AUSGABE 03

IT insider

TECHNIK. BUSINESS. TRENDS.

IT-SUPPORT

Daten – das Öl des 21. Jahrhunderts?

IT-INFRASTRUKTUR

Herr der Datenflut werden
Immer mehr Daten werden tagtäglich in Unternehmen generiert. Wie lassen sie sich verwalten?

IT-SICHERHEIT

Kein Backup? Kein Mitleid.
Daten dürfen auf keinen Fall verloren gehen. Ein zuverlässiges Backup-Management hilft dabei.

IT-SICHERHEIT

Daten im Visier von Cyberkriminellen
Cyberkriminelle haben Daten als perfektes Druckmittel entdeckt. Schützen Sie Ihr Unternehmen!

IT-SERVICE .NETWORK

Sehr geehrte
Damen und Herren,
liebe Geschäftspartner,

mehr als die Hälfte der Unternehmen in Deutschland gibt an, dass die Corona-Krise die Einbindung und Nutzung von Daten in Unternehmensprozesse verstärkt hat. Durch die Auswirkungen der Pandemie auf die Wirtschaft hat sich gezeigt, dass Unternehmen die neuen Möglichkeiten des Datenzeitalters nutzen müssen, wenn sie langfristig überleben und im Wettbewerb bestehen wollen. Und es hat sich außerdem sehr deutlich gezeigt, dass eine am Geschäftsziel ausgerichtete Datenstrategie die Entscheidungsfindung verbessern, die Performance steigern und maßgeblich zu Wettbewerbsvorteilen beitragen kann.

Nachdem wir uns bereits mit den ersten beiden Ausgaben des ITinsiders und den Schwerpunkten auf das mobile Arbeiten und die Digitalisierung ganz nah am Zeitgeschehen bewegt haben, wollen wir es mit dieser dritten Ausgabe – der ersten im Jahr 2021 – genauso halten und das Thema Daten als Leitthema in den Fokus rücken. Sollten Sie unser Magazin erstmals kennenlernen, lassen Sie uns noch einmal kurz die Intention dahinter erläutern: Mit dem ITinsider beleuchten wir IT-Themen, die für kleine und mittelständische Unternehmen relevant sind – und damit auch für Sie! Und eine kurze Notiz am Rande: Sollten Sie Interesse an den ersten beiden Ausgaben haben, melden Sie sich bei uns, denn dann stellen wir sie Ihnen gern digital bereit.

Aber zurück zu dieser Ausgabe. Zuerst werden wir klären, wieso Daten überhaupt so wichtig sind und wie es dazu kommt, dass sie als das »Öl des 21. Jahrhunderts« gelten. Dann steigen wir tiefer ein. Wie können Unternehmen der Datenflut Herr werden, die immer höhere Wellen schlägt? Wie sollten Daten am besten gespeichert werden – auf dem Server, in der Cloud oder beides? Wie steht es aktuell um den Datenschutz? Welche Gefahren drohen in Bezug auf Unternehmensdaten? Und welche (Zukunfts-)Visionen gibt es für die Datennutzung – falls sie noch nicht Realität sind.

Auf viele dieser Fragen wird Ihnen dieses Magazin erste Antworten liefern. Aber es gilt wieder einmal: Letztendlich muss das Thema Daten für jedes Unternehmen individuell betrachtet werden. Sie benötigen dabei Unterstützung? Dann stehen wir Ihnen als kompetenter IT-Dienstleister wie immer gern zur Verfügung. Wir wünschen Ihnen viel Spaß bei der Lektüre!

Ihr Systemhaus

INHALT

IT-SUPPORT

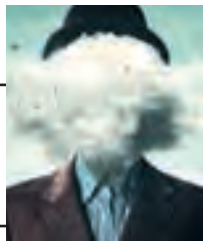
Daten – das Öl des 21. Jahrhunderts?
Daten haben eine immer größere Bedeutung. Aber warum genau gelten sie als so wertvoll?

04 | 05

IT-INFRASTRUKTUR

Data Storage – Cloud oder eigener Server?
Daten lassen sich klassisch auf dem eigenen Server oder in der Cloud speichern. Aber was macht Sinn?

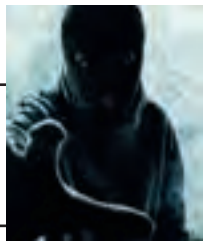
08 | 09



IT-SICHERHEIT

Daten im Visier von Cyberkriminellen
Cyberkriminelle haben Daten als perfektes Druckmittel entdeckt. Schützen Sie Ihr Unternehmen!

12 | 13



IT-SUPPORT

Daten weg – und jetzt?
Wichtige Daten sind Ihnen verloren gegangen? Vielleicht hilft Ihnen eine Datenrettung aus der Patsche.

16 | 17

IT-INFRASTRUKTUR

Herr der Datenflut werden
Immer mehr Daten werden tagtäglich in Unternehmen generiert. Wie lassen sie sich verwalten?

06 | 07

IT-SICHERHEIT

Datenschutz: Bleiben Sie DSGVO-konform!
Auch die DSGVO hat beim Thema Daten ein Wörtchen mitzureden. Was sind die Herausforderungen?

10 | 11

IT-SICHERHEIT

Kein Backup? Kein Mitleid.
Daten dürfen auf keinen Fall verloren gehen. Ein zuverlässiges Backup-Management hilft dabei.

14 | 15

IT-INFRASTRUKTUR

Big Data & Analytics – eine Zukunftsvision?
Mit den richtigen Analyseverfahren lassen sich Daten noch besser nutzen. Wie sieht die Lage aktuell aus?

18 | 19

IMPRESSUM

Herausgeber
SYNAXON AG | Falkenstraße 31 | D-33758 Schloß Holte-Stukenbrock
Telefon 05207 9299 – 200 | Fax 05207 9299 – 296
E-Mail info@synaxon.de | www.synaxon.de
Redaktion
André Vogtschmidt (V.i.S.d.P.), Janina Kröger
Ansprechpartner
André Vogtschmidt | andre.vogtschmidt@synaxon.de

Konzept / Gestaltung
Mirco Becker
Druck
Wentker Druck GmbH | Gutenbergstraße 5 – 7 | 48268 Greven
www.wentker-druck.de

Stand 04/2021. Irrtümer und Druckfehler vorbehalten. Bildnachweise stock.adobe.com: # ©;

Daten – das Öl des 21. Jahrhunderts?

Vielleicht haben Sie diese Aussage auch schon gehört: Daten sind das Öl des 21. Jahrhunderts. Sie treiben inzwischen die Maschinerie eines jeden Unternehmens an und sprudeln aus vielen verschiedenen Quellen. Sie nützen aber herzlich wenig, wenn sie nicht aufbereitet oder – um im Sprachbild zu bleiben – raffiniert werden. Eine Einführung zum Thema Daten.

Daten sind Treibstoff für Unternehmen

Einen Tag lang ohne jegliche Daten auskommen – wäre das in Ihrem Unternehmen noch denkbar? Würde der Betrieb problemlos weiterlaufen, wenn Ihnen keinerlei Kundendaten zur Verfügung stehen? Wenn Informationen zu Absprachen, Verträgen oder Projekten nicht aufgerufen werden können? Wenn weder Sie noch Ihre Mitarbeiter auf die E-Mail-Postfächer zugreifen können? Ohne die Abläufe in Ihrem Unternehmen zu kennen, ist die Antwort wohl diese: Nein, vermutlich nicht.

