Cyber attack – Frequently Asked Questions

Date: 28 April 2022

Has any data been affected by the attack and if so which data?

According to the latest findings, there has been a data breach and the extent is currently being analysed.

As far as we can currently tell, e-mail addresses and passwords of our employees were accessed. As soon as we became aware of this, we immediately took appropriate countermeasures and changed all passwords as a precaution.

How seriously / to what extent was KSB affected by the attack?

KSB was attacked in a targeted manner. The attack compromised a few of our servers and several devices. By taking rapid and rigorous action, we were able to prevent any lasting damage.

What analysis processes have been performed and what measures have been implemented?

We detected irregularities on one server at a very early stage and very quickly decided to disconnect the entire company from the Internet to prevent any further intrusion, contain the damage and prevent encryption. Our IT department is working together with external specialists to repair the damage.

All systems were shut down so that a complete analysis could be performed. This precautionary measure limited our communications and production had to be interrupted for several days at a number of sites. Our analysis to date has shown that only a few of our servers were compromised during the attack.

We are in the process of starting up our servers again and are naturally prioritising security over speed. In the first step, we reconnected the servers for communication and production. The next steps are being carried out according to internal priorities. All servers are being forensically examined before they are put back into operation and set up from scratch if necessary; all servers are also being additionally hardened.

What is the current progress with repairing the damage?

Any systems that were compromised have been re-built from scratch.

The most important systems for communication and production have been up and running again since the middle of calendar week 16. The repair work is proceeding swiftly and according to plan. Every day, new systems are being made available for use.

We expect that all major systems worldwide will be available again by mid-May.

Which government agencies did you inform and what support was provided?

We immediately informed the state authority responsible for data privacy and protection in Rhineland-Palatinate and filed a criminal complaint. The police and public prosecutor's office are investigating the case. We are giving our full cooperation to the authorities. The Rhineland-Palatinate Ministry of Economics has also offered us support.

Reporting requirements in countries outside Germany have been fulfilled via our local companies.

What are you doing to prevent renewed attacks?

We are investigating exactly what happened in detail with external specialists. We will use the findings and insights gained from the prevented cyber attack to make our IT systems even more resilient by implementing technical and organisational measures to ensure cyber prevention and detection.

What is the status of the web site?

The www.ksb.com web site and our local web pages are online again. Regular updates on the progress of our work will be posted here.

A number of functions such as the Web Shop and selection programs are not available yet. Work is currently underway to re-integrate them.