

What type of cyber attack is the Leschaco Group dealing with?

Leschaco is dealing with a ransomware attack called PYSa, a variant of Mespinoza family. Characteristic of this type of attack is that access to devices is blocked or data contained on them is encrypted. This was also the case at Leschaco.

What was Leschaco's response to the attack?

All affected parts of the network were immediately disconnected from the Internet. This deprived the attackers of control or the possibility of remote control. We took immediate action by forming a task force (of more than 100 people) to make sure that the ransomware could not spread further and started the IT forensically analysis. From then on, the preparation for a safe and speedy recovery of our IT landscape was on the way.

Was the whole server landscape affected?

No. The ransomware attacked parts of our IT landscape hosted by external service providers. Our EDI converter has not been compromised. Our communication platforms and channels were not affected by this incident.

How was the malware able to enter the IT infrastructure of the Leschaco Group and has data been stolen / leaked?

In general: The intention behind ransomware attacks is primarily to harm the affected companies, paralyze their systems and extort a ransom. Since this type of attack is not uncommon, it is easy to draw on empirical values. This means that, usually, no other data misuse is to be expected. Together with the authorities, everything was done to prevent misuse and disclosure of data.

You will understand that no further comments can be made on this subject at the moment, because this incident has been a criminal attack. Our experts are in in-depth analysis on that subject. We will provide more information about the incident once the analysis has been finalized.

Has the incident been reported to the authorities?

Yes, the incident has been reported immediately to the relevant local and international authorities.

Is there a danger for external partners coming from Leschaco?

Based on the current status of this FAQ there is no component within the Leschaco IT environment that puts external partners at risk. The rebuilding of our IT systems is executed in strict compliance with the

guidance of our IT security experts and only after the IT forensic investigation has been successfully completed. Our top priority in restoring our operations is to leave no risk of infection to our partners.

Is communication between Leschaco and customers / business partners possible?

Yes. Communication via Microsoft365 and Outlook or Exchange is not affected and possible without any restrictions. Our Electronic Data Interchange (EDI) with our customers takes place via a SaaS EDI converter. This was not affected by the incident and the channel is secure. In- and outbound EDI messaging is up and running again.

For security reasons, Leschaco is following a whitelist concept. Computers are currently only communicating with computers under known IP addresses, or more precisely: with the computers of our customers and business partners that have been checked and approved by IT security.

How are operations working?

Since Friday, September 03, 2021, we can say, that the most important interfaces and routines to our customers and business partners are available:

- The new set-up of our Citrix server farm allows operations with our customers and business partners within secured Citrix Access Workspace environments
- The core of our transport management system ABS and SAP is back into operation
- Our Tank Container System (TCS) including our fleet management is fully integrated
- The most important file servers are available
- New order processing via EDI is functional; Business critical messages, like VGM, B/L and booking requests are transferred to customers and business partners

Can I log on to Leschaco portals/applications?

We are aware that there will be obstructions or restrictions at one point or another in our worldwide network of operations. This is linked to our indispensable focus on maximum security in all regards. The data exchange with external systems will be consequently limited to what is necessary and only eased after IT forensic recommendation as all our systems are on-going subject to IT forensic monitoring. Security always comes before speed.

How will Leschaco counter such incident in the future?

With as much effort as before. Including the knowledge and experiences we gain right now. We will provide more information about the incident once the analysis has been finalized. We will keep our customers and business partners informed about further improvements.

FAQ

Ransomware Security Incident at Leschaco on August 21, 2021



LESCHACO

Forwarding is our passion. Since 1879.

Where do I find up to date information?

Up to date information is provided on our website under customer/customer-advisories and on our twitter channel. If you have any further questions, please reach out to your known Leschaco contact.

Disclaimer

Please note that all information reported in this FAQ is to the best of our knowledge at the time of writing. The information corresponds to the date in the footer of this document. The information will be updated in a regular manner.