Man könnte also sagen, dass Daten inzwischen der Treibstoff für einen Großteil der Geschäftsprozesse in einem Unternehmen sind. Und ohne diesen Treibstoff kommt nichts – oder zumindest so gut wie nichts – in Gang. Je nach Branche trifft diese Aussage wohl in einem unterschiedlichen Maße zu. Aber unabhängig davon, ob es sich um einen kleinen oder mittelständischen Betrieb, eine Rechtsanwaltskanzlei oder eine Arztpraxis handelt, ist an dieser Tatsache nichts mehr zu rütteln: Die Abhängigkeit von einer ständigen Datenverfügbarkeit ist in diesen digitalen Zeiten enorm. Und daran wird sich auch in Zukunft höchstwahrscheinlich nichts mehr ändern.

So wertvoll wie Öl

Die Konsequenz daraus ist, dass Daten von unschätzbarem Wert sind – eben genau wie Öl. Denn: Wenn der Datenzugriff problemlos funktioniert und der Datenfluss im Unternehmen reibungslos verläuft, ist die Grundlage für funktionierende Geschäftsprozesse geschaffen und der wirtschaftliche Erfolg kann wiederum darauf aufbauen. Dabei sind Daten selbstverständlich kein Garant für hohe Gewinne. Sie sorgen aber dafür, dass Geschäfte überhaupt abgewickelt und Umsätze erzeugt werden können.

Und nicht nur das. In Ihren Daten steckt der gesamte Wissenspool Ihres Unternehmens. Jede Kommunikation, die Sie jemals mit internen und externen Kontakten geführt haben, jedes Projekt, das Sie umgesetzt haben, und jede Innovation, die Sie entwickelt haben, lässt sich irgendwo wiederfinden. Auf den Punkt gebracht: Das gesamte Know-how und die gesamte Expertise stecken in Ihren Unternehmensdaten. Aber das ist nicht der einzige Grund, weshalb Daten als so wertvoll wie Öl gehandelt werden.

Aus den Daten Lehren ziehen

Aus den im Unternehmen vorhandenen Daten lassen sich nämlich auch sehr viele Lehren für zukünftige Geschäftsentscheidungen ziehen. Zuerst ein ganz praktisches Beispiel: Sie haben ein Projekt geplant und durchgeführt und es ging in die Hose. Oder Sie haben ein neues Produkt entwickelt, letztlich hat es aber nicht so funktioniert, wie gedacht. Durch die Dokumentation all dessen können Sie aus Ihren Fehlern lernen und das Produkt weiterentwickeln, bis es zum Erfolg wird.

Eine Studie nennt dazu eine interessante Information: Bei Unternehmen mit einer ausgereiften Datennutzung ist die Wahrscheinlichkeit zehn Mal höher, dass sie mehr als 20 Prozent ihres Umsatzes mit neuen, innovativen Produkten und Services erzielen – nämlich weil sie vorhandene Daten auswerten, gezielt für ihre Entscheidungen nutzen und dadurch ihren vollen Wert ausschöpfen. Lesen Sie dazu auch den Beitrag »Big Data & Analytics« auf den Seiten 18/19. Dieser geht auf die Datenanalyse noch genauer ein.

Daten sprudeln aus vielen Quellen

Jeden Tag entstehen in Unternehmen neue Daten – und sprudeln dabei sozusagen aus vielen Quellen. Und darum hinkt der Vergleich mit Öl auch etwas. Denn während der Rohstoff Öl eine endliche Ressource ist, sagen die Zukunftsprognosen immer größere Datenberge voraus, die sich immer schneller auftürmen. So hat sich die Anzahl digitaler Informationen seit 2005 alle zwei Jahre verdoppelt. Setzt sich dieser Trend so fort, könnten allein im Jahr 2025 weltweit 175 Zettabyte an Daten erzeugt werden. Das Datenzeitalter ist definitiv eingeläutet.

Aber wie können Unternehmen mithalten? Wie lassen sich aus den Mengen von Daten genau die Informationen herausfiltern, die gerade benötigt werden? Einerseits gibt es inzwischen verschiedene Datenanalyse-Tools, die dabei helfen. Andererseits sollte jedes Unternehmen für sich eine individuelle Datenstrategie entwickeln. So eine Datenstrategie ist allerdings ein ziemliches Brett. Nicht nur Datenverwaltung und Datennutzung sind darin festzulegen; vielmehr sollten auch Datenspeicherung und Datensicherung darin bestimmt werden. Wie? Das erklären wir Ihnen im folgenden Beitrag.

Herr der Datenflut werden

Fast die Hälfte der in einer Studie befragten Mittelständler gibt an, dass das Datenvolumen in ihrem Unternehmen schon jetzt so schnell ansteigt, dass es nicht mehr mit der Entwicklung Schritt halten kann. Bei vielen von ihnen taucht daher die Frage auf: Wie können wir der Datenflut Herr werden?

Daten – das Thema wird immer komplexer

Haben Sie schon einmal versucht, sich in das Thema »Daten« einzuarbeiten? Falls ja, haben Sie vermutlich diese Erfahrung gemacht: Es ist ein schwieriges Unterfangen. Das ist aber eigentlich auch nicht verwunderlich. Denn: Mit dem rasanten Wachstum des Datenvolumens geht ein ebenso rasanter Anstieg an Herausforderungen einher. Und daher ist es genauso wenig verwunderlich, dass sich viele kleine und mittelständische Unternehmen zunehmend überfordert fühlen.

Dabei hat alles recht einfach begonnen: mit der elektronischen Datenverarbeitung (EDV). Kundendaten konnten damit in Datenbanken erfasst werden, die Mitarbeiter konnten sie verwalten. Mit der Zeit wurden die Aufgaben dann aber komplexer. Immer mehr Mitarbeiter sollten Daten finden und möglichst zeitgleich darauf zugreifen können; gleichzeitig sollten Datenverluste durch Hardware-Defekte oder falsche Bedienung verhindert werden; und dann wollte auch noch der Datenschutz ein Wörtchen mitreden. Durch die neuen Anforderungen entstand schließlich eine neue Disziplin: das Daten-Management.

Was fällt unter Daten-Management?

Zum Daten-Management gehören jede Menge Prozesse – angefangen beim Erheben der Daten über ihre Ablage und Archivierung bis hin zur Löschung. Das heißt: Es wird der gesamte Lebenszyklus von Daten betrachtet, weshalb vom Data Life Management (DLM) die Rede ist. Sicherheit und Schutz der Daten haben dabei immer höchste Priorität. Im Groben läuft das Daten-Management wie folgt ab:

1. Datenerhebung

Die Datenerhebung wird durch die Faktoren Datensparsamkeit und Datenqualität bestimmt. Festgelegt durch die europäische Datenschutzgrundverordnung (DSGVO) gilt, dass nur die nötigsten Informationen gesammelt werden dürfen und bei personenbezogenen Daten die Einwilligung der Betroffenen zur Datenverarbeitung vorliegen muss. Zudem sollte die Erfassung von Daten sorgfältig und im tatsächlich benötigten Format erfolgen, um spätere Nachfragen, Nachbearbeitungen und/oder fehleranfällige Konvertierungen von vornherein zu vermeiden.

