

# PRAXISLEITFADEN „DATENSICHERHEIT UND DATENSCHUTZ“



**„EINE GEFAHR, DIE MAN KENNT, IST KEINE GEFAHR MEHR.“**

*Hans Joachim von Zieten*

# DATEN – DAS WICHTIGSTE GUT

Daten und Informationen sind ein wichtiges, ja sogar ein überlebenswichtiges, Gut des Unternehmens und müssen daher umfassend geschützt werden. Die Daten müssen bei Bedarf stets verfügbar sein, dürfen nicht verloren gehen oder unerlaubt verändert werden. Ferner muss gewährleistet sein, dass nur berechtigte Personen darauf zugreifen können. Bei fehlenden Sicherheitsmechanismen kann das Unternehmen ernsthaft Schaden nehmen oder sogar in eine existenzbedrohende Krise stürzen. Die Geschäftsführer und Vorstände des Unternehmens sind dafür verantwortlich, dass geeignete Sicherheitsmechanismen implementiert und genutzt, sowie dass die gesetzlichen Vorschriften in diesem Zusammenhang eingehalten werden. Bei Versäumnissen drohen der Unternehmensleitung aber auch anderen verantwortlichen Mitarbeitern sowohl zivil- als auch strafrechtliche Folgen.

Die Datensicherheit nach innen und außen ist dabei als kontinuierlicher Prozess und nicht als einmalige Implementierung einer starren Technologie zu sehen. Die Unternehmen werden heute mit vielfältigen potentiellen Bedrohungen konfrontiert, wobei sich die Bedrohungen von Zeit zu Zeit auch ändern oder neue hinzukommen. Der Umfang und die Wirksamkeit der Sicherheitsmechanismen sollte daher regelmäßig überprüft und gegebenenfalls erweitert und angepasst werden.

Oftmals wird beim Thema Sicherheit nur an Zugriffsschutz, Viren und Hacker gedacht, doch das Thema ist weitaus umfangreicher und vielschichtiger. So schreiben gesetzliche Regelungen, wie das „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich“ (KonTraG) oder der Sarbanes-Oxley-Act (SOX), aber auch die Basel II Richtlinie der Banken unter anderem ein umfassendes Risikomanagement vor. In diesem Zusammenhang muss zum Beispiel nachgewiesen werden, wie die Daten im Unternehmen durch geeignete Richtlinien, Best Practices und Verfahren kontrolliert und geschützt werden.

Beim Thema Sicherheit darf nichts dem Zufall überlassen werden oder von einzelnen Mitarbeitern abhängen, schließlich kann die Existenz des Unternehmens auf dem Spiel stehen. Nur mittels interner Prozesse, Regeln und Arbeitsabläufe lassen sich alle relevanten Vorschriften einhalten sowie die erforderliche Datensicherheit und der notwendige Datenschutz gewährleisten.

Diese komplexen Identitäts-, Autorisierungs- und Sicherheits-Prozesse lassen sich allerdings nur mit Hilfe Workflow-basierter Komponenten bzw. umfassender Sicherheitslösungen zuverlässig implementieren. Diese müssen dabei so offen und flexibel sein, dass sie sich problemlos in die bestehende IT-Infrastruktur integrieren lassen.

## DATENSICHERHEIT ALS GRUNDVORAUSSETZUNG

Im Unternehmen müssen Mitarbeiter, Partner und Kunden immer und überall Zugriff auf alle, für sie relevanten, Informationen und Dienste haben. Gleichzeitig muss aber ein unerlaubter Zugriff auf die Unternehmensdaten zuverlässig verhindert werden. Die Existenz des Unternehmens kann auf dem Spiel stehen, wenn die Daten durch einen unglücklichen Zufall, einen Anwenderfehler, Sabotage oder durch den Ausfall einer entscheidenden Systemkomponente plötzlich und möglicherweise unwiederbringlich verloren gehen. Solchen Risiken ist jedes Unternehmen ausgesetzt und diese können jederzeit eintreten. Dabei geht es nicht nur um die Frage ob die Daten überhaupt wieder hergestellt werden können, sondern auch wie schnell das Unternehmen wieder in den Normalbetrieb zurückkehren kann. Jede auch noch so kurze Betriebsunterbrechung kann hohe Kosten zur Folge haben. Es sind daher entsprechende Mechanismen erforderlich, die eine regelmäßige automatische Sicherung aller Daten gewährleisten und eine schnelle Wiederherstellung der Daten im Fall der Fälle ermöglichen. Muss ein unterbrechungsfreier Betrieb oder eine Wiederaufnahme des Betriebs innerhalb kürzester Zeit sichergestellt werden, dann sind darüber hinaus entsprechende weitere Vorkehrungen zu treffen.

