TÖLVUMÁL

Tímarit Skýrslutæknifélags Íslands

• E • F • N • I •

ISSN-NÚMER:

• RITSTJÓRASPJALL •

Það fór ekki mikið fyrir útvarpsfrétt fyrr í vetur þess efnis að tölvuglæpir á árinu 2000 hefðu verið fleiri en næstu fimm ár þar á undan samanlagt. Þetta mun hafa verið niðurstaða evrópskrar ráðstefnu um öryggismál og burtséð frá því hvað flokkast undir glæp og hvað ekki þá hafa tilvikin verið nægilega mörg til að vekja nokkurn ugg og umtal. Ekki er á það bætandi að frétta að rússneskir tölvuþrjótar hafi komist yfir tugir þúsunda krítarkortanúmera með skipulögðum innbrotum í þekkt vefsetur. Vefverslun má ekki við áföllum þegar mikið liggur við að vinna traust notenda um öryggi slíkra viðskipta. Til að bæta gráu ofan á svart kom í ljós í framhaldi að stuldur á númerunum var mögulegur þar sem þeir sem ráku vefsetrin höfðu ekki endurbætt hugbúnað sinn til að hindra innbrot þótt það hafi staðið til boða um alllangt skeið.

Til þessa hefur það verið undir hverjum og einum komið hvernig, og jafnvel hvort, hug- og vélbúnaður tölva hefur verið varinn. Fyrir utan hættur á skemmdum og stuldi sem að upplýsingunum hefur stafað hefur bæst við að fartölvur koma æ meira í staðinn fyrir stóru gráu borðtölvurnar og þær eru í meiri hættu gagnvart stuldi eins og dæmin hafa sannað. Það liggur ljóst fyrir að þörf er á markvissum áætlunum og aðgerðum til að gera tölvuumhverfi, tæki og gögn, eins vel varin og kostur er.

Í ljósi umræðunnar þótti því við hæfi að hefja þennan árgang Tölvumála með því að helga blaðið öryggismálefnum frá ýmsum sjónarhornum en Skýrslutæknifélagið stóð einnig að ráðstefnu í upphafi ársins þar sem öryggismál voru í brennidepli.

Svo snúið sé að jákvæðari tíðindum er rétt að geta þess að núna er hægt að nálgast Tölvuorðasafnið í Orðabanka íslenskrar málstöðvar www.ismal.hi.is/ob/birta/ og handhægt að hafa síðuna í bakgrunni þegar verið er að rita um upplýsingatæknina en áður var einungis aðgangur að því í áskrift. Tölvumál hafa einnig stigið það skref að vera fáanlegt sem Acrobat skjal á heimasíðu Skýrslutæknifélagsins, www.sky.is/tim_alm.htm. Síðasta tölublað ársins 2000 er þar nú þegar og öll ný tölublöð verða einnig vistuð þannig.

Einar H. Reynis

TÖLVUMÁL

Tímarit Skýrslutæknifélags Íslands

1. - 2. tbl. 26. árg. Apríl 2001

Tölvumál er vettvangur umræðna og skoðanaskipta um upplýsingatækni sem og fyrir málefni félagsins. Óheimilt er að afrita á nokkurn hátt efni blaðsins að hluta eða í heild nema með leyfi viðkomandi greinahöfunda og ritstjórnar.

Blaðið er gefið út 5-6 sinnum á ári í 1.200 eintökum.

Prentun og umbrot:
Ísafoldarprentsmiðja hf.

Ritstjóri og ábm.:
Einar H. Reynis

Aðrir í ritstjórn:
Arnaldur Axfjörð
Jóhann Ásgrímsson
Baldur Sigurðsson
Kristján Geir Arnþórsson

Auglýsingar:
Ásta Jensdóttir

Aðsetur:
Laugavegi 178, 2. hæð,
105 Reykjavík
Sími: 553 2460

Netfang:
sky@sky.is

Heimasíða SÍ:
http://www.sky.is

Framkvæmdastjóri SÍ:
Hólmfríður Arnardóttir

Áskrift er innifalin í félagsaðild að Skýrslutæknifélagi Íslands.

• SKÝRSLUTÆKNIFÉLAG ÍSLANDS •

Skýrslutæknifélag Íslands er félag einstaklinga, fyrirtækja og stofnana á sviði upplýsingatækni. Markmið félagsins eru m.a. að breiða út þekkingu á upplýsingatækni og stuðla að skynsamlegri notkun hennar og að skapa vettvang fyrir faglega umræðu og tengsl milli félagsmanna.

Starfsemin er aðallega fólgin í, auk útgáfu tímarits, að halda fundi og ráðstefnur með fyrirlestrum og umræðum um sérhæfð efni og nýjungar í upplýsingatækni.

Félagsaðild er tvennskonar; aðild gegnum fyrirtæki og einstaklingsaðild.

Greitt er fullt félagsgjald fyrir fyrsta mann frá fyrirtæki, hálft fyrir annan og fjórðungsgjald fyrir hvern félaga umfram tvo frá sama fyrirtæki. Einstaklingar greiða hálft gjald. Félagsgjöld 2001 eru: Fullt gjald kr. **15.700,** hálft gjald kr. **7.850** og fjórðungsgjald kr. **3.925.**

Aðild er öllum heimil.

Er línan frá í fyrra að springa utan af þér?

Tenging við ljósleiðaranet Títan er ekki bara hagkvæmari kostur þegar litið er til stofnkostnaðar, flutningsgetu og mánaðargjalds heldur býður Títan fyrirtækjum upp á nær óþrjótandi stækkunarmöguleika vegna hins mikla sveigjanleika sem ljósleiðaratenging býður upp á. Eftir að viðskiptavinur hefur stofnað ljósleiðaratengingu þarf eftir það einungis eitt símtal til að auka eða minnka gagnaflutningsmöguleikana en hægt er að auka þá upp í 1000 Mb/s (1Gb/s)!

1,5 - 2 Mb/s

Þjónustuaðili	Títan	Landssíminn	Íslandssími
Þjónusta	Títan 2	ADSL+	SDSL
Bandvídd	2 Mb/s	1,5 Mb/s	2 Mb/s
Stofngjald*	40.000 kr.	56.229 kr.	45.000 kr.
Mánaðargjald án vsk.**	20.848 kr.	26.667 kr.	25.000 kr.

Stækkun á samböndum

Þjónustuaðili	Títan	Landssíminn	Íslandssími
Þjónusta	Títan 10	ADSL+	SDSL
Bandvídd	10 Mb/s	6 Mb/s	4 Mb/s
Stofngjald*	5.000 kr.	2.410 kr.	15.000 kr.
Mánaðargjald án vsk.**	32.852 kr.	45.462 kr.	35.000 kr.

*Öll verð án vsk. **Innifalið í öllum mánaðarverðum er 4 GB í gagnaflutning á mánuði.

Sími | Internet | Gagnaflutningar | Sími 512 9090

TÍTAN
-í sambandi við framtíðina

Skýrsla stjórnar fyrir árið 2000 – 32. starfsár

Flutt á aðalfundi 26. febrúar 2001

Óskar B. Hauksson

Aðalfundur félagsins í fyrra var haldinn í kjölfar eins stærsta verkefnis sem tölvumenn hafa staðið frammi fyrir en miklum tíma og fjármunum hafði verið varið í að leysa svonefndan 2000 vanda. Sem betur fer reyndust afleiðingar hans verða mun minni en búist hafði verið við og gátu því félagsmenn farið að horfa fram á veginn og sinna áhugaverðari verkefnum. Segja má að starfsemi félagsins á síðasta ári hafi tekið mið af þessu en árið var að venju viðburðaríkt í starfsemi Skýrslutæknifélagsins og enn var slegið met í aðsókn að atburðum sem haldnir voru á vegum þess.

Félagar í Skýrslutæknifélaginu voru í lok ársins 790 talsins og fjölgaði þeim nokkuð á liðnu ári. Gera má enn betur í félagaöflun og verður það væntanlega hlutverk nýrrar stjórnar að blása til sóknar í þeim efnum.

Ráðstefnu- og fundahald

Ráðstefnu- og fundahöld voru að venju fyrirferðamest í starfsemi félagsins. Ráðstefnuhald var óvenju mikið en félagið hélt alls 8 hálfsdagsráðstefnur sem 1476 manns sóttu.

Fyrsta ráðstefna ársins bar yfirskriftina, Frá óreiðu til árangurs, og var haldin í samvinnu við Félag um skjalastjórn. Að leiða saman tölvumenn og þá sem fást við skjalastjórnun var einkar áhugavert og til marks um þær breytingar sem eru að verða í upplýsingatækni þar sem tvinnast saman sífellt fleiri fræðigreinar sem nýta sér möguleika tækninnar í því að ná árangri.

Að venju fylgist félagið með nýjungum en einkar fróðleg ráðstefna var haldin um þróun vef- og nettækninnar. Mikill áhugi var á þessari ráðstefnu og voru þátttakendur alls 242 en sýning var einnig haldin í tengslum við hana sem tókst afar vel. Ráðstefna um svokallaðar kerfisveitur var haldin í maí en þá var umræðan um þá möguleika sem felast í úthýsingu (e. outsourcing) í hámarki.

Nýr flokkur upplýsingakerfa, svokölluð viðskiptatengslakerfi (e. CRM), eru í brennidepli og vinna fjölmörg fyrirtæki að innleiðingu slíkra kerfa til að ná betri árangri í þjónustu, markaðssetningu og sölustjórnun. Haldin var í nóvember ráðstefna um þetta málefni þar sem áhersla var lögð á að vanda þyrfti vel undirbúning innleiðingu slíkra kerfa sem mörg hver eru afar umfangsmikil og snerta marga þætti í rekstri fyrirtækja.

Frá upphafi hefur Skýrslutæknifélagið beitt sér fyrir faglegri stjórnun í tölvumálum og var haustráðstefna félagsins um stjórnun upplýsingatækni mikilvægt innlegg í þá umræðu. Mörg fyrirtæki og stofnanir velta fyrir sér leiðum til að takast á við sívaxandi kostnað við rekstur og þróun upplýsingakerfa. Ljóst er að beita þarf nýjum aðferðum við stjórn þessa mikilvæga málaflokks eigi árangur að nást og þeir fjármunir sem varið er í upplýsingatækni að nýtast sem best.

Mikil umræða hefur verið um persónuvernd á undanförnum misserum og árum. Setning nýrra laga á síðasta ári um persónuvernd markaði tímamót á þessu sviði. Skýrslutæknifélagið hélt ráðstefnu í samvinnu við Staðlaráð Íslands um persónuvernd í viðskiptum og stjórnsýslu. Þess má einnig geta að félagið tilnefndi tvo menn í stjórn Persónuverndar sem er ný stofnun sem m.a. tekur við hlutverki Tölvunefndar.

Á jólaráðstefnu félagsins var fjallað um þráðlaus staðarnet en þráðlaus tækni á ýmsum sviðum hefur verið að ryðja sér til rúms. Einkar áhugavert verður að fylgjast með þessari þróun á komandi misserum en ekki er ljóst hvaða staðlar verða ofan á við útfærslu þessarar tækni.

Áhugaverð ráðstefna var haldin um Konur og upplýsingasamfélagið en hún var haldin í samvinnu við Verkefnisstjórn

um upplýsingasamfélagið, Jafnréttisráð, Rannsóknastofu í kvennafræðum, Félag tölvunarfræðinga, Jafnréttisnefnd Háskóla Íslands, Verkfræðingafélagið og Menntamálaráðuneytið. Þátttakendur voru um 250 og vakti ráðstefnan mikla athygli í fjölmiðlum. Mikill áhugi er innan stjórnar Skýrslutæknifélagsins að fá fleiri konur inn í félagið en þær eru nú um 18% félagsmanna. Einnig mun verða leitast við að fá fleiri konur inn í stjórn félagsins.

Eins og sést af þessari upptalningu hefur starfsemi félagsins verið mjög fjölbreytt á liðnu ári sem markast af því hversu upplýsingatæknin snertir mörg svið. Vonandi hafa sem flestir félagsmenn fundið eitthvað áhugavert efni í dagskrá Skýrslutæknifélagsins.

Eins og áður segir var sett met í aðsókn á árinu en alls sóttu 1476 manns hefðbundna fundi og ráðstefnur félagsins og komu að meðaltali 185 á hvern atburð. Þetta þýðir að aðsókn hefur aukist í heild um 9% á milli ára og meðalaðsókn á fundi um 52%.

Útgáfumál

Útgáfa Tölvumála er ein af meginþáttum í þjónustu við félagsmenn en alls voru gefin út 5 tölublöð, samtals 176 blaðsíður með 37 greinum. Greinar í Tölvumálum voru einkar áhugaverðar ef á heildina er litið og virðast hafa aukið áhuga yngri aldurshópa á að gerast félagar í Skýrslutæknifélaginu. Auglýsingaöflun gekk mjög vel á árinu og standa þær tekjur nær alfarið undir útgáfunni.

Tölvuökuskírteini — TÖK

Haldið var áfram á þeirri braut sem mörkuð hafði verið við að innleiða TÖK í íslensku menntakerfi. Gert var sérstakt kynningarátak í upphafi ársins sem vakti töluverða athygli í fjölmiðlum landsins og voru fyrstu hæfnisskírteinin afhent við hátíðlega athöfn í Ráðhúsi Reykjavíkur.

Áfram var unnið að því að fá til liðs við okkur fleiri prófmiðstöðvar en þær eru nú alls 15 talsins og gefin hafa verið út 68 TÖK skírteini.

Vinna þarf betur að því að koma TÖK á framfæri sérstaklega gagnvart ráðningarfyrirtækjum og stuðla þarf að því að stærri fyrirtæki gerist prófmiðstöðvar. Einnig liggur fyrir að endurnýja þarf námsefni og koma prófunum á vefinn.

Erlent samstarf

Áfram var haldið á þeirri braut að efla erlent samstarf með þátttöku okkar í CEPIS og norrænu samstarfi. Á vettvangi CEPIS ber hæst góður árangur tölvuökuskírteinisins í Evrópu en það styrkir verulega fjárhag samtakanna. Skrifstofa CEPIS hefur verið flutt til Frankfurt og búið er ráða faglegan framkvæmdastjóra í fullt starf. Undirbúningur er kominn vel á veg að evrópsku hæfniskerfi fyrir fagfólk í upplýsingatækni en mikil þörf er á vottun þekkingar sem er óháð einstökum stórfyrirtækjum á sviði tölvubúnaðar.

Skýrslutæknifélagið er fullgildur aðili í þessu samstarfi Evrópuþjóða og hefur það verið tvímælalaust styrkur í okkar starfi.

Afkoma

Afkoma félagsins var mjög góð en alls nam hagnaður þess 2,6 milj. króna. Þetta er mun betri árangur en árið á undan.

Rekstur skrifstofu

Flutt var í nýtt húsnæði að Laugavegi 178 og breyttist við það aðstaða félagsins til hins betra. Félagið er nú með séraðstöðu fyrir báða starfsmenn sína auk þess sem ágæt aðstaða er fyrir gögn og smærri fundi innan veggja skrifstofunnar. Félagið hefur einnig aðgang að sameiginlegu rými með Staðlaráði.

