrsta og öðru.

Hér má sjá nánar niðurstöður áðurnefndrar könnunar um helstu áhættuþætti í rekstri upplýsingakerfa:

Einkatölvur:

1) Starfsmenn eyða gögnum af slysni.
2) Starfsmenn hleypa tölvuvírusum inn í kerfið.
3) Starfsmenn skrá óvart inn röng gögn.

Miðtölvur:

1) Starfsmenn ná sér í aðgang að gögnum eða kerfum með ólögmætum hætti.
2) Starfsmenn skrá óvart inn röng gögn.
3) Aðgreining starfa er engin eða ónóg.

Nettengdar tölvur:

1) Utanaðkomandi aðilar, t.d. tölvuþrjótar ná sér í aðgang að gögnum eða kerfum með ólögmætum hætti.
2) Öryggisráðstafanir breytast ekki í takt við örar tæknibreytingar.
3) Starfsmenn ná sér í aðgang að gögnum eða kerfum með ólögmætum hætti.

Stórtölvur:

1) Starfsmenn skrá óvart inn röng gögn.
2) Áföll eins og eldur, flóð og rafmagnsleysi.
3) Starfsmenn ná sér í aðgang að gögnum eða kerfum með ólögmætum hætti.

Ofangreind könnun sýnir ljóslega hve mikilvægt er að starfsmenn séu vel upplýstir um öryggismál og að við hönnun upplýsingakerfa sé gert ráð fyrir ítarlegri villuprófun gagna við skráningu til þess að koma í veg fyrir að röng gögn fari inn í kerfin.

2.4 Alnetið

Áhættuþættir þeir sem tengjast notkun Alnetsins eru margir vegna þess að það býður upp á margar tegundir þjónustu-

þátta. Meðal þeirra eru tölvupóstur, Veraldarvefurinn, skráarflutningar, spjallrásir og fréttahópar. Hverjum þjónustuþætti fylgja einhverjar sérstakar hættur en sameiginlegir áhættuþættir þeirra allra eru sá samskiptamáti sem notaður er á Alnetinu, flóknar uppsetningar á öryggisatriðum og skortur á öryggis- og umgengnisreglum vegna notkunar Alnetsins hjá stofnunum og fyrirtækjum. Nánar verður fjallað um þessi atriði hér á eftir en í 5. kafla sem fjallar um öryggisráðstafanir er nánar farið í einstaka þjónustuþætti Alnetsins og hvað hægt er að gera til þess að draga úr þeirri hættu sem fylgir notkun þeirra með ákveðnu verklagi og notkun sérstakra forrita.

1. Samskiptaaðferð Alnetsins er ótrygg

Samskipti á Alnetinu byggja á TCP/IP-samskiptastaðli. Samskiptamáti þessi sem er tiltölulega einfaldur í uppbyggingu inniheldur fáa öryggisþætti. Því er mjög erfitt að tryggja öryggi vegna margra þeirra þjónustuþátta sem Alnetið býður upp á. Margir þeirra veikleika sem tengjast þessum þjónustuþáttum eru vel þekktir meðal tölvuþrjóta, sem nýta sér þá til innbrota í tölvukerfi, skemmdarverka og fjársvika.

Vegna hins einfalda samskiptastaðals er erfitt að tryggja leynd þeirra upplýsinga sem fara um Alnetið. Hlerun þar er tiltölulega auðveld þar sem meiri hluti samskiptanna er ekki dulkóðaður. Þetta á við um tölvupóst, lykilorð, skráarsendingar o.fl. Því er ekki hægt að gefa sér þá forsendu að þær upplýsingar sem fara um Alnetið séu eingöngu aðgengilegar þeim sem móttekur þær. Alnetið er í raun eins og sveitasíminn var hér fyrr á árum; hægt var að hlera símtöl að gefnu því skilyrði að viðkomandi væri á sömu símalínu og samtölin fóru fram á.

Einnig er sá galli á þessum samskiptamáta að auðvelt er að sigla undir fölsku flaggi á Alnetinu því ekki er hægt að staðfesta hver er sendandi upplýsinga. Á Alnetinu er hægt að viðhafa algera nafnleynd auk þess sem hægt er að vera með nafnlaus póstföng. Þar að auki geta einstaklingar eða fyrir-

tæki auðveldlega villt á sér heimildir með því að breyta stillingum á tölvum sínum, þannig að þær gefi rangar og villandi upplýsingar um það frá hverjum upplýsingar koma.

Gerð hefur verið tillaga að öruggari útgáfu af TCP/IP, svonefnd 6. útgáfa, en hún hefur enn ekki hlotið almenna útbreiðslu.

2. Flóknar uppsetningar öryggisþátta

Öryggisþættir í netkerfum geta oft verið nokkuð flóknir í uppsetningu og eftirliti. Öryggisþættir sem ekki eru rétt uppsettir geta leitt til þess að óviðkomandi aðilar geta komist í gögn viðkomandi ríkisaðila.

Þegar sett er upp nýtt upplýsingakerfi er oftast slökkt á flestum öryggisatriðum vegna Alnetsins til þess að auðvelda uppsetninguna. Ef ekki er hugað að því að virkja aftur þessa innbyggðu öryggisþætti kunna upplýsingakerfi að vera mjög opin án þess að ríkisaðilar geri sér grein fyrir því.

3. Skortur á öryggis- og umgengnisreglum

Víða skortir á að settar hafi verið nauðsynlegar öryggis- og umgengnisreglur vegna Alnetsins. Ef þetta hefur ekki verið gert, getur verið erfitt að tryggja öryggi viðkomandi upplýsingakerfis.

2.5 Tölvuveirur

Tölvuveirur geta valdið verulegum rekstrartruflunum í upplýsingakerfum. Tölvuveirur eru forrit sem geta fjölfaldað sig með því að bæta forritsbút við öll forrit. Tölvuveirur ráðast oftast á ræsigeira diska eða skjöl af tiltekinni tegund. Til viðbótar þessum fjölföldunareiginleika geta forrit þessi gert þann óskunda sem skemmdarvargarnir sem skrifuðu þau hafa upphugsað. Tölvuveirur berast inn í upplýsingakerfi

með öðru efni, þ.e. aðallega á disklingum og skrám sem koma af Alnetinu.

Önnur tegund forrita sem ætlað er valda skemmdum eru svonefndir „Trójuhestar“. Þeir eru forrit sem gera allt annað en viðkomandi notandi heldur að þau séu að gera. Slík forrit geta valdið skemmdum eða veitt óviðkomandi aðilum aðgang að gögnum viðkomandi starfsmanns og öllum öðrum gögnum sem hann hefur aðgang að. Til þess að koma í veg fyrir að „Trójuhestar“ komist inn í kerfi ríkisaðila er mikilvægt að á upplýsingakerfum þeirra séu aðeins keyrðar viðurkenndar útgáfur hugbúnaðar, sem kerfisstjóri hefur gengið úr skugga um að vinni eins og til er ætlast.

2.6 Rafræn viðskipti

Á undanförnum árum hafa rafræn viðskipti ört vaxið og er ljóst að þau muni aukast enn frekar á næstu árum. Rafrænum viðskiptum fylgir sá möguleiki, sem reyndar er mismikið nýttur af ýmsum ástæðum, að draga mjög úr pappírsgögnum. Upptaka rafrænna viðskipta hjá ríkisaðilum eykur mjög kröfur til öryggis því í mörgum tilvikum koma sjálfvirk kerfi og færslur nú alfarið í stað handvirkra verkferla og skjala.

Í áðurnefndri könnun endurskoðenda upplýsingakerfa töldu 24,5% að rafræn viðskipti ykju mjög á áhættu í fjárhagskerfum, 60,8% töldu hana aukast nokkuð en 14,7% lítið.

2.7 Eldsvoðar og vatnsskemmdir

Meðal þeirra áhættuþátta sem tengjast rekstrartruflunum í upplýsingakerfum eru bruni og vatnsskemmdir. Vatnsskemmdir geta átt sér stað sem afleiðing slökkvistarfs eða af öðrum orsökum. Mikilvægt er því að fyllstu öryggisráðstafanir séu gerðar til þess að minnka hættu á bruna og vatnstjóni og að tiltæk séu í neyðaráætlun fyrirmæli um viðbrögð við slíku.

Brunamálastofnun ríkisins hefur eftirlit með brunamálum hér á landi. Reglugerð nr. 200/1994 gildir um eigið eftirlit eigenda og forráðamanna með brunavörnum í atvinnuhúsnæði. Í fylgiskjali með þessari reglugerð eru ítarlegar leiðbeiningar um framkvæmd áðurnefnds eftirlits sem teknar hafa verið saman af Brunamálastofnun ríkisins. Æskilegt er að forstöðumenn stofnana kynni sér þessar leiðbeiningar.

2.8 Náttúruhamfarir

Þó svo að menn geti talið það ásættanlegt að upplýsingakerfi fyrirtækja í almennum atvinnurekstri séu óvirk vegna náttúruhamfara er slíkt algerlega óviðunandi fyrir suma ríkisaðila, t.d. heilbrigðisstofnanir og löggæslu. Í miklum náttúruhamförum eru veikustu hlekkir upplýsingakerfa oftast rafmagns- og símakerfið.

Erfitt getur verið að koma þeim upplýsingakerfum sem uppbyggð eru með svonefndri biðlara/miðlara högun í gagnið aftur eftir að þau hafa hrunið vegna náttúruhamfara eða af öðrum ástæðum. Skýringin á þessu er sú að gögnum kerfisins kann að vera dreift víða og því gæti þurft að koma mörgum tölvumiðstöðvum í gang áður en hægt er að koma kerfinu aftur í gagnið. Af þessum sökum þarf sérstaklega að huga að rekstraröryggi kerfa sem byggð eru upp með þessum hætti. Rétt er hins vegar að taka fram að oft á tíðum eru öll gögn geymd miðlægt í biðlara/miðlara upplýsingakerfum og í þeim tilvikum hafa rekstrartruflanir þar sem gögn eru ekki geymd minni áhrif en ella.

2.9 Opnun upplýsingakerfa ríkisins

Í stefnuyfirlýsingu ríkisstjórnarinnar frá 23. apríl 1995 er lagður grunnur að stefnumótun í málefnum upplýsingasamfélagsins. Í henni kemur fram að tryggður verði aðgangur fólks að opinberum upplýsingum, dregið verði úr skrifræði í samskiptum borgaranna við stjórnvöld og afnumin óþörf

laga- og reglugerðarákvæði. Samhliða þessu verði þjónusta ríkisins sniðin að nútímatækni, t.d. með nettengingu þjónustustofnana og pappírslausum viðskiptum.

Í stefnuyfirlýsingunni er gert ráð fyrir að upplýsingakerfi ríkiskerfisins verði opnuð almenningi. Af þessum sökum má búast við að tölvupóstssamskipti ríkisaðila við almenning á Alnetinu og á milli ríkisaðila aukist enn frekar á næstu árum. Stefnan hefur í för með sér að gera verður mun strangari öryggiskröfur til þeirra upplýsingakerfa sem aðgengileg eru almenningi en þeirra sem eingöngu eru aðgengileg starfsmönnum viðkomandi aðila. Nauðsynlegt kann að vera að aðskilja það upplýsingakerfi sem aðgengilegt er almenningi og það sem notað er innan viðkomandi stofnunar eða fyrirtækis ef í því síðarnefnda er unnið með trúnaðarupplýsingar sem ekki er talið ásættanlegt að óviðkomandi aðilar komist í. Auk þessa er nauðsynlegt fyrir ríkisaðila að huga vel að öryggisþáttum tölvupósts og vefþjóna.

2.10 Hugbúnaðarfyrirtæki verða gjaldþrota

Ef rekstur ríkisaðila er háður tiltekinni gagnavinnslu verður að vanda val nýs hugbúnaðar hvort sem um er að ræða hugbúnað sem sérsmíðaður er fyrir viðkomandi aðila eða ekki. Ekki er nóg að horfa á kosti og galla hugbúnaðarins heldur verður og að horfa til þekkingar, reynslu og stöðu þess aðila sem framleiðir og viðheldur honum eða selur hann.

Ef hugbúnaðarfyrirtæki, sem ríkisaðili treystir á um þjónustu og viðhald á mikilvægum hugbúnaði, verður gjaldþrota eða hættir starfsemi, getur rekstraröryggi ríkisaðilans verið stefnt í voða ef annar aðili tekur ekki þegar við þjónustu hugbúnaðarins. Því er mikilvægt þegar ríkisaðili semur við hugbúnaðarfyrirtæki um gerð upplýsingakerfis, að ákvæði séu í samningnum um að ríkisaðilinn fái eintak af forritunarkóta kerfisins ef hugbúnaðarfyrirtækið verður gjaldþrota eða hættir starfsemi og ef áframhaldandi þjónusta er ekki tryggð.

Í þessu sambandi er rétt að benda á viðauka 3 í Innkaupahandbók RUT-nefndarinnar frá 1998, en í honum er að finna samningsákvæði um eignarhald og umráðarétt. Um þau segir þar að ákvæðin hafi verið notuð í nokkrum samningum ríkisstofnana við verktaka í hugbúnaðargerð og í flestum tilvikum ættu þau að tryggja nægjanlega rétt ríkisins sem verkkaupa til fullra umráða yfir hugbúnaðinum.

2.11 Lykilstarfsmenn hætta skyndilega störfum

Oft á tíðum eru tölvudeildir ríkisaðila fámennar. Skyndilegt brotthvarf eins eða tveggja lykilstarfsmanna getur því haft verulegar rekstrartruflanir í för með sér ef eftirmenn hafa ekki næga þekkingu og þurfa hjálparlaust að koma sér inn í nýja starfið. Mikilvægt er því að fleiri en einn starfsmaður hafi þekkingu á öllum þáttum í uppbyggingu og rekstri upplýsingakerfa viðkomandi og ekki er síður mikilvægt að þau séu vel skjöluð.

2.12 Tölvubrot

Tölvur eru æ oftar notaðar til refsiverðrar háttsemi eða í tengslum við hana. Í þessum kafla verður fjallað um tölvubrot en þau eru í raun ekki sérstakur brotaflokkur heldur aðferð eða umhverfi sem tiltekin brot eiga sér stað í.

1. Rannsókn á tölvubrotum

Meðal þeirra sérstöku verkefna sem Ríkislögreglustjóra ber að hafa með höndum samkvæmt a. lið 2. mgr. 5. gr. lögreglulaga nr. 90/1996 er að starfrækja lögregluranns óknardeild sem rannsakar skatta- og efnahagsbrot. Tölvubrot sem tengjast efnahagsbrotarannsóknum, svo og innbrot í tölvu-

kerfi („hacking“), heyra undir þessa deild sem nefnd er efnahagsbrotadeild.

Tiltölulega stutt er síðan sá möguleiki varð raunhæfur að nota tölvur við refsiverða háttsemi. Nú er hins vegar talið að með ári hverju sé æ stærri hluti auðgunarbrota framinn með tölvu. Enn sem komið er hafa þó ekki verið gerðar neinar tölfræðilegar athuganir hér á landi þessu til sönnunar. Dómar hafa hins vegar þegar fallið hér vegna tiltekinna blekkinga sem menn í fyrirtækjum, stofnunum og bönkum hafa staðið fyrir í fjárhagskerfum til að reyna að fela fjárdrátt. Þar hafa starfsmenn í sumum tilvikum gert tilteknar kúnstir í fjárhagskerfum en í öðrum hafa þeir notfært sér tiltekin hugbúnaðarkerfi til þess að búa til færslur sem myndað hafa grundvöll peningagreiðslna til þeirra eða nákominna. Í sumum þessara dæmdu tilvika er um að ræða fjársvik upp á milljónir króna.

Algengustu brot þar sem tölvur koma við sögu eru:

a) Skjalafals sem liður í fjársvikum, tollsvikum o.þ.h.
b) Bókhaldsbrot af ýmsu tagi, til að dylja fjárdrátt eða annað misferli.
c) Innbrot í tölvukerfi („hacking“).
d) Brot á höfundarréttarlögum, þ.e. ólögleg dreifing hugbúnaðar.

Við rannsókn tölvubrota er algengt að í ljós komi að öryggismál, þ.á.m. innra eftirlit, eru í miklum ólestri. Einnig að ekki eru fyrirliggjandi starfslýsingar sem geta skipt miklu máli vegna umboðssvika, þ.e. þegar rannsakað er hvort starfsmaður hefur farið út fyrir þær heimildir sem hann hefur í starfi sínu.

2. Leiðbeiningar Ríkislögreglustjóra vegna tölvuinnbrota

Í eftirfarandi undirköflum verður gerð grein fyrir helstu atriðum sem auðveldað geta lögreglunni rannsókn ef grunur er um innbrot í tölvukerfi eða tilraun til þess.

