UNIVERSITETERNES INFORMATIONSSIKKERHED UNDER ANGREB

AARHUS UNIVERSITET

1. NOVEMBER 2021

PETER BRUUN NIELSEN
VICEDIREKTØR

LIDT OM MIG

- Peter Bruun, Vicedirektør og it-chef på Aarhus Universitet siden 2015 – tidligere it-driftchef i Region Midtjylland
- Formand for universiteternes Informationssikkerhedsforum CISU
- Medlem af det nationale Cybersikkerhedsråd
- Omvendt – har set lyset!

TRUSSELSBILLEDET

DKCERT – TRENDRAPPORT 2021

Cyberspionage: Meget høj – Forskningsdata i de forkerte hænder

Cyberkriminalitet: Meget høj – Ransomware – manglende tilgængelighed i lang tid

Cyberaktivisme: Lav – manglende tilgængelighed i lang tid

Cyberangreb fra fremmede stater mod Infrastruktur: Lav

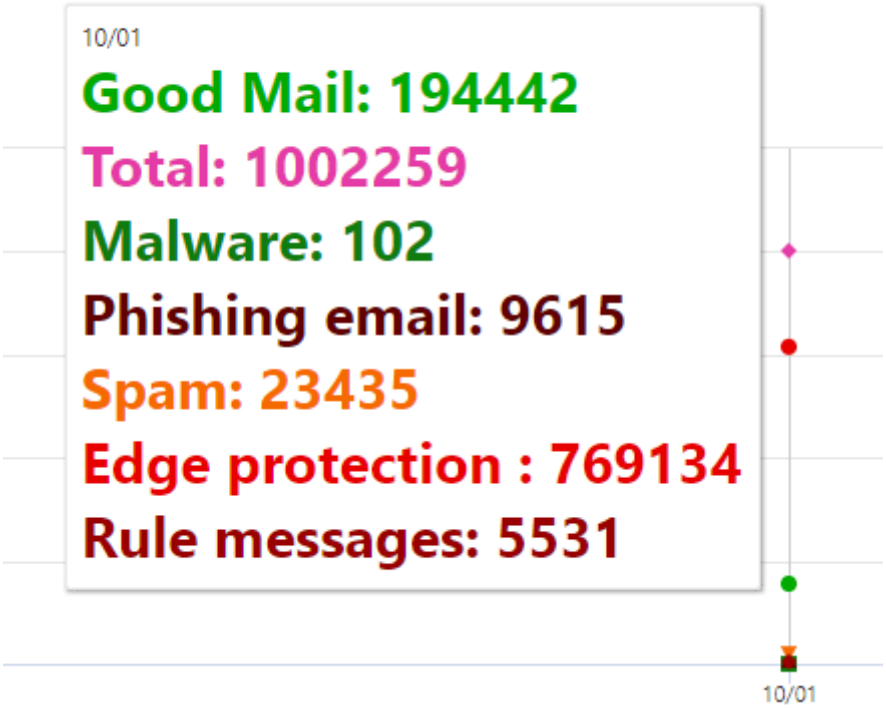
Insidertruslen: Meget høj – offer for ransomware/utilsigtet deling af fortrolige/følsomme data

HVORFOR ER VI ATTRAKTIVE?

- Forskningsområdet er blevet et nationalt sikkerhedsanliggende
- Nemme ofre ? – åbent og tillidsfuldt miljø
- Meget diverst it-miljø med mange åbne grænseflader
- Ikke tradition for hårde politikker på it-sikkerhedsområdet

HVAD ER VI UDSATTE FOR?

- Phisningangreb
- Malware
- Ransomware
- Spionage
- CEO-fraud
- Licenstyveri



HVAD GØR VI FOR AT BESKYTTE OS?

- Organisatorisk foranstaltninger
- Tekniske foranstaltninger
- Awareness

ORGANISATORISK FORANSTALTNINGER

- ISO27001med modifikationer
  - Management review – informationssikkerhedspolitik/risikobillede/tiltag
  - Modenhedsmålinger – reviews fra eksterne
  - Risikovurderinger
  - Procesmodenhed
- Formalisering af informationssikkerhedsorganisationen
  - Centralt informationssikkerhedsudvalg + decentrale udvalg (fakultet)
  - Ophæng til øverste ledelse (Bestyrelserne?)
  - Behov for præcisering af rolle- og ansvarsfordeling
  - DPO-samarbejde
- Organisering af operationel informationssikkerhed
  - SPOC på de enkelte universiteter under opbygning
  - MISP

TEKNISKE FORANSTALTNINGER

- Begrænsning af adgang til netværk: 802.1 x, VPN + microsegmentering, NAC
- Begrænsning af misbrug af adgange: To-faktor autentifikation, fjernelse af lokale admin-rettigheder, øget kontrol med priviligerede adgang
- SIEM-løsninger – logning/analyse/respons
- Microsoft Defender (Endpoints, Office365, Identity, Cloud APPs security
- Scanninger (DKCERT), Penetrationstest -> krav om opgradering/isolering
- Intrusion Detecting Systems/Intrusion Prevention Systems
- AD-hardening + sikring af backup

- Automatisering og anvendelse af kunstig intelligens i stigende grad forudsætning for at kunne løse opgaven

AWARENESS

- Phisingkampagner – fingerede phisning-angreb
- Målrettede informationskampagner
- Træning/uddannelse eks. i forbindelse med ansættelse
- Øget fokus på at uddanne/inddrage øverste ledelse
- Krav indarbejdes i projektmodeller

UDFORDRINGER FOR SEKTOREN

- Åbne miljøer, valgfrihed og skyggeit fortsat normen på universiteterne
- Meget diverst it-miljø og mange legacysystemer
- Ressourceknaphed og rekrutteringsproblemer
- Informationssikkerhed opfattes fortsat som besværligt og begrænsende af mange brugere
- Manglende erkendelse af at vi alle bliver ramt på et tidspunkt?

ANBEFALINGER

- Involvér den øverste ledelse – de skal kende risikobilledet og acceptere den valgte strategi og planer
- Forbered jer på det værst tænkelige – kan AD reetableres?/findes der en backup/beredskabsplaner inkl kommunikation/adgang til ekspertbistand + nye miljøer
- Find det rette mix af tekniske løsninger og implementer i bund
- Automatisering og anvendelse af kunstig intelligens nødvendig
- Brugerorganisationen skal hjælpes – snak så de forstår jer
- Kompetenceudvikling af interne ressourcer kan delvist løse rekrutteringsindsats – kombinér med eksterne konsulenter/leverandører i opstartsfasen
- Samarbejde mellem universiteterne skal intensiveres

Insert Quote text, for next level ENTER and TAB

- INSERT NAME

AARHUS
UNIVERSITET