HSW | RECHTSANWÄLTE HARDER SEDLMEIER WEITZEL

Mandanteninformation

Haftungsrisiken nach einem Cyber-Security-Angriff

Ausgangssituation

Ein Cyber-Security-Angriff setzt Unternehmen erheblichem Stress, Aufwand und Kosten aus. Was Sie sofort nach der Entdeckung tun sollen, rät Ihnen unsere Mandanteninformation „Richtiges Handeln nach einem Cyber-Security-Angriff“. Sind alle Schäden beseitigt, das Erpressungsgeld bezahlt oder die verschlüsselten Daten aus Backups wiederhergestellt, geht der Ärger meist erst richtig los.

Die zuständige Aufsichtsbehörde hat ein Ermittlungsverfahren eingeleitet und prüft, ob durch den Angriff Ordnungswidrigkeiten begangen wurden. In der Regel droht dann ein Bußgeld. Oft herrscht verbreitet noch der Irrglaube „so teuer kann das ja nicht werden!“.

Bußgeldrahmen

Das Bußgeld nach Art. 83 Abs. 4 Buchstabe a) DS-GVO beträgt bis zu 10 Mio € bei Einzelpersonen, bei Unternehmen bis zu 2% des weltweiten Jahresumsatzes – und zwar des gesamten Konzerns, selbst wenn sich der Vorfall in einer kleinen Tochtergesellschaft zugetragen hat!

> ***Praxistipp:*** *Empfindlich ist das Bußgeldrisiko für große Unternehmen bzw. solche, die einem großen Konzern angehören. Denn Anknüpfungspunkt ist stets der weltweite Konzernumsatz.*

Wer muss das Bußgeld zahlen?

In diesem Punkt ist die DS-GVO nicht auf Anhieb verständlich: Es trifft den für die Verarbeitung der Daten „Verantwortlichen“.

Ob damit nur das Unternehmen gemeint ist oder einzelne Personen oder Geschäftsführer, war unter Juristen lange umstritten. Dann haben zwei Urteile weitgehend Klarheit geschaffen: Zunächst hatte der EuGH in seinem Urteil vom 10.7.2018 (C-25/17) geurteilt, der „für die Verarbeitung Verantwortliche“ könne eine natürliche oder eine juristische Person sein, und auch bei juristischen Personen könne es mehrere Akteure geben, so dass neben der juristischen auch natürliche Personen haften könnten.

Nachdem so die Tür geöffnet war, war es nur eine Frage der Zeit, bis ein nationales Gericht einen Schritt weiter ging. Das geschah in Deutschland 2021. Nach einem Urteil des OLG Dresden vom 30.11.2021 (4 U 1158/2) kann das Bußgeld auch direkt vom Geschäftsführer eines Unternehmens verlangt werden, und zwar neben einem oder mehreren direkt Verantwortlichen.

Jenes Urteil hat weithin Beachtung gefunden; zum Teil wird es als unangemessen kritisiert. Oft wird es so kommentiert, dass nun *jeder* Geschäftsführer eines Unternehmens persönlich Bußgelder nach der DS-GVO befürchten muss. Diese Sorge ist bislang jedoch unbegründet: In jenem Urteil ging es um einen Geschäftsführer, der persönlich an den Datenschutzverstößen beteiligt war. Falsch sind jedoch immer noch im Web anzufindende Informationen (z.B. hier: https://keyed.de/blog/haftung-bussgeld-datenschutz/), nach denen Geschäftsführer oder Vorstände nicht direkt für Bußgelder des Unternehmens haften.

Was genau ist nun der Anknüpfungspunkt für eine persönliche Haftung für Bußgelder? Verantwortlich im Sinne der DS-GVO ist jede natürliche oder juristische Person, die alleine oder gemeinsam mit anderen über die Zwecke und die Mittel der Verarbeitung von personenbezogenen Daten entscheiden kann und dies auch tut. Aus der Entscheidungsfreiheit folgern die Gerichte, dass weisungsgebundene Angestellte nicht „verantwortlich“ im Sinne der DS-GVO sind. Anders liegt dies bei Geschäftsführern, Vorständen und leitenden Angestellten wie in der Regel dem CIO eines Unternehmens.