## UNTERNEHMENSWEITES IDENTITY- UND ACCESS-MANAGEMENT

Schon ein einziger verärgertes ehemaliger Mitarbeiter, der noch Zugang auf sensible Kundendaten hat, kann einen hohen Schaden im Unternehmen anrichten. Erschreckend dabei ist, dass Erfahrungen zufolge bis zu 30% der ehemaligen Mitarbeiter weiterhin Zugriff auf Unternehmensanwendungen besitzen. Bei Mitarbeitern in unterschiedlichsten Abteilungen und mehreren Niederlassungen, sowie zahlreichen geschäftskritischen Anwendungen – wie dies für viele Unternehmen charakteristisch ist – keine leichte Aufgabe. Effizient und damit sicher lösen lässt sich dieses Management der Nutzungs- und Zugriffsrechte nur durch ein automatisches Identitätsmanagement. Normalerweise wird für jede Anwendung eine eigene Benutzerkennung mit Passwort benötigt. Mit einer Identity- und Access-Management-Lösung lässt sich dagegen das Anlegen, Löschen und Ändern der Zugriffsrechte von Benutzern und ganzen Gruppen über vordefinierte Regeln (Policies) und Genehmigungen weitgehend automatisiert ausführen. Für die Administratoren bedeutet dies, dass neue Benutzer einfach und schnell integriert und Mitarbeiter, die das Unternehmen verlassen haben, innerhalb weniger Minuten komplett und zuverlässig aus dem Workflow herausgenommen werden können. Nach einer Untersuchung des Marktforschungsunternehmens Gartner lassen sich alleine durch die Automatisierung der Passwort-Verwaltung – welche nur einen kleinen Teil der Aufgaben des Identitätsmanagement darstellt – in einem Unternehmen mit 10.000 Angestellten fast 650.000 US-Dollar einsparen. Auch die Anwender profitieren von einer derartigen Lösung, durch Single-Sign-On können sie nach einer einmaligen Authentifizierung auf alle Anwendungen, für die sie berechtigt sind, zugreifen – ohne sich künftig erneut anmelden zu müssen.

## **SICHERHEIT – EINE FRAGE DES VERTRAUENS**

Vertrauen ist gut, Kontrolle ist besser. Nicht nur die Bedrohung von außerhalb, sondern auch von innerhalb des Unternehmens wird mehr und mehr zum Problem. Oftmals wird übersehen, dass auch Personen denen Vertrauen entgegengebracht wird oder die Sonderrechte bzw. besondere Zugriffsmöglichkeiten genießen, unerlaubt auf Daten zugreifen, sowie Daten stehlen oder manipulieren könnten. Da sie die meisten Sicherheitsmechanismen selbst implementiert haben, können sie diese auch meist problemlos umgehen oder aushebeln. Damit ein Datenbank-Administrator oder ein anderer hochprivilegierter User nicht auf Anwendungsdaten innerhalb der Datenbank zugreifen kann, sind technisch ausgereifere Mechanismen innerhalb der Datenbank erforderlich. Auch diese Sicherheitstechnologien sind nur dann effizient, wenn sie automatisiert werden können, flexibel und anpassungsfähig sind und sich durch Audits und Berichte überprüfen lassen.

## **COMPLIANCE – EINHALTUNG VIELFÄLTIGER REGELUNGEN UND GESETZE**

Nicht nur große Aktiengesellschaften und internationale Konzerne sondern ebenso kleine und mittelständische Unternehmen müssen heute hinsichtlich der Datensicherheit zahlreiche Regelungen und Gesetze beachten. Neben dem Bundesdatenschutzgesetz (BDSG) und anderen nationalen Gesetzen, gehören hierzu auch verschiedene EU-Richtlinien und internationale Konventionen, aber auch branchenspezifische Regelungen. Auch hier lässt sich die Einhaltung dieser vielfältigen Vorgaben und gesetzlichen Bestimmungen am Besten durch automatisierte Prozesse und Workflows gewährleisten. Durch den Einsatz einer geeigneten Lösung lässt sich eine ausreichende Risikovorsorge (Compliance) entsprechend den Forderungen von Richtlinien, wie Basel II, Sarbanes Oxley oder den einschlägigen Datenschutzgesetzen, nachweisen und gleichzeitig das Risiko einer persönlichen Haftung der Führungskräfte minimieren oder ganz vermeiden.

