Eines unserer Husky Systeme, welches seit Jahren bei einem unserer Kunden betrieben wird, wurde von einem Verschlüsslungsvirus angegriffen. Auslöser war das Öffnen einer Datei.

Ergebnis:

- 4 infizierte physische Clients
- 1 infizierter physischer Server inkl. verschlüsseltem Backup
- 25 infizierte virtuelle Server bzw. Clients
- Über 1 Millionen verschlüsselte Dateien
- Erpressungsversuch im 5-stelligen Bereich zur Freigabe (Entschlüsselung) der Daten

Da der Virus zeitversetzt erst nach Mitternacht seine Verschlüsselungsaktivität aufgenommen hat, hatte er genügend Zeit sich im gesamten Netzwerk zu verbreiten.

Trotz des großen Schadens und der damit verbundenen Ausfallzeiten, konnten alle Rechner des Husky - Systems® aus den Sicherungen komplett wiederhergestellt werden. Diese Datensicherungen lagen in dem von Husky Systems® verwalteten Speicher. Dieser ist für den Virus nicht angreifbar – somit total sicher.
Nicht so die physischen Clients und Server außerhalb Husky Systems®, da auch deren Sicherungen durch den Virus verschlüsselt wurden. Durch die notwendige komplette Neuinstallation und Einrichtung dieser Maschinen war ein Datenverlust leider unvermeidlich.

Bei dieser Schadensgröße wurde die Kriminalpolizei, Bereich CyberCrime, eingeschaltet, die diesen Angriff aufgenommen hat und in Zusammenarbeit mit LKA und BKA untersucht. Diese bestätigten, dass unser Kunde mit Husky-Systems® „sehr gut aufgestellt“ ist. Das ist mit herkömmlichen Client-Server-Systemen leider nicht immer der Fall.

Wir werden durch dieses Ereignis natürlich weiter an der Sicherheit von Husky-Systems® arbeiten, sind aber beruhigt, dass wir in solch einem Fall gut gerüstet sind.

Bitte prüfen Sie dringend, ob Ihre Datensicherung über das Firmennetz erreichbar ist. Ist dies der Fall, besteht die größte Gefahr, dass Ihre Daten bei solch einem Angriff verschlüsselt und somit unbrauchbar werden.

Ihre Datensicherung sollte unabhängig vom Firmennetz sein. Wie unser Husky-Systems®

Für Rückfragen stehen wir natürlich gerne zur Verfügung.

P.S. Auch die Kriminalpolizei empfiehlt:
Bei unsicheren Dateien, sei es in Mails, Downloads oder USB Stick, prüfen Sie und Ihre Mitarbeiter diese immer erst über virustotal.
https://www.virustotal.com/#/home/upload

Weitere Informationen vom LKA-Niedersachsen „Wie schütze ich mich von Phishingmails?“
https://www.polizei-praevention.de/themen-und-tipps/phishing.html

Informationen vom BKA „Digitale Erpressung“
https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html