PLEITE AUS DEM NICHTS NETZ

Wer in die Insolvenz schlittert, hat schlecht gewirtschaftet – könnte man meinen. Doch auch finanziell kerngesunde Unternehmen können von heute auf morgen in Liquiditätsschwierigkeiten kommen und damit ihre Existenz riskieren: Cybercrime ist eine der gefährlichsten und gleichzeitig am meisten unterschätzten Bedrohungen für die Liquidität von Unternehmen in der heutigen Zeit.

Es ist ein Donnerstag, als im bayerischen Klinikum Grafenfels *(Name geändert)* der erste Rechner ausfällt. Die Patienten liegen nichtsahnend auf ihren Zimmern, als nach und nach immer mehr Abteilungen Probleme melden und ein Computerbildschirm nach dem anderen schwarz wird – bis schließlich die gesamte IT des Krankenhauses zusammenbricht. Die Ärzte und Schwestern haben keinen Zugriff mehr auf Patientendaten, nicht einmal die Telefonanlage funktioniert noch. Die Klinikleitung meldet das Krankenhaus umgehend von der Integrierten Rettungsleitstelle ab. Krankenwagen werden umgeleitet, Notfallpatienten in andere Kliniken verlegt, die restlichen Patienten müssen weitestgehend ohne IT-Unterstützung behandelt werden. Medikamentenlisten werden für jeden einzelnen Patienten händisch neu erstellt – ein unfassbarer Aufwand.

Was klingt wie Stoff für einen Krimi, ist ein realer Fall. Ausgelöst durch eine Malware, versteckt in einem E-Mail-Anhang, den ein Klinik-Mitarbeiter unvorsichtigerweise öffnete. Es dauerte Tage, bis die Systeme des Krankenhauses einigermaßen wiederhergestellt waren. Patienten seien zu keinem Zeitpunkt in Gefahr gewesen, gab das Klinikum damals bekannt. Der materielle Schaden jedoch war immens: Vertrauensverlust, Verdienstausfälle, außerdem ließ das Klinikum alle Bankkonten sperren, um den finanziellen Schaden zumindest einzudämmen.

SORGLOSIGKEIT TROTZ STEIGENDER GEFAHR

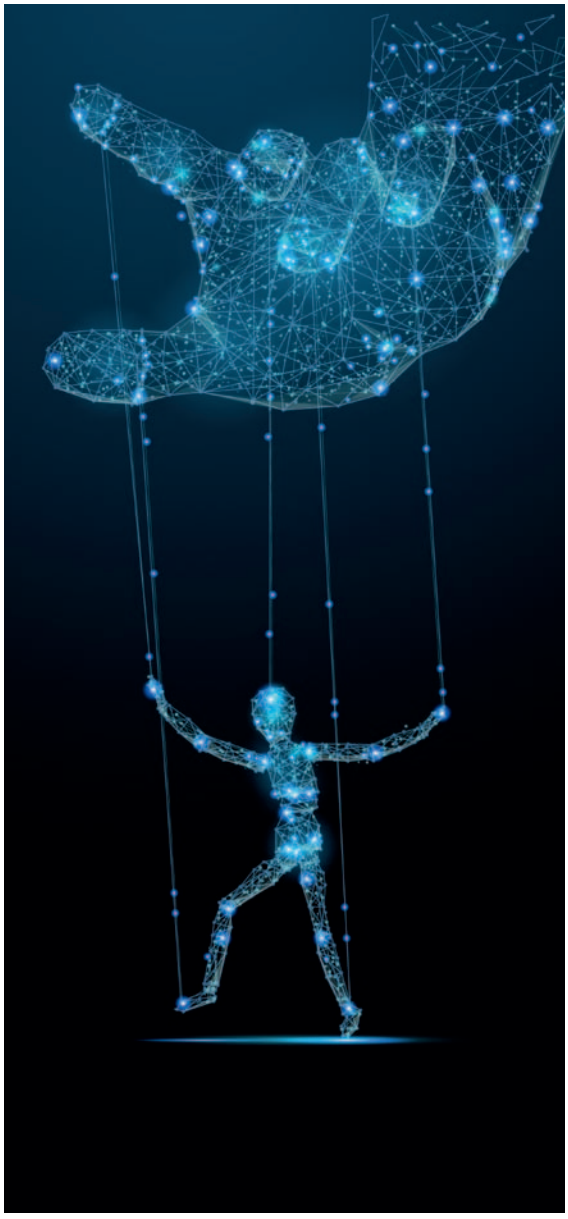
Von heute auf morgen kann ein Unternehmen von Cybercrime betroffen sein. Das Klinikum Grafenfels hat den Angriff trotz finanzieller Einbußen „überlebt". Andere Unternehmen haben nicht so viel Glück – stillstehende Produktion im eigenen Haus, Lücken in der Lieferkette bei Zulieferern, hohe Geldzahlungen in Form von „Lösegeld", um auf die eigenen Dateien wieder zugreifen zu können: Auch jedes noch so gesunde Unternehmen kann durch einen Cyber-Angriff innerhalb kürzester Zeit starke Liquiditätsprobleme bekommen oder sogar zahlungsunfähig werden.