2. Datenspeicherung

Entscheidend ist neben dem Speicherformat der Speicherort. Unternehmen müssen festlegen, ob sie ihre Daten lokal oder in der Cloud speichern wollen – oder beides kombinieren (sie dazu S. 8/9). Dabei sind sowohl Datenschutz als auch Datensicherheit zu berücksichtigen. Daten sollten vor Verlust, ungewollter Veränderung und unberechtigten Zugriffen geschützt sein. Um dies zu gewährleisten, sind

Arten des Daten-Managements

- **Enterprise Resource Planning Systems (ERP):** Ein ERP-System erfasst und berücksichtigt sämtliche Ressourcen eines Unternehmens, darunter Personal, Arbeitsmittel und Material. Bekannte Hersteller von ERP-Lösungen sind SAP, Sage, Oracle und Microsoft.

- **Master Data Management (Zentrale Stammdatenverwaltung):** Mit dem Master Data Management lassen sich Kerndaten eines Unternehmens – beispielsweise Mitarbeiterdaten und Kundendaten – zentralisieren und überarbeiten. Ziele sind eine einheitliche Datenqualität und daraus resultierend eine bessere Nutzbarkeit. Einige ERP-Systeme beinhalten diese Funktion bereits.

- **Content-Management-Systeme (CMS):** Kern ist vor allem das Informationsmanagement. Das CMS kann zum Beispiel ein zentrales Intranet im Unternehmen sein. Oft lassen sich auch Aufgaben wie das Formular-Management oder Datenbanken integrieren.

- **Dokumenten-Management-Systeme (DMS):** Das Dokumenten-Management ist ein Teilbereich des Daten-Managements. Formulare werden bereitgestellt, Ablage und Archivierung darüber ausgeführt.

eine Rechteverwaltung und eine Verschlüsselung notwendig. Regelmäßige Updates und Backups, sichere Passwörter, Virenschutz und Firewall sorgen zudem für Datensicherheit.

3. Datenarchivierung
Für Unternehmen gibt es inzwischen eine gesetzliche Pflicht zur Aufbewahrung bestimmter Daten. Darunter fallen beispielsweise Rechnungen und Steuerunterlagen, die im Fall einer Steuerprüfung vorzulegen sind. Sie werden vielleicht aktuell nicht benötigt, sind aber im Archiv aufzubewahren. Die Datenarchivierung muss daher grundsätzlich Bestandteil eines Daten-Management-Konzepts sein.

4. Datenlöschung
Werden Daten nicht mehr benötigt und unterliegen sie nicht der Aufbewahrungspflicht, sollten sie gelöscht werden. Andernfalls kommt es zu ungewollten Datenbergen, die unnötig Speicherressourcen belegen. Vor allem personenbezogene Daten sind sicher (!) zu löschen.

Datenanalyse setzt Daten-Management die Krone auf
Wichtig ist, dass Unternehmen ein Konzept entwickeln, damit die Datenflut sie nicht unvorbereitet erfasst. Verschiedene Lösungen (siehe Kasten), häufig auch in Kombination, helfen dabei, die Datenmassen, die aus verschiedenen Quellen sprudeln, in die richtigen Kanäle zu lenken und in zentralen Datenbanken zu erfassen. Letztlich geht es aber nicht nur darum, Daten richtig zu speichern und Datenbanken ständig aktuell zu halten (Stichwort: Datenintegrität). Es geht auch darum, größtmögliche Lehren aus den Daten zu ziehen und ihr Potenzial somit voll und ganz auszuschöpfen. Aber das ist wieder ein anderes Thema. Mehr dazu erfahren Sie auf den Seiten 18/19.

Fest steht: Zuallererst müssen Unternehmen mit einem soliden Daten-Management ein sicheres Fundament schaffen, um darauf mit umfassenden Datenanalysen aufbauen zu können. Wir unterstützen Sie gern dabei, eine Datenstrategie für Ihr Unternehmen zu entwickeln und geeignete Lösungen zu implementieren. Kontaktieren Sie uns!

Data Storage: Cloud oder eigener Server?

Das Speichern und Archivieren ist ein wichtiger Teil der Datenverarbeitung. Aber wo genau sollen Unternehmensdaten gespeichert werden? Welche Möglichkeiten gibt es? Wie findet ein Unternehmen die individuell richtige Speicherart? Ein Blick auf das Thema Data Storage.

Wohin mit den Daten?
Wenn immer mehr Daten erzeugt werden, stellt sich in jedem Unternehmen irgendwann unweigerlich die Frage: Wohin damit? Die Herausforderung ist es, ausreichende Speicherkapazitäten aufzubauen, eine geeignete Speichermethode zu finden, die Verwaltung der Daten zu organisieren und für eine bestmögliche Datenverfügbarkeit zu sorgen. Das Problem an der Sache: Es gibt im Zusammenhang mit Daten-Management, Datenspeicherung, Datenverwaltung etc. kein allgemeingültiges Vorgehen, das für jedes Unternehmen anwendbar ist.

Warum ist das so? Der Hauptgrund ist, dass die Gegebenheiten in jedem Unternehmen anders sind. Das beginnt schon mit den Unterschieden in der IT-Infrastruktur. Ein Unternehmen hat zwanzig Büroarbeitsplätze, ein anderes 200. In manchen Unternehmen ist die IT-Infrastruktur sehr fortschrittlich aufgebaut, in anderen hinkt man etwas hinterher. Hinzu kommt, dass jedes Unternehmen andere Business-Software benötigt und jede auf ihre eigene Weise in die IT-Umgebung eingebunden werden muss. Derlei Unterschiede gibt es noch viel mehr.

Lokale Datenspeicherung – der Klassiker
Bevor die Cloud am Horizont auftauchte, war die lokale Datenspeicherung das Mittel der Wahl. Aber auch hier gibt es Variationen. Bei sehr kleinen Unternehmen reicht(e) oft schon eine externe Festplatte. Größere Unternehmen setz(t)en häufig auf sogenannte NAS-Systeme. Sie bestehen aus zwei oder mehr Festplatten, auf denen Daten parallel gespeichert werden. Der Vorteil: Geht eine Festplatte kaputt, kann sie problemlos ausgetauscht werden, auf der oder den anderen Festplatten sind die Daten weiterhin vorhanden. Ein weiterer Plus-Punkt dieses Speichermediums ist der vergleichsweise geringe Kostenfaktor. Nachteile: Die Speicherkapazitäten sind irgendwann erschöpft und die Hardware kann ausfallen oder veralten, sodass neue angeschafft werden muss.

Ab einer gewissen Unternehmensgröße wird häufig in einen eigenen (physischen!) Server investiert – oder sogar in mehrere. Bei einer solchen Server-Lösung sind dann HDDs (Hard Disk Drive) und/oder SSDs (Solid State Drives) als Speichermedien involviert. Der Vorteil eines eigenen Servers ist, dass Daten direkt vor Ort gespeichert sind und Unternehmen großen Einfluss darauf haben, wie sie Server und Daten schützen. Zudem haben sie völlig freie Hand darin, welche Software sie benutzen oder mit welchen individuellen Konfigurationen sie arbeiten wollen.

Cloud zieht auf – neue Art des Speicherns
Eine immer größere Rolle bei der Datenspeicherung spielt die Cloud. Dabei hatte sie es

anfangs schwer, überhaupt Fuß zu fassen. Zu groß war die Skepsis hinsichtlich der Datensicherheit – sowohl im Hinblick auf ihre Verfügbarkeit als auch in Bezug auf unberechtigten Zugriff. Und Unternehmen, die sich auf das Wagnis einlassen wollten, hatten häufig damit zu kämpfen, Cloud-Lösungen in ihre bestehende IT-Infrastruktur zu integrieren.

