Bild: © Thaut Images - stock.adobe.com

Die Folgen von Cyberangriffen – ein Überblick

Datenklau mit Erpressung, Spionage oder Sabotage: Es gibt kaum noch Unternehmen in Deutschland, die von Cyberattacken verschont bleiben.

Die Digitalisierung von Geschäftsabläufen führt in vielen Fällen zu einer Reduzierung der Kosten und gleichzeitig zu einer Erhöhung der Effizienz von Produktions- und Unternehmensprozessen. Hierdurch steigt allerdings auch das Interesse an der (unberechtigten) Erlangung dieser Daten durch Dritte.

Warum ist das Thema wichtig?

In den vergangenen Jahren hat sich das Risiko für Unternehmen, Opfer eines Cyberangriffs zu werden, dramatisch erhöht. Eine aktuelle Studie[1] des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) sah etwa im Betrachtungszeitraum 2020 bis 2021 nahezu neun von zehn Unternehmen von Cyberangriffen betroffen. Die Angriffsmuster sind vielfältig und umfassen zum Beispiel „man-in-the-middle"-Angriffe, DDoS, Phishing, Spoofing, Malware oder Ransomware. Nach einer Schätzung von BITKOM belaufen sich die hierdurch entstandenen Schäden im Betrachtungszeitraum 2020 / 2021 auf über 220 Milliarden € (zum Vergleich: 2018 / 2019: „nur" 103 Milliarden €).

Wie schützt man sich?

Umfassender Schutz der IT-Infrastruktur ist kostenintensiv. Daher sollte stets vor der Einführung etwaiger Maßnahmen der Schutzbedarf der einzelnen Verarbeitungsvorgänge ermittelt werden. Hierfür kann ein IT-Sicherheitskonzept entwickelt werden, dessen Ziel es ist, die Verfügbarkeit, Integrität und Vertraulichkeit der verarbeiteten Daten sicherzustellen. Hierzu werden die verarbeiteten Daten klassifiziert und den einzelnen Schutzbedarfsklassen entsprechende technische und organisatorische Schutzmaßnahmen zugeordnet. Eine solche organisatorische Schutzmaßnahme ist etwa die regelmäßige Schulung der Mitarbeiter zur Schaffung der erforderlichen „Awareness" und zur Sicherstellung der risikoaversen Nutzung der IT-Systeme.

Was tun, wenn es zu einem Cyberangriff kommt?

Sollte es doch einmal zu einem Cyber-Angriff kommen, gilt es vor allem, zügig zu handeln. Insbesondere die folgenden Maßnahmen sollten daher in Betracht gezogen werden: Es sollten umgehend der IT-Sicherheitsverantwortliche und der Datenschutzbeauftragte informiert und in den zu bildenden Krisenstab einbezogen werden. Mit diesen ist zu eruieren, ob es durch den Vorfall zu einer Verletzung des Schutzes personenbezogener Daten kam. Sofern dies der Fall ist und sofern die Verletzung zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, ist binnen 72 Stunden nach Bekanntwerden die Verletzung bei der zuständigen Datenschutz-Aufsichtsbehörde zu melden. Sofern die Verletzung nicht nur zu einem „Risiko", sondern zu einem „hohen Risiko" führt, sind auch die betroffenen Personen unverzüglich über den Vorfall zu benachrichtigen. Unterlassene Meldungen können zu empfindlichen Bußgeldern und Schadensersatzforderungen führen, weshalb bei Unsicherheiten dringend die Hinzuziehung von auf Datenschutzrecht spezialisierten Rechtsanwälten empfohlen wird.

Bei dem Verdacht auf eine Straftat sind durch die Erstattung einer Strafanzeige auch die Ermittlungsbehörden einzubeziehen. Sämtliche Bundesländer haben hierfür Zentrale Ansprechstellen Cybercrime (kurz: ZAC) eingerichtet, die auf die Ermittlung in solchen Fällen und die krisengerechte Täterkommunikation spezialisiert sind.

Wer haftet für die Schäden des Angriffs?

Im Falle eines Cyberangriffs ist der erste Anspruchsgegner natürlich der Angreifer selbst. Diesen zu ermitteln, ist Ziel des strafrechtlichen Ermittlungsverfahrens. Bleiben die Ermittlungen erfolglos, bleibt das Unternehmen jedoch zumeist „auf seinen Kosten sitzen". Um dieses Risiko abzufedern, gibt es etwa die Möglichkeit, eine Cybercrime-Versicherung abzuschließen, wobei ein genaues Studium der Versicherungsbedingungen stets zu empfehlen ist.

Nicht zu vernachlässigen ist darüber hinaus das Risiko der direkten Inanspruchnahme der Geschäftsleitung, also zum Beispiel der Geschäftsführung einer GmbH oder des Vorstands einer AG, im Falle der unterlassenen Umsetzung gesetzlich (zum Beispiel durch die DSGVO) vorgeschriebener technischer und organisatorischer Maßnahmen.

Manuel Poncza, Rechtsanwalt,
und Tom Sänger,
wissenschaftlicher Mitarbeiter

Heuking Kühn Lüer Wojtek,
Partnerschaft mit beschränkter Berufshaftung von Rechtsanwälten und Steuerberatern,
Frankfurt am Main

[1] https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr

Kurzvortrag: Die rechtlichen Folgen von Cyberangriffen

Seit Beginn der Covid-19-Pandemie hat sich der durch Cyberangriffe entstandene Schaden noch einmal mehr als verdoppelt. Ein halbstündiger Fachvortrag mit Nachfragemöglichkeit informiert Unternehmen am Donnerstag, 25. November, ab 8.30 Uhr darüber, welche rechtlichen Konsequenzen ein solcher Angriff nach sich zieht, welche Probleme hierbei zu berücksichtigen und wie diese zu lösen sind. Referent ist Rechtsanwalt Manuel Poncza.

Der Vortrag ist Teil der Webinarreihe „Kurz mal Recht". Die Teilnahme kostet 29,00 € pro Person. Das Webinar findet über GoToMeeting statt, benötigt werden ein internetfähiges Gerät und eine Möglichkeit, den Ton abzuspielen. Anmeldungen sind über den QR-Code möglich oder bei Yvonne Sommer, Tel. 06181 9290-8411, E-Mail y.sommer@hanau.ihk.de.