UIMCommunic@tion
praxisnah.gut.informiert.

10/2021
Ausgabe für Österreich

Inhaltsverzeichnis ++ Datenschutz beim Mailversand ++ Online-Formular-Center für Informationssicherheit ++ Ohne Software-Updates drohen Strafen ++ Lieferantenbewertung ++ **Neue Covid-19-Verordnung**

Risiken erkennen und mindern: Auch beim Mail-Versand?!

Sicherheit und Datenschutz beim Mailversand unverzichtbar

Das Versenden persönlicher Daten per Mail ist in jedem Unternehmen Gang und Gäbe. Unternehmen müssen die dabei bestehenden Risiken im Datenschutz und bei der Informationssicherheit durch geeignete Maßnahmen mindern. Für Unternehmen ist insbesondere die individuelle Risikoanalyse ein geeignetes Hilfsmittel, um die richtigen Maßnahmen zu treffen.

Grundsätzlich müssen sich die Verantwortlichen im Unternehmen bei Nutzung von E-Mail-Diensteanbieter davon überzeugen, dass der Anbieter hinreichende Garantien für die Einhaltung der Anforderungen der DSGVO bietet. Neben den Risiken, die auf dem Transportweg der Mail bestehen, gilt es auch die Risiken für ‚ruhende Daten' zu beachten, die vor und nach dem Versand bestehen. Beide Risikogruppen lassen sich durch geeignete Verschlüsselungsverfahren mindern. Transport-verschlüsselungen garantieren nur ein Mindestmaß an Sicherheit auf dem Übertragungsweg. Der Schutz der Daten, auch nach dem Versand einer Mail, kann letztlich nur durch eine Ende-zu-Ende-Verschlüsselung gewährleistet werden. Ferner gilt, auch wenn die Verantwortung für Sicherheit bei derm Verseandung personenbezogener Daten per E-Mail grundsätzlich beim Sender liegt, dass auch der Empfänger geeignete Vorkehrungen zur Wahrung der Vertraulichkeit treffen muss.

Bei der praktischen Umsetzung sollten Unternehmen die konkreten Anwendungen und Geschäftsfälle in Fallgruppen mit normalen und hohen Risiken beim Empfangen und Versenden vom E-Mails einteilen.

Unternehmen, die gezielt sehr sensible Daten per Mail entgegennehmen, müssen einerseits die Voraussetzungen zum Empfang der Nachrichten über einen verschlüsselten Kanal schaffen. Um zusätzlich die Authentizität der empfangenen Nachrichten zu prüfen, empfiehlt es sich, auf eine elektronische Signatur zurückzugreifen, die den Absender verifiziert. Bei hohem Risiko sollte eine geeignete Ende-zu-Ende-Verschlüsselung zur Verfügung gestellt werden.

Beim Versand sensibler Daten ist ebenfalls eine Transportverschlüsselung obligatorisch. Auch hier sollte bei hohem Risiko neben einer qualifizierten Verschlüsselung der Datenübertragung auch eine Ende-zu-Ende-Verschlüsselung genutzt werden. Besondere Anforderungen gelten zudem beim Versand von E-Mail-Nachrichten mit geheim zu haltenden Inhalten gemäß § 203 StGB (beispielsweise Daten von Ärzten oder Rechtsanwälten). Hier muss zusätzlich sichergestellt werden, dass nur die Stellen die Nachricht entschlüsseln können, denen der ihr Inhalt der Nachricht auch offenbart werden darf.

Dies zeigt: Vor dem Ergreifen von Maßnahmen sollte stets eine Risikoanalyse oder die Klassifizierung von Informationen und Systemen stehen, um angemessene und ausreichende Maßnahmen zu ergreifen. „Es lässt sich schwer generalisieren, welche Maßnahmen in welchem Unternehmen getroffen werden sollten" erklärt der erfahrende IT-Sicherheitsfachmann und UIMC-Geschäftsführer Dr. Jörn Voßbein. „Die individuelle Risikoanalyse ist unverzichtbar." Betroffenen Unternehmen rät Dr. Voßbein, sich frühzeitig mit den Themen auseinanderzusetzen.

Neu: Online-Formular-Center jetzt auch für Informationssicherheit!

Wir haben das Online-Formular-Center ergänzt und um die Informationssicherheit erweitert. Dieser Kurs ist im **eCollege** nicht für alle User freigeschaltet. Sie haben keinen Zugang?

Also: Lizensieren Sie es jetzt, um uneingeschränkten Zugriff auf viele nützliche Formulare rundum die Informationssicherheit zu erhalten.