Nýr framkvæmdastjóri

Í lok desember var ráðinn nýr framkvæmdastjóri, Hólmfríður Arnardóttir, sem tók í upphafi þessa árs við störfum af Svanhildi Jóhannesdóttur sem láta varð af störfum af heilsufarsástæðum. Stjórn félagsins býður Hólmfríði velkomna til starfa og þakkar jafnframt Svanhildi fyrir sérstaklega vel unnin störf á þeim 10 árum sem hún hefur unnið fyrir félagið.

Stiklað hefur verið á stóru í starfsemi Skýrslutæknifélagsins á síðasta ári sem var mjög viðburðaríkt eins og komið hefur fram. Starfsemi félagsins vakti einnig mun meiri athygli fjölmiðla en áður hefur þekkst en gera þarf enn betur í þeim efnum. Starfsemi Skýrslutæknifélagsins byggir að verulegu leyti á sjálfboðavinnu

en fjölmargir einstaklingar, innan og utan stjórnar, hafa lagt hönd á plóginn og eflt starfsemi félagsins. Þeim vil ég þakka sérstaklega og vonast til að þeir starfi áfram með félaginu að þeim áhugaverðu verkefnum sem fram undan eru. Einnig vil ég þakka starfsmönnum Skýrslutæknifélagsins þeim Svanhildi Jóhannesdóttur framkvæmdastjóra og Ástu Jensdóttur fyrir gott starf á liðnu ári.

Óskar B. Hauksson

Stjórn 2000 og framkvæmdastjóri

Svanhildur Jóhannesdóttir framkvæmdastjóri, Einar H. Reynis meðstjórnandi er hjá Landssíma Íslands, Magnús Sigurðsson meðstjórnandi er hjá Landsteinum, Stefán Kjærnested fyrrverandi gjaldkeri er hjá Ríkisbókhaldi, Hjálmtýr Hafsteinsson varamaður er dósent í tölvunarfræði við HÍ, Eggert Ólafsson fyrrverandi varaformaður er hjá Borgarverkfræðingsembættinu, Hulda Guðmundsdóttir meðstjórnandi er á tölvudeild Ríkisspítala, Óskar B. Hauksson fyrrverandi formaður er hjá Tal hf. og Ingi Þór Hermnannsson fyrrverandi ritari er hjá Olíufélaginu hf.

Ný stjórn og framkvæmdastjóri – 2001

Hólmfríður Arnardótttir framkvæmdastjóri, Einar H. Reynis meðstjórnandi er hjá Landssíma Íslands, Stefán Kjærnested varaformaður er hjá Ríkisbókhaldi, Sigurborg Gunnarsdóttir varamaður er hjá Tölvumiðstöð sparisjóðanna, Hjálmtýr Hafsteinsson, varamaður er dósent í tölvunarfræði við HÍ, Ingi þór Hermannsson meðstjórnandi er hjá Olíufélaginu hf., Brynja Guðmundsdóttir gjaldkeri er fjármálastjóri hjá Skýrr, Eggert Ólafsson formaður er hjá Borgarverkfræðingsembættinu og Svana Helen Björnsdóttir ritari er framkvæmdastjóri Stika.

Frá Orðanefnd

Sigrún Helgadóttir

Að beiðni ritnefndar Tölvumála las formaður orðanefndar allar greinar sem birtast í þessu blaði. Greinarnar voru orðteknar og í sumum tilvikum var höfundum bent á að nota önnur orð. Stundum reyndi orðanefndin að finna heiti ef þau vantaði eða endurskoða eldri heiti. Fjallað verður stuttlega um þau orð sem ástæða þykir að geta um. Hér koma fyrir heiti sem birtast í greinunum eða heiti sem eru notuð í sambandi við upplýsingavernd og orðanefndin vill sérstaklega vekja athygli á. Sumar greinarnar í blaðinu fjalla um frumvarp að íslenskum staðli, frÍST BS 7799, sem er þýðing á breska staðlinum BS 7799, og verður því rætt um nokkur heiti sem þar birtast. Orðanefndinni er ekki kunnugt um afdrif tillagna sinna til ritstjórnar og höfunda greina. Þess vegna er ekki trygging fyrir því að þau orð sem nefndin mælti með séu notuð í greinunum.

encrypt, decrypt

Í 3. útgáfu *Tölvuorðasafns* voru gefnar þýðingarnar *dulrita* fyrir **encrypt** og *ráðning* fyrir **decryption.** Sögnin **decrypt** yrði þá þýdd með *ráða*. Síðastliðið haust fór orðanefndin yfir frumvarp um rafundirskriftir. Þá gafst tækifæri til þess að skoða þessar þýðingar betur. Þá kom fram sú tillaga að nota frekar *dulráða* fyrir **decrypt**. Þarna eru komin samstæð orð, *dulrita* og *dulráða*. Orðanefndin skorar á alla þá sem tala um upplýsingavernd að útrýma hinni hræðilegu sögn *dulkóða*. Mörgum finnst *kóði* vera sóðalegur, sauðalegur og kauðalegur.

public key encryption, single key encryption, public key, private key

Public key encryption og **single key encryption** eru tvær aðferðir við að dulrita og dulráða gögn. Þegar aðferðin **single key encryption** er notuð eru upplýsingar dulritaðar og dulráðnar með sama lykli. Þess vegna er lagt til að sú aðferð sé kölluð *einlykla dulritun*. Þegar notuð er aðferðin **public key encryption** eru notaðir tveir lyklar sem vinna saman. Báða lyklana þarf til þess að dulrita og dulráða upplýsingar. Unnt er að dulrita og dulráða með hvorum lyklinum sem er. Hver sem tekur þátt í slíkum gagnasendingum hefur yfir að ráða tveimur lyklum, **private key** sem er haldið leyndum og **public key** sem er til reiðu fyrir aðra. Sá sem sendir gögn leitar að **public key** viðtakanda gagnanna og dulritar gögnin með honum. Viðtakandi dulræður gögnin með eigin **private key**. Einnig er unnt að dulrita gögn með **private key** sendanda. Viðtakandi dulræður gögnin síðan með **public key** sendanda og þar með er sannað að gögnin séu frá þeim sem ræður yfir samsvarandi **private key**. Þegar 3. útgáfa Tölvuorðasafns var undirbúin lagði orðanefndin til að **private key** héti *einkalykill* og **public key** *dreifilykill*. Hugmyndin var sú að dreifilykli væri dreift til þeirra sem vildu nota hann. Nýlega hefur nefndin endurskoðað þessar þýðingar og reynt að átta sig betur á merkingu þessara heita. Báðir lyklarnir eru í eðli sínu einkalyklar. Ný tillaga er því sú að kalla **private key** *leynilykil*, þar sem honum er haldið leyndum og **public key** *reiðulykil* þar sem hann er til reiðu fyrir alla sem vilja nota hann. Í Tölvuorðasafninu var gefin þýðingin *ósamhverf dulmálsfræði* fyrir **public key cryptography** þar sem nota þarf tvo lykla sem eru ekki eins. Ný tillaga er að kalla **public key encryption** *tvílykla dulritun* í samræmi við *einlykla dulritun* fyrir **single key encryption**. **Public key cryptography** mætti þá kalla *tvílykla dulmálsfræði*. Lýsinguna á tvílykla dulritun hér að ofan mætti endurrita á eftirfarandi hátt með því að nota orðin *leynilykill* og *reiðulykill*:

> Hver sem tekur þátt í slíkum gagnasendingum hefur yfir að ráða tveimur lyklum, *leynilykli* og *reiðulykli*. Sá sem sendir gögn leitar að *reiðulykli* viðtakanda gagnanna og dulritar gögnin með honum. Viðtakandi dulræður gögnin með eigin *leynilykli*. Einnig er unnt að dulrita gögn með *leynilykli* sendanda. Viðtakandi dulræður gögnin síðan með *reiðulykli* sendanda og þar með er sannað að gögnin séu frá þeim sem ræður yfir samsvarandi *leynilykli*.

Gott væri að fá skoðun lesenda á þessum tillögum.

electronic signature

Bein þýðing á heitinu **electronic signature** er *rafræn undirskrift*. Til þæginda mætti hugsanlega stytta það í *rafundirskrift*.

(hyper)link, url

Heitið **url** er skammstöfun á **uniform resource locator** og í 3. útgáfu Tölvuorðasafns var gefin þýðingin **veffang**. Samkvæmt Tölvuorðasafninu er *veffang* ‘stafastrengur sem auðkennir annaðhvort lýðnetssetur eða skrá eða þjónustu sem unnt er að fá aðgang að á lýðnetssetri’. Dæmi um veffang er ‘http://www.ismal.hi.is/ob/’ sem er veffang Orðabanka Íslenskrar málstöðvar. En nú virðist sem menn rugli saman veffanginu og einhvers konar tilvísun í veffangið. Margir nota orðið *tengil* eða enska orðið „link“ þar sem eðlilegra væri að nota orðið veffang. Menn tala um að ‘fara inn á tengla eða linka’ eða jafnvel ‘opna tengla eða linka’. Þessir ‘tenglar’ eru oft á heimasíðum og virðast þá vísa á veffang annarrar heimasíðu. Einnig hefur sést orðið *krækja* í þessari merkingu. Orðanefndin fjallaði nýlega um þýðingu á **link** að gefnu tilefni. Fram kom sú hugmynd að kalla **link** *fangvísi* eða einfaldlega *vísi*. Fangvísirinn vísar á veffang, vistfang skjals eða e.t.v. tiltekinn stað í skjali. En oft virðist sem eðlilegra væri að tala um veffangið sjálft. Í þriðju útgáfu Tölvuorðasafns er **hyperlink** þýtt sem *stikluleggur*. Svo virðist sem **link** sé einfaldlega stytting á **hyperlink**. **Hyperlink** er skilgreint sem ‘tilvísun frá tilteknum stað í stikluskjali (hypertext document) til tiltekins staðar í öðru skjali eða sama skjali’. Heitið *fangvísir* getur því mjög vel átt við þetta og tölvunotendur vilja e.t.v. frekar nota það en *stiklulegg*. Einnig mætti koma á framfæri þeirri hugmynd að nota heitið *staðfang* um vefföng og önnur vistföng.

confidentiality, availability, integrity

Þetta eru heiti á þremur grundvallarhugtökum í *frÍST BS 7799*. **Confidentiality** er þar þýtt með *trúnaður*. Trúnaður er ‘það að tryggja að upplýsingar séu aðeins tiltækar þeim sem til þess hafa heimild’. Orðið *trúnaður* virðist því eiga vel við. Í þýðingunni er notað orðið *aðgengileiki* fyrir **availability** en í 3. útgáfu Tölvuorðasafns eru gefnar þýðingarnar *tiltækileiki* og *aðgengileiki*. **Availability** er notað í staðlinum um ‘það að tryggja að upplýsingar og önnur tilföng séu tiltæk þeim sem til þess hafa heimild þegar þess er óskað’. Orðanefndinni finnst enn þá að orðið *tiltækileiki* nái betur merkingu orðsins **availability** í þessu sambandi og leggur því til að það sé notað. Í þýðingunni er notað orðið *heilindi* um **integrity**. Í Tölvuorðasafninu er **data integrity** þýtt með *heilleiki gagna* og skýrt sem ‘eiginleiki gagna sem felst í því að nákvæmni og samkvæmni haldist án tillits til þess hvaða breytingar eru gerðar’. Orðabókarskýring á orðinu *heilindi* er: ‘1. heilsa, heilbrigði. 2. FT hreinskilni, einlægni, falsleysi’. Það er því mjög vafasamt að nota það um **integrity**. Orðanefndin leggur því eindregið til að notað sé orðið *heilleiki* um **integrity**. (Skilgreiningar á **confidentiality** og **availability** hér að ofan eru tilraun greinarhöfundar til þess að þýða skilgreiningar í BS 7799).

infrastructure

Það hefur vafist fyrir ýmsum að finna nothæfa þýðingu á enska orðinu **infrastructure**. Í Orðabanka Íslenskrar málstöðvar má m.a. finna heitin *grunnkerfi*, *innviðir*, *innri gerð* og *innvirki* sem þýðingar á **infrastructure**. Þar sem þetta orð kom fyrir í einni greininni sem orðanefndin fór yfir gafst tækifæri til þess að huga að því hvort finna mætti betri þýðingu. Þá kom fram sú tillaga að nota *innangerð* um **infrastructure** og er þeirri tillögu hér með komið á framfæri.

outsourcing

Orðanefndin gerði fyrir nokkru tilraun til þess að finna íslenskt heiti á það fyrirbæri sem kallast á ensku **outsourcing**. Í orðabók á veraldarvef (FOLDOC) fannst skýring sem lauslega mætti þýða ‘það að borga öðru fyrirtæki fyrir þjónustu sem starfsmenn fyrirtækisins hefðu annars sinnt, t.d. þróun hugbúnaðar’. Í Hagfræðiorðasafni er gefin þýðingin *utankaup*, hk. ft. og skilgreint sem ‘Kaup á framleiðsluhlutum,

tiltekinni þjónustu eða sérfræðiþekkingu frá aðilum utan eigin fyrirtækis.‘Orðanefndin lagði á sínum tíma til að kalla **outsourcing** *aðkaup* eða *aðkeypta þjónustu*. Margir virðast nota um þetta heitin *hýsing* eða *úthýsing*. Í þýðingu á BS 7799 er þetta kallað *notkun verktaka*. Í 3. útgáfu Tölvuorðasafnsins er *hýsing* haft um **content hosting** sem er skylt **outsourcing** en ekki nákvæmlega það sama.

Orðanefndin gerði nýlega aðra atlögu að því að finna heiti fyrir **outsourcing**. Í texta sem fannst á netinu er reynt að skýra muninn á **outsourcing** og því að kaupa þjónustu af öðrum samkvæmt verktakasamningi. Samkvæmt því virðist hugmyndin með **outsourcing** vera sú að fela öðrum tiltekið verkefni með ákveðnum skilyrðum en skipta sér að öðru leyti ekki af því hvernig verktakinn innir verkið af hendi. Það virðist því vera nauðsynlegt að finna sérstakt heiti á þetta fyrirbæri. Eftir miklar umræður komst orðanefndin að þeirri niðurstöðu að best væri að nota tvö mismunandi heiti, *úthýsingu* og *hýsingu,* eftir því hvort litið er á málið frá sjónarhóli kaupanda eða seljanda þjónustunnar. Sá sem kaupir þjónustuna *úthýsir* verkefninu og kaupir *hýsingu*. Sá sem selur þjónustuna *hýsir* verkefnið eða býður *hýsingu*. En vert er að benda á að þarna er verið að teygja á merkingu sagnarinnar að *úthýsa* en samkvæmt Íslenskri orðabók merkir hún ‘neita um húsaskjól, gistingu’. Orðanefndin telur að ekki verði alvarlegur árekstur þó að notað sé orðið *hýsing* bæði um **hosting** og **outsourcing**.

firewall

Í 3. útgáfu Tölvuorðasafns er gefin þýðingin *netvörn* á enska heitinu **firewall** en margir virðast vilja þýða beint og tala um *eldvegg*. Orðanefndin leggur eindregið til að orðið *netvörn* sé notað. Það er erfitt að ímynda sér ‘eldvegg’ inni í miðlaranum í tölvuherberginu.

