Hvernig forgangsröðum við fjármagni í netöryggislausnir og hvenær gerum við nóg

Linda Kristmannsdóttir

Maí 2024

FESTI

Áskoranir

- Velja réttu lausninar
  - Hverjar eru „réttu“ lausnirnar
  - Fá ráðgjöf frá öryggissérfræðingum
  - Forgangsraða innleiðingu á lausnum eftir vægi öryggis
- Forgangsraða fjármagni í öryggislausnir
  - Upplýsingagjöf til stjórnenda
  - Gera áætlun um innleiðingu lausna
  - Upplýsingaöryggi er ekki valkvætt það er grunnkrafa
- Fræða starfsmenn
  - Stöðug áminning um netöryggismál til að auka öryggisvitund
  - Mælingar á árangri af fræðslu
- Búa til viðbragðsáætlun
  - Skilgreina rekstrarsamfelluáætlun
  - Æfa viðbragð

FESTI

Hvatar fyrir stjórnendur

- Opin umræða um netárásir
  - Margföld aukning í netárásum síðastliðin ár
    - 1.266 atvik tilkynnt árið 2023 á móti 700 atvikum árið 2022
  - Stjórnendur meira tilbúnir til að segja frá árásum
    - Mikilvægt að opna umræðuna og segja frá, þannig lærum við öll
- Löggjöf
  - Innleiðing á GDPR
    - Sektarákvæði fyrir gagnaleka persónugagna
  - Innleiðing á NIS2
    - Fleiri fyrirtæki falla undir skilgreininguna
    - Áhersla á áætlun um samfelldan rekstur
    - Krafa um aukið netöryggi og tilkynningarskyldu
    - Aukin ábyrgð æðstu stjórnenda

FESTI

NIS - Vital suppliers

- Healthcare
- Transport
- Energy
- Digital service providers
- Banks and financial market infrastructure
- Digital infrastructure
- Water supplies

NIS2 - Added industries

- Food
- Providers of public electronic communications networks or services
- Space
- Waste water and waste management
- Public administration
- Digital services such as social networking services platforms and data centre services
- Postal and courier services
- Manufacturing of certain critical products

Öryggislausnir

- Öryggislausnir
  - Hvað á að verja og vakta
  - Hvaða lausnir á að velja
    - Mikilvægt að horfa á umhverfið í heild sinni
    - Herða upp á aðgangsstýringum og einangra gömul kerfi
  - Hvernig mælum við árangur af innleiðingu öryggislausna
    - Margar lausnir eru með mælikvarða sem segir til um öryggisskor
  - Hvenær gerum við nóg
    - Öryggismenning er vegferð og við getum aldrei verið 100% örugg

- Öryggissérfræðingar
  - Fæst fyrirtæki með sérmenntaða netöryggissérfræðinga
    - Mikill skortur á öryggissérfræðingum í heiminum
    - Nám í netöryggi í HR/HÍ
  - Nýtum okkur ytri sérfræðinga, sækjum ráðgjöf

