Netárás á Brimborg

Maður tryggir ekki netöryggi eftir á!

Örstutt um Brimborg

Meginstarfsemi

Umfang 2022:
Heildarvelta:
29,9 ma.
Stöðugildi: 248

dollar.

Thrifty CAR RENTAL

MAX1 BÍLAVAKTIN

Netglæpir
eru vaxandi vandamál

Hvers vegna upplýsir Brimborg um netárásina?

Allt sem við gerum skal endurspeglast í loforði Brimborgar um að vera öruggur staður til að vera á.

Því trúum við að það sé samfélagsleg skylda okkar að upplýsa ef það má verða til þess að forða öðrum fyrirtækjum og einstaklingum frá netárás og þannig lagt okkar af mörkum til að gera samfélagið öruggara.

brimborg

Öruggur staður til að vera á

Viðbragð við netárás

Fyrsta viðbragð

- Aðfararnótt 29. ágúst
  - Netárás sem leiddi til gagnagíslatöku
  - Origo neyðarnúmer virkjað
  - Framkvæmdastjórar níu viðskipta- og rekstrarsviða upplýstir
    - Allir starfsmenn sviða upplýstir
    - Slökkt á öllum útstöðvum

Fjárkúgunarbréf

Skjáskot úr fjárkúgunarbréfi frá líklega rússneskum hóp sem kallar sig Akira. Engar upphæði nefndar. Fylgdu eftir fjárkúgun eftir 7 daga með tölvupósti.

Hi friends,

We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us.

Install TOR Browser to get access to our chat room

Keep in mind that the faster you will get in touch, the less damage we cause.

If you're indeed interested in our assistance and the services we provide you can reach out to us following simple instructions:

Skref 2

- Þriðjudagsmorgun 29. ágúst
  - Origo teymi virkjað vegna netkerfis, þjóna, gagnagrunna, símkerfis og ýmissa hugbúnaðarlausna
    - 09:00 Meginákvörðun
      - Allir sérfræðingar Origo í viðbragð 24/7
      - Strauja þjóna, gagnagrunna og útstöðvar
      - Byggja allt upp aftur frá grunni
      - Lesa inn afrit
      - Ekki hafa samband við fjárkúgunarhóp og ekki borga

Skref 3

- Syndis teymi virkjað vegna rannsóknar á netárás, hvenær og hvernig ráðist var inn, hvernig árásaraðili athafnaði sig í kerfi og hvort gögn hafi verið tekin og ráðgjöf
  - Niðurstaðan: Komist yfir lykilorð og farið inn um VPN tengingu
    - Við vitum hver notandinn er og ræddum við hann
    - Ekki vitað hvort lykilorðið náðist í gegnum tölvupóst, vefsíðu eða í gegnum veikleika í eldvegg svo dæmi séu tekin
    - En að öðru leiti náði Syndis að rekja alla atburðarásina

Skref 4

- Annata teymi virkjað vegna uppsetningar á Dynamics AX upplýsingatæknikerfi

- Tækniher Brimborgar stofnaður sem samanstóð af ýmsum starfsmönnum Brimborgar

- Teams rás stofnuð – 43 á rásinni þegar mest var
  - + 20 manna tækniher

Mat á þjónustustigi án virkra kerfa

- Dæmi
  - Engin aðgangur að varahlutakerfum birgja
  - Enginn aðgangur að varahlutum eða dekkjum í vöruhúsi
  - Enginn aðgangur að nýjum eða notuðum bílum á lager
  - Símkerfi niðri
    - Beintengdum símanúmer samdægurs við GSM neyðarþjónustusíma
  - Margvísleg kerfi önnur niðri

Viðbragð gagnvart viðskiptavinum

- Ákvörðun
  - Upplýsa opið um stöðuna
  - Gera allt sem hægt væri til að tryggja þjónustu
    - Handskrifa vöru- og þjónustuúttektir
  - Fresta þjónustu sem mögulegt væri að fresta
  - Viðskiptavinir tóku hnökrum á þjónustu afar vel

Opinberar tilkynningar

Tilkynning send til Persónuverndar og CERT-IS samdægurs

Gátt vegna tilkynningar um öryggisbrest

Tilkynninguna ber að senda til Persónuverndar án ótilhlýðilegrar tafar og, ef mögulegt er, eigi síðar en 72 klst. eftir að ábyrgðaraðili varð brestsins var.

