Beredskabshåndtering af kritisk hændelse

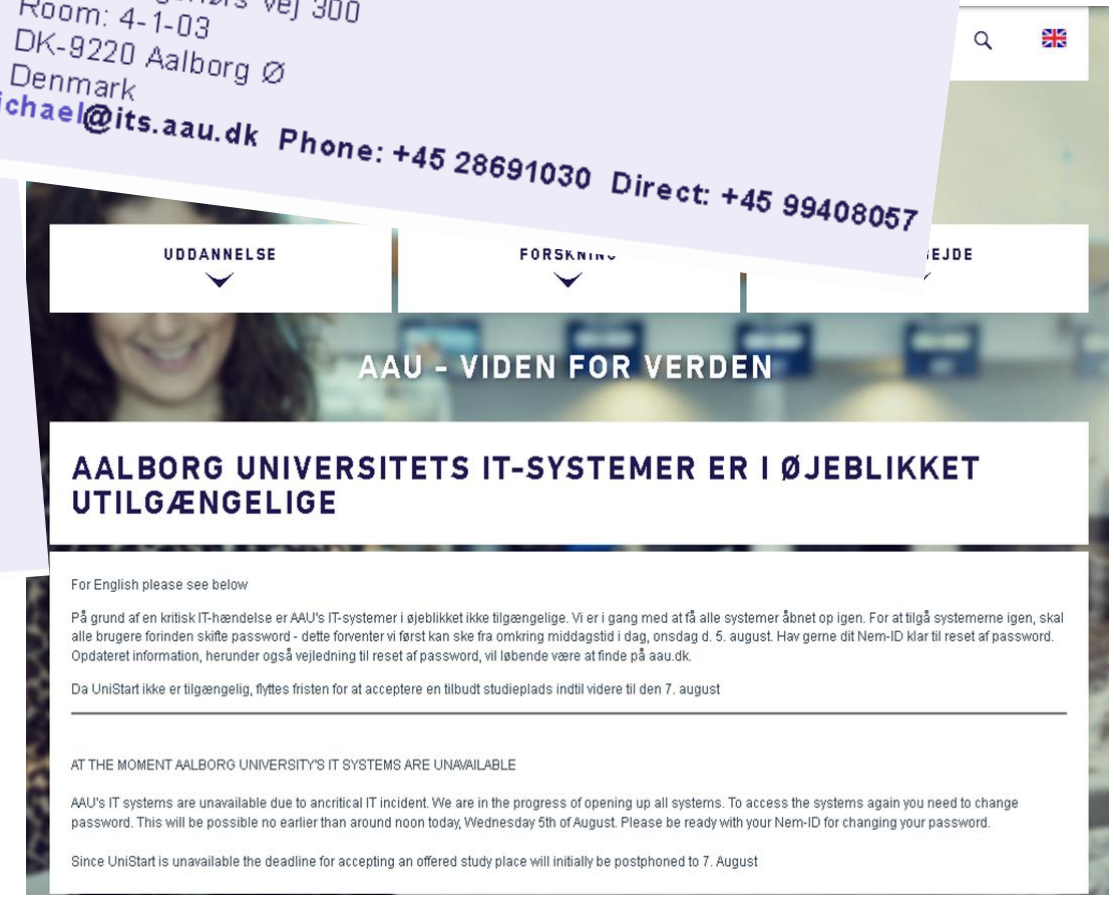
Finn Büttner og Michael Collin- 2021-11-03

AALBORG UNIVERSITET

Hvem er vi?

