DENMARK SWEDEN NORWAY IRELAND

Kære Picassokunde. 5. juli 2021

Vi har tidligere informeret om det omfattende højteknologisk hackerangreb som Techotel og vores kunder blev udsat for den 9. juni 2021 kl. 02.53 og hvor de kriminelle havde skaffet sig adgang til Techotels kundenetværk, via et stjålet eller afluret password fra en af vore kunder sammen med oplysninger om kundens IP-adresse. Angrebet medførte, at data på servere blev krypteret og vi modtog krav om betaling af løsepenge.

Som vi også har informeret om, påbegyndte vi straks aktiviteter for at udbedre angrebet, og af hensyn til vores kunder besluttede vi at betale et millionbeløb til de kriminelle for at kunne dekryptere hurtigt. Beløbet blev betalt allerede dagen efter angrebet havde fundet sted. Imidlertid viste det sig, at de kriminelle havde forårsaget beskadigelser af systemerne, således at disse ikke straks kunne dekrypteres med den modtagne software fra de kriminelle og et større udbedringsarbejde blev straks iværksat med assistance fra anerkendte specialistfirmaer.

Vi har også redegjort for, at vi foretog anmeldelse til Datatilsynet og har løbende orienteret Datatilsynet omkring det passerede.

Via "driftinfo" er der løbende orienteret om arbejdet med udbedring. Vi vil også gerne give en kort teknisk redegørelse for de aktiviteter, som vi har foretaget for at genetablere systemer og om muligt optimere sikkerheden i tilknytning til arbejdet med dekryptering og udbedring af skader forvoldt af de kriminelle.

- Vi har formateret og foretaget geninstallering af de SQL Cluster serverne som benyttes til Picasso Databaser ligesom det er sket for Picasso Exefiles Cluster miljøet.
- Alle 240 servere i hostingcentret er blevet slettet, gennemgået for vira og genetableret med Windows Server 2019.
- Alle NAS og SAN som benyttes af Picasso er blevet formateret ned til RAID niveau og alle Active Directory og ADFS Servere er blevet geninstalleret.
- Uagtet anvendte Linux servere har ikke været berørte, er disse blevet viruskontrolleret ligesom OS er opdateret.
- Backup infrastruktur er blevet geninstalleret med Database Backups lagering i Microsoft Azure Cloud.

AK Techotel A/S | Sandager 8 | 2605 Brøndby
Phone +45 36 46 11 55 | Fax +45 36 44 20 06
www.techotel.dk | techotel@techotel.dk
CVR 75456611

DENMARK SWEDEN NORWAY IRELAND

- Netværksrouters port antal er reduceret og er sikret med Cisco NextGen Firepower IPS og IDS sikkerhed.
- Sikkerheden er yderligere optimeret med implementering af udvidet Two-Factor Validering.
- Alle brugeres Passwords er blevet fornyet og med anvendelse af 18+ karakterer.
- For at sikre mod at mails til kunderne indeholdende malware og anden virus kan få adgang til Picasso, anvendes Office Outlook ikke af Picasso. Picasso anvender alene Picasso mail, som kun afsender mails fra Picasso, men ikke modtager mails.

Vi håber, at dette giver et rimeligt indtryk af det betydelige og omkostningsfulde arbejde der er udført for at genetablere systemer og om muligt optimere sikkerheden.

Afslutningsvis skal vi opfordre vores kunder til at anmelde angrebet til deres eget erhvervsforsikringsselskab, da dækning på "Cyberforsikring" eller lignende normalt også gælder hostede løsninger.

Med venlig hilsen
AK Techotel A/S

Klaus Ahrenkilde
CEO

AK Techotel A/S | Sandager 8 | 2605 Brøndby
Phone +45 36 46 11 55 | Fax +45 36 44 20 06
www.techotel.dk | techotel@techotel.dk
CVR 75456611