Inzwischen setzt sich die Cloud immer mehr durch. 2015 sahen die Verhältnisse noch so aus: 66 Prozent des weltweiten Datenaufkommens wurden lokal gespeichert, nur 31 Prozent in der Cloud. Jetzt, im Jahr 2021, hat die Cloud die lokalen Speichermedien überholt – nämlich etwa im Verhältnis 55 zu 38 Prozent. Die Cloud punktet durch mehr Flexibilität und Skalierbarkeit auf der einen Seite und geringen Investitionskosten, wenig administrativem Aufwand und schonendem Ressourceneinsatz auf der anderen Seite. Zudem macht sie mobile Arbeitsweisen möglich und unterstützt die Digitalisierung.

Cloud oder eigener Server?

Die Frage, ob Cloud, Server oder eine Kombination aus beidem am besten geeignet ist, lässt sich pauschal nicht beantworten. Viele Faktoren spielen bei der Entscheidung mit hinein, viele Aspekte müssen berücksichtigt werden. Und mit der Entscheidung für ein bestimmtes Speichermedium oder eine Kombination verschiedener Speichermedien ist das Thema Daten auch längst nicht abgeschlossen. Es muss auch die Frage nach der passenden Speichermethode gestellt werden.

Es ist daher durchaus verständlich, wenn Sie der ganzen Daten-Thematik bisher so gut wie möglich ausgewichen sind. Die gute Nachricht: Wir stehen Ihnen dabei gern zur Seite, schauen uns die Gegebenheiten bei Ihnen vor Ort an, haben dabei Risiken und Herausforderungen im Blick und decken Potenziale auf, die die jeweiligen Speichermedien und -methoden speziell für Ihr Unternehmen haben. Übergeben Sie die Thematik einfach an uns als Profi und erhalten Sie im Gegenzug eine stichhaltige Datenstrategie, die alle erdenklichen Aspekte beinhaltet. Hört sich gut an? Dann melden Sie sich!

Datenschutz – bleiben Sie DSGVO-konform!

Spätestens seit Inkrafttreten der DSGVO im Jahr 2018 wissen Unternehmen, dass sie das Thema Datenschutz ernst nehmen müssen. Aber auch drei Jahre später sind noch viele Baustellen offen – und es kommen weitere hinzu. Welche neuen Herausforderungen gibt es im Jahr 2021?

Datenschutz – seit langer Zeit ein Thema
Als die ersten Meldungen zu einer geplanten europäischen Datenschutzgrundverordnung (DSGVO) publik wurden, schlugen sie ziemlich hohe Wellen. Viele Unternehmen sahen sich plötzlich einem komplexen Thema gegenüber, das Interesse an Informationen dazu war entsprechend groß. Fast hätte man meinen können, Datenschutz habe vorher keine Rolle gespielt. Ein Blick zurück in die Vergangenheit zeigt aber etwas anderes.

Schon im Jahr 1968 begann der Europarat damit, sich mit der Gefährdung der Privatsphäre durch die automatische Datenverarbeitung zu beschäftigen. Die Notwendigkeit, Einzelpersonen davor zu schützen, dass ihre personenbezogenen Daten automatisch gesammelt, gespeichert, verarbeitet und weitergegeben werden, wurde schon damals diskutiert. Das Ergebnis war die »Datenschutzkonvention Nr. 108«, die Anfang 1981 »zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten« verabschiedet worden ist.

DSGVO reformiert bestehende Regeln
Die Konvention war der Startschuss für einen gemeinsamen europäischen Datenschutz. 1995 folgte mit der EU-Datenschutzrichtlinie der nächste Schritt. Das Ausmaß und die Qualität der elektronischen Datenverarbeitung entwickelten sich aber so rasant weiter, dass die EU-Kommission im Jahr 2012 erneut eine Reform ankündigte. 2015 lag der erste Entwurf auf dem Tisch, 2016 wurde die europäische Datenschutzgrundverordnung verabschiedet. Als Stichtag für das Inkrafttreten wurde der 25. Mai 2018 festgesetzt.

Neu war das Thema Datenschutz im Frühjahr 2018 also nicht. Und obwohl die DSGVO mit zwei Jahren Vorlauf angekündigt worden war, hatten einige Unternehmen zum Stichtag noch nicht alle notwendigen Vorkehrungen getroffen. Andere dagegen haben große Anstrengungen zur Verbesserung ihrer Datensicherheit gemäß DSGVO unternommen. Egal zu welcher dieser Gruppen ein Betrieb heute gehört – tätig werden müssen im Jahr 2021 angesichts neuer Anforderungen wohl alle.

Herausforderungen für den Datenschutz
Es hat sich nämlich gezeigt, dass die Corona-Krise erhebliche Auswirkungen auf IT-Sicherheit und Datenschutz hat. Das liegt einerseits daran, dass sich die IT-Infrastrukturen verändert haben. Andererseits nutzen Cyberkriminelle die Situation gezielt aus – durch Angriffe auf Remote-Verbindungen und Phishing-Kampagnen mit Corona-Bezug. Unternehmen sind nun besonders gefordert, ihre Infrastruktur abzusichern und ihre Sicherheitstechnik auf Stand zu halten.

Eine weitere Herausforderung hat ein recht neues Urteil des Europäischen Gerichtshofs zu Tage gefördert. Darin wurde festgelegt, dass europäische Daten nur in Drittländern gespeichert werden dürfen, wenn Daten dort mindestens einen gleichwertigen Schutz genießen, wie es die DSGVO innerhalb der europäischen Union vorsieht. Der Europäische Datenschutzausschuss hat dazu Handlungsempfehlungen veröffentlicht. Bei einem Verstoß drohen Strafen und Bloßstellung.

Zahl der Bußgeldbescheide steigt
Bei den Bußgeldern scheinen die Datenschutzbehörden inzwischen härter durchzugreifen. 2020 wurden 301 Bußen ausgesprochen – ein Anstieg von 60 Prozent im Vergleich zu 2019 mit 187 Bußgeldbescheiden. Die Höhe der Bußgelder lag bei insgesamt 48 Millionen Euro. Damit Unternehmen nicht in der Statistik für 2021 landen, sollten sie dringend handeln. Wir beraten Sie gern und setzen den Datenschutz für Sie um!

Das sind die häufigsten Versäumnisse

Besonders für kleine und mittelständische Unternehmen (KMU) sind die umfassenden Datenschutzregeln häufig schwer umzusetzen und einzuhalten. Daher kommt es immer wieder zu denselben Versäumnissen. Das sind die Top 3:

- **Platz 1: Fehlende Zuteilung von Ressourcen**
  Datenschutz ist ein dauerhafter Prozess mit häufigen Veränderungen und muss immer im Blick behalten werden – und dafür muss es Ressourcen geben.
- **Platz 2: Mangelnder Fokus auf IT-Sicherheit**
  Datenschutz beginnt nicht bei Speicherung und Nutzung von Daten, sondern bei der IT-Sicherheit. Der Weg zu den Daten ist so abzusichern wie die Daten selbst.
- **Platz 3: Fehlende Einbindung eines Datenschutzbeauftragten**
  Datenschutz erfordert Zeit, Geld und Know-how. Wer einen effektiven Datenschutz betreiben möchte, sollte am besten einen Experten in den Prozess einbinden.