1. Tilkynna eða kæra til lögreglu vakni grunur um tölvubrot

Efnahagsbrotadeild Ríkislögreglustjóra hvetur fyrirtæki og stofnanir til þess að tilkynna alltaf ef upp kemst um innbrot eða tilraun til innbrots í tölvukerfi. Hver ríkisaðili verður svo að meta það hvort hann vill kæra brotin og fara fram á opinbera rannsókn. Deildin bendir í því sambandi á, að hún virðir trúnað og skal skv. 1.tl. 8. gr. lögreglulaga, annast rannsókn brota í samráði við kærendur. Ástæða þess að mælt er með tilkynningu ef aðilar vilja ekki kæra, er m.a. sú, að þá komast rannsóknaraðilar e.t.v. að því, að sá grunaði hefur komið við sögu í öðrum tölvubrotamálum, án þess að kæra hafi komið fram. Slíkt kallar á sérstök viðbrögð af hálfu lögreglunnar.

Í viðauka greinargerðar þessarar eru birtar leiðbeiningar efnahagsbrotadeildar Ríkislögreglustjóra um kærusmíð (eða tilkynningu). Í þeim koma fram hvaða upplýsingar eru nauðsynlegar og gagnlegar við rannsókn hennar á viðkomandi broti.

2. Lögregla á að rekja slóð en ekki brotaþoli

Mikilvægt er að lögregla sé kölluð til sem fyrst eftir að grunur vaknar um innbrot í tölvukerfi eða tilraun til þess, hvort sem menn ætla að kæra eða tilkynna um brot. Mælt er gegn því að aðilar reyni sjálfir að rannsaka slíkt, þar sem það getur ef ekki er rétt að því staðið, spillt líkum á því að brot upplýsist. Í mörgum tilvikum kemur til greina að halda leiðinni opinni fyrir tölvuþrjótinn um tíma í þeim tilgangi að standa hann að verki. Slíkt þyrfti að gerast í samráði við rannsóknaraðila.

3. Tölvudagbók er mikilvægt sönnunargagn

Meðal mikilvægra sönnunargagna í dómsmálum gegn tölvuþrjótum eru upplýsingar í dagbók tölvukerfis („log-skrá"), en í hana eru vélrænt skráðir ýmsir atburðir í kerfinu. Nauðsynlegt er að dagbókarfærslurnar nái til tölvukerfisins alls, þ.e. einnig til beina, gátta og annars tengibúnaðar. Enn hefur ekki fallið dómur hér á landi um sönnunargildi slíkra dagbóka vegna tölvuinnbrota.

Um verndun og geymslutíma dagbókar

Öruggast er að búa jafnóðum til tvöfalda dagbók, þ.e. að afrita færslur sem til verða í dagbók jafnóðum yfir á annan geymslustað, t.d. aðra vél. Með slíku má auka líkur á því að dagbók sé til ef tölvuþrjótar hafa getað eyðilagt frumfærslur dagbókar í því skyni að hylja slóð sína. Dagbækur eða afrit þeirra þarf að geyma í a.m.k. 6 mánuði.

Hvaða sönnunaratriði eiga að vera í dagbók?

Leggja verður áherslu á að eftirfarandi atriði komi fram í dagbók upplýsingakerfis:

1) Dagsetning og tími vegna upphafs og loka tölvusamskipta.
2) Hver tengist, þ.e. símanúmer viðkomandi, IP-númer tölvu og kenniorð. Upplýsingar um það síðasta geta reyndar verið villandi því oft er verið að nota kenniorð annars aðila.

Rétt er að geta þess hér að í 5. kafla sem fjallar um öryggisráðstafanir er sérstakur kafli um tölvudagbækur.

Ríkisendurskoðun hvetur ríkisaðila eindregið til þess að tilkynna tölvuinnbrot til lögreglu jafnvel þó ekki sé tilefni til kæru. Ástæðan er sú að hún býr e.t.v. yfir vitneskju um að sami aðili hafi brotist víða annars staðar inn án þess að kæra hafi komið fram. Tilkynningar geta þar með aukið líkur á því að tölvuþrjótur náist.

3. Tölvubrot og hegningarlögin

Með lögum nr. 30/1998, voru gerðar breytingar á hegningarlögum nr. 19/1940 til þess að mæla refsiverða ýmsa háttsemi sem tengist tölvum og notkun þeirra.

Í greinargerð með frumvarpi að lögunum er fjallað nokkuð heildstætt um brot þau sem kölluð eru einu nafni tölvubrot. Það hugtak er notað sem samheiti yfir ýmsa óréttmæta (ólögmæta) háttsemi sem framin er með því að nota tölvu, eða sem beinist að tölvum, forritum eða gögnum og upplýsingum sem varðveittar eru í tölvum eða á tölvutæku formi.

Í greinargerðinni eru þau tölvubrot, sem hér skipta máli, flokkuð á eftirfarandi hátt:

1) Skemmdarverk á tölvubúnaði.
2) Brot framin með því að nota tölvu:

   a) Auðgunarbrot, b) tölva notuð til þess að leyna broti, c) stuldur á tölvutækum gögnum, d) skattsvik og e) skjalabrot.
3) Óheimil notkun á tölvum.
4) Innbrot í tölvukerfi („hacking“).

Hér á eftir verður lauslega fjallað um þessar tegundir tölvubrota.

1. Skemmdarverk á tölvubúnaði

Þegar um er að ræða skemmdarverk sem tengjast tölvum og notkun þeirra, má greina á milli skemmdarverka á tölvuvélbúnaði og samskiptalínum og skemmdarverka á forritum eða gögnum með útþurrkun eða breytingum. Eignarspjallaákvæði almennra hegningarlaga nr. 19/1940 tekur nú til allra þessara tilvika, auk þess sem það nær og til breytinga á gögnum eða forritum sem felast í því að koma þar fyrir tölvuveirum sem geta haft í för með sér truflanir á tölvuvinnslu eða eyðileggingu á gögnum eða forritum. Líklegt má

telja að undir þetta ákvæði falli og fjöldasendingar tölvupósts sem sendar eru í þeim tilgangi að valda miklu álagi á tölvukerfi þannig að það geti ekki sinnt eðlilegri þjónustu og hrynji jafnvel.

Mörg dæmi finnast um skemmdarverk í mótmælaskyni við tiltekna atvinnustarfsemi og má þar nefna sem dæmi að seljendur loðfelda hafa lent í slíku. Til dæmis var vefsíðum þekkts loðskinnasala á Alnetinu breytt af aðilum sem uppsigað var við loðskinnaiðnaðinn.

2. Brot framin með því að nota tölvu

Brot framin með tölvu geta verið margvísleg en flest þeirra eiga það sameiginlegt að með þeim er stefnt að auðgun í einni eða annarri mynd.

1. Auðgunarbrot

Af auðgunarbrotum, sbr. XXVI. kafla almennra hegningarlaga nr. 19/1940, sem koma til greina með notkun tölva má nefna þjófnað, fjárdrátt, fjársvik og umboðssvik. Breytingin á lögunum frá því í vor miðaði að því að styrkja refsiákvæðin um fjársvik og umboðssvik, önnur ákvæði auðgunarbrotakaflans voru talin ná til þess að brot væru framin með tölvum. Breytingin fólst í því að nýrri grein var bætt við hgl. sem nær til þess ef maður á ólögmætan hátt breytir, bætir við eða eyðileggur tölvuvélbúnað, eða gögn eða forrit sem geymd eru á tölvutæku formi, eða hefur með öðrum hætti gert ráðstafanir sem eru til þess fallnar að hafa áhrif á niðurstöðu tölvuvinnslu.

2. Tölva notuð til að leyna broti

Hér er átt við þau tilvik þegar tölva er notuð til þess að eyða slóð eftir brot. Ekki er talið að í slíkum tilvikum komi upp sérstök refsiréttarleg álitaefni þótt tölva sé notuð við að fremja brot.

3. Stuldur á tölvutækum gögnum

Hér er fyrst og fremst átt við að afrituð séu gögn eða upplýsingar sem geymdar eru á tölvutæku formi.

4. Skattsvik

Tölvur hafa oft verið notaðar við ýmiss konar bókhaldsbrot, meðal annars með það að markmiði að hagræða skattskilum. Ekki er talin þörf á sérstökum refsiákvæðum vegna skattabrota þar sem tölvur koma við sögu.

5. Skjalabrot

Rangfærsla upplýsinga og gagna sem geymd eru á tölvutæku formi telst ekki til skjalabrota samkvæmt hefðbundnum viðhorfum í refsirétti. Þar sem viðskipti manna í millum fara í vaxandi mæli fram með tölvusamskiptum er ljóst að þörfin fyrir refsivernd er sú sama og þegar notuð eru skrifleg gögn í hefðbundnum skilningi. Vegna þessa voru gerðar breytingar á þremur þeirra greina almennra hegningarlaga sem fjalla um skjalabrot, til þess að þær næðu og til upplýsinga og gagna sem geymd eru á tölvutæku formi.

3. Óheimil notkun á tölvum

Með þessum tilvikum er átt við það þegar maður nýtir sér tölvu eða tölvubúnað annars manns í heimildarleysi. Annars vegar getur verið um að ræða algjöran heimildarskort, þ.e. þegar notandinn hefur enga heimild, og hins vegar þær aðstæður þegar notandinn fer út fyrir notkunarheimildir sínar, t.d. starfsmaður í atvinnufyrirtæki. Í fyrra tilvikinu mætti vafalaust refsa fyrir nytjastuld ef skilyrðum þess ákvæðis hegningarlaga væri að öðru leyti fullnægt. Sama ætti við um síðara tilvikið ef um mjög alvarlegt brot er að ræða.

4. Innbrot í tölvukerfi

Ljóst er að innbrotstilraunum í tölvukerfi hefur fjölgað verulega á undanförnum árum og búast má við því að þeim fjölgi enn[4].

[4] Viðtal við Arnar Jensson aðstoðaryfirlögregluþjón hjá embætti Ríkislögreglustjóra, Morgunblaðið 10. maí 1998, bls. 24.

Á undanförnu eina og hálfa ári hefur efnahagsbrotadeild Ríkislögreglustjóra rannsakað fjögur innbrot í tölvukerfi. Meðal þeirra eru innbrot í tölvukerfi heilbrigðisfyrirtækis og Alnetsþjónustuaðila.

Ekki er alltaf ljóst hvort markmið með innbrotum í tölvukerfi er að komast að gögnum vegna hnýsni eða í auðgunarskyni eða hvort það er að valda tjóni með hreinni skemmdarstarfsemi. Vitað er að oft er innbrot markmið í sjálfu sér og að komast sem víðast innan kerfisins sem brotist er inn í. Ljóst er að í mörgum innbrotum vinnur tölvuþrjóturinn skemmdarverk þegar hann reynir að fela slóð sína með því að eyðileggja allar skrár sem gefa vísbendingar um það hver hann er. Önnur leið til þess að fela slóð er sú að brjótast inn í tölvukerfi frá tölvukerfi sem viðkomandi tölvuþrjótur hefur áður brotist inn í. Hugsanlega hvílir skaðabótaskylda á ríkisaðila ef tölvuþrjótur hefur notað tölvukerfi hans til innbrota og skemmdarverka í tölvukerfi þriðja aðila.

Ákvæði almennra hegningarlaga um bréfleynd sem flokkast undir brot gegn friðhelgi einkalífs, nær nú einnig til þeirrar háttsemi að maður verði sér úti um aðgang að gögnum eða forritum annarra sem geymd eru á tölvutæku formi. Átt er við það sem á erlendum málum er kallað „hacking“. Brot gegn friðhelgi einkalífs eru einkarefsibrot sem lögreglan rannsakar ekki.

Þegar stór og mikilvæg kerfi ríkisaðila eru sett upp er algengt að fjallað sé um slíkt í fjölmiðlum eða blöðum gefnum út af viðkomandi tölvusala. Þeir síðast nefndu sækjast eðlilega eftir því að koma slíkum upplýsingum á framfæri þar sem þær geta haft mikið auglýsingagildi fyrir þá. Ef í slíkri umfjöllun felst nákvæm lýsing á þeim búnaði sem ríkisaðilar eru að taka í notkun, getur það ýtt undir að þeir sem vita um öryggisveikleika í honum, reyni að nýta sér þá. Benda má í þessu sambandi á, að hugsanlegt er að öryggiskerfi hafi setið á hakanum við uppsetningu nýja tölvukerfisins og að starfsmenn ríkisaðila hafi enn ekki gert sér nægilega vel grein fyrir mögulegum innbrotsleiðum inn í það. Ríkisaðilar ættu því að forðast að veita óviðkomandi

aðilum nákvæmar upplýsingar um hug- og vélbúnað sinn og hvernig uppsetningu hans er háttað.

3. Gerð áhættumats

Áhættumat felst í því að meta mikilvægi upplýsingakerfa fyrir viðkomandi stofnun eða fyrirtæki og hvaða áhættuþættir geta haft áhrif á öryggi kerfanna. Einnig hvaða líkur eru á því að áhættan verði að raunveruleika og valdi truflun eða stöðvun á rekstri viðkomandi og hverjar verði líklegar afleiðingar hennar.

Í kaflanum hér á eftir er fjallað um áhættumat, þörfina á stöðugu endurmati, nauðsyn þess að stofnaður sé öryggishópur til þess að hafa yfirumsjón með öryggismálum á hverjum stað og þau verkefni sem ættu að vera í verkahring hans.

3.1 Mikilvægi upplýsingakerfa

Mikilvægur liður áhættumats er að gera sér grein fyrir þeim verðmætum sem felast í upplýsingakerfum viðkomandi ríkisaðila, þ.e. búnaði, gögnum og upplýsingum. Meginreglan er sú að aðalverðmætin felast í gögnunum sjálfum.

Mismunandi stig rekstraröryggis ræðst af líkum á tjóni sem viðkomandi ríkisaðili getur orðið fyrir, fjárhagslegu eða vegna álitshnekkis, auk þess sem líkur á tjóni starfsmanna og viðskiptavina, vegna þess að tiltekin upplýsingakerfi stofnunar eða fyrirtækis eru ónothæf, skiptir og máli. Ef líklegt er að það valdi áðurnefndum aðilum miklu tjóni ef kerfin eru óvirk, jafnvel þó það sé aðeins í stuttan tíma, þarf rekstraröryggi að vera mikið en ef lengd tímans skiptir ekki öllu kann að vera fjárhagslega hagkvæmt að leggja minna upp úr því.

1. Gögn eru mikilvæg verðmæti

Skilningur á verðmæti gagna og upplýsinga er forsenda þess að gerðar séu nauðsynlegar öryggisráðstafanir til verndar þeim.

Forstöðumenn ríkisaðila ættu ætíð að hafa í huga að upplýsingar og gögn eru bæði mikilvæg verðmæti og nauðsynleg fyrir viðkomandi rekstur. Af þessum sökum verður að vernda þau með sérstökum öryggisráðstöfunum.

2. Flokkun upplýsingakerfa og gagna

Hluti áhættumats felst í flokkun upplýsingakerfa og þeirra gagna og upplýsinga sem þau geyma, eftir mikilvægi þeirra fyrir starfsemi viðkomandi ríkisaðila. Flokkunin er nauðsynleg með tilliti til þess öryggis sem viðhafa þarf vegna einstakra kerfa því það getur verið mismunandi eftir kerfum.

1. Flokkun upplýsingakerfa

Flokka verður hvert upplýsingakerfi eftir því hve nauðsynlegt það er fyrir daglegan rekstur en það fer eftir því og þeim tíma sem ásættanlegt er að það sé óaðgengilegt.

Vegna hvers upplýsingakerfis þarf því að spyrja um lengd þess tíma sem ásættanlegt er að það sé ónothæft. Svarið felur í raun í sér hve mikið rekstraröryggi kerfisins þarf að vera og umfang öryggisráðstafana vegna þess. Rekstur þeirra kerfa sem skilgreind hafa verið sem ómissandi fyrir viðkomandi stofnun eða fyrirtæki krefst eðlilega mun meiri öryggisráðstafana en þeirra sem skipta litlu máli í rekstrinum. Gagnslítið er til dæmis að miða öryggisráðstafanir við að koma tilteknu upplýsingakerfi aftur í notkun tveimur sólarhringum eftir áfall ef starfsemin þolir ekki að missa það í einn sólarhring.

Flokkun upplýsingakerfa nýtist og við gerð neyðaráætlunar bæði hvað varðar nauðsynlegt umfang hennar og vegna ákvarðana um í hvaða röð skuli setja kerfin upp ef tölvukerfið hrynur af einhverjum ástæðum.

