BEST GRUPPE

BEST Aktuell

Cyber-Risiken: Richtige Datensicherung essenziell | Folgen von Cyber-Attacken vielfach versicherbar

Düsseldorf, 30. März 2017 – Die virtuellen Angriffe mit Hilfe von Kryptojanern hatten im letzten Jahr Hochkonjunktur. Die wohl bekannteste, sogenannte Ransomware ist Locky, die Mitte 2016 nicht nur Unternehmen und ganze Krankenhäuser lahm legte, sondern auch bei Privatpersonen erfolgreich Schaden anrichten konnte. Das Prinzip: Ein Hacker verschafft sich mittels Kryptotrojanern, oftmals via „verseuchter" E-Mail, Zugang zu Rechnern und Netzwerken. Der Schädling verbreitet sich dann auf unterschiedlichstem Weg und verschlüsselt alle Dateien, die er „zu sehen" bekommt. Anschließend fordert der Hacker Lösegeld für die Entschlüsselung der „geenterten" Daten. Trotz aller technischen und organisatorischen Vorsichtsmaßnahmen ist niemand gefeit vor einem Cyberangriff. Gut zu wissen: Versicherbar ist nicht alles, aber zum Glück viel.

Ende letzten, Anfang diesen Jahres verschafften sich Kriminelle vermehrt auf ganz perfide Art Zugriff auf Daten: getarnt als Online-Bewerbung auf tatsächlich ausgeschriebene Stellen. Der vermeintliche Absender: die Bundesagentur für Arbeit. Die Empfänger: nicht nur Mitarbeiter in Personalabteilungen, sondern gerade bei kleineren und mittelständischen Unternehmen auch Geschäftsführer. Sie wurden dazu animiert, die „Bewerberdaten" aktiv von der „Bundesagentur" herunter zu laden. Damit öffneten sie jedoch Tür und Tor ins Herz des Unternehmens. Denn tatsächlich hatte die digitale Post keine Bewerberdaten, sondern besagte Schadsoftware „im Gepäck". Sicherheitseinstellungen wurden auf diese Weise einfach unterlaufen. Das Verschlüsseln von Daten, schlimmstenfalls sogar der vollständige Datenverlust und Betriebsstillstand waren Folgen. Die Anfrage nach dem „Interesse an Entsperrung gegen Gebühr" kam prompt.

Dies zeigt einmal mehr: Trotz aller technischen und organisatorischen Vorsichtsmaßnahmen ist niemand gefeit vor einem Cyberangriff. Es wird immer wieder kreative Lösungen für kriminelle Angriffe geben, von denen sich der Mensch täuschen lässt. Auch die beste Technik hilft nicht, denn Mitarbeiter und Geschäftsführer können im Alltag gar nicht immer so bedacht handeln, dass „unsichtbare Kriminelle" keinen Zugang finden. Letztlich ist auch das Vorgehen mittels „Fake-News" wie E-Mails mit dem Absender des Vorgesetzten eher „ein leichtes Unterfangen". So sind häufig E-Mail-Accounts jedermann frei zugänglich und auch Firmensignaturen können im Netz leicht besorgt und fremd verwendet werden.

Um dennoch zu gewährleisten, dass Daten nicht unwiederbringlich verloren gehen, ist die richtige Datensicherung essenziell - auch die von lokalen Geräten. Im Falle eines Falles können die extern gesicherten Daten zügig wieder ins System eingespielt und der Geschäftsbetrieb wieder aufgenommen werden. Doch Vorsicht: Die Datensicherung alleine hilft nur bedingt – ohne Test, ob die Daten auch wieder einspielbar sind, ist man nur vermeintlich auf der sicheren Seite.

Wenngleich der Schaden minimiert werden kann, so bleibt ein Cyber-Angriff i.d.R. nicht ohne Folgen. Versicherbar ist nicht alles, aber zum Glück viel. Die Grundlage für eine maßgeschneiderte Lösung stellt hierbei immer eine Bewertung der individuellen Risiken, der eingesetzten Sicherheitstechnik, der notwendigen Daten, des persönlichen Haftungsrisikos und auch der Organisationsstruktur und möglichen Mitarbeiterschulung dar.

Kennen Sie Ihr Risiko? Wir nehmen dies gerne unter die Lupe und finden die für Sie richtige Lösung. Wir freuen uns auf Ihre Nachricht!