Tilkynningar á vef Brimborgar

29.08.2023

Netárás á kerfi Brimborgar

Aðfararnótt 29. ágúst var gerð netárás á hluta upplýsingakerfa Brimborgar og gögn tekin í gíslingu. Um leið og starfsmenn Brimborgar urðu þessa varir voru helstu sérfræðingar landsins fengnir að borðinu til að...
Lesa meira

04.09.2023

Uppfært: Starfsemi í eðlilegt horf eftir netárás, rannsókn sérfræðinga í gangi

Í kjölfar netárásar á tölvukerfi Brimborgar þar sem hluti gagna var læstur hefur Brimborg gripið til ýmissa ráðstafanna til að loka á aðgang árásaraaðila til dæmis með lokun á aðgöngum, endurræsingu lykilorða og fleir...
Lesa meira

Ýmsar aðrar tilkynningar

- Til starfsmanna
- Til birgja
- Til fjármálastofnana
- Til annarra þjónustuaðila eins og rekstraraðila annarra hugbúnaðarkerfa

- Daglegar stöðuuppfærslur til starfsmanna
- Reglulegar stöðuuppfærslur til ýmissa birgja
- Reglulegar stöðuuppfærslur til CERT-IS
  - Heimild til Origo og Syndis að upplýsa CERT-IS strax um allt sem viðkom árásinni eftir framgangi rannsóknar

Persónuverndar fyrirspurnir

Þrjár persónuverndarfyrirspurnir komu frá viðskiptavinum

- Svarað samdægurs þó með fyrirvara um að þá var ekki komin endanleg niðurstaða um mögulegan gagnastuld. Síðar var staðfest að ekki var um gagnastuld að ræða.

Umfjöllun fjölmiðla

29.8: Fyrsta tilkynning Brimborgar
29.8: Fyrsta frétt RÚV
29.8: Fyrsta frétt mbl.is
30.8: Viðtal í Síðdegisútvarpi RÚV
31.8: Fyrsta frétt á visir.is
31.8: Önnur frétt á visir.is
1.9: Eftirfylgnifrétt á mbl.is
4.9: Önnur tilkynning Brimborgar
4.9: Frétt RÚV með viðtali við CERT-IS

Fyrsta tilkynning Brimborgar 29.8.2023: https://www.brimborg.is/is/frettir/netaras-a-kerfi-brimborgar
Frétt RUV 29.8.2023: https://www.ruv.is/frettir/innlent/2023-08-29-alvarleg-netaras-gerd-a-brimborg-og-gogn-tekin-i-gislingu-390632
Frétt mbl.is 29.8.2023: https://www.mbl.is/frettir/innlent/2023/08/29/netaras_a_brimborg_og_gogn_tekin_i_gislingu/
Frétt visir.is: 31.8.2023: https://www.visir.is/g/20232456827d/rannsaka-enn-hvort-thrjotar-hafi-komist-yfir-gogn-brimborgar
Frétt visir.is 31.8.2023: https://www.visir.is/g/20232456951d/brimborg-lati-vidskiptavini-og-starfsmenn-vita-af-oryggisbresti
Frétt mbl.is 1.9.2023: https://www.mbl.is/frettir/innlent/2023/09/01/netkerfi_brimborgar_ad_komast_a_rol/
Önnur tilkynning Brimborgar 4.9.2023: https://www.brimborg.is/is/frettir/uppfaert-starfsemi-i-edlilegt-horf-eftir-netaras-rannsokn-serfraedinga-i-gangi
Frétt RUV 4.9.2023: https://nyr.ruv.is/frettir/innlent/2023-09-04-brimborg-brast-rett-vid-i-kjolfar-alvarlegrar-netarasar-390968

Staðan 48 tímum eftir netárás

- Fimmtudagsmorgun 31. ágúst
  - Flestir mikilvægustu þjónar komnir upp
  - Flestir mikilvægustu gagnagrunnar komnir upp
  - Dynamics AX kerfið komið í gang
  - Um 190 útstöðvar straujaðar, uppsettar aftur og komnar í virkni
  - Nýtt símkerfi farið að virka að hluta

  - Starfsemin var því komin í gang

Mat á áhrifum netárásar á veltu

Veltuvöxtur ársins 2022 vs 2021: 31,0%

Veltuvöxtur jan-júlí 2023 vs 2022: 26,1%

Starfsemin að mestu komin í gang 48 tímum eftir árás og að fullu fyrir lok september.

