Wer haftet bei Datenschutz-verstößen?

Durchschnittlich 295 Cyberstraftaten pro Tag hat das Bundeskriminalamt im vergangenen Jahr allein in Deutschland registriert – das sind insgesamt mehr als 108.000 Angriffe auf die IT-Sicherheit. Die Dunkelziffer liegt noch wesentlich höher.

Von Arne Wolff

Weltweit mussten Pipelines abgeschaltet, Schlachthöfe stillgelegt und Krankenhäuser geschlossen werden, weil es Cyberkriminellen gelungen war, Ransomware in ungenügend geschützte IT-Systeme einzuschleusen. Und nicht selten folgen solchen Attacken auch noch ein Bußgeld seitens der Datenschutz-Aufsichtsbehörden und Schadenersatzforderungen durch betroffene Kunden.

Zu professionell agieren internationale Hackerbanden, zu vielfältig sind die Angriffsvektoren, als dass man sich gegen alle Eventualitäten absichern könnte. In den genannten Beispielen wurde eine Verschlüsselungssoftware (Ransomware) ins Unternehmen eingeschleust, die Datenbestände verschlüsselt und ein Lösegeld erpresst. Zu den Kosten durch den Stillstand des Unternehmens kamen noch die Kosten für die Datenwiederherstellung – entweder durch Aufspielen eines Back-ups oder durch Zahlungen an die Erpresser.

Und allzu oft droht die Gefahr nicht einmal von außen. Ein freigesetzter Mitarbeiter macht Datenschutz-Defizite öffentlich oder eine interne E-Mail geht versehentlich an den großen Verteiler – und schon muss man der Datenschutzaufsicht Rede und Antwort stehen. Meistens resultieren Bußgelder aus Datenpannen, die der zuständigen Aufsichtsbehörde gemeldet werden und bestehende Missstände in der Datenverarbeitung offenbaren.

Neben technischen Mängeln ist es vor allem menschliches Fehlverhalten, das teure Konsequenzen hat. Da liegt der Gedanke

Bildquelle: © Photo by Bill Oxford on Unsplash

nahe, das Verursacherprinzip anzuwenden und die Person, die den Schaden verschuldet hat, finanziell in die Pflicht zu nehmen. Und tatsächlich ist das unter Umständen möglich, wobei sich die Höhe des Regresses anteilig nach der Schwere des Verschuldens bemisst. Die Verteilung der Haftung regelt das Zivilrecht – mehr Details dazu finden Sie unten.

Eine andere Möglichkeit, das finanzielle Risiko bei der Datenverarbeitung zu reduzieren, ist der Abschluss einer sogenannten Cyber-Versicherung. Während nach herrschender Meinung in Deutschland Bußgelder nicht versicherbar sind, werden aber zahlreiche andere Kosten übernommen, die infolge von Datenpannen und Cyberattacken auf ein Unternehmen zukommen können – zum Beispiel

- professionelles Krisenmanagement
- Datenwiederherstellung
- Kosten bei Betriebsunterbrechung
- Beauftragung externer IT-Forensiker
- Beauftragung von Fachanwälten zur Abwehr ungerechtfertigter Bußgelder
- Schadenersatzforderungen von Kunden
- PR/Callcenter
- Kreditschutz- und Kreditüberwachungsservices
- strafrechtliche Verteidigung

Da diese Versicherungssparte noch sehr jung ist, unterscheiden sich die Produkte je nach Anbieter teilweise sehr voneinander – also Augen auf beim Vergleichen!

Als positiven Nebeneffekt einer solchen Police kann man werten, dass die Versicherer in der Regel ein (umgesetztes) IT-Sicherheitskonzept voraussetzen und so ihre Kunden zwingen, einen gewissen Mindeststandard einzuhalten. «

Unser Autor ist Diplominformatiker (TU) und Berater für Datenschutz und Informationssicherheit bei Althammer & Kill.

Kontakt:

Sören Hartmann
Althammer & Kill GmbH & Co. KG
Roscherstraße 7, 30161 Hannover

Telefon: +49 511 330603-0
Fax: +49 511 330603-48
E-Mail: vapv@althammer-kill.de
Internet: www.althammer-kill.de

Haftet das Unternehmen oder die Mitarbeitenden?

Zum einen können die zuständigen Aufsichtsbehörden nach Art. 83 DSGVO Bußgelder verhängen, zum anderen können betroffene Personen nach Art. 82 DSGVO einen Schadensersatzanspruch geltend machen – und zwar gegenüber dem Verantwortlichen, also dem Unternehmen. Mitarbeitende können nur im Innenverhältnis mit dem Arbeitgeber für solche Verstöße haften. Das Arbeitsverhältnis ist aus rechtlicher Sicht ein Schuldverhältnis mit gegenseitigen Rechten und Pflichten. Die Mitarbeitenden treffen dabei Sorgfaltspflichten; insoweit haben sie auch die Einhaltung datenschutzrechtlicher Vorgaben zu beachten. Verstoßen Mitarbeitende nun gegen die Vorgaben und verursachen dadurch einen Schaden beim Arbeitgeber, so können auch Mitarbeitende dem Arbeitgeber gegenüber haften, und zwar je nach Grad ihres Verschuldens:

- Leichte Fahrlässigkeit: Der Mitarbeitende haftet nicht. Es geht hier um geringfügige Verstöße, die jedem Mitarbeitenden im Laufe der Zeit passieren können.
- Mittlere Fahrlässigkeit: Der Mitarbeitende haftet anteilig. Der genaue Umfang der Haftung richtet sich nach Billigkeits- und Zumutbarkeitsgesichtspunkten. Dabei werden etwa die Höhe des Schadens, der Grad des Verschuldens, das Risiko der Tätigkeit, die Höhe des Arbeitsentgelts, die Versicherbarkeit des Risikos, aber gegebenenfalls auch persönliche Umstände berücksichtigt.
- Grobe Fahrlässigkeit: Der Mitarbeitende haftet grundsätzlich voll. Eine Haftungseinschränkung ist jedoch möglich, wenn der Verdienst des Arbeitnehmers in einem deutlichen Missverhältnis zum Schadensrisiko der Tätigkeit steht. Als Haftungsobergrenze werden dabei regelmäßig drei Bruttomonatsgehälter vorgeschlagen.
- Vorsatz: Der Mitarbeitende haftet vollumfänglich.

Der Grad der Fahrlässigkeit ist immer eine Einzelfallentscheidung, denn die Gerichte berücksichtigen viele Einzelfaktoren und gewichten sie unter Umständen unterschiedlich. In einigen Sonderfällen kann der Mitarbeitende auch selbst Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO werden, etwa weil er eigenmächtig oder im eigenen Interesse handelt – dies kommt aber eher selten vor.