Hvernig brúum við bilið?

Öryggisskuld er stjórnunarlegt viðfangsefni. Ekki tæknilegt.

Sigfinnur Valur Viggósson · CISO, Origo · April 2026

Þegar svarið var löng þögn

Á hvað er ég að horfa?
- og hvað viltu að ég geri?

Vandinn var ekki tæknin.

Vandinn var tungumálið. Tæknimenn tala um veikleika. Stjórnendur þurfa að heyra um afleiðingar.

Öryggisskuld snýst um stjórnun. Hún er ekki tæknileg áskorun.

Við getum tekist á við hana á einfaldan hátt:

1. Setjum fram afleiðingar með skýrum hætti – hættum að tala um veikleika og veikleikastig
2. Bjóðum stjórnendum upp á val – ekki vandamál
3. Skilum áhættum til eigenda, tryggjum eignarhald – tryggjum skilning á afleiðingu áhættu
4. Greiningartími, viðbragðstími, öryggisskor, ofl. – Til að stjórna þá þurfum við að mæla

Hvað er öryggisskuld?

Tækniskuld vs. öryggisskuld

Tækniskuld
- Hægir á framþróun
  - Öll vinna verður þyngri

Öryggisskuld
Safnar vöxtum í kyrrþey. Gjaldfellur öll í einu þegar varnir bresta.

Birtist sem:
Niðritími · Glatað traust · Lagaleg ábyrgð · Fjárhagslegt tjón

Fjórar birtingamyndir öryggisskuldar

01 Tæknileg skuld

Óuppfærð kerfi og úreld högun

02 Nýjungar skapa skuld

Gervigreind og skýjalausnir án stýringa og ramma

03 Stjórnunarskuld

Reglur sem lifa á pappir en ekki í menningunni

04 Leiðtogaskuld

Skortur á skilningi, skýru eignarhaldi og ábyrgð stjórnenda

Heimild: ISACA Security Debt Index, 2025

Hvernig mælum við öryggisskuld?

Security Debt Index (ISACA, 2025)

SEVERITY

Hvaða áhrif hefur vandinn á reksturinn?

DURATION

Hversu lengi hefur vandinn verið til staðar?

VELOCITY

Hversu hratt fjölgar sambærilegum vandamálum?

Mælikvarðar — þýddir yfir á máli stjórnenda

Skor 1-5 fyrir hvern þátt → SDI heildarskor → Stígur hann eða lækkar hann yfir tíma?

Fáum við greidda leigu, fyrir að hýsa utanaðkomandi? origo.

241

DAGAR

Meðaltími frá innbroti til uppgötvunar — IBM 2025

Við útvistum vöktun

Treystum á þjónustuaðila (MSP) — Þjónustuaðilinn þekkir ekki alltaf hverjir eru í þínu umhverfi.

Við þekkjum ekki hvað er eðlileg hegðun

Án skilgreinds grunnviðmiðs (baseline) þá erum við blind — við þekkjum ekki hvað er eðlilegt.

Prófanir og viðbragð

Viðbragðsáætlun sem ekki hefur verið prófuð er ekki til. Við getum ekki væntingastýrt þegar á reynir.

Hver á áhættuna - og veit hann af því?

origo.

Tæknimenn segja

- Óplástraðir veikleikar í 47 kerfum.
- 5 veikleikar með CVE-high.
- 2 internet netþjónar í úreldri útgáfu.

Tæknilegar staðreyndir, stjórnendur skilja ekki.

BILIÐ

MISSKILNINGUR

Stjórnendur þurfa

- Ef þessir veikleikar eru nýttir — getum við átt von á niðurtíma sem kostar X milljónir á dag
- Þessir fimm veikleikar eru þeir sem árásarmaður myndi nýta fyrst — þeir eru opnar dyr.
- Þessir tveir netþjónar eru utan við allar varnir — við sjáum ekki ef einhver er inni.

Áhætta sem á eiganda er stjórnað.

Hérna á milli lifir áhættan góði lífi.

Leiðtogaskuldin - ósýnilega

ISACA nefnir leiðtogaskuld: þegar öryggi er meðhöndlað sem hvert annað IT-verkefni — án skýrs eignarhalds og ábyrgðar stjórnenda.

Rannsóknin segir

- Færri en 15% stjórnarmanna hafa þekkingu á upplýsingaöryggi.
- Þegar enginn í stjórninni skilur vandann, hver spyr þá réttu spurningarnar?

NIS2 og DORA breyta leiknum

- Ábyrgð stjórnenda er nú bundin í lög
- Öryggisstjórinn er einstaklingur sem á **ekki** að sitja einn uppi með ábyrgðina.
- Vanræksla er ekki lengur ósýnileg.