Hér á eftir er sýnt dæmi um hvernig hægt er að flokka upplýsingakerfi út frá þeim tíma sem ásættanlegt telst að þau séu óstarfhæf:

1) Óstarfhæft í allt að 1 klukkustund

Starfsemin lamast ef viðkomandi upplýsingakerfi er óstarfhæft. Ásættanleg stöðvun þess er allt að **59 mínútum.**

2) Óstarfhæft í allt að 1 dag

Starfsemin skerðist allverulega ef viðkomandi upplýsingakerfi er óstarfhæft. Ásættanleg stöðvun þess er á bilinu **1 - 24 klukkustundir.**

3) Óstarfhæft í allt að 1 viku

Starfsmenn nota upplýsingakerfið þó nokkuð í daglegu starfi sínu og stöðvun þess hefur í för með sér nokkra skerðingu á þeirri þjónustu sem ríkisaðilinn á að veita. Ásættanleg stöðvun kerfisins er **allt að 7 dögum.**

4) Óstarfhæft í allt að 2 vikur

Starfsemin getur gengið óbreytt í nokkurn tíma án þess að viðkomandi kerfi, t.d. fjárhagsbókhald, sé í gangi, en hefur ekki bein áhrif á getu ríkisaðilans til að veita þá þjónustu sem hann á að veita. Ásættanleg stöðvun kerfisins er á bilinu **8 - 15 dagar.**

5) Óstarfhæft í meira en 2 vikur

Upplýsingakerfið er notað til þess að framkvæma mánaðarlegar vinnslur og ekki kemur að sök þó þær dragist í nokkra daga, þó svo að það valdi

nokkrum óþægindum, t.d. færsla fjárhagsbókhalds hjá litlum aðilum. Ásættanleg stöðvun kerfisins er **lengri en 15 dagar.**

Eins og tekið er fram hér framar er sú flokkun sem hér er sett fram út frá lengd þess tíma sem ásættanlegt telst að upplýsingakerfi stöðvist aðeins sett fram í dæmaskyni og hver og einn ríkisaðili verður að setja slíka flokkun upp út frá sínum eigin forsendum.

2. Flokkun gagna

Mismunandi er hve gögn sem geymd eru í upplýsingakerfum eru viðkvæm gagnvart breytingum eða því að óviðkomandi aðilar geti séð þau. Flokkun gagna er því nauðsynleg eftir því hve mikilvægt er að þær upplýsingar sem í kerfinu eru séu áreiðanlegar, þ.e. réttar, heildstæðar og gildar og hve mikla leynd þarf að viðhafa vegna þeirra. Gögnin geta verið allt frá því að vera viðkvæmar persónuupplýsingar, sem falla undir lög nr. 121/1989 um skráningu og varðveislu persónuupplýsinga, yfir í það að engar hömlur eru settar á aðgang að þeim.

Flokkun gagna þarf líka að fara fram út frá nauðsynlegri tíðni afritatöku þeirra, þ.e. hvort ásættanlegt er að gögn sem skráð voru í upplýsingakerfi í gær, í síðustu viku eða síðasta mánuði, tapist. Það hvort gögn eru til á pappír eða ekki hefur væntanlega áhrif á þessa flokkun.

Af framansögðu er ljóst að flokka þarf gögn og upplýsingar í upplýsingakerfum út frá því öryggisstigi sem nauðsynlegt er til að tryggja varðveislu þeirra.

Í innkaupahandbók RUT-nefndarinnar kemur eftirfarandi fram: *„Öryggiskröfur í tölvumiðstöðvum, er vista miðlæg gögn fyrir hið opinbera, ættu að minnsta kosti að vera á stigi C2 samkvæmt öryggisstaðli varnarmálaráðuneytis Bandaríkjanna.“*

Í Evrópu hefur vegna öryggisflokkunar gagna verið stuðst við annað kerfi en í Bandaríkjunum. Samsvörun er þó á milli þessara kerfa og kemur hún fram í töflunni hér á eftir.

Evrópa	Bandaríkin	Enskt heiti
E0	D	Minimal Protection
E1	C1	Discretionary Security Protection
E2	C2	Controlled Access Protection
E3	B1	Labeled Security Protection
E4	B2	Structured Protection
E5	B3	Security Domains
E6	A1	Verified Design

Hér á eftir verður því nánar lýst hvað felst í þeim öryggisstigum sem varnarmálaráðuneyti Bandaríkjanna hefur skilgreint og skipta máli fyrir ríkisaðila hér á landi, m.a. vegna áðurnefndra leiðbeininga RUT-nefndarinnar. Þessi öryggisstig eru hentug viðmiðun þar sem öll algengustu stýrikerfi tölvukerfa ríkisaðila eiga uppruna sinn í Bandaríkjunum og hafa verið metin eftir þessu kerfi. Oft er vísað til þessara stiga þegar fjallað er um öryggisþætti stýrikerfanna í handbókum þeirra. Rétt er að vekja athygli á því að þó svo að framleiðendur segi að tiltekið kerfi eigi að geta náð t.d. C2 öryggisstigi, þá er ekki víst að það hafi fengið opinbera vottun. Til þess að ganga úr skugga um hvort svo sé, er bent á veffang http://radium.ncsc.mil/tpep/ en þar er að finna upplýsingar um vottun kerfa.

Þess ber að geta hér að í janúar 1996 gáfu Bandaríkin, Bretland, Þýskaland, Frakkland, Kanada, Holland og Belgía sameiginlega út drög að nýjum öryggisstaðli fyrir hinn fjölþjóðlega markað. Númer staðalsins mun væntanlega verða ISO/IEC 15408 og heiti hans „Common Criteria for Information Technology Security Evaluation“ (CCITSE) en venjulega er vísað til hans sem „Common Criteria“ (CC). Í honum er skilgreint í hvaða tilgangi neytendur, hönnuðir og matsmenn geta notað hann. Hér skal dæmi tekið af neytendum en þeir eiga að geta notað staðalinn til þess að:

1) Finna þann flokk öryggisráðstafana sem fellur að áhættumati þeirra.

2) Finna þær vörur sem viðurkennt hefur verið að falli undir þann flokk.

3) Birta öryggiskröfur sínar til þess að seljendur tölvubúnaðar geti hannað vörur sem uppfylla þær.

Samkvæmt upplýsingum Staðlaráðs Íslands eru áðurnefnd staðladrög ófrágengin og ekki vitað hvenær þau verða samþykkt.

Þar sem nýi ISO-staðallinn hefur enn ekki tekið gildi verður í greinargerð þessari að styðjast við öryggisstaðal varnarmálaráðuneytis Bandaríkjanna. Hér á eftir verða í stórum dráttum rakin einkenni þeirra þriggja öryggisstiga sem flest kerfi ríkisaðila hér á landi falla nú undir.

1) Öryggisstig D

Til öryggisstigs D teljast óörugg tölvukerfi eða kerfi sem ekki hafa verið öryggismetin. Samsvarandi stig er í Evrópu auðkennt með **E0**.

Kerfi sem lenda í þessu stigi geta haft ýmsa öryggisþætti innbyggða þó svo að þeir standist ekki þær kröfur sem gerðar eru í stigi C1.

2) Öryggisstig C1

Til öryggisstigs C1 teljast tölvukerfi þar sem aðgangur að kerfinu er bundinn við minnstu kröfur sem hægt er að gera um aðgangstakmarkanir. Samsvarandi stig er í Evrópu auðkennt með **E1**.

Í tölvukerfum sem teljast til öryggisstigs C1 þurfa eftirfarandi skilyrði að vera uppfyllt:

2.1 Aðgangur er takmarkaður með aðgangsorði. Notandi þarf að skrá það áður en önnur samskipti eru möguleg við tölvukerfið.

2.2 Aðgangur að uppsetningu og eyðingu aðgangsorða er eingöngu heimill þeim sem hafa kerfisstjóraréttindi.

3) Öryggisstig C2

Til öryggisstigs C2 teljast tölvukerfi þar sem strangar aðgangstakmarkanir eru að kerfinu og hægt er að halda dagbók sem gefur upplýsingar um hver gerir hvað og hvenær. Samsvarandi stig er í Evrópu auðkennt með **E2**.

Í tölvukerfum sem ná C2 öryggisstigi þurfa eftirfarandi skilyrði að vera uppfyllt auk skilyrðanna sem eru í stigi C1:

3.1 Við hverja aðgerð á tölvukerfið að geta greint hvaða notandi framkvæmir hana.

3.2 Aðgangsorð að tölvukerfinu eru tengd tilteknum einstaklingum og þeir einir eiga að geta notað þau.

3.3 Hægt er að hindra tiltekinn notanda eða hóp notenda í því að fá aðgang að tilteknum skrám eða skráarsöfnum.

3.4 Mögulegt er að takmarka aðgang notenda við lestur skráa, þ.e. þeir geta ekki breytt skrám.

3.5. Notendur eru gerðir ábyrgir fyrir aðgangi sínum og engin hóplykilorð eru leyfileg.

3.6 Hægt er að halda dagbók („log-skrá“) yfir atburði í kerfinu. Þess er krafist að eftirfarandi upplýsingar séu fyrirliggjandi í dagbókinni:

a) Vegna notkunar á aðgangsforritum:

   Dagsetning, tími, notendaauðkenni, númer jaðartækis (skjánúmer) og hvort aðgangstilraun heppnaðist eða mistókst.

b) Vegna tilrauna til þess að fá aðgang að skrám sem háðar eru aðgangstakmörkunum:

   Dagsetning, tími, notendaauðkenni, skráarheiti og hvort aðgangstilraun heppnaðist eða mistókst.

c) Vegna skráa sem búnar eru til eða eytt ef þær eru háðar aðgangstakmörkunum:

   Dagsetning, tími, notendaauðkenni, tegund aðgerðar og heiti skráar sem tengist aðgerðinni, t.d. að búa til eða eyða notendanafni, stöðva eða ræsa kerfi o.s.frv.

3.7 Hægt er að setja svokallaða endurskoðunarslóð á aðgerðir einstakra notenda.

3.2 Stofnun öryggishóps

Stofnanir og fyrirtæki ríkisins þurfa að koma á fót sérstökum vinnuhópi vegna öryggis upplýsingakerfa sinna eða fela einum aðila að sjá um þau ef stofnun er fámenn. Í öryggishópnum þarf að vera til staðar bæði sérþekking á viðfangsefnum viðkomandi ríkisaðila og öryggi upplýsingakerfa. Stærri ríkisaðilar ættu að leita til utanaðkomandi öryggissérfræðinga ef ekki til staðar næg þekking innan stofnunar eða fyrirtækis.

Öryggishópur á að:

1) Safna saman á einn stað þekkingu á öryggismálum upplýsingakerfa og viðhalda henni.

2) Meta áhættu og endurskoða matið reglulega. Við matið skal hafa að leiðarljósi að beint samhengi sé á milli öryggis upplýsingakerfa og þeirra hagsmuna sem í húfi eru ef viðkomandi stofnun eða fyrirtæki getur ekki sinnt hlutverki sínu.

3) Kanna þær öryggisráðstafanir sem hann telur koma til greina til þess að bregðast við áður metinni áhættu.

4) Kynna forstöðumanni viðkomandi ríkisaðila áhættumat sitt og þær öryggisráðstafanir sem hópurinn telur færar til verndar upplýsingakerfunum. (Á grundvelli þessa mótar forstöðumaðurinn öryggisstefnu vegna upplýsingakerfa og velur þær öryggisráðstafanir sem hann telur best henta til þess að ná markmiðum hennar).

5) Endurskoða áhættumat sitt reglulega og endurmeta einnig reglulega þær öryggisráðstafanir sem viðhafðar eru til verndar upplýsingakerfum viðkomandi ríkisaðila.

6) Fylgjast reglulega með því að starfsmenn virði þær öryggisráðstafanir sem ákveðnar hafa verið.

7) Sjá til þess að tekið sé tillit til öryggissjónarmiða strax við hönnun og gerð nýrra upplýsingakerfa.

8) Gera neyðaráætlun, prófa hana og viðhalda reglulega.

Til þess að tryggja að öryggishópar geti sem best sinnt verkefnum sínum þurfa forstöðumenn ríkisaðila að tryggja þeim, sem í þeim starfa, svigrúm til þess innan reglulegs vinnutíma þeirra. Jafnframt þarf að tryggja tæknilega og faglega þekkingu hópsins.

3.3 Hætta sem steðjað getur að öryggi kerfanna

Í 2. kafla greinargerðar þessarar er fjallað um nokkra helstu áhættuþætti í rekstri upplýsingakerfa. Við framkvæmd áhættumats þarf öryggishópurinn að gera sér grein fyrir mögulegum ógnunum sem steðjað geta að upplýsingakerfum viðkomandi stofnunar eða fyrirtækis, veikleikum þeirra og þeim áhrifum sem þetta hvort tveggja getur haft á rekstrarhæfi kerfanna, gæði gagna og gagnaleynd. Ljóst er að áhætta er mismikil m.a. eftir eðli starfseminnar.

Við áhættumat skiptir mestu máli að gera sér grein fyrir tiltekinni hættu og bregðast við henni á skynsamlegan hátt, þ.e. með öryggisráðstöfunum sem leiða til þess sem í greinargerð þessari er nefnt „viðunandi öryggisstig“, sbr. nánar kafla 5.1 um val á öryggisráðstöfunum.

3.4 Líkur á því að áhætta verði að raunveruleika

Ekki er skynsamlegt fyrir öryggishópinn að reyna að meta mjög nákvæmlega líkurnar á því að tilteknir áhættuþættir valdi truflun á rekstri upplýsingakerfa viðkomandi með því að gefa ógnunum vægi í tölum né heldur að meta nákvæmlega fjárhagslegt tjón ef til slíks kæmi. Heppilegra er að meta hvort áhætta sé mikil eða lítil. Ástæðan er sú að nákvæmar upplýsingar um tíðni óhappa af völdum tiltekinna áhættuþátta liggja yfirleitt ekki fyrir, því oft er raunveruleg ástæða óhapps óþekkt og einnig gætir tilhneigingar til þess að halda tilteknum tegundum óhappa leyndum. Einnig er

ofangreint mat tímafrekt og erfitt er að staðfesta það og endurskoða.

Af framangreindum ástæðum er erfitt, ef ekki ómögulegt, að ákvarða nákvæmlega hvaða öryggisráðstafanir eru hagkvæmastar á grundvelli samanburðar á kostnaði við tilteknar öryggisráðstafanir og hugsanlegu tjóni vegna ónógs öryggis. Öryggishópar verða því við áhættumat hverju sinni að treysta á bestu fáanlegu upplýsingar og eigin dómgreind. Upplýsingar um ógnanir og veikleika má fá úr fagtímaritum um tölvumál, fréttabréfum frá aðilum sem sérhæfa sig í öryggismálum upplýsingakerfa og fagfélögum þeirra sem tengjast tölvugeiranum, auk eigin reynslu. Við líkindamat verður öryggishópurinn alltaf að hafa í huga að varasamt getur verið að styðjast við upplýsingar sem safnað hefur verið varðandi tölvuumhverfi sem er gjörólíkt því sem nú er verið að meta, m.a. vegna örra tæknilegra framfara.

Eftir að áhætta hefur verið skilgreind og flokkuð sem annað hvort mikil eða lítil, skal öryggishópurinn benda á hagkvæmustu öryggisráðstafanir sem hægt er að viðhafa til þess að draga úr þeirri áhættu sem hann telur að sé fyrir hendi. Ákvörðunin um öryggisráðstafanir er forstöðumannsins sem tekur við valið tillit til eðlis gagna og upplýsinga, mikilvægis þeirra fyrir starfsemi viðkomandi og kostnaðar við ráðstafanirnar.

Hver ríkisaðili fyrir sig þarf að þróa hentugar aðferðir við áhættumat þar sem beint samband er á milli öryggis upplýsingakerfa og þeirra hagsmuna, sem í húfi eru, ef viðkomandi stofnun eða fyrirtæki getur ekki sinnt hlutverki sínu.

3.5 Hugsanlegar afleiðingar rekstrartruflana

Afleiðingar þess að öryggi upplýsingakerfa er ekki nægilegt geta verið ýmsar. Í Innkaupahandbók um upplýsingatækni

1998, telur RUT-nefndin upp í eftirfarandi fimm liðum, dæmi um afleiðingar öryggisslysa:

1) **Töpuð verðmæti**

   Orsök þess getur verið þjófnaður á gögnum, forritum, vélum eða vinnslutíma, eða að fjármagnsflutningur eigi sér stað vegna heimildarlauss aðgangs að fjárumsýslukerfum. Þá getur tap hlotist af bilunum, svo sem í geymslumiðlum eða vegna mistaka.

2) **Skert réttaröryggi**

   Um það getur verið að ræða, t.d. vegna þess að rangar upplýsingar eða síðbúin uppfærsla gagna verður til þess að ákvarðanir eru teknar á röngum forsendum.

3) **Leyndarrof**

   Þetta þýðir að einhver utanaðkomandi kemst viljandi eða óviljandi í trúnaðarupplýsingar. Ef um er að ræða upplýsingar um hagi einstaklinga getur það varðað við lög um skráningu og meðferð persónuupplýsinga.

4) **Glatað trúnaðartraust**

   Um það getur verið að ræða t.d. ef að villur í gögnum, gölluð kerfi eða misnotkun þeirra leiðir til þess að almenningur treystir ekki lengur opinberum stofnunum.

5) **Tap vegna rekstrarstöðvunar**

   Rekstrarstöðvun getur kostað yfirvinnugreiðslur, seinkun á afgreiðslu og tjón hjá viðskiptavinum.

Upptalningin hér að ofan nær m.a. til dæma sem varða leynd og gæði gagna en umfjöllun um þau atriði er utan

megin umfjöllunarefnis greinargerðar þessarar eins og áður hefur verið bent á.