Internet

Í 3. útgáfu Tölvuorðasafns var lagt til að nota orðið *Lýðnet* um *Internet*. Orðanefndin kýs enn að nota það heiti en vill nú rita það með litlum staf, þ.e. *lýðnet*.

virus

Almenn sátt virðist um að nota orðið *veira* fyrir **virus** og er eindregið lagt til þess að menn noti það en ekki orðmyndina *vírus*.

cookie

Fyrir nokkru var orðanefndin beðin um þýðingu á þessu fyrirbæri og lagði þá til þýðinguna *smygildi* en því orði hefur ekki verið haldið á lofti. Með því að leita í fyrrnefndri orðabók á vefnum fæst skilgreining sem þýða mætti sem ‘upplýsingapakki sem sendur er í tölvu notanda þegar hann fær aðgang að vefmiðlara og er síðan sendur til baka í hvert skipti sem notandinn fær aðgang að þeim miðlara’. Þegar smygildið kom til umræðu í nefndinni var sú tilfinning sterkust að verið væri að smygla sér inn í tölvu notandans. Smygildi er skylt sögninni að smjúga. Þessu orði er hér með komið á framfæri.

PIN

PIN er skammstöfun á **personal identification number**. Bent er á þýðinguna *einkanúmer*, sem er í Tölvuorðasafninu.

password

Einu sinni enn skal það ítrekað að heppilegra er að nota *aðgangsorð* fyrir **password** en *lykilorð*. *Lykilorð* á að nota sem þýðingu á **key word** sem er ekki það sama og **password**.

smart card

Margir nota *snjallkort* um **smart card** þótt sumir segi enn þá „smart kort“. Í Tölvuorðasafninu er gefin þýðingin *gjörvakort* um **smart card** enda er gjörvakort ‘kort með gjörva og geymslu fyrir gögn’. Að mati orðanefndarinnar lýsir orðið *gjörvakort* betur hlutverki kortsins en *snjallkort*. Það má einnig benda á að orðið *snjallkort* hefur vissan annmarka. Þegar orð er myndað þannig að lýsingarorð er fyrri liður og nafnorð seinni liður er lýsingarorðið venjulega lýsing á seinni liðnum. Dæmi um þetta er *hollvinur*, þ.e. ‘vinur sem er hollur’. En það er erfitt að hugsa sér að dauðir hlutir séu snjallir, þótt það geti átt við menn og hugmyndir. Einnig má benda á að oft eru nafnorð í seinni lið slíkra orða afleidd. Má þar nefna orð eins og *góðæri*,

jafndægri og *blágresi*. Sú leið virðist ekki fær þegar snjallkortið er annars vegar. Ef menn vilja kenna kortið við 'snilld' mætti e.t.v. búa til orð eins og *snilldarkort* eða *snillikort*. Þess má geta að Púki Friðriks Skúlasonar kvartar yfir orðinu *snjallkort* en finnur ekkert athugavert við orðin *snilldarkort* og *snillikort*. En eins og lesendur Tölvumála vita notar Friðrik í forriti sínu reglur um það hvernig samsett orð skuli búin til. Að lokum skal tekið fram að orðanefndin mælir eftir sem áður með orðinu *gjörvakort*.

SSO

Í einni greininni sem á að birta í blaðinu var talað um **SSO** sem mun vera skammstöfun á **Single Sign On**. Einnig var talað um SSO-búnað og SSO-kerfi. Orðanefndin hugleiddi hvort nota mætti *einskráning* um **SSO** og tala jafnframt um *einskráningarbúnað* og *einskráningarkerfi*.

registry file

Í sömu grein kom fyrir orðið *skrásetningaskrá* (**registry-skrá**). Orðanefndin giskaði á að „registry-skrá" væri **registry file** á ensku. Ef menn vilja nota þessa þýðingu ætti orðmyndin að vera *skrásetningarskrá*. En það orð er e.t.v. ekki heppilegt þar sem *skrá-* kemur fyrir tvisvar í því. Eftir að hafa skoðað þessa skrá í tölvunni veltir orðanefndin því fyrir sér hvort unnt sé að nota *búnaðarskrá*. Þarna virðist vera skrá um allan búnað tölvunnar, bæði vélbúnað og hugbúnað.

verify

Að gefnu tilefni skal bent á að orðanefndin telur að *sannprófa* sé nákvæmari þýðing á **verify** en *sannreyna*.

risk assessment, risk analysis

Í frÍST BS 7799 virðist ýmist notað *áhættumat* eða *áhættugreining* um **risk assessment**. Það virðist þó merkingarmunur á þessum orðum og eðlilegra virðist að nota *áhættumat* sem þýðingu á **risk asessment** og *áhættugreiningu* sem þýðingu á **risk analysis**.

information security

Enskt heiti fyrrnefnds staðals er „Information Security Mangement". Í staðlinum er **information security** skilgreint sem 'varðveisla trúnaðar, heilleika og tiltækileika upplýsinga'. Það virðist því liggja beint við að þýða **information security** með *upplýsingavernd* eins og þýðandinn gerir en ekki *upplýsingaöryggi*.

information product

Þetta heiti er í staðlinum og virðist ná yfir hvers kyns upplýsingar. Orðanefndin leggur til að þetta sé kallað *fróðbúnaður* í samræmi við fyrri tillögur nefndarinnar um að stytta ýmis heiti þar sem *upplýsingar* koma fyrir og nota *fróð* í staðinn.

skýrslurækni

Að lokum ein gamansaga úr starfi orðanefndar. Lesendur Tölvumála muna eflaust að fyrir jól var talað um að breyta nafni Skýrslutæknifélagsins í „takt við nýja tíma". Fyrir aðalfund var lögð tillaga um að nýtt heiti yrði „SKÝ - Félag um upplýsingatækni". Sem betur fer var þessi tillaga ekki borin undir atkvæði. En formaður orðanefndar sat aðalfundinn og sendi síðan öðrum nefndarmönnum tölvuskeyti til þess að greina frá afdrifum tillögunnar. Þá vildi ekki betur til en svo að „ásláttarpúkinn" fór á kreik og í titli skeytisins stóð „Nýtt nafn á Skýrsluræknifélagið". Orðanefndarmenn tóku fljótt við sér og spurt var hvort ekki væri dygð að vera „skýrslurækinn" eins og guðrækinn, kirkjurækinn, trúrækinn og þjóðrækinn? Vonandi hafa allir lesendur Tölvumála tileinkað sér þá dygð að vera skýrsluræknir.

Niðurlagsorð

Eins og áður hvetur orðanefnd lesendur Tölvumála til þess að láta heyra í sér. Orðanefndin vill gjarnan fá tillögur og óskir um ný orð. Hafa má samband við formann í síma 580 8400, tölvupóstfang: sigrun.h@simnet.is. Einnig má benda lesendum á Orðabanka Íslenskrar málstöðvar þar sem eru rúmlega 30 orðasöfn aðgengileg öllum, þar með talin 3. útgáfa Tölvuorðasafns. Orðabankinn var opnaður öllum notendum 1. janúar 2001. Veffang orðabankans er eins og áður segir: http://www.ismal.hi.is/ob/.

Öryggi tölvukerfa

Sigurður Erlingsson

Helsta ógn fyrirtækja er misnotkun innanhúss eða um 80% allra tölvumisferla og aðeins 20% kemur utan frá

Hvaða ógnir steðja að tölvukerfum? Markaðurinn hérlendis virðist hræðast mest innbrot frá utanaðkomandi aðilum í tölvukerfin sín, hvort heldur stuldur eða eyðing á gögnum eða önnur skemmdarverk. Margir hafa sett upp miðlæga eldveggi (netvörn) til að stjórna aðgengi að tölvukerfunum og utanaðkomandi umferð. En er það helsta ógn tölvukerfa? Eru þær lausnir sem eru við lýði hér á landi nægjanleg vernd? Miðað við erlendar kannanir þá er helsta ógn fyrirtækja misnotkun innanhúss eða um 80% allra tölvumisferla og aðeins 20% kemur utan frá. Reyndar er í sumum tilfellum sambland, þ.e. misnotkun eða réttara sagt rangnotkun á tölvu innanhúss getur orsakað ógn utanað.

Ef um 80% af misnotkun er innanhúss, hverjar eru þá þær ógnanir og hvað er til ráða? Til að byrja með þarf að skilgreina vel aðgengi hvers starfsmanns, umgangur hans með trúnaðarskjöl á tölvukerfinu. Einnig er rétt að skoða hvernig er staðið að notkun og meðhöndlun á aðgangsorðum sem og notendanöfnum.

Aðgangsstjórnun

Þegar er verið að taka á þessum vandamálum er oft byrjað á því að setja reglur um aðgangsorð, þau skulu vera samsett af bókstöfum og tölustöfum og yfirleitt ekki þekkt orð, þvinga notendur að skipta um aðgangsorð á 30 – 90 daga fresti og svo framvegis. Þessar reglur eru mjög góðar, en í flestum tilfellum falla þær á því að aðgangsorðin eru oft það flókin og sérstaklega þar sem notendur þurfa mörg mismunandi aðgangsorð, þá er það oftast reglan að þeir rita þessi aðgangsorð niður á blað og geyma nálægt tölvunni. Þessi stranga regla er þar af leiðandi fallin um sjálft sig því utanaðkomandi á greiða leið að tölvukerfinu. Til að leysa þennan vanda, og einnig til að minnka álag á kerfisstjóra við að leiðbeina notendum við útskiptingu á aðgangsorðum, er rétt að skoða möguleika á að setja upp aðgangsstjórnunarkerfi fyrir tölvukerfi.

Einkaeldveggurinn lokar öllu aðgengi að tölvunni og tölvukerfinu fyrir utanaðkomandi aðilum.

Sá aðgangsstjórnunarbúnaður sem ég ætla að taka dæmi um vinnur þannig að notendur þurfa ekki lengur að nota aðgangsorð og notendanafn. Þessar upplýsingar eru vistaðar á snjallkorti, þannig að þegar notandi skráir sig inn í tölvukerfið þá setur hann snjallkortið í snjallkortalesara, slær inn PIN kóða til að opna kortið. Þá sér aðgangsstjórnunarkerfið um að lesa gögnin af snjallkortinu og opna aðgang. Þessi lausn er sérstaklega hentug fyrir þá aðila sem þurfa síðan að skrá sig inn á mismunandi kerfi með aðgangsorði, því hægt er að láta einingu í aðgangsstjórnunarkerfinu um að halda utan um öll þau aðgangsorð, svokallað Single Sign On (SSO). SSO búnaðurinn heldur utan um öll aðgangsorð í tölvukerfinu fyrir hvern notanda fyrir sig og sér um að opna aðgang þegar notandinn óskar þess. SSO kerfið sér einnig um að skipta um aðgangsorð í mismunandi kerfum án þess að notandi verði var við það. Kostir notenda eru þeir að í stað margra aðgangsorða áður þá þarf einungis að muna PIN númer að snjallkortinu. Kostir kerfisstjóra er að öll umsýsla með öll aðgangsorð fer fram á einum stað í SSO kerfinu og lokun á aðgengi notenda sem hættir er einföld: Kortið skráð ógilt. Kostir eiganda tölvukerfisins eru að minni líkur eru á að óviðkomandi aðili sé á svæði sem hann á ekki að vera á. Með strangri stjórnun á gögnum í aðgangsstjórnunarkerfinu er hægt að stýra

Ýmislegt er í gangi í tölvunni án þess að notandi verði var við það.

á öflugan hátt aðgengi og meðhöndlun með gögnum, eins og hvaða gögn má prenta út, senda í tölvupósti eða eyða. Aðgangsstjórnunarkerfi er búnaður sem eykur öryggi tölvukerfisins til muna og einnig mun þægilegra í notkun fyrir notendur og kerfisstjóra.

Netið

En skoðum betur notkun á Internetinu, netpósti og samtengingu á milli tölva og tölvukerfa og hversu örugg þessi samskipti eru. Í upphafi er rétt að spyrja spurningar eins og:

Veistu hvað gerist á bak við tjöldin á meðan þú vafrar grunlaus um netið?

Hefurðu aldrei áhyggjur af því, sem gæti verið að fara fram á meðan þú ert að greiða í gegnum netbankann eða uppfæra vefsíðuna, eða einfaldlega þegar þú ert að skoða póstinn þinn?

Flestir Internetnotendur hafa litla hugmynd um hvað er í raun og veru að gerast á tölvunni um leið og vefsíða er heimsótt. Sannleikurinn er sá að tölvan og tölvunetið getur verið opið fyrir hverskyns áreiti og árásum, jafnvel þó að miðlægur eldveggur sé til staðar.

Á sumum síðum eru settar í gang aðgerðir sem t.d. fylgjast með hvaða hnappa notandinn er að nota á lyklaborðinu og jafnvel er skoðað innihald diska

Við prófun tölvuöryggissérfræðinga hjá Arcis ehf, þar sem skoðað er í sérstakri skjámynd hvað er að gerast í tölvunni þegar verið er að fara á hinar ýmsu vefsíður, kom í ljós að mikill fjöldi af „kökum“ er vistaður á tölvunni. Á sumum síðum eru settar í gang aðgerðir sem t.d. fylgjast með hvaða hnappa notandinn er að nota á lyklaborðinu og jafnvel er skoðað innihald diska. Ýmsar grunsamlegar aðgerðir eru einnig í gangi, eins og fikt við skrásetningaskrá (registry-skrá) tölvunnar sem er mjög alvarlegur hlutur því sú skrá sér um allar stillingar á tölvunni, breytingar á henni geta stöðvað virkni forrita eða jafnvel tölvunnar sjálfrar.

Ógnirnar eru líklega meiri en við gerum okkur grein fyrir

Einkaeldveggur

Einkaeldveggur er ný og öflug öryggislausn sem verndar tölvur fyrir árás frá Interneti eða innraneti og getur hann verið púslið sem vantar til að laga heildarmyndina. Einkaeldveggurinn er settur upp á útstöðvar, hvort heldur er fartölvu eða borðtölvu og verndar þær fyrir innbrotum og árásum sem miðlægur eldveggur eða veiruvarnarhugbúnaður ráða ekki í öllum tilfellum við.

Einkaeldveggurinn bægir frá hættulegum hugbúnaði sem oft er vistaður frá Internetinu án vitundar notenda og lokar einnig öllum aðgangi að tölvunni og tölvunetinu fyrir utanaðkomandi. Notkun á Java og ActiveX forritum á Internetinu hefur aukið enn frekar á hættuna fyrir notendur að fá hættulegar sendingar til sín. Forrit getur einfaldlega komið sér fyrir í tölvunni eða á tölvunetinu um leið og smellt er á hnapp á einhverri síðu. Misjafnt er hvað þessi hugbúnaður er að gera, en það er allt frá því að eyða upp minni í tölvunni og þannig hægja á allri vinnslu, opna aðgang fyrir utanaðkomandi til að „njósna“, eyðileggja eða eyða gögnum og gera tölvuna óstarfhæfa.

Miðlægur eldveggur er nauðsynlegur í öllum tölvukerfum, en dugar ekki einn og sér miðað við þær ógnir sem eru til staðar. Gáttir á eldveggjum eru hafðar opnar fyrir t.d. Internetsamskipti, póstsamskipti og jafnvel einhver fleiri. Þessar gáttir eru nýttar af utanaðkomandi aðilum til að tengjast tölvukerfinu og þá oftast í gegnum útstöðvar sem heimsækja vefsíður á Internetinu. Þess vegna er nauðsynlegt að stjórna aðgengi þeirra þannig að þeim gáttum sé einnig lokað.

