

HAGNÝT RÁÐ – VÖKTUN OG SKRÁNING

Logga allt!

Hádegisverðarfundur Ský
Grand Hótel - 1. október 2014



Arnaldur F. Axfjörð
Sérfræðingur

DAGSKRÁ

Vöktun og skráning

Kröfur

Útfærsla

Hagnýt ráð



Vöktun og skráning



HVAR ER VAKTAÐ OG SKRÁÐ?

- Netþjóðar
 - Netstýrikerfi
 - Gagnagrunnar
 - Vefþjóðar
- Netbúnaður
 - Tengingar og umferð í netbúnaði
 - Netumsjón
- Netvarnir
 - Eldveggir
 - Innbrotsskynjunarkerfi (IDS)
- Skeytamiðlun

HVAR ER VAKTAÐ OG SKRÁÐ?

- Kerfishugbúnaður
 - Afritun
 - Vinnslur
- Notendahugbúnaður
- Útstöðvar
 - Stýrikerfi útstöðva
- Snjallsímar
 - Staðsetning – GPS
- Nettengd tæki
 - Prentarar
 - Skannar
 - Fjölnotatæki

HVAR ER VAKTAÐ OG SKRÁÐ?

- Aðgangskerfi
 - Kort og kóði
- Eftirlitsmyndavélar
- Iðnstýritölvur
 - Frystigeymslan
 - Framleiðslulínan
 - Kaffivélin!
- Gagnaskráningartæki – *data loggers*
 - Bifreiðar, vinnuvélar, flugvélar – „svarti kassinn“
 - Holter
 - Hitastig, rakastig, titringur, þrýstingur, ...
- Flestur annar búnaður sem hefur örgjörva

TEGUNDIR SKRÁNINGAR

- Atburðaskráning – *event logs*
 - Aðgerðir notenda
 - Innskráning, útskráning
 - Notkun sérréttinda
 - Notkun forrita og kerfa
 - Færslur framkvæmdar af notendum
 - Notkun skráa
 - Aðgerðir notenda með sérréttindi
 - Aðgerðir kerfa
 - Frávik
 - Villur
 - Öryggisatvik
- Færsluskráning – *transaction logs*
- Skeytaskráning – *message logs*
 - Viðskiptaskeyti
 - IM, VoIP, IRC, P2P skráarsöfn, netleikir

TEGUNDIR SKRÁNINGAR

- Vöktun notenda
 - Lyklaborð og mús – *keylogger, cursor tracking*
 - Skjámyndir – myndskleið
 - Aðgerðir
- Stafrænar slóðir – fótspor (á Internetinu)
 - Slóðir í rafrænni þjónustu
 - Smekkur, áhugi, skoðanir, trú, val, staðsetning, ...
- Notkunarmynstur notanda – *user profile*
 - Notkun, hegðun
- Greining búnaðar – *device forensics*
 - Stýrikerfi, vafri o.fl.

Kröfur



UNDIRLIGGJANDI KRÖFUR

- Hvað þarf að skrá
- Hvað má skrá
- Hvað má ekki skrá
- Hversu lengi þarf að varðveita skráningu
- Hversu lengi má varðveita skráningu
- Hver má hafa aðgang að skráningu
- Hver ætti ekki að hafa aðgang að skráningu

TILGANGUR SKRÁNINGAR

- Viðvaranir
 - Rekstraröryggi og áætlanir um rýmd og afköst
 - Öryggisatvik
- Rekjanleiki
 - Staðfesting á aðgerðum og vinnslum
 - Greining á villum og rekstrartruflun
 - Aðgengi að gögnum
 - Afmörkun ábyrgðar
- Úttektarslóðir
 - Hlíting við kröfur
 - Staðfesting á aðskilnaði hlutverka
 - Vernd á viðkvæmum upplýsingum

TILGANGUR SKRÁNINGAR

- Endurrétting kerfa – *recover from crashes*
 - Færslur í gagnagrunnum
 - Villupolin kerfi
- Sannanir
 - Viðbrögð við atvikum – agaferli, lögsókn
 - Leki á upplýsingum
 - Sönnun á sakleysi
- Greining
 - Aðlögun þjónustu
 - Söfnun upplýsinga og sala

