WIE UNTERNEHMEN DIE MELDEPFLICHT ERFÜLLEN

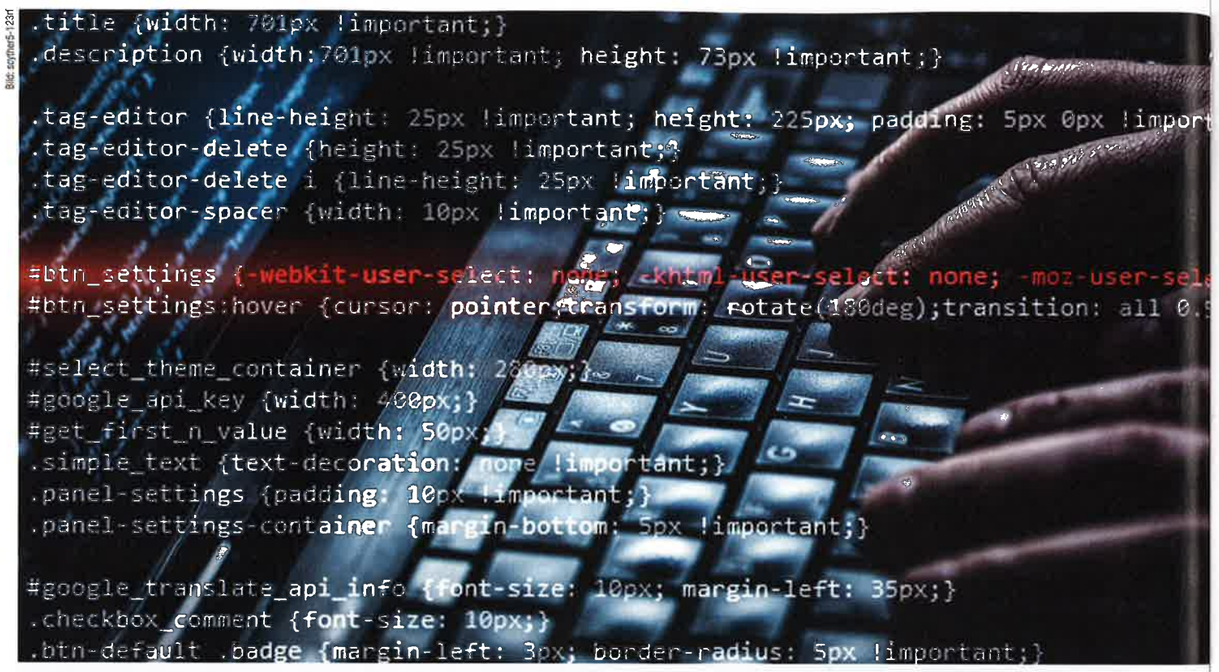

Bild: scyther5 / 123rf

Datenpannen und Cyber-Angriffe prägen heutzutage die Schlagzeilen und sind aus den alltäglichen Nachrichten nicht mehr wegzudenken. Attacken können schnell zu einem beträchtlichen Problem für Unternehmen werden. Nicht nur der Imageschaden ist enorm; auch die Kosten sind exorbitant: Wie die kürzlich durchgeführte Umfrage eines Spezialisten zeigt, kostet ein Security-Vorfall, der erst nach einer Woche entdeckt wird, ein Großunternehmen im Schnitt 1,2 Millionen US-Dollar.

Autoren: Dr. Ernst Georg Berger und Laura Hofmann **Redaktion: Axel Pomper**

➤ Unternehmen mussten zumindest datenschutzrechtlich bisher keine existenzbedrohenden Sanktionen befürchten. Doch mit Einführung der Datenschutzgrundverordnung (EU-DSGVO) am 25. Mai 2018 muss nicht nur eine Vielzahl neuer und ausführlicher Pflichten beachtet werden, auch die drohenden Strafen bei einem Verstoß sind empfindlich gestiegen. Mit Bußgeldern von bis zu 20 Millionen Euro oder bis zu vier Prozent des gesamten Jahresumsatzes des vorangegangenen Geschäftsjahres, müssen sie sich bis zum Ende der Umsetzungsfrist am 25. Mai 2018 entsprechend vorbereiten. Die Zeit läuft.