UIMC.austria (eine Marke der UIMC Dr. Vossbein GmbH & Co KG), Fleischmarkt 1/6/12, A-1010 Wien
Tel.: +43 1 20 5107 3383, E-Mail: consultants@uimc.at, Internet: www.UIMC.at

Ohne Software-Updates Strafen, Imageverlust und Diebstahl riskieren

Die niedersächsische Datenschutzbeauftragte hat im vergangenen Jahr Geldbußen in Höhe von 10,56 Millionen Euro verhängt. Finanzmittel, die den betroffenen Unternehmen an anderen Stellen für Investitionen fehlen dürften. Besonders ärgerlich hierbei: Die meisten Strafzahlungen sind vermeidbar. „Das Thema Datenschutz darf nicht unter Verschiedenes behandelt werden, sondern gehört in die Pole-Position eines jeden Unternehmens. Sensibilität und Ernsthaftigkeit im Umgang mit den Regeln der DSGVO sind wichtig, um das eigene Unternehmen datenschutzkonform zu gestalten und Strafen zu vermeiden“, erklärt der erfahrene Datenschutzfachmann und UIMC-Geschäftsführer Dr. Jörn Voßbein. Dazu zählen auch technisch-organisatorische Maßnahmen. Ein Beispiel: Ein Unternehmen aus dem Bereich der Arzneimittelherstellung bekam dies jetzt zu spüren: Es wurde zu einer Strafzahlung verpflichtet. Was war geschehen?

Den gesamten Beitrag finden Sie unter:
www.uimc.at/news

Outsourcing: „Vertrauen ist gut, Kontrolle ist besser“

Starke Verflechtungen prägen unser Geschäftsleben. So werden immer öfter Services an Externe ausgelagert. Von der Lohnabrechnung über Cloud- und weitere IT-Dienstleistungen bis hin zum Outsourcing von Entwicklungsarbeiten. Alle Auslagerungen haben eins gemeinsam: Wer sich eines externen Dritten bedient, muss sich über dessen Verlässlichkeit und Leistungsfähigkeit bei der Datenverarbeitung sicher sein; egal ob durch die Datenschutzgrundverordnung, durch einen Auftraggeber oder intrinsisch motiviert. Schließlich kann der Verlust vertraulicher Daten verheerende Konsequenzen für das eigene Unternehmen haben. Ganz nach dem Motto „Vertrauen ist gut, Kontrolle ist besser“ sollte eine eingehende und regelmäßige Prüfung stattfinden. Doch nach welchem Maßstab und welcher Methodik sollte man hier vorgehen? **Im März 2022 werden wir Ihnen in unserem kostenfreien web.eCollege „9 nützliche Tipps für eine Lieferantenbewertung“ vorstellen.**

Den gesamten Beitrag finden Sie unter:
www.uimc.at/news

Sie haben das letzte web.eCollege verpasst, würden aber gerne noch mehr zum Thema „Basis-Absicherung nach IT-Grundschutz“ erfahren? Dann schauen Sie sich die Unterlagen und/oder die Aufzeichnung an:

http://update.uimcollege.de

Sie können sich als Gast anmelden. Hierzu geben Sie bitte den Code ein, den Sie bei uns erfragen können.
Sofern Sie als Kunde bereits Zugangsdaten für einen anderen Kurs im eCollege haben, können Sie sich auch „selbst einschreiben“. Die Einschreibung bleibt einen Monat bestehen.

web.eCollege
kompakt praxisnah informieren

Die nächsten Termine [kostenfrei]
10.11.2021: TTDSG: Ein Kurz-Überblick und 5 Tipps für die Umsetzung
08.12.2021: 5 Normen in der Informationssicherheit und welche sind sinnvoll?
19.01.2022 5 Tipps für ein gutes Löschkonzept

Anmeldung unter www.uimc.at/webecollege

Datenschutz bei neuer COVID-19-Maßnahmenverordnung

Nach der kommenden „3. COVID-19-Maßnahmenverordnung“ der Republik Österreich gelten auch am Arbeitsort Maßnahmen, die umzusetzen sind. Insbesondere aus datenschutzrechtlicher Sicht bedeutsam sind hierzu Fragen zu Kontrollen des Dienstgebers im Hinblick auf die 3G-Regelung. **Hierüber haben wir alle Kunden ausführlich informiert.** Sie benötigen mehr Infirmationen? Dann kommen Sie auf uns zu.