CYBER

# Horrorszenario...

Foto: Ken Schluchtmann, diephotodesigner.de

## ...Ransomware-Angriff – was tun?

Es ist passiert: Das IT-System des Ingenieurbüros steht still, die Bildschirme bleiben schwarz, der Zugriff auf alle E-Mails, Daten, Programme und das gesamte bürointerne LAN ist nicht mehr möglich. Stattdessen erscheint die gefürchtete ellenlange Nachricht der Hacker – weiß auf schwarzem Hintergrund: Sie fordern hohe Kryptozahlungen und drohen damit, sensible Daten preiszugeben. Und das alles kurz vor Finalisierung einer großen Ausschreibung – Panik bricht aus. Genau das haben Markus D., Geschäftsführer eines Ingenieurbüros, und sein Team aus 14 Mitarbeitern erlebt.

### In Unternehmen längst die Realität

Ein Horrorszenario, das sich mittlerweile fast täglich abspielt, wenn Unternehmen von sogenannten Ransomware-Gruppen wie z. B. Lockbit angegriffen werden. Dabei sind die Opfer längst nicht immer große, bekannte Player. Vielfach handelt es sich um kleine oder mittelständische Unternehmen,


auch Ingenieurbüros zählen dazu. Was allerdings alle betroffenen Unternehmen vereint: In 95 Prozent der Fälle ist der der Grund für den Angriff die Schwachstelle Mensch. Genauso wie im analogen Leben, suchen die Täter nach passenden Einfallmöglichkeiten. Bildlich gesprochen: Welche Tür ist nicht verriegelt, welches Fenster steht noch einen Spalt offen? Erspähen die Angreifer auch nur eine Lücke,

schlagen sie zu. Erst danach wird analysiert, wen sie an der Angel haben und wieviel Geld man erpressen kann.

### Unterschiedliche Formen der Erpressung

Die Erpressungsgegenstände bei Ransomware-Angriffen variieren. Entweder werden nur Daten und Programme verschlüsselt, die dann nicht mehr genutzt werden können. Außerdem kann es vorkommen, dass Daten abgezogen werden – das Unternehmen ist nicht mehr alleiniger Besitzer. Die Täter drohen zusätzlich damit, die Daten zu veröffentlichen. Das kann gerade bei personenbezogenen Informationen sehr heikel sein. Einige Tätergruppen agieren besonders perfide: Sie scheuen sogar nicht davor zurück, Mitarbeiter des Unternehmens zu kontaktieren und drohen ihnen und auch deren Familienmitgliedern.

### Gravierende Folgen für Unternehmen

Stellt sich nach einer Lageanalyse durch die eigene IT, oder den IT-Dienstleister, auf den man sich verlassen hat, schließlich heraus, dass auch die Back-Ups betroffen sind, wird die Situation schnell ungemütlich. Die Opfer stehen vor einem Dilemma. Denn alle Optionen, die auf dem Tisch liegen, haben Vor- und Nachteile. Der erste Reflex der Unternehmen lautet meist, in keinem Fall der Erpressung nachzugeben und schalten zunächst die Polizei ein – auf alle Fälle der richtige Schritt. Dennoch müssen Unternehmen sich mit den Konsequenzen des Ransomware-Angriffs beschäftigen. Was heißt das für den Fortbestand der Firma? Wie hoch ist der Schaden pro Tag, solange die IT ausfällt? Welcher Umsatz entgeht, weil keine Aufträge bearbeitet oder an Land gezogen werden können? Wie lange dauert es, bis alles wieder läuft – und was kostet das? Alle diese Fragen brauchen schnell Antworten.

Das Ergebnis kann verheerend sein, z. B. wenn klar wird, dass ein Unternehmen binnen weniger Wochen nicht mehr zahlungsfähig ist. Die Kosten für Wiederanlauf und Betriebsunterbrechung sind die Treiber im Bereich der Schadensumme. Eventuell ist der Schaden so groß, dass sogar die Verhandlungen mit den Angreifern eine Option darstellt.

Foto: Ken Schluchtmann, diephotodesigner.de

## ÜBER DEN AUTOR

Oliver Schneider ist Geschäftsführender Gesellschafter der RiskWorkers GmbH. Seit über 20 Jahren ist er als sogenannter Kidnap Response Consultant tätig und hat mit Entführern, Erpressern und Piraten auf der ganzen Welt verhandelt. Seit einigen Jahren berät er Unternehmen auch bei Cyber Erpressungen, sowohl präventiv als auch reaktiv. Als Autor hat er das Buch „Der Wille entscheidet" veröffentlicht, wo er einen spannenden Einblick seinen Tätigkeit gibt.

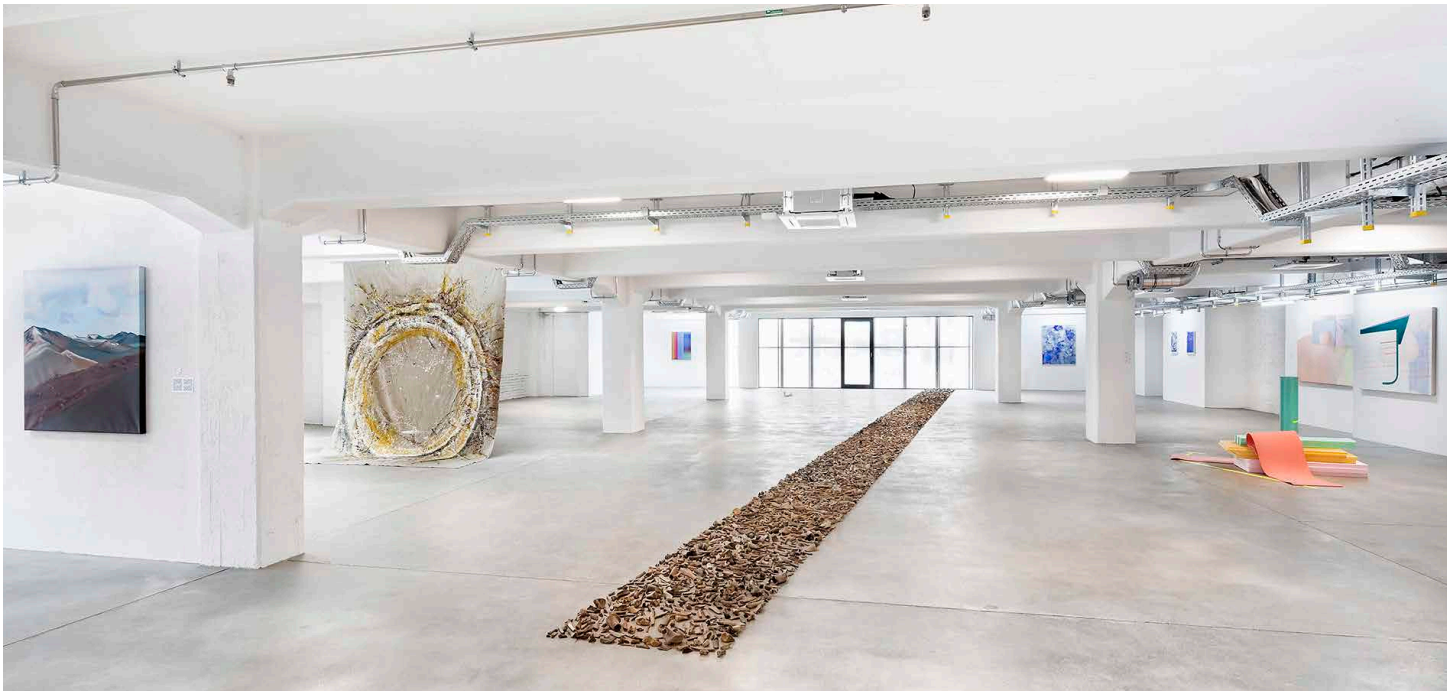

Foto: Ken Schluchtmann, diephotodesigner.de

### Mit einer Cyber-Versicherung auf alles vorbereitet sein

Die Antworten auf die oben gestellten Fragen hatte Markus D. schnell parat. Denn er hatte vorausschauend bereits vor drei Jahren eine Cyber-Versicherung abgeschlossen. Er konnte sich noch dunkel daran erinnern, dass auch etwas von Krisenmanagement und Verhandlungsunterstützung in der Police stand. Und eine 24/7 Hotline gab es, soweit er wusste, auch noch.

Relativ schnell hatte Markus D. die Spezialisten aus dem Netzwerk des Versicherers am Telefon. Erfahrene Krisenmanager, IT-Forensiker, Verhandlungsspezialisten, IT-Rechtsbeistand, Kommunikationsprofis, alle wurden direkt nach dem Angriff durch das Notfallcenter alarmiert. Ein erstes Teams-Meeting und der Austausch von Informationen liefen sofort an. Genutzt wurde dazu die gmail-Adresse der Ehefrau - in der Not geht vieles.

### Unterstützung durch kompetente Experten

Die Forensik machte sich sofort daran, den Schaden einzugrenzen, die Lücken im System zu schließen und eine erste Schadenhöhe zusammen mit dem Inhaber zu eruieren. Bezogen auf den Faktor Zeit und die zu erwartende Schadenhöhe in einem mittleren sechsstelligen Betrag erwogen die Experten schließlich auch die Option, mit den Tätern zu sprechen. Dazu hat die Versicherung Verhandlungsspezialisten zur Verfügung gestellt, die entsprechende Erfahrung im Umgang mit Cyber-Kriminellen mitbringen. Denn der Polizei ist es tatsächlich untersagt, über Lösegeld zu verhandeln. Nach fünf harten Verhandlungstagen war endlich ein Deal erreicht: Die Täter erhielten einen fünfstelligen Betrag und stellten im Gegenzug den Entschlüsselungscode zur Verfügung. Die IT-Forensik konnte danach sämtliche Systeme und Dateien entschlüsseln. Nach sechs Tagen lief die gesamte IT des Ingenieurbüros wieder. Und die Ausschreibungsunterlagen konnten dank einer Fristverlängerung drei Tage verspätet an den Kunden übermittelt werden. Ende gut, alles gut?

## Fazit:

Nicht immer gehen Ransomware-Angriffe so glimpflich aus, wie gerade eben geschildert. Chaos im Management und mangelnde Erfahrung im Umgang und der Bewertung einer solchen Situation sind eher die Regel. Deshalb ist es wichtig, sich frühzeitig auf dieses Szenario einzustellen. Wie ist mein Unternehmen aufgestellt? Ist die Versicherungslösung adäquat und wird im Worst Case auch Lösegeld gecovert? Eine Cyber Versicherung bietet hier wertvolle Unterstützung: Denn anders als bei jeder anderen Versicherungslösung deckt sie nicht nur den finanziellen Schaden ab, sondern stellt durch ein breites Assistance Netzwerk schnelle und professionelle Hilfe bereit. Sie sorgt dafür, dass Spezialisten in das Krisenmanagement integriert werden, die bei der Lagebeurteilung und der Problemlösung unvoreingenommen und mit kühlem Kopf reagieren. Denn in diesem Fall wollen alle Beteiligten – Versicherer, Unternehmen und Krisenprofis - das Gleiche: die Schäden so gering wie möglich halten. Und gerade in dieser Situation stimmt ein Grundsatz mehr denn je: Zeit ist Geld.

**Autor**

**Oliver Schneider** M.Sc.
Geschäftsführender Gesellschafter/
Managing Director
RiskWorkers GmbH
www.riskworkers.com
Email: oliver.schneider@riskworkers.com

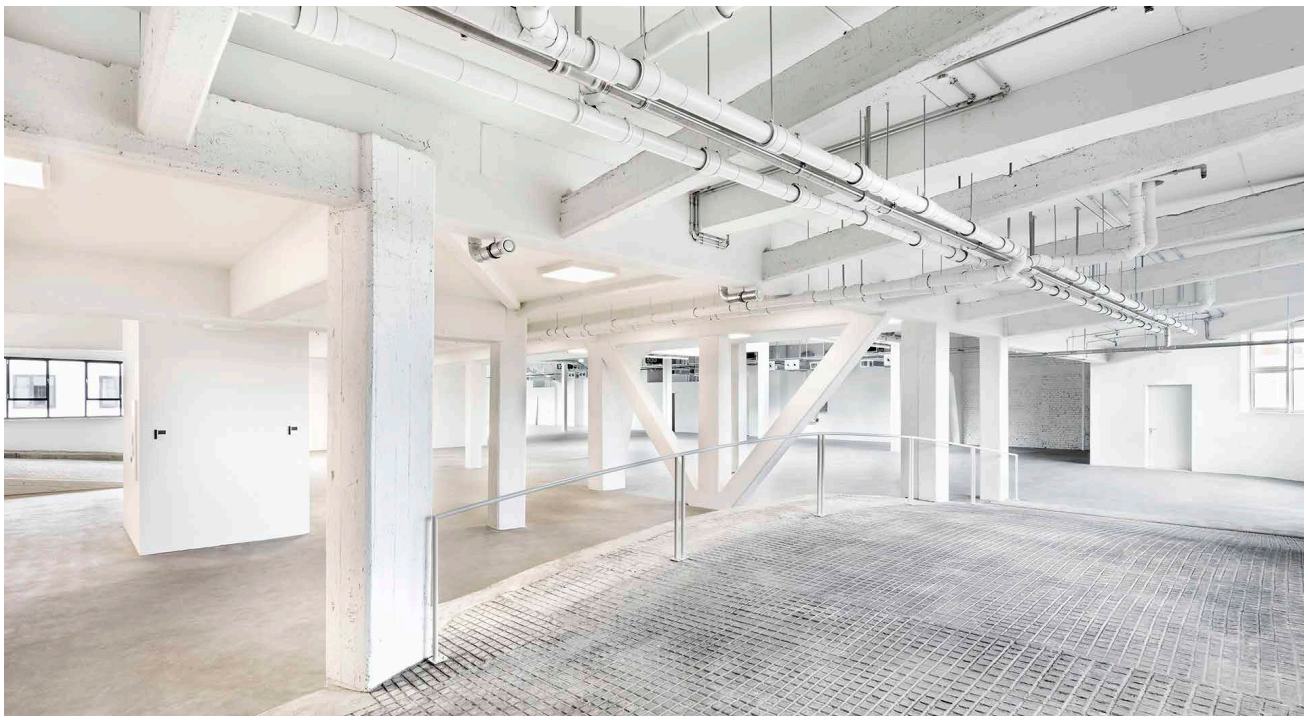

Foto: Ken Schluchtmann, diephotodesigner.de