Michael Collin
~~Supportchef~~ CISO
AAU Employee
AAU IT Services - Support Services
Staff ID: 109897
Selma Lagerløfs Vej 300
Room: 4-1-03
DK-9220 Aalborg Ø
Denmark
Mail: michael@its.aau.dk Phone: +45 28691030 Direct: +45 99408057

Finn Büttner
Systems Administrator
AAU Employee
IT Security Operation Center
Staff ID: 124691
Selma Lagerløfs Vej 300
Room: 4-2-32
DK-9220 Aalborg Ø
Denmark
Mail: fib@its.aau.dk Direct: +45 99409396



AALBORG UNIVERSITET

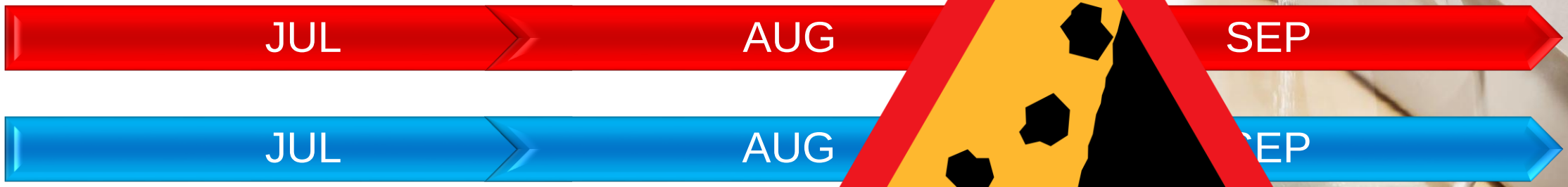
Tidslinje 2020 – FAKTISK…

- AAU opdagede noget mistænkeligt i juli
- Ulykken blev standset,1. uge i august
- AAU 80% i drift, 2. uge i august
- Udredning varede ind i efteråret
- **Pris >2½ mil.kr.**

AALBORG UNIVERSITET

Tidslinje 2020 - HVIS-NU-IKKE...

- AAU rammes af ransomware september
- AAU Studie udsat 2 måneder
- AAU AD genetableret medio september
- AAU mail tilgængelig ultimo september
- AAU medarbejderecomputere ultimo oktober
- **PRIS: >25 mil. kr.**



AALBORG UNIVERSITET

Meget kort om hvad der teknisk var sket

Dato	Angreb	Hvorfor (- nu fikset)
2020-07-01	Username/Password fundet ved bruteforce på Exchange autodiscovery	For simpel (kort) password politik
2020-07-20	Fundet username/password genbrugt, selvom password er ”nulstillet”	Password-reset service gør det muligt at genbruge password.
2020-07-25	Azura MFA bording af AD-konto	MFA bordingproces for studerende adskilt fra kontooprettelse
2020-07-25	VPN MFA bording af AD-konto	Terminal Services anset for on-site netværk
2020-07-25	VPN-forbindelse til infrastruktur	Mangelfuld netværkssegmentering
2020-07-26	Privilege escalation og Lateral movement, AD takeover	Usikker anvendelse af domain administrator konti
2020-07-26	Info om infrastruktur fra administrator mailbokse	Info delt som vedhæftet dokumenter