Veltuvöxtur ágúst og sept 2023 vs 2022: 55,1%

Stærstu ágúst og september mánuðir sögunnar

Snöggt viðbragð starfsmanna og sérfræðinga frá Origo, Syndis og Annata gerði það að verkum að áhrif á rekstur voru í lágmarki hvað veltu varðar.

Kostnaður

Það mætti skipta kostnaðinum upp í þrennt

- Kostnaður sem hefði að hluta átt að hafa fallið til áður
- Kostnaður sem hefði fallið til kannski á næstu árum til að tryggja framúrskarandi netöryggi
- Beinn viðbótarkostnaður vegna netárásar

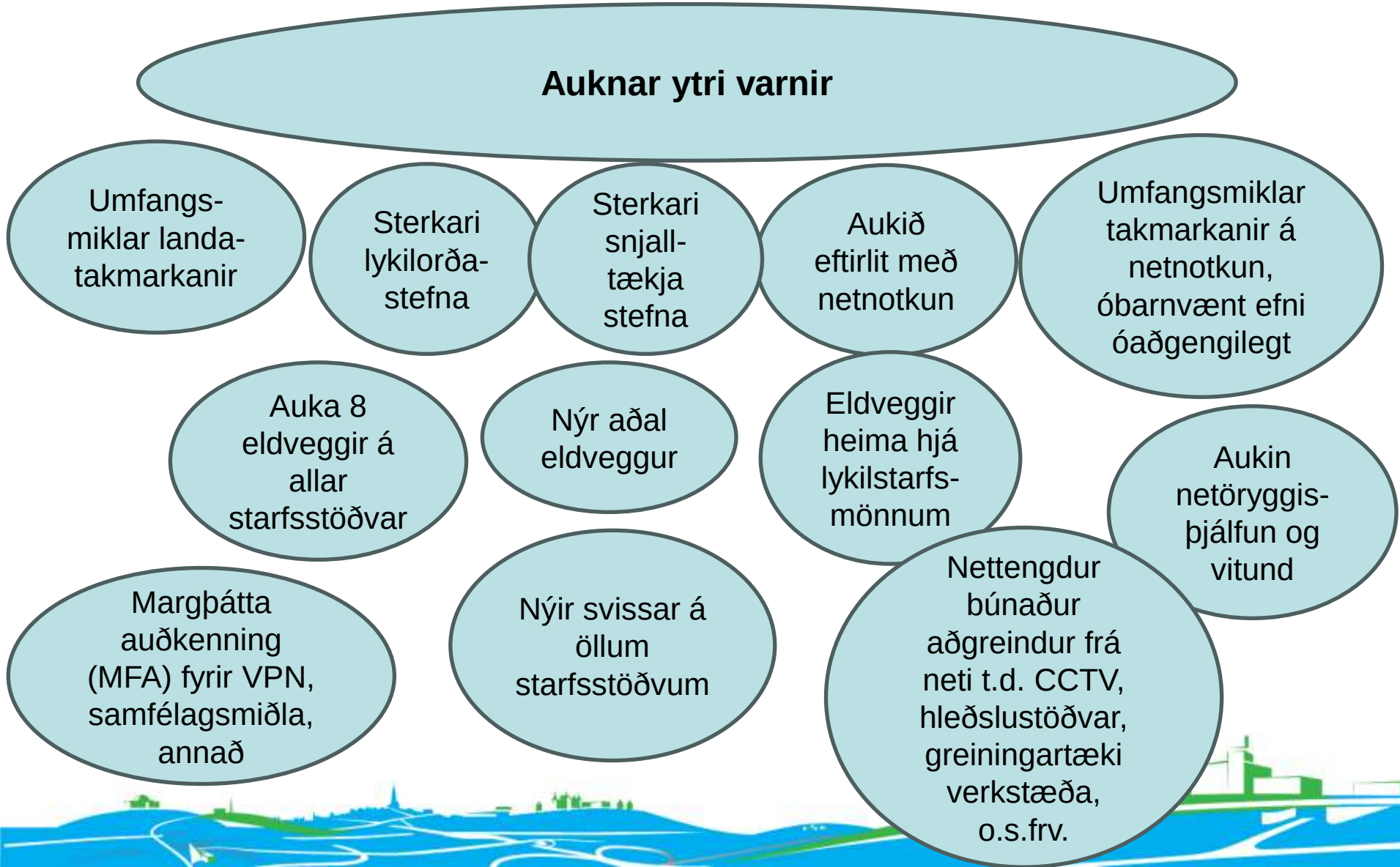
100 daga áætlun

Umbreyting gekk framúrskarandi vel

Markmið:
Brimborg verði í hópi þeirra bestu í upplýsingatækniöryggi

100 daga áætlun
- **Lauk 7. desember 2023**
- **Jafnvel meira framkvæmt en upphafleg áætlun gerði ráð fyrir**

Ytri varnir


Auknar ytri varnir
Umfangs-miklar landa-takmarkanir
Sterkari lykilorða-stefna
Sterkari snjall-tækja stefna
Aukið eftirlit með netnotkun
Umfangsmiklar takmarkanir á netnotkun, óbarnvænt efni óaðgengilegt
Auka 8 eldveggir á allar starfsstöðvar
Nýr aðal eldveggur
Eldveggir heima hjá lykilstarfs-mönnum
Aukin netöryggis-þjálfun og vitund
Margþátta auðkenning (MFA) fyrir VPN, samfélagsmiðla, annað
Nýir svissar á öllum starfsstöðvum
Nettengdur búnaður aðgreindur frá neti t.d. CCTV, hleðslustöðvar, greiningartæki verkstæða, o.s.frv.

Innri varnir

Auknar innri varnir
Zero Trust Network

Net aðgangs-takmarkanir milli starfsstöðva og innan

Net beint út frá starfsstöðvum, aðeins nauðsynleg þjónusta sótt á innra netið