Treffen nun die genannten Personen im Unternehmen allein oder gemeinsam eine Entscheidung, die Pflichten nach der DS-GVO verletzt, kann gegen das Unternehmen *und* die an der Entscheidung beteiligten Leitungspersonen ein Bußgeld verhängt werden.

Praxistipp:	*Bußgelder nach der DS-GVO können direkt und persönlich den Geschäftsführern, Vorständen und leitenden Angestellten (wie in der Regel dem CIO) eines Unternehmens auferlegt werden.*

Schadensersatzvorschriften

Was für die Bußgelder nach der DS-GVO gilt, ist genauso für Schadensersatzansprüche aus Art. 82 Abs. 1 DS-GVO anzuwenden. Auch diese richten sich an den für die Verarbeitung von Daten „Verantwortlichen“.

Praxistipp:	*Geschäftsführer, Vorstände und leitende Angestellte (wie in der Regel der CIO) eines Unternehmens haften direkt und persönlich auch für Schadensersatz, der nach der DS-GVO verlangt wird.*

Deshalb hat das OLG Dresden im genannten Urteil auch die Geschäftsführer zur Zahlung von Schadensersatz verurteilt.

Persönliche Haftung durch die Hintertür: Der gesellschaftsrechtliche Regress

Selbst wenn Behörden oder Geschädigte nur das Unternehmen in Anspruch nehmen, sicher wiegen können sich die an einer Pflichtverletzung beteiligten Manager noch nicht. Als Geschäftsführer oder Vorstände droht Ihnen nämlich der Regress, also die persönliche Haftung im Rückgriff des Unternehmens auf das Privatvermögen der Manager.

Liegt ein Bußgeldbescheid nach der DS-GVO vor, ist damit ein Pflichtverstoß festgestellt. Die Unternehmensleitung (also Geschäftsführer und Vorstände) müssen sich über die sie treffenden Pflichten ausreichend informieren und diese umsetzen. Verletzt die Unternehmensleitung diese Sorgfaltspflicht, macht sie sich dem Unternehmen gegenüber persönlich haftbar (der Geschäftsführer nach § 43 Abs. 2 GmbHG, der Vorstand nach § 93 Abs. 2 AktG).

Nun ist es nicht so, dass jeder Bußgeldbescheid wegen eines erfolgreichen Cyberangriffs stets zu einem Regressanspruch des Unternehmens führt. Nach dem AktG gilt zum Beispiel: „*Eine Pflichtverletzung liegt nicht vor, wenn das Vorstandsmitglied bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln*.“ In einem solchen Fall kann der handelnde IT-Vorstand sich gegen die Rückgriffshaftung erfolgreich zur Wehr setzen und das Bußgeldrisiko beim Unternehmen verbleiben.

Praxistipp:	*Geschäftsführer und Vorstände, die nach einem Cyberangriff für Bußgeld- oder Schadensersatzzahlungen persönlich in Regress genommen werden, sollten die unterschiedlichen Verschuldensmaßstäbe genau prüfen. Je nach Sachlage lässt sich der Haftungsrückgriff abwehren.*

Unser Fazit:
Bei einem erfolgreichen Cybersecurity-Angriff droht in aller Regel ein Ermittlungsverfahren durch die Datenschutzaufsicht. Der Angriff indiziert nämlich ein unzureichendes Schutzniveau für personenbezogene Daten.

Die Bußgeldrisiken sind vor allem bei Konzernunternehmen erheblich. Leitungspersonen im Unternehmen wie Geschäftsführer, Vorstände und CIOs können direkt und persönlich auf die Zahlung von Bußgeld und Schadensersatz in Anspruch genommen werden. Zusätzlich – wenn auch nicht in jedem Fall – drohen Geschäftsführern und Vorständen die persönliche Haftung gegenüber ihrem Unternehmen.

Ihre Ansprechpartner für dieses Thema:

Rechtsanwalt Bernd H. Harder
Rechtsanwalt Dr. Christian Weitzel