AK TECHOTEL

DENMARK SWEDEN NORWAY IRELAND

Dear Picasso Customer

5 July 2021

We have previously informed about the extensive high-tech hacker attack that Techotel and our customers were exposed to on June 9, 2021 at 02:53 where the criminals had gained access to Techotel's customer network via a stolen or hacked password from one of our customers together with information about the customer's IP address. The attack resulted in data on our servers being encrypted and we received demands for ransom payment.

As we have also informed, we immediately started work to repair the attack, and for the sake of our customers, we decided to pay a million to the criminals in order to decrypt quickly. The amount was paid the day after the attack had taken place. However, it turned out that the criminals had caused extensive damage to the systems so that these could not be immediately decrypted with the software received from the criminals, and a major repair work was immediately initiated with the assistance of recognized specialist companies. We have also reported the incident to the Danish Data Protection Agency and have continuously informed the Danish Data Protection Agency about what has happened. Via "operation info" there is ongoing information about the repair work. We would also like to give a brief technical account of the activities we have undertaken to re-establish systems and, if possible, optimize security in connection with the work of decryption and repair of the damage caused by the criminals.

- We have formatted and reinstalled the SQL Cluster servers used for Picasso Databases, just as we have done for the Picasso Exefiles Cluster environment.
- All 240 servers in the hosting facility have been deleted, crawled for viruses and re-established with Windows Server 2019.
- All NAS and SANs used by Picasso have been formatted down to RAID level and all Active Directory and ADFS Servers have been reinstalled.
- Although Linux servers used have not been affected, these have been virus checked just as the OS has been updated.
- Backup infrastructure has been reinstalled with Database Backup storage in Microsoft Azure Cloud.

- The number of network router ports is reduced and secured with Cisco NextGen Firepower IPS and IDS security.
- Security is further optimized with the implementation of extended Two-Factor Validation.
- All users' Passwords have been renewed and with the use of 18+ characters.
- To ensure that emails to customers containing malware and other viruses can be accessed by Picasso, Office Outlook is not used by Picasso. Picasso only uses Picasso Email, which only sends mails from Picasso, but does not receive mails.

We hope that this gives a fair impression of the significant and costly work that has been done to re-establish systems and, if possible, optimize security. Finally, we must encourage our customers to report the attack to their own insurance company, as coverage on "Cyber Insurance" or similar usually also applies to hosted solutions.

Kind regards
AK Techotel A/S

Klaus Ahrenkilde
CEO