Daten im Visier von Kriminellen

Cyberkriminelle haben Daten als das ultimative Druckmittel für sich entdeckt. Es reicht ihnen inzwischen nicht mehr, Malware in Unternehmensnetzwerke einzuschleusen und Daten dort zu verschlüsseln. Jetzt ziehen sie die Daten vorher ab und drohen mit ihrer Veröffentlichung, sollte kein Lösegeld gezahlt werden.

Unternehmen sind das Lieblingsopfer von Cyberkriminellen

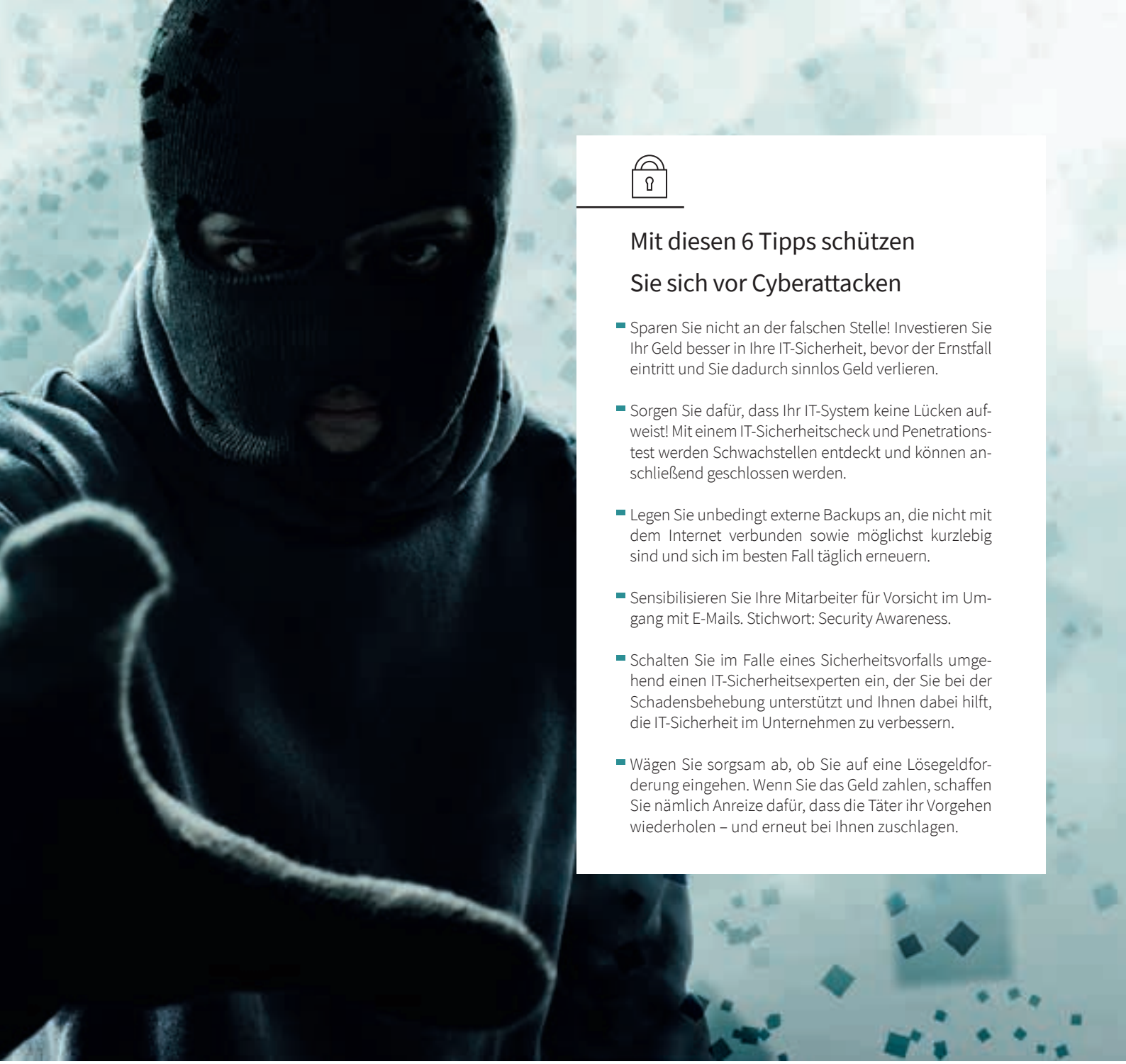
Es lässt sich nicht anders sagen: Cyberkriminelle haben in Angriffen auf Unternehmen ein absolut lukratives Zubrot gefunden. Sie versuchen, mit ihren Attacken Malware in Unternehmensnetze einzuschleusen, dort sämtliche Daten zu verschlüsseln und das Opfer dadurch handlungsunfähig zu machen – denn dann ist die Not am größten und das Opfer ist besonders gewillt, dem Spuk durch die Zahlung eines Lösegeldes ein möglichst schnelles Ende zu bereiten. Besonders in einer solchen Situation zeigt sich nämlich, wie abhängig Unternehmen inzwischen von der ständigen Datenverfügbarkeit sind.

Ob klein, mittelständisch oder groß – immer mehr Unternehmen sind mittlerweile bezüglich der Gefahren sensibilisiert und sorgen mit einem zuverlässigen Backup-Management vor (siehe Seiten 10/11). Die Daten können daraus wiederhergestellt und die Lösegeldforderung kann getrost ignoriert werden. Das haben auch die Cyberkriminellen bemerkt. Sie gehen zunehmend zu einer neuen, noch fieseren Taktik über: Bevor sie Daten verschlüsseln, kopieren sie sie auf ihre Server und drohen mit einer Veröffentlichung der Daten, sollte kein Lösegeld gezahlt werden.

Cyberangriffe machen Schlagzeilen

Das Problem an der Sache: Ein erfolgreicher Cyberangriff bleibt oft nicht vor der Öffentlichkeit verborgen; und noch schlimmer wiegt der Fall, wenn plötzlich immer mehr sensible Unternehmensdaten im Internet auftauchen. Meist ist es dann unmöglich, den Sicherheitsvorfall aus den Schlagzeilen zu halten. Und natürlich: Positiv sind solche Schlagzeilen nicht. Unangenehme Fragen werden unter anderen von den zuständigen Datenschutzbehörden gestellt. Wie konnte das passieren? Hat das Unternehmen in Bezug auf die IT-Sicherheit geschlampt? Sind personenbezogene Daten von dem Datendiebstahl betroffen und im Internet aufgetaucht? Ein solcher Image-Schaden droht zumindest kurzfristig das Geschäft zu schädigen. Hinzu kommt der finanzielle Schaden durch die direkten Folgen des Angriffs.

Im Jahr 2020 haben so einige Unternehmen in Deutschland diese leidige Erfahrung machen müssen. Der Automobilzulieferer GEDIA war darunter. Über eine Sicherheitslücke war Ransomware in das Firmennetz gelangt, das gesamte Netzwerk wurde verschlüsselt. Aus Sicherheitsgründen entschieden sich die Verantwortlichen für eine komplette Systemabschaltung. Den Angreifern war es aber gelungen, schon im Vorfeld 50 Gigabyte an internen Daten zu kopieren. Nach und nach veröffentlichten sie sie im Internet. Vermutlich weil das Unternehmen sich weigerte, das geforderte Lösegeld zu zahlen.



