HSW | RECHTSANWÄLTE HARDER SEDLMEIER WEITZEL

Mandanteninformation

Richtiges Handeln nach einem Cyber-Security-Angriff

Ausgangssituation

Ein Cyber-Security-Angriff setzt Unternehmen erheblichem Stress, Aufwand und Kosten aus. Der gefühlt größte Ärger geht erst los, wenn alle Schäden beseitigt, das Erpressungsgeld bezahlt oder die verschlüsselten Daten aus Backups wiederhergestellt sind. Doch lassen Sie es gar nicht erst soweit kommen, denn sonst verschärfen sich Ärger und Kosten!

Richtiges Handeln

Das Wichtigste *sofort* nach Verdacht oder Entdeckung eines Cyber-Security-Angriffs:

> ***Praxistipp:*** *Setzen Sie sich in Abstimmung mit Ihrem Datenschutzbeauftragten sofort mit der Datenschutzaufsicht in Verbindung!*

Erfolgt diese Information verspätet, setzen Sie sich einem Verschleierungsverdacht aus. Die verzögerte Meldung erhöht deshalb bei Vorliegen einer Ordnungswidrigkeit die Bußgelder.

Steht fest, welche Daten abhandengekommen sind bzw. im Zugriff durch Hacker waren, müssen die Betroffenen davon informiert werden. Das kann einige Tausende bis Hunderttausende Informations-Schreiben erfordern. Sind z.B. Bankdaten abhandengekommen, drohen Schadensersatzforderungen der Betroffenen. Diese haben erheblichen Aufwand für die Beantragung eines neuen Kontos und die Änderung der Kontoinformationen bei allen Abbuchenden. Jener Vorgang zieht sich über Wochen und Monate hin.

> ***Praxistipp:*** *Prüfen Sie – in enger Abstimmung mit Ihrem Datenschutzbeauftragten und ggf. Datenschutzjuristen – früh und genau, welche Informationen Sie aufgrund des Vorgangs an welche Personenkreise erteilen müssen!*

Schrecken verbreitet meist schon früher die Datenschutzaufsicht. Um die Bußgelder zu minimieren, ist diese – hoffentlich – sofort in alle Maßnahmen zur Feststellung und Minimierung der Schäden eingebunden worden. Im weiteren Schriftverkehr mit der Behörde wird den Beteiligten schlagartig klar: Da läuft ein strafrechtliches Ermittlungsverfahren!

In dem Augenblick werden dem Management oft erst die beiden Seiten der Medaille „DS-GVO“ bewusst. Mental immer unter „Datenschutzrecht“ weggespeichert, hat diese EU-Verordnung zwei gleichberechtigte Schutzgegenstände: Datensicherheit *und* den Datenschutz. Datensicherheit erfordert nichts anderes als IT-Sicherheit. War ein Cyber-Angriff erfolgreich, indiziert das eine unzureichende Datensicherheit – kurz gesagt einen Anfangsverdacht.

Dann stellt sich das Management rasch die Frage: Was kann mir oder dem Unternehmen nun geschehen: Muss ich gar ins Gefängnis? Oder hafte ich mit meinem Privatvermögen?

Strafrechtlich kein Risiko

Die gute Nachricht zuerst: Niemand im Unternehmen muss eine Strafbarkeit wegen des erfolgreichen Cyber-Angriffs befürchten. Das deutsche Bundesdatenschutzgesetz enthält in § 42 zwar eine Strafvorschrift. Die droht Freiheitsstrafen bis zu drei Jahren an – allerdings nur für besonders harte Fälle der Übermittlung, Beschaffung oder Verarbeitung von „*nicht allgemein zugänglichen personenbezogenen Daten*“.

Praxistipp:	*Hacker, die sich mit einem Cyber-Angriff solche Daten erschleichen, müssen eine Freiheitsstrafe befürchten.* *Die Opfer eines Cyber-Angriffes werden indes nicht kriminalisiert.*

Ordnungswidrigkeitstatbestände

Sowohl die DSGVO als auch das BDSG enthalten eine Reihe von Ordnungswidrigkeits-Vorschriften. Bei einem Cyberangriff ist für das betroffene Unternehmen nur eine einzige davon einschlägig: Es ist Art. 83 Abs. 4 Buchstabe a) DS-GVO.

Danach handelt ordnungswidrig, wer keine geeigneten technischen und organisatorischen Maßnahmen zum Schutz der verarbeiteten personenbezogenen Daten ergriffen hat. Jede Unternehmens-IT verarbeitet personenbezogene Daten. Ein Cyber-Angriff hat fast stets einen Zugriff auf bzw. den Abfluss bzw. die Löschung von personenbezogenen Daten als Ergebnis. Ein solcher Vorfall indiziert also, dass die ergriffenen Maßnahmen nicht ausreichend geeignet waren.

Praxistipp:	*War ein Cyber-Angriff erfolgreich, indiziert das unzureichende Schutzmaßnahmen bei der IT-Sicherheit. Deshalb eröffnet die Datenschutzaufsicht in jedem Fall ein Ordnungswidrigkeiten-Verfahren und prüft, ob ein Bußgeld verhängt werden soll.*

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.*

So weit unsere Kurzinformation zum richtiges Vorgehen nach Entdeckung eines Cyber-Security-Angriffs oder auch nur des begründeten Verdachts. War der Angriff erfolgreich, werden Sie nach den Bußgeld- und Haftungsrisiken fragen. Dazu informiert Sie eine gesonderte Mandanteninformation.

Ihre Ansprechpartner für dieses Thema:

Rechtsanwalt Bernd H. Harder
Rechtsanwalt Dr. Christian Weitzel