Drohnen, Dienstleister und Datensicherung

Ihr Datenschutz-Info-Blatt

Ausgabe 10/2026



Liebe Leserin, lieber Leser,

moderner Datenschutz ist ohne sichere Technologie nicht mehr denkbar. Gleichzeitig bringen schnelle technologische Entwicklungen neue Risiken für die Privatsphäre mit sich. Das zeigen zum Beispiel Drohnen, die längst auch von Unternehmen eingesetzt werden. Im ersten Beitrag erfahren Sie, in welchen Bereichen sie zum Einsatz kommen und was dabei für den Datenschutz zu beachten ist.

Die wachsende technische Komplexität führt dazu, dass Unternehmen zunehmend auf IT-Dienstleister setzen. Die Verantwortung für den Datenschutz bleibt jedoch beim Unternehmen. Zudem können Schwachstellen bei Dienstleistern auch die Daten ihrer Auftraggeber gefährden, wie der zweite Beitrag zeigt.

Technik bietet aber auch neue Schutzmöglichkeiten, etwa Speichermedien, die Online-Erpresser nicht mehr verschlüsseln können. Wie der dritte Beitrag zeigt, schränkt dieser Schutz zugleich die Möglichkeiten zum Löschen der Daten ein.

Den Abschluss bildet ein Beitrag über scheinbar überholte Technologien und Verfahren, die wirksam vor den Folgen von Cyberangriffen schützen können. Es muss also nicht immer die neueste Technik sein – wohl aber eine sichere.

Ihr Frank Berns, Datenschutzbeauftragter

Abheben mit Verantwortung: Datenschutz beim Drohneneinsatz



Viele denken bei Drohnen in erster Linie an deren militärischen Einsatz, etwa im Ukraine-Krieg. Dabei gerät leicht aus dem Blick, welche wichtige Rolle Drohnen inzwischen für die Wirtschaft spielen. Ihr Einsatz wirft manchmal auch Fragen des Datenschutzes auf. Diese lassen sich mit einer sorgfältigen Planung in der Regel gut lösen.

Vielseitige Helfer im Unternehmensalltag

Nach einem Sturm gilt es, rasch zu klären, ob Gebäude Schäden erlitten haben. Ein Dach soll vermessen werden, um dort eine Solaranlage anzubringen. Ein Unternehmen möchte sein weitläufiges Firmengelände mit möglichst geringem Aufwand überwachen. All dies sind Situationen, in denen Drohnen äußerst hilfreich sein können. Sie ermöglichen einen schnellen ersten Überblick, aber auch exakte Messungen, etwa von Flächen. Kein Wunder, dass sie immer öfter zum Einsatz kommen.

Drohnen sind kein Spielzeug

Selbstverständlich gelten für den Einsatz von Drohnen gesetzliche Spielregeln. Sie finden sich vor allem im Luftrecht. Für Drohnen mit reinem Spielzeugcharakter gelten geringere Anforderungen. Ihre Reichweite ist meist gering, ihre Fähigkeiten sind es ebenfalls. Wer eine Drohne als echtes Arbeitsinstrument einsetzen will, benötigt je nach Gerät und Einsatz einen entsprechenden Kompetenznachweis – umgangssprachlich „Drohnenführerschein“ genannt. Damit dürfen Geräte mit teils beachtlichem Gewicht und ebenso beachtlichen Fähigkeiten gesteuert werden. Gerade solche leistungsfähigen Drohnen sind für Unternehmen von Interesse.

Sicherheit hat höchste Priorität

Wer im Straßenverkehr unterwegs ist, muss sich umsichtig verhalten. Schließlich soll niemand zu Schaden kommen. Das gilt ebenso für Drohnenflüge. So ist es grundsätzlich verboten, Menschenansammlungen mit einer Drohne zu überfliegen. Unter besonderen Voraussetzungen kann ein solcher Einsatz dennoch zulässig sein, etwa bei Freiluftkonzerten. Dafür gelten jedoch strenge Anforderungen an die eingesetzte Drohne und die Durchführung des Flugs.

Auch der Datenschutz fliegt mit

Selbstverständlich gilt auch beim Einsatz von Drohnen die DSGVO, sobald personenbezogene Daten verarbeitet werden. Konkret bedeutet das: Soll zum Beispiel ein Gelände vermessen werden, müssen die Verantwortlichen betroffene Personen angemessen über den Einsatz informieren. Wer sich nicht unbedingt auf dem Gelände aufhalten muss, kann es während des Drohnenflugs verlassen.