Vandinn er eftirlit, ekki traust

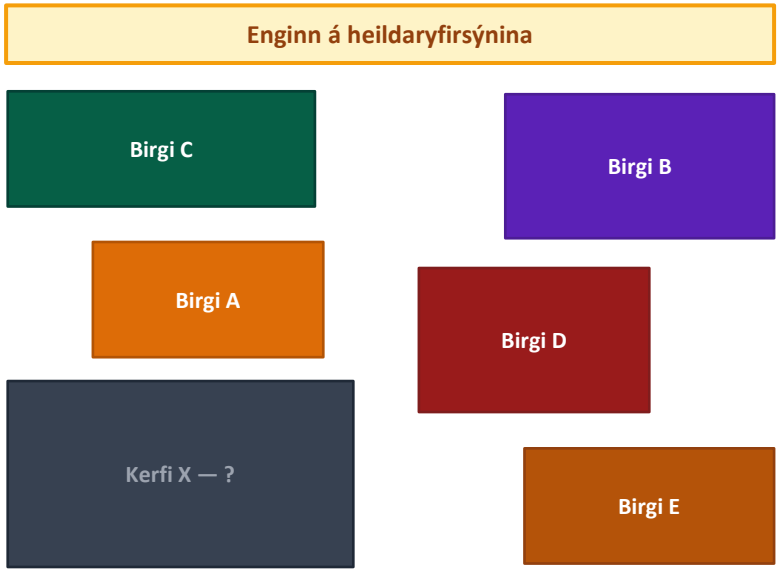
- Ef allar upplýsingar koma í gegnum öryggisstjórann — er þetta eintal, ekki samvinna.
- **Ég þekki þetta vel.**

Þegar þið talið við stjórnendur, eða þegar stjórnendur tala við ykkur, er það **samtal** eða **eintal**?

Bútasaumur er ekki arkitektúr — Hver er við stýrið?

Þegar birgjum er ekki stýrt markvisst — þá verður útfærslan á þeirra forsendum, ekki á þínum.

BÚTASAUMUR



TÖKUM STJÓRNINA

1 Skortur á arkitektúr – er ávísun á glundroða
Ef birgjarnir þínir eiga arkitektúrinn — þá ert þú leigutaki í eigin húsi með “langan” óuppsegjanlegan leigusamning.

2 Skýrar kröfur og rammi áður en birgjar hefja vinnu
Verktakar leysa verkefnin sem þeir fá. Ef þú setur ekki reglurnar — þá útfæra þeir verkefnið á sinn hátt, ekki þinn.

3 Markviss birgjastjórnun
Þeir geta þjónustað — en þú verður að eiga hönnunina og vera byggingarstjórinn.

“Treystir þú birgjunum til þess að byggja hús fyrir þig án teikninga og án byggingastjóra?”

Framkvæmdin — við vitum hvað þarf að gera. Af hverju gerum við það ekki?

> *Security maturity is not measured by what exists in policy documents.*
> *It is measured by what is enforced in production.*
>
> - Microsoft

01

Stolin auðkenni virka

- Vegna þess að MFA er ekki virkt alls staðar.
- Eitt stolið lykilorð er nóg til að komast inn.

02

Gömul kerfi eru virk og ópötsuð

- Vegna þess að uppfærslum er frestað.
- Árásarmaður þarf ekki að leita að gati — gatið er þekkt.

03

Réttindi of víðtæk

- Vegna þess að enginn þekkir aðganginn, er hann ekki fjarlægður.
- Gullnáma fyrir árásaraðila .

Þetta eru ekki ný vandamál. Vandinn er ekki greiningin — vandinn er framkvæmdin.

Hvernig brúum við bilið — í reynd

1

Þýðum áhættuna

Ekki CVE-stig. Ekki tæknilegar skýringar. Niðritími, tekjutap, orðspor og lagalegar skyldur.

2

Gefum stjórnendum val — ekki vandamál

Þrjár leiðir: Gera ekkert og afleiðing þess / Lágmarksúrbætur / Leysa málið að fullu. Ákvörðunin er þeirra.

3

Skráum ákvarðanirnar — hverjar sem þær eru

Tryggum að áhættan hafi eiganda. NIS2 og DORA gera þetta að lögbundinni kröfu.

4

Mælum það sem skiptir máli

Greiningartími, viðbragðstími, hraði á lokun öryggigata ofl. Ef við mælum ekki — stjórnum við ekki.

origo.

Viðnámsþróttur byrjar ekki á tækni.

Hann byrjar á sameiginlegum skilningi.

Viðnámsþróttur er langhlaup, en ekki spretthlaup.

Öryggisskuld er leiðtogavandi — ekki tæknilegur vandi.

Þýddu áhættu yfir í afleiðingar. Bjóddu upp á val — ekki vandamál.

Skráðu ákvarðanirnar — tryggðu að áhættan eigi skýran eiganda. NIS2 og DORA gera það að lögbundinni kröfu.

Mældu það sem skiptir máli og birtu niðurstöðurnar reglulega — þá er staðan ljós.

Til umhugsunar: *Ef þú opnar öryggisstjórnkerfið þitt i dag - hversu stórt er bilið á milli þess sem er sagt og þess sem er gert?*

Sigfinnur Valur Viggósson · CISO, Origo sigfinnur.valur.viggosson@origo.is