FRÍÐHELGI EINSTAKLINGA

- Skráning getur innihaldið viðkvæm gögn og persónugreinanlegar upplýsingar
- Vöktun þarf að vera í málefnalegum tilgangi
- Tryggja þarf viðeigandi verndun persónuupplýsinga
- Vinnsla persónuupplýsinga þarf að vera í samræmi við tilgang og þær ekki geymdar lengur en þörf krefur

STÝRINGAR ÚR ISO27K

- Búa til og varðveita atburðaskrá, og rýna reglulega
- Gera viðeigandi ráðstafanir til að tryggja friðhelgi
- Vernda skráningarbúnað og atburðaskrár gegn fikti og óheimilum aðgangi
 - Vernda gegn óheimilum breytingum á atburðaskrár og rekstrarvandamálum í skráningarbúnaði
 - Kerfisstjórar ættu ekki að hafa réttindi til að eyða skráningu á sínum aðgerðum eða gera skráningu óvirka
- Skilgreina og innleiða verklagsreglur fyrir að finna, safna, afla og varðveita upplýsingar sem gætu verið sannanir
 - Sönnunargögn fyrir meðhöndlun agabrota eða lögbrota

Útfærsla



STJÓRNUN Á VÖKTUN OG SKRÁNINGU

- Aðgerðir
 - Söfnun á skráningu
 - Margbreytileg snið
 - Sértek snið
 - Falskar meldingar (t.d. IDS)
 - Miðlæg söfnun á skráningu
 - Staðlað snið
 - Varpanir á milli sniða
 - Langtíma varðveisla á skráningu
 - Greining á skráningu
 - Í rauntíma
 - Eftirá – magngreining
 - Leit í skráningu
 - Skýrslur úr skráningu
- Skeyti
 - Úttektarskár og -slóðir
 - Atburðaskrár
 - O.fl.

GREINING Á SKRÁNINGU

- Dæmigerðar ástæður greiningar
 - Hlíting við öryggisreglur
 - Hlíting við lög eða úttektarkröfur
 - Bilanagreining á kerfum
 - Réttargreining (vegna rannsókna)
 - Viðbrögð við öryggisatvikum
- Virkni og tækni
 - Samkeyrsla (mismunandi kerfi og skeytasnið)
 - Mynsturgreining
 - Flokkun og merking (fyrir síðari tíma notkun)
 - Greining á venlum (leit að stökum atburðum í skráum frá mörgum kerfum)
 - Gervi-blindni (þekkja og hunsa algenga atburði)