Ógnirnar eru líklega meiri en við gerum okkur grein fyrir. Mjög mikið er um að verið sé að skoða hvað hver og einn er að gera þegar hann er að ferðast um á Internetinu. Gylliboðum um frían hugbúnað sem hægt er að nálgast fylgir oft óumbeðinn bónus, eins og trójuhestur sem plantar sér um leið í tölvunni eða tölvukerfinu og

Við erum flutt úr sveitinni í stórborgina

opnar gátt inná tölvukerfið fyrir þann sem bauð þessa fríu notkun.

En er þessi ógn þá orðin það mikil að ekki sé þorandi að leyfa Internetaðgang að tölvukerfum? Mitt svar er neitandi, en stjórnendur fyrirtækja verða að aðlaga sig að breyttum aðstæðum. Við erum flutt úr sveitinni í stórborgina í þeim skilningi, ekki er óhætt að skilja dyr og glugga eftir opna, loka verður öllum aðgengileiðum ekki einungis aðalhurðinni. Einkaeldveggurinn er eitt púslið sem vantaði til að gera myndina heila, tryggja öryggi gagna, minnka hættu á eyðileggingu og þjófnaði. Notendur geta með mun meira öryggi notað Internetið og tölvupóst án þess að eiga á hættu að valda óbætanlegum skaða.

Ýmislegt er hægt að tína til fleira í þeim leiðum sem hægt er að fara til að auka öryggi tölvukerfa. Fyrsta skrefið hjá stjórnendum fyrirtækja er að fá upp skýra stöðu mála og síðan fá tillögur að bættu öryggi frá fyrirtækjum sem sérhæfa sig í tölvuöryggismálum.

Sigurður Erlingsson
framkvæmdastjóri Arcis ehf.

Hér má sjá Svanhildi Jóhannesdóttur fyrrverandi framkvmdastjóra með gjöf sem hún fékk frá Skýrslutæknifélagi Íslands en Opin Kerfi styrkti félagið við kaup á þessari fistölvu.

Öryggisgæsla, nýir möguleikar

Bergsteinn R. Ísleifsson

Hefur fjarskiptabyltingin breytt einhverju fyrir öryggisgæslu? Þegar horft er til baka nokkur ár aftur í tímann virðist í fyrstu lítið hafa gerst. Þegar betur er að gáð, hefur ýmislegt gerst. Öryggiskerfi eru í grunninn til að sinna:

- Viðvörun gagnvart innbroti.
- Viðvörun gagnvart öðru skilgreindu hættuástandi (eldur,vatn, hiti, o.s.frv.)
- Stjórnun á aðgangi hver hefur aðgang hvar og hvenær.
- Boðum til öryggismiðstöðvar um hættuástand.

Undanfarin ár og ekki síst á þessu og síðasta ári hefur þróunin verið hröð, kröfurnar aukast og fjarskiptaleiðum fjölgar.

Verkefnunum og möguleikum hefur einnig fjölgað mjög. Hér ætla ég að minnast á nokkra möguleika sem áhersla hefur verið lögð á.

Fyrir öryggisvörð og viðbragðsaðila er fátt betra en að hafa sem nákvæmastar upplýsingar um viðvörun þegar brugðist er við

- Nákvæmar upplýsingar um hættuástand berist til öryggismiðstöðvar.
- Öryggismiðstöð hefur aðgang að myndavélum á vaktstað yfir IP-net.
- Öryggismiðstöð vaktar kerfi gegnum IP-net í stað hefðbundinna símalína.
- Fyrirtæki stjórnar aðgangi allra starfsmanna í mismunandi útibúum frá sama stað.

Nákvæmar upplýsingar berast til öryggismiðstöðvar

Fyrir öryggisvörð og viðbragðsaðila er fátt betra en að hafa sem nákvæmastar upplýsingar um viðvörun þegar brugðist er við.

Þróunin í lausnum á myndgæslu yfir net hefur verið geysilega ör á síðustu árum

Gott dæmi er að ímynda sér stórt hús og það eina sem er vitað er að kerfi hefur skynjað boð um innbrot. Þetta voru þær upplýsingar sem öryggisverðir sem svöruðu innbrotsboðum höfðu úr að spila fyrir nokkrum árum síðan.

- Í dag þegar öryggisvörður svarar t.d. innbrotsboði hefur hann upplýsingar um:
- Hvenær kerfið var síðast sett á vörð, og hver gerði það.
- Hvaða skynjari og hvar í húsinu kom fyrst boð um innbrot.
- Hafa fleiri skynjarar og þá hvaða gefið boð?
- Viðvörunarsögu hússins.
- Upplýsingar um sérstaka áhættu.

Með þessar upplýsingar er auðveldara að sinna skoðun á staðnum. En samt sem áður er þetta *eins og að skoða húsnæði með bundið fyrir augun,* við höfum ýmsa skynjara en ekki vissu. Því ríkir enn óvissa um ástand þar til öryggisvörður hefur komið á staðinn og staðfest hvað er að.

Öryggismiðstöð hefur aðgang að myndavélum á vaktstað yfir IP-net

Í dag er Öryggismiðstöð Íslands með aðgang að myndavélakerfum nokkurra fyrirtækja yfir IP-net. Þróunin í lausnum á myndgæslu yfir net hefur verið geysilega ör á síðustu árum. Nú þegar bandvíddargjöld lækka og hverfa innan Íslands þá skapast miklir möguleikar. *Nú er öryggisgæsla ekki eins og blindingsleikur.* Öryggisvörður getur haft augu á staðnum um leið og boð berst. Því getu hann kannað húsnæði strax og gert ráðstafanir þó að hann sé ekki staddur á staðnum.

Fyrir notendur opnast einnig nýr heimur. Það er auðvelt í dag að velta upp lausn þar sem notandi fær sms boð á símann sinn þegar einhver hringir á dyrabjöllunni heima, smellir á síðu á netinu og sér mynd af þeim sem stendur fyrir utan og getur tala við hann í gegnum dyrasímann. Ef hann kýs að hleypa t.d. iðnaðarmanni sem von var á inn, er stutt á hnapp. Síðan má fylgjast með viðkomandi.

Þetta er dæmi um notkun sem möguleg er í dag. Eða þá að leikskólar eða grunnskólar gefi foreldrum aðgang á heimasíðu sinni að myndavélum skólans á ákveðnum tímum. Þannig er hægt að fylgjast með skólaskemmtunum sem æskilegt væri að „útvarpa“ á netinu til að foreldrar geti fylgst með án þess að eyða meiri tíma í akstur til og frá skóla heldur en skemmtun varir. Öryggismiðstöð notar síðan sömu myndavélar til öryggisgæslu.

Í örri þróun er einnig vistun myndmerkja yfir net og mun öryggismiðstöð bjóða viðskiptavinum sínum að vista myndmerki frá þeim á öruggum stað þar sem afrit eru trygg

Í örri þróun er einnig vistun myndmerkja yfir net og mun öryggismiðstöð bjóða viðskiptavinum sínum að vista myndmerki frá þeim á öruggum stað þar sem afrit eru trygg. Gæði stafrænnar upptöku eru óumdeilanlega betri en fléttuð (multiplexuð) upptaka á myndband.

Augljós kostur í upptöku er að tengja hreyfingu í myndfleti við upptöku. Til hvers að vista mynd eftir mynd þar sem ekkert breytist. Nærtækara væri að vista einungis ef eitthvað er að gerast, hreyfing hefur verið greind eða tíminn er mikilvægur. Með stafrænni upptöku má sameina þetta allt, að mynd sé einungis vistuð ef ástæða er til.

Fyrir öryggisgæslu eru allar fréttir af aukinni netvæðingu og meiri bandvídd mikilvægar. *En því miður er varaorka og öryggi þessara neta í neyð enn spurning* sem ekki hefur fengist endanlegt svar við.

Fyrirtæki stjórnar aðgangi allra starfsmanna í mismunandi útibúum frá sama stað

Hér áður gat þrautin verið þyngri ef óskað var eftir því að margir staðir væru samtengdir sem um eitt heildar öryggiskerfi væri að ræða. Niðurstaðan var oftar en ekki sú að líta á eitt hús sem eitt kerfi og öll stjórnun og breytingar væru gerðar á viðkomandi stað. Möguleg var einungis samtenging aðgangskerfa með leigulínum.

Nú þykir sjálfsagt að hægt sé að byggja upp innbrotaviðvörun, aðgangs- og almennt öryggiskerfi, sem eina heild í mörgum byggingum. Staðlaður hugbúnaður leyfir stjórn á mörgum stöðum frá einni staðsetningu eins og um eina einingu sé að ræða.

Öryggismiðstöð Íslands býður heildarlausnir fyrir fyrirtæki þar sem samskipti kerfisins fara um þær IP-fjarskiptalagnir sem þegar eru til staðar. Á þann hátt er ekki verið að auka rekstrakostnað við fjarskipti. Til viðbótar öryggis nýtir búnaðurinn aðrar fjarskiptaleiðir í neyð (t.d. símalínur, GSM, D-rás ISDN)

Frá völdum stöðum er þannig hægt að fylgjast með stöðu öryggiskerfa eða opnunar á hurðum, hita í rýmum og öðrum viðvörunum sem þörf er á.

Það virðist sem nú fyrst sé sú hugsjón í sjónmáli að vegalengdir skipti ekki máli. Á hagkvæman hátt getur öryggismiðstöð nú sinnt öryggisgæslu í fyrirtækjum allan sólarhringinn eins og öryggisvörður væri á staðnum.

Bergsteinn R. Ísleifsson, framkvæmdastjóri Öryggismiðstöðvar Íslands hf.

Að lesa staðal - til öryggis

Stjórnun upplýsingaverndar - 1. hluti: Vinnureglur fyrir stjórnun upplýsingaverndar

Þorgeir Sigurðsson

Staðallinn gengur út frá því að upplýsingar séu verðmæti og þess vegna þurfi að gæta þeirra eins og fjármuna

Hvort sem mönnum líkar það betur eða verr, munu með vaxandi tölvunotkun og aukinni notkun stafrænna gagna, verða til sífellt stærri gagnabankar með sífellt verðmætari upplýsingum sem fara verður með af nærgætni og í samræmi við lög.

Staðlar eru sjaldan skemmtilegir aflestrar. Oft er gert ráð fyrir að aðeins tæknimenn séu færir um að skilja þá og sjaldan sem stjórnendur fyrirtækja kæra sig um að kynnast þeim of náið. frÍST BS 7799 er hins vegar óvenjulegur staðall að því leyti að hann lýsir ekki tæknilausnum, enda er hann ætlaður stjórnendum fyrirtækja og er vonast til að hann verði þeim fyrirmynd að stefnumörkun sem verður að vera skiljanleg hverjum starfsmanni fyrirtækisins eða stofnunarinnar.

Góðar starfsvenjur

frÍST BS 7799 er frumvarp að íslenskum staðli um öryggismál sem er til umsagnar fram til 1. apríl 2001. Um er að ræða þýðingu á breskum staðli, BS 7799, sem einnig hefur verið gerður að ISO/IEC staðli (ISO 17799). Staðallinn gengur út frá því að upplýsingar séu verðmæti og þess vegna þurfi að gæta þeirra eins og fjármuna. Við getum hugsað um staðalinn sem nokkurs konar gátlista sem stjórnendur ættu að lesa sér til áminningar um ýmis atriði og til að koma á sameiginlegum skilningi þegar kröfur eru gerðar um upplýsingaöryggi eða persónuvernd. Hins vegar verður hvert fyrirtæki að útfæra staðalinn nánar og laga að sínum þörfum. Í staðlinum segir eftirfarandi í lok inngangs (bls 4):

> „...Líta má á þessar reglur um góðar starfsvenjur sem fyrstu drög að leiðbeiningum sem laga þarf að þörfum einstakra fyrirtækja. Ekki er víst að allar leiðbeiningar eða eftirlitsaðgerðir eigi við. Ennfremur kann að vera þörf á frekari eftirlitsaðgerðum sem ekki er getið um í þessu skjali. Í slíkum tilvikum kann að vera gagnlegt að varðveita tilvísanir sem auðvelda þeim sem annast úttektir og samstarfsaðilum að kanna hvort kröfur séu uppfylltar...“

Ætlunin með BS 7799 er sú að íþyngja fyrirtækjum ekki um of með viðamiklum eftirlitskerfum og vottunarferlum. Engu að síður þarf að vera hægt að sannprófa með óháðum vottunaraðilum að farið hafi verið að þeim kröfum sem staðallinn og nánari stefnumörkum hvers fyrirtækis kveður á um. Þetta getur aðeins orðið ef markmið og kröfur um upplýsingavernd hvers fyrirtækis eru opinberar og öllum ljósar.

Minni hætta á misnotkun

Við gerð staðalsins voru þarfir fjölþjóðlegra stórfyrirtækja með mörgum útibúum hafðar í huga og var Shell leiðandi í því starfi. Í slíkum fyrirtækjum er nauðsynlegt að tryggja að allar deildir og verktakar noti sömu viðmið, m.a. til að minnka hættu á misnotkun upplýsinga við skipti á gögnum. Til að skýra nauðsyn á slíkum sameiginlegum viðmiðum getum við hugsað okkur að lögregluembættin væru með skrár með ítarlegum upplýsingum um öll fíkniefnamál. Slíkar upplýsingar eru auðvitað vandmeðfarnar en gera verður kröfur um að aðrir sem hafa aðgang að þeim, t.d. Tollstjóraembættið vegna rannsókna á smyglmálum, hafi sams konar reglur um meðferð þeirra eins og lögreglan.

Meðal dæma sem taka má um atriði sem nefnd eru í staðlinum og gæti þurft að hafa á gátlistum fyrirtækja eru efirfarandi:

- Þörfin á því að gera áhættumat, þ.e. meta hverjar líkur séu á frávikum í öryggismálum og hversu alvarlegar afleiðingar þau geta haft.
- Þörfin á því að skrifa stefnumótunarskjal um upplýsingavernd. Þetta gæti t.d. þýtt fyrir myndbandaleigu að taka fram að farið verði með upplýsingar um viðskipti viðskiptavina sem trúnaðarmál.
- Þörfin á því að gera tiltekinn aðila ábyrgann fyrir fjárhagslega mikilvægum gögnum, svo að tryggt sé að það sé einhver aðili innan fyrirtækis sem sjái sér skylt að verja upplýsingaeigur þess.
- Þörfin á áætlunum til að tryggja órofinn rekstur þegar fyrirtæki verður fyrir

áföllum, t.d. vegna rafmagnsleysis.
- Þörfin á því að skilgreina örugg svæði í kringum upplýsingavinnslu og að skipuleggja starfsemi fyrirtækisins þannig að ekki sé óþarfa umferð um slík svæði.

Hvort sem mönnum líkar það betur eða verr, munu með vaxandi tölvunotkun og aukinni notkun stafrænna gagna, verða til sífellt stærri gagnabankar með sífellt verðmætari upplýsingum sem fara verður með af nærgætni og í samræmi við lög. Á sama tíma, munu sífellt fleiri einstaklingar og tölvukerfi vinna með slíkar upplýsingar með aukinni netvæðingu og samtengingu kerfa. Þetta mun verða til þess að þörf verður á vönduðum og raunsæjum verklagsreglum fyrirtækja sem BS 7799 er ætlað að leggja grunn að.

