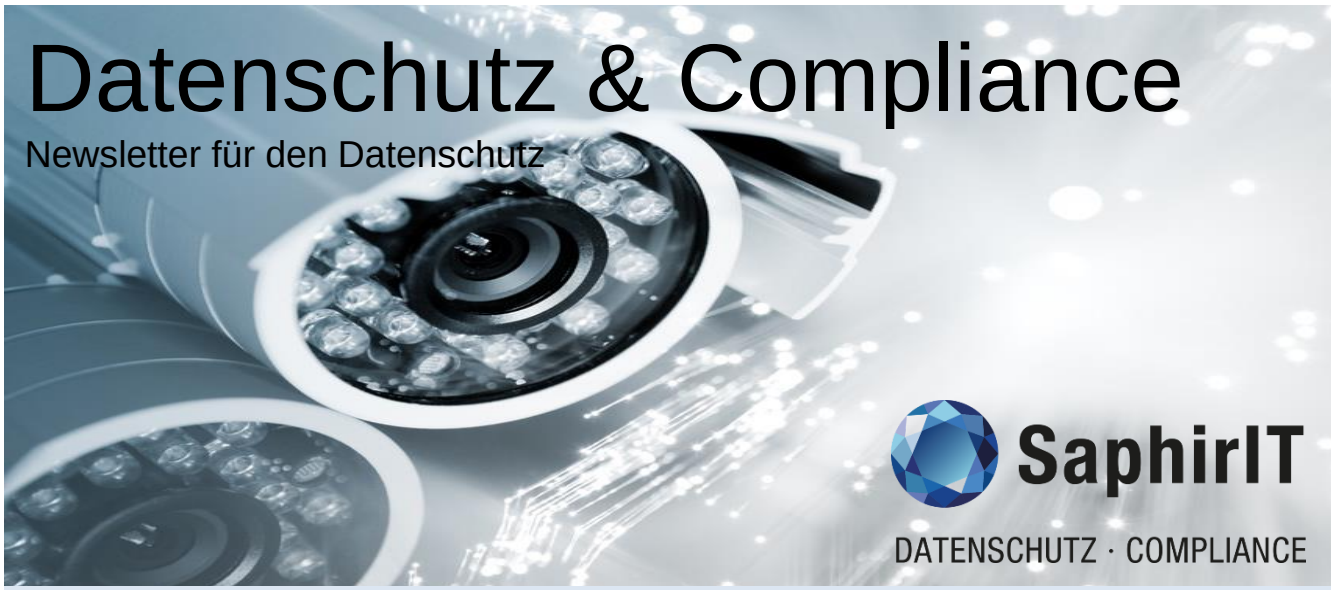

Ausgabe Dezember 2019 | Seite 141 - 144

INHALT

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren Newsletter Dezember 2019.

Wir wüschen allen unseren Leserinnen und Lesern frohe Weihnachten und einen guten Start ins neue Jahr.

Viel Spaß bei der Lektüre. Bei Fragen oder Anmerkungen sprechen Sie uns gerne an.

Mit freundlichen Grüßen
Ihre SaphirIT GmbH

Verabschiedung vom Wechselzwang für Passwörter

Bisher galt es als unbedingt notwendig, dass die Passwörter am Arbeitsplatz regelmäßig, alle 90-180 Tage, zu wechseln sind.

Diese Ansicht ist nach Aussage des Landesbeauftragten für Datenschutz und Informationssicherheit Baden-Württemberg überholt. Demnach ist der bisher gültige Zwang, Passwörter in regelmäßigen Zeitabschnitten zu ändern nicht mehr notwendig. Vielmehr solle auf die Sicherheit der Passwörter größeren Wert gelegt werden. Dieser Ansicht hat sich jetzt auch das Bundesamt für Sicherheit in der Informationstechnik angeschlossen. In seinem im Oktober neu vorgestellten „Final Draft zum IT-Grundschutz-Baustein ORP.4 Identitäts- und Berechtigungsmanagement“ heißt es unter ORP.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme [IT-Betrieb] (B): „IT-Systeme oder Anwendungen sollten nur mit einem validen Grund zum Wechsel des Passworts auffordern. Reine

zeitgesteuerte Wechsel sollten vermieden werden. Es müssen Maßnahmen ergriffen werden, um die Kompromittierung von Passwörtern zu erkennen. Ist dies nicht möglich, so sollte geprüft werden, ob die Nachteile eines zeitgesteuerten Passwortwechsels in Kauf genommen werden können und Passwörter in gewissen Abständen gewechselt werden."

Sofern es Unternehmen danach möglich ist zu überprüfen, ob das verwandte Passwort Dritten bekannt geworden ist, kann von der Festlegung eines festen Zeitintervalls zur Änderung der Passwörter daher in Zukunft abgesehen werden.

Passwörter sollten in jedem Fall regelmäßig überprüft werden. Helfen kann hierbei beispielsweise die Folgende Seite: https://checkdeinpasswort.de/.

„Whitepaper" der DSK zu technischen Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich

Die DSK (Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder) hat am 07.11.2019 ein „Whitepaper" zu den technischen Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich herausgegeben. In diesem „Whitepaper" ist ein Kriterienkatalog aufgestellt, anhand dessen geprüft werden kann, ob ein Messenger-Dienst im Gesundheitsbereich (aber auch in allen anderen Bereichen in denen mit sensiblen personenbezogenen Daten gearbeitet wird) eingesetzt werden darf.

Der berufliche oder gewerbliche Einsatz von Messenger-Diensten unterliege datenschutzrechtlichen Vorgaben, denen gängige Messenger-Dienste bisher nicht oder nur unzureichend entsprächen.