ÞROSKI Í VÖKTUN OG SKRÁNINGU

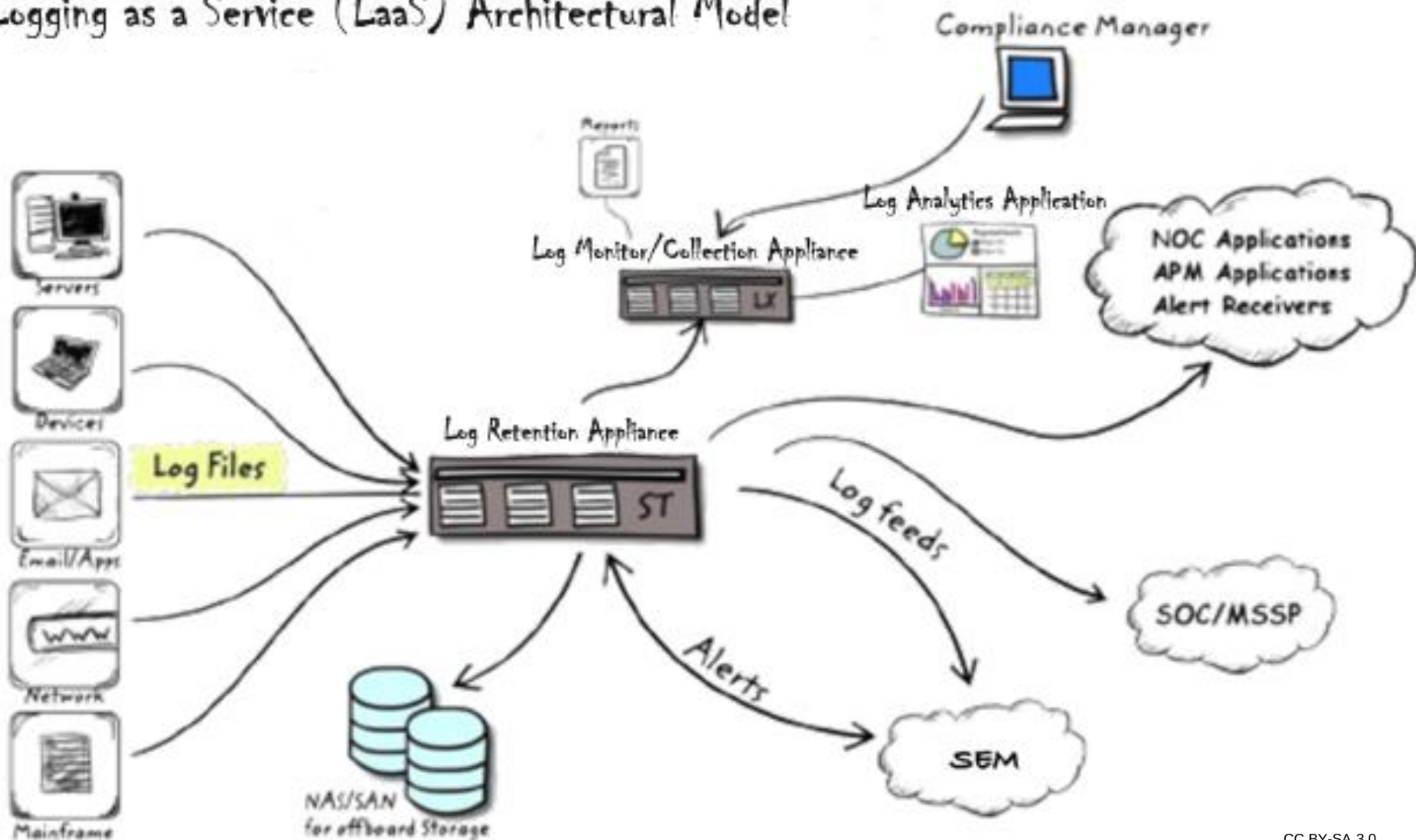
- Stig 1
 - Fyrirtækið notar skráningu í mismunandi búnaði til að reyna að þekkja mynstur sem gefur til kynna árás á ytri öryggismærum.
- Stig 2
 - Með samþættum lausnum getur fyrirtækið notað skráningu til að nema aðgengi og notkun á trúnaðarupplýsingum innan öryggismæra.
- Stig 3
 - Greiningartól geta rakið og vaktað virkni og tiltækileika kerfa og upplýsingaeigna, sérstaklega það sem er talið mjög mikilvægt.
- Stig 4
 - Fyrirtækið samþættir skráningu mismunandi viðskiptakerfa til að auka virði í starfseminni.
- Stig 5
 - Fyrirtækið sameinar vöktun á raunlægum og rökrænum aðgangi í einu kerfi.