Die Bilder dürfen keine höhere Auflösung haben, als für die Vermessung erforderlich ist. Personen, die dennoch erfasst werden, sollten möglichst nur schemenhaft und nicht identifizierbar sein. Der Wunsch, eine Vermessung mithilfe einer Drohne rasch und kostengünstig durchzuführen, kann ein berechtigtes Interesse im Sinn der DSGVO darstellen. Ob dies der Fall ist, muss jedoch für den jeweiligen Einsatz geprüft werden. Die DSGVO lässt damit genügend Raum für den Einsatz dieser Technik. Wer Sicherheit und Datenschutz von Anfang an berücksichtigt, kann die Vorteile der Technik verantwortungsvoll nutzen.

Was Sie selbst beachten sollten

Setzen Sie eine Drohne nicht eigenständig für betriebliche Zwecke ein. Stimmen Sie den geplanten

Einsatz vorher mit den zuständigen Stellen im Unternehmen ab. Das gilt besonders, wenn Personen, Fahrzeuge, Gebäude oder angrenzende Grundstücke aufgenommen werden könnten. Achten Sie außerdem darauf, nur die Bilder und Daten zu erfassen, die für den vorgesehenen Zweck tatsächlich erforderlich sind.

Cyberangriff auf Dienstleister: Eigener Schutz allein reicht nicht

Datenpannen und IT-Sicherheitsvorfälle bei Dienstleistern können auch das eigene Unternehmen treffen. Beim Datenschutz muss man deshalb über die Unternehmensgrenzen hinausdenken.

Cyberangriffe treffen auch Dritte

Stellen Sie sich vor, Sie arbeiten in einem Fotostudio. Da Kundenfotos als personenbezogene Daten zu schützen sind, hat das Fotostudio eine Reihe von Schutzmaßnahmen ergriffen, um mögliche Hackerangriffe auf die Fotoarchive abzuwehren. Trotzdem erbeuten Datendieben Fotos Ihrer Kunden. Wie kann das sein? War die Datensicherheit im Fotostudio doch nicht ausreichend?

Tatsächlich kommt es nicht allein auf den Datenschutz und die Datensicherheit in dem Unternehmen an, in dem Sie arbeiten. Der Grund: Die meisten Unternehmen arbeiten mit Dienstleistern zusammen und gewähren diesen zu bestimmten Zwecken Zugriff auf Kundendaten. Das kann zum Beispiel der Fall sein, wenn Fotos von Kunden auf Tassen oder andere Gegenstände gedruckt werden. Diese Aufgabe übernimmt dann ein Dienstleister im Auftrag des Fotostudios.

Wird dieser Dienstleister erfolgreich angegriffen, können auch die Kundendaten des Fotostudios betroffen sein.

Ein Fall aus der Praxis

Genau das ist passiert: Ein technischer Dienstleister mit Sitz in Nordrhein-Westfalen wurde Opfer eines IT-Angriffs. Zahlreiche Fotografinnen, Fotografen und Fotostudios nutzen diesen Dienstleister, um Fotos für ihre Kundinnen und Kunden verarbeiten und bereitstellen zu lassen.

Die Angreifer hatten sich unbefugt Zugriff auf die Cloud-Infrastruktur des Dienstleisters verschafft. Dort stahlen sie Fotos und andere Kundendaten und löschten diese anschließend beim Dienstleister. In den Tagen nach dem Vorfall begann der Dienstleister damit, die betroffenen Fotografinnen, Fotografen und Fotostudios zu informieren. Diese mussten prüfen, welche Risiken für ihre Kundinnen und Kunden bestanden. Je nach Ergebnis dieser Prüfung mussten sie den Vorfall der zuständigen Datenschutzaufsichtsbehörde melden und betroffene Personen benachrichtigen.

Fotodienstleister sind dabei nur ein Beispiel von vielen. Dienstleister stehen besonders im Fokus von Cyberkriminellen, weil sich über ihre Systeme die Daten zahlreicher Kunden erbeuten lassen.

