Sehr geehrte Damen und Herren,
liebe Kundinnen und Kunden,

immer wieder geistern Meldungen über Sicherheitslücken und Cyberangriffe durch die Medien. Oft sind diese gespickt mit technischen Details, die man möglicherweise als „IT-Laie“ nicht versteht bzw. nicht einordnen kann. Wir wollen Ihnen zeigen, was solche Meldungen bei Ihnen auslösen sollten.

Ferner informieren wir Sie in dieser Ausgabe über den Rechtsstreit der Deutsche Wohnen SE gegen die Berliner Aufsichtsbehörde über die Rechtmäßigkeit des Bußgeldbescheides in Höhe von 14,5 Mio. EUR.

Aus der Praxis geben wir Ihnen Tipps für den unverschlüsselten Datenaustausch über E-Mail. Diese Ausgabe schließen wir mit Hinweisen zu Auswahl und Bewertung von Videokonferenzsystemen hinsichtlich deren Datenschutzkonformität.

Wir wünschen Ihnen eine informative Lektüre!

Ihr

Asmus Eggert

Inhalt

Meldungen über Cyberangriffe und Sicherheitslücken des BSI - und nun?

Regelmäßig informiert das Bundesamt für Sicherheit in der Informationstechnik (BSI) über Cyberattacken, Schwachstellen oder sonstige Risiken, die zu Schäden in Unternehmen und Behörden führen können (Systemausfällen, Datendiebstahl, Datenmanipulation etc.). Ein solches Beispiel ist die Meldung des BSI vom 05.03.2021, zuletzt aktualisiert am 17.03.2021, über als Rot (höchste Bedrohungsstufe) eingestufte Schwachstellen bei MS Exchange Servern. Die Meldung hat ein breites Medienecho erzeugt.

Reicht es nun, dass man als Verantwortlicher diese Information zu Kenntnis nimmt und darauf vertraut, es werde das eigene Unternehmen schon nicht treffen bzw. im Rahmen der regulären

Updates werde das Problem schon behoben werden? Klare Antwort: NEIN, hier muss **sofort** gehandelt werden!

Die IT-Sicherheit ist als sog. technischer Datenschutz Bestandteil der Technischen und Organisatorischen Maßnahmen (TOM) nach Art. 32 DSGVO. Danach ist bei den eingesetzten TOM der „Stand der Technik" zu berücksichtigen. Gibt es also in einem im Unternehmen eingesetzten System, Programm oder einer Anwendung Sicherheitsupdates, so wird damit der Stand der Technik angepasst. Grundsätzlich wird daraus die Verpflichtung abgeleitet, diese Updates sofort (!) zu installieren. Ferner ist zu prüfen, ob es zu einer Datenpanne gekommen ist. Ist das der Fall, sind die in der DSGVO vorgesehenen Maßnahmen einzuleiten (Meldung an die Aufsichtsbehörde, Information der Betroffenen etc.).

Praxishinweis:

- Sorgen Sie dafür, dass Sie bzw. die relevanten Stellen im Unternehmen über aktuelle Themen der IT-Sicherheit informiert sind (Newsletter etc.).
- Klären Sie bei Bedrohungslagen mit der IT (bzw. Ihrem externen IT Dienstleister) die Relevanz für Ihr Unternehmen und welche Risiken konkret bestehen. Veranlassen Sie das Abstellen der Risiken soweit nicht bereits geschehen. Dokumentieren Sie dies.
- Prüfen Sie, ob es zu einer Datenpanne gekommen ist. Falls ja, gehen Sie nach dem hierfür vorgesehen Verfahren vor.
- Bei Vorfällen mit kritischer Bedrohungslage ist zu empfehlen, auf der Internetseite der zuständigen Datenschutz-Aufsichtsbehörde nachzuschauen, ob hier Einschätzungen und Handlungsvorgaben zu finden sind.
  Im oben genannten Fall der Schwachstellen bei MS Exchange Servern haben sich die Behörden sehr schnell positioniert. Hervorzuheben ist an dieser Stelle die uneinheitliche Haltung der Aufsichtsbehörden zur Konstellation, dass es zwar zu keiner Panne gekommen ist, das Update aber verspätet installiert wurde. Einige Behörden gehen hier davon aus, dass schon diese Situation die Meldepflicht auslöst.