THE SYSLOG PROTOCOL

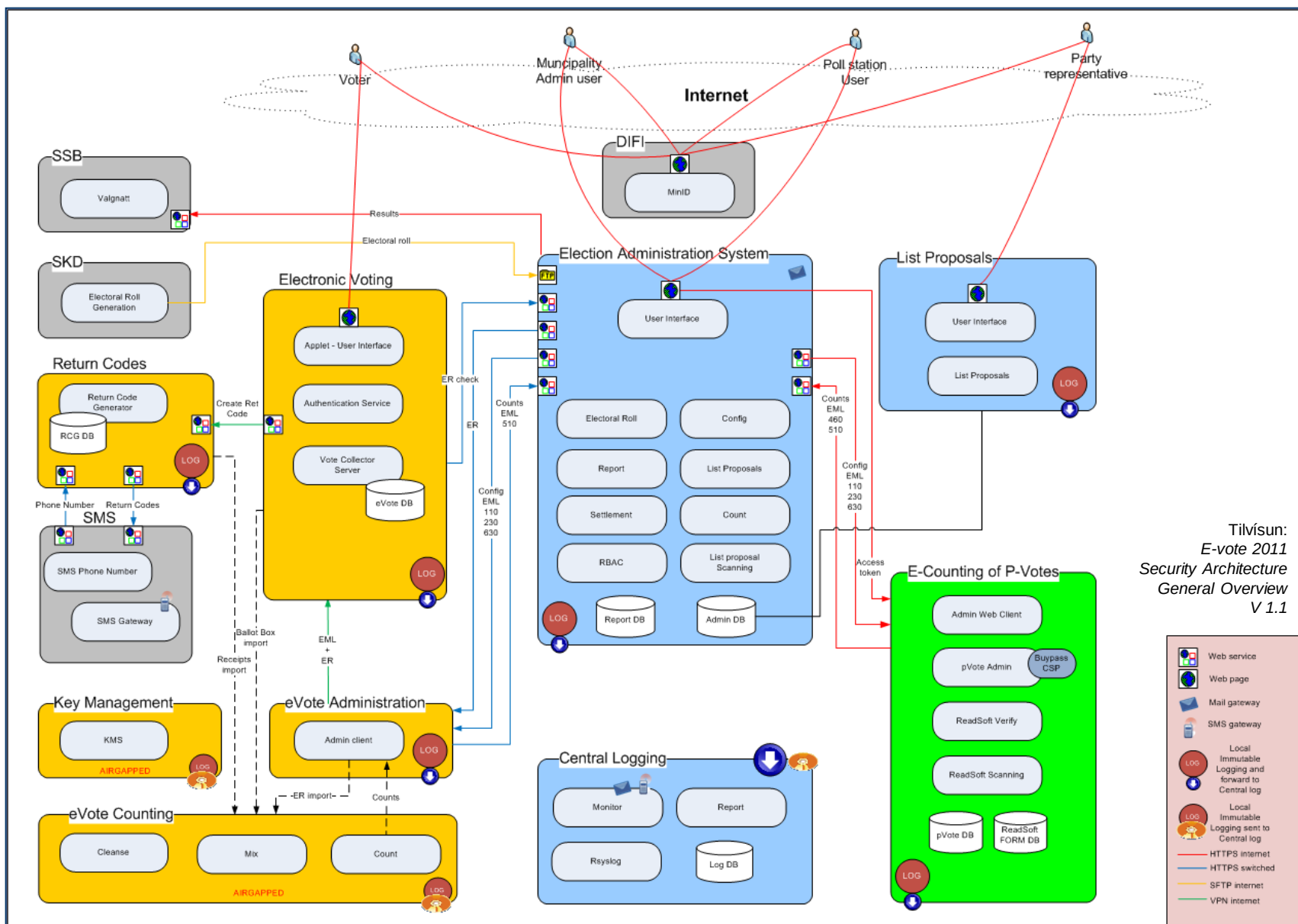
- Staðall fyrir skráningarskeyti tölvukerfa – RFC 5424
 - Stutt af fjölda tækja og búnaðar
 - Hægt að nota til að samþætta skráningu á einn stað
- Notagildi skráningar
 - Stjórnun tölvukerfa
 - Úttektarslóðir
 - Almennar upplýsingar
 - Greining
 - Bilanaleit
- Alvarleikaflokkar
 - Neyð – *emergency*
 - Árvekni – *alert*
 - Alvarlegt – *critical*
 - Villa – *error*
 - Viðvörðun – *warning*
 - Tilkynning – *notice*
 - Upplýsingar – *info*
 - Villuleit - *debug*

LOGGING AS A SERVICE (LaaSS)