Unsichere Dienstleister als Hintertür

Die niedersächsische Datenschutzaufsichtsbehörde warnt ausdrücklich vor zunehmenden Angriffen auf IT-Dienstleister, da sich solche Attacken für Cyberkriminelle besonders „lohnen“: Ein einziger erfolgreicher Angriff kann zahlreiche Auftraggeber und sehr viele Menschen zugleich betreffen. Deshalb kommt den Schutzvorkehrungen von IT-Dienstleistern eine besondere Bedeutung zu. Dienstleister müssen die ihnen anvertrauten Daten durch technische und organisatorische Maßnahmen absichern und ihre Auftraggeber unverzüglich informieren, sobald sie von einem entsprechenden Vorfall Kenntnis erlangen.

Vorfälle bei Dienstleistern können immer auch das eigene Unternehmen als Auftraggeber betreffen –

unabhängig davon, ob es sich um Dienstleister aus den Bereichen Foto, IT oder anderen Bereichen handelt. Denn wer personenbezogene Daten im Auftrag verarbeiten lässt, behält eigene datenschutzrechtliche Pflichten. Das Unternehmen muss seine Dienstleister sorgfältig auswählen, die Verarbeitung vertraglich regeln und prüfen, ob ein Vorfall bei der zuständigen Datenschutzaufsichtsbehörde gemeldet werden muss.

Die niedersächsische Datenschutzaufsichtsbehörde gibt zu bedenken: „Wer die Verarbeitung personenbezogener Daten auslagert, lagert dadurch nicht automatisch die Verantwortung aus. Verantwortliche müssen ihre Dienstleister sorgfältig auswählen, gerade dann, wenn besonders sensible Daten verarbeitet werden."

Eigene Datensicherheit ist Pflicht – reicht aber nicht

Damit das Unternehmen, bei dem Sie tätig sind, den Datenschutz gewährleisten kann, müssen alle intern vorgeschriebenen Maßnahmen für die Sicherheit der Daten ergriffen und dauerhaft umgesetzt werden – technisch wie organisatorisch. Das allein reicht jedoch nicht aus. Auch Dienstleister können Zugriff auf personenbezogene Daten des Unternehmens erhalten, zum Beispiel wenn die Buchhaltung ausgelagert wird, wenn IT-Dienste genutzt oder Kundenfotos durch Dritte auf Tassen gedruckt werden.

Deshalb ist es wichtig, bei der Auswahl der Dienstleister nicht nur auf den Preis, sondern immer auch auf den Datenschutz und die Datensicherheit zu achten.

Datenschutz und Datensicherheit müssen feste Bestandteile der Einkaufs- und Auftragsbedingungen sein. Andernfalls können IT-Sicherheitsvorfälle und Datenpannen „durch die Hintertür" ins Unternehmen gelangen – etwa durch Sicherheitslücken und Datenschutzmängel bei einem Dienstleister. Auf für den Auftraggeber kann das schwerwiegende Folgen haben, darunter den Verlust von Kunden und Vertrauen, Haftungsansprüche sowie Sanktionen durch die Aufsichtsbehörden.

Was Sie selbst beachten sollten

Beauftragen Sie keine Dienstleister eigenständig mit der Verarbeitung personenbezogener Daten und übermitteln Sie ihnen keine Daten ohne vorherige Freigabe. Beziehen Sie die zuständigen Stellen für Einkauf, IT-Sicherheit und Datenschutz frühzeitig ein. Informieren Sie diese außerdem unverzüglich, wenn Sie bei einem Dienstleister einen möglichen Datenschutz- oder IT-Sicherheitsvorfall bemerken. Je früher das Unternehmen reagieren kann, desto besser lassen sich mögliche Schäden begrenzen.

Wenn Löschen nicht möglich ist: Datenträger sicher vernichten



Um sich vor Ransomware-Attacken und Online-Erpressung zu schützen, setzen Unternehmen zunehmend auf Speicherlösungen, deren Inhalte sich nachträglich nicht mehr verändern oder löschen lassen. Dieser Schutz wirft jedoch eine wichtige Frage auf: Wie lassen sich die Löschpflichten des Datenschutzes erfüllen, wenn einzelne Daten technisch nicht mehr gelöscht werden können?

Ransomware zählt zu den größten Online-Gefahren

Wenn IT-Sicherheitsbehörden in ihren Lageberichten vor zunehmenden Cyberangriffen warnen, wird eine Art von Schadsoftware immer wieder genannt: Ransomware. Diese Erpressungstrojaner versuchen, wertvolle und sensible Daten zu verschlüsseln. Die Opfer können dann nicht mehr auf ihre Daten

zugreifen, sofern ihnen kein geschütztes Backup zur Verfügung steht.

