

Sicherer Safe für die Kronjuwelen

Geschäftsdaten stellen für ein Unternehmen die Kronjuwelen dar, die es so zu sichern gilt, dass sie weder ausspioniert noch verfälscht werden können. Vor allem dürfen sie eines nicht: Verloren gehen.

von jürgen arnold* | juergen.hoefling@informationweek.de



Daten sind Wertgegenstände und gehören in den Tresor.

Auch für kleinere und mittelständische Unternehmen wird der Datenbestand zunehmend geschäftskritisch. So ist denn auch in nahezu jedem Unternehmen das Thema Datensicherheit in irgendeiner Form auf der Tagesordnung, die Sicht auf die Dinge und die Vorgehensweise sind aber oft dilettantisch. Letztlich geht es um die Themen Datensicherheit/Datenschutz, Datenintegrität und Datenverfügbarkeit, die im Folgenden kurz umrissen werden sollen, weil bei deren Bestimmung und Abgrenzung in vielen Unternehmen ziemlich viel Verwirrung herrscht.

Die großen Themen, um die es geht

Bei dem Themenkomplex Datenschutz/Datensicherheit handelt es sich darum, die Informationen vor dem Zugriff Dritter zu schützen. Dabei regelt der Datenschutz im Sinne des Bundesdatenschutzgesetzes die rechtliche Verantwortung, die Unternehmen bezüglich der Erhebung und der sicheren Verwahrung personenbezogener Daten haben. Datensicherheit dagegen bezieht sich auf EDV-Daten im weiteren Sinn, zum Beispiel auf die Sicherung von Konstruktionszeichnungen, Geschäftszahlen oder Kundenlisten, also die Sicherung all dessen, was man als die Vitaldaten einer Firma betrachten kann – und was gerade deswegen zum Ziel von Industriespionage werden könnte. Maßnahmen zur Datenintegrität haben bei jedem Datenzugriff sicherzustellen, dass die gelieferten Informationen auch der Wahrheit entsprechen. Manipulationen oder Fehlinformationen müssen entweder

unterbunden oder wenigstens als Fehlinformationen erkannt und gekennzeichnet werden.

Bei der Datenverfügbarkeit schließlich geht es darum, dafür zu sorgen, dass die Daten, wann immer sie gebraucht werden, in hinreichender Zeit verfügbar sind. Entsprechende Maßnahmen sind verschiedene Stufen der Redundanz, Datensicherung und Notfallplanung.

Schutz-Szenarien

Ein Konzept für den Umgang mit den Daten, die in einem Unternehmen anfallen, ist nur dann gut, wenn alle diese drei Komponenten berücksichtigt werden. Nimmt man sich der Aufgabenstellungen im Einzelnen an, ergeben sich die folgenden Szenarien.

Um im Sinne von Datenschutz und Datensicherheit den unerlaubten Zugriff auf die Daten unterbinden zu können, sind verschiedene Zugriffsebenen zu unterscheiden. Um den Zugriff auf das Firmennetz aus dem Internet zu regeln, werden heute fast überall Firewalls eingesetzt, die von der Stange zu kaufen sind und durchweg einen sehr hohen Sicherheitsstandard erreicht haben. Allerdings ist hier darauf zu achten, dass zum einen die Einstellungen der Firewalls sinnvoll und sicher sind und dass es zum anderen keinerlei weiteren Zugang zum Firmennetz gibt. Leider sind unzureichend gesicherte WLAN-Zugänge oder ISDN-Einwahlleitungen zu Firmennetzen immer noch an der Tagesordnung.

In den Bereich Datensicherheit gehören auch Firmenrichtlinien wie das Deaktivieren von Diskettenlaufwerken oder von USB-Ports an Arbeitsrechnern, um das Mitnehmen von Daten zu verhindern. Dabei ist bei den Sicherheitsvorgaben natürlich zwischen Sicherheit und Produktivität abzuwägen.

Die ersten Schritte zur Sicherung der Datenintegrität sind identisch mit denen des Datenschutzes: Der Zugriff wird auf das sachlich und verfahrenstechnisch notwendige Maß beschränkt. Außerdem werden Änderungsmöglichkeiten eingegrenzt und Lösungen wie beispielsweise Archivsysteme installiert, welche die Verwaltung und Überwachung aller archivierten Daten garantieren.

Das Ziel der Datenverfügbarkeit ist es, die benötigten Daten jederzeit zugänglich zu halten, um die Ge-