Eine dieser neuerdings strengeren und umfangreicheren Pflichten für datenverarbeitende Unternehmen besteht in der Meldung von Verletzungen des Schutzes personenbezogener Daten an die zuständigen Aufsichtsbehörden nach Artikel 33 DSGVO und die korrelierende Benachrichtigung des Betroffenen nach Artikel 34 DSGVO. Diese Pflicht ist nicht neu, doch sieht die DSGVO einige gravierende Änderungen vor. Obwohl bereits im BDSG von einer „unverzüglichen" Meldung gesprochen wurde, muss nun eine konkrete Frist von 72 Stunden eingehalten werden, die den bisherigen Interpretationsraum empfindlich einschränkt.

Unternehmen müssen also schnellstmöglich handeln, wenn ein solcher Vorfall vorliegt. Doch wen betrifft diese Meldepflicht nach Artikel 33 DSGVO überhaupt?

Betroffen sind alle Unternehmen, die personenbezogene Daten verarbeiten. Sie sind im Rechtssinne „Verantwortlicher" für den Schutz der Daten. Neben diesen echten Verantwortlichen werden nun auch Auftragsverarbeiter in die Pflicht genommen. Das sind Unternehmen, die lediglich personenbezogene Daten für ein eigentlich verantwortliches Unternehmen verarbeiten. Nach den neuen Regelungen der DSGVO gibt es nun eine gemeinsame Verantwortung („Joint Control").

Was ist zu melden?

Nicht jeder Datenschutzverstoß ist gleich ein meldepflichtiger Vorfall. Aber wie erkennt man ihn? Jegliche IT-Sicherheitsvorfälle oder Verstöße gegen eine Regelung der DSGVO könnten hierbei relevant sein, daher muss bei jeder Datenpanne, Leak oder ähnlichem Vorfall im Einzelfall geprüft werden, ob tatsächlich ein meldepflichtiger Verstoß vorliegt.

Diese Prüfung ist – spätestens nach der neuen Rechtslage – sehr ernst zu nehmen, denn eine leichtfertige und vor allem falsche Einschätzung könnte den Verantwortlichen Millionen kosten. Es muss genauestens geprüft werden, ob personenbezogene Daten betroffen sind und um welche Datenkategorie es sich handelt. Denn nur so kann eingeschätzt werden, ob ein Risiko für die Rechte und Freiheiten des Betroffenen bestehen.

Liegt ein nach Artikel 33 DSGVO meldepflichtiger Vorfall vor, muss dieser in der Meldung genauestens erläutert, eventuelle Folgen für Betroffene erörtert und die geplanten und ergriffenen Maßnahmen beschrieben werden, die das verantwortliche Unternehmen für die Handhabung des Vorfalls für angemessen hält. All dies muss innerhalb von 72 Stunden nach Feststellung der Verletzung geschehen. Eine Sachverhaltsaufklärung dürfte innerhalb einer so kurzen Frist in den meisten Fällen gerade bei geringer Erfahrung mit Meldungen an Aufsichtsbehörden kaum möglich sein; Unternehmen werden in ein datenschutzrechtlich höchst brisantes Dilemma gebracht.

Das Verhalten des Verantwortlichen ist in einem solchen Ernstfall jedoch ausschlaggebend für die Berechnung eines möglichen Bußgeldes. Die zuständige Aufsichtsbehörde beachtet bei der Berechnung nämlich viele Faktoren – insbesondere, wie sich Verantwortliche in einer solchen Situation verhalten haben und welche Sicherheitskonzepte vorlagen. Auch die Frage, wie der Vorfall der Behörde bekannt wurde, spielt später eine Rolle.