Häufig stehlen die Kriminellen die Daten zusätzlich. Sie drohen damit, diese zu verkaufen oder zu veröffentlichen, wenn das betroffene Unternehmen kein Lösegeld zahlt. Eine Zahlung bietet jedoch keine Gewähr dafür, dass die Daten tatsächlich wiederhergestellt oder nicht doch veröffentlicht werden.

Manipulationsschutz mit einem Haken

Als Reaktion auf die Ransomware-Gefahr setzen Unternehmen zunehmend Speicherlösungen ein, bei denen einmal gespeicherte Daten für einen festgelegten Zeitraum nicht mehr verändert oder gelöscht werden können. Man spricht von WORM-Speichern. Die Abkürzung steht für „Write Once, Read Many" – einmal schreiben, mehrfach lesen.

Die Idee dahinter: Auch Kriminelle sollen die gespeicherten Daten nicht mehr manipulieren oder verschlüsseln können. Dieser Schutz hat jedoch einen Haken: Solange die festgelegte Unveränderbarkeit gilt, kann auch das Unternehmen die Daten nicht ohne Weiteres löschen.

Testen Sie Ihr Wissen

Die Lösungen finden Sie am Ende des Beitrags.

Frage 1: Können Cyberkriminelle Daten auf einem ordnungsgemäß geschützten WORM-Speicher verschlüsseln, stimmt das?

1. Ja, wenn die Angreifer Zugriff auf den Speicher haben, können sie auch die dort abgelegten Daten mit Ransomware verschlüsseln.
2. Nein, die unveränderbar gespeicherten Daten können grundsätzlich nicht nachträglich verschlüsselt werden. WORM-Speicher allein reichen als Schutz vor Ransomware jedoch nicht aus.

Frage 2: Können Unternehmen Daten auf WORM-Speichern jederzeit selbst löschen, ist das richtig?

1. Ja, mit dem richtigen Passwort lassen sich die Daten jederzeit löschen.
2. Nein. Solange die festgelegte Unveränderbarkeit gilt, können die Daten grundsätzlich auch vom Unternehmen selbst nicht gelöscht werden. Deshalb müssen Löschpflichten bereits bei der Planung berücksichtigt werden.

Löschpflichten gelten weiterhin

Wer WORM-Speicher zum Schutz vor Ransomware einsetzt, muss die Löschpflichten der Datenschutz-Grundverordnung (DSGVO) von Anfang an berücksichtigen. Personenbezogene Daten dürfen grundsätzlich nicht länger gespeichert werden, als es für den jeweiligen Zweck erforderlich oder aufgrund gesetzlicher Aufbewahrungspflichten vorgeschrieben ist.

Unternehmen müssen deshalb schon vor dem Einsatz festlegen, welche Daten wie lange unveränderbar gespeichert werden dürfen. Die Dauer des technischen Löschschutzes muss zu den geltenden Aufbewahrungs- und Löschfristen passen. Entsteht dennoch eine Löschpflicht, bevor sich einzelne Daten technisch entfernen lassen, muss das Unternehmen geeignete Maßnahmen ergreifen. Je nach Speichertechnik und Schutzkonzept kann es erforderlich sein, den Zugriff auf die Daten zu sperren und den betreffenden Datenträger sicher zu vernichten.

Datenträger gehören nicht in den Müll

Unter Vernichtung versteht man die physische Zerstörung eines Datenträgers. Sie ist eine unwiderrufliche Form des Löschens und kommt sowohl bei analogen als auch bei digitalen Datenträgern in Betracht.

Datenträger mit schützenswerten Informationen, etwa personenbezogenen Daten oder Geschäftsgeheimnissen, müssen sicher vernichtet werden. Dabei ist sicherzustellen, dass sich die darauf gespeicherten Informationen nicht oder nur mit unverhältnismäßig hohem Aufwand wiederherstellen lassen.

Wie die Vernichtung technisch umgesetzt wird und ob sie intern durch eine festgelegte Stelle oder extern durch einen Dienstleister erfolgt, regelt das Entsorgungs- und Vernichtungskonzept des Unternehmens. Auf keinen Fall darf ein Datenträger einfach in den Müll gelangen – auch dann nicht, wenn er defekt oder unbrauchbar erscheint.

In der Praxis lassen sich selbst scheinbar unlesbare Speichermedien mit speziellen Methoden teilweise oder sogar vollständig auslesen. Das darf nicht passieren, wenn die darauf gespeicherten Daten gelöscht werden müssen.