3.6 Svör að loknu áhættumati

Að loknu áhættumati eiga að liggja fyrir svör við eftirfarandi spurningum:

1) Hversu mikið þarf rekstraröryggi upplýsingakerfa að vera, þ.e. hve langan tíma er ásættanlegt að einstök upplýsingakerfi séu óstarfhæf?

2) Hversu mikið þarf varðveisluöryggi gagna að vera, þ.e. hvað er ásættanlegt að gögn sem sett hafa verið inn í kerfið tapist langt aftur í tímann og hve mikinn kostnað hefur það í för með sér ef endurskrá þarf þau?

3) Hve mikil þarf gagnaleyndin að vera, þ.e. eru viðkvæmar persónuupplýsingar geymdar í kerfinu eða eru gögn þess eðlis að engar hömlur eru settar á aðgang að þeim?

4) Hversu mikilvægt er að þær upplýsingar sem í kerfinu eru séu áreiðanlegar, þ.e. réttar, heildstæðar og gildar?

3.7 Endurmat áhættu

Vegna hraðrar þróunar upplýsingatækninnar þarf stöðugt að endurskoða öryggi upplýsingakerfa til þess að tryggt sé að öryggisráðstafanir séu bæði viðeigandi og virkar. Stöðugt áhættumat er liður í heildarendurskoðun á öryggi upplýsingakerfa.

Meðal þeirra breytilegu þátta sem tengjast áhættumati vegna upplýsingakerfa, eru áhættuþættir sem tengjast högun upplýsingakerfa, tæknilegum þáttum, þekktum veikleikum hugbúnaðar, sjálfvirkni upplýsingakerfa og rafrænum sendingum gagna.

4. Mótun öryggisstefnu

Þar sem öryggi er huglægt hugtak er nauðsynlegt að skilgreina öryggismarkmið vel áður en þær ráðstafanir sem eiga að ná þeim eru valdar.

4.1 Ábyrgð forstöðumanna á öryggi upplýsingakerfa

Í 13. kafla Innkaupahandbókar RUT-nefndarinnar, sem fjallar um öryggismál, er sérstakur kafli um öryggisstefnu og er í honum sett fram eftirfarandi regla: *„Stjórnendur stofnana þurfa að taka virkan þátt í mótun öryggismálastefnunnar. Ella næst ekki viðunandi öryggi.“*

Vegna mikilvægis upplýsingakerfa fyrir rekstur stofnana og fyrirtækja ríkisins ætt eitt af hlutverkum forstöðumanna þeirra að vera að taka endanlegar ákvarðanir um umfang þeirra öryggisráðstafana, sem beita á, til þess að vernda eigið upplýsingakerfi ásamt þeim gögnum og upplýsingum sem það geymir. Þetta þýðir með öðrum orðum að forstöðumenn bera ábyrgð á rekstraröryggi upplýsingakerfis stofnunar sinnar eða fyrirtækis á sama hátt og þeir bera ábyrgð á öðrum þáttum rekstrarins. Því er eðlilegt að þeir meti hvaða gögn og upplýsingar eru nauðsynlegar til þess að reksturinn gangi sem eðlilegast fyrir sig, hverjar afleiðingarnar eru ef gögn eru ekki í lagi, gagnaleynd er rofin eða gögn eru ekki aðgengileg.

Vegna ábyrgðar forstöðumanna á upplýsingakerfum ríkisaðila ættu meðal mikilvægustu verkefna þeirra að vera að:

1) Móta viðeigandi öryggisstefnu vegna upplýsingakerfa og ákveða þær öryggisráðstafanir sem ná

eiga markmiðum hennar. Fyrirliggjandi áhættumat er forsenda þess að hægt sé að móta öryggisstefnu og ákveða öryggisráðstafanir.

2) Ganga úr skugga um það með reglulegu millibili að þær öryggisráðstafanir sem ákveðnar hafa verið nái markmiðum öryggisstefnunnar.

3) Ganga úr skugga um það með reglulegu millibili að starfsmenn og stjórnendur virði þær öryggisráðstafanir sem ákveðnar hafa verið.

Umfang ofangreindra verkefna og með hve formlegum hætti þau eru framkvæmd er háð umfangi tölvuvinnslu og mikilvægi hennar fyrir viðkomandi ríkisaðila.

Vert er að fjalla sérstaklega um ábyrgð forstöðumanna í þeim tilvikum þegar upplýsingakerfi viðkomandi ríkisaðila er varðveitt hjá öðrum. Í samningi stofnunar eða fyrirtækis við sérhæfða tölvumiðstöð um varðveislu og þjónustu við tiltekið upplýsingakerfi ætti að taka fram í hverju nauðsynlegar öryggisráðstafanir skuli felast. Með þeim skal reynt að vernda mikilvæg gögn og upplýsingar sem viðkomandi kerfi geymir, kerfið sjálft og annan búnað sem nauðsynlegur er til að tryggja öryggi viðkomandi upplýsingakerfis. Í þessum tilvikum tekur forstöðumaður ríkisaðila í raun ákvarðanir um þær öryggisráðstafanir sem viðhafa skal en hann felur öðrum framkvæmd þeirra. Rétt er að geta þess að dæmi eru um það, sbr. hin svokölluðu landskerfi, að ráðherra skrifi undir slíkan samning en ekki einstakir forstöðumenn. Vísti ríkisaðili eigið upplýsingakerfa krefst það vinnu við öryggisgæslu sem þeir ríkisaðilar sem geyma upplýsingakerfi sín í sérhæfðum tölvumiðstöðvum, losna að hluta til við.

Framangreind ábyrgð forstöðumanna leiðir til þess að þeir starfsmenn sem eru sérfræðingar um öryggi upplýsingakerfa, t.d. yfirmenn tölvudeilda viðkomandi stofnunar eða fyrirtækis, bera ábyrgð á öryggi upplýsingakerfa gagnvart forstöðumanni en ábyrgð gagnvart utanaðkomandi aðilum er

hjá forstöðumanninum sjálfum. Yfirmenn tölvudeilda gegna hins vegar mjög veigamiklu fræðslu- og ráðgjafarhlutverki gagnvart forstöðumönnum, sem felst m.a. í því að upplýsa þá um þá áhættuþætti sem haft geta áhrif á öryggi upplýsingakerfanna og þá þörf og möguleika sem eru á því að bregðast við þeim. Öryggissérfræðingar eru jafnframt lykilmenn í hópi sem nauðsynlegt er að setja á laggirnar til þess að huga með reglubundnum hætti að öryggismálum upplýsingakerfa viðkomandi ríkisaðila. Ef sérþekking á öryggismálum í upplýsingakerfum er ekki til staðar hjá ríkisaðila og mikið er í húfi að þessi mál séu í lagi þyrfti ríkisaðilinn að leita til sérfræðinga á þessu sviði.

4.2 Þörf á opinberri samræmingu öryggismála

Mikilvægt er að starfandi sé á vegum ríkisins nefnd eða hópur sem samræmir aðgerðir í öryggismálum upplýsingakerfa stofnana og fyrirtækja ríkisins.

Í bæklingnum „Íslenska upplýsingasamfélagið - Álitsgerð starfshópa“, sem gefinn var út af ríkisstjórn Íslands í október 1996, eru skilgreind tvö markmið vegna opinberrar stjórnsýslu:

> *„1) Beita skal upplýsingatækninni í allri starfsemi hins opinbera í þeim tilgangi að bæta þjónustu þess við almenning og fyrirtæki, auka skilvirkni og lækka kostnað.*
>
> *2) Allir landsmenn skuli hafa jafnan aðgang að opinberri þjónustu.“*

Í bæklingnum eru síðan skilgreindar 8 meginleiðir sem fara skal til að ná ofangreindum markmiðum. Í 5. leið, sem fjallar um skipulag, öryggi, aðgengi og verðlagningu gagna, segir m.a.:

> *„Skilgreina skal öryggiskröfur sem gera þarf vegna varðveislu, reksturs og leyndar gagna í vörslu opinberra aðila.“*

Í kaflanum um framkvæmd og ábyrgð á leiðunum segir í 5. lið, sem ber yfirskriftina „Skipulag og öryggi gagna“ :

> *„Skipaður verði starfshópur á vegum fjármálaráðuneytis til að vinna að samræmingu og skilgreiningu á öryggiskröfum gagnasafna í vörslu hins opinbera. Starfshópurinn verði skipaður fulltrúum hagsmunaaðila.“*

Fjármálaráðuneytið hefur enn ekki skipað þennan starfshóp. Hins vegar hefur RUT-nefndin, þ.e. ráðgjafanefnd um upplýsinga- og tölvumál, sem starfar á vegum fjármálaráðuneytis og verkefnisstjórnar um framkvæmd upplýsingastefnu, stuttlega fjallað um og skilgreint kröfur til öryggis upplýsingakerfa í Innkaupahandbók um upplýsingatækni 1998 sem víða er vitnað til í greinargerð þessari.

4.3 Mótun öryggisstefnu

Öryggisstefna er sá grundvöllur sem öryggisráðstafanir byggja á, þ.e. hún kallar á að tekið sé upp sérstakt verklag og tæknilegir eftirlitsþættir til þess að tryggja öryggi upplýsingakerfa viðkomandi ríkisaðila. Eins og áður hefur komið fram er áhættumat undanfari mótunar öryggisstefnu og forsenda þess að hægt sé að setja hana fram. Skýrt skal greina á milli öryggisstefnu og þeirra öryggisráðstafana sem eiga að tryggja að markmiðum hennar sé náð.

Öryggisstefna á að liggja fyrir í örstuttu máli, helst á einni A4 blaðsíðu. Öryggisráðstöfunum skal hins vegar lýsa í öðru skjali í mun ýtarlegra máli. Skjalfesting öryggisstefnu og þeirra öryggisráðstafana sem ákveðnar eru, hefur í för með sér að auðveldara er að koma upplýsingum um þær á framfæri við þá sem málið varðar, hvort sem það eru starfsmenn, samstarfsaðilar eða viðskiptavinir viðkomandi.

Hver stofnun og fyrirtæki ríkisins þarf að móta sérstaka öryggisstefnu vegna upplýsingakerfa sinna. Í öryggisstefnu eiga að birtast þau meginmarkmið sem viðkomandi ríkisaðili stefnir að því að ná með öryggisráðstöfunum sínum.

Í öryggisstefnu vegna upplýsingakerfa eiga einungis að koma fram þau atriði sem forstöðumenn telja að leggja eigi höfuðáherslu á varðandi öryggi þeirra. Dæmi um atriði sem eiga heima í öryggisstefnu eru t.d.:

a) Yfirlýsing um mikilvægi þeirra gagna sem geymd eru í upplýsingakerfum viðkomandi ríkisaðila og hverjar geta orðið afleiðingarnar ef öryggi þeirra er ekki tryggt.
b) Yfirlýsing um þá ábyrgð vegna öryggismála upplýsingakerfa sem felst í tilteknu starfi. Hér þarf m.a. að greina á milli ábyrgðar forstöðumanns, öryggishóps og almennra starfsmanna.
c) Yfirlýsing um að áhersla sé lögð á að stjórnendur og starfsmenn þekki öryggisstefnu viðkomandi og skilji forsendur hennar þar sem slíkt auki líkurnar á ábyrgri hegðun þeirra og þar með því að þeir virði þær öryggisráðstafanir sem forstöðumaður hefur valið til að tryggja öryggi upplýsingakerfa viðkomandi ríkisaðila.

Í kafla 4.6 hér á eftir er sýnt hvernig öryggisstefna stofnunar getur litið út.

4.4 Skilningur starfsmanna mikilvægur

Með tilkomu staðarneta, Alnetsins og tölvupósts, hafa flestir tölvunotendur hjá ríkisaðilum nú aðgang að gífurlegu magni upplýsinga og geta átt samskipti við mikinn fjölda annarra tölvunotenda á einfaldan og hraðvirkan hátt. Þessu fylgir ýmis hætta m.a. sú að nettengingar margfalda líkur á því að vandamál á einni tölvu geti haft áhrif á allar tölvur á

viðkomandi neti. Til þess að draga úr þeirri hættu er nauðsynlegt að fræða starfsmenn um öryggismál.

Mikilvægt er að forstöðumenn stofnana og fyrirtækja ríkisins kynni starfsmönnum sínum gildandi öryggisstefnu vegna upplýsingakerfa viðkomandi og þær öryggisráðstafanir sem tryggja eiga að markmið hennar náist. Starfsmenn eru líklegri til þess að virða öryggisráðstafanir ef þeir hafa skilning á tilgangi þeirra og þeirri ábyrgð sem hvílir á þeim sjálfum til þess að tryggja rekstraröryggi upplýsingakerfanna.

Líta ætti á eftirlit með öryggisráðstöfunum sem þjónustu í stað þess að telja hlutverk þess eingöngu það að þvinga starfsmenn til þess að fylgja settum reglum. Þetta viðhorf byggir á þeirri forsendu að almennur skilningur sé á tilgangi og markmiðum öryggisráðstafana og þær seú almennt viðurkenndar.

4.5 Öryggisstefnu þarf sífellt að endurmeta

Miklu af því eftirliti sem hafa þarf með öryggi í upplýsingakerfum má sinna með sérstökum hugbúnaðareftirlitskerfum sem stöðugt fylgjast með fyrirfram skilgreindum öryggisatriðum. Ef fyrirfram skilgreind vandamál koma upp gera kerfin þegar viðvart þannig að umsjónarmenn þeirra geta gripið til viðeigandi ráðstafana.

Áður er komið fram að sífellt þarf að fylgjast með og endurmeta þá hættu sem steðjað getur að upplýsingakerfum viðkomandi ríkisaðila. Breyttir áhættuþættir kalla á endurmat öryggisstefnu og hugsanlega breyttar öryggisráðstafanir.

4.6 Dæmi um öryggisstefnu

Eftirfarandi er dæmi um það hvernig öryggisstefna ríkisstofnunar gæti litið út.

Öryggisstefna vegna upplýsingakerfa stofnunarinnar

- Gögn og upplýsingar í upplýsingakerfum stofnunarinnar eru mikilvæg verðmæti og nauðsynleg fyrir rekstur hennar. Því þarf að vernda þau með sérstökum öryggisráðstöfunum. Afleiðingar þess að öryggis upplýsingakerfis er ekki gætt geta m.a. orðið þær að:

  1) Stofnunin missir traust almennings.
  2) Leynd vegna viðkvæmra upplýsinga um persónuleg og fjárhagsleg málefni er rofin.
  3) Viðkvæm gögn tengd rekstrinum komast í hendur óviðkomandi aðila.
  4) Stofnunin getur orðið skaðabótaskyld vegna ólögmætra athafna eða skemmdarverka sem framin hafa verið með tölvubúnaði hennar og baka þriðja manni tjón.
  5) Tölvu- og netbúnaður stofnunar, ásamt gögnum hennar, er misnotaður eða eyðilagður.
  6) Fjársvik eiga sér stað.
  7) Dýr og rekstrartruflandi atvik koma upp.
  8) Ekki er fylgt lögum og reglugerðum.
  9) Innan stofnunar skapast neikvætt andrúmsloft sem haft getur óæskileg áhrif.
  10) Grunur getur fallið á saklausa starfsmenn vegna skemmdarverka eða fjársvika sem gerð eru á aðgangsorði þeirra.

- Alltaf skal liggja fyrir skrifleg verkaskipting innan stofnunarinnar. Í henni eru skilgreind tiltekin störf ásamt þeirri ábyrgð sem þeim fylgir og hverjar eru aðgangsheimildir að upplýsingakerfum stofnunarinnar. Fram skal og koma fram hvaða starfsmenn gegna hverju starfi fyrir sig. Lykilstörfum skal úthlutað til fleiri en eins starfsmanns.

- Markvisst skal unnið að því að allir starfsmenn stofnunarinnar þekki öryggisstefnu og forsendur hennar, til þess að auka líkur á því að þeir fylgi þeim öryggisráðstöfunum sem ákveðnar hafa verið til þess að tryggja öryggi upplýsingakerfa stofnunarinnar.

4.7 Öryggisstefna einstakra ráðuneyta og stofnana

Ýmis ráðuneyti og stofnanir hafa tekið saman og sett sér öryggisstefnu. Hér verður tekið dæmi um eina slíka.

