DCeo
DIGITAL LEDELSESRÅDGIVNING

Ramt af hackere..

September 2022

Kristian Bluhme

- 44 år og bor i Gug (Aalborg)

Fhv. Kommerciel direktør for Daarbak og

Tidl. en del af i direktionen.

- IT
- E-commerce / Marketing
- Indkøb
- Butikker
- Kundeservice
- ISO / Lean

DCeo
DIGITAL LEDELSESRÅDGIVNING

Værdier

SAMMENHOLD

Vi står sammen. Vi fejrer i medgang, og vi støtter hinanden i modgang.

FORANDRINGSVILLIG

Vi går forrest, vi udvikler os, og vi handler på nye ideer, udfordringer og ambitioner.

RESPEKT

Vi respekterer os selv, hinanden og verden omkring os. Vi holder altid, hvad vi lover.

POSITIV

Vi tror på os selv, hinanden og virksomheden. Vi ved, at gode arbejdsdage ikke bare sker, de bliver skabt.

RESULTATORIENTERET

Vi sætter mål, og vi når dem. Alt, hvad vi laver, skaber værdi for kunderne, virksomheden og medarbejderne.

ARBEJDSOM

Vi er stolte af vores arbejdsindsatser, og vi går ikke på kompromis med kvaliteten af vores arbejde.

Sagen meldes til politiet

Kære Kristian Bluhme,

De har d. 19. marts 2021 anmeldt afpresning via ransomware til politiet. I den forbindelse har vi brug for de nedenfor oplistc oplysninger for at kunne behandle Deres sag:

- 3 krypterede filer på max ca. 5 mb. Gerne .zip eller .7Z fil.
- Kopi af filer, programmer eller andet der ved gennemgang af serveren findes efterladt af gerningsmændene. Fx krypteringssoftwaren. Gerne som .zip eller .7Z fil.
- Hvis det konstateres at adgangen til jeres computere var gennem RDP (Remote Desktop Port), s hvis muligt en kopi af hele loggen for den kompromitterede RDP port.
- Kopi af spor som gerningsmændene har efterladt i deres forsøg på at fremme deres brugerstatus.

Hvis der eventuelt skulle være andet på computerne/serverne, som I vurderer kunne have interesse for sagen, så et kopi af dette.

Såfremt I har kontaktet gerningsmanden:

- Bitcoinadresse til gerningsmanden, hvis den haves.
- Mail fra gerningsmanden, hvis I har været i kontakt med gerningsmanden (vedhæftet mailen fra gerningsmanden, så mailheaderen kan udlæses)
- Såfremt der er betalt løsesum, filen, typisk decrypt.exe, som blev benyttet til at låse filerne op.

Det hele må gerne samles i en .zip eller .7Z fil.

Det er politiets anbefaling, at der ikke betales løsesum.

- Der er mulighed for at finde dekrypteringsværktøjer på NoMoreRansom.org, der måske kan dekryptere jeres filer. Alternativt kan harddisken gemmes, da siden opdateres løbende.