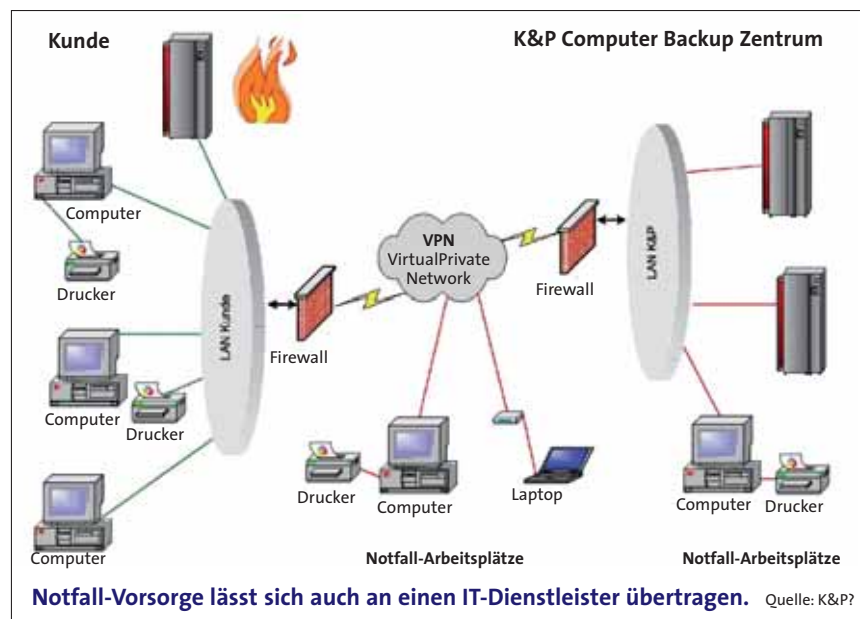
schäftsprozesse nicht zu gefährden. Ein erster Schritt in diese Richtung besteht darin, die relevanten Datenkomponenten in einem Unternehmen zu identifizieren und ein Konzept für die Verteilung der Daten auf den Systemen zu erarbeiten. Oft werden wichtige Kundendaten immer noch nur auf den Notebooks der entsprechenden Außendienstmitarbeiter vorgehalten, was sowohl aus dem Blickwinkel der Datensicherheit wie der Datenverfügbarkeit nicht befriedigen kann. Firmenrelevante Daten gehören auf zentrale Server. Die entsprechenden Server, Netzwerkkomponenten und Stromversorgungseinheiten sind dabei redundant auszuliegen.

Versäumnisse und Fehlhandlungen

Trotz aller Vorkehrungen kommt es immer wieder zu Datenverlusten. Deshalb werden die klassischen Sicherungsprogramme benötigt, mit denen die Daten auf weitere Medien kopiert, archiviert oder an einen anderen Standort ausgelagert werden können. Obwohl inzwischen so gut wie alle größeren Firmen zentrale Backup- und Archivsysteme betreiben, sind diese Sicherungen aber oft weder vollständig noch qualitativ befriedigend. In vielen Fällen wird dies aber erst erkannt, wenn es zu spät ist, das heißt, wenn die vermeintlich verfügbaren Informationen rückgesichert werden sollen.

Ungenügende Sicherungsdaten entstehen durch folgende Versäumnisse und Fehlhandlungen:

- Die Vorschriften für die Sicherung sind nicht vollständig. Oft unterbleibt eine aktuelle und vollständige Aufstellung der relevanten Daten oder die Regeln in den Backupssystemen erzeugen keine vollständigen Sicherungen.
- Firmen-Richtlinien sind nicht vorhanden oder werden nicht eingehalten. Hat es sich beispielsweise eingebürgert, dass jeder Mitarbeiter »seine« Daten auf seinem Rechner vorhält, ist eine vollständige Datensicherung kaum mehr möglich.
- Dateien sind offen. Die üblichen Sicherungssysteme kopieren Dateien bitweise. Damit dies reproduzierbar funktioniert, dürfen sich aber die Dateien während des Sicherungslaufs nicht verändern. Backup-systeme erkennen zwar üblicherweise das Problem, können es aber nicht lösen. Eine Lösung bietet hier ein definierter Zeitplan mit zeitgesteuerten Abläufen. Eventuell sind auch erweiterte Lösungen und Plugins einzusetzen, die applikationsspezifisch offene Dateien verarbeiten können.
- Man verlässt sich auf einzelne Sicherungen. Das meistverwendete Sicherungsmedium ist heute immer noch das Magnetband. Magnetbänder haben zwar eine extrem hohe Stabilität und Lebensdauer, allerdings ist es immer noch fahrlässig, sich bei der Sicherung auf ein einzelnes Band zu verlassen.
- Ausgaben der Backuproutinen werden nicht kontrolliert. Üblicherweise werden von den Sicherungs-



programmen Fehler protokolliert und auch gemeldet. Dadurch könnten Ausfälle von einzelnen Dateien und ganzen Datenbereichen erkannt werden. Oft hat aber das Bedienpersonal der Systeme dafür nicht die Qualifikation.

- Wenn Magnetbänder hohen Temperaturschwankungen ausgesetzt sind oder in der Nähe von starken Magnetfeldern gelagert werden, erhöht sich die Wahrscheinlichkeit des Datenverlusts deutlich.

Notfallplan auf Papier vorhalten

Für den verantwortlichen Umgang mit den eigenen Daten benötigt ein Unternehmen ein Gesamtkonzept, das die vorhandenen Speicherdaten im Lichte der hier erörterten Aspekte analysiert und bewertet. Aufbewahrungspflichten sind dabei ebenso in Betracht zu ziehen wie Folgekosten bei Systemabstürzen oder anderen Notfällen. Desgleichen sind Systempriorisierungen mit einer Bewertung der Auswirkungen von Ausfällen zu berücksichtigen sowie der menschliche Faktor. Zusätzlich sind die Konzepte regelmäßig auf ihre Aktualität zu überprüfen. Ihre Tauglichkeit muss durch zyklische, aussagekräftige Tests bewiesen werden. Ein im Ernstfall auch funktionierender Notfall-Plan enthält die Verfahren und die Reihenfolge zur Wiederherstellung einzelner oder aller Daten, entsprechend der Dringlichkeit und der logischen Zusammenhänge. Dieser Plan muss im Übrigen auf Papier ausgedruckt werden. Wer nämlich im Falle eines EDV-Notfalls auf einen Katastrophenplan zugreifen will, der nur in elektronischer Form auf einem Server gespeichert ist, könnte mit seinen Rettungsversuchen schon scheitern, bevor er mit ihnen überhaupt begonnen hat. ■

* Dr. Jürgen Arnold ist Bereichsleiter Software bei K&P Computer GmbH