Heilbrigðis- og tryggingamálaráðuneytið gaf á árinu 1997 út bækling um „Stefnumótun í upplýsingamálum innan heilbrigðiskerfisins“. Í honum er sérstakur kafli um öryggismál og segir þar:

„Upplýsingakerfi heilbrigðisstofnana og heilbrigðisnet þurfa að uppfylla strangar öryggiskröfur. M.a. þarf að tryggja að varðveisla og aðgengi að tölvutækum gögnum sé jafngott eða betra en að pappírsgögnum. Unnt er að gera mismiklar öryggiskröfur til einstakra þátta netsins.“

Í bæklingnum er spurt hvað felist í öryggi. Ráðuneytið svarar því á eftirfarandi hátt:

> „Að gögn séu rétt og aðgengileg þeim sem aðgangsrétt hafa þegar þörf er á.
>
> Að gögn séu óaðgengileg fyrir óviðkomandi.
>
> Að gögn séu varin gegn þjófnaði, eldi, náttúruhamförum o.þ.h.
>
> Að alltaf séu til áreiðanleg afrit af gögnum.
>
> Að gögn sem fara um net komist til rétts viðtakanda ósködduð og á réttum tíma.“

Markmiðið með öryggisstefnu Heilbrigðis- og tryggingamálaráðuneytisins er að:

> „Áreiðanlegar upplýsingar verði aðgengilegar fyrir þá sem aðgangsrétt hafa en allar upplýsingar verði óaðgengilegar fyrir óviðkomandi.“

Í bæklingnum er síðan lýst þeim leiðum sem fara á til þess að ná ofangreindu markmiði. Þær lýsa í raun þeim verkefnum sem vinna þarf vegna öryggismála og ýmsum grundvallarreglum sem gilda skulu. Ljóst er að þær verða heilbrigðisstofnanir að hafa í heiðri en á hverjum og einum stað þarf að útfæra reglurnar eftir því sem við á.

5. Öryggisráðstafanir

Eftir að öryggishópurinn hefur framkvæmt áhættumat vegna upplýsingakerfa stofnunar eða fyrirtækis, þ.e. viðurkennt og flokkað tiltekna áhættu sem mikla eða litla, og forstöðumaður mótað öryggisstefnu á grundvelli þessa, er næsta skref að öryggishópurinn kanni þær öryggisráðstafanir sem koma til greina til þess að ná fram markmiðum öryggisstefnunnar og draga úr þeirri áhættu sem steðjað getur að upplýsingakerfunum. Að lokinni þessari könnun gerir hópurinn forstöðumanni grein fyrir því hvaða öryggisráðstafanir hópurinn telur koma til greina og hverjar þeirra hann telur hagkvæmastar.

Endanleg ákvörðun um öryggisráðstafanir liggur hjá forstöðumanni sem tekur við valið tillit til eðlis gagna og upplýsinga, mikilvægis þeirra fyrir starfsemi viðkomandi og kostnaðar við ráðstafanirnar.

Eins og fram kom í kaflanum um öryggisstefnuna bera forstöðumenn ábyrgð á öryggi upplýsingakerfa stofnunar sinnar eða fyrirtækis. Þetta felur m.a. í sér að þeir þurfa að taka endanlegar ákvarðanir um val á þeim öryggisráðstöfunum sem vernda eiga upplýsingakerfi viðkomandi.

Lýsing á öryggisráðstöfunum á að vera skrifleg til þess að öllum notendum upplýsingakerfanna séu þær ljósar, hægt sé að meta fylgni starfsfólks við þær og virkni þeirra til verndar upplýsingakerfunum.

Í RUT-handbókinni 1998 segir svo á bls. 95: *„Umfangi og skipulagi öryggismála verði lýst í öryggishandbók, sem sniðin er að aðstæðum á hverjum stað. Í henni skal lýst þeim öryggisþáttum sem tilgreindir eru í kaflanum hér að framan. Taka ber tillit til ISO 7498-2.“*

Hugtakið öryggisráðstafanir er í greinargerð þessari notað í víðri merkingu og nær það til allra þeirra ráðstafana sem gerðar eru til þess að tryggja öryggi upplýsingakerfa viðkomandi ríkisaðila.

Öryggisráðstöfunum má skipta í eftirfarandi þrjá flokka:

1) Stjórnunar- og skipulagsráðstafanir.
2) Umhverfis og aðbúnaðarráðstafanir.
3) Tæknilegar ráðstafanir.

Stuðst verður við þessa flokkun hér á eftir og fjallað um hvern flokk fyrir sig. Flokkunin er sú sama og byggt er á í RUT-handbókinni 1998.

5.1 Val á öryggisráðstöfunum

Öryggisráðstafanir skal sníða að þjónustu- og viðskiptalegum þörfum viðkomandi ríkisaðila í stað þess að taka upp almennar kröfur um þær án mats á því hvort þær eiga við eða ekki. Árangursrík útfærsla á öryggisráðstöfunum gerir bæði kröfu til þess að þær séu valdar af kostgæfni og að stöðugt sé fylgst með því hvort þær skila tilætluðum árangri eða ekki.

Eins og fram kom í 3. kafla um gerð áhættumats er flokkun upplýsingakerfa og þeirra gagna og upplýsinga sem þau geyma, liður í slíku mati. Flokkun kerfa felst í því að meta hve lengi hægt er að una því að hvert upplýsingakerfi sé óvirkt. Um flokkun gagna má segja að ef gögn eru ekki viðkvæm fyrir því að óviðkomandi aðilar geti séð þau, en einhver þeirra eru hins vegar viðkvæm gagnvart breytingum, þarf öryggiskerfið að miða að því að tryggja að ekki geti aðrir breytt gögnunum en þeir sem til þess hafa sérstaka heimild. Ef gögn eru það viðkvæm að utanaðkomandi aðilar mega alls ekki komast í þau þarf öryggiskerfið að taka mið af þeirri staðreynd. Út úr áhættumati eiga því að koma svör

við því hve umfangsmiklar öryggisráðstafanir vegna hvers upplýsingakerfis fyrir sig þurfa að vera.

Í 3. kafla um áhættumat kom og fram að ekki liggja yfirleitt fyrir mjög áreiðanlegar líkinda- og kostnaðartölur sem hægt er að nota við áhættumat. Það sama gildir um kostnað af tilteknum öryggisráðstöfunum. Við val á þeim verða forstöðumenn því að treysta á bestu fáanlegar upplýsingar og eigin dómgreind. Hér má ekki gleyma því mikilvæga hlutverki sem öryggishópurinn gegnir við að upplýsa forstöðumann viðkomandi stofnunar eða fyrirtækis um þá möguleika sem til staðar eru.

Val á öryggisráðstöfunum byggist alltaf á því hvað telst vera viðunandi öryggi. Þegar meta skal hvað telst viðunandi öryggi, þarf m.a. að hafa í huga að ríkisstofnanir og ríkisfyrirtæki skulu að jafnaði einungis kaupa þær tryggingar sem skylt er að hafa lögum samkvæmt, sbr. rgl. 33/1988 um kaup ríkisins á vátryggingum. Meginreglan er að ríkisaðilum er hvorki heimilt að kaupa rekstrarstöðvunartryggingar né aðrar frjálsar vátryggingar. Samkvæmt reglugerðinni er tjón á munum í eigu ríkisins, eða tjón sem það ber ábyrgð á samkvæmt lögum, réttarvenju eða samningum, í sjálfsáhættu viðkomandi ríkisaðila og greiðist af rekstrar- og framkvæmdafé hans. Ef um meira tjón er að ræða en að það verði greitt af rekstrar- og framkvæmdafé viðkomandi, er heimilt að sækja um sérstaka fjárveitingu vegna þess. Verði eignatjón skal fjármálaráðuneytið í samráði við ráðuneyti stofnunar meta hvort eign verði endurnýjuð og hvað teljist hæfilegar bætur fyrir hana. Því má segja að ríkissjóður baktryggi ríkisaðila með óbeinum hætti vegna atvika sem þeir væru væntanlega tryggðir gegn ef slíkt væri heimilt. Þrátt fyrir þetta er nauðsynlegt að ríkisaðilar viðhafi viðunandi rekstraröryggi.

Ekki er raunhæft að gera ráð fyrir því að hægt sé að ná hinu fullkomna 100% öryggi. Vegna tæknilegra öryggisráðstafana má benda á að ef mikið er um innbyggð öryggisatriði í upplýsingakerfum, getur hefðbundin notkun þeirra orðið flókin og seinvirk. Dýrt er að starfsmenn eyði stórum hluta vinnutíma síns og tölvur afli sínu í það að glíma við alls kyns öryggiskerfi. Annar ókostur hás öryggisstigs er að það getur leitt til þess að starfsmenn sinni ekki villum eða til-

kynningum um þær því þeir halda að eftirlitskerfið muni sjá um leiðréttingu þeirra. Eðlilegt er talið að á bilinu 2 - 17% tölvuafls fari í öryggisráðstafanir, mismunandi eftir því hve miklar öryggiskröfur eru gerðar í viðkomandi kerfi.

Ríkisendurskoðun telur að stofnanir og fyrirtæki ríkisins þurfi að huga vandlega að því að samræmi sé á milli öryggisráðstafana í upplýsingakerfum og þeirra hagsmuna sem þær eiga að gæta.

5.2 Öryggiskröfur til landskerfa

Í samkomulagi fjármálaráðherra og Skýrr hf. frá 17. febrúar 1997 er í kaflanum um almennar kröfur til landskerfa m.a. fjallað um þær öryggiskröfur sem gerðar eru til landskerfa sem vistuð eru hjá Skýrr hf. Ríkisendurskoðun telur að gera eigi jafnstrangar öryggiskröfur til annarra kerfa þó svo að þau séu vistuð hjá öðrum aðilum en Skýrr hf.

Eftirfarandi kröfur eru settar fram í samkomulagi þessu:

„Almennar kröfur til landskerfa

Skilgreining hugtaka

Landskerfi eru gagnasöfn og upplýsingakerfi hins opinbera, sem eru innbyrðis vensluð, eiga sér stoð í lögum og nauðsynleg eru til reksturs stjórnsýslunnar. Kerfisrekandi er í skilningi þessa skjals hver sú stofnun sem rekur landskerfi eða hvert það fyrirtæki er tekur að sér viðhald og rekstur slíks kerfis í umboði stofnunar eða ráðuneytis.“

„Samvirkni kerfanna

.....“

„Aðgangsöryggi

- *Fylgja skal viðurkenndum alþjóðlegum öryggisstöðlum.*

- *Húsnæði sem hýsir landskerfi skal varið fyrir aðgangi óviðkomandi manna. Að vinnslusölum, vinnustöðvum og gagnageymslum komist ekki aðrir en þeir sem tilskilin leyfi hafa.*
- *Kerfi og skrár séu varin með aðgangsorðakerfi eða öðrum viðurkenndum hætti fyrir óheimilli notkun og skemmdarverkum sem komið gætu eftir gagnanetum.*

Gagnaöryggi

- *Öll gögn í landskerfum eru trúnaðarmál og er óheimilt að veita um þau upplýsingar, munnlega eða með öðrum hætti. Engum skulu veittar aðgangsheimildir nema að fengnu leyfi eiganda upplýsinganna, og skal honum með reglubundnum hætti gerð grein fyrir hverjir hafi slíkar heimildir á hverjum tíma. Þetta gildir einnig um starfsmenn kerfisrekanda.*
- *Afrit skulu tekin og varðveitt af öllum gögnum og forritum samkvæmt áætlun sem aðilar gera í sameiningu.*
- *Öryggisafrit og frumrit skal ekki varðveita í sama húsi.*
- *Tryggja skal að gögn sem einu sinni eru komin inn í kerfin glatist ekki. Verði stórfelld ófyrirséð áföll, svo sem bruni, jarðskjálftar og svo framvegis, ber að gera ráðstafanir til að ekki tapist meira en færslur dagsins.*
- *Tryggja skal að rétt gögn séu afhent réttum viðtakanda.*
- *Gögn í aðalskrám og öðrum kerfum ríkisins skulu samnýtt til að koma í veg fyrir margskráningu og draga úr hættu á villum.*

Rekstraröryggi

- *Landskerfin skulu vera nýtanleg 99,8% af skilgreindum þjónustutíma, samanber III. kafla.*
- *Svartími í sívinnslu skal vera innan við 1 sek. í 90% tilvika, mældur þar sem fjarvinnslulína tengist kerf-*

isrekanda innan veggjar á vistunarstað (hér: innan veggja Skýrr).

- *Þess sé gætt að enginn einn starfsmaður kerfisrekanda meðhöndli upplýsingasöfn og hugbúnað neins kerfis á öllum stigum framleiðslu og þjónustu.*
- *Notkun gagna og forrita skal skráð þannig að öll notkun verði rakin til tiltekins kenninafns notanda eftir á og tímasett ef þörf gerist, allt að einum mánuði eftir að skráning fer fram. Slík skráning skal vera sjálfvirk og innbyggð í kerfin þar sem því verður við komið. Frekari kröfur sem verkkaupi kann að gera um rekjanleika vegna meðhöndlunar á viðkvæmum upplýsingum verður að semja um sérstaklega og fella inn í kerfin eftir því sem við á."*

Þegar vísað er til viðurkenndra alþjóðlegra öryggisstaðla í kröfunum hér að ofan mun vera átt við þá staðla sem fjallað er um í Innkaupahandbók RUT-nefndarinnar en nánar er fjallað um þá öðrum stað í greinargerð þessari.

5.3 Stjórnunar- og skipulagsráðstafanir

Með stjórnunarlegum öryggisráðstöfunum er hér átt við ýmsar reglur og verkferli í rekstri upplýsingakerfa sem stuðla eiga að öryggi þeirra. Með skipulagslegum öryggisráðstöfunum er hér átt við verkaskiptingu og ábyrgð starfsmanna sem lið í öryggismálum stofnunar eða fyrirtækis.

1. Stjórnunarlegar öryggisráðstafanir

Í greinargerð þessari er mælt með setningu ýmissa reglna sem telja má til stjórnunarlegra öryggisráðstafana. Það sem er sameiginlegt með reglum þessum er að þær eru teknar af forstöðumanni stofnunar eða öðrum yfirmönnum.

Dæmi um stjórnunarlegar reglur geta verið ýmsar verklagsreglur sem forstöðumaður setur starfsmönnum um notkun

Alnetsins innan viðkomandi stofnunar eða fyrirtækis. Margar stjórnunarlegar reglur koma fram í kaflanum um tæknilegar öryggisráðstafanir þar sem reglurnar eru oft nátengdar þeim. Sem dæmi um slíkar stjórnunarlegar reglur má nefna reglur um skráarflutninga til og frá viðkomandi ríkisaðila, reglur um að starfsmenn leiti að tölvuveirum í öllum skrám sem þeir setja inn í viðkomandi upplýsingakerfi og að þeir tilkynni kerfisstjóra strax ef þeir verða varir við veirusmit.

2. Verkaskipting og ábyrgð starfsmanna

Miklu máli skiptir að skipurit ríkisaðila séu skýr og vel skilgreind. Skrifleg starfslýsing þarf að liggja fyrir vegna hvers starfs án tillits til þess hver gegnir því. Í henni þarf að koma fram lýsing á starfinu, hvaða upplýsingakerfi eru notuð í því, hvaða aðgangur er að hverju þeirra og hvaða ábyrgð fylgir starfinu. Þegar slíkar starfslýsingar liggja fyrir eru þær tengdar tilteknum starfsmönnum. Lykilstörfum er úthlutað til fleiri en eins starfsmanns svo að enginn sé ómissandi.

Mikilvægt er að verkaskipting vegna reksturs upplýsingakerfa sé ekki með þeim hætti að aðeins einn starfsmaður í tölvudeild hafi þekkingu á lykilatriðum í rekstri eða uppbyggingu upplýsingakerfa, þannig að ef hans nýtur ekki við, geti komið til rekstrartruflana eða neyðarástands hjá viðkomandi ríkisaðila.

Í þessu samhengi er rétt að fjalla aðeins um starf kerfisstjóra en hann gegnir mikilvægu starfi vegna öryggismála upplýsingakerfa. Algengt er að kerfisstjórar beri of mikla ábyrgð, hafi of mikið að gera, hafi óskilgreint verksvið, hafi of lítinn tíma til símenntunar, séu illa skipulagðir vegna þess að þeir láta stjórnast af þeim atburðum sem upp koma í erli dagsins og séu ómissandi. Afleiðingar þessa geta t.d. verið að kerfisstjóri fer ekki reglulega yfir dagbók („log-skrá“) tölvukerfis og hann veiti öllum starfsmönnum lesaðgang að gögnum, jafnvel þó að um viðkvæm gögn sé að ræða, til þess að reyna að minnka kvabb þeirra. Mikilvægt er með tilliti til öryggismála að séð sé til þess að kerfisstjóri hafi skilgreint

verksvið, beri rétta ábyrgð, fái símenntun, sé skipulagður og geti rólegur farið í frí.

Aðskilnaður starfa er mikilvægur liður í því að tryggja gott innra eftirlit. Aðskilja þarf t.d. störf forritara og tölvara ekki síður en bókara og gjaldkera, (vegna starfa hinna síðarnefndu vandast þó málið ef um er að ræða rafræn viðskipti). Aðskilnaður milli forritara og tölvara er framkvæmdur með þeim hætti að tölvuvinnsluumhverfinu er skipt í raunumhverfi og þróunarumhverfi. Hefðbundin vinnsla gagna fer fram í raunumhverfinu og stjórnar tölvari aðgangi að því en í þróunarumhverfi prófar forritari þau forrit sem hann er að vinna við. Mikilvægt er að forritarar hafi ekki aðgang að raunumhverfi vegna þess að eingöngu skal gera prófanir á forritum í þróunarumhverfi.

Rétt er að nefna það hér að skilgreining tiltekinna starfa þ.e. verksviðs og ábyrgðar, sem því fylgir, ásamt því hvaða aðgangsheimildir að tilteknum upplýsingakerfum fylgja starfinu, getur skipt miklu máli vegna rannsókna á umboðssvikum, þ.e. þeim tilvikum þegar menn fara í starfi sínu út fyrir umboð sitt.