DCeo
DIGITAL LEDELSESRÅDGIVNING

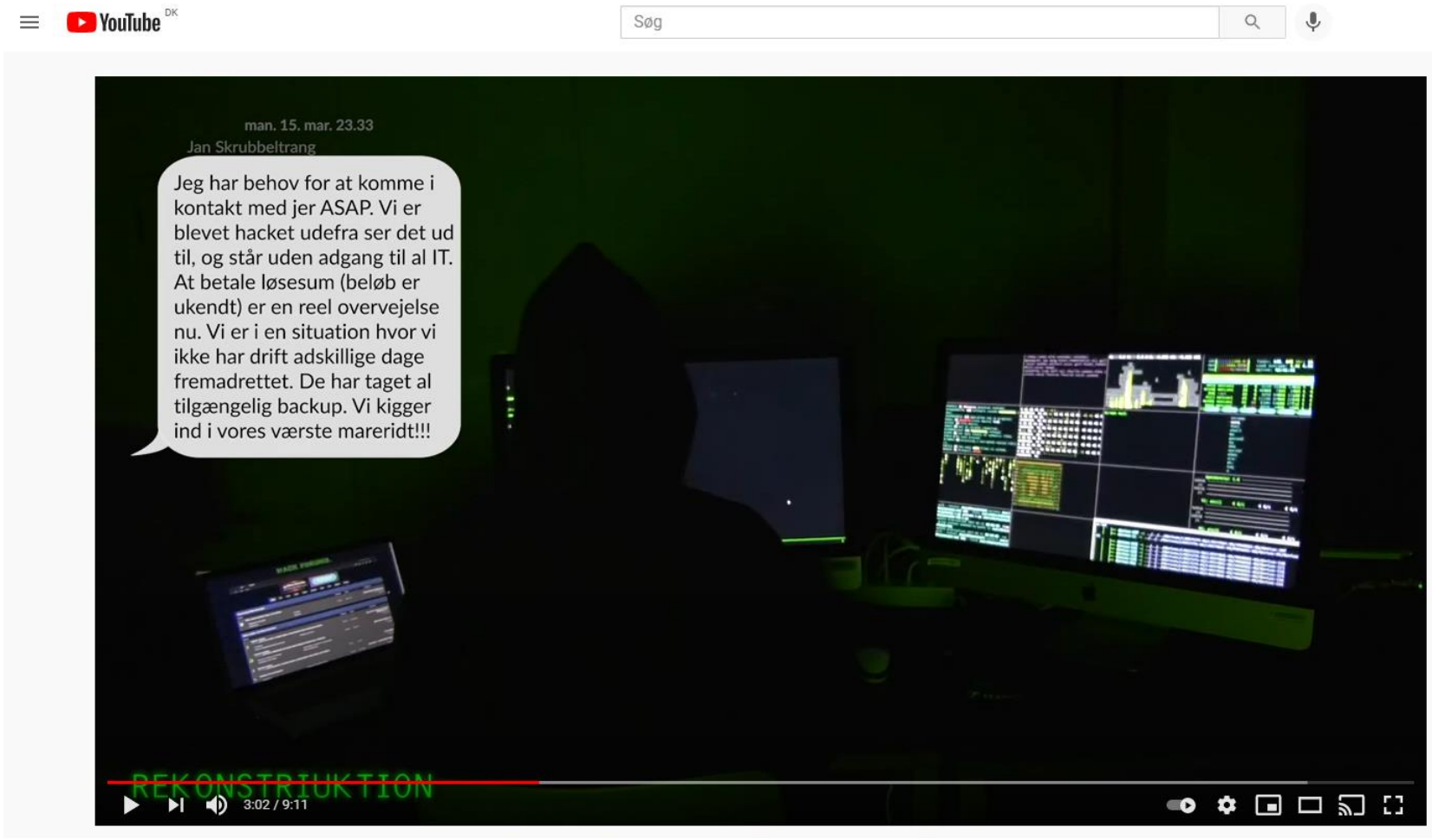
Hvad har vi lært?

- Flere systemer placeres fremadrettet i skyen og ikke i huset
- To-faktor for at få adgang til vores netværk
- Krypterede linjer mellem vores afdelinger
- Ingen mulighed for installation af egne programmer
- Bedre scanningssystemer og lidt forsinkelse på mails
- Scanning på alle links i mails
- Bedre beredskabsplan i forhold at komme hurtigere i drift igen - Penetrationstest
- Sikkerhedstræning løbende af alle medarbejdere – større awareness
- Bedre backup-sikkerhed + mere eksternt

DCeo
DIGITAL LEDELSESRÅDGIVNING

Vil I vide mere?

Se video på Youtube: https://www.youtube.com/watch?v=eOMRM-_WzRo&t=1s



DCeo
DIGITAL LEDELSESRÅDGIVNING

Mine kontaktoplysninger

Kristian Bluhme

kristian@dceo.dk
93 91 91 22

www.linkedin.com/in/**bluhme**

DCeo
DIGITAL LEDELSESRÅDGIVNING