Mit diesen 6 Tipps schützen Sie sich vor Cyberattacken

- Sparen Sie nicht an der falschen Stelle! Investieren Sie Ihr Geld besser in Ihre IT-Sicherheit, bevor der Ernstfall eintritt und Sie dadurch sinnlos Geld verlieren.
- Sorgen Sie dafür, dass Ihr IT-System keine Lücken aufweist! Mit einem IT-Sicherheitscheck und Penetrationstest werden Schwachstellen entdeckt und können anschließend geschlossen werden.
- Legen Sie unbedingt externe Backups an, die nicht mit dem Internet verbunden sowie möglichst kurzlebig sind und sich im besten Fall täglich erneuern.
- Sensibilisieren Sie Ihre Mitarbeiter für Vorsicht im Umgang mit E-Mails. Stichwort: Security Awareness.
- Schalten Sie im Falle eines Sicherheitsvorfalls umgehend einen IT-Sicherheitsexperten ein, der Sie bei der Schadensbehebung unterstützt und Ihnen dabei hilft, die IT-Sicherheit im Unternehmen zu verbessern.
- Wägen Sie sorgsam ab, ob Sie auf eine Lösegeldforderung eingehen. Wenn Sie das Geld zahlen, schaffen Sie nämlich Anreize dafür, dass die Täter ihr Vorgehen wiederholen – und erneut bei Ihnen zuschlagen.

Lösegelder in Rekordhöhe

Die Lösegeld-Forderungen werden im Übrigen immer saftiger – das hängt vielleicht auch mit der bereits beschriebenen Tatsache zusammen, dass die Cyberkriminellen durch den Diebstahl der Daten ein noch größeres Druckmittel haben als bei der alleinigen Verschlüsselung. Das Kupfer-Unternehmen KME, das im Jahr 2020 ebenfalls ins Visier geriet, sah sich deswegen einer Lösegeldforderung in Höhe von 7,5 Millionen US-Dollar gegenüber. Die Angreifer hatten im Netzwerk unter anderem Unternehmensbilanz und Versicherungspolice gefunden und die Höhe ihrer Forderung daran ausgerichtet.

Auch in diesem Fall wurde mit der Veröffentlichung der sensiblen Daten gedroht. KME entschied sich dazu, mit den Kriminellen in Verhandlungen zu gehen. Am Ende kam es zu einer Einigung: 1,27 Millionen US-Dollar zahlte das Opfer und erhielt daraufhin den Dekryptor zur Entschlüsselung der Daten. Sozusagen als Dreingabe gaben die Angreifer noch Tipps, wie sich der Konzern besser schützen kann.

Jedes Unternehmen kann zum Ziel werden

Unternehmen sollte also bewusst sein, dass Daten nicht nur für sie selbst einen hohen Wert haben, sondern auch für Cyberkriminelle ein lukratives Geschäft versprechen. Und das wiederum bedeutet: Die Unternehmensdaten sind so gut wie nur möglich zu schützen! Einerseits helfen hier natürlich technische Sicherungsmaßnahmen wie Antivirus-Software, Firewall, Backup und Co. Insbesondere das Home Office und sichere Verbindungen zum Firmennetzwerk müssen dabei mit berücksichtigt werden, denn hier besteht eine erhöhte Gefahr.

Andererseits gilt es, sämtliche Mitarbeiter für Gefahren aus der Cyberwelt zu sensibilisieren. Denn: Das Jahr 2020 hat gezeigt, dass – aus Sicht der Angreifer – vor allem Phishing-E-Mails zum Erfolg geführt haben. Um möglichst viele Opfer zu einem gefährlichen Klick zu verleiten, werden aktuelle Trends instrumentalisiert – die Corona-Pandemie war dabei besonders vertreten. Die gute Nachricht: Ob technische Maßnahmen oder Mitarbeiter-Sensibilisierung – wir unterstützen Sie!

Kein Backup? Kein Mitleid.

Damit wichtige Daten nicht abhanden kommen, reicht das alleinige Speichern nicht aus. Unternehmen benötigen zusätzlich ein zuverlässiges Backup, aus dem verlorene Daten wiederhergestellt werden können. Wer hier nicht vorsorgt, hat im schlimmsten Fall Pech gehabt.

Daten sind häufig in Gefahr
Cyberattacken sind die Bedrohung Nr. 1 für Unternehmensdaten (siehe Seiten 12/13). Sie sind aber keineswegs die einzige Gefahr. Daten können nämlich auch durch einen technischen Defekt des physischen Speichermediums zerstört werden. Menschliche Fehler sind auch denkbar; ein falscher Klick hat schon in so manchem Betrieb zu einem Datenverlust geführt. Und dann wäre da noch Mutter Natur, die durchaus ihre Tücken hat – zum Beispiel wenn ein Blitzeinschlag für einen Kurzschluss sorgt oder ein Hochwasser die Hardware unbrauchbar macht.

Sind die Daten weg, ist der Schaden für das betroffene Unternehmen groß. Es können vielleicht keine Termine mehr aufgerufen, keine E-Mails eingesehen, keine Kundenakten geöffnet werden. Das bedeutet in vielen Fällen, dass nicht weitergearbeitet werden kann. Und das wiederum heißt, dass das Unternehmen Zeit und Geld verliert. Sollten die Daten gar nicht wieder auftauchen, ist der Fall noch schlimmer – dann steht nämlich die gesamte Existenz auf dem Spiel.

Mit Backup Daten sichern
Aber wie lässt es sich verhindern, dass wichtige – wenn nicht sogar alle – Unternehmensdaten auf einem (physischen) Speichermedium verloren gehen? Richtig: Man sorgt dafür, dass sie doppelt und dreifach gesichert sind – und zwar durch ein Backup. Ist so ein Backup vorhanden, können auf dem eigentlichen Speicher verloren gegangene Daten mit vergleichsweise geringem Aufwand aus dem Backup wiederhergestellt und die Arbeit nach einem nur kurzen Aussetzer fortgesetzt werden.

Dann ist das Problem doch einfach gelöst. Oder? Nicht ganz. Ein effizientes Backup-Management einzurichten, ist häufig eine komplizierte Angelegenheit, bei der es viele Aspekte zu berücksichtigen gilt. Unter anderem sind gesetzliche Vorgaben zu erfüllen. Denn: Unter anderem verpflichtet die Datenschutzgrundverordnung zur Langzeitarchivierung bestimmter Unternehmensdaten.

Finden Sie Ihre Backup-Strategie!
Aber wie lässt sich ein rechtssicheres Backup einrichten? Hilfreich ist, wenn zunächst ein Datensicherungskonzept zur Sicherung der Unternehmensdaten aufgestellt wird – inklusive Backup-Strategie. Diese Strategie sieht für jedes Unternehmen anders aus. Zunächst ist daher eine Bestandsaufnahme nötig. Diese erfasst IT-Systeme, Anwendungen und Daten sowie die Backup-Anforderungen, die sich aus den geschäftlichen Anforderungen und den gesetzlichen Regelungen ergeben. Zudem sind die Geschäftsdaten nach ihrer Relevanz zu bewerten. Und dann muss definiert werden, welche Speichermedien sich im individuellen Fall am besten eignen.

Es stellen sich aber noch weitere Fragen. Soll die Datensicherung auf lokalen Datenträgern, in der Cloud oder in einer Kombination aus beidem erfolgen? Mit welchem Tool soll die Datensicherung durchgeführt werden? Wer verwaltet das Backup? Wer prüft regelmäßig, ob es zuverlässig funktioniert? Und in welchen Zeitabständen sollen die Daten im Backup gespeichert werden? Die Liste an Fragen ließe sich an dieser Stelle noch weiter ausführen.