5.4 Umhverfis- og aðbúnaðarráðstafanir

Hér á eftir eru talin upp nokkur dæmi um það sem átt er við með öryggisráðstöfunum sem tengjast umhverfi tölvukerfis og aðbúnaði þess.

- Afrit skulu geymd innanhúss á stað sem metinn er eldheldur í a.m.k. 6 klst. Afrit skulu einnig geymd á öruggum stað utan stofnunar eða fyrirtækis.
- Gluggalaust tölvuherbergi skal alltaf vera læst eða á svæði þar sem aðgangur er takmarkaður við tiltekna starfsmenn.
- Tölvubúnaður í tölvuherbergi skal vera á sérstökum rafmagnsöryggjum.

- Hvorki eiga að vera vatnsrör né miðstöðvarofnar í tölvuherbergi.
- Engir prentarar eiga að vera í tölvuherbergi.
- Tölvuherbergi skal ekki notað sem pappírsgeymsla.
- Netþjónar og gáttir skulu tengdar við rafbakhjarl (UPS) til þess að koma í veg fyrir stöðvun af völdum rafmagnstruflana.
- Allar tölvulagnir í stofnuninni/fyrirtækinu skulu vera í lokuðum stokkum.
- Reykskynjari skal vera í tölvuherbergi fyrir ofan netþjóna.
- Halon-slökkvitæki skal geymt fyrir utan dyr tölvuherbergis.
- Allur tölvubúnaður skal vera í að a.m.k. 10 cm. hæð frá gólfi til þess að minnka líkur á vatnstjóni.

5.5 Tæknilegar ráðstafanir

Með tæknilegum ráðstöfunum er átt við aðgerðir í tölvukerfinu sjálfu til að gera það öruggt, t.d. notkun lykilorða, tvöföldun á viðkvæmum vélahlutum og fleira af því tagi sem fjallað verður um hér á eftir.

1. Afmörkun netumhverfis

1. Innranet og ytranet

Aðskilnaður innra- og ytranets er mikilvægt öryggisatriði sem byggir á því að öll mikilvæg gögn og upplýsingar séu skilyrðislaust geymd á innraneti ríkisaðila en á ytraneti einungis gögn sem öllum almenningi er heimill aðgangur að. Með slíku fyrirkomulagi má draga úr tjóni af innbrotum því þá eru góðar líkur á því að tölvuþrjótar komist ekki lengra en í ytranetið þar sem engin viðkvæm gögn er að finna.

2. Upphringisamband

Almennt ætti ekki að leyfa starfsmönnum að tengja mótald við tölvur sínar. Slík uppsetning getur gert viðamiklar öryggisráðstafanir að engu.

Takmarka ætti eins og kostur er notkun upphringisambanda við tölvukerfi ríkisaðila. Séu innhringingar leyfðar í undantekningartilvikum, þarf símalínan að vera tengd símanúmerabirti svo hægt sé að rekja úr hvaða síma er hringt, hvenær og hve lengi tenging varði.

3. Lokuð net

Þegar ríkisaðilar eiga í mikilvægum samskiptum sín á milli, ættu þau að fara fram á lokuðu neti en ekki á opnu neti eins og Alnetinu. Aðgang að lokuðu neti ætti að takmarka eins og kostur er við ákveðna aðila sem erindi eiga í slíkan lokaðan samskiptahóp.

4. Eldveggir

Eldveggur er tölvubúnaður sem ætlað er það hlutverk að hindra óheimila umferð inn í og út úr staðarneti ríkisaðila sem tengt er við Alnetið eða tölvunet annars aðila.

Þær varnir sem eldveggir geta veitt eru að:

- Hindra óæskileg tölvusamskipti.
- Beina utanaðkomandi tölvusamskiptum inn í tölvu sem telst vera örugg.

- Fela viðkvæmar tölvur sem ekki er auðvelt að tryggja gegn umferð frá Alnetinu.
- Halda dagbækur um samskipti til og frá því tölvuneti sem verið er að verja.
- Hindra að upplýsingar um nafn tölvukerfis, tegund þess, jaðartæki og notendaauðkenni fari út á Alnetið.
- Vera betur í stakk búnir til þess að staðfesta uppruna en einstök notendaforrit.

Ekki geta allir eldveggir uppfyllt ofangreindar kröfur. Mismunandi öflugan eldvegg þarf eftir því hve mikilvægt það er, að enginn komist inn í viðkomandi tölvukerfi.

Allir ríkisaðilar sem eru tengdir eða ætla að tengjast Alnetinu ættu að nota einhverja ofangreindra ráðstafana því mjög miklar líkur eru á því að reynt verði að brjótast inn í viðkomandi tölvukerfi eftir að það hefur verið tengt við Alnetið. Einnig er nauðsynlegt að brýnt sé fyrir starfsmönnum að óheimilt sé að fara aðrar leiðir inn á Alnetið en í gegnum eldvegg ríkisaðilans. Ef starfsmenn eru með mótöld á tölvum sínum sem gera þeim kleift að tengjast Alnetinu með beinum hætti er eldveggurinn gagnslítill.

5. FTP- skráarflutningur

Einn af þeim þjónustuþáttum sem Alnetið býður upp á er FTP-skráarflutningur á milli ólíkra aðila. Almennt ætti að vera hægt að nálgast skrár frá ríkisaðila með FTP-skráarflutningi en varast ætti að heimila utanaðkomandi aðilum að nota FTP-skráarflutning til þess að senda skrár til tölvukerfis ríkisaðila. Dæmi eru t.d. um að FTP-skrárflutningur hafi verið notaður til þess að geyma ólöglegt eða ósiðlegt efni í tölvukerfi án vitundar eiganda kerfisins.

Þegar ríkisaðili þarf að taka á móti skrám frá utanaðkomandi aðilum ætti að gera það í gegnum tölvupóst. Með þeim hætti fer alltaf einhver starfsmaður í gegnum þær skrár sem settar eru inn í tölvukerfi ríkisaðilans.

2. Tvöfaldur vélbúnaður

Leita þarf uppi alla veikustu hlekkina í tölvukerfinu þannig að allir þeir einstöku þættir sem geta valdið víðtækum rekstrartruflunum séu þekktir. Oft getur t.d. tiltölulega ódýr vélbúnaður valdið víðtækum rekstrartruflanir ef mjög margir treysta á hann. Í slíkum tilvikum er rétt að huga að því að styrkja þessa veikustu hlekki kerfisins með því að hafa þennan vélbúnað tvöfaldan.

Ákvörðun um hve mikið skuli hafa af tvöföldum búnaði er háð því hve dýrum rekstrartruflunum hann getur valdið ef hann bregst. Ef mjög dýrt er fyrir viðkomandi ríkisaðila að upplýsingakerfi verði fyrir smávægilegum rekstrartruflunum, t.d. að ekki er talið ásættanlegt að það sé óvirkt lengur en í eina mínútu, væri viðeigandi ráðstöfun að jafnaði að hafa allan sameiginlegan búnað tvöfaldan og hafa bæði aðaltölvukerfi og varatölvukerfi stöðugt í gangi. Auk þess þyrfti að vera til staðar sjálfvirk skipting yfir á varakerfi ef aðalkerfi bilar. Ef ásættanlegt telst að upplýsingakerfi geti verið óvirkt í allt að eina klukkustund þarf væntanlega að hafa vélbúnað tvöfaldan, þó svo að varakerfið sé ekki haft í gangi og skipting yfir á það sé handvirk ef aðaltölvukerfi viðkomandi ríkisaðila bilar.

Þá lágmarkskröfu til tvöföldunar á vélbúnaði sem gera verður hjá öllum ríkisaðilum er að diskspeglun sé á sameiginlegum netþjóni. Harðir diskar eru það ódýrir í dag að varla er réttlætanlegt að til rekstrartruflana komi vegna skemmda í hörðum diskum netþjóns.

3. Aðgangsheimildir

Eftir því sem gagnavinnsla flyst nær hinum almenna notanda breytist eðli þess umhverfis sem öryggi þarf að ná til. Þegar vinnsla fer fram í einkatölvuumhverfi þarf að huga að öðrum og mun fleiri öryggisþáttum en í stórtölvuumhverfi þar sem notandinn hefur í því fyrrnefnda einnig aðgang að stýrikerfi og vélbúnaði.

Mikilvægt er að forstöðumenn eða yfirmenn deilda en ekki kerfisstjórar ákveði hvaða aðgangsheimildir að upplýsingakerfum fylgja tilteknu starfi, án tillits til þess hver sinnir því. Kerfisstjórar eða starfsmenn þeirra sjá hins vegar um að veita aðganginn.

Þess má til fróðleiks geta að bandaríska ríkisendurskoðunin telur að þeir tveir þættir sem séu í mestum ólestri í öryggismálum hjá stofnunum og fyrirtækjum ríkisins þar í landi séu aðgangsmál og skortur á neyðaráætlunum.

1. Notkun lykilorða

Notkun lykilorða í upplýsingakerfum er venjulega með þeim hætti að notandi er spurður um lykilorð þegar hann kemur að viðkomandi kerfi. Í flestum tilvikum getur hann skráð lykilorð sitt í upphafi vinnudags og síðan haft aðgang að kerfinu allan daginn. Sum fjölnotendakerfi eru þannig að notanda er „hent út“, þ.e. lokað á aðgang hans ef hann notar það ekki í tiltekinn tíma.

Algengt er að tölvur standi opnar inn í tiltekið upplýsingakerfi án þess að verið sé að vinna við það. Hver sem er getur þá gengið að tölvunni og gert það sem sá sem skráði sig inn í kerfið hefur heimild til þess að gera hafi hann til þess nægilega þekkingu. Ef hann gerir eitthvað merkist það þeim sem skráði sig inn í kerfið ef færslur merkjast auðkennum notenda.

Tölvur ættu ekki að vera opnar ef enginn er að vinna við þær. Óþægilegt er hins vegar fyrir starfsmenn sem nota tölvur aðeins annað slagið að vera alltaf að skrá sig inn í kerfið. Úr því má bæta með því að nota skjávara með lykilorði. Ef opin tölva hefur staðið ónotuð í fyrirfram skilgreindan tíma, er sett tiltekin bráðabirgðalokun á tölvuna, sem felst í því að notandinn þarf að skrá sérstakt skjávaralykilorð til þess að geta haldið vinnu sinni áfram.

Aðgangsþjónusta Skýrr hf. hefur gefið út reglur um aðgangs- og leyniorð[5] og gilda þær vegna þeirra upplýsingakerfa ríkisaðila sem vistaðar eru hjá fyrirtækinu. Auk reglna um notkun aðgangsorða er þar að finna leiðbeiningar um það hvenær og hvernig sívinnslunotendur eiga að breyta leyniorði sínu ásamt reglum um það hvernig leyniorðið á að vera. Í reglunum kemur m.a. fram eftirfarandi:

„*<u>Hvenær skal breyta leyniorði?</u>*

1.1 Notendur geta breytt leyniorði sínu hvenær sem er og fyrirvaralaust. Sjálfsagt er að breyta orðinu samstundis ef menn grunar að óviðkomandi hafi fengið um það vitneskju.

1.2 Gildistími leyniorða er nálægt fjórum mánuðum (120 dagar). Að þeim tíma liðnum krefur öryggiskerfi tölvunnar notendur um nýtt leyniorð.

1.3 Með sjö daga fyrirvara birtist aðvörun á skjánum um að tími gildandi leyniorðs renni út tiltekinn dag. Þá er rétt að breyta leyniorðinu strax við næsta hentugt tækifæri. Hafi orðinu ekki verið breytt hinn tilgreinda dag, eru menn (sbr. 1.2) krafðir um nýtt leyniorð áður en þeir fá að halda áfram.

<u>Hvernig á leyniorð að vera?</u>

Ekki er leyfilegt að nota alla stafi né allar samsetningar af orðum sem leyniorð. Um það gilda eftirfarandi reglur:

*2.1 Leyniorð skal vera **minnst fimm stafir** og **mest átta stafir** að lengd.*

2.2 Broddstafi, á, é, í, ó, ú og ý, og íslensku sérstafina, þ, æ, ö, og ð, má ekki hafa í leyniorðum.

2.3 Áður notað leyniorð eða orðhluta má ekki nota á ný fyrr en eftir að önnur ólík orð hafa verið notuð a.m.k. þrisvar sinnum.

2.4 Fjórir fyrstu stafir leyniorðs mega ekki vera hluti úr nafni notandans eða aðgangsnafni hans.

[5] Reglur um aðgangs- og leyniorð, Skýrr hf. apríl 1996.

2.5 Þá skal á það bent að menn skyldu leitast við að velja sér leyniorð sem ekki er líklegt að aðrir giski á hvert er. Þó þarf helst að vera gott að muna það. Til álita kemur t.d. að bæta tölustaf við annars algengt orð, dæmi: „hes8pa“ eða „mastur9“.

Ríkisendurskoðun telur að ríkisaðilar eigi að hafa reglur Skýrr hf. til viðmiðunar þegar þeir gera kröfur vegna aðgangs- og lykilorða í upplýsingakerfum sínum.

2. Verndun lykilorða

Aldrei verður um of brýnt fyrir starfsmönnum það grundvallaratriði varðandi öryggi upplýsingakerfa, að halda lykilorðum sínum leyndum. Ekki má gefa öðrum upplýsingar um lykilorðið, hvorki samstarfsmönnum né öðrum og ekki skal skrifa það niður á blað eða í bók sem blasir við eða er auðfinnanleg. Vakin skal athygli á því að í öryggisstaðli C2 sem lýst er í kafla 3.1.2.2 hér að framan, kemur fram að í þeim kerfum, sem uppfylla skilyrði hans eru notendur gerðir ábyrgir fyrir aðgangi sínum.

4. Afritataka

Langmikilvægasta atriðið til þess að tryggja rekstraröryggi upplýsingakerfa ríkisaðila er að ætíð séu til fullnægjandi afrit af gögnum og hugbúnaði. Gera verður kröfu um að varðveisluöryggi sé tryggt í þeim upplýsingakerfum sem hafa þýðingu fyrir ríkissjóð. Nauðsynlegt er því að setja skýrar verklagsreglur um afritatöku, meðferð, prófun, geymslu og eyðingu afrita.

Í Innkaupahandbók RUT-nefndarinnar 1998 er eftirfarandi regla sett fram: *„Takið afrit reglulega og nægilega oft. Geymið afrit á öðrum stað eða fleiri en einum stað.“*

Áður en fyrirkomulag afritatöku er ákveðið verður að svara þeirri spurningu hvort ásættanlegt sé að gögn sem skráð voru í upplýsingakerfi í gær, í síðustu viku eða síðasta mánuði, tapist. Hvort gögn eru til á pappír eða ekki hefur væntanlega áhrif á svör við þeirri spurningu.

Oft eru gögn sem skráð hafa verið í upplýsingakerfi einnig til á pappír og því er hægt að skrá þau aftur ef þau tapast en það getur verið óhemju dýrt. Við skipulagningu á tíðni og umfangi afritatöku þarf m.a. að taka tillit til þessa.

Oftast er algerlega óásættanlegt að gögn sem einu sinni hafa verið skráð í upplýsingakerfi glatist. Af þessum sökum verður að leggja mjög þunga áherslu á það að afritatakan sé í lagi. Engin önnur öryggisráðstöfun í upplýsingakerfum er jafn mikilvæg og afritatakan.

1. Stórtölvuumhverfi

Ekki verður í greinargerð þessari fjallað sérstaklega um afritatöku í stórtölvuumhverfi, þ.e. í sérhæfðum tölvumiðstöðvum, að öðru leyti en því að benda á að í kaflanum um öryggiskröfur til landskerfa hér fyrr í greinargerðinni er vitnað í samning á milli fjármálaráðuneytisins og Skýrr hf., en í þeim samningi er fjallað um þessi mál undir liðnum gagnaöryggi.

2. Netkerfi

Lágmarkskrafa til afritatöku í netkerfi er að á hverri nóttu sé tekið hlutaafrit, þ.e. afrit af þeim skrám, sem breyst hafa frá því að síðast var tekið heildarafrit. Heildarafrit ætti að taka mánaðarlega, auk þess sem geyma ætti mánaðarafritin sex mánuði aftur í tímann. Ástæða þess að nauðsynlegt er að geyma gögn svo lengi er að oft uppgötvast ekki fyrr en seint og um síðir að gögn eða forrit eru ónýt, t.d. af völdum tölvuveira, en þær geta legið lengi í upplýsingakerfi án þess að eftir þeim sé tekið. Auk þessa skal halda til haga öllum upp-

runalegum disklingum og geisladiskum með hugbúnaði sem notaður er innan viðkomandi ríkisstofnunar eða fyrirtækis.

