MOLAR ERU LÍKA BRAUÐ

Gerðu þér mat úr dagbókum

Skýrslutæknifélagið 1. okt 2014

Jónas S Sverrisson

SKILGREININGAR

Dagbók = Log

Aðgerðaskrá = Log

Hreyfingaskrá = Log

Færsluskrá = Log

Kerfisdagbók = Log

KÆRA DAGBÓK

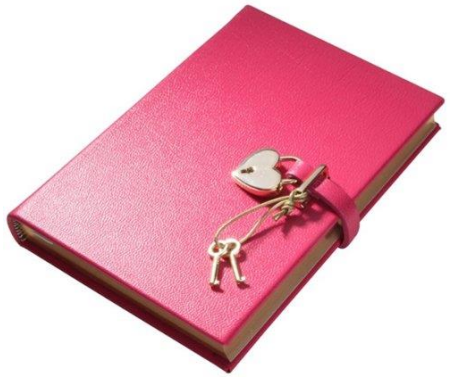
Dagbækur innihalda oft mjög viðkvæmt efni sem getur valdið verulegum óþægindum ef óviðkomandi nær aðgangi.

Innihald dagbóka ætti að vera eins rétt og mögulegt er annars er hætta á mistúlkun efnisins.

Mikilvægt að hafa allar dagsetningar réttar ef nauðsynlegt er að sýna fram á eitthvað.

Enn mikilvægara er að stýra aðgangi að dagbókinni.

Þá er mjög mikilvægt að koma í veg fyrir breytingar á dagbók.



#mammaekkilesadagbokina

HVAR ERU DAGBÆKURNAR

Netvirki

Leiðstjórar

Stýrikerfi

Eftirlitskerfi (hiti, raki, hreyfing, lásar ...)

Hugbúnaður

Gagnagrunnar

Símkerfi

Bílar

ILLU AUGUN ÞÍN ...

Hvers virði eru dagbækur í augum vonda kallsins

- Stundum innihalda þær notandanafn, lykilorð, tölvupóst, símanúmer, kennitölur ... (Vodafone)
  - Nýtist öðrum til frekari illvirkja þegar dagbókum hefur verið dreift á netinu
- Mögulegt að sjá hvernig álag er á kerfum og fela sig þegar mest er að gera
- Mögulegt að breyta dagbókum til að sýna annan veruleika (sýndardagbók?)
- Ef dagbók er tóm eða hefur verið eytt þá er ljóst að eitthvað hefur gerst – það eru bara engar aðrar upplýsingar til um hvað gerðist.

Vondir kallar geta líka framkvæmt greiningu á dagbókum, sér í hag.

BLÁU AUGUN ÞÍN ...

Hvers virði eru dagbækur í augum góða konunnar

- Rekjanleiki aðgerða.
  - Of seint fyrir barnið að detta ofan í brunninn
- Sönnun á framkvæmd
- Gefur mynd af stöðunni á hverjum tíma
- Nýtist til mælinga t.d. bandvídd – erum við að fá þá bandvídd sem við greiðum fyrir?
  - Bandvíddarmælingar geta gefið til kynna bilanir í kerfum t.d. ef afritun er ekki að fara fram á tilsettum tíma
- Nýtist til að sýna fram á hlýtingu – ertu að gera það sem þú átt að gera.
- Nýtist í greiningu á bilunum, svikum, innbrotum ...

Mikilvægt að skoða innihald dagbóka til að auka öryggi

- Ýmis búnaður til, til þess að greina innihald dagbóka

ÞÚ SKALT ...

ISO 27001:2013

- A.12.4 Dagbókaskráningu og eftirlit
  - Markmið: Að skrá atburði og búa til sönnunargögn
- A.12.4.1 Atburðaskráning (Event logging)
- A.12.4.2 Verndun dagbókaupplýsinga (Protection of log information)
- A.12.4.3 Dagbækur kerfisstjóra og rekstrarstjóra (Administrator and operator logs)
- A.12.4.4 Samstilling klukkna (Clock synchronisation)

Reglugerð um rafræna reikninga

Lög um bókhald

HINGAÐ OG EKKI LENGRA

Varnir gegn misnotkun dagbóka

- Ef nauðsynlegt er að geyma viðkvæmar upplýsingar í dagbókum, notið þá dulritun.
- Sendið allar dagbækur á einn stað.
  - Tryggir aðgangsstjórnun, kerfisstjórar hafa ekki aðgang að dagbókum nema til lestrar.
  - Senda dagbækur í skýin?
- Tryggið að ekki verði hægt að breyta, eyða eða bæta við færslum í dagbækur.
- Tryggið að allar dagbækur nýti sömu klukku.
  - Gott að hafa réttan tíma en algjörlega nauðsynlegt að allar dagbækur hafi sama tíma
  - Rekjanleiki aðgerða milli kerfa er ómögulegur ef klukkur hafa ekki verið samstilltar

GALLIN ER SÁ AÐ ...