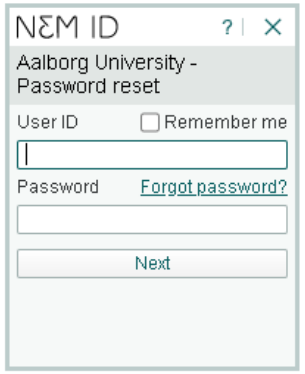
Ny adgangskode til din AAU kont

reset.aau.dk/sib/sibpwd/sibpwdnemidlogin.aspx

Ny adgangskode til din AAU konto

NemID

Log in using NemID

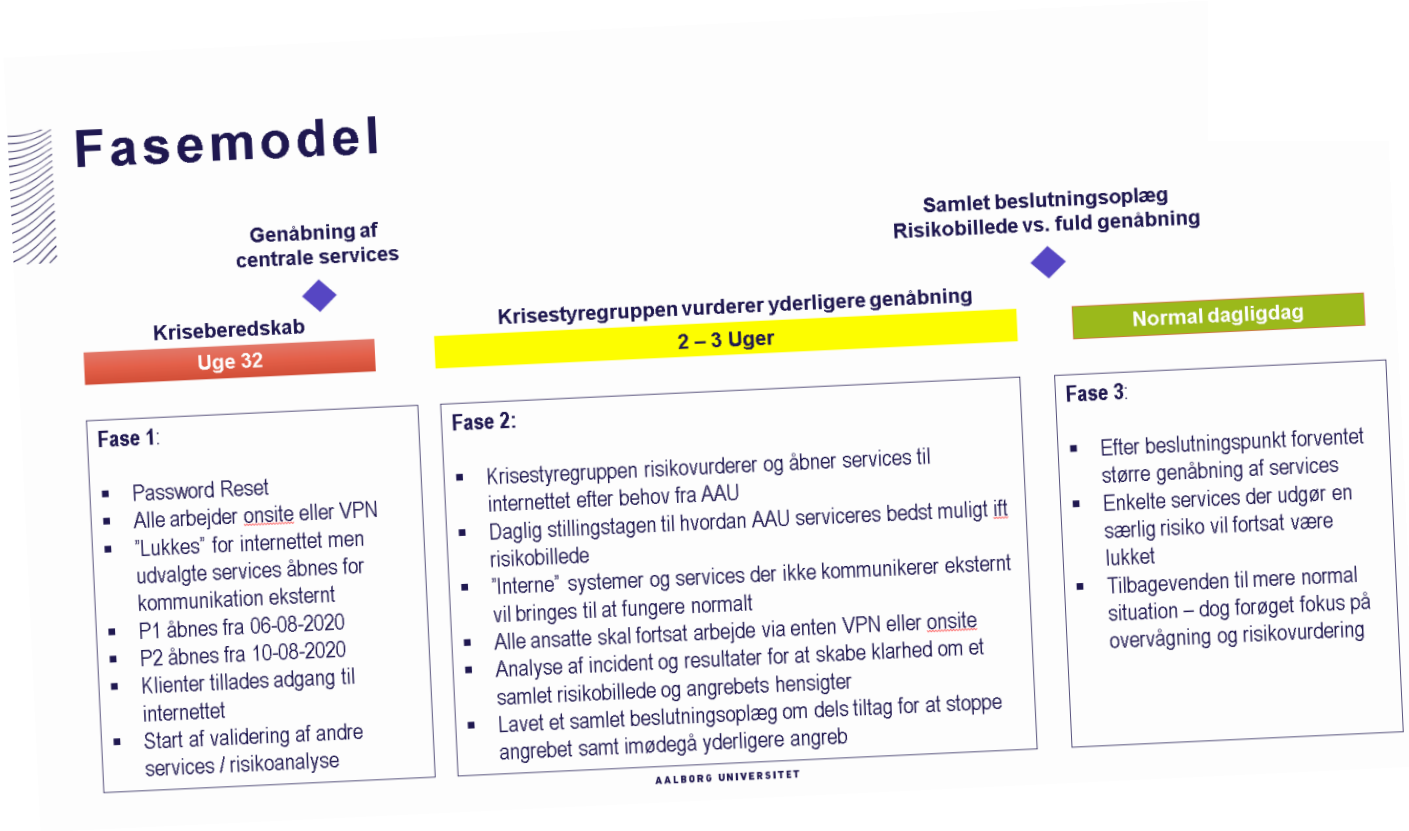


Security reminder

Close all browser tabs when you are done using NemID services.

Beredskabs-aktivering

- Et velrenommeret internationalt IR-firma
  - Få symptomer synlige
  - Ingen kendskab til “vores” logs - ikke rette kompetencer
- Beredskabsaktivering
- Beredskabsgruppe etableret
- CSIS
  - Flere symptomer synlige
  - Indsigt via Proof of Concept etableret kort før
- Topledelse inddrages
- Meget styret kommunikation internt og eksternt
- Kontrolleret nedlukning med kommunikation til alle
  - CSIS
    - Kendskab til angrebsvektorer og I besiddelse af forensics værktøjer
    - Onsite og meget koncentreret – Meget instruerende
- Kontrolleret genåbning til “ny normal” med kommunikation til alle



