ÖRUGG BIRGJAKEÐJA

Er það mögulegt?

Bjarni Hallgrímur Bjarnason,
sérfræðingur í upplýsingaöryggi.

Fjarskiptastofa

Birgjakeðjan – hvað meinum við með því?

Öryggi birgjakeðjunnar snýst um að tryggja öryggi alls ferlisins sem vörur, þjónusta og upplýsingar fara í gegnum, frá uppruna þeirra til lokaafurðar.

Nær yfir allt framleiðsluferlið:

- frá framleiðslu íhluta
- við forritun hugbúnaðar
- þjónustu

Áhætta getur komið fram á öllum stigum ferlisins.

Fjarskiptastofa

Áttar þú þig á því hvar þú stendur í birgjakeðjunni?

1. Er ég framleiðandi, birgir, samþættari eða endanlegur notandi?

2. Hvaða þjónustu eða vöru veiti ég, og hversu mikilvæg eru þau fyrir aðra aðila í birgjakeðjunni?

Fjarskiptastofa

Lykilspurningar sem þú þarft að hafa svörin við!

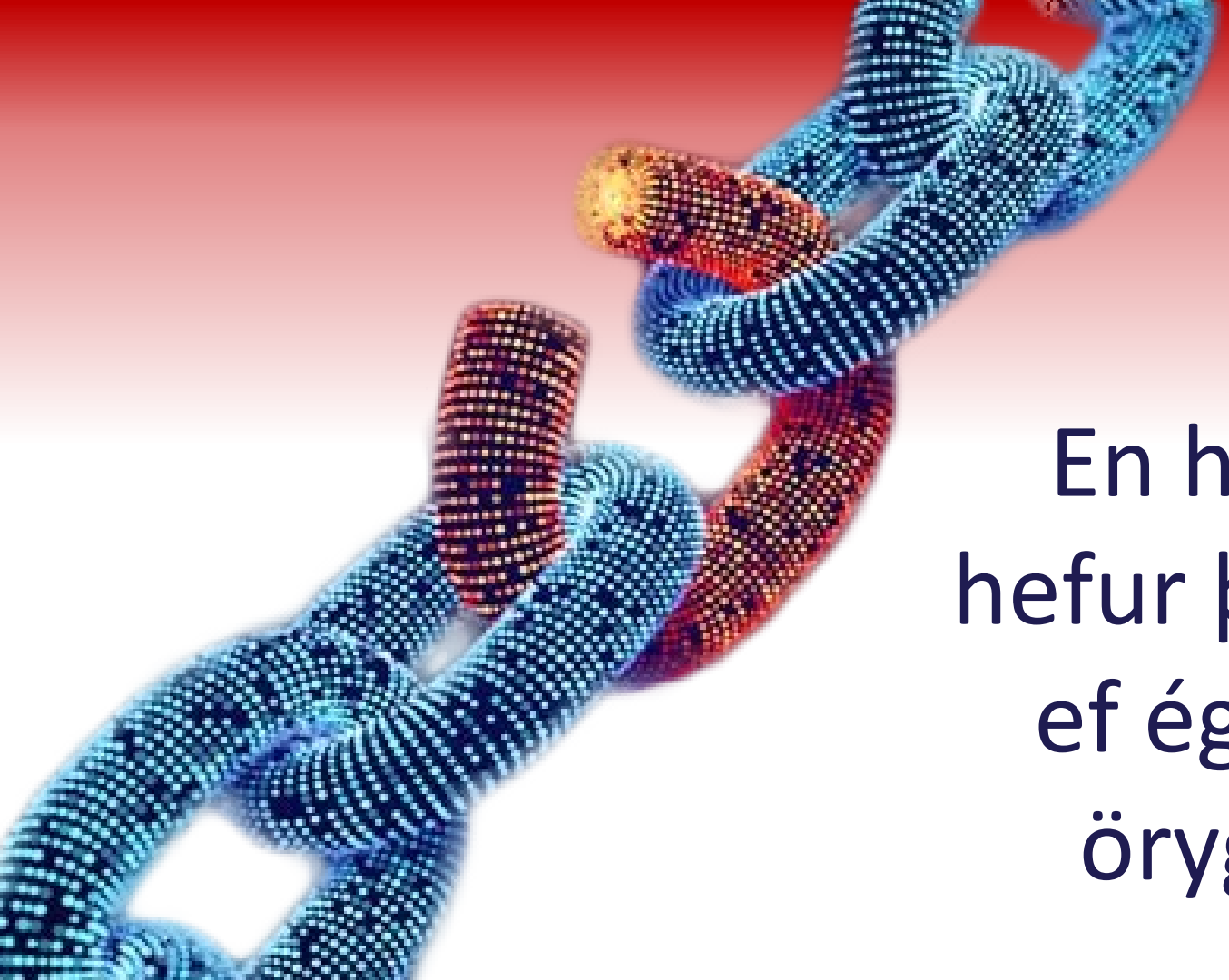
Hversu útsettur er ég fyrir net- og upplýsingaöryggisáhættu í gegnum birgjakeðjuna?

