DATENPANNEN UND DATENKLAU – WANN MELDEPFLICHT UND WIE VORGEHEN NACH DER DSGVO

Viele Unternehmen erleiden fast täglich Datendiebstähle und Datenpannen. Doch was sollte man tun, wenn es beim Datenschutz zu einer Panne kommt? Was hat ein Unternehmen zu tun, wenn es erfahren will, ob ein Angriff auf personenbezogene Daten Ihrer IT-Infrastruktur erfolgte, der beispielweise von einem unverschlüsselten USB-Stick mit sensiblen Daten ausging?
Eine Datenpanne/Datenklau kann auch eine unbewusste Veröffentlichung von personenbezogenen Daten im Internet sein, der Zugriff nach einer Hackerattacke auf eine Datenbank, oder auch der bloße Verlust eines Laptops oder Mobiltelefons.
Die EU-Datenschutzgrundverordnung sieht vor, dass für Aufsichtsbehörden bei Datenpannen verschärfte Meldepflichten bestehen, die eine Informationspflicht gegenüber Auftraggebern verlangt. Das Unternehmen sollte in diesem Fall achtsam, schnell und juristisch korrekt darauf antworten, um juristische Nachteile zu vermeiden.

1. Datenschutzpannen und einen Datenklau schnell erkennen

Welche Zeit vergeht, in der sich ein Unternehmen einem Datendiebstahl bewusst wird? Ein Schaden durch einen Diebstahl kann begrenzt werden, wenn ein Unternehmen mögliche Vorfälle zeitnah erkennt und sofort Gegenmaßnahmen einleitet, um einen Schaden abzuwenden. Die IT-Abteilung sollte daher sensibilisiert für Auffälligkeiten sein. Es sollte kontrolliert werden, ob bei der Informationssicherheit erforderliche technische Maßnahmen im Vorfeld getroffen wurden, sodass von den zuständigen Verantwortlichen ungewöhnliche Ereignisse überprüft und wahrgenommen werden
Dabei ist zu beachten:
-Wurde bei fehlgeschlagenen Anmeldeversuchen eine Warnung erstellt, die auf unerlaubte Zugriffe des Dateisystems hindeutet? Wie wird diese Warnung im System behandelt?
-Wird der Datenverkehr einem Monitoring unterzogen? Was ist die Vorgehensweise bei Abnormalitäten im System?
-Erfolgt bei den zentralen Servern eine periodische Kontrolle des Eingangs der Daten?
-Sind bei möglichen Pannen die Meldewege eines Problems allen Mitarbeitern bekannt?
-Besteht eine regelmäßige Kontrolle der zentralen Server?
-Gibt es für den Datennotfall ein zentrales Regelungsdokument?

2. Reaktionsplan zur Wahrungsfrist

In einem zweiten Schritt sollte ein Reaktionsplan zur Bewältigung von Datenpannen geschaffen werden, der im Unternehmen bekannt ist. Dabei ist es sehr wichtig, dass die Definition des Datenschutzvorfalls daraus hervorgeht und dass bestimmte Rollen konkret Mitarbeitern zugewiesen sind. Nur so kann bei einem Datenschutzvorfall ein Data Breach Incident Team gebildet werden, welches sofortige Maßnahmen ergreift und eine möglicherweise notwendige Meldung an die betroffenen Personen und/oder Behörde vorbereitet.

3. Gesetzliche Informationspflicht nach Art. 33 und Art. 34 DSGVO

Der Artikel 33 der DSGVO sieht vor, dass bei einer Verletzung des Schutzes von personenbezogenen Daten der Verantwortliche diese aufgrund dieser Datenschutzgrundverordnung innerhalb von 72 Stunden der zuständigen Aufsichtsbehörde mitzuteilen hat. Zur Erleichterung der Mitteilung haben die Aufsichtsbehörden umfangreiche Eingabemasken eingerichtet, die online bearbeitet werden können.
Von einer Meldung ist nur dann abzusehen, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten einer natürlichen Person führt.
Bei der Verarbeitung von Daten im Auftrag hat jedoch der Auftragnehmer den Verantwortlichen unverzüglich über die Datenpanne zu informieren und den Verantwortlichen bei der Meldung der Datenpanne zu unterstützen, indem er dem Verantwortlichen die ihm zur Verfügung stehenden Informationen bereitstellt (Art.28 Abs. 3 lit. f DSGVO).

4.Vorgehen nach der Meldung

Wichtig: Keinesfalls endet der Umgang mit der Datenpanne nur mit der Meldung bei der Aufsichtsbehörde und ggfs. der Wiederherstellung des Normalbetriebs. Bereits bei der Meldung wird hier abgefragt, welche Maßnahmen zur Eindämmung des Risikos akut unternommen wurden und zukünftig werden. Teil der Dokumentation des Datenschutznotfalls ist daher auch die Aufarbeitung und das Implementieren von weiteren Maßnahmen, die einen nochmaligen Datenschutzvorfall dieser Art verhindern können.