Insbesondere der Einsatz vom weit verbreiteten Dienst WhatsApp führe bei einer geschäftlichen Nutzung zu einer Reihe von Problemen, die einen datenschutzkonformen Einsatz weitestgehend ausschließen.

Thematisch ist das „Whitepaper" in vier Bereiche gegliedert:

1. Messenger-Applikation
   Hier werden unter anderem Aspekte zur Umsetzung von notwendigen Informationspflichten der Betroffenen thematisiert.

2. Kommunikation
   In diesem Bereich wird ausführlich auf die Art und Weise einer notwendigen Verschlüsselung eingegangen.

3. Sicherheit der Endgeräte
   Hier werden notwenige Maßnahmen aufgeführt die über einen wirksamen Zugriffsschutz verfügen (PIN, biometrische Lösungen).

4. Plattform/Betrieb
   Im vierten Teil wird auf die Notwendigkeit von Auftragsverarbeitungsvereinbarungen, sowie das Durchführen einer Datenschutzfolgenabschätzung eingegangen.

Inhaltlich muss bei der betrieblichen Verwendung eines Messengers das „Whitepaper“ dahingehend durchgegangen werden, ob es sich bei den einzelnen Vorgaben um eine „Soll-Vorschrift“ oder um eine „Muss-Anforderung“ handelt.

Wenig überraschend dürfte es sein, dass WhatsApp nicht für einen datenschutzkonformen Einsatz in Unternehmen geeignet ist.

Inzwischen gibt es allerdings eine Vielzahl von Messenger-Diensten die wohl den datenschutzrechtlichen Vorgaben der DSK und damit auch der Datenschutzgrundverordnung genügen.

Sollten Sie Fragen hinsichtlich eines Messengers haben, den Sie bei sich im Unternehmen nutzen können, sprechen Sie uns gerne an.

Das „Whitepaper“ der DSK können Sie unter: https://www.lda.brandenburg.de/media_fast/4055/Whitepaper_Messenger_im_Krankenhausbereich.pdf abrufen.

Knapp 10.000.000 EUR Bußgeld für 1&1 – Relevanz auch für kleinere Unternehmen

Der Bundesbeauftragte für den Datenschutz Ulrich Kelber hat auf Basis der Datenschutzgrundverordnung ein Bußgeld in Höhe von 10 Millionen Euro gegen das Telekommunikationsunternehmen 1&1 verhängt.

Hauptgrund für das hohe Bußgeld sei, dass das Unternehmen Kundendaten am Telefon nicht ausreichend geschützt habe. Es sei Anrufern problemlos möglich gewesen durch die Angabe von Namen und Geburtsdatum „weitreichende Informationen zu weiteren personenbezogenen Kundendaten“ zu erhalten, so der Bundesbeauftragte für den Datenschutz.

Das Unternehmen habe damit gegen Artikel 32 der Datenschutzgrundverordnung (DSGVO) verstoßen, da die getroffenen technischen und organisatorischen Maßnahmen nicht ausreichten, um die Verarbeitung personenbezogener Daten systematisch zu schützen.

Interessant ist, dass das hohe Bußgeld verhängt wurde, obwohl das Unternehmen sich „einsichtig und äußerst kooperativ“ gezeigt hatte. Zudem werde momentan bereits „ein neues technisch und datenschutzrechtlich deutlich verbessertes Authentifizierungsverfahren eingeführt“.

Der Bundesbeauftragte begründete das Bußgeld damit, dass der Verstoß durch das Unternehmen ein Risiko für den gesamten Kundenbestand der 1&1 dargestellt habe.

Sollten Sie bei sich im Unternehmen Kontakt zu Kunden am Telefon haben, sollten Sie einmal prüfen wie eine Authentifizierung bei Ihnen abläuft. Nach Ansicht des Bundesbeauftragten für Datenschutz dürfte jedenfalls eine Abfrage von Namen und Geburtsdatum zur Authentifizierung nicht ausreichen. Wichtig bei insbesondere besonders schützenswerten Daten → Arztpraxen, etc.

Sollten Sie diesbezüglich Fragen haben sprechen Sie uns gerne an.

Parallel zu diesem Bußgeld hat der Bundesbeauftragte ein weiteres Bußgeld gegen ein kleines Unternehmen (auch ein Telekommunikationsanbieter) verhängt. Das Bußgeld belief sich auf „nur“ 10.000 EUR. Das Bußgeld wurde verhängt, da das Unternehmen trotz mehrfacher Aufforderung seiner gesetzlichen Verpflichtung zur Benennung eines betrieblichen Datenschutzbeauftragten nicht nachgekommen war. Bei der Höhe des Bußgeldes sei berücksichtigt worden, dass es sich um ein „Kleinstunternehmen“ handelt.

Die Verhängung dieser beiden Bußgelder zeigt sehr deutlich, dass die Behörden es längst nicht mehr nur auf die „großen Unternehmen“ abgesehen haben. Ein durchaus hohes Bußgeld kann jedes Unternehmen treffen. Nicht nur aus diesem Grund sollte jedes Unternehmen ob klein oder groß alles Notwendige veranlassen um einem Datenschutzverstoß vorzubeugen und einem Bußgeld somit von vornherein aus dem Weg zu gehen.

SaphirIT GmbH
Sutthauser Straße 285
49080 Osnabrück
Geschäftsführer
Amtsgericht Osnabrück

www.saphirit.de
USt-ID-Nr. DE268765300
Frank W. Stroot
HRB 20385

Oldenburgische Landesbank AG
IBAN DE29 2802 0050 5042 8200 00
BIC OLBODEH2XXX

Telefon 0541/60079296
Telefax 0541/60079297
datenschutz@saphirit.de