Mikið magn – kostnaður - tími

Til hvers?

Hver á að lesa þetta?

Hvenær á að lesa þetta?

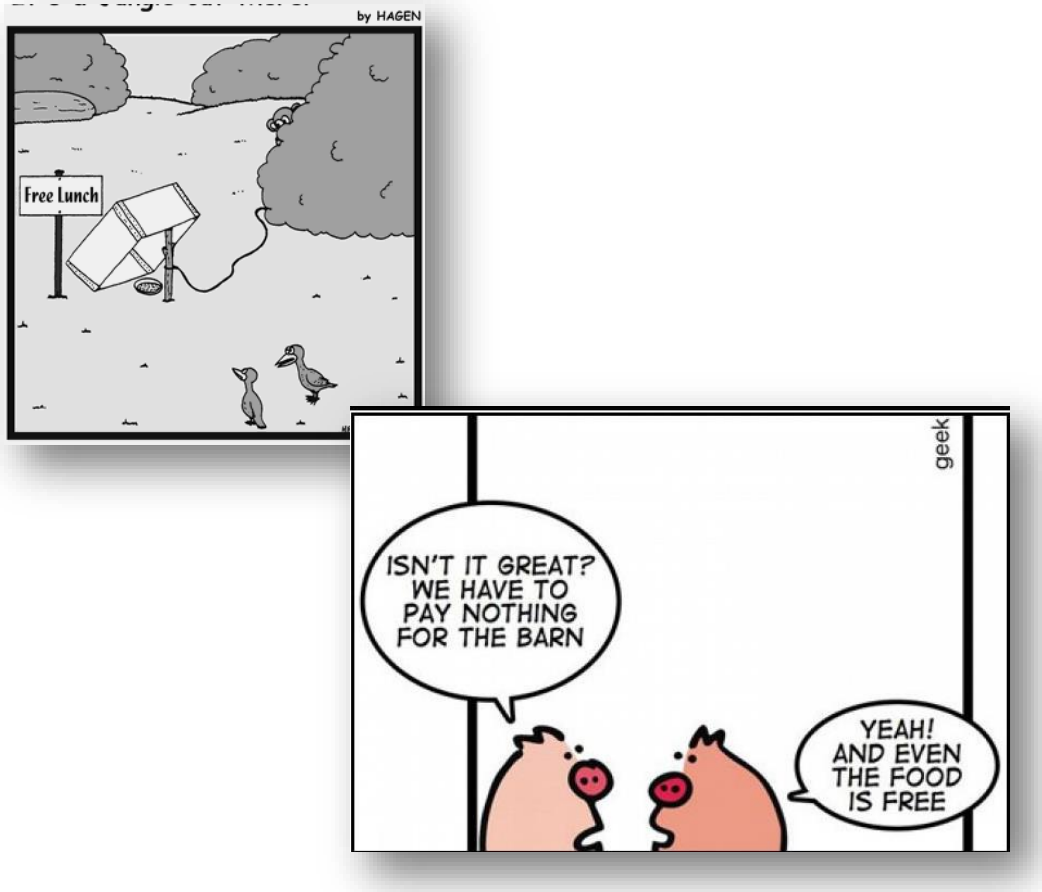
Hvað er nóg?

Fullt af ryki?

Yfirskrifaðar dagbækur (hringbók) – tapaðar upplýsingar

Notað í röngum tilgangi

ÞAÐ ER NÚ HÆGT AÐ GERA SÉR MAT ÚR ÖLLU



Mögulegt að gera sér mat úr aðgerðadagbókum.

- Facebook
- Google
- Og allir hinir

Ef þú situr ekki við borðið þá ertu á matseðlinum.

EITTHVAÐ FLEIRA?