Es zeigt sich: Schützt ein Unternehmen seine Daten mithilfe unveränderbarer Speicher vor Ransomware, muss es zugleich die spätere Löschung oder sichere Vernichtung einplanen. Andernfalls scheitern die Kriminellen möglicherweise an der Verschlüsselung – Datendiebe könnten aber dennoch an unzureichend entsorgte Datenträger gelangen.

Was Sie selbst beachten sollten

Entsorgen Sie betriebliche Datenträger niemals eigenmächtig oder über den Hausmüll. Das gilt auch für beschädigte Festplatten, USB-Sticks, Speicherkarten, CDs und andere scheinbar unbrauchbare Medien. Geben Sie solche Datenträger ausschließlich bei der dafür vorgesehenen Stelle im Unternehmen ab und beachten Sie die internen Vorgaben zur Aufbewahrung und Vernichtung. Fragen Sie im Zweifel nach, bevor Sie einen Datenträger entsorgen.

Die Lösungen zu den Quizfragen

Lösung zu Frage 1: Antwort 2 ist richtig. Daten auf einem ordnungsgemäß geschützten WORM-Speicher können nach ihrer Speicherung grundsätzlich nur noch gelesen, aber nicht mehr verändert werden. Eine nachträgliche Verschlüsselung wäre eine solche Veränderung. Da Angreifer die Daten unter Umständen trotzdem lesen und stehlen könnten, sind weitere Schutzmaßnahmen erforderlich.

Lösung zu Frage 2: Auch hier ist Antwort 2 richtig. Solange die festgelegte Unveränderbarkeit gilt, können die Daten grundsätzlich auch vom Unternehmen selbst nicht gelöscht werden. Wäre eine Aufhebung dieses Schutzes jederzeit mit einem einfachen Passwort möglich, könnten Angreifer versuchen, dieses Passwort zu erbeuten. Unternehmen müssen deshalb schon vor dem Einsatz festlegen, wie lange Daten unveränderbar gespeichert werden dürfen und wie sie die Löschpflichten anschließend erfüllen.

Offline-Backups: Bewährter Schutz statt Technik von gestern

So manches Unternehmen setzt zur Sicherung seiner Daten inzwischen wieder auf ein „Offline-Backup“. Dazu speichert es wichtige Daten beispielsweise mindestens einmal täglich auf externen Festplatten. Diese werden anschließend sicher verwahrt und haben keinerlei Verbindung zu einem Netzwerk. Das hat einen ernsten Hintergrund, den Sie kennen sollten.

Datennetze sind unverzichtbar

Datennetze unterschiedlichster Art bilden das Nervensystem, wenn nicht sogar das Nervengeflecht aller modernen Unternehmen. Das gilt für firmeninterne Netze ebenso wie für Verbindungen mit dem öffentlich zugänglichen Internet. Hinzu kommen nicht öffentliche Netzwerke, die beispielsweise Unternehmen

innerhalb desselben Konzerns miteinander verbinden. Ohne Cloud-Lösungen könnten viele Unternehmen kaum noch arbeiten. Der Einsatz von KI-Systemen steigert die Bedeutung von Datennetzen zusätzlich.

Doch jedes Netz kann zum Einfallstor werden

Die enorme Nützlichkeit von Datennetzen ist allerdings nur die eine Seite der Medaille. Die andere: Grundsätzlich kann jedes Datennetz zum Einfallstor für Schadsoftware werden. Zahlreiche Unternehmen haben bereits schlimme Erfahrungen mit Ransomware gemacht. Hat sich eine solche „Erpressersoftware“ erst einmal in einem IT-System ausgebreitet, sind die Folgen meist dramatisch. Die Schadsoftware verschlüsselt alle Daten, auf die sie zugreifen kann, und macht sie dadurch unbrauchbar. Das kann dazu führen, dass sich in einem Firmengebäude keine einzige Tür mehr öffnen lässt. Im schlimmsten Fall – und dieser tritt keineswegs selten ein – steht das gesamte Unternehmen still.

Im Ernstfall zählt ein sauberes Backup

In einer solchen Situation stellt sich die Frage, wie alles wieder in Gang kommen soll. Von zentraler Bedeutung sind dabei Datenbestände, die nachweislich nicht von der Schadsoftware betroffen sind. Bei Daten, die ständig in ein Netzwerk eingebunden sind, lässt sich dies kaum mit hundertprozentiger Sicherheit garantieren. Das gilt trotz aller Sicherheitsmaßnahmen, um die sich selbstverständlich jedes Unternehmen bemüht. Denn zwischen den Angreifern, die beispielsweise Ransomware einsetzen, und den Verteidigern aufseiten der Unternehmen findet ein ständiger Wettlauf statt. Dabei gelingt es den Angreifern leider immer wieder, zumindest zeitweise die Oberhand zu gewinnen.