Þorgeir Sigurðssson er framkvæmdastjóri FUT (Fagráð í upplýsingatækni)

Nýir viðskiptahættir með UNSPSC

- eitt alþjóðlegt flokkunarkerfi fyrir vörur og þjónustu

Guðbjörg Björnsdóttir

Netvæðing viðskipta milli fyrirtækja (B2B) á sér nú stað víða um heim. Væntingar flestra eru að ná megi fram lægri kostnaði, betri yfirsýn, betri stjórnun og stærri mörkuðum

Vel skipulagt, alþjóðlegt flokkunarkerfi fyrir vörur og þjónustu er ein af undirstöðum þess að bæði seljendur og kaupendur njóti hagræðingar af netvæðingu innkaupa og þátttöku í rafrænum markaðstorgum. UNSPSC (Universal Standard Products and Services Classification) - er þannig kerfi. Það er meðal annars útbreitt á helstu rafrænu markaðstorgum fyrirtækja og var nefnt sem viðmið í nýlegu útboði Ríkiskaupa um rekstur á rafrænu markaðstorgi ríkisins (RMR).

Fyrir kaupendur og seljendur

Rafræn viðskipti hafa vakið áhuga fyrirtækja vegna þeirra möguleika sem í þeim felast til að gera innkaup hagkvæmari. Enda hafa erlendar kannanir leitt í ljós að með rafvæðingu innkaupa megi lækka kostnaðinn við þau um meira en helming. En rafvæðing viðskipta hefur kosti fyrir seljendur ekki síður en kaupendur.

Umfang viðskipta, svo sem magn, upphæðir, fjöldi færslna, samskipti og „handavinna“ starfsmanna, er sífellt að aukast. Um leið verður flóknara fyrir stjórnendur að greina upplýsingar og halda yfirsýn. Leitin að hagstæðum samningum tekur aldrei enda. Af þessu vex jafnt og þétt þörfin fyrir hagræðingu í aðfangakeðjunni og staðlað skipulag á upplýsingum. Með stöðlun og þeirri auknu sjálfvirkni sem netvæðing viðskipta býður uppá má ná verulegri hagræðingu, lækkun kostnaðar, meiri hraða og auknum viðskiptum - fyrir bæði kaupendur og seljendur.

Helstu ástæður kaupenda fyrir þátttöku í rafrænum viðskiptum eru þær að þeir vilja lækka kostnað og bæta innkaupaferli og fjármálastjórnun. Seljendur eru óðum að gera sér grein fyrir því að með rafrænum viðskiptum geta þeir lækkað kostnað, bætt áætlanagerð og stjórnun, treyst viðskiptasambönd, stækkað markaði og grætt upplýsingar um markaðshlutdeild. Ennþá er þó stærsta ástæðan fyrir þátttöku þeirra þrýstingur frá kaupendum. Því er óhætt að segja að þau fyrirtæki sem eru stórir kaupendur stýri þessari þróun í átt að nýjum viðskiptaháttum, þrátt fyrir að ávinningur seljenda geti verið mikill.

UNIVERSAL STANDARD PRODUCTS AND SERVICES CLASSIFICATION

Vöruhópur **44** **- Skrifstofubúnaður, fylgihlutir og rekstrarvörur**

Flokkur
- **10** - Skrifstofuvélar, fylgihlutir og rekstrarvörur
- **11** - Fylgihlutir fyrir skrifstofur og skrifborð
- **12** - Rekstrarvörur fyrir skrifstofur

Tegund
- **15** - Rekstrarvörur fyrir póstsendingar
- **16** - Rekstrarvörur á skrifstofu
- **17** - Skriffæri
- **18** - Leiðréttingarbúnaður
- **19** - Blek- og blýfyllingar

Heiti
- **02** - Blýfyllingar
- **04** - Blekfyllingar

Blekfyllingar = UNSPSC flokkun **44 - 12 - 19 - 04 - (vörunúmer)**

UNSPSC
SRÍ
Staðlaráð Íslands

Eccma eru samtök sem vinna að þróun og notkun staðla í alþjóðlegum rafrænum viðskiptum

UNSPSC er opið alþjóðlegt flokkunarkerfi fyrir vörur og þjónustu og útbreitt á helstu rafrænu markaðstorgum fyrirtækja

Það skal vanda sem lengi á að standa

Þótt dæmi séu um að stórfyrirtæki reki sjálf rafrænan innkaupavettvang þar sem þau tengjast sínum birgjum, þá verður sífellt algengara að bæði kaupendur og seljendur notfæri sér þjónustu fyrirtækja sem sérhæfa sig í rekstri innkaupakerfa eða markaðstorga. Sum þessara fyrirtækja eru reyndar stofnuð af stórum kaupendum.

Á rafrænum viðskiptavettvangi geta viðskiptin farið þannig fram að allt upplýsingaflæðið, t.d. pantanir, staðfestingar og færslur, berist sjálfkrafa um kerfið þannig að birgða- og fjárhagsbókhald seljanda og kaupanda er uppfært jafnharðan.

Með þessu fyrirkomulagi safnast mikilvægar upplýsingar um vöruviðskipti fyrir bæði kaupendur og seljendur, upplýsingar sem nýta má til frekari þróunar viðskiptanna og til betri innkaupa- og birgðastjórnunar. Því meiri sem stöðlunin og sjálfvirknin er því meiri hagræðing næst. Vandað skipulag er forsenda fyrir góðum árangri í rafrænum viðskiptum – alveg eins og í annarri verslun. Á viðskiptavettvangi þar sem fyrirtæki geta keypt og selt vörur þarf skipulag og flokkun vörulista að vera með þeim hætti að mikilvægar upplýsingar séu aðgengilegar. Til þess er UNSPSC flokkunarkerfið notað.

Hvað er UNSPSC?

UNSPSC er opið alþjóðlegt flokkunarkerfi fyrir vörur og þjónustu. Notkun á kerfinu er öllum heimil án endurgjalds og er almenn útgáfa aðgengileg á Netinu, uppfærð ársfjórðungslega. Kerfið er í stöðugri þróun og ný útgáfa með viðbótum og breytingum kemur á tveggja vikna fresti. Til að fylgjast með þessum nýjungum í kerfinu og taka þátt á þróun þess, gerast fyrirtæki félagar í samtökum sem heita Eccma og greiða 250 Bandaríkjadali í árgjald.

Electronic Commerce Code Management Association, eða Eccma, eru samtök sem vinna að þróun og notkun staðla í alþjóðlegum rafrænum viðskiptum. Samtökin halda utan um allt skipulag og þróun UNSPSC. Þau urðu til þegar Sameinuðu þjóðirnar og alþjóðafyrirtækið Dun & Bradstreet sameinuðu flokkunarkerfi sín fyrir vöru og þjónustu í eitt kerfi: UNSPSC. Félagar í Eccma eru fjölmörg stór og smá fyrirtæki, samtök og stofnanir. Sameiginlegur tilgangur þeirra er að styðja uppbyggingu og alþjóðlega útbreiðslu kerfisins.

Fyrir nokkrum árum gerði Dun & Bradstreet könnun sem staðfesti að algengast var að fyrirtæki notuðu eigin innri númerakerfi til að flokka og greina vöruviðskipti. Einnig voru dæmi um að atvinnugreinahópar ynnu saman að því að staðla vöruflokkunarkerfi til að auðvelda viðskipti og upplýsingastjórnun. Þeir sem þessi samræmingarvinna tókst hjá lentu síðan í vandræðum með að viðhalda kerf-

Því meiri stöðlun og samræming þeim mun meiri hagræðing næst í rafrænum viðskiptum

unum. UNSPSC er eina opna flokkunarkerfið fyrir vörur og þjónustu sem er alþjóðlega viðurkennt og útbreitt, einkum í rafrænum viðskiptum.

UNSPSC vöruflokkunarkerfið gerir fyrirtækjum kleift að flokka, með samræmdum hætti, vörur og þjónustu sem þau kaupa og selja. Með því fæst yfirgripsmikil mynd af viðskiptum fyrirtækisins og greining upplýsinga verður mun auðveldari. Greiður aðgangur að þýðingarmiklum upplýsingum um vöruviðskipti leiðir til betri stjórnunar, lægri kostnaðar og aukinna afkasta fyrirtækja. Því fleiri sem nota sama flokkunarkerfi fyrir vöru og þjónustu því fyrirhafnarminna verður að tengja saman vöruupplýsingar milli fyrirtækja ætli þau að taka upp rafrænt viðskiptasamband.

Eitt alþjóðlegt kerfi auðveldar vöruviðskipti verulega. Samræmd eða stöðluð flokkun á vörum og vörutegundum auðveldar leit, eykur áreiðanleika upplýsinga, auðveldar kostnaðargreiningu, áætlanagerð, stjórnun, ákvarðanatöku og eftirlit, lækkar kostnað við vörustjórnun og gerir sjálfvirkar færslur mögulegar.

Stig af stigi eftir þörfum

UNSPSC er stigskipt eða þrepaskipt flokkunarkerfi sem þýðir að hægt er að greina innkaup og vörusölu í misyfirgripsmiklum þrepum eftir þörfum fyrirtækisins sem nýtir upplýsingarnar.

Stigskiptingin samanstendur af tveggja, fjögurra, sex og átta stafa númeruðum þrepum.

Efsta þrepið er „vöruhópurinn“ (segment) með tveggja stafa númer. Undir hverjum vöruhópi eru margir mismunandi „flokkar“ (family) sem halda númeri vöruhópsins framan við eigin tveggja stafa númer. Undir hvern flokk raðast svo mismunandi „tegundir“ (class) sem halda númeri vöruhópsins og flokksins fyrir framan eigin tveggja stafa númer. Undir hverri tegund eru síðan mörg „vöruheiti“ (commodity) sem hvert hefur tveggja stafa númer aftan við númerin sem segja til um hvaða tegund varan tilheyrir innan hvaða flokks og hvaða vöruhóps.

Þannig er t.d. hægt að greina upplýsingar um „skrifstofubúnað, fylgihluti og rekstrarvörur“ með því að skoða allan vöruhópinn sem hefur númerið *44* í kerfinu. Nákvæmari greining gæti tekið til mismunandi flokka í vöruhópnum, t.d. 44 *10* „skrifstofuvélar, fylgihlutir og rekstrarvörur“, eða 44 *12* „rekstrarvörur fyrir skrifstofur“. Enn nánari greining væri tegundarnúmerið *19* í flokki 12, þ.e. 44 12 19 „blek- og blýfyllingar“. Og þeir sem vilja greina vöruviðskiptin enn frekar geta skoðað vöru*heitin* undir blek- og blýfyllingum. Blekfyllingar eru samkvæmt UNSPSC flokkun 44 12 19 04. Í rafrænum viðskiptakerfum er þetta númer síðan

tengt við auðkennisnúmer vörunnar sjálfrar.

UNSPSC auðkennir ekki einstakar vörur og kemur því ekki í stað vörunúmera birgja eða strikamerkinga. UNSPSC sinnir hlutverki sem þessum númerakerfum er ekki ætlað að sinna; að gefa yfirsýn yfir vöruviðskipti í þrepum eftir þörfum þess sem þarf á upplýsingunum að halda. Allar gerðir blekfyllinga safnast á eitt UNSPSC flokkunarnúmer en vörunúmerin geta verið mörg og frá mörgum seljendum.

Með frumkvæði núna getur Ísland skipað sér í forystusveit þeirra sem móta viðskiptahætti framtíðarinnar

Kapp er best með forsjá

Því meiri stöðlun og samræming sem viðskiptaheimurinn kemur sér saman um, þeim mun meiri hagræðing næst í rafrænum viðskiptum. Menn þurfa að vera sammála um hvaða staðlar og kerfi eru notuð til að „byggja“ verslanirnar, í stað þess að eyða dýrmætum tíma og fjármunum í mismunandi lausnir sem síðar þarf að tengja saman eða samræma.

Sjálfvirkni í viðskiptum kallar einfaldlega á margskonar samræmingu upplýsinga- og gagnakerfa. Fyrirtæki sem ætla að taka upp rafrænt viðskiptasamband sín á milli þurfa að nota sömu kerfi eða samræma og samtengja þau kerfi sem í notkun eru. Í innkaupakerfum er eitt slíkt samræmingarverkefni í því fólgið að taka mismunandi uppbyggða vörulista frá mörgum ólíkum birgjum og tengja saman í einn vel skipulagðan vörulista. Takmarkið er að viðskiptin sjálf og greining upplýsinga gangi sem greiðast fyrir sig með sem minnstum tilkostnaði.

Samkvæmt þessu er eitt alþjóðlegt flokkunarkerfi fyrir vörur og þjónustu, sem er viðhaldið á einum stað og þróað af þeim sem hagsmuna eiga að gæta, betra en mörg mismunandi „einkakerfi“ fyrirtækja, atvinnugreina eða þjóða.

Staðlaráð Íslands gerðist félagi í Eccma í október 2000 og tekur þátt í þróun UNSPSC innan Eccma samtakanna, býður ráðgjöf og þjónustu við flokkun samkvæmt kerfinu og vinnur að íslenskri þýðingu á því. Þýðingin er unnin í samstarfi við Netis hf., annan íslenskan félaga í Eccma. Netis hefur notað flokkunarkerfið til að skipuleggja vörulista á innkaupavettvangi sem fyrirtækið rekur á Netinu. Nánari upplýsingar um Eccma og UNSPSC er að finna á vefnum: *http://eccma.org* og *http://eccma.org/unspsc*.

Miðað við þann áhuga á veruflokkunarkerfinu sem Staðlaráð hefur orðið vart við á undanförnum mánuðum, er líklegt að íslenskum notendum UNSPSC og félögum í Eccma fjölgi hratt á næstunni. Með yfirstandandi rafvæðingu innkaupa íslenska ríkisins og samstöðu um samræmda flokkun á vörulistum birgja eftir UNSPSC kerfinu er Ísland gengið í forystusveit þeirra sem móta viðskiptahætti framtíðarinnar.

Guðbjörg Björnsdóttir er forstöðumaður þróunarsviðs Staðlaráðs Íslands

Hvað er nægilega öruggt?

Föst viðmið með tilkomu staðla

Jónas St. Sverrisson

Með tilkomu ÍST BS 7799 fæst í fyrsta sinn raunverulegur möguleiki á föstu viðmiði til öryggis

Undanfarna mánuði hefur orðið gífurleg breyting á viðhorfi til öryggismála upplýsingakerfa. Svo mikil hefur breytingin verið að greinarhöfundur telur að árið 2001 verði ár öryggis á Íslandi. Í þau 13 ár sem höfundur hefur unnið að öryggismálum hefur aldrei verið jafn mikið að gerast á þessu sviði. Fyrir nokkrum misserum voru aðeins örfá fyrirtæki sem buðu upp á sérhæfða ráðgjöf í öryggismálum en í dag vilja allir bjóða slíka ráðgjöf, þjónustu eða vörur tengdum öryggismálum. Það eru ekki bara íslensk fyrirtæki sem hafa orðið vör við þessa breytingu heldur hafa erlend fyrirtæki einnig farið að sækja inn á íslenska markaðinn í meira mæli.