Eine Kurzschlussreaktion kann verheerend sein. Erst kürzlich verhängte die französische Aufsichtsbehörde eine Strafe in Höhe von nur 50.000 Euro gegenüber einem internationalen Autovermieter, der die Daten von 35.000 Kunden unabsichtlich auf seiner Webseite veröffentlichte. Das Unternehmen kooperierte mit den Behörden und kam mit einem blauen Auge davon. In Hinsicht auf die nun steigenden Bußgelder zeigt dieser Fall, wie wichtig eine gute Vorbereitung und eine Kooperation mit den Behörden sein können.

Daher sollten sich Verantwortliche vorbereiten. Selbstverständlich ist eine umfassende IT-Sicherheitspolitik notwendig. Es lässt sich kaum ausschließen, dass eine böswillige Attacke oder die Unachtsamkeit eines Mitarbeiters zu einer meldepflichtigen Verletzung führt. Mit zunehmenden Cyber-Attacken auf Unternehmen ist ein meldepflichtiger Vorfall nur noch eine Frage der Zeit.

Hinzu kommt, dass Verantwortliche in bestimmten Fällen nicht nur die zuständigen Aufsichtsbehörden informieren müssen, sondern ebenso die Betroffenen. An diese Benachrichtigung knüpft die EU-DSGVO gewisse Voraussetzungen, deren Einhaltung Pflicht ist. Auch wenn diese nicht innerhalb der 72-Stunden-Frist erfolgen müssen, ist Vorsicht geboten. Es bedarf Fingerspitzengefühl, Betroffene ausreichend zu informieren und nicht unnötig zu beunruhigen, um so weitere Konsequenzen zu vermeiden, die etwa eine unglücklich formulierte Meldung an einen Kunden mit sich bringen kann.

Was müssen Unternehmen also tun?

Grundsätzlich sollten Verantwortliche gewisse Mechanismen oder Regeln verbindlich einführen, die im Notfall greifen und wertvolle Zeit sparen. Zuständigkeiten müssen festgelegt und Meldepflichten organisiert werden. Ein funktionierender und vor allem schnell durchzuführender Maßnahmenkatalog ist unerlässlich. Gleichzeitig muss gewährleistet werden, dass eine fachkundige und sorgfältige Prüfung ebenso schnellstmöglich umgesetzt wird. Für manches Unternehmen kann es sinnvoll sein, den Ernstfall zu üben.

Kümmern sich Verantwortliche frühzeitig um solche Maßnahmen und können sie diese korrekt anwenden – und vor allem den Behörden gegenüber vorweisen – kann dies eventuell sogar ein drohendes Bußgeld verhindern. Allgemein gilt, dass eine umfangreiche Vorbereitung auf die neuen Pflichten und Aufgaben, die sich für Verantwortliche aus der DSGVO ergeben, unerlässlich ist. Hierbei ist für viele Unternehmen die Bestellung eines internen oder externen Datenschutzbeauftragten unabdingbar, der sich um die Erstellung eines Konzeptes kümmert. Bei den als meldepflichtig anzusehenden Datenverletzungen sollten stets erfahrene Berater eingebunden werden. Die Datenschutzbehörden werden von ihrer hinzugewonnenen Kompetenz umfassend Gebrauch machen. Darauf müssen sich die Unternehmen einstellen.

ES MUSS GENAUESTENS GEPRÜFT WERDEN, OB PERSONENBEZOGENE DATEN BETROFFEN SIND UND UM WELCHE DATENKATEGORIE ES SICH HANDELT.

Rechtsanwalt Ernst Georg Berger ist Vorstand von Clarius.Legal sowie Partner bei Schalast, Laura Hofmann ist Informationsjuristin und Datenschutzbeauftragte bei Clarius.Legal.