Dennoch scheinen viele Unternehmen die Gefahren durch Cybercrime zu unterschätzen. Dabei ist es nicht so, dass die Unternehmer in Deutschland die Brisanz des Themas nicht generell erkennen würden: 72 Prozent der Manager im Mittelstand halten das Risiko durch Cyberkriminalität für hoch. Die Zahlen bestätigen das: Das Bundesamt für Verfassungsschutz zählt alle drei Minuten einen Angriff auf einen Betrieb in Deutschland. 55 Milliarden Euro jährlich entstehen der deutschen Wirtschaft an Schaden durch Cybercrime, über 80.000 Fälle werden jährlich registriert. Und das ist laut Bundeskriminalamt nur die Spitze des Eisbergs: Die Dunkelziffer sei „unvorstellbar groß", weil kein Unternehmen Interesse daran hat, dass ein IT-Sicherheitsleck oder ein Datendiebstahl bekannt wird. Schließlich wäre das massiv geschäftsschädigend.

ATTACKE DURCH DIE DATENLEITUNG
Statistisch wird alle drei Minuten in Deutschland ein Unternehmen von kriminellen Hackern angegriffen.

Trotz dieser horrenden Zahlen und des durchaus vorhandenen Problembewusstseins: Wenn es um das eigene Unternehmen geht, üben sich viele in Sorglosigkeit. „Uns betrifft das nicht", ist ein häufig gehörter Satz. Nur 34 Prozent aller Firmen halten sich überhaupt für potenziell gefährdet; nicht wenige meinen, ihr Unternehmen sei entweder zu klein oder die dort anfallenden Daten nicht interessant genug für Kriminelle.

Ein Trugschluss, denn gerade kleine und mittlere Betriebe gehören mittlerweile zu den Opfern. 46.000 Euro: Das ist der durchschnittliche Schaden, den Cyber-Kriminalität bei Unternehmen mit weniger als 500 Mitarbeitern verursacht. Die Gefahr dabei lauert nicht nur im entstandenen Schaden selbst, sondern vor allem in den Folgen: Die eigene Liquidität kann erheblich leiden, und je nach Dauer und Schwere eines Cyber-Angriffs kann dieser sogar für ein ansonsten finanziell solide aufgestelltes Unternehmen im schlimmsten Fall die Insolvenz bedeuten – aus heiterem Geschäftshimmel.



SOCIAL ENGINEERING – SCHWACHSTELLE MENSCH
Viele Betrugsszenarien der Cyberkriminellen nutzen gezielt die Gutgläubigkeit und Loyalität von Mitarbeitern aus. Regelmäßige Schulungen sollten daher ebenso Pflicht sein wie IT-Sicherheitstests.

IT-SICHERHEIT HAT AUSWIRKUNG AUF BONITÄT

„Statt Vorsorge in der IT-Sicherheit zu treffen", sagt Markus Henschel, Geschäftsführer des IT-Sicherheitsspezialisten Allgeier Core, „fokussieren sich die Unternehmen nur auf andere Gefahren wie einen Blackout der Stromleitungen." Ein großer Fehler, findet er: „Je besser die IT-Systeme eines Unternehmens geschützt sind, desto besser ist es gegen Cyber-Angriffe abgesichert", erklärt er. „Ist das hingegen nicht der Fall, kann jedes ansonsten noch so gesunde Unternehmen aus dem Nichts angegriffen, erheblich geschädigt und schlimmstenfalls in die Pleite getrieben werden."