Verstoß gegen Datenschutz: Rechtstreit um Deutsche Wohnen geht weiter

Im Oktober 2019 hatte die Berliner Aufsichtsbehörde (BlnBDI) ein Bußgeld in Höhe von 14,5 Millionen EUR gegen die Deutsche Wohnen SE erlassen. Sie warf der Deutschen Wohnen vor, ein Archivsystem für Mieterdaten nicht DSGVO-konform geführt zu haben. Die Gesellschaft, die mit einem Bestand von rund 165.700 Einheiten zu den größten Vermietern der Hauptstadt zählt, habe darin personenbezogene Informationen wie Gehaltsbescheinigungen, Selbstauskunftsformulare, Steuer-, Sozial- und Krankenversicherungsangaben sowie Kontoauszüge gespeichert und nicht überprüft, ob dies zulässig oder überhaupt erforderlich gewesen sei.

Gegen diesen Bußgeldbescheid ist die Deutsche Wohnen gerichtlich vorgegangen. Das Landgericht Berlin hat nun am 18.02.2021 entschieden, dass Bußgelder gegen juristische Personen nur verhängt werden könnten, wenn eine nachgewiesene konkrete Handlung von Leitungspersonen oder gesetzlichen Vertreter:innen dargelegt wird, die zu dem Bußgeldtatbestand geführt hat. Das Fehlen eines solchen Nachweises sei ein Verfahrenshindernis. Als Folge hat das Gericht das Bußgeld-verfahren gegen die Deutsche Wohnen SE eingestellt, ohne sich in der Sache mit den von der Berliner Aufsichtsbehörde festgestellten Datenschutzverstößen auseinanderzusetzen. Gegen die Entscheidung des Landgerichts hat die Berliner Aufsichtsbehörde über die Staatsanwaltschaft Beschwerde eingelegt.

Praxishinweis: Der Fall ist ein guter Anlass, auf die Notwendigkeit einer funktionierenden Datenschutzorganisation hinzuweisen. Unabhängig vom schuldhaften Verhalten einzelner Personen im Unternehmen muss die Geschäftsleitung zum eigenen Schutz vor persönlicher Haftung und zum Schutz vor Haftung des Unternehmens dafür sorgen, dass sie sich kein Organisationsverschulden zurechnen lassen muss. Hätte die Berliner Aufsichtsbehörde ein Organisationsverschulden im Bußgeldbescheid festgestellt, hätte das Landgericht nämlich das Verfahren nicht eingestellt. Zur Entlastung von einem Organisationsverschulden gehört es, Verantwortlichkeiten festzulegen und Handlungsvorgaben und Regelungen zu treffen, deren Einhaltung regelmäßig geprüft werden (z.B. über Richtlinien, wie einer Datenschutz-Unternehmensrichtlinie). Werden hierbei intern Verstöße festgestellt, müssen hieraus Konsequenzen abgleitet werden. Die entscheidenden Stichworte an dieser Stelle sind: Verbindlichkeit, Nachhaltigkeit und Konsequenz!

E-Mail: Was ist zu beachten, wenn Kunden eine unverschlüsselten Datenaustausch wollen?

Briefe schreiben, ausdrucken und per Post verschicken? Das kommt heute in der geschäftlichen Kommunikation immer weniger vor. Durchgesetzt hat sich die Kommunikation per E-Mail.

Bei unverschlüsselten E-Mails besteht allerdings die Gefahr, dass übersandte Daten ohne Kenntnis von Sender:innen und Empfänger:innen von Dritten abgefangen und gelesen werden können. Es besteht zudem die Gefahr, dass Geschäftsgeheimnisse Konkurrenten auf diese Weise bekannt und gegen die korrespondierenden Parteien verwendet werden können. Ohne Verschlüsselung ist die Kommunikation per E-Mail mit dem Versenden einer Postkarte vergleichbar. Bei der Postkarte wissen alle, dass man dieses Medium nur für banale Nachrichten nutzt, wie etwa Urlaubsgrüße.

Durchgesetzt hat sich die Kommunikation per E-Mail, weil sie geringe Anforderungen hat und schnell und kostengünstig ist. Sobald jedoch personenbezogene Daten über diesen Weg verschickt werden sollen, gilt die Verpflichtung zur Wahrung der Vertraulichkeit. Der Verantwortliche muss also sicherstellen, dass die Daten Unberechtigten nicht offengelegt werden. Das kann man erreichen, indem man die E-Mails verschlüsselt versendet. Das setzt jedoch voraus, dass auf beiden Seiten, also bei beiden korrespondierenden Parteien, die Voraussetzungen für eine Verschlüsselung geschaffen wurden. D.h. beide Seiten müssen digitale Signaturen anschaffen und einrichten sowie die öffentlichen “Schlüssel“ austauschen. Das ist alles mit einem gewissen Aufwand verbunden, dem sich viele Unternehmen noch verweigern.

