

# Zehn Schritte zum Schutz sensibler Daten

Der Schutz vor Datenverlust ist für Unternehmen aller Größen ein wichtiges Thema. Einer der Gründe dafür ist die Tatsache, dass die zunehmend mobilen Angestellten immer mehr sensible Daten mit sich führen. Unternehmen kaufen heutzutage mehr Laptops als Desktop-Computer, und diese Laptops enthalten jede Menge an wichtigen Informationen: Datensätze zu Patienten, Kunden und Angestellten, geistiges Eigentum, Finanzdaten und Kennwörter.

Da immer mehr Daten immer häufiger außerhalb der Netzwerkgrenzen im Umlauf sind, stellen sie für Internetkriminelle ein lohnendes Ziel dar. Und Sicherheitsvorfälle nehmen zu. Laut dem McAfee-Bericht zum Thema Wirtschaft ohne Sicherheit beobachtete das Forschungsteam im ersten Halbjahr 2009 fast ebenso viele neue Malware-Varianten (1,2 Millionen eindeutige Varianten) wie im gesamten Jahr 2008 (1,5 Millionen).

Die Kosten für die Behebung einer einzigen Datenkompromittierung können schnell die Kosten übersteigen, die für einen sicheren Schutz angefallen wären. Tatsächlich kam es im letzten Jahr bei einem Fünftel aller mittelständischen Unternehmen zu einem Sicherheitsvorfall – mit Einnahmeverlusten von durchschnittlich 41.000 US-Dollar.<sup>1</sup>

## Schritt 1: Analyse der Vorschriften, denen Ihr Unternehmen unterliegt.

Ihr Unternehmen unterliegt jeder Menge Gesetze, Vorschriften und Branchenrichtlinien. Während sich früher nur die Bereiche Gesundheitsversorgung und Finanzen sowie Behörden mit Compliance befassen mussten, bleibt heute kaum ein Unternehmen von entsprechenden Regelungen und Vorschriften verschont. Unabhängig vom Standort und der Größe – jedes Unternehmen sollte über einen gut durchdachten Datenschutzplan verfügen.

Das beginnt damit, dass Sie vielleicht Gesetze und Vorschriften der Länder einhalten müssen, in denen sich Ihre Kunden und Lieferanten befinden. Bedenken Sie jedoch, dass diese Regelungen meist dazu dienen sollen, die Daten zu schützen, mit denen Personen, Patienten, Kunden oder Angestellte eindeutig identifiziert werden können. Gleichzeitig werden diese Anforderungen häufig schon erfüllt, wenn diese wichtigen Daten durch Verschlüsselung geschützt sind. Natürlich müssen Sie herausfinden, wie diese Anforderungen auf Ihr Unternehmen anzuwenden sind. Insgesamt gilt jedoch, dass Datenschutz immer sinnvoll ist.

## Schritt 2: Identifizierung unbekannter Inhaltsrisiken

Für Mitarbeiterdaten, Kreditkarteninformationen oder medizinische Unterlagen gilt der gleiche Grundsatz: Sie benötigen die richtigen Tools, um Ihr Netzwerk auf bekannte Risiken prüfen zu können. Diese Tools sollten Dateifreigaben, Datenbanken, Content-Management-Datenbanken und alle anderen Datenspeicher scannen können, die in Ihrem Unternehmen eingesetzt werden. In vielen Fällen wissen Unternehmen, wo sich ein Teil dieser Daten befindet – beispielsweise auf dem Server der Finanz- oder Personalabteilung. Die Erkennungsmechanismen müssen jedoch in der Lage sein, alle Orte zu finden, an denen sich vertrauliche Informationen befinden. Denken Sie dabei zum Beispiel an ältere Server, Desktop-Computer oder andere Ressourcen, die vom IT-Team schon lange nicht mehr gewartet werden. Außerdem müssen die Erkennungsmechanismen in der Lage sein, regelmäßig automatisch nach neuen Ressourcen zu suchen, die in Ihrem Netzwerk erstellt oder hinzugefügt werden.

### Kernpunkte

Unternehmen müssen ihre Daten schützen, da die Folgen bereits bei einer einzigen Kompromittierung verheerend sein können:

- Entgangene Einnahmen
- Hohe Strafen
- Rufschädigung des Unternehmens
- Verlorenes Kundenvertrauen

Mit diesen 10 empfohlenen Verhaltensweisen können Sie Ihre sensiblen Daten schützen:

- Erfassung aller Vorschriften, denen Ihr Unternehmen unterliegt
- Identifizierung unbekannter Inhaltsrisiken
- Kommunikation mit den Datennutzern
- Wissen, wo sich vertrauliche Daten befinden
- Festlegung offizieller Regeln zur Erstellung und Änderung von Richtlinien
- Einrichtung von Mechanismen zur Warnung und Durchsetzung
- Delegation von Kontrollen und Verantwortungsbereichen
- Maximierung vorhandener IT-Investitionen
- Entscheidung für einen plattform-basierten Ansatz
- Bedarfsgerechte Anpassung der Lösung

1. Bloor Research: The Security Paradoxon Survey („Umfrage Das Sicherheitsparadoxon“), Dezember 2009.

**Aktuelle Beispiele für schwerwiegende Datenkompromittierung:**

- *Februar 2010* – Festplatten mit Gesundheitsdaten von 500.000 Kunden wurden bei BlueCross BlueShield gestohlen. Zu den Daten gehörten Namen, Adressen, Diagnosen, Sozialversicherungsdaten und Geburtsdaten.
- *Januar 2009* – Ein Laptop mit Namen, Adressen, Sozialversicherungsdaten und Fingerabdrücken wurde aus einem verschlossenen Büro der Continental Airlines in Newark, New Jersey, gestohlen.
- *August 2009* – Ein Laptop wurde von einem Dienstleister der amerikanischen Nationalgarde gestohlen. Auf dem Laptop waren personenbezogene Daten von 131.000 Soldaten gespeichert, einschließlich Namen, Sozialversicherungsdaten und Bonuszahlungen.

**Schritt 3: Kommunikation mit den Datennutzern**

Effizienter Datenschutz beginnt damit, dass genau bekannt ist, welche Daten im Unternehmen besonders wichtig sind. Beziehen Sie die Verantwortlichen mit ein, und erkundigen Sie sich nach den Daten, die von den jeweiligen Abteilungen generiert und genutzt werden. Wer verarbeitet welche Daten? Was machen diese mit den Daten? Wie arbeiten sie zusammen? Wo werden die Daten gespeichert und archiviert? Welcher Mitarbeiter in der Abteilung fungiert als autorisierter Kontakt, wenn Probleme auftreten?

Die Mitarbeiter in den einzelnen Abteilungen kennen ihre Daten, sodass sie diese wichtigen Fragen leicht beantworten können. Es wäre weder angemessen noch sