Betriebsunterbrechung durch Cyber-Angriff – Ein immer häufigeres Szenario

Kelkheim, 19. Dezember 2017

Bildquelle Flickr: Blogtrepreneur CC Lizenz

Es war eines der gefürchtetsten Schreckensszenarien für Unternehmen und Sicherheitsexperten, das was sich im Februar 2016 abspielte: Ein Cyber-Angriff legte das Lucaskrankenhaus in Neuss lahm. Hackern war es gelungen einen Virus im Computersystem zu platzieren und den Zugriff auf die sensiblen Krankenhausdaten zu sperren. Nach Zahlung eines Lösegeldes würden sie die Daten wieder entschlüsseln, behaupteten die Cyber-Kriminellen. Das Krankenhaus ging nicht darauf ein. Die Computerexperten des Hospitals nahmen stattdessen das gesamte IT-System vom Netz und arbeiteten wochenlang daran, die Daten wiederherzustellen. So lange konnte das Krankenhauspersonal nicht auf ihre IT zurückgreifen, Patientendaten nicht eingesehen werden. Die Mitarbeiter mussten wieder mit Papier und Stift, Fax und Post arbeiten. Es dauerte Monate bis der normale Betrieb wieder hergestellt war. Der Schaden war enorm: Rund ein Fünftel der geplanten Operationen musste abgesagt werden, die Notaufnahme konnte nur eingeschränkt arbeiten. Dem Krankenhaus entgingen

nicht nur Einnahmen, sondern es entstanden zudem hohe Kosten, da teure externe IT-Spezialisten beauftragt werden mussten, um den Betrieb wieder zum Laufen zu bekommen.

Betriebsunterbrechungen sind das Schadensrisiko Nummer 1 für Unternehmen

Betriebsunterbrechungen sind laut des Allianz Risk Barometer das Schadensrisiko Nummer 1 für Unternehmen. Aber während früher Schäden an den Produktionsstätten die Hauptursache für Betriebsunterbrechungen waren, verschiebt sich dies inzwischen in Richtung Nicht-Schaden-Ereignisse. Und solche Betriebsunterbrechungen ohne Schäden an den Anlagen sind nicht weniger kostspielig. Wie das oben geschilderten Beispiel des Lucaskrankenhauseses zeigt.

Ein wesentlicher Grund, warum sich die Ursachen für Betriebsunterbrechungen in Richtung Nicht-Schadensfälle verschieben, ist die zunehmende Digitalisierung. Unternehmen sind in immer stärkerem Maße abhängig von Software und (Echtzeit-)Daten, setzen immer öfter zur Optimierung ihrer Prozesse und Steuerung ihrer Produktionsabläufe auf Cloud-Ware und Fernsupport, bekommen ihre Updates regelmäßig über das Internet. Viren, die die Software infizieren, Cyber-Angriffe, die den Zugriff auf die Unternehmens- und/oder Kundendaten blockieren und ähnliche Attacken, führen immer öfter zu Betriebsausfällen.

Das gilt auch für so genannte DDoS-Angriffen. DDoS steht für Distributed Denial of Service. Bei diesen Attacken wird die Website oder auch der Online-Shop mit einer extrem großen Anzahl von Anfragen quasi bombardiert, was dazu führt, dass der Server überlastet wird und die Website, der Online-Shop nicht mehr erreichbar ist. Für viele Unternehmen heißt dies: Es entgeht ihnen ein beträchtlicher Umsatz.

Solche DDoS-Attacken haben in den vergangenen Jahren stark zugenommen. Experten gehen davon aus, dass es bis zum Jahr 2020 weltweit 17 Millionen sein werden; das ist eine Steigerung um 25 Prozent pro Jahr. In den vergangenen Jahren waren auch die Website großer Unternehmen nicht vor solchen Angriffen gefeit: Im Oktober 2016 legte das MiraiBotnet teilweise die Webseiten von Netflix, Twitter, CNN und dem Guardian lahm. Cyberrisiken betreffen alle. Sowohl große als auch kleine Unternehmen, Produktionsbetriebe genauso wie

Dienstleister, Online-Händler ebenso wie Finanzunternehmen.

Cyber-Attacken werden ausgeklügelter – der Schutz gegen Betriebsunterbrechung muss mitziehen

Die Cyber-Kriminelle werden immer erfinderischer, ihre Attacken immer komplexer und richten immer mehr Schaden an. Gleichzeitig sind Cyberrisiken noch relativ neu und daher von vielen Versicherern nicht automatisch in einer Versicherung gegen Betriebsunterbrechungen abgedeckt. Versicherer müssen nun neue Auslöser für Betriebsunterbrechungen in ihre Bedingungen einschließen.

Unternehmen sollten bei einer Versicherung gegen Betriebsunterbrechungen prüfen, ob diese auch Cyber-Ereignisse einschließt sowie weitere nicht durch einen Schaden verursachte Unterbrechungen, wie Stromausfälle, Lieferkettenstörungen, Folgen eines Terrorangriffs oder politische Gründe, abdeckt.

Über die gb.online gmbh

Die gb.online gmbh hat sich auf die berufliche Absicherung von Freelancern spezialisiert und bietet mit www.easy-insure.eu das umfangreichste Online-Versicherungsportal für freie und beratende Berufe in Deutschland. Seit 2011 können Selbstständige und Unternehmen bis 1 Million Euro Umsatz pro Jahr hier ihre beruflichen Risiken versichern.

Steigt der Umsatz, und wird eine individuelle Lösung benötigt, so steht mit dem Schwesterunternehmen groot bramel versicherungsmakler gmbh ein verlässlicher Partner zur Seite, der seit über 25 Jahren Gewerbetreibende und industriellen Unternehmen in Versicherungsfragen vertritt. Die groot bramel versicherungsmakler gmbh ist in 18 Ländern vertreten und begleitet sie, wohin auch immer sich ihr Geschäftsfeld entwickelt.

Kontaktdaten

gb.online gmbh
Frankfurter Straße 93
65779 Kelkheim

Ansprechpartner: Lutz-Hendrik Groot Bramel, Geschäftsführer

Folgen Sie uns auch auf	