Gestanet beint á netið á lokuðu hotspot, sama netöryggistefna á gestaneti

Efldar tölvupósts- og vírusvarnir

Skilgreining á hlutverki upplýsinga-öryggisstjóra

Notendur fá aðeins aðgang að skilgreindri þjónustu frá skilgreindum vélum

Takmarkanir á notkun útstöðva

Takmarkanir á samskiptum milli útstöðva og þjóna

24/7 vöktunar-samningur við Syndis auk útstöðvavöktunar

Auka ávinningur

Heildarvirkni kerfa bætt

Bættur hraði og virkni upplýsinga-tæknikerfis

Ljósleiðaralagnir tvöfaldaðar

Ljósleiðara-gagnamagn fimmfaldað út og tífaldað fyrir notendur

Tvöfalt öryggi innleitt víða

Nýtt símkerfi innleitt

Hvíld

Des ´23 – jan ´24
100 daga áætlun kallaði á mjög mikla vinnu og gríðarlegan fókus
Hvíld nauðsynleg en komin vissa um gott öryggi

Natni við smáatriði, rýni, prófanir, æfingar

Feb ´24 – maí ´24
Þráðurinn tekinn upp

Reglulegar innbrots-prófanir, veiðipósta-æfingar, o.s.frv.

Veikleikagreiningar
AD
Azure
Aftra
fleira

Rýni á stillingum öryggis-búnaðar

Upplýsinga-öryggisstefna

Styrkja enn frekar afritatöku

Aukin öryggis-meðvitund starfsmanna

Vottun

DDOS árás föstudaginn 17. maí frá kl. 11 til 19 í miðri eldveggja uppfærslu.
Gott álagspróf sem við stóðumst vel

Viðhorf og metnaður til netöryggis

Maður tryggir ekki netöryggi eftir á!

Viðhorf og metnaður

Eigenda

Stjórnenda

Starfsmanna

Ytri tæknimanna og ráðgjafa

Veikleikagreining dæmi
AD
72/100
32/100
16/100
2/100

Samfélagsins

Takk fyrir