„Das Wichtigste ist: Die Sicherheit zur Chefsache machen“

Der FPS-Partner zu den Cyberattacken auf Wirtschaft und Verwaltung

Börsen-Zeitung, 15.10.2022

■ Herr Hansen, Firmen und Behörden geraten zunehmend ins Visier von Cyberattacken. Der Branchenverband Bitkom geht von jährlichen Schäden allein in Deutschland von 200 Mrd. Euro aus. Mit welchen Maßnahmen können Unternehmen sich schützen?

100-prozentige Sicherheit gibt es nicht. Egal, wie viel Geld Unternehmen in technische Maßnahmen und die Sensibilisierung ihrer Mitarbeiter investieren, es gibt keine Unverwundbarkeit. Die allermeisten Angriffe werden nicht von Profis durchgeführt und könnten mit einer smarten IT-Sicherheitsstrategie verhindert werden. Das Wichtigste ist: Die Sicherheit zur Chefsache machen und ihr eine höhere Priorität einräumen.

■ Was passiert bei einem Angriff?

Meistens führen Hacker einen Ransomware-Angriff durch. Dabei wird eine Schadsoftware, beispielsweise ein als ein seriöser E-Mail-Anhang getarnter Trojaner, in ein Unternehmensnetzwerk so eingeführt, dass sämtliche Daten einschließlich operativer Steuerungs- und Betriebssysteme verschlüsselt werden. Oftmals stehen dann alle Systeme still. Zudem kopieren sich die Erpresser die Daten und drohen mit ihrer Veröffentlichung, wenn den Lösegeldforderungen nicht nachgekommen wird.

■ Wie sollte man mit Lösegeldforderungen umgehen?

Zunächst einmal: Gesetzeswidrig ist es nicht, Lösegeld zu zahlen. Insbesondere wenn keine sauberen und unverschlüsselten Back-ups vorhanden sind, muss über die Zahlung eines Lösegelds nachgedacht werden. Gleichzeitig erhöhen Lösegeldzahlungen den Anreiz für Kriminelle, weitere Taten zu begehen. Daher werden immer wieder politische Forderung erhoben, das Zahlen von Lösegeld gesetzlich zu verbieten.

Hauke Hansen

■ Wie sieht ein guter Notfallplan aus?

Ein Notfallplan enthält vor allem die zu treffenden Sofortmaßnahmen. Denn im Falle eines Angriffs kommt es darauf an, innerhalb von Minuten oder Stunden reagieren zu können, um die Folgen zu begrenzen. Ganz oben auf dem Plan steht: Wer ist zu informieren und wie passiert das, wenn E-Mail und Telefon nicht mehr funktionieren? Wer zieht den Stecker, um zu verhindern, dass der Angriff weiter um sich greift? Wie kann die Geschäftstätigkeit aufrechterhalten beziehungsweise schnellstmöglich wiederhergestellt werden?

■ In welchen Fällen tragen Versicherungen den Schaden?

Versicherungen übernehmen Schäden, die bei dem angegriffenen Unternehmen entstanden sind, etwa im Falle einer Betriebsunterbrechung oder Kosten für die Wiederherstellung der IT-Systeme; eine Cyberhaftpflichtversicherung übernimmt die Schäden, die Dritten durch den Angriff entstanden sind. Betroffene Unternehmen ohne spezielle Cyberversicherung können in ihre Haftpflichtversicherung schauen. Oftmals sind dort Cyberangriffe abgedeckt. Cyberrisiken sind schwer zu kalkulieren. Daher ist derzeit zu beobachten, dass Versicherungen vor dem Abschluss einer Police die bestehende IT-Infrastruktur genauer unter die Lupe nehmen und erhebliche Investitionen in die IT-Sicherheit fordern.

■ Welche Haftungsrisiken gehen Vorstände und Geschäftsführer ein?

Die Pflichten des Unternehmens und seiner Geschäftsleitung im Zusammenhang mit der IT-Sicherheit sind gesetzlich nicht zentral geregelt. Aber die Geschäftsleitung ist im Rahmen Ihrer Verantwortung für die Unternehmens-Compliance gehalten, geeignete Maßnahmen zu treffen, um Entwicklungen früh zu erkennen, die den Fortbestand der Gesellschaft gefährden.

■ Trifft es zu, dass gehackten Unternehmen auch noch behördliche Bußgelder drohen, sie also zweimal zur Kasse gebeten werden?

Das ist durchaus denkbar – nämlich dann, wenn die IT-Infrastruktur sich nicht auf dem Stand der Technik befunden hat. Der Gesetzgeber unterstreicht durch eine gesetzliche Regelung in der Datenschutz-Grundverordnung die Bedeutung der IT-Sicherheit und will Unternehmen durch finanziellen Druck dafür sensibilisieren. Im EU-Ausland haben Datenschutzbehörden in diesem Zusammenhang schon Millionenbußgelder verhängt. Die deutschen Aufsichtsbehörden verfolgen einen anderen Ansatz. Sie sehen in den gehackten Unternehmen zutreffenderweise die Opfer, die nicht noch zusätzlich bestraft werden sollten.

Dr. Hauke Hansen ist Partner der Kanzlei FPS und spezialisiert auf den Bereich Cybersicherheit.
Die Fragen stellte Helmut Kipp.