Hvað veldur þessari breytingu?

Einn hlutur öðrum fremur hefur valdið þessari breytingu en það er þróun Internetsins en auk þess hafa auknar kröfur til varðveislu persónulegra upplýsinga einnig haft mikil áhrif.

Eftir því sem notkun fyrirtækja og traust þeirra á Internetinu hefur aukist því meiri þörf er fyrir að hafa allan rekstur öruggann og áreiðanlegann. Ef netverslun ætlar sér að ganga í augun á viðskiptavinum verður hún, í viðbót við það að líta vel út og vera auðveld í notkun, að sýna fram á öryggi og traust. Viðskiptavinir verða að fá tilfinningu og tryggingu fyrir því að þau gögn sem verða til við viðskipti þeirra verði meðhöndluð sem trúnaðargögn og að þau verði varin á viðeigandi hátt.

Hvernig er hægt að sýna fram á traust og öryggi?

Traust og öryggi fæst með því að setja fasta stefnu í öryggismálum, viðeigandi verklagsreglur og nota réttan búnað auk reglulegrar þjálfunar starfsmanna. Hægt er að auka traustið og öryggið með því að byggja öryggiskerfi upp samkvæmt staðli. Þegar staðall er notaður er búið að setja fast viðmið sem hægt er að gera úttekt útfrá. Þannig verður auðveldara að sýna fram á nægilega gott öryggi og þar með auka traustið. Að geta sýnt fram á traust og öryggi getur skipt sköpum fyrir mörg fyrirtæki.

Nýr staðall

Með tilkomu ÍST BS 7799 fæst í fyrsta sinn raunverulegur möguleiki á föstu viðmiði til öryggis en það er forsenda þess að geta sagt til um hvað teljist nægilega öruggt.

BS 7799 staðallinn er í raun ekki nýr staðall. Hollenska viðskipta- og iðnaðarráðuneytið gaf út *Code of Practice for Information Security Management* árið 1993 sem síðan var formlega gert að breskum staðli árið 1995. Upp frá því hefur vegur þessa staðals farið vaxandi og nú er svo komið að hann hefur náð athygli manna í Bandaríkjunum sem segir nokkuð um ágæti staðalsins. Það má segja að BS 7799 sé um þessar mundir á fljúgandi ferð um allan heim. Staðallinn er byggður á bestu venjum fjölmargra fyrirtækja í fararbroddi. Hann inniheldur aðgerðir sem almennt eru taldar vera nauðsynlegar ábyrgum rekstri.

Ekki bara fyrir tölvufólk

Öryggi upplýsingakerfa er ekki eingöngu fyrir tölvusérfræðinga heldur fellur það vel að ábyrgð og verkefnum stjórnenda og annarra starfsmanna. Öryggi er í raun meira stjórnunarlegt mál fremur en tæknilegt eins og mörgum hættir til að hugsa. Tæknin er einungis notuð til þess að fullnægja hluta af þeim kröfum sem settar eru um öryggi. Stórum hluta af kröfum til öryggis er fullnægt með stjórnunarlegum aðgerðum.

Staðallinn hentar öllum

Staðallinn er gerður með allar stærðir og tegundir fyrirtækja í huga. Vegna sveigjanleika hans er mögulegt að beyta honum á minnstu og stærstu fyrirtæki. Einn af kostum BS 7799 er að fyrirtæki geta valið að beyta staðlinum á hluta af starfsemi sinni. Þannig er hægt að byrja

smátt og bæta síðan við eftir þörfum og kröfum hverju sinni.

Þó svo staðallinn geti hentað öllum þá verður að segjast eins og er að vissar tegundir fyrirtækja hafa meira við hann að gera en aðrar.

Vottun

Eðlilegur fylgifiskur staðla er vottun. Fá fyrirtæki hafa þörf á vottun í tengslum við BS 7799. Fyrirtæki sem byggja sín öryggiskerfi upp samkvæmt staðlinum verða að meta hver ávinningurinn af vottun er. Fyrirtæki sem hafa mikla þörf fyrir að sýna fram á virkt öryggiskerfi til þess að auka traust viðskiptavina og samstarfsaðila ættu að huga sterklega að vottun. Í sumum tilfellum getur vottun virkað sem markaðsafl - hver vill ekki fremur skipta við fyrirtæki sem hefur vottað öryggiskerfi heldur en fyrirtæki án vottunar? Það sem þarf að hafa í huga hér er að vottun tekur langan tíma, krefst mikils undirbúnings og stöðugs viðhalds og síðast en ekki síst þá verður að vera einhver ávinningur.

Í sumum tilfellum getur vottun virkað sem markaðsafl

Innleiðing ÍST BS 7799

Fyrirtæki verða að vera tilbúin að setja talsverða fjármuni og tíma í vinnu við innleiðingu staðalsins. Samkvæmt reynslu KPMG standa og falla verkefni með þátttöku starfsmanna. Ef ekki er næg þátttaka eða starfsmenn fá ekki nægan tíma í verkefnið þá er betra að sleppa því. Innleiðing staðalsins krefst sérþekkingar á fyrirtækinu sem einungis starfsmenn hafa. Ráðgjafar geta stjórnað verkinu og miðlað af reynslu og sérþekkingu á staðlinum en þeir geta ekki unnið alla vinnuna.

Fyrirtæki verða að vera tilbúin að setja talsverða fjármuni og tíma í vinnu við innleiðingu staðalsins

Þegar unnið er að innleiðingunni er eðlilegt að starfsmenn sem koma að verkinu komi frá öllum deildum. Þannig fæst gleggst mynd af fyrirtækinu, þörfum þess og kröfum til öryggis. Mikilvægt er að hafa í huga að öryggi upplýsingakerfa nær yfir öll gögn, sama á hvaða formi þau eru.

Fjármögnun verksins

Þar sem mörgum hættir til þess að líta á staðalinn sem tæknilegt mál þá liggur beint við að fjármagna innleiðinguna af þeim fjármunum sem tölvu- eða upplýsingadeild fyrirtækis hefur til umráða. Eins og áður hefur verið bent á þá er innleiðingin stjórnunarlegt ferli og því ætti fjármögnun svona verkefnis fremur að vera hluti af fjárhagsáætlun yfirstjórnar. En auðvitað þegar öllu er á botninn hvolft þá koma fjármunirnir úr sama vasa.

Árið 2001

Í upphafi greinarinnar var því haldið fram að árið 2001 verði ár öryggis á Íslandi. Síðustu tvö ár hefur verið fjárfest í miklum mæli í nýjum tölvukerfum. Aukning á tölvubúnaði þýðir að það er verið að framkvæma stöðugt meiri tölvuvinnslu gagna. Með aukinni tölvuvinnslu verða fyrirtæki að treysta meira og meira á búnaðinn, en án hans er í mörgum tilfellum ekkert hægt að vinna. Að auki hafa fleiri fyrirtæki en áður tengt innri net sín við Internetið og þar með opnað netkerfi sín fyrir alheiminum og í leiðinni búið til öryggisvandamál. Það gefur því augaleið að þörfin fyrir öryggi hefur aukist verulega.

Þeim sem bjóða upp á þjónustu tengda öryggismálum upplýsingakerfa mun væntanlega fara fjölgandi á árinu rétt eins og gerist í öðrum greinum þar sem vöxtur er. Almenningur mun verða áþreifanlega var við aukið öryggi með tilkomu sérstakra skírteina fyrir rafundirskriftir og dulritun gagna. Þessi rafrænu skírteini opna möguleika á auknum rafrænum samskiptum almennings við ríki og sveitafélög sem aftur eykur þörfina fyrir þjónustu á sviði öryggis. Það má því segja að framundan er spennandi ár þar sem öryggi verður vonandi haft í fyrirúmi.

Nánari upplýsingar má finna á eftirfarandi vísum.

http://www.c-cure.org/
http://www.kpmg.is/bs7799

Jónas St. Sverrisson vinnur við ráðgjöf í öryggismálum upplýsingakerfa hjá KPMG Ráðgjöf ehf.

Er BS-7799 góð leið til að vaxa?

Oddur Hafsteinsson og Jónatan S. Svavarsson

Samkeppni á þessum markaði muni byggja á þekkingu, gæðum og öryggi

Þegar fyrirtækin stækka, og eðlileg endurnýjun á sér stað þá eru það kerfin sem þurfa að taka við

Upplýsingar eru auðlind

Á undanförum árum hafa ASP-fyrirtæki verið að skjóta upp kollinum, sum hratt og af myndarskap en minna hefur borið á öðrum. Það hlutverk sem þessi fyrirtæki eru að taka að sér er bæði mikið og mikilvægt – í nútíma rekstri eru upplýsingar auðlind, og nýting þessarar auðlindar það sem getur ráðið úrslitum um velgengni fyrirtækjanna.

Ástæða þess að undirritaðir skrifa þessa grein eru sú að við trúum því að samkeppni á þessum markaði muni byggja á þekkingu, gæðum og öryggi – aðilar sem ætli að fara í þessa samkeppni á öðrum forsendum heltast fljótt úr lestinni.

Það er því mikilvægt fyrir þá sem ætla að vera með að vera upplýstir um hvaða leiðir eru færar og að þeir geti metið hvort þær séu fýsilegar fyrir þá.

Hýsing - stýring vaxtar

Á síðasta ári var fyrirtækið Hýsing stofnað til að byggja upp þjónustu eftir hugmyndafræði ASP.

Verkefnið er ögrandi og fyrirtækið er komið vel af stað – ekki stórt, en á réttri leið.

Stjórnendur fyrirtækisins telja að markaður fyrir þjónustu fyrirtækisins muni vaxa mjög hratt og að stærsta ögrunin verði að stýra vextinum – án þess að misstíga sig.

Við höfðum skoðað BS-7799 lítillega – sem mögulega leið til að tryggja öryggismál í okkar starfsemi. Staðlar eru sjaldan aðlaðandi, en þessi var í léttara laginu.

Eftir stutta skoðun þá lenti þetta mál aftar í röðinni, að mörgu er að hyggja öðru en stöðlum!

Heimsókn Dr. Overbeek

Í lok febrúar kom Dr. ir. P.L. Overbeek frá KPMG í Hollandi til Íslands og okkur var boðið að taka þátt í kynningarfundi um staðalinn, kosti hans og galla. Kynningin var ekki verri en það að við óskuðum eftir fundi með Dr. Overbeek til að fara yfir möguleika Hýsingar til að taka upp kerfi og verklag sem uppfyllti kröfur staðalsins.

Spurningin hjá okkur snerist um hvort við gætum notað staðalinn sem leiðarljós (Guide Lines) við uppbyggingu kerfa og verklagsreglna hjá okkur.

Við skilgreindum starfsemi okkar, sem er miðlægur rekstur upplýsingakerfa, og hvað við þyrftum að vera sérstaklega vakandi fyrir. Þar var það vöxturinn sem Dr. Overbeek benti á – meðan fyrirtækin eru smá þá er hægt að treysta á þekkingu og reynslu einstakra starfsmanna, menn redda hlutunum.

Þegar fyrirtækin stækka, starfsmönnum fjölgar og eðlileg endurnýjun á sér stað þá eru það kerfin sem þurfa að taka við.

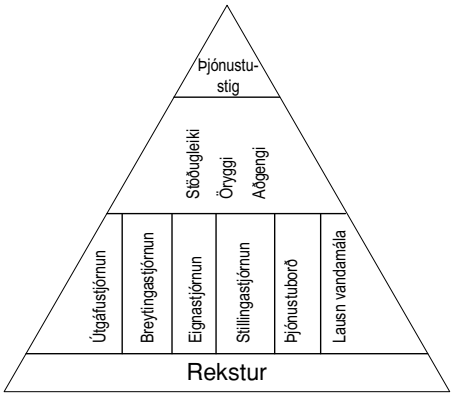
Þannig að með því að vinna kerfisbundið að uppbyggingu fyrirtækisins þá séum við bæði að stýra vextinum og að undirbúa okkur undir framtíðina.

Annar ávinningur sem hann benti á var að með kerfisbundinni vinnu sem miðaði að vottun, væru fyrirtækin að fara í gegnum þroskaferli þar sem menn gætu stuðst við reynslu ráðgjafa – sem hafa öðlast sína reynslu með því að vinna með fyrirtækjum á sama sviði. Með því að tryggja bakstuðning frá erlendum ráðgjafa erum við að víkka sjóndeildarhring okkar á þessu sviði.

World Class IT

World Class IT (WCIT) er heitið á heildarlausn sem KPMG býður viðskiptavinum sínum sem starfa við upplýsingatækni.

Um er að ræða breitt svið lausna sem hafa verið prófaðar í stórum sem smáum fyrirtækjum um allan heim. Með því að skoða stöðu Hýsingar út frá þessari aðferðarfræði verður tryggt að við fáum reynslu inn sem snertir ekki aðeins öryggismál, heldur nær yfir alla stjórnun fyrirtækisins. Á mynd 1. má sjá á hverju WCIT aðferðafræðin byggir.



Niðurstaðan

Niðurstaðan í þessu máli er sú að Hýsing hefur ákveðið að leita aðstoðar KPMG við frekari mótun á starfsemi félagsins. Sú vinna tekur bæði mið af reglum BS 7799 og WCIT aðferðum KPMG um rekstur tölvufyrirtækja.

Í framhaldi af því munum við taka ákvörðun um hvort við leggjum áherslu á staðalinn eða förum aðrar leiðir.

Ljóst er að á ári öryggisins og við mótun hýsingarfyrirtækjanna verða gerðar kröfur. Það er því bara að standa sig.

Oddur Hafsteinsson ráðgjafi hjá KPMG Ráðgjöf ehf.
Jónatan S. Svavarsson er framkvæmdastjóri Hýsingar ehf.

Hvað með öryggið?

Aðkeypt rekstrarþjónusta eða eigin uppbygging

Sæberg Sigurðsson og Indriði Þröstur Gunnlaugsson

Við uppbyggingu tölvumála í fyrirtækjum eru öryggismál eitt mikilvægasta umhugsunarefnið

Á liðnum áratug hefur bylting átt sér stað í öryggismálum eins og á svo mörgum öðrum sviðum. Áður fyrr snérust öryggismál flestra fyrirtækja aðallega um að tryggja veraldlegar eigur gegn innbrotum og skemmdarverkum. Nú er staðan orðin sú hjá fjölmörgum fyrirtækjum að tjón á veraldlegum eigum, eins og húsnæði og tölvubúnaði, yrði minniháttar í samanburði við tjónið sem yrði ef gögn í upplýsingakerfi fyrirtækisins skemmdust eða væri stolið.

Forsvarsmenn fyrirtækja sem bera saman kostnað við varnir veraldlegra eigna annars vegar og upplýsinga hins vegar, að teknu tilliti til verðmæta þessara þátta, gætu orðið undrandi. Þeir gætu jafnvel freistast til að hætta hefðbundinni öryggisgæslu og viljað einbeita sér að vörnum inni í upplýsingakerfunum - En málið er ekki svona einfalt.