Í algengum, litlum og ódýrum segulbandsstöðvum er hægt að afrita a.m.k. 8 gígabæti á eina segulbandspólu. Algengasta fyrirkomulag afritatöku í netkerfum þar sem gagnamagn ásamt forritum er innan áðurnefndra marka er að taka heildarafrit daglega alla virka daga auk þess sem heildarafrit er tekið einu sinni í mánuði. Oft er einnig um leið og færsla er gerð í mikilvægan gagnagrunn, tekið afrit af henni annað hvort á segulband, með diskaspeglun eða speglun á netþjóni.

3. Einkatölvur

Ef einkatölvur starfsmanna eru tengdar tölvuneti er venjan sú að reglur gilda um það að öll mikilvæg gögn og upplýsingar skulu vistaðar á staðarnetinu og einstakir starfsmenn þurfa ekki að sjá um afritatöku af gögnum og upplýsingum viðkomandi ríkisaðila því umsjónarmaður staðarnetsins sér um hana.

Ef einkatölvur starfsmanna eru hins vegar ekki nettengdar horfir málið öðruvísi við. Ef á vélum þeirra eru geymd mikilvæg gögn og upplýsingar stofnunar eða fyrirtækis ætti daglega að taka afrit af öllum gögnum. Nú er t.d. hægt að fá svokölluð „zip-drif“, sem eru mjög ódýr, til þess að taka afrit af gögnum á einkatölvu. Diskettur í þessi drif taka 100 megabæti. Ef einkatölvurnar geyma gögn sem ekki eru mjög mikilvæg, eru kröfur til afritatöku minni. Lágmarkskrafa vegna afritatöku á einmenningstölvu er þó að geymdar séu þrjár kynslóðir af gögnum sem afritaðar hafa verið á mismunandi tíma. Þetta á að tryggja að þótt eitt afrit hafi eyðilagst sé alltaf til annað sem er heilt.

4. Segulmiðlar

Ýmsar tegundir afritunarbúnaðar athuga um leið og þær afrita hvort afritið sem verið er að búa til sé í lagi eða ekki og birta athugasemd þar um. Aðrar tegundir afritunarbúnaðar gera þetta ekki og því er sá möguleiki alltaf til staðar að afritun hafi mistekist, t.d. vegna þess að galli er í disklingi, segulbandi eða geisladiski sem afritað er á.

Ef afritunarbúnaðurinn athugar ekki hvort afrit sé í lagi verður að prófa það til að ganga úr skugga um að svo sé. Annars er hætt við að viðkomandi búi við falskt öryggi.

Þó svo að afritunarbúnaður athugi hvort afrit sé í lagi er nauðsynlegt að afrit séu prófuð reglulega með því að athuga hvort hægt sé að ná afriti af segulmiðli. Ekki er nóg að taka trúanlega yfirlýsingu framleiðenda búnaðarins um að svo sé. Í sumum tilvikum getur t.d. verið erfiðleikum háð að ná skrá af segulmiðli ef í heiti hennar er íslenskur stafur. Þar að auki geta margir þættir valdið því að afrit eru ekki nothæf s.s. óhreinindi, gallar í segulmiðlum, þeir eru orðnir gamlir og slitnir eða hafa yfirfyllst og ekki náð að taka afrit af öllum gögnunum.

Endingartími afrita er mismunandi. Því þarf að athuga hve langan líftíma framleiðendur segulmiðla ábyrgjast. Sérstaklega á þetta við um svokallaðar DAT-afritunarspólur því endingartími þeirra er tiltölulega stuttur. Mjög mikilvægt er að segulmiðlar séu endurnýjaðir reglulega.

5. Geisladiskavæðing afritatöku

Nú þegar endurskrifanlegir geisladiskar eru orðnir tiltölulega ódýrir er eðlilegt að horft sé til þeirra við töku afrita sem geyma á í einhvern tíma. Líklegt er og að mun meira af gögnum verði geymt lengur en hagkvæmt hefur verið hingað til á öðrum afritunarmiðlum.

6. Sala á gömlum tölvubúnaði

Ef tölvur sem teknar hafa verið úr notkun eru seldar er um tvær leiðir er að ræða, annað hvort að selja harða diska aldrei með þeim eða að þurrka forrit og gögn út af diskunum. Útþurrkun verður að að fara þannig fram að alls ekki sé hægt að ná forritum og gögnum tilbaka af þeim. Það má t.d. gera með sérstökum forritum.

7. Varðveisla tölvugagna

Þó svo að yfirskrift 5. kafla greinargerðar þessarar sé „Öryggisráðstafanir“ verður hér á eftir fjallað um sérstaka lagaskyldu til varðveislu gagna þar sem hún tengist óhjákvæmilega þeim reglum sem ríkisaðilar setja sér um afritatöku og geymslu afrita. Annars vegar er um að ræða varðveisluskyldu samkvæmt lögum nr. 145/1994 um bókhald og hins vegar samkvæmt lögum nr. 66/1985 um Þjóðskjalasafn.

1. Kröfur bókhaldslaga

Í mörgum tilvikum geyma upplýsingakerfi gögn sem falla undir ákvæði laga um bókhald nr. 145/1994. Í 20. gr. laganna er gerð krafa um að allar bækur sem fyrirskipaðar eru í lögunum, ásamt bókhaldsgögnum og fylgiskjölum, svo og bréf, myndrit og skeyti eða samrit þeirra, þar með talin gögn sem varðveitt eru í tölvutæku formi, á örfilmu eða annan sambærilegan hátt, skulu varðveittar hér á landi á tryggan og öruggan hátt í sjö ár frá lokum viðkomandi reikningsárs. Jafnframt kemur fram að ef tölvubúnaði, sem nauðsynlegur er til að kalla fram bókhaldsgögn, er breytt eða fargað, ber að prenta gögnin í upprunalegu formi eða yfirfæra þau á nýjan miðil þannig að áfram verði unnt að kalla þau fram á meðan 7 ára fresturinn er ekki liðinn.

2. Kröfur laga um Þjóðskjalasafn

Samkvæmt lögum nr. 66/1985 um Þjóðskjalasafn er safninu m.a. lögð sú skylda á herðar að safna og varðveita skjöl, þ.á.m. á tölvutæku formi.

Í 7. kafla handbókar um skjalavörslu Stjórnarráðs Íslands[6] er því lýst hvernig gögn á tölvutæki formi eru sömu lögmálum háð og önnur skjöl hvað varðar nákvæma lýsingu á því hvað á að varðveita og hvernig upplýsingarnar verða gerðar aðgengilegar í skjalasafni. Í kaflanum er lögð sérstök áhersla á skráningu kerfislýsinga. Eftir afhendingu tölvugagna ber Þjóðskjalasafn ábyrgð á geymslu þeirra og viðhaldi. Þann fyrirvara er þó að finna í lok 7. kaflans að Þjóðskjalasafn Íslands taki því aðeins við tölvugögnum að viðeigandi húsnæði verði tilbúið til afnota. Að sögn Þjóðskjalasafns hefur það nú síðla árs 1998 enn ekki getað tekið á móti tölvugögnum vegna aðstöðuleysis.

Nýverið hefur nefnd sem starfaði á vegum menntamálaráðuneytisins skilað af sér tillögum um endurskoðun á reglum um hvaða tölvugögnum skuli skila til Þjóðskjalasafnsins og með hvaða hætti.

Ljóst er að skjalalaus viðskipti aukast sífellt og um leið fjölgar þeim ríkisaðilum sem nota upplýsingakerfi er geyma gögn um slík samskipti, sbr. t.d. málaskrárkerfi ráðuneytanna. Telja verður brýnt að Þjóðskjalasafni verði gert kleift að sinna því lögboðna hlutverki sínu að varðveita tölvugögn svo koma megi í veg fyrir að upplýsingar og gögn á slíku formi glatist.

5. Veiruvarnir

Tölvuveirur geta valdið verulegum rekstrartruflunum í upplýsingakerfum ríkisaðila. Mikilvægt er því að ríkisaðilar grípi til viðeigandi ráðstafana gegn þeim.

Varnir gegn tölvuveirum felast í þremur samverkandi þáttum. Í fyrsta lagi að til staðar séu veiruvarnarforrit. Í öðru lagi að til séu verklagsreglur um meðhöndlun skráa og forrita sem tekin eru inn í upplýsingakerfi viðkomandi og loks í þriðja lagi að afrit séu tekin reglulega.

[6] Handbók um skjalavörslu Stjórnarráðs Íslands, útgefin af Þjóðskjalasafni Íslands 1991

1. Veiruvarnarforrit

Veiruvarnarforrit þurfa að vera til staðar í tölvukerfum ríkisaðila. Slík forrit eru áhrifarík vörn gegn flestum tölvuveirum. Mikilvægt er hins vegar að uppfæra þau reglulega þar sem stöðugt koma fram nýjar veirur eða ný afbrigði eldri veira.

2. Verklagsreglur

Almennum starfsmönnum ríkisaðila ætti ekki að vera heimilt að hlaða forritum niður af Alnetinu með tölvubúnaði hans og til notkunar þar, þar sem engin trygging er fyrir því að hugbúnaður sem sóttur er á Alnetið sé laus við tölvuveirur eða „Trójuhesta“ sem valdið geta tjóni. Allur hugbúnaður sem notaður er ætti að vera settur upp af kerfisstjóra eða staðfestur af honum sem útgáfa sem hann telur örugga. Með því að hafa stjórn á þeim hugbúnaði sem keyrður er á tölvukerfi ríkisaðilans er verulega dregið úr hættu á veirusmiti, ef undan eru skildar fjölvaveirur í ritvinnslu- og töflureiknisskjölum, en þær eru vaxandi vandamál.

Setja ætti reglur um það með hvaða hætti og hverjir hafi heimild til þess að setja forrit eða tölvutæk gögn inn í viðkomandi tölvukerfi og frá hverjum slík forrit og gögn mega koma.

Einnig ætti að setja reglur um að starfsmenn veiruleiti í öllum skrám sem þeir setja inn í viðkomandi tölvukerfi og tilkynntu kerfisstjóra strax ef þeir verða varir við veirusmit til þess að hann geti þegar gripið til viðeigandi ráðstafana. Þar að auki ætti kerfisstjóri að veiruleita allt tölvukerfið a.m.k. einu sinni í viku, ef ekki er sjálfvirkt veiruvarnarforrit í gangi sem gerir aðvart ef grunur leikur á að smit hafi borist í kerfið.

3. Regluleg afritataka

Regluleg afrit þurfa að vera til af öllum hugbúnaði þannig að hægt sé að setja ósýkt forrit og skrár inn í tölvukerfið í stað þeirra sem sýkst hafa eða eyðilagst.

4. Java og ActiveX

Vefvafrar sem notaðir eru til að fletta Veraldarvefnum eru sífellt að verða fullkomnari og öflugri verkfæri. Þetta hefur í för með sér að þeir fela í sér aukna áhættu ef ekki er hugað að tilteknum öryggisþáttum.

Mjög algengt er að vefsíður innihaldi forrit sem skrifuð eru í Java, JavaScript eða ActiveX, sem eru vélaróháð forritunarmál. Sérstök hætta getur stafað af því að opna slíkar vefsíður, því við það getur skoðandinn sett í gang keyrslu á skaðlegu forriti án þess hann verði þess var. Upplýsa þarf notendur um hvaða hættur geta stafað af Java, JavaScript og ActiveX forritum á Alnetinu. Almennt ættu menn að vinna á Alnetinu með því að stilla vefvafra sína þannig að vefsíður sem skrifaðar eru í Java, JavaScript eða ActiveX komist ekki inn í tölvukerfi viðkomandi og birtist þar því ekki. Í þeim tilvikum sem menn treysta því að þau forrit vinni rétt, er tímabundið hægt að breyta þessum stillingum. Rétt er hins vegar að benda á það að mikil þróun er á þessu sviði og stöðugt koma fram nýjar og öruggari útgáfur af vefvöfrum og áðurnefndum forritunarmálum.

6. Dagbækur

Mikilvægt öryggisatriði í tölvukerfi er að halda víðtæka dagbók, („log-skrá“) yfir það sem gerist í kerfinu, m.a. um óreglulega atburði og aðgangsmál. Dagbækur verða einnig að ná til beina, gátta og annars tengibúnaðar. Ef slíkar dagbækur eru ekki haldnar og skoðaðar reglulega vita menn t.d. ekki hvort brotist hefur verið inn í tölvukerfi þeirra. Tölvudagbók gegnir mikilvægu hlutverki við rannsókn á tölvubrotum.

Í dagbók þarf að vera hægt að skrá mismunandi upplýsingar eftir því hvort verið er að nota eða reyna að nota aðgangsforrit, fá aðgang að skrám sem háðar eru aðgangstakmörkunum, hvort verið er að búa til eða eyða skrám sem háðar eru aðgangstakmörkunum o.fl. Vegna áðurgreinds er m.a. skráð í dagbókina, dagsetning, tími, notendaauðkenni, númer jaðartækis, hvort aðgerð tókst eða aðgangstilraun heppnaðist eða mistókst o.s.frv.

Í þeim tölvukerfum sem uppfylla skilyrði öryggisstigs C2 og lýst er í kafla 3.1.2.2 hér að framan eru settar fram ákveðnar kröfur um þær upplýsingar sem skrá skal í dagbók.

Í tölvuinnbroti reynir tölvuþrjótur oft að hylja slóð sína. Til þess að sjá við slíku, þarf að skrá dagbókina á tvo ólíka staði samtímis því ólíklegt er að hægt sé að breyta báðum eintökum hennar í sama innbrotinu.

7. Póstveitur

Þrátt fyrir að ekki sé hægt að staðfesta réttan uppruna tölvupósts og auðvelt sé fyrir óviðkomandi að lesa tölvupóst til annarra, ef ekki er gripið til sérstakra öryggisráðstafana, er tölvupóstur nú sú þjónusta sem mikilvægust er á Alnetinu. Nauðsynlegt er því fyrir ríkisaðila að huga vel að öryggisþáttum hans.

Ríkisaðilum er bent á að kynna sér leiðbeiningar[7] RUT-nefndarinnar um tölvupóst, sjá vefsíður nefndarinnar á http://www.stjr.is/rut/. Einnig skal vakin athygli á því að ritstjórn stjórnarráðsvefsins vinnur að gerð reglna um framsetningu á vefsíðum ríkisaðila og eru þeir hvattir til þess að kynna sér þessar reglur þegar þær birtast á vefsíðum Stjórnarráðsins.

[7] Tölvupóstur í ríkisstofnunum, Vandamál og úrlausnir. Skýrsla vinnuhóps á vegum RUT-nefndar í maí 1998.

Í þessum kafla verður stuttlega fjallað um nokkra þætti sem snúa að öryggi tölvupósts og skyldra Alnetsþjónusta, þ.e. póstlista og fréttahópa.

Eins og áður segir geta menn ekki verið öruggir um að sendandi sé sá sem fram kemur í tölvupósti á Alnetinu. Ef staðfesta þarf uppruna hans verður að nota sérstök öryggisforrit, sem byggja á því að dulkóða tölvupóstinn og/eða tölvupóstkerfi, sem nota innbyggða öryggisþætti. Með því að viðhafa slíkar öryggisráðstafanir næst tvennt, annars vegar að réttur sendandi kemur fram og hins vegar að enginn annar aðili hefur getað lesið póstinn.

Í tölvukerfum verður að gera sérstakar ráðstafanir til þess að koma í veg fyrir fjöldasendingar á pósti, þ.e. stanslausar sendingar tölvupósts til tölvupósthúss þar til það er orðið fullt og getur ekki starfað eðlilega. Slíkar fjöldasendingar geta verulega truflað eða lamað heilu tölvukerfin. Hægt er að bregðast við þessu með því að takmarka stærð og fjölda þeirra skeyta sem tölvupóstkerfi má taka við frá einum aðila sama daginn.

1. Fréttahópar og póstlistar

Einn þeirra þjónustuþátta sem Alnetið býður upp á kallast fréttahópar. Í þeim er fólk sem skiptist á skoðunum og reynslu um ýmislegt sem tengist starfi þess eða áhugamálum en þau síðarnefndu geta verið hin fjölbreyttustu eins og vitað er og ekki öll siðleg eða lögleg. Fréttahópar geta valdið miklu álagi á Alnetssamband ríkisaðila ef fjöldi þeirra er ekki takmarkaður. Ekki er þörf fyrir þessa þjónustu hjá ríkisaðilum nema í sérstökum tilvikum. Meginreglan ætti því að vera að takmarka ætti aðgang að henni.

Annar þjónustuþáttur Alnetsins kallast póstlistar. Almennt er ekki þörf fyrir þá þjónustu nema í sérstökum tilvikum t.d. vegna samskipta við skyldar stofnanir eða fyrirtæki erlendis.

Ef ekki er bannað að starfsmenn sendi skeyti frá tölvu á vinnustað sínum inn í fréttahópa eða póstlista á Alnetinu, ætti a.m.k. að setja reglur um það að koma verði fram í

skeyti sem ekki er sent á vegum viðkomandi ríkisaðila, að þær skoðanir sem í því birtast séu persónulegar skoðanir þess sem það sendir en ekki viðkomandi ríkisaðila. Ástæða þessa er sú að ríkisaðili kann að verða fyrir álitshnekki eða honum stefnt fyrir meiðyrði vegna skoðana sem birtast í skeyti sem tengt er heiti hans og birtist opinberlega í fréttahópi eða póstlista á Alnetinu. Einnig væri hægt að setja reglu um að ef starfsmenn senda persónulegar skoðanir inn í fréttahópa, eigi þeir að nota nafnlausar póstveitur, eins og t.d. hotmail.com en þar geta þeir fengið póstföng til nota vegna samskipta um áhugamál sín.