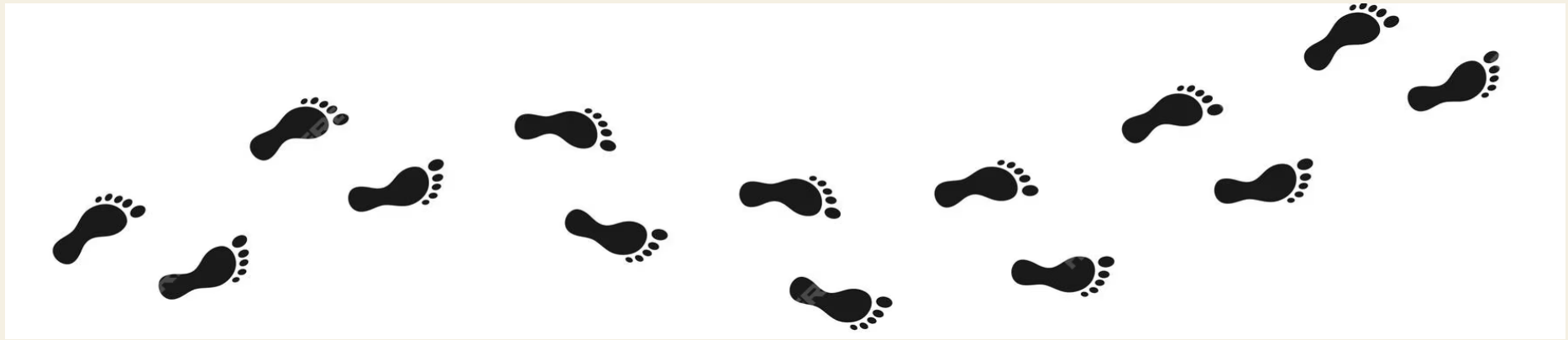
FESTI

Viðbragðsáætlun

- Skjala viðbragðsáætlun
  - Forgangsraða verkefnum
    - Skilgreina mikilvægustu kerfin
    - Tímamæla endurheimt á kerfum
    - Skilgreina lykilaðila
  - Stór hópur í hverju fyrirtæki hefur hlutverk
    - Ábyrgð á rekstrarsamfellu
    - Fjárhagsleg útgjöld við endurheimt
    - Fréttatilkynningar
    - Verndun mannauðs
    - Lagaleg skylda fyrirtækis
  - Æfa viðbragðið
    - Æfing með stjórnendum og lykilstarfsfólki
    - Gera prófanir á endurheimt reglulega
    - Viðhalda viðbragðsáætlun
    - Óvandað og óundirbúið viðbragð getur skaðað ímynd fyrirtækis

FESTI

Skrefin í átt að auknu netöryggi



FESTI

Miðlægt umhverfi

- Öryggi í miðlægu umhverfi
  - Miðlægt umhverfi í hýsingu
    - Þjónustuaðili hýsingar sér um
      - öryggispakka
      - plástrun netþjóna og útstöðva
      - afritatöku
  - Öryggislausnir
    - Innleiddum CTEM hugbúnað til að fylgjast með plástrun, öryggisstillingum og veikleikum
    - Samningur við netöryggissérfræðinga sem sjá um veikleikaskönnun
    - Gerum vefveiðiprófanir á starfsmenn
    - Innleiddum MFA og ADAudit
    - Notendur ekki „local admin“ á tölvunum sínum
    - Erum með „Privileged access management“ hugbúnað
    - Innleiddum hugbúnað fyrir „ransomware protection“
    - Marglaga aðgangar fyrir notendur með aukinn aðgang
    - Einangrun á kerfum sem ekki er unnt að plástra
    - Soc þjónusta með 24/7 vöktun

FESTI

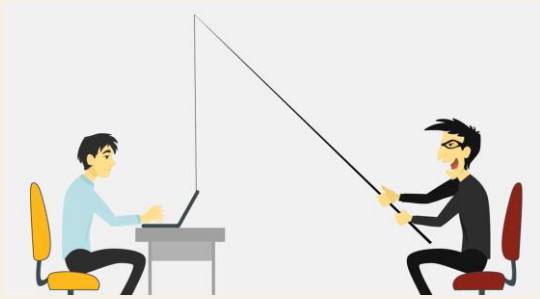
Skýjaumhverfið

- Hýsing í AWS
  - Keyrum vef- og app lausnir okkar í AWS
    - Keyrum hátt í tækistakknum og nýtum þjónustur frá AWS varðandi öryggi
    - Gerum veikleikaskan eins og fyrir miðlægt umhverfi
- Öryggi í AWS
  - Takmörkum alla snertifleti
  - Dulkóðum samskipti
  - Hægt að rekja allar breytingar á umhverfinu
  - Loggum nánast allt sem er að gerast
  - Gefum minnstu mögulegu réttindi
  - Notum „infrastructure as code“
  - Deployment í gegnum CI/CD
  - VPN á milli „onprem“ og AWS
  - Security á öllum lögum
    - Network, Load balancer, application
  - Þjónustur sem við nýtum okkur
    - WAF (web application firewall)
    - Cloudwatch til að monitore, logga og tracka breytingar.
    - SCP (Service Control Policies)
    - Cloudtrails, Guard Duty, Security Hub

FESTI

Öryggisvitund

- Þekkingarmiðlum til starfsfólks
  - Kennsluefni fyrir starfsfólk
    - Myndrænt kennsluefni
    - Alltaf aðgengilegt
  - Samþykktar vefveiðárásir þar sem við mælum árangur
    - Síðast gáfu 1,7% starfsmanna upp lykilorð, áður voru það 15,7%
  - Sterk lykilorð
    - Aðgreina vinnunetfang frá persónulegum aðgengi
    - Ekki nota sömu lykilorð í vinnu- og einkaaðgöngum
  - Stöðug áminning um netöryggismál til að auka öryggisvitund
    - Ennþá eru um 90% af öllum innbrotum í gegnum vefveiðar
    - Fjöldinn allur af lykilorðalekum í gegnum árin
- Næstu skref
  - Skrifborðsæfing með lykilfólki og stjórnendum
    - Í samstarfi við ytri öryggissérfræðinga
  - Vinna við viðbragðaáætlun og leikbækur



FESTI

Takk fyrir

“You can´t have a high level of cybersecurity if you don´t have a minimum level of cybersecurity.”

Juhan Lepassaar, Executive Director - ENISA

FESTI