Uppbygging upplýsingakerfisins með tilliti til öryggis

Við uppbyggingu tölvumála í fyrirtækjum eru öryggismál eitt mikilvægasta umhugsunarefnið. Þegar forsvarsmenn fyrirtækja velja á milli þess að byggja upp eigið tölvukerfi eða leita til rekstrarþjónustuaðila ættu þeir fyrst að leita svara við tveimur grundvallarspurningum: „Hvernig getur fyrirtæki mitt tryggt öryggi eigin upplýsingakerfa?“ og „hvernig er öryggi upplýsingakerfa okkar tryggt í höndum rekstrarþjónustuaðila?“

Að mörgu er að hyggja þegar leitað er svara við þessum spurningum og fólk skyldi varast að láta sér nægja einföld svör frá tæknifólki, eins og „við setjum bara upp eldvegg“ eða „vélasalurinn okkar verður í gamalli bankahvelfingu“. Staðreyndin er sú að vegna smæðar flestra íslenskra fyrirtækja geta fæst þeirra byggt upp upplýsingakerfi sem uppfyllir ýtrustu öryggiskröfur. Jafnvel þau fyrirtæki sem ættu að hafa burði til þess eiga fullt í fangi með daglegan rekstur vegna skorts á sérfræðiþekkingu og við slíkar aðstæður sitja flókin mál eins og öryggismál iðulega á hakanum.

Tökum sem dæmi grunnþátt hvers upplýsingakerfis, vélasalinn. Hefur fyrirtækið yfir vélasal að ráða þar sem tryggt er að hitastig er hæfilegt og stöðugt, þar sem lagnaleiðir eru öruggar, brunavarnir eru í lagi og vöktun er á leka, innbrotum o.s.frv.? Ef ekki, hvað myndi kosta að koma upp slíkum sal eða gera endurbætur á þeim gamla?

Hvað með fyrirbyggjandi þætti eins og öryggisbúnað, afritun, viðhald og möguleika á skjótum viðbrögðum við bilunum? Hver og einn þessara þátta greinist í fjölmarga undirþætti sem of langt er að telja upp í stuttri grein, en þeir vekja allir upp sömu spurninguna: „Hvar fæ ég sérfræðiþekkinguna sem fyrirtækið þarf og hvernig get ég viðhaldið henni?“

Leitað út fyrir fyrirtækið

Þótt fyrirtæki búi svo vel að hafa á að skipa hæfu starfsfólki sem getur rekið upplýsingakerfi þess frá degi til dags, þá neyðist það líklega til að leita út fyrir fyrirtækið eftir sérfræðiþekkingu ef það vill tryggja ásættanlegt öryggi. Ekki reynist nóg að sækja þessa þekkingu einu sinni því stöðugt eru að koma upp nýir fletir á öryggismálum sem kalla á aðlögun upplýsingakerfa. Á Íslandi eru sárafáir sem búa yfir mikilli þekkingu eða reynslu á þessu sviði og það er ofvaxið flestum fyrirtækjum að byggja upp slíka þekkingu innanhúss.

Fyrirtækjum dugar líka fæstum að fá eingöngu tæknilega ráðgjöf um öryggismál því að miklu leyti snúast öryggismál um margvíslega aðra þætti eins og skipulag og stefnumörkun. Síðast en ekki síst snúast öryggismál um félagslega þætti á vinnustað. Tæknilegt öryggi er harla máttlítið ef starfsfólk lítur ekki á það sem sitt hlutverk að verja upplýsingar fyrirtækisins eins og hverjar aðrar eigur þess. Virkja þarf allt starfsfólk í uppbyggingu öryggismála og vekja það til vitundar um verðmæti upplýsinga

fyrirtækisins. Þá fyrst þegar almenn sátt næst um það hve mikil verðmæti liggja í upplýsingum verður það jafn sjálfsagt fyrir starfsfólk að læsa tölvunni sinni þegar það skreppur frá, eins og það er sjálfsagt að læsa fyrirtækinu að kvöldi.

Margs konar ógnanir frá Internetinu, eins og innbrot, veirur og skemmdarverk, færast stöðugt vöxt

Skipulegar varnir

Margs konar ógnanir frá Internetinu, eins og innbrot, veirur og skemmdarverk, færast stöðugt vöxt. Stöðugt fjölgar þeim sem nýta sér möguleika Internetsins og í september árið 2000 voru u.þ.b. 300 milljónir notenda að vefnum. Ef við gefum okkur að 0,1% þessara notenda stundi innbrot eða skemmdarverk, eru það um 300 þúsund manns. Engin stjórn er á Internetinu og því þarf hver og einn að tryggja öryggi eigin gagna og kerfa.

Fátt er til varnar annað en skipuleg vinnubrögð og góður öryggisbúnaður. Fyrirtæki eru hvert af öðru að átta sig á því að með því að tryggja öryggi upplýsingakerfanna standa þau betur að vígi í samkeppni. Krafa viðskiptavina um öryggi upplýsinga hefur jafnt og þétt orðið meira áberandi og löggjafinn hefur nú fylgt í kjölfarið með ný lög nr. 77/2000 um persónuvernd, skráningu og verndun persónuupplýsinga. Áhrifa þessara laga er lítið farið að gæta á yfirborðinu en framundan er mikið uppbyggingarstarf í öryggismálum fjölmargra fyrirtækja og stofnana sem mörg hver eiga bara um tvennt að velja; að taka á öryggismálunum eða að leggja upp laupana.

Til leiðsagnar fyrirtækjum við uppbyggingu öryggismála er helst að leita í öryggisstaðla og nú virðist sem breski staðallinn BS 7799 verði ráðandi þegar kemur að vottun öryggiskerfa.

Innleiðing öryggiskerfis samkvæmt staðlinum er unnin í nokkrum skrefum og að mörgu að hyggja áður en fyrirtæki geta hafið sjálft vottunarferlið. Lokatakmarkið er að koma á skilvirku öryggiskerfi þar sem áhætta skilgreindra áhættuþátta er metin og tilhögun þeirra endurskoðuð með reglulegu millibili.

Mismunandi er hvaða leið fyrirtæki velja til að koma öryggiskerfinu á. Í stórum dráttum er byrjað á því að skilgreina öryggisstefnu. Áhættumat með lykilstarfsmönnum og stjórnendum fylgir í kjölfarið. Þar er farið yfir verðmæti fyrirtækisins og þeim gefið gildi í samræmi við áhættu og veikleika. Afurð áhættumatsins er stigagjöf sem notuð er við forgangsröðun áhersluþátta. Mikilvægt er að aðgerðir til að minnka áhættu séu unnar með og af starfsfólki fyrirtækisins. Það er gert til að nýta sérfræðiþekkingu starfsfólksins og til að koma á almennri öryggisvitund, en einnig til að tryggja áframhaldandi virkni og endurnýjun viðkomandi aðgerða. Í þessari vinnu verður til nákvæm og ítarleg öryggishandbók sem öryggiskerfið byggir á.

Innan skamms má búast við því að viðskiptavinir rekstrarþjónustuaðila upplýsingakerfa spyrji: „Eruð þið með vottað öryggiskerfi?“ Eins og er getur enginn rekstrarþjónustuaðili á Íslandi svarað þessari spurningu játandi en á næstu misserum munu þeir aðilar sem það geta vafalaust standa feti framar samkeppnisaðilunum.

Sæberg Sigurðsson, forstöðumaður gæða- og öryggismála hjá Áliti hf.
Indriði Þröstur Gunnlaugsson, verkefnisstjóri í öryggismálum hjá Áliti hf.

ÍST BS 7799 - heilbrigð skynsemi

Hannes Sigurðssson

Þegar fjallað er um öryggi upplýsinga er þrennt sem hafa ber í huga, það er; trúnaður, heilindi og aðgengileiki upplýsinga

BS 7799 er vel unninn staðall, skiljanlegur almennum lesendum og ekki sérstaklega ætlaður tölvusérfræðingum

Hvaða verðmætum þínum er hægt að stela, án þess að svipta þig þeim og án þess að þú verðir þess var?

Hvaða verðmætum þínum er hægt að breyta, svo þau verði þér gagnslaus?

Hvaða verðmætum þínum getur þú glatað, án þess að getað endurheimt þau?

Svarið við öllum þremur spurningunum er upplýsingar.

Upplýsingar eru í dag mestu verðmæti fyrirtækja, ásamt mannauðnum sem skapar þær og gerir þær að verðmætum fyrir fyrirtækin. Mestu verðmætin liggja ekki í tölvubúnaðinum, húseignunum né öðrum „áþreifanlegum“ eignum, þau liggja í sjálfum upplýsingunum.

Það er því mikilvægt að fyrirtæki verji og tryggi öryggi upplýsinga sinna sem best. Að minnsta kosti á sama hátt eða betur en þau verja og tryggja öryggi annarra eigna sinna.

Það er þó ekki hægt að tryggja upplýsingar á sama hátt og „áþreifanlegar“ eignir. Ef tölvubúnaður er tryggður hjá tryggingafyrirtæki, er eiganda hans tryggð ákveðin peningaupphæð, sem er ígildi þess sem hann tapaði. Það sama er ekki hægt að gera varðandi upplýsingar. Þú tryggir þær ekki hjá tryggingafélagi og færð ígildi þeirra greitt ef þær glatast eða spillast. Það getur enginn tryggt öryggi upplýsinganna annar en eigandi þeirra eða ábyrgðaraðili.

Þrjú grunnatriði upplýsingaverndar

Þegar fjallað er um öryggi upplýsinga er þrennt sem hafa ber í huga, það er; trúnaður, heilindi og aðgengileiki upplýsinga.

Með trúnaði upplýsinga er átt við að upplýsingar séu einungis aðgengilegar þeim sem til þess hafa sérstaklega heimild og engum öðrum. Með heilindum upplýsinga er átt við að upplýsingar séu heilar og áreiðanlegar. Með aðgengileika upplýsinga er átt við að þeir sem til þess hafa sérstaka heimild hafi aðgang að þeim, hvar og hvenær sem þörf krefur.

Þetta eru þrjú grunnatriði upplýsingaverndar og megininntakið í BS 7799 staðlinum.

Staðallinn er kjörið verkfæri til þess að hjálpa eigendum og ábyrgðaraðilum upplýsinga til að verja og tryggja öryggi þeirra sem best.

Fyrir og eftir BS 7799

Breski staðallinn BS 7799: Code of practice for information security management kom fyrst út árið 1995. Hann er fyrst og fremst stjórnunarstaðall, en ekki tæknistaðall, og segir hvað þarf að gera til að tryggja öryggi upplýsinga sem best, en ekki hvernig það skal gert.

Áður en BS 7799 kom fram notuðu margir m.a. tæknistaðla eins og Orange Book (Department of Defence Trusted Computer Evaluation System Criteria) frá Bandaríska varnarmálaráðuneytinu. Orange Book ásamt öðrum stöðlum lagði svo grunninn að alþjóðlegum tæknistaðli, Common Criteria (ISO/IEC 15408:1999). Common Criteria leggur m.a. grunninn að öryggi gagnagrunns á heilbrigðissviði sem Íslensk erfðagreining vinnur að.

BS 7799 staðallinn kom út í annarri útgáfu vorið 2000, örlítið bættur frá fyrstu útgáfunni. Þýðing á þeirri útgáfu hefur nú verið lögð fram sem frumvarp að ÍST-staðli.

Fyrir þá sem unnið hafa að öryggi upplýsingamála hjá fyrirtækjum var koma BS 7799 kærkomin og auðveldaði hann mörgum að vinna markvisst að öryggismálum upplýsinga. Nú þegar ráðist hefur verið í íslenskun á staðlinum má ætla að hann verði aðgengilegri enn stærri hópi.

BS 7799 er vel unninn staðall, skiljanlegur almennum lesendum og ekki sérstaklega ætlaður tölvusérfræðingum. Staðallinn er því aðgengilegur og fræðandi lestur. Ég bjóst aldrei við að ég myndi segja þetta um staðal. Það má fastlega gera ráð fyrir nokkurri útbreiðslu hans hérlendis eins og í Evrópu. Ekki má þó búast við að hann nái sömu sölu Harry Potter.

Sé tekið með markvissum hætti á öryggismálum upplýsinga (t.d. með ÍST BS 7799) verður fyrirtækið síður fyrir alvarlegum öryggisbrotum og þau verða uppgötvuð fyrr (og frekar)

BS 7799 er fyrst og fremst heilbrigð skynsemi þegar litið er til öryggis upplýsinga og upplýsingavernd.

Megin þættir og markmið ÍST BS 7799

Þegar litið er á þá meginþætti sem ÍST BS 7799 tekur á, sést að um er að ræða atriði sem eru ágætlega þekkt hjá flestum sem að þessum málum vinna. Margir eru að vinna að þessum málum og vilja gera betur. Sumir hafa einhverra hluta vegna frestað þessari vinnu eða átt erfitt með að byrja. Staðallinn ætti að vera ágætis verkfæri fyrir þá, því hann auðveldar okkur að ganga skipulega að þessari vinnu.

Sama regla gildir hér og í gæðastöðlum; gerðu það sem þú segir, segðu það sem þú gerir og sýndu fram á að þú gerir það sem þú segist gera.

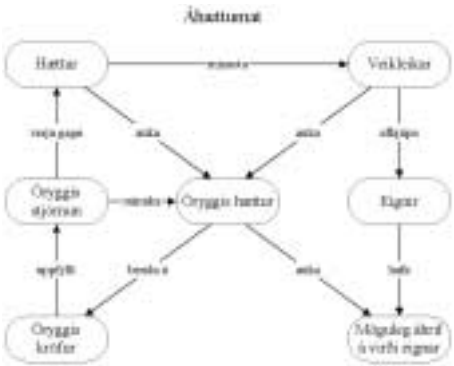
Nánar er farið í staðalinn á öðrum stað í þessu blaði og fer ég því ekki í uppbyggingu hans hér né innihald. Þó ber að nefna meginþætti þá sem hann fjallar um og skýr markmið þeirra þátta. Sjá í töflu 1.

Þegar ákveðið er að nota ÍST BS 7799

Þegar ákveðið er að taka á öryggismálum skv. ÍST BS 7799 hjá fyrirtækinu þarf að byrja á því að skilgreina öryggisstefnu fyrirtækisins, því næst skilgreina umfang upplýsingaverndar, gera áhættumat og stýra áhættunni, setja eftirlitsmarkmið og eftirlitsaðgerðir og útbúa yfirlýsingu um markmið og leiðir.

Stefna fyrirtækisins varðandi öryggi upplýsinga þarf að koma frá yfirstjórn fyrirtækisins, annars er hún marklaus. Hún skal vera sá grunnur sem öll upplýsingaöryggismál fyrirtækisins byggja á. Öryggisstefnan þarf að vera skýr og á skiljanlegu máli öllum þeim sem hana þurfa að þekkja. Skilgreina einnig umfang upplýsingaverndarinnar og setja skýra ramma, þ.e. á hverju skal taka og hverju ekki.

Áður en ráðist er í að verja upplýsingar eða upplýsingakerfi fyrirtækisins þarf að gera mat á þeirri hættu sem að þeim steðjar. Hættur og ógnir geta verið margar og mismunandi, allt eftir eðli upplýsinganna, upplýsingakerfum, vinnuferlum, ytra og innra umhverfi, fólki, stjórnun og skipulagi o.s.frv. Mynd 1 sýnir hvaða atriði hafa ber í huga þegar áhætta er metin.