Hvert er uppstreymi vara og þjónustu (mínir birgjar)?

Hvert er niðurstreymi vara og þjónustu (mínir viðskiptavinir)?

Hversu háður er ég þriðju aðilum fyrir nauðsynlega þjónustu eða vöru?

Fjarskiptastofa



Fjarskiptastofa

En hvaða áhrif hefur það á aðra ef ég verð fyrir öryggisatviki?

Innlent | mbl | 2.10.2024 | 13:19 | Uppfært 13:49

Rafmagnsleysið nær yfir Norðurland og Austfirði

Samkvæmt upplýsingum frá Rarik nær rafmagnsleysið yfir stóran hluta landsins. *Kort/Rorik*

Sló út við reglubundið viðhald

Oddur Ævar Gunnarsson skrifar 2. október 2024 14:05

svæðinu varð við reglubundið viðhald hjá
ð til þess að rafmagnstruflanir urðu á hálfu
ust í verksmiðjunni.

Innlent | mbl | 2.10.2024 | 16:44 | Uppfært 17:59

Varaaflsstöð ræst til að vernda bankainnviði

Gagnaverið í Korputorgi „pikkaði upp" rafmagnsleysið að sögn Borealis en þar er haldið utan um „mikilvæga samfélagslega innviði". *mbl.is/Hori*

mbl.is

Agnar Már Másson
agnarmar@mbl.is

Setja bókamerki

Varaflsstöð gagnavers í Korputorgi, þar sem er m.a. haldið utan um gögn frá Reiknistofu bankanna, fór í gang eftir að gagnaverið nam rafmagnsleysi í gagnaveri á Blönduósi.

Rafmagnslaust varð á hálfu landinu í dag, nánar tiltekið á Austurlandi og Norðurlandi, eftir að rafmagn sló út hjá Norðuráli á Grundartanga og olli truflunum í flutningakerfum Landsnets og RARIK.

Borealis Data Center sem rekur þrjú gagnaver á landinu m.a. eitt á Blönduósi fann fyrir áhrifum rafmagnsleysisins og þurfti að reiða sig á varafl til að halda þjónustu gangandi.

Fjarskiptastofa

Innlent | mbl | 19.7.2024 | 8:24 | Uppfært 21:28

Kerfisbilun hjá Microsoft: Flugvélar kyrrsettar

Orsökin er enn

20%

CrowdStrike IT outage affected 8.5 million Windows devices, Microsoft

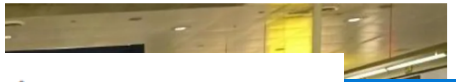
Ástæða kerfisbilunar fundin og unnið að lausn

Share Save

- Kerfisbilun er hjá Microsoft vegna hugbúnaðaruppfærslu á vegum fyrirtækisins CrowdStrike, sem hefur áhrif um allan heim.
- Flugvélar hafa verið kyrrsettar og lokað fyrir umferð um suma flugvelli.
- Röskun er á bókasafnskerfum á Íslandi.
- CrowdStrike segist hafa einangrað bilunina og vinnur að lausn.
- Talið er að virði CrowdStrike hafi lækkað um 16 milljarða dollara vegna atviksins.

Fréttastofa RÚV
19. júlí 2024 kl. 07:56, uppfært kl. 17:21

A A A



gi

ræða, heldur kerfisbilun og að hennar.

íslensku samfélagi og kerfinu u klukkutímana og bregðast við

Global IT Crowdstri… outage could take time to fix

19 July 2024

Fjarskiptastofa

:(

Your PC r
just collec
you.

20% comp

For

If you call a support person, give them this info:

Stop code: CRITICAL_PROCESS_DIED

Fyrirhyggja er besta vörnin - vegna CrowdStrike atviksins 19. júlí 2024

Arnar Freyr Guðmundsson skrifar 22. júlí 2024 11:31

Bandaríska netöryggisfyrirtækið CrowdStrike var stofnað árið 2011 af núverandi forstjóra þess George Kurtz. Fyrirtækið veitir margvíslega og víðtæka þjónustu á sviði netöryggis og er með tæplega 30 þúsund viðskiptavini á heimsvísu. Yfir 82% af stofnunum hinna 50 bandarískra fylkja eru viðskiptavinir netöryggisfyrirtækisins. Um klukkan fjögur aðfararnótt síðastliðins föstudags, 19. júlí, sendi CrowdStrike frá sér uppfærslu á veiruvörn sína, Falcon Sensor.