Backup ist ein Muss
Festhalten lässt sich letztlich Folgendes: An einer Backup-Lösung führt angesichts der gesetzlichen Bestimmung und der Bedeutung von Daten für jedes Unternehmen kein Weg mehr vorbei. Kümmern Sie sich rechtzeitig darum! Denn in diesem Fall gilt besonders: Wer zögert, den bestraft das Leben.

Keine Lust auf Backup?

Für Unternehmen, die sich mit dem Thema Backup nicht unbedingt selbst befassen möchten – oder es aufgrund mangelnder Ressourcen nicht können – gibt es eine sehr einfache Lösung: Sie können einen Experten damit beauftragen. Dafür sind wir genau der richtige Ansprechpartner. Wir erarbeiten mit Hilfe ihres Inputs ein passendes Datensicherungskonzept und die bestmögliche Backup-Strategie für die individuellen Anforderungen des jeweiligen Unternehmens – vielleicht sogar für das Ihre? Selbstverständlich setzen wir das Gesamtkonzept auch gern für Sie um. Und auch dann lassen wir Sie nicht allein. Mit unserem Backup-Management begleiten wir Ihren Backup-Prozess auch dauerhaft und stellen damit sicher, dass die Datensicherung zuverlässig funktioniert.

Daten weg. Und jetzt?

Das Horrorszenario ist eingetreten, wichtige Unternehmensdaten sind weg. Ein Backup existiert nicht. Ist jetzt alles verloren? Vielleicht ja. Vielleicht gibt es aber auch noch eine Möglichkeit, die Daten zu retten. Ein Interview mit den Datenrettern von Ontrack.

Wie häufig musste Ontrack 2020 Unternehmensdaten retten?
Ontrack: 2020 wurde das Team von Ontrack in Deutschland in mehr als 4.000 Fällen von Unternehmen kontaktiert und um Hilfe gebeten. Wichtige oder gar kritische Unternehmensdaten waren »verloren« und mussten wiederhergestellt werden.

Was waren die häufigsten Ursachen für den Datenverlust?
Ontrack: Bei einzelnen Festplatten oder einzelnen SSDs gab es vier sehr häufige Fehler: erstens die physikalische Beschädigung durch Stöße oder Herunterfallen; zweitens elektronische Schäden; drittens das fehlerhafte Löschen/Überschreiben; und viertens die »Überalterung«, wenn Medien zu lange genutzt wurden. Bei den Servern und Speichersystemen bzw. RAID-Systemen sind vor allem physikalische Schäden bei einzelnen Speichermedien aufgetreten, die zum Ausfall des gesamten Systems führten. Dann gab es fehlerhafte Updates, die zum Überschreiben und damit Löschen von größeren Datenmengen führten. Auch Beschädigungen oder Verschlüsselungen von Daten durch Cyberangriffe kamen sehr häufig vor – oftmals durch Ransomware-Attacken, die größere Datenbereiche verschlüsselt haben.

Lässt sich sagen, wie gravierend die Datenverluste waren, mit denen Kunden zu Ihnen kamen? Wie groß war der Schaden für das jeweilige Unternehmen?
Ontrack: Eine Pauschalisierung ist schwierig. Die Unternehmen kommen zu uns, weil ihnen unternehmenswichtige Daten fehlen, ohne die das Unternehmen nur schwer weiterkommt. Betroffen sind oft Kundendatenbanken oder die Buchhaltung, Produktionsdaten, Anlagensteuerungen, Rezepturen, nicht selten auch der gesamte E-Mail-Verkehr einer ganzen Abteilung, Bestelldatenbanken usw. Die Wiederbeschaffung ist oft nicht möglich oder sehr aufwändig. Nicht selten beträgt ein Schaden mehrere 100.000 Euro bis hin zu mehreren Millionen Euro, wenn Daten nicht wiederhergestellt werden können.

In wie viel Prozent der Fälle war der Rettungseinsatz erfolgreich?
Ontrack: Pauschal können wir sagen, dass wir in mehr als 80 Prozent der Fälle alle oder einen Teil der für die Kunden wichtigen Daten wiederherstellen konnten. Wenn Datenträger physikalisch so stark beschädigt sind, dass keine „Materie“ mehr vorhanden ist, kann leider das beste Datenrettungsunternehmen keine Daten wiederherstellen.

Wissen Sie, wie genau die Konsequenzen bei den Fällen aussahen, in denen die Datenrettung nicht erfolgreich war?
Ontrack: Das ist schwierig zu sagen, da wir oft keine weiteren Informationen von den Kunden bekommen und wir sie in der schwierigen Situation nicht zusätzlich mit diesen Fragen „belasten“ wollen. Doch wir kennen mittelständische Unternehmen, die Teilbereiche schließen mussten. Bei Privatkunden kann es sein, dass wertvolle persönliche Erinnerungen wie Hochzeitsbilder oder Babyfotos für immer verloren sind, wenn die externe Festplatte, die als Bildspeicher genutzt wurde, durch einen Sturz erheblichen Schaden genommen hat.

Datenrettung in 6 Schritten

- Erste kostenfreie Evaluierung des Datenverlusts am Telefon mit den Experten von Ontrack; Erläuterung zum Prozess der Datenrettung
- Bei Einzel-Medien schnelle Evaluierung innerhalb von vier Stunden im Labor; bei Servern oder Speichersystemen detaillierte Diagnose im Labor
- Nach der Evaluierung oder Diagnose verlässliche Information an den Kunden, welche Daten zu wie viel Prozent wiederhergestellt werden können
- Kunde erteilt Auftrag zur Datenrettung; die Spezialisten von Ontrack arbeiten je nach Dringlichkeit auch über Nacht oder am Wochenende; falls der Kunde keinen Auftrag erteilt, gehen die Datenträger zurück, Kosten fallen dann nur für Versand und Diagnose an
- Gerettete Daten werden verschlüsselt und dem Kunden auf einem oder mehreren Datenträgern zugestellt (Express oder Direktlieferung); kleinere aber zeitkritische Datenmengen können online übermittelt werden
- Bei Bedarf Unterstützung beim Wiedereinspielen der Daten in die bestehende IT-Infrastruktur

Gab es im Jahr 2020 einen besonders spektakulären Fall?
Ontrack: Wir haben im vergangenen Jahr die Anfrage eines mittelständischen Maschinenbauunternehmens erhalten. Durch eine Ransomware-Attacke wurden 90 Prozent aller Daten teilweise gelöscht und verschlüsselt. Speziell die technischen Zeichnungen von wichtigen Maschinen, die das Herz des Unternehmens darstellen, waren weg. Ohne diese Unterlagen konnten keine Maschinen verkauft und angeliefert werden, da das Unternehmen verpflichtet ist, diese Verbraucherinformationen mitzuliefern. Das Unternehmen wurde erpresst und hatte bereits eine hohe Summe im sechsstelligen Euro-Bereich bezahlt. Die vom Erpresser gelieferten Daten haben trotzdem nicht funktioniert und der Kunde hat sich an uns gewandt. Mit unserer Entwicklungsabteilung in den USA und unseren Datenrettungsexperten in Deutschland waren wir in der Lage, die wichtigsten Kundendaten wiederherzustellen und zur Verfügung zu stellen. Der Kunde war natürlich sehr erleichtert und überglücklich, seine unternehmenskritischen Daten wiederzubekommen.