Þegar áhættumat hefur verið gert, skal vinna að leiðum til að stýra áhættunni þ.e. með stjórnunar- og skipulagslegum aðferðum, vinnuferlum, tækni-, hug- og vélbúnaði o.fl. Niðurstöður úr áhættumatinu, öryggisstefna fyrirtækisins ásamt skilgreindu umfangi upplýsingaverndar skal leggja til grundvallar áhættustjórnuninni.

Tafla 1

Hluti	Markmið
Stefna um upplýsingavernd	Að stjórnendur veiti leiðbeiningar og stuðning varðandi upplýsingavernd
Skipulag öryggismála	Að stjórna öryggi upplýsingamála innan fyrirtækisins
Flokkun upplýsinga	Að tryggja að upplýsingaeignir njóti viðeigandi verndarstigs
Starfsmannaöryggi	Að minnka áhættu á mannlegum mistökum, þjófnaði, svikum, eða misnotkun búnaðar
Raunlægt öryggi og umhverfisöryggi	Að koma í veg fyrir óheimilan aðgang, tjón og truflanir á athafnasvæði fyrirtækisins og upplýsingum þess
Stjórnun á fjarskiptum og rekstri	Að tryggja réttan og öruggan rekstur upplýsingavinnslubúnaðar
Aðgangsstýring	Að stjórna aðgengi að upplýsingum
Kerfisþróun og viðhald	Að tryggja að öryggi sé innbyggt í upplýsingakerfi
Stjórnun til að tryggja órofinn rekstur	Að koma í veg fyrir röskun á viðskiptastarfsemi og að verja mikilvæg viðskiptaferli fyrir áhrifum af meiri háttar bilunum eða áföllum
Samræmi	Að koma í veg fyrir brot gegn refsilöggjöf og einkamálarétti, laga-, reglugerðar- eða samningsskyldum, og hvers kyns öryggiskröfum

Því næst þarf að setja markmið varðandi eftirlit og velja viðeigandi eftirlitsaðgerðir skv. staðlinum (og utan hans ef þörf krefur) svo öryggisstefnu fyrirtækisins sé fylgt.

Af hverju að nota ÍST BS 7799?

Með því að taka á öryggismálum með hjálp ÍST BS7799 ná fyrirtæki með heildstæðum og skipulegum hætti utan um öryggismál eigin upplýsinga. Þegar vinnuferli hafa verið skráð verður öll vinna markvissari og það leiðir til lækkunar á rekstrarkostnaði sem og þjálfunarkostnaði starfsfólks. Sé tekið með markvissum hætti á öryggismálum upplýsinga (t.d. með ÍST BS 7799) verður fyrirtækið síður fyrir alvarlegum öryggisbrotum og þau verða uppgötvuð fyrr (og frekar). Sýnileg vinna að þessum málum bætir auk þess ímynd fyrirtækisins og traust umhverfisins gagnvart því. Síðast en ekki síst, verða þessi mál sýnileg stjórnendum og ábyrgðaraðilum fyrirtækisins, en ekki hulin, sem því miður er víða tilfellið. Þess vegna ætti tilkoma þessa staðals að vera hvatning og mikli hjálp fyrirtækjum til að taka markvisst á öryggi eigin upplýsingamál.

Heimildir:
Frumvarp að ÍST - staðli
* ÍST BS 7799 Stjórnun upplýsingaverndar- 1.hluti: Vinnureglur fyrir stjórnun upplýsingaverndar
* ÍST BS 7799 Stjórnun upplýsingaverndar - 2.hluti: Forskriftir fyrir upplýsingaverndarkerfi

Frá British Standards Institute (BSI):
* Information Security Management: An Introduction (PD3000)
* Preparing for BS7799 Certification (PD3001)
* Guide to BS7799 Risk Assessment and Risk Management (PD3002)
* Are you ready for a BS7799 Audit? (PD3003)
* Guide to BS7799 Auditing (PD3004)
* Selecting BS7799 Controls (PD3005).

Athyglisverðar heimasíður um BS 7799:

Det Norske Veritas:
http://www.dnv.com/certification/Services/BS7799.htm
DISC: http://www.c-cure.org/

Hannes Sigurðsson er gagnaöryggisstjóri Íslenskrar erfðagreiningar

Svipmyndir frá Linux ráðstefnu

Á Linux ráðstefnunni, sem haldin var þann 15. mars síðastliðinn í Salnum í Kópavogi, var leitast við að svara spurningum eins og hver leyndardómurinn sé á bak við gæði frjáls hugbúnaðar og hver staða hans og Linux sé í dag. Bjarni R. Einarsson velti einnig upp athyglisverðum spurningum um stöðu Linux í kennsluumhverfi grunnskólanna og sérstöðu Microsoft í því tilliti. Nokkur fyrirtæki héldu sýningu í tilefni ráðstefnunnar en þau eru Teymi, Opin kerfi, Firmanet, Nýherji og Arcís.

Hér má sjá Eric S. Reymond frá Pennsylvaníu í Bandaríkjunum, en hann talaði um þróun í hugbúnaðargerð fyrir tilstilli opins hugbúnaðar.

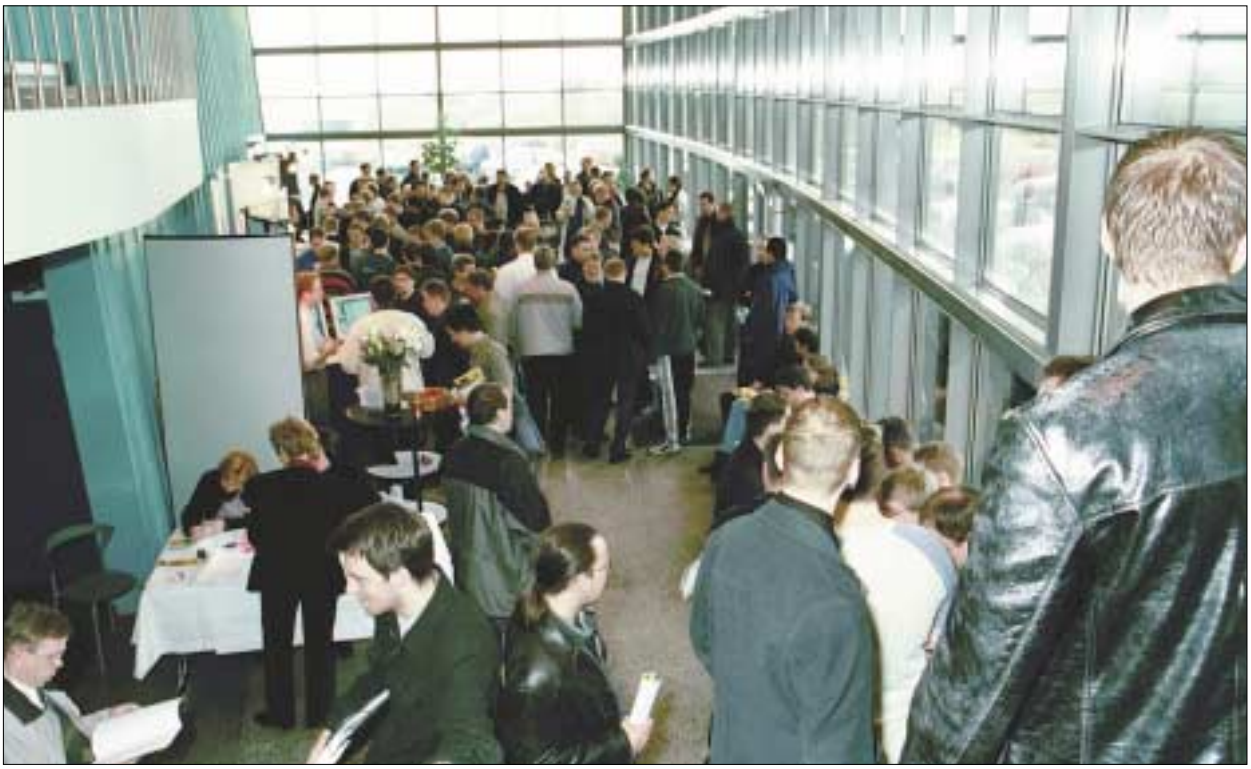
Alan Cox frá Bretlandi talaði um þróun Linux kjarnans, útgáfu 2.4, en Alan er talinn standa næst Linus Torvalds í virðingastiganum í hugum LINUX- notenda.

Gylfi Árnason framkvæmdastjóri Opinna kerfa talaði um áhrif Linux á rekstrarumhverfi tölvudeilda og tölvufyrirtækja.

Heiðar Þór Guðnason forstöðumaður tölvuþjónustu Íslenskrar erfðagreiningar skýrði frá reynslu þeirra af Linux.

Bjarni R. Einarsson tölvunarfræðingur og netverji, talaði um sjálfstætt menntakerfi með frjálsum hugbúnaði.

Arnar Hrafn Gylfason sýndi KDE umhverfið og talaði um reynslu sína sem notandi.



Tæplega 300 manns sóttu Linux ráðstefnuna.

Ráðstefnur og sýningar

Hér er listi Tölvumála yfir helstu ráðstefnur og sýningar út árið.

Einnig er listi yfir tilvísanir á vefsetur ráðstefnufyrirtækja og annarra aðila þar sem eru upplýsingar um ráðstefnur og sýningar.
Ábendingar eru vel þegnar. Vinsamlegast sendið þær til Arnaldar F. Axfjörð; afax@alit.is.

eBusiness Conference and Expo
Ráðstefna og sýning um búnað og tækni í rafrænum viðskiptum.
Tími: 24.-26. apríl 2001.
Staður: London, England.
Tilvísun: http://www.ebusinessexpo.com

ASPWorld Conference & Expo
Ráðstefna og sýning um kerfisveitur.
Tími: 24.-27. apríl 2001.
Staður: Washington D.C., Bandaríkin.
Tilvísun: http://www.aspworldexpo.com/

XML í rafrænum viðskiptum
Ráðstefna um notkun XML í rafrænum viðskiptum.
Tími: Apríl 2001.
Staður: Reykjavík.
Tilvísun: http://www.sky.is

Networld+Interop 2001 Las Vegas
Ráðstefna, sýning og námskeið um netkerfi, fjarskiptatækni og Internetið.
Tími: 6.-11. maí 2001.
Staður: Las Vegas, Nevada, Bandaríkin.
Tilvísun: http://www.key3media.com/interop/

Gartner Group US Spring Symposium/ITxpo 2001
Ráðstefna á vegum Gartner Group með áherslu á stefnumótun í upplýsingatækni.
Tími: 7.-10. maí 2001.
Staður: Denver, Colorado, Bandaríkin.
Tilvísun: http://www.gartner.com

COMMON Spring 2001 Conference
Ráðstefna, sýning og námskeið um IBM búnað og lausnir.
Tími: 13.-17. maí 2001.
Staður: New Orleans, Louisiana, Bandaríkin.
Tilvísun: http://www.common.org/

JavaOne, Sun's 2001 Worldwide Java Developer Conference
Ráðstefna fyrir þrónaraðila í Java.
Tími: 3.-8. júní 2001.
Staður: San Francisco, California, Bandaríkin
Tilvísun: http://java.sun.com/javaone/

eBusiness Conference and Expo
Ráðstefna og sýning um búnað og tækni í rafrænum viðskiptum.
Tími: 12.-14. júní 2001.
Staður: San Jose, Kalifornía, Bandaríkin.
Tilvísun: http://www.ebusinessexpo.com

Networking the Learner
Alþjóðleg ráðstefna um upplýsingatækni í menntamálum
Tími: 29. júlí-3. ágúst 2001.
Staður: Kaupmannahöfn.
Tilvísun: http://www.wcce2001.dk/

Networld+Interop 2001 Atlanta
Ráðstefna, sýning og námskeið um netkerfi, fjarskiptatækni og Internetið.
Tími: 9.-14. september 2001.
Staður: Atlanta, Georgia, Bandaríkin.
Tilvísun: http://www.key3media.com/interop/

Linux Business Expo Atlanta
Ráðstefna og sýning um Linux og rafræn viðskipti.
Tími: 10.-14. september 2001.
Staður: Atlanta, Georgia, Bandaríkin.
Tilvísun: http://www.key3media.com

eBusiness Conference and Expo
Ráðstefna og sýning um búnað og tækni í rafrænum viðskiptum.
Tími: 12.-13. september 2001.
Staður: Bonn, Þýskaland.
Tilvísun: http://www.ebusinessexpo.com

Networld+Interop 2001 Paris
Ráðstefna, sýning og námskeið um netkerfi, fjarskiptatækni og Internetið.
Tími: 18.-20. september 2001.
Staður: París, Frakkland.
Tilvísun: http://www.key3media.com/interop/

Orbit/COMDEX Europe
Ráðstefna í Evrópu um upplýsingatækni almennt.
Tími: 25.-28. september 2001.
Staður: Basel, Sviss.
Tilvísun: http://www.messebasel.ch/orbitcomdex/

Gartner Group US Fall Symposium/ITxpo 2001
Ráðstefna á vegum Gartner Group með áherslu á stefnumótun í upplýsingatækni.
Tími: 8.-12. október 2001.
Staður: Lake Buena Vista, Flórída, Bandaríkin.
Tilvísun: http://www.gartner.com

Gartner Group Europe Fall Symposium/ITxpo 2001
Ráðstefna á vegum Gartner Group með áherslu á stefnumótun í upplýsingatækni.
Tími: 5.-8. nóvember 2001.
Staður: Cannes, Frakkland.
Tilvísun: http://www.gartner.com

COMDEX Fall 2001
Ráðstefna um upplýsingatækni almennt.
Tími: 12.-16. nóvember 2001.
Staður: Las Vegas, Nevada, Bandaríkin.
Tilvísun: http://www.comdex.com

eBusiness Conference and Expo
Ráðstefna og sýning um búnað og tækni í rafrænum viðskiptum.
Tími: 11.-13. desember 2001.
Staður: New York City, New York, Bandaríkin.
Tilvísun: http://www.ebusinessexpo.com

Tilvísanir á vefsíður ráðstefnufyrirtækja og annarra sem halda utan um upplýsingar um ráðstefnur og sýningar:

Ráðstefnur og fundir á vegum Skýrslutæknifélags Íslands:	http://www.sky.is
AS/400 ráðstefnur:	http://www.events400.com/
Ráðstefnur fyrir Microsoft búnað:	http://msevents.microsoft.com/isapi/events/usa/enu/default.asp
Ráðstefnur á vegum Key3Media Events:	http://www.key3media.com/
Ráðstefnur á vegum IBC UK Conferences Limited:	http://www.ibc-uk.com/
Ráðstefnur á vegum IIR:	http://www.iir-conferences.com/
Ráðstefnur á vegum Frost & Sullivan:	http://www.frost.com/conferences/
Ráðstefnur á vegum IDG World Expo:	http://www.idgworldexpo.com/
Upplýsingavefur TSCentral:	http://ww0.tscentral.com/
Upplýsingavefur ExpoBase:	http://www.expobase.com/
Upplýsingavefur TSNN:	http://www.tsnn.com/
Leitarvefur fyrir viðburði um allan heim:	http://www.expoworld.net

Samantekt á birtum greinum í 25. árgangi Tölvumála

Samantekt á birtum greinum í 25. árg.

5. tbl.