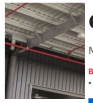
Fjarskiptastofa

Credit: nikapress / Shutterstock

In March 2017, personally identifying data of hundreds of millions of people was stolen from Equifax, one of the credit reporting agencies that assess the financial health of nearly everyone in the United States.

NotPetya cyber-attack cost TNT at least $300m

20 September 2017



Russian military to blame for NotPet cyber attack, says UK Foreign Office

Ministers say Moscow 'almost certainly' behind attack that crippled computers in 65 countries

Benjamin Kentish Political Correspondent • Thursday 15 February 2018 11:11 GMT

0 Comments

Boeing to spend $4B plus to fix safety, supply chain woes: CFO

The aerospace company is pushing to lower instances of components being completed outside a production line's typical flow.

Published March 20, 2024

Boeing Is The Biggest Problem For The Supply Chain, Survey Finds

Michael Bruno July 22, 2024

Dráttur á notkun MAX-véla Icelandair helsta ástæða meiri svartsýni en áður

Tryggvi Páll Tryggvason skrifar 28. ágúst 2019 12:15

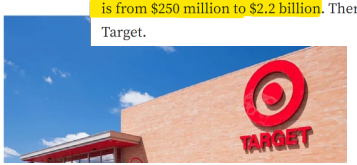
Target Data Breach

Rithik V Gopal · Follow

Published

134 1

to Target systems for over a month before the breach was detected. Independent sources around the world have made a rough estimation that the cost of fraudulent charges resulting from the stolen credit card numbers is from $250 million to $2.2 billion. There are over 80 lawsuits filed against Target.



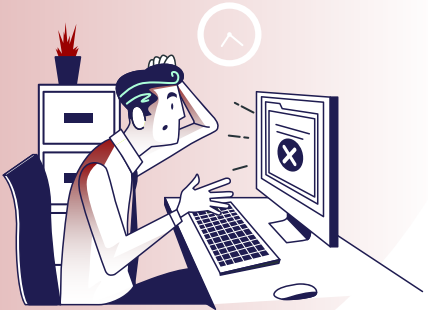
Tæplega þrjú þúsund slasaðir eftir að símboðar sprungu

Atli Ísleifsson og Samúel Karl Ólason skrifa 17. september 2024 14:38

Fjarskiptastofa

Fjarskiptastofa

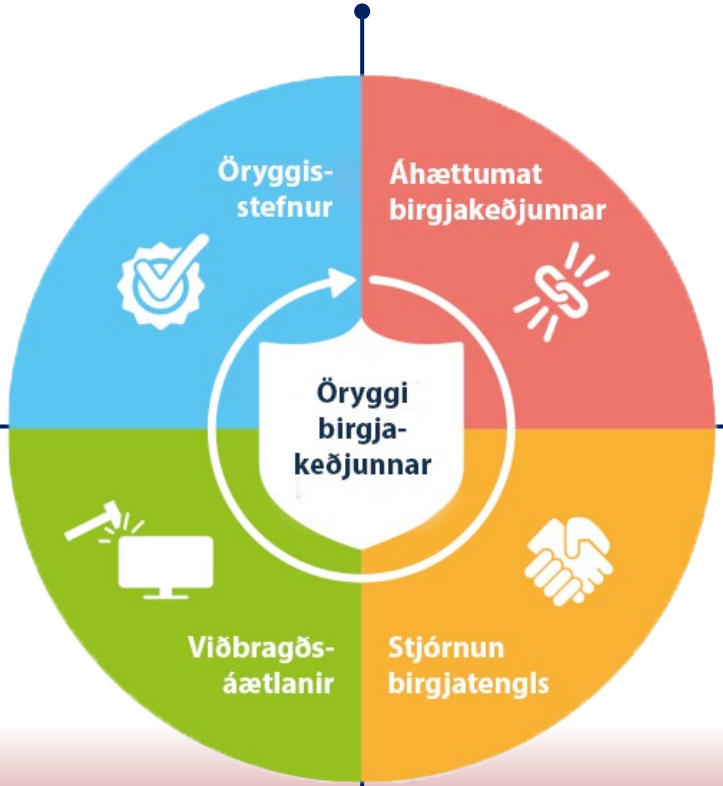
Örugg birgjakeðja?
Öruggari birgjakeðja?



Kröfur, leiðbeiningar, staðlar...

- Netöryggislög og samhliða reglugerðir (NIS1, NIS2)
- ISO 27000, 28000, 31000 staðlaraðir
- NIST cybersecurity framework
- Good Practices for Supply Chain Cybersecurity frá ENISA

Hvað eiga þessar öryggisráðstafanir sameiginlegt?



