Symbolbild: Sicherung vor Absturz

05.12.2017 11:31 CET

Umsetzung DSGVO - Noch ist Zeit für eine Absicherung vor empfindlichen Sanktionen

Die Uhr tickt. Das neue Jahr steht vor der Tür und im Mai wird es ernst mit der EU-DSGVO. Das Rauschen im Blätterwald oder der Traffic im Internet hat erhebliche Ausmaße angenommen. Doch ist das Thema so heiß, wie es gekocht wird?

Drei praxisorientierte Fragen zur EU-DSGVO an den geschäftsführenden Gesellschafter der jurcons Beratungs- und Informations GbR Hagen Albus:

Herr Albus, medial ist die EU-DSGVO massiv in Deutschland angekommen. Auch die Meldungen, dass gerade der Mittelstand nicht ausreichend vorbereitet ist, überschlagen sich geradezu. Teilen Sie diese Meinung?

Albus: Nun ja, ich würde gern eine Lanze für den Mittelstand brechen, aber leider zeichnet meine tägliche Arbeit ein anderes Bild. Besonders der Wirkungsbereich und die Höhe der Sanktionen werden oft nicht als Risikofaktoren erkannt. Stand heute gehen viele mittelständische Unternehmen davon aus, dass sie gar nicht betroffen sind und wenn doch, sind bisher verhängten Sanktionen für Datenschutzverstöße in Höhe von € 5000-10.000 auch für kleinere Unternehmen zu verkraften.

Doch ab Mai ändert sich das grundlegend. Nehmen wir als Beispiel ein Unternehmen mit 80 Mitarbeitern und einem Umsatz von vielleicht € 8.000.000. Wird hier ein Verstoß gegen Vorgaben aus der DS-GVO festgestellt, drohen dann Sanktionen in einer Höhe von bis zu 4 % des Jahresumsatzes. Das sind dann in unserem Beispiel € 320.000! Alternativ könnte auch ein Bußgeld in Höhe von bis zu € 20 Mio. verhängt werden. Ersterer Betrag ist für dieses Unternehmen sicherlich schon existenzbedrohend, zweiterer hingegen bereits existenzvernichtend.

Allerdings ist nicht zu erwarten, dass die Aufsichtsbehörden bei jedem Verstoß den verfügbaren Sanktionsrahmen gleich in voller Höhe ausschöpfen – die DSGVO kennt hierzu deutliche Differenzierungen. Das Problem an sich allerdings wird akut. Hier kann ich nur empfehlen, sich Rat einzuholen. Noch ist Zeit dazu.

Doch bevor Sanktionen verhängt werden, müssen Datenschutzverstöße durch die Aufsichtsbehörde erst einmal festgestellt werden. Bevor dies eintritt liegt die Vermutung nahe, doch erst einmal so weiter machen zu können wie bisher?

Albus: Auf den ersten Blick ist das sicher nicht ganz falsch, stellt aber durchaus ein erhebliches (finanzielles) Risiko dar. Zum einen ist zu erwarten, dass die Aufsichtsbehörden ihre Ressourcen aufstocken werden und auf der anderen Seite gibt es eine schnell zu identifizierende Schwachstelle. Ich würde ganz einfach zunächst nach dem Datenschutzbeauftragten fragen. Ich behaupte, dass viele Unternehmen das Risiko, das von der Nichtbestellung eines Datenschutzbeauftragten ausgeht, unterschätzen. Und damit sind die Sanktionen sofort real.

Datenschutz bleibt in jedem Fall Aufgabe der Geschäftsleitung, ob mit oder ohne Datenschutzbeauftragten. Und gibt es keinen Datenschutzbeauftragten, vielleicht auch, weil gar keiner bestellt werden muss, bleibt gleichwohl die Geschäftsleitung in der Pflicht. Also frage ich dann, wenn es um meine personenbezogenen Daten geht, dort nach. Die DS-GVO kennt dann einen Zeitrahmen, in dem zu antworten ist. Das erhöht natürlich den Organisationsaufwand.

Wie in vielen anderen Vorschriften wird auch beim Datenschutz auf Maßnahmen nach „Stand der Technik“ verwiesen. Können Sie an einem Beispiel erklären, was das nun konkret in der Praxis bedeutet?

Albus: Sehr anschaulich kann man das an meiner eigenen Berufsgruppe darstellen. Bekanntlich bin ich ja neben der Tätigkeit als geschäftsführender Gesellschafter der jurcons auch noch Rechtsanwalt. Rechtsanwälte gehören ebenso wie Ärzte oder Steuerberater zu einer Berufsgruppe, die einer besonderen Verschwiegenheitspflicht unterliegen. Da auch hier der Vorzug des schnellen Informationsaustausches via E-Mail genutzt wird, kann man, unabhängig von Technologien, wohl feststellen, dass unverschlüsselte E-Mails beispielsweise grundsätzlich weder dem Gebot der Verschwiegenheit noch bei der Übermittlung personenbezogener Daten dem „Stand der Technik“ aus der DS-GVO entsprechen. Bestimmte Landesdatenschutzbeauftragte haben hierzu schon klar Stellung bezogen. Nun kann sich jeder die Frage stellen, wie das persönlich gehandhabt wird. Aber auch hierfür können Lösungen gefunden werden.

Vielen Dank für das Gespräch.

Das Interview führte Andreas Liefeith von procilon.

---

internationale Standards und Vorgaben. Einige Produkte wurden u. a. nach Common Criteria EAL 4+ AVA VAN.5 (Angriffspotential hoch) evaluiert und zertifiziert. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erteilte eine Zertifizierung für die Lösung zur Langzeitarchivierung qualifiziert signierter Dokumente. Das einzigartige Produktspektrum reicht von einfacher Dateiverschlüsselung im Browser über Signaturanwendungen, Identity- & Access-Management bis hin zu kompletten Infrastrukturen für Vertrauensdiensteanbieter nach EU-eIDAS-Verordnung. Vielfältige sichere Services aus der Cloud runden das Portfolio ab.

www.procilon.de

Kontaktpersonen

Andreas Liefeith
Pressekontakt
Leiter Marketing & Unternehmenskommunikation
presse@procilon.de
034298 4878 10