Datatilsyn, registrerede, politi og Version2

- Lovpligtig underretning til datatilsyn indenfor 72 timer
  - CISO afsender – Jurister og topledelse involveret
  - 1. underretning forholdsvis bred, da omfang endnu ikke var afdækket i detaljer – Heldigvis ingen specifikke detaljer i underretning!
  - Politianmeldelse – En registrering – Ingen blå blink
  - Forskellige underretninger af registrerede omkring lækkede personoplysning
  - Løbende opdatering til datatilsyn efterhånden, som afdækning afslører detaljer
  - AAU kommunikerede eksternt meget tæt efter opdatering af datatilsyn
  - Dialog med datatilsyn om agtindsigtsproblematik
    - Datatilsyn var/er af den opfattelse, at de er forpligtet til at give indsigt i ALT der underrettes om – Dog ikke personnavne
    - Datatilsyn vurderede, at en aktiv politianmeldelse ikke var grundlag for at udskyde svar på aktindsigt
  - Version2 brugte agtindsigt til løbende at indhente viden og lavede journalistisk vinkel (læs sensationspresse)
  - Konklusion:
    - Vær OBS på agtindsigt når konsekvensen for de registrerede vurderes og når registrerede orienteres
    - Vær OBS på at arbejdet med at stoppe angreb og reetablere drift sker samtidig med at sensationshungrende presse arbejder


ING/VERSION2

NYHEDER BLOGS DEBAT JOB SEKTIONER MERE IT-TALENT

Aalborg Universitet hacket: »De kan have skaffet sig adgang til forskning og alle andre oplysninger«

(Illustration: AAU)

I sidste uge lukkede Aalborg Universitet ned for alle interne it-systemer på grund af en såkaldt 'kritisk hændelse'. Nu viser en aktindsigt, at ukendte hackere måske har haft adgang til blandt andet forskningsdata, HR og økonomisystem.

Adam Fribo Tirsdag, 11. august 2020 - 3:45 23

Brug af eksterne eksperter – hvad fik vi ud af det?

	Hvad gav det os?	Ville vi prioritere partnere en anden gang?
Datatilsynet	!?	Det skal vi
Politi	Ingen blå blik. IOC'er til efterforskning.	Det skal vi
DK-CERT	Forbindelse til CFCS.	Det skal vi
CFCS	IOC'er til efterforskning.	Det skal vi
CSIS	Hurtig reaktion og respons	Sandsynligt
Velrenommeret internationalt IR-firma	Tror ikke vi havde de rigtige personer tilgængelige	Måske

Organisatoriske tiltag

- Sikkerhedsteam konsolideret i IT Services
- AD sikkerhedsreview gennemført
- MFA ændring implementeret
- Kommissorium for Informationssikkerhedsudvalg (ISU) opdateret
- ISU formandskab placeret hos Universitetsdirektør
- *SOC*
- *Opdatering af beredskabsplan*

SOC

- SOC
  - Alarmhåndtering med adgang til rette logs
  - Ekstern hjælp (24/7)
    - Leverandørskifte
      - Tekniske kompetencer
      - Procesmæssige kompetencer
  - Vi bliver fortsat klogere på os selv og leverandørerne

Beredskabsplaner opdateret

- Udgangspunkt i igangværende arbejde
  - Beriget med hvad vi gjorde
  - Og hvad vi bagefter har evalueret os til
- Håndtering af Cyber-hændelser skal ske anderledes end ved ”almindelige” driftsnedbrud
- - men øvelse gør mester!

Tak for at I lyttede

- Sikkerhed er ikke bedre end det svageste led
- Ekstern hjælp er ikke bedre end den viden og information, som de får adgang til
- Vær klar på det værste – Beredskabet skal også være funktionsdygtigt på de mest kompetente holder ferie
- Når det sker, så husk i konsekvensvurderingen at tage højde for agtindsigt og presse

- Spørgsmål?