Öryggisstefna birgjakeðjunnar

- Skuldbinding um að stýra birgjakeðjunni og fylgja uppfylla kröfur laga og staðla um bestu framkvæmd og kröfur hagsmunaaðila
- Virkt áhættumat og viðvarandi eftirlit, þ.e.a.s. greina og meta öryggisáhættu reglulega
- Velja birgja byggt á öryggiskröfum og viðhafa eftirlit með birgjum
- Innleiða sterkar öryggisráðstafanir, svo sem öruggar þróunaraðferðir, breytingarstjórnun, dulritun og aðgangsstýringar
- Stefna samþykkt af stjórnendum og innleidd á öllum stigum
- Stefnan endurskoðuð reglulega, þegar verulegar breytingar verða á rekstri og í kjölfar alvarlegra atvika

Fjarskiptastofa

Áhættumat

- Áhættumeta kerfisbundið alla birgja til að skilgreina veikleika og hugsanlega öryggisógnir
- Framkvæma skal áhættumatið reglulega til að halda utan um nýjar ógnir eða breytingar í birgjakeðjunni
- Flokka birgja eftir áhættu, þar sem mikilvægir birgjar fá nánari athugun og eftirlit
- Búa til viðbragðsáætlanir í samræmi við niðurstöður áhættumats til að draga úr áhrifum mögulegra öryggisatvika
- Fara eftir bestu venjum varðandi áhættumat, svo sem ISO27005 og 31000

Fjarskiptastofa

Val á birgja

- Val á birgja skal fyrst og fremst taka mið af kröfum fyrirtækisins
- Áður en til samnings kemur skal framkvæma áreiðanleikakönnun, m.t.t þarfa fyrirtækisins
- Meta skal birgja eftir því hvort þeir uppfylli viðeigandi öryggisstaðla og bestu venjur
- Tryggja að hjá birgjanum sé gagnsæ stjórnun
- Áhættumeta þær áhættur sem gæti fylgt birgjanum

Er samningur til staðar?

- Skriflegur samningur skal skilgreina skyldur, hlutverk og ábyrgð aðila, m.a. varðandi net- og upplýsingaöryggi.
- Samningurinn skal skilgreina viðbrögð við öryggisatvikum
- Setja fram í samningi að birginn skuli starfa í samræmi við gildandi lög hvers tíma, sem og þær kröfur sem félagið setur þeim (t.d. dulritun og aðgangsstýringu)
- Tryggja að birginn taki ábyrgð ef til þess kemur, t.d. vegna atviks, og þá skilgreina hugsanlegar bætur vegna þess
- Samningurinn skal innihalda ákvæði um eftirlit

Viðbragðsáætlun

- Til staðar skulu vera skjalfestar viðbragðsáætlanir sem tilgreinir skýrlega hlutverk birgja ef upp koma atvik
- Tryggja skal að birgjar séu upplýstir um þeirra hlutverk í meðhöndlun atvika
- Áætlunin skal skýrlega tilgreina tengiliði, aðaltengiliði sem og varatengiliði og boðleiðir. Tryggja skal að hægt sé að miðla upplýsingum hratt og örugglega ef þörf krefur
- Viðbragðsáætlun skal einnig tilgreina eftirfylgni atviks, t.d. með ítarlegri greiningu á atviki, orsök og viðbragð. Niðurstöður skulu skjalfestar í atvikaskýrslu og draga skal lærdóm til að bæta öryggisferla og framtíðarviðbrögð skv. niðurstöðum.
- Uppfylla kröfur netöryggislaga um um upplýsingagjöf og tilkynningaskyldu

Fjarskiptastofa

Og auðvitað eru fleiri atriði…

- Til staðar skal vera skrá yfir alla þá birgja sem vörur og þjónusta hjá fyrirtækinu er háð.
- Virkt eftirlit með birgjum
- Innri úttektir á stjórnkerfi net- og upplýsingaöryggis
- Að til staðar sé fræðsla og þjálfun starfsmanna **og birgja**
- Tryggja stöðugar umbætur

Fjarskiptastofa

Lokaorð?

Ábyrgðin er ykkar!

Ekki horfa blint á vottanir hjá birgjum!

Það er ykkar að áhættumerta ykkar birgja,
og vera með ykkar birgjakeðju á hreinu!

Stuðla að stöðugum umbótum, alltaf!

Árangursmælingar.

Fjarskiptastofa

Takk fyrir

bjarnihallgrimur@fjarskiptastofa.is

Fjarskiptastofa

Gagnlegt efni til skoðunar?

7. gr. netöryggislaga nr. 78/2019

13. gr., 15. gr. og 16. gr. reglugerðar nr. 866/2020

NIS 2 (DIRECTIVE (EU) 2022/2555)

A.5.19, A.5.20, A.5.21, A.5.22 og A.8.30 í ÍST EN ISO/IEC 27001:2023

Good Practices for Supply Chain Cybersecurity frá ENISA

GV.SC, GV.OC-02, GV.OC-05, GV.RM-05, ID.RA-10, ID.IM-02 í NIST CSF 2.0

ISO28000 staðlaröðin