Kafli 10: Gagnaöryggi

IT Essentials 5.0

Þýðing: Tómas Jónsson

Cisco Networking Academy®
Mind Wide Open™

Mikilvægi gagnaöryggis

- Persónuupplýsingar, rekstraráætlanir, fjármálaupplýsingar, einkaleyfi og þjóðaröryggi eru sett í uppnám ef að öryggisáætlun og öryggisreglum er ekki fylgt
- Tæknimaðurinn hefur ríkar skyldur og ábyrgð varðandi gagnavernd

Öryggisógnanir

Mögulegar tölvuógnir:

- innri ógnir
  - starfsfólk getur veirusmitað tölvur, af slysni
- ytri ógnir
  - ytri notendur geta ráðist að kerfinu, með skipulögðum eða tilviljanakenndum hætti

Mismunandi tölvuöryggisárásir:

- efnislegir
  - þjófnaður, skemmdir og/eða eyðilegging tölvubúnaðar
- gögn
  - eyðing gagna, spjöll á gögnum, aðgangshindranir, óleyfilegur aðgangur eða gagnaþjófnaður

Tilkynningar, njósnahugbúnaður og blekkingar

Spillihugbúnaður (malware) er hver sá hugbúnaður sem er hannaður til þess að valda skemmdum á eða trufla virkni tölvukerfa:

- **„Adware”** – hugbúnaður sem birtir tilkynnningar á tölvu, oft birt í „pop-up”-glugga
- **„Spyware”** – hugbúnaði er laumað inn á tölvu, án tilverknaðar eða vitneskju notandans. Hugbúnaðurinn skráir og sendir frá sér aðgerðir og athafnir notandans.
- **„Phishing” -** hakkari lætur líta út fyrir að hann vinni fyrir lögmæt samtök eða stofnun og óskar eftir því að fórnarlambið láti upplýsingar í té, sv.s. notendanafn og/eða lykilorð

Veirur, ormar, Trójuhestur og „Rootkits”

- **Tölvuveira** er hugbúnaður eða forrit sem er búið til af ráðnum hug af tölvuhakkara. Tölvuveirur geta safnað viðkvæmum og/eða mikilvægum upplýsingum eða að eyðileggja eða spilla gögnum
- **Tölvuormur** er sjálfafritað forrit, sem nýtir netkerfi til þess að margfalda sjálfa sig og dreifa sér á milli nettækja. Minnsti skaði sem ormar valda er þó aðeins að draga úr bandbreidd og samskiptahraða
- **Trojuhestur** er svikahugbúnaður í dulargervi sem lítur út eins og lögmætt forrit. Nafnið fær forritið vegna þess að það kemst inn í tölvu, sem eitthvað áhugavert og /eða nytsamt.
- **Veiruvarnarforrit** er hannað til þess að greina, afvirkja og fjarlægja tölvuveirur, tölvuorma eða Trojuhesta, áður en að þau smita tölvuna
- **„Rootkit”** er svikaforrit sem nær fullum yfirráðum yfir tölvukerfi. Oft er þetta bein árás á tölvukerfi, með því að nýta þekkta veikleika eða lykilorð.

Veföryggi

Tól sem efla vefsíður en geta gert tölvurnar varnarlausar:

- **,,Active X”** – stýrir aðgerðum á vefsíðum
- **,,Java”** – leyfir keyrslu smáforrita í vafra
- **,,Java Script”** – hefur samskipti við HTML ,,source”-kóða til þess að leyfa gagnvirkni á vefsíðum
- **,,Adobe Flash”** – notað fyrir gagnvirknismiðla, sv.s. hreyfimyndir og tölvuleikir á Vefnum
- **,,Microsoft Silverlight”** – notað til þess að skapa fjölbreyttan gagnvirkan miðil fyrir Vefinn, líkt blossa (flash)

Hægt er að stilla flesta Vafra, til þess að koma í veg fyrir árasir, dæmi:

- **,,ActiveX”-síun**
- **,,Pop-up” hindrari**
- **,,SmartScreen”-síun í Internet Explorer**