Logging as a Service (LaaS) Architectural Model

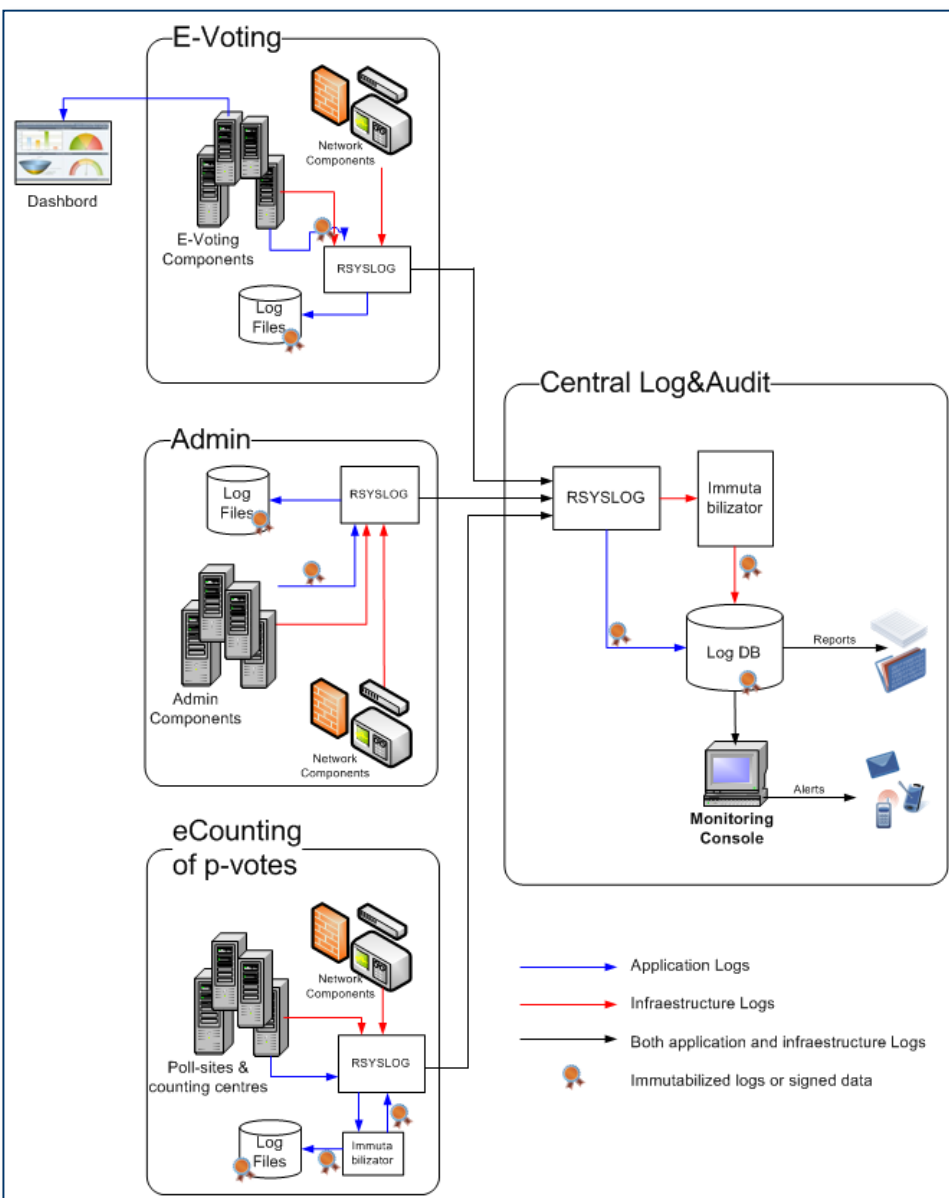


DÆMI: E-VOTE Í NOREGI – ARKITEKTÚR



Tilvísun:
E-vote 2011
Security Architecture
General Overview
V 1.1

E-VOTE Í NOREGI – ATBURÐASKRÁNING OG ÚTTEKTIR



- Skráningu er safnað frá atburðum bæði í hugbúnaði og í innviðum
- Skráningu er safnað í hverju þriggja kerfanna
- Afrit sent í miðlægt skráar- og úttektarkerfi
- Til að koma í veg fyrir fikt í skráningu er stöðugt bætt við tætigildi af fyrri færslum (HMAC)
- Færslur eru fiktvarðar í kerfunum áður en þær eru sendar í miðlæga kerfið
- Staðlaðar atburðaskráningar í innviðum eru fiktvarðar í miðlæga kerfinu

Tilvísun:
E-vote 2011
Security Architecture
General Overview
V 1.1

SAMÞÆTT STJÓRNUN ATBURÐA OG ÖRYGGIS

- *SIEM – Security Information and Event Management*
- Samþættir stjórnun upplýsingaöryggis og stjórnun öryggisatburða
- Selt sem hugbúnaður, sértækur búnaður eða útvistuð þjónusta
- Algeng notkun
 - Söfnun, greining og birting á upplýsingum frá nettengdum búnaði og öryggiskerfum
 - Umsjón með auðkenningu og aðgangi
 - Stjórnun á veikleikum og verkfæri fyrir hlítingu við reglur
 - Atburðarskráning stýrikerfa, gagnagrunna og notendaforrita
 - Gagnasöfnun um ytri ógnir