Was empfehlen Sie Unternehmen, um einen solchen Datenverlust zu vermeiden? Gibt es bestimmte Richtlinien?
Ontrack: Eine umfassende Backup-Strategie ist in der heutigen IT-Welt für Unternehmen unerlässlich. Bei so vielen Möglichkeiten, Daten zu verlieren, müssen Firmen verstehen, wie sie ihre Daten erfolgreich sichern können, um sicherzustellen, dass sie keinen unvorhergesehenen Datenverlust erleiden. Wir empfehlen als Teil dieser Backup-Strategie grundsätzlich die Anwendung der sogenannten 3-2-1-Backup-Regel. Dazu braucht es eine kurze Erklärung. Daten sollten **drei** Mal gespeichert werden, nämlich einmal als Live-/Produktionsdaten und zudem mit zwei Backups, um Redundanz zu gewährleisten. Dann sollten Unternehmen **zwei** verschiedene Technologien für ihre Backups verwenden. Je nach ihren Bedürfnissen stehen dafür zahlreiche Medientypen zur Verfügung: NAS, externe Festplatten, Flash-Speicher, Magnetbänder, die Cloud, usw. Letzter Teil der Regel ist es, immer **eins** der Backups außerhalb des Standorts oder Firmengeländes aufzubewahren. Nach unserer Erfahrung funktioniert diese 3-2-1-Regel wirklich gut.

Big Data & Analytics – eine Zukunftsvision?

Daten gelten als das Öl des 21. Jahrhunderts, weil sich aus ihnen wertvolle Erkenntnisse ziehen lassen. Aus diesem Grund gehen Unternehmen vermehrt dazu über, Unmengen an (Roh-)Daten zu sammeln – Big Data. Durch Analyse-Mechanismen sollen sie ihren Wert entfalten.

Daten sammeln und profitieren
Daten zu sammeln, ist gut und schön. Wichtiger ist allerdings, dass Unternehmen davon auch tatsächlich profitieren. Und das gilt für alle erdenklichen Bereiche. Was hilft es beispielsweise, wenn nützliche Informationen zu Kunden auf Laufwerken, in Datenbanken, E-Mails und Co. wild verteilt sind? Profitieren lässt sich von diesem Datenschatz erst, wenn die Informationen zusammengeführt werden, denn dann entfaltet sich ein umfassendes Bild zu jedem einzelnen Kunden. Mit den richtigen Strategien lassen sich auf dieser Basis gezielt passende Angebote unterbreiten. Sogar noch mehr: Produkte können nach den spezifischen Bedürfnissen verbessert werden.

Das heißt, dass die Anwendungsfälle vielseitig sind. Sie beginnen bei Marktanalysen und Kundensegmentierungen in Vertrieb und Marketing; sie gehen weiter mit der Steigerung der Kosteneffizienz und der Möglichkeit von Trendanalysen in der Produktentwicklung; sie beinhalten die Erfassung von Maschinendaten in Echtzeit und die Früherkennung von Problemen in der Produktion; sie helfen bei der Optimierung von Lieferketten und Transportkosten in Distribution und Logistik und reichen bis zu Risikoerkennung und Echtzeit-Reaktion im Bereich Finanzen/Controlling.

Datengetriebene Entscheidungen treffen
Es geht also letztlich darum, durch die Analyse des Informationspools datengetriebene Entscheidungen treffen zu können. Die Umsetzung dessen erfolgt in diesem Zyklus: Sammlung von Daten, Aufbereitung der Daten, Analyse der Daten, Umsetzung der Erkenntnisse. Dann kann der Zyklus erneut beginnen. Unternehmen, die den Weg der datengetriebenen Analyse gehen wollen, benötigen dazu vor allem die passenden technischen Hilfsmittel. Einerseits müssen Daten erzeugt und in den Zyklus eingeführt werden, andererseits braucht es entsprechende Tools, die zielgerichtet die Analysen durchführen. Im Idealfall sind diese Tools sogar selbstlernend, sodass sie auf Basis vieler Daten ihre Leistungsfähigkeit automatisch optimieren und zu neuen Erkenntnissen führen.

Zukunftsvision oder Realität?
Tatsächlich greifen bereits viele große Konzerne auf Big Data und Big Data Analytics zurück. Zunehmend erkennt aber auch der Mittelstand, dass genau dieses Thema den Geschäftserfolg entscheidend beeinflussen kann. Die erwähnten technischen Hilfsmittel sind daher auch schon mehr als eine Vision für die Zukunft – sie sind bereits Realität. Es existieren schon heute verschiedene Software-Lösungen – als Desktop-Anwendung und/oder Cloud-Lösung – und machen vielfältige Analysen möglich. Auch geeignete Hardware steht bereit.

Ein Beispiel dafür ist Hardware in der Edge. Dabei rücken IT-Ressourcen wie Rechenleistung und Speicherkapazität näher an den Ort, an dem die Daten entstehen. Oft wird dann schon vor der Weiterleitung der Daten in die Datenbank eine Vorsortierung vorgenommen. Die Vorteile: eine schnellere Datenverarbeitung, verbesserte Ausfallsicherheit, höhere Datensicherheit (durch geringeren Datentransfer) und kontinuierliche Datenverfügbarkeit. Mit »Edge in a Box« stellt APC by Schneider Electric dafür eine einfache, kosteneffiziente und kompakte Lösung bereit.

»Edge in a Box«: starke Rechenleistung
Die Edge ist dabei häufig dort, wo kein Rechenzentrum zu finden ist. Das können je nach Branche Büros, Niederlassungen, Werke und Filialen sein. An diesen Orten stehen selten eigene Server, obwohl genau dort wertvolle Daten entstehen. Mit drei verschiedenen »Edge in a Box«-Bundles will Schneider Electric gemeinsam mit Hewlett Packard Enterprise (HPE) einen einfachen, kostengünstigen und skalierbaren Einstieg ins Edge Computing bieten. Es handelt sich dabei um besonders leise Hardware mit geringen Ausmaßen, für die sich so ziemlich überall ein Platz finden lässt.

So ein Bundle sorgt zum Beispiel vor Ort im Büro dafür, dass kritische Unternehmensdaten lokal gespeichert oder die Desktops und Apps der Mitarbeiter virtualisiert werden. Die gemeinsame Lösung von Schneider Electric, HPE und StorMagic ist schnell und einfach zu implementieren und kann auf Wunsch mit der Next-Gen DCIM-Plattform (Data Center Infrastructure Management) EcoStruxure IT von Schneider Electric ausgestattet werden. Mit Echtzeit-Datenanalysen und prädiktiven Servicefunktionen ermöglicht die Remote-Management-Funktion von EcoStruxure Unternehmen außerdem die Zusammenarbeit mit Managed Services Providern (MSPs).

Und spätestens hier kommen wir ins Spiel. Wir unterstützen Sie nicht nur bei der Implementierung einer solchen Lösung, sondern sind mit unseren Managed Services auch gern als Ihr dauerhafter IT-Betreuer im Einsatz. Dadurch können wir die Verfügbarkeit ihrer IT-Umgebung deutlich verbessern. Interesse? Dann lassen Sie sich von uns beraten!

APC
by Schneider Electric

ÜBERREICHT DURCH

cosoft computer consulting gmbh

Borkener Str. 134a
48653 Coesfeld

Telefon +49 2541 94750
E-Mail info@cosoft.de

http://www.cosoft.de