Und nicht nur das: Schließlich bewegt sich jedes Unternehmen in einem Netzwerk aus Kunden, Lieferanten und finanzierenden Banken, die ebenso betroffen sein könnten. So können auch Probleme der Geschäftspartner die eigene Liquidität gefährden: durch ausbleibende Zahlungen, ausbleibende Aufträge oder Lücken in der Lieferkette.

„Angesichts der massiven Zunahme von Sicherheitsvorfällen ist es sehr wichtig, den IT-Sicherheitsstandard des Partner-Unternehmens einschätzen zu können", meint Henschel. Also entwickelte er mit seiner Firma das Rating-Tool „Ratingcy", das den IT-Faktor bei der Bonitätsbewertung von Unternehmen mit einschließt. Heißt also: schlechte IT-Sicherheit, schlechtere Bonität.

SICHERHEITSTESTS OFFENBAREN SCHWÄCHEN

„Ratingcy" ermöglicht es Unternehmen über ein Online-Portal, die eigene IT-Sicherheit zu überprüfen *(siehe auch Kasten auf Seite 15)*. Am Ende steht ein „Cyber Risk Score", der den aktuellen Stand der IT-Sicherheit des Unternehmens widerspiegelt. „In Verbindung mit dem durchschnittlichen Branchenwert können sich Unternehmen dann mit anderen vergleichen", erklärt Henschel. „Sie wissen damit, ob und wie stark sie ihre IT-Struktur verbessern müssen."

Ein wichtiger Baustein der Überprüfung können auch sogenannte Penetrationstests sein: Dabei werden absichtlich bestimmte, vorher definierte Systembestandteile und Anwendungen eines Netzwerks attackiert, um unautorisiert in das System eindringen zu können. „Auf Basis dieses Cyber-Sicherheits-Checks ist es möglich, geeignete Maßnahmen zu ergreifen, um die Organisation ganzheitlich besser schützen

zu können", erklärt Henschel. Von zunehmender Bedeutung ist die Social Engineering-Methode, bei der der Faktor Mensch in den Mittelpunkt des Untersuchungsansatzes gestellt und dessen Sicherheitsverhalten geprüft wird. „Ziel unserer Überprüfung kann es daher auch sein, durch Ausnutzung von Gutgläubigkeit, Hilfsbereitschaft oder auch Unsicherheit von Mitarbeitern an vertrauliche Unternehmensinformationen zu gelangen und somit bestehende Sicherheitslücken aufzuzeigen", erläutert Henschel das Vorgehen.

Erschreckend oft haben er und sein Team Erfolg – und sorgen dann meist für ungläubiges Staunen auf Seiten der Unternehmen. „Das Bild der Hacker, die nachts mit Maske kommen, ist Vergangenheit", weiß Henschel. „Heute muss durch Awareness-Trainings in Unternehmen eine nachhaltige Sensibilisierung von Mitarbeitern stattfinden." Dass es bei manchen Firmen schon an Selbstverständlichkeiten hapert, weiß Henschel aus jahrelanger Erfahrung: „Wenn ich meine Passwörter und meine wichtigsten Informationen zum IT-System nur digital dokumentiert habe, gehe ich bei einem Hackerangriff sprichwörtlich in die Knie", warnt er. Sein Tipp: Ein analoges Fax-Gerät mit eigener Leitung für die Außenkommunikation im Notfall.

VORSICHT STATT NACHSICHT

„Wer rechtzeitig und regelmäßig seine IT-Systeme überprüft und auf dem neusten Stand hält, kann Cybercrime-Angriffe gut abwehren", sagt Henschel, der aber betont, dass es einen hundertprozentigen Schutz hierbei nicht gibt. In jedem Fall, so Henschel, zahlt ein hoher IT-Sicherheitsstandard entscheidend auf den Unternehmenswert ein. Und schützt vor Gefahr und finanziellem Schaden. Damit ein Hackerangriff nicht an die Existenz geht.

EH

INFOS UND TIPPS

Viele Informationen, Zahlen, Fakten und Tipps rund um das Thema Cybercrime finden Sie auf unserer Webseite **www.eh-cybercrime.de**