2. Siðareglur INTIS

INTIS, sem sér um hinn íslenska hluta Alnetsins, hefur sett ýmsar siðareglur vegna notkunar þess, sjá vefsíður fyrirtækisins http://www.isnet.is.

Ein af reglum INTIS er sú að umferð vegna hvers kyns óumbeðinnar „fjöldadreifingar á upplýsingum“, svo sem auglýsinga, stjórnmálaáróðurs og „keðjubréfa“ eða dreifing efnis á póstlista, sem snertir ekki viðfangsefni hans, er að öllu jöfnu óleyfileg. Fyrirtækið útskýrir hugtakið „fjöldadreifing á upplýsingum“ á þann hátt að átt sé við söfnun netfanga einstaklinga til að útbúa dreifilista, sem notaðir eru til að senda óumbeðinn tölvupóst til þeirra. Einnig er átt við misnotkun póstlista með því að senda þeim sem á honum eru efni sem er óviðkomandi viðfangsefni hans og notkun Usenet (vegna fréttahópa), til að auglýsa eða dreifa upplýsingum sem ekki fjalla um viðfangsefni viðkomandi hóps, eða senda sama efni í marga hópa samtímis. Áðurnefnda hegðun telur INTIS brot á siðareglum Alnetsins og dónaskap sem hvorki sé viðkomandi fyrirtæki né einstaklingi til framdráttar.

5.6 Neyðaráætlun

Stofnanir og fyrirtæki ríkisins þurfa að útbúa skriflegar neyðaráætlanir sem hægt er að grípa til við náttúruhamfarir,

bruna og önnur óhöpp. Sérstakur hluti neyðaráætlunar skal vera vegna upplýsingakerfis viðkomandi ríkisaðila og skal hann ná til allra upplýsingakerfa hans.

Í Innkaupahandbók RUT-nefndarinnar um upplýsingatækni 1998, eru á bls. 94 eftirfarandi reglur um neyðaráætlanir:

„Allar stofnanir eiga að hafa virka neyðaráætlun, sama hversu einföld upplýsingakerfi þeirra eru. Ef upplýsingakerfið er einfalt í sniðum er neyðaráætlunin það líka. Munið að geyma prentað eintak af neyðaráætlun í öðru húsnæði.“

Þeir þrír þættir sem mestu máli skiptir að séu í góðu lagi í öryggismálum stofnana og fyrirtækja ríkisins eru afritataka, aðgangsmál og neyðaráætlanir.

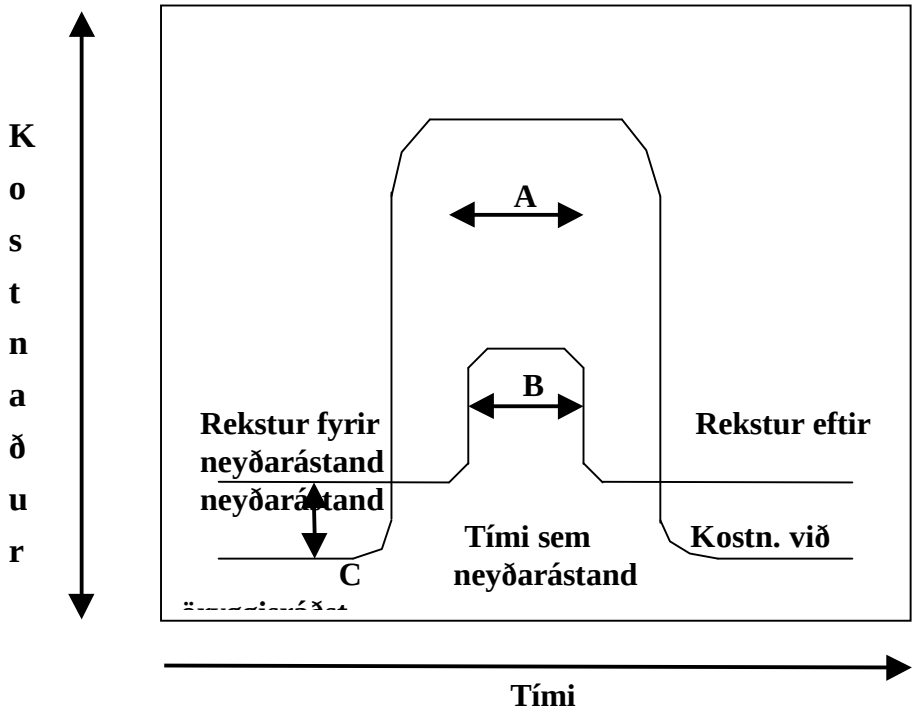
1. Markmið og ávinningur

Markmið neyðaráætlunar vegna upplýsingakerfa er að lágmarka rekstrartruflanir af þeirra völdum með því að koma rekstri kerfanna aftur í gang á sem stystum tíma og draga eins og kostur er úr því tjóni sem stöðvun þeirra veldur. Neyðaráætlun á að tryggja að starfsmenn velji eftir neyðartilvik, réttustu leiðirnar við það að koma upplýsingakerfum viðkomandi ríkisaðila aftur í gang.

Neyðaráætlun verður að taka mið af rekstrarþörfum viðkomandi ríkisaðila. Gagnslítið er til dæmis að miða neyðaráætlun við að koma tilteknu upplýsingakerfi aftur í notkun tveimur sólarhringum eftir áfall, ef starfsemin þolir ekki að missa það nema í einn sólarhring. Eins og áður hefur komið fram fer við áhættumat fram flokkun á upplýsingakerfum viðkomandi ríkisaðila með tilliti til mikilvægis þeirra og er þá horft til þess hve lengi er ásættanlegt að tiltekið upplýsingakerfi sé ónothæft. Þessi flokkun hefur áhrif á umfang neyðaráætlunar, en vegna hennar þarf að gera sér

grein fyrir því hve langan tíma tekur að koma hverju upplýsingakerfi aftur í gagnið eftir áfall. Í neyðaráætluninni þarf að koma fram í hvaða röð skal setja upplýsingakerfi upp eftir áfall. Hér þarf að athuga að máli getur skipt við röðun kerfanna hvenær áfall verður, vegna mikilvægra vinnslna í byrjun/lok mánaðar/árs.

Myndinni hér fyrir neðan er ætlað að sýna tengslin á milli kostnaðar og ávinnings af þeim öryggisráðstöfunum sem miða af því að lágmarka tjón vegna neyðartilvika**.**



Mynd 2. Rekstrarkostnaður og ávinningur af öryggisráðstöfunum sem miða af því að draga úr kostnaði vegna neyðartilvika[8].

Skýringar við bókstafina á myndinni hér fyrir ofan:

A = Kostnaður vegna neyðarástands þegar engu fjármagni hefur verið varið til öryggisráðstafana vegna neyðartilvika.

B = Kostnaður vegna neyðartilviks þegar fjármagni hefur verið varið til öryggisráðstafana vegna neyðartilvika.

C = Rekstrarkostnaður vegna öryggisráðstafana sem miða að því að draga úr kostnaði vegna neyðartilvika.

[8] Contingency Planning and Disaster Recovery. Computer Technology Research Corp., 1997.

2. Gerð og viðhald

Hér á eftir er rakið lið fyrir lið það verkferli sem fara þarf í gegnum við gerð og viðhald neyðaráætlunar sem er eitt af verkefnum öryggishópsins. Eftirfarandi gefur hugmynd um umfang slíks verkefnis, auk þess sem upptalningin getur verið leiðbeinandi fyrir þá sem það þurfa að vinna:

1) Skipuleggja verkefnið

- Gera vinnuáætlun vegna verkefnisins.
- Kanna og meta núverandi verklag við töku afrita.
- Kanna og meta núverandi ráðstafanir vegna öryggis upplýsingakerfa.

2) Forgangsraða upplýsingakerfum

- Raða upplýsingakerfum í þá röð sem þau verða sett upp í eftir neyðartilvik. Hér skal stuðst við þá flokkun kerfa sem fram fór við áhættumat, þ.e. út frá því sjónarmiði hve lengi væri ásættanlegt að hvert kerfi væri óvirkt.

3) Skilgreina lágmarks gagnavinnsluþarfir

- Meta lágmarkskröfur til gagnavinnslu einstakra upplýsingakerfa þegar neyðarástand ríkir.

4) Meta valkosti og velja leiðir

- Skilgreina og meta þær leiðir sem færar eru við endurgangsetningu upplýsingakerfa þegar neyðarástand ríkir.
- Velja þá leið sem fara skal við endurgangsetningu upplýsingakerfanna.

5) Útbúa neyðaráætlun vegna upplýsingakerfa

- Búa til neyðaráætlun, þ.e. verklag sem viðhafa skal við endurgangsetningu upplýsingakerfa og ákveða hver ber ábyrgð á henni.

- Skjalfesta neyðaráætlunina.

6) Prófa neyðaráætlun

- Búa til áætlun vegna reglulegra prófana á neyðaráætlun vegna upplýsingakerfa.
- Prófa neyðaráætlunina.
- Skjalfesta niðurstöður prófunar.
- Meta niðurstöður prófunar.

7) Viðhalda neyðaráætlun

- Taka tillit til breytinga á upplýsingakerfum.
- Taka tillit til nýrra upplýsingakerfa.
- Taka tillit til breytinga á starfsliði.
- Endurskoða tíðni prófana.

6. Eftirlit og endurmat öryggismála

6.1 Mat á því hvort öryggisráðstafanir eru virtar

Meta þarf hvort starfsmenn virða þær öryggisráðstafanir sem forstöðumaður hefur ákveðið að ná skuli markmiðum öryggisstefnu vegna upplýsingakerfa viðkomandi ríkisaðila. Til þess að hægt sé að framkvæma slíkt mat verður að liggja fyrir skrifleg ítarleg lýsing á þessum öryggisráðstöfunum. Mat á því að starfsmenn virði þessar ákvarðanir forstöðumanns, er í eðli sínu ekki frábrugðið mati á því að virtar séu ákvarðanir hans á öðrum sviðum.

Starfsmenn viðkomandi ríkisaðila og/eða utanaðkomandi aðilar geta metið hvort öryggisráðstafanir vegna upplýsingakerfa séu virtar. Niðurstöður slíks mats geta kallað á ýmis viðbrögð, svo sem áminningar eða breytingar á reglum eða verklagi en geta einnig leitt til þess að forstöðumenn eru gerðir ábyrgir fyrir því sem miður hefur farið.

6.2 Endurmat öryggisráðstafana

Mikilvægt er að vel sé fylgst með tæknilegum nýjungum sem auðveldað geta öryggiseftirlit. Öryggisráðstafanir sem þykja góðar í dag geta verið úreltar á morgun. Ef þær eru ekki endurmetnar reglulega geta þær vakið falska öryggiskennd auk þess að sóa tíma og fjármunum í aðgerðir, sem ekki duga eða eiga ekki við. Reglulega þarf því að endurmeta öryggisráðstafanir á sama hátt og endurmeta þarf áhættu og öryggisstefnu viðkomandi ríkisaðila.

7. Viðauki - Leiðbeiningar efnahagsbrotadeildar um kærusmíð

Hér á eftir fylgja „Leiðbeiningar efnahagsbrotadeildar Ríkislögreglustjóra um kærusmíð vegna innbrots (tilraunar til innbrots) í tölvukerfi“.

Efnahagsbrotadeildin leggur mikla áherslu á að ætli viðkomandi fyrirtæki eða stofnun að kæra brot sé lögregla kölluð til strax og grunur vaknar um innbrot eða tilraun til þess. Nánar er fjallað um æskileg viðbrögð í kafla 2.9.2.

Upplýsingar um kæranda:

Einstaklingur:

Fullt nafn, kennitala, heimili og sími.

Fyrirtæki:

Nafn fyrirtækisins/stofnunarinnar, kennitala, starfsstaður, sími og faxnúmer.

Upplýsingar um starfsemina í stuttu máli:

Nöfn og símanúmer:

- Forsvarsmanns,
- tengiliðs vegna kærunnar,
- hugsanlegra vitna og samstarfsaðila í málinu.

Upplýsingar um tölvuumhverfið:

- Lýsing á tölvubúnaðinum (í stuttu máli),
- hve margir notendur eru tengdir og hvernig,
- hve mörg mótöld (hve margir geta tengst í einu),
- hvaða öryggisráðstafanir eru fyrir hendi?

Hvað gerðist:

Lýsing á því sem gert var:

- Hvernig komst upp um verknaðinn?
- Beindist atlagan gegn einhverju sérstöku, sérstökum hlutum kerfisins, sérstökum notendum?
- Gætu þeir hlutar kerfisins sem atlagan beindist að verið áhugaverðir fyrir einhverja sérstaka aðila?
- Tímasetning, sem nákvæmust.
- Brotavettvangur, um hvaða tölvu var farið við atlöguna, er hægt að benda á hvar brotamaðurinn vann að atlögunni? Gott væri að lýsa í þessum hluta hvaða aðferðum beitt var til að komast inn í tölvukerfið í sem skýrustu máli, þó nákvæmlega. Þannig gefst innsýn í getu og kunnáttu brotamannsins og um leið gefur það mynd af brotavilja. Benda á skipanir í log-skrám eða öðrum skrám úr tölvu brotaþolans sem sýna hvað brotamaðurinn er að gera hverju sinni.
- Sjálft brotið, sem nákvæmust lýsing á því sem gerðist, stutt gögnum svo sem log-skrám og öðrum skrám úr tölvu brotaþolans. Hvað gerði brotamaðurinn sem kæran beinist að? Er til dæmis hægt að sjá hvernig brotamaðurinn aflaði sér aðgangs, þurfti hann ekki aðgangsorð, notaði hann aðgangsorð annars, notaði hann sitt eigið aðgangsorð? Benda á skipanir í log-skrám eða öðrum skrám úr tölvu brotaþolans sem sýna hvað brotamaðurinn er að gera hverju sinni.

Hafa í huga að þeir sem vinna við netkerfi hafa tíðast miklu meiri þekkingu á tæknilegum atriðum varðandi kerfin, en þeir sem við lögreglumálum taka vegna þeirra. Því er best, í þessum hluta sem öðrum hlutum kærunnar, að gefa sem besta lýsingu á „mannamáli“, en láta fylgja með gögn sem skýra tæknileg atriði.

Hvaða tjóni olli brotamaðurinn:

- Urðu skemmdir á vélbúnaði?
- Urðu skemmdir á hugbúnaði?
- Urðu skemmdir á gögnum?
- Olli verknaðurinn vinnutapi?
- Olli verknaðurinn aukinni vinnu?
- Stefndi verknaðurinn einhverjum hagsmunum í hættu?

Afstaða til kröfu um að brotamanninum verði refsað fyrir verknaðinn og að honum verði gert skylt að bæta það tjón sem verknaðurinn hefur og kann að hafa valdið.

Best er að geta tilgreint fjárhagslegt tjón, í það minnsta til bráðabirgða, en bótakröfu ætti helst að leggja fram við lögregluranns óknina, til að hægt sé að bera hana undir sakborninginn.

Grunaður:

- Er einhver sérstakur grunaður?
- Ástæður fyrir gruninum, studdar gögnum.
- Ferill hins grunaða.
- Hvað gæti fundist í tölvu hins grunaða, sem gæti tengt hann brotinu?

Fylgiskjöl með kæru:

Láta fylgja með kærunni sem mest af gögnum til að styðja það sem haldið er fram og vísa í kærunni í viðkomandi fylgiskjöl. Tölusetja fylgiskjölin og telja þau upp í töluröð aftast í kærunni.

Helstu heimildir

Information Security Management

Learning From Leading Organizations,

United States General Accounting Office, maí 1998

Contingency Planning and Disaster Recovery

Computer Technology Research Corp., 1997.

Systems Auditability and Control, Module 10 – Contingency Planning

The Institute of Internal Auditors, 1991.

Innkaupahandbók um upplýsingatækni 1998

Fjármálaráðuneytið/RUT-nefndin, febrúar 1998.

Internet Security Policy: A Technical Guide

NIST Special Publication 800-XX

http://csrc.nist.gov/isptg/html/ISPTG.html

Perceived Security Threats to Today's Accounting Information Systems: A Survey of CISAs

IS Audit & Control Journal, Volume III, 1996

Reglur um aðgangs- og leyniorð

gefnar út af aðgangsþjónustu Skýrr hf. í apríl 1996.

Handbók um skjalavörslu Stjórnarráðs Íslands

útgefin af Þjóðskjalasafni Íslands 1991.

Tölvupóstur í ríkisstofnunum, vandamál og úrlausnir

Skýrsla vinnuhóps á vegum RUT-nefndar í maí 1998, sjá http://www.stjr.is/rut/.