## FAZIT

Das IT-Management ist heute im Hinblick auf die Datensicherheit und den Datenschutz mit umfangreichen Anforderungen konfrontiert. Diese reichen von der Forderung nach einer mehr oder weniger unterbrechungsfreien Verfügbarkeit der Daten, über eine Beschränkung des Datenzugriffs nur für Berechtigte bis hin zur Einhaltung zahlreicher gesetzlicher und sonstiger Vorgaben. Traditionelle Sicherheitsmaßnahmen, wie eine einfache Zugriffskontrolle, sind hier längst nicht mehr ausreichend. Neben den Bedrohungen von außen kommt immer mehr eine Bedrohung von innen hinzu. Die Art und das Ausmaß der Gefährdung erfordern heute technisch ausgereifere Mechanismen innerhalb der Datenbank und den Einsatz umfassender Sicherheitslösungen. Sicherheitstechnologien sind jedoch nur dann effizient, wenn sie automatisiert werden können, transparent sind, sowie flexibel und anpassungsfähig präventiv schützen. Zudem muss deren Wirksamkeit jederzeit durch Audits überprüfbar und nachweisbar sein. Schließlich gehören die Daten zu den wichtigsten Gütern eines Unternehmens und da sollte nichts dem Zufall überlassen werden.

Die dargestellten Ausführungen sind ohne Gewähr und sollen Ihnen die Anforderungen und Perspektiven von Systemen zur Wahrung des Datenschutzes und der Datensicherheit näher bringen. Natürlich können diese Hinweise nicht alle gesetzlichen Regelungen und sonstigen Aspekte des Datenschutzes und der Datensicherheit beleuchten, und dienen daher nur der allgemeinen Information.

# CHECKLISTE

## Datensicherheit und Verfügbarkeit

Aktion	Priorität	ja	nein
Werden alle wichtigen Unternehmensdaten regelmäßig durch Backup gesichert?			
Können Sie bei einem Ausfall eines Systems ausreichend schnell wieder in den Normalbetrieb zurückkehren?			
Verfügen Sie über Möglichkeiten um die bei Datenverlust verlorenen Informationen schnell wieder herzustellen?			
Sind die auf externe Medien gesicherten Backup-Daten im Falle eines Diebstahls vor einem unerlaubten Zugriff geschützt?			
Prüfen Sie die Funktion und Vollständigkeit Ihrer Backup-Mechanismen regelmäßig?			
Müssen Sie einen unterbrechungsfreien Betrieb gewährleisten, um nach einem Ausfall innerhalb kürzester Zeit den Betrieb wieder aufnehmen zu können?			
Haben Sie Ihre Backups an einem sicheren Ort verwahrt, so dass diese nicht durch Diebstahl, Feuer oder Wasser verloren gehen können?			
Sind Ihre Unternehmensdaten auch bei der Übertragung an mobile Geräte ausreichend im Hinblick auf einen unberechtigten Zugriff geschützt?			

## Identity- und Access-Management

Aktion	Priorität	ja	nein
Können Sie sicherstellen, dass nur der jeweils berechtigte Personenkreis auf bestimmte Daten und Anwendungen zugreifen kann?			
Verfügen Sie über ein automatisiertes Identitätsmanagement, mit dem sich die Festlegung der Zugangsberechtigungen für die Anwender (Mitarbeiter, Partner, Kunden, etc.) zentralisieren und entsprechend der, im Unternehmen aufgestellten, Regeln gewährleisten lässt?			
Haben Sie effektive Maßnahmen im Einsatz, um internen Bedrohungen, wie beispielsweise Datendiebstahl oder Sabotage, wirksam vorzubeugen?			
Verfügen Sie über Möglichkeiten, um auch bei einer großen Zahl von Anwendern die Zugriffsrechte für Anwendungen und Daten effektiv zu verwalten und kontrollieren zu können?			
Nutzen Sie beim Austausch und der Übertragung vertraulicher Daten (z.B. Kreditkartendaten, Patientendaten) den Branchennormen entsprechende Sicherheitsprotokolle und -mechanismen?			

# CHECKLISTE

## Integrität und Compliance

Aktion	Priorität	ja	nein
Können Sie die Integrität der Unternehmensdaten gewährleisten und eine unerlaubte Manipulation von Daten effektiv verhindern?			
Werden alle Informationen, die im Zusammenhang mit der Rechnungslegung stehen, entsprechend den gesetzlichen Regelungen revisionssicher archiviert?			
Können Sie durch automatisierte Prozesse und Workflows gewährleisten, dass die gesetzlichen Bestimmungen eingehalten werden?			
Können Sie einen Nachweis für eine ausreichende Risikovorsorge (Compliance) entsprechend den Forderungen von Richtlinien, wie Basel II, Sarbanes Oxley oder den einschlägigen Datenschutzgesetzen, beibringen?			
Erfüllt Ihr Unternehmen die rechtlichen Vorgaben entsprechend dem Bundesdatenschutzgesetz (BDSG), Sarbanes-Oxley-Act (SOX) oder KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich)?			