

Cyberangriff – Fragen und Antworten

Stand: 26.4.2022

Sind Daten von dem Angriff betroffen und welche sind es?

Nach neusten Erkenntnissen sind Daten abgeflossen. In welchem Umfang dies erfolgt ist, wird derzeit analysiert.

Nach aktuellem Stand sind E-Mail-Adressen und Passwörter unserer Mitarbeiter abgeflossen. Wir haben sofort nach Bekanntwerden geeignete Gegenmaßnahmen ergriffen und vorsorglich alle Passwörter neu vergeben.

Wie stark / in welchem Umfang ist KSB von dem Angriff betroffen?

KSB ist gezielt angegriffen worden. Wenige unserer Server sowie einige Endgeräte sind bei dem Angriff kompromittiert worden. Durch das sehr schnelle und konsequente Handeln haben wir nachhaltige Schäden verhindert.

Wie ist der Analyse-Prozess erfolgt und welche Maßnahmen wurden ergriffen?

Wir haben in einem sehr frühen Stadium Unregelmäßigkeiten auf einem Server festgestellt und dann sehr schnell entschieden, das gesamte Unternehmen vom Internet abzukoppeln, um ein weiteres Eindringen zu verhindern, den Schaden einzudämmen und eine Verschlüsselung zu verhindern. Zur Schadensbekämpfung arbeitet unsere IT mit externen Spezialisten zusammen.

Zur geordneten Analyse haben wir sodann alle Systeme heruntergefahren. Das hatte zur Folge, dass unsere Kommunikation eingeschränkt und unsere Produktion an mehreren Standorten für wenige Tage ausgesetzt waren. Die bisherige Analyse hat ergeben, dass nur wenige unserer Server bei dem Angriff kompromittiert worden sind.

Beim Wiederherstellen der Server geht Sicherheit vor Schnelligkeit. Zunächst wurden die Server für Kommunikation und Produktion wiederhergestellt. Für die weiteren Schritte gibt es eine interne Priorisierung. Alle Server werden vor Inbetriebnahme forensisch untersucht und bei Bedarf neu aufgesetzt, alle Server werden zusätzlich gehärtet.

Wie ist der aktuelle Stand der Schadensbeseitigung?

Dort, wo Systeme kompromittiert wurden, wurden diese von Grund auf neu aufgesetzt.

Die wichtigsten Systeme für Kommunikation und Produktion sind seit Mitte KW 16 wieder hochgefahren. Die Arbeiten gehen zügig und planmäßig voran. Jeden Tag werden neue Systeme für den produktiven Einsatz zur Verfügung gestellt.

Wir gehen davon aus, dass Mitte Mai alle wesentlichen Systeme weltweit wieder zur Verfügung stehen.

Welche staatlichen Behörden wurden informiert und welche Unterstützung wurde gegeben?

Wir haben sofort die zuständige Landesbehörde für Datenschutz in Rheinland-Pfalz informiert sowie Strafanzeige erstattet. Polizei und Staatsanwaltschaft ermitteln. Die Behörden werden von uns vollumfänglich unterstützt. Das Wirtschaftsministerium Rheinland-Pfalz hat uns zudem Unterstützung angeboten.

Etwaige Meldepflichten in den Ländern außerhalb Deutschlands sind über unsere jeweiligen Landesgesellschaften vorgenommen worden.

Was tun Sie, um erneute Angriffe zu verhindern?

Wir klären den Sachverhalt mit externen Spezialisten vollumfänglich auf. Die Erkenntnisse aus dem abgewehrten Cyberangriff nutzen wir, um unsere IT-Systeme durch technische und organisatorische Maßnahmen der Cyberprävention und -detektion noch resilienter zu machen.

Wie ist der Status der Homepage?

Die Homepage www.ksb.com sowie die jeweiligen Landesseiten sind wieder online. Hier werden regelmäßig Updates über den Fortschritt der Arbeiten veröffentlicht.

Einige Funktionen wie Webshop und Auslegungsprogramme stehen derzeit noch nicht zur Verfügung. An deren Einbindung wird derzeit gearbeitet.