DÆMIGERÐIR ÞÆTTIR Í SIEM KERFUM

- **Gagnasöfnun**
 - Safnar göngum, m.a. frá netkerfi, öryggiskerfum, netþjónum, gagnagrunnum og notendaforritum, til að auðvelda eftirlit og tryggir að mikilvægir atburðir séu í forgrunni.
- **Fylgni**
 - Leitar að sameiginlegum eigindum og tengir atburði frá ólíkum búnaði saman í nothæfar upplýsingar.
- **Viðvaranir**
 - Greinir samtengda atburði og viðvaranir til að melda áríðandi þætti, t.d. á mælaborð eða með tölvupósti.
- **Mælaborð**
 - Tekur gögn um atburði og varpar þeim í upplýsandi gröf til að hægt sé að sjá mynstur eða til að þekkja aðgerðir sem eru ekki í samræmi við þekkt mynstur.
- **Hlíting**
 - Safnar saman gögnum um hlítingu og gerir skýrslur fyrir öryggis-, stjórnunar- og úttektarferli.
- **Varðveisla**
 - Safnvistar söguleg gögn til að styðja greiningu á fylgni yfir tímabil og til að uppfylla hlítingarkröfur um varðveislu. Langtímavarðveisla gagnag er mikilvæg fyrir réttarrannsóknir.
- **Réttargreining**
 - Gerir mögulegt að leita þvert á atburðaskrár í mismunandi búnaði og yfir tímabil byggt á tilgreindum viðmiðum.

MIKILVÆGI TÍMASKRÁNINGAR

- Nákvæmni í skráningu
 - Rannsóknir
 - Sannanir í málarekstri
 - Kröfur í lögum og reglum
 - Kröfur í samningum
 - Hlíting við staðla
 - Kröfur til innri vöktunar
- Allar klukkur ættu að vera samstilltar við eina tímaveitu

Hagnýt ráð



HAGNÝT RÁÐ

- Meta áhættu upplýsinga og ákvarða stýringar, mælingar og eftirlit
 - Atburðaskrár og færsluskráning eru líka upplýsingar
 - Staðfesta hvað þarf að skrá og vakta
- Þekkja gögn fyrirtækisins og kröfur um vernd
 - Flokka gögnin eftir viðkvæmni
 - Þekkja kröfur um aðgengi
 - Þekkja kröfur um varðveislutíma
- Marka stefnu í vöktun, eftirliti og skráningu
 - Staðfesta tilgang og markmið með skráningu
- Vita hvað er skráð í öllum búnaði
 - Ekki skrá óþarfa upplýsingar
 - Forðast persónugreinanlegar upplýsingar
 - Kortleggja allar viðkvæmar upplýsingar
- Útfæra vöktun og skráningu – og innleiða

HAGNÝT RÁÐ

- Lágmarka réttindi að skráningargögnum og búnaði
 - Endurskoða aðgangsstýringar að skráningargögnum
 - Muna eftir öllum búnaði – t.d. fjölnotatækjum
 - Takmarka réttindi kerfisstjóra að skráningu á eigin aðgerðum
- Huga að afritun á skráningarupplýsingum
 - Eru persónuupplýsingar hugsanlega geymdar of lengi á afritum?
 - Eru trúnaðarupplýsingar óvart settar á afrit?
- Tryggja að tímafærslur séu nægilega nákvæmar
 - Vegna rekjanleika og sannana
- Þekkja vöktun og skráningu í vefsetri fyrirtækisins
 - Vita hvað vefgreiningartólin eru að gera
 - Hafa yfirsýn á skráningu og möguleika
 - Tryggja að skráningarupplýsingar séu verndaðar á viðunandi hátt
- Gera sérstakar ráðstafanir til að verjast leka á viðkvæmum upplýsingum
 - Rekja aðgengi að skrám
 - Vakta afritun og tilfærslu skjala
 - Útiloka saklausa

TAKK FYRIR!

ADMON
RÁÐGJÖF

Arnaldur F. Axfjörð
arnaldur.axfjord@fjr.is