Wie geht man nun damit um, wenn man mit Kund:innen, Vertragspartner:innen, Mandant:innen oder Patient:innen Datenaustauschen muss und diese keine Verschlüsselten E-Mailaustausch wünschen?

Praxishinweis: Bieten Empfänger:innen keine Möglichkeit für den Austausch verschlüsselter E-Mails, die personenbezogene Daten enthalten, dann sollte man in jedem Fall Alternativen zum unverschlüsselten Versand prüfen und mit diskutieren. Zu nennen sind: die Daten in verschlüsselten oder Passwort geschützten E-Mail-Anlagen zu schicken. Wichtig ist hier, das Passwort auf einem abweichenden Kommunikationsweg zu übermitteln. Alternativ kommt eine Web-Download-Plattform in Betracht, auf der Empfänger:innen die Daten abrufen können. Die Plattform muss allerdings auch wieder zugangs- und zugriffgeschützt sein und der Download muss über eine verschlüsselte Verbindung erfolgen. Besteht auch diese Alternative nicht, bleibt in Fällen, in denen sich die auszutauschenden personenbezogenen Daten lediglich auf die empfangende Partei beziehen, ggf. der Weg, dass man sich das Einverständnis des/der Empfänger:in dazu einholt und sich so von seiner Verpflichtung gegenüber dem/der Empfänger:in entbindet. Dieses Einverständnis kann z. B. bereits in den Verträgen zwischen den Parteien verankert werden (Dienstleistungs- oder Mandantenverträge) oder gesondert eingeholt werden. Wir haben Ihnen ein Muster einer

Einverständniserklärung im Downloadbereich für Bestandskunden bereitgestellt.
Wenn Sie Unterstützung benötigen, sprechen Sie Ihren Berater gerne an.

Videokonferenzsysteme: Wie finde ich das richtige System?

Mit den Lockdowns der Covid-19 Pandemie ist der Bedarf an Video- und Webkonferenzsystemen rasant gestiegen. Die Anbieter haben rasch reagiert, sich positioniert und ihre Systeme stark ausgebaut. Das Medium wird inzwischen in fast allen Lebensbereichen, sowohl privat als auch geschäftlich, genutzt. Die Bandbreite der angebotenen Systeme ist groß und unübersichtlich.

Da bei einer Web-/Videokonferenz auch immer personenbezogene Daten verarbeitet werden (z.B. IP-Adresse, Nutzerdaten), stellt sich regelmäßig die Frage, ob und wie diese datenschutzkonform eingesetzt werden können.

Alle, die hier vor der Herausforderung stehen, sich für ein System zu entscheiden, stellen fest, dass es keine klaren Antworten bzw. verbindliche Empfehlung seitens der Aufsichtsbehörden für ein System gibt. Das liegt z.B. daran, dass die Systeme diverse Konfigurations- und Nutzungsoptionen haben und dass die Anbieter permanent an der Weiterentwicklung ihres Produkts arbeiten und das abgebildete Prüfungsergebnisse daher oft nur eine kurze Halbwertszeit hätten.

Wir haben in unserem Downloadbereich eine Checkliste eingestellt, mit der wir ausgewählte Systeme geprüft und bewertet haben.

Dieser Checkliste können Sie entnehmen, wie eine Bewertung eines Systems aussehen kann. Sie können die Tabelle also nutzen, um ein System zu prüfen, für das Sie sich interessieren. Sie ist auch geeignet, ein bereits eingesetztes System zu re-evaluieren. Die Bewertung können und sollten Sie anschließend als Dokumentation Ihrer Prüfung und Risikoeinschätzung nutzen. So kommen Sie der Dokumentationspflicht nach Art. 5 DSGVO nach. Wenn Sie Unterstützung benötigen, wenden Sie sich an Ihren Berater.

Impressum

mip Consult GmbH
Wilhelm-Kabus-Straße 9
10829 Berlin
Tel: +49 (0) 30 – 20 88 999 – 00
Fax: +49 (0) 30 – 20 88 999 – 88
Redaktion: Stefan Ax, Yanick Röhricht, Asmus Eggert

Internet: www.sofortdatenschutz.de und www.blog.sofortdatenschutz.de
E-Mail: sofortdatenschutz@mip-consult.de

Vertretungsberechtigte Geschäftsführer: Asmus Eggert, Uwe Leider
Registergericht: Amtsgericht Berlin-Charlottenburg
Registernummer: HRB 121869
USt.-Identnr.: DE249276018
Verantwortlich nach § 18 Abs. 2 MStV: Asmus Eggert