Praxisfälle zeigen das Risiko

Was das bedeuten kann, musste beispielsweise eine sehr große Arztpraxis in Brandenburg erleben. Die Praxis betreute ständig fast 8.000 Patientinnen und Patienten und wurde Opfer einer Ransomware-Attacke. Die Kriminellen verschlüsselten den gesamten Datenbestand der Praxis von etwa 75 Gigabyte. Zwar gab es drei Festplatten, die als Sicherungsmedien dienten. Zum Zeitpunkt des Angriffs waren jedoch alle drei gleichzeitig an das IT-System angeschlossen, dessen Daten sie sichern sollten. Deshalb konnte die Ransomware auch auf diese Festplatten zugreifen und die dort gespeicherten Daten verschlüsseln. Im Ergebnis gab es keine unverschlüsselte Kopie mehr, die sich hätte zurückspielen lassen. Die Daten der Praxis waren unwiederbringlich verloren.

Ein weiteres Beispiel ereignete sich laut Presseberichten in Aschaffenburg. Ein Textilunternehmen wurde Opfer einer Ransomware-Attacke und konnte keine Aufträge mehr ausführen. Auch die Kommunikation mit den Kunden war kaum noch möglich. Am Ende stellte das Unternehmen einen Insolvenzantrag. Ob es sich davon wieder erholen kann, war zunächst offen.

Die 3-2-1-Regel bleibt aktuell

Die klassische „3-2-1-Regel“ für Backups gibt es seit vielen Jahren. Sie besagt: Von wichtigen Daten sollten insgesamt drei Exemplare vorhanden sein – das Original und zwei Sicherungskopien. Diese sollten auf mindestens zwei unterschiedlichen Arten von Speichermedien liegen. Eine Kopie sollte räumlich getrennt an einem anderen Standort aufbewahrt werden. Besonders wirksam gegen Ransomware ist eine Sicherung, die nicht dauerhaft mit dem Netzwerk verbunden ist.

Das wirkt auf manche fast schon antiquiert. Doch dieser Eindruck täuscht. Den Wert dieses Vorgehens zeigt der Ernstfall: Sollte es notwendig sein, ein oder mehrere Netze vollständig neu aufzubauen, stehen aktuelle oder zumindest weitgehend aktuelle Daten zur Verfügung, auf die die Schadsoftware nicht zugreifen konnte. Sie bilden die Grundlage dafür, dass das Unternehmen seinen Betrieb wieder aufnehmen kann.

Auch Behörden empfehlen Offline-Backups

Wer knappe Merksätze schätzt, wird beim Bundesamt für Sicherheit in der Informationstechnik (BSI) fündig: „Die Daten müssen in einem Offline-Backup gesichert werden.“ Das BSI empfiehlt Offline-

Backups ausdrücklich als Schutzmaßnahme gegen Ransomware. Auch Datenschutzaufsichtsbehörden betonen die Bedeutung sicherer und vom Netzwerk getrennter Datensicherungen.

Wenn Ihr Unternehmen dieser Empfehlung folgt, setzt es also keineswegs auf eine überholte Technik. Vielmehr ergreift es eine bewährte Schutzmaßnahme, die im Ernstfall entscheidend für die Wiederherstellung der Daten und die Fortführung des Betriebs sein kann.

Was Sie selbst beitragen können

Halten Sie sich an die internen Vorgaben zur Datensicherung und speichern Sie wichtige betriebliche Daten ausschließlich an den dafür vorgesehenen Orten. Schließen Sie keine privaten oder nicht freigegebenen Speichermedien an betriebliche Geräte an. Melden Sie verdächtige Vorgänge oder mögliche Sicherheitsvorfälle unverzüglich an die zuständige Stelle in Ihrem Unternehmen.

Impressum
Redaktion:
Frank Berns, Datenschutzbeauftragter, Geschäftsführer
Anschrift:
Konzept 17 GmbH
Westring 3
24850 Schuby
Amtsgericht Flensburg: HRB 12329
Telefon: 0049 4621 5 30 40 50
E-Mail: mail@konzept17.de