„InPrivate” í vafra

- **„InPrivate”** hindrar vefvafra í því að vista neðangreindar upplýsingar:
  - notendanafn
  - lykilorð
  - vefkökur
  - vefrápssaga
  - skammtíma vefskrár
  - gagnasnið
- Vafri geymir skammtímaskrár og vefkökur en upplýsingarnar hverfa, þegar „InPrivate”-lotu lýkur
- Til þess að virkja „InPrivate”-vöfrun í Windows:
  - hægri smelltu á **Internet Explorer > Start InPrivate Browsing**

Ruslpóstur

- **Ruslpóstur** er óumbeðinn tölvupóstur sem mögulegt er að nýta til þess að senda skaðleg viðhengi eða villandi innihald
- **,,Popups”** eru gluggar sem opnast sjálfkrafa og eru hannaðir til þess að vekja athygli notandans og að birta honum mismunandi auglýsingar eða tilkynningar

Notið ruslpóstsíur, veiruvarnarhugbúnað, ,,popup-hindrara og þekkt einkenni svikapósts, til þess að glíma við þetta

TCP/IP árásir

TCP/IP-svítan stýrir samskiptum á Netinu. Hægt er að vanstilla og ráðskast með staðalinn til þess að hindra notendur í því að nálgast eðlilega og lögmæta þjónustu.

- **þjónustuhindrun (DoS)** – sendir nægilega margar beiðnir til þess að yfirhlaða þjóninn og þannig að hann geti síður sinnt sínu hlutverki eða jafnvel stoppað
- **dreifð þjónustuhindrun (DDoS)** – árás frá mörgum tölvum, kallast **,,zombies”** eða **,,botnets”**
- **,,SYN”-flæði** opnar TCP port tilviljanakennt og bindur tölvuna með miklu magni af fölsum SYN-beiðnum. SYN er stytting á ,,synchronization” og er beiðni um stofnun samskipta yfir net.
- **,,Spoofing” eða stæling –** notar tilbúin IP- eða MAC-vistföng til þess að villa um fyrir áreiðanlegum tölvum
- **Maðurinn í Miðjunni –** hlerun samskipta á milli tölva til þess að stela upplýsingum, sem er umbreytt yfir netkerfi
- **endursending –** gagnasendingar eru hleraðar og vistaðar af hakkaranum og síðan notaðar til óheimillar auðkenningar
- **DNS-eitrun -** breyting á DNS-skráningum til þess að beina umferð að svikaþjónum

Félagslegt yfirskin

- **„Social engineer”** er maður sem er fær um að fá aðgang að búnaði eða netkerfi með því að blekkja notendur til þess að láta af hendi trúnaðarupplýsingar, sv.s. lykilorð og notendanöfn

- Til þess að varast félagslegt yfirskin skaltu:
  - aldrei gefa upp lykilorðin þín
  - biddu alltaf ókunnar persónur, sem gefa sig á tal við þig um tölvur eða net, að gera grein fyrir sér
  - takmarkið aðgengi netgesta
  - fylgist með netnotendum
  - aldrei senda lykilorð
  - læstu alltaf tölvunni þegar þú gengur frá skrifborðinu
  - leyfðu aldrei neinum að fylgja þér um dyr, sem eru aðgangsstýrðar

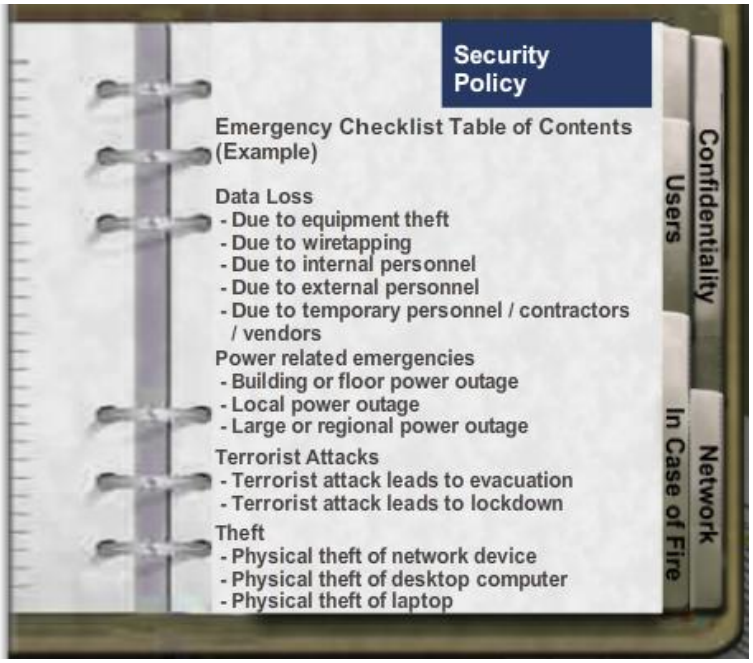
Förgun harðra diska og endurvinnsla

- Eyðið út af öllum hörðum drifum, notið síðan viðurkennd úteyðingartól, til að þurrka gögnin endanlega út
- Afseglun harðra diska, í þar til gerðu tæki er einnig möguleiki
- Eina leiðin til þess að fulltryggja eyðingu er að eyðileggja diskana að fullu með kramningu og einnig SSD-drif og geisladiska
- **Endurvinnsla harðra diska –** harða diska er hægt að endurnýta eftir endurforsnið

Öryggisáætlun

- Öryggisáætlun á að útlista hvernig fyrirtæki eða stofnun skipuleggur sín tölvuöryggismál

- Dæmi um svör við spurningum í öryggisáætlun:
  - hvaða einingar kerfisins þurfa varnir ?
  - hverjar eru mögulegar ógnir?
  - hvaða möguleikar eru á því að fylla upp í öryggisholur ?
  - hvernig skal haga þjálfun og menntun starfsfólks ?



Skilyrði í öryggisáætlun

Öryggisáætlun ætti m.a. að innihalda:

- ferli til þess að skipuleggja netöryggi
- ferli til þess að yfirfara og endurskoða gildandi netöryggi
- almennt öryggislíkan fyrir tölvukerfið
- leyfileg notendahegðun
- notendahegðun sem ekki er leyfð
- hvað ætti að skrásetja og hvernig á að geyma skrásetningarnar ?, viðburðaskrá (Event Viewer), kerfisskrásetningar (system log files) eða öryggisskrásetningar (security log files)
- netaðgangur í gegnum aðgangsskilyrði
- gagnaauðkenni, sv.s. notendanöfn, lykilorð, lífeinkenni eða snjallkort

Notendanöfn og lykilorð

Stefnumótun fyrir notendanöfn og lykilorð:

- breyta skal algengum sjálfgefnum notendanöfnum, sv.s. ,,administrator” eða ,,guest”
- netumsjónarmaður, ,,admin”, skilgreinir nafnareglu fyrir notendanöfn
- þrjú stig lykilorðsvarna gætu verið:
  - **BIOS**
  - **login**
  - **net**

Lykilorðastefna

Leiðbeiningar til þess að setja saman sterk lykilorð:

- **Lengd –** notið að a.m.k. átta rittákn
- **Flækjustig –** að lykilorð sé samsett úr stórum sem litlum bókstöfum, tölustöfum og sértáknum. Nota skal tákna víða um lyklaborðið, ekki samliggjandi tákn eða bókstafi.
- **Breytileiki –** endurnýjaðu lykilorð oft. Láttu minna þig á að skipta reglulega um lykilorð fyrir tölvupóst og netbanka ekki sjaldnar en á þriggja til fjögurra mánaða fresti.
- **Fjölbreytni** – notaðu mismunandi lykilorð fyrir hinar ýmsu þjónustur og vefsíður

Skrár og skráasafnaréttindi

- Réttindaþrep eru skilgreind til þess að takmarka aðgang einstaklinga eða hópa að gögnum
- **NTFS** – skráakerfi sem notar skrásetningu skráabreytinga áður en breytingar á skrám eiga sér stað
  - breytingar er mögulegt að skrá miðað við notanda, dagsetningu eða tíma
  - inniheldur dulkóðunarmöguleika
- **FAT 32** - engin dulkóðun
- **„Principle of Least Privilege" –** leyfa notendum aðeins aðgang að nauðsynlegum auðlindum
- **Takmörkuð notendaréttindi -**. ef að einstaklingi eða hóp er neitað um aðgang, yfirskríður þessi neitun önnur réttindi sem viðkomandi kann að hafa

Verndun gagna

Mikilvægi og verðmæti búnaðar og tækja er oft mun minna en mikilvægi og verðmæti þeirra gagna sem vistuð eru á tækjunum. Það eru nokkrar skynsamlegar leiðir til þess að vernda gögnin:

- hugbúnaðareldveggur
- snjallkortaöryggi
- lífeinkennaöryggi
- gagnaafrit
- dulkóðun gagna

Dulkóðun gagna

- Dulkóðun – gögnum er umbreytt með því að nota flókið algóritma, til þess að gera gögnin ólæsileg
- **„Encrypting File System" (EFS)** er eiginleiki í Windows, sem dulkóðar gögn
- **„BitLocker"** getur auðveldlega dulkóðað allt harða drifið
- **„Trusted Platform Module" (TPM)** er sérstök rafrás, sem sett er í móðurborðið og notuð fyrir bæði vél- og hugbúnaðarauðkenningu
  - TPM geymir stoðupplýsinar á grunnþjóni, sv.s. dulkóðunarlyklum, stafrænum staðfestingum og lykilorð

Varnir gegn spillihugbúnaði

- **„Malware”** er spillihugbúnaður sem settur er upp á tölvu, án vitneskju eða leyfis notandans
- Það getur þurft nokkur mismunandi varnarforrit gegn spillihugbúnaði og fjölskönnun, til þess að fjarlægja spillihugbúnaðinn að fullu
- Þau varnarforrit sem þarna um ræðir gætu verið: vírusvörn, vörn gegn njósnahugbúnaði, „adware”-vörn og vörn gegn blekkinga-hugbúnaði

Algengir dulkóðunarstaðlar

- **„Hash”-dulkóðun** notar stærðfræðiföll til þess að mynda tölugildi, sem ekki verður jafnað við gögnin
- **Samhverf dulkóðun** gerir kröfur um að báðir aðilar noti dulkóðunarlykil til þess að kóða og afkóða gögnin
- **Ósamhverf dulkóðun** notar tvo lykla, einkalykil og almennan lykil

„Service Set Identifiers”

- **„Service Set Identifier”** (SSID) er nafn á þráðlausu neti. Þráðlaus aðgangspunktur breiðvarpar SSID, sem sjálfgefin stilling, svo að þráðlaus tæki, geti fundið þráðlausa netið.
- Til þess að afvirkja SSID breiðvarp er t.d. hægt að nota neðangreinda slóð: **Wireless > Basic Wireless Settings >** veldu **Disabled** fyrir SSID breiðvarp **> Save Settings > Continue**
- Í þessu felst ekki mikið öryggi, en það minnkar þó mikið líkur á að hakkað sé inn á þráðlaust net, sem ekki birtist hakkaranum, heldur þarf hann að slá nafn netsins handvirkt inn

Þráðlaus aðgangur

- **Þráðlaus loftnet**
  - til þess að hindra dreifingu út fyrir ákveðið netsvæði er hægt að setja upp stefnuvirk loftnet eða svonefnd mynsturloftnet, sem mynda afmarkað sendisvæði, fyrir ákveðna notendur
- **Aðgangur nettækis**
  - í fyrstu tengingu nettækis, ætti alltaf að breyta sjálfgefnu notandanafni og lykilorði
- **Wi-Fi vernduð uppsetning (WPS)**
  - notandi tengist þráðlausum aðgangspunkti með verksmiðjustilltu PIN, sem oft er prentað á límmiða
  - þróað hefur verið forrit sem hlerar netumferð og endurbirtir WPS PIN og fyrirframsendan dulkóðunarkykil
  - afvirkjaðu WPS á þráðlausa aðgangspunktinum, ef mögulegt er

Eldveggir

Hardware Firewall	Software Firewall
Dedicated hardware component	Available as third-party software, cost varies
Initial cost for hardware and software updates can be expensive	Free version included with Windows operating system
Multiple computers can be protected	Typically protects only the computer on which it is installed
No impact on computer performance	Uses the CPU, potential impact on computer performance

Port-sending og port-ræsing

- **Port-sending** er reglutengd aðferð til þess að beina netumferð á milli tækja á aðskildum netum:
  - Er notað þegar að opna verður ákveðið port svo að ákveðinn hugbúnaður og forrit geti haft samskipti við tæki á öðrum netum
  - Rúter ákveður hvort að senda eigi netumferð á ákveðið tæki, samkv. portnúmeri, dæmi: port 80 fyrir HTTP
- **Port-ræsing** gerir rúter kleift að framsenda gögn tímabundið, í gegnum inn-port á ákveðnu tæki
  - Sem dæmi, tölvuleikur gæti notað port 27000 til 27100 til þess að tengjast öðrum notendum. Þetta er port-ræsing.

Aðferðir til búnaðar- og tækjaverndar

- Búnaðar- og tækjaöryggi er oft jafnmikilvægt og gagnaöryggi. Mögulegt er að verja netbúnað m.a. með:
  - traustum samskiptaklefum, traustum tækjaskápum eða búrum
  - með kapallásum og öryggisskrúfum, til þess að festa búnaðinn
  - þráðlausri skynjun ef óviðkomandi kemst inn
  - vélbúnaðareldveggjum
  - netumsjónarkerfi sem skynjar breytingar í vírun og tengibrettum
- **Tveggja þátta auðkenning –** öryggi með skörun tveggja aðskildra varnarþátta, til þess að hindra óviðkomandi aðgang að viðkvæmum gögnum
  - dæmi um tveggja þátta auðkenningu er notkun bæði lykilorðs og snjallkorts

Öryggisvélbúnaður

- **Það eru nokkrar gerðir varna fyrir tölvubúnað:**
  - notið búnað með kapallásum
  - læsið herbergjum sem hýsa samskiptabúnað
  - notið öryggisskrúfur í búnað og í búnaðarfestingar
  - notið læst öryggisbúr utan um mikilvægan tölvubúnað
  - merkið búnað og setjið í hann skynjara, sv.s. rafeindaauðkenningu (RFID)
  - setjið upp viðvörunarbjöllur, tengdar hreyfiskynjurum
  - notið vefmyndavélar með hreyfiskynjun og eftirlitshugbúnaði
- **Aðgangstakmarkanir og auðkenning:**
  - snjallkort sem innihalda notandaupplýsingar, þ.á.m. mismunandi öryggissvæði
  - skynjarar fyrir lífauðkenni sem m.a. fingrafar, augnhimna og handar- eða höfuðlag
  - öryggisvarsla
  - eftirlitskerfi, hreyfi- eða hitaskynjarar, tækjaauðkenni (RFID)

Þjónustupakkar og öryggisviðbætur

- Reglulegar öryggisuppfærslur eru mikilvægar, til þess t.d. að verjast veirum og ormum
- Tæknimaðurinn verður að hafa innsýn í hvernig og hvenær eigi að setja upp viðbætur og uppfærslur
- **Viðbætur** eru kóðaviðbætur sem framleiðendur setja fram, t.d. til að ráða niðurlögum nýuppgvötvaðrar tölvuveiru eða tölvuorms
- **Þjónustupakki** er samsetning viðbóta og uppfærslna

- Windows hleður sjálfkrafa niður og uppfærir sjálfkrafa eða samþykkisstýrt;
  - **Start > All Programs > Windows Update > Change settings**

Gagnaafritun

- Hægt er að stilla afritun í Windows handvirkt eða tímastillt sjálfvirk afritun

- Til þess að stilla Windows-afritun í fyrsta skipti, fylgið neðangreindri slóð:

  Start> All Programs > Maintenance >Backup and Restore >Set up backup

Type of Backup	Description
Full or Normal	This backup type copies all selected files and marks each file as having been backed up.
Incremental	This backup type backs up only files that have been created or changed since the last full or incremental backup. Restoring files requires that you have the last full backup set and all incremental backup sets.
Differential	This backup type copies only files that have been created or changed since the last full backup. Restoring files requires that you have the last full and one differential backup.
Daily	This backup type copies all selected files that have been modified the day that the daily backup has been performed.
Copy	This backup type copies all selected files but does not mark them as having been backed up.

Uppsetningar á mismunandi eldveggjum

- **Eldveggur** síar þá netumferð sem valin er, frá netkerfi eða tölvu
- **Takmarkandi öryggisstefna** – eldveggur opnar aðeins nauðsynleg port
- Stillingar á Windows-eldvegg eru mögulegar á tvo vegu:
  - **sjálfvirkt** – notandinn fær skilaboð eins og **„Keep Blocking”**, **„Unblock”** eða **„Ask Me Later”** fyrir óumbeðnar beiðnir
  - **umsjón með öryggisstillingum** – notandinn bætir við forriti og porti, sem krafist er fyrir hugbúnað á neti

Uppsetning aðgengi og réttinda

- Notendahópur sem vinnur að svipuðum verkefnum getur fengið aðgang í gegnum hópréttindi
- Þegar starfsmaður lætur af störfum, ætti að gæta þess að eyða út aðgangi og réttindum hans, þegar í stað
- Hægt er að veita gestum aðgang, í gegnum ,,Guest”-aðgang

Vandamálaleit; komið fram með kenningu

- Setjið saman lista yfir algengustu orsakir öryggisvandamála:
  - tölvuveira
  - Trojuhestur
  - tölvuormur
  - njósnahugbúnaður
  - ,,adware”
  - spillihugbúnaður
  - blekkingar
  - veik lykilorð
  - óvarðir tölvusalir
  - óvarin vinnusvæði

Reyndu á hvort að kenningin sé rétt

- Reyndu á kenningar, eina í einu og þá einföldustu og augljósustu fyrst:
  - aftengdu tölvu frá netinu
  - uppfærðu vírusvarnir
  - skannaðu tölvuna fyrir smiti
  - athugaðu síðustu uppfærslur á stýrikerfi og stýrikerfisviðbætur
  - endurræstu tölvuna eða netbúnaðinn
  - skráðu þig inn sem annar notandi, til þess að breyta lykilorði
  - verðu og fylgdstu með tölvusölum
  - verðu vinnusvæði
  - framfylgdu öryggisstefnu
- Ef að orsakir vandans hafa ekki fundist, þarf að setja fram nýjar og hugsanlegri dýpri kenningar

Fullreyndu virkni alls kerfisins með fyrirbyggjandi ráðstöfunum

- Virkni kerfis reynd
  - endurskannið tölvuna til þess að fulltryggja að ekkert smit sé til staðar
  - endurskannið tölvuna til þess að fulltryggja að ekkert njósnaforritsmit sé til staðar
  - skoðið öryggishugbúnaðarskráningar, log, til þess að tryggja að engin vandamál séu enn til staðar
  - prófið net- og Nettengingar og samskipti
  - tryggðu að öll forrit ræsi og keyri rétt
  - sannreynið að rétt auðkenni dugi til aðgangs að auðlindum, sv.s. prenturum eða gagnagrunnur
  - gangtu úr skugga um að allt netaðgengi sé í lagi
  - gangtu úr skugga um að öryggisstefnu sé framfylgt

Samantekt úr 10. kafla

- Með því að fylgja vel gerðri öryggisáætlun mun vernda tölvur og nettæki, auk tölvugagna gegn þjófnaði, skemmdum og tölvuhökkun
- Öryggisógnir geta komið innan tölvukerfis eða að utan
- Tölvuveirur og ormar eru algengar tölvuógnir
- Þróun, viðhald og notkun öryggisstefnu ætti að nægja til þesss að verja bæði búnað og gögn
- Haldið stýrikerfinu og hugbúnaði rétt uppfærðu og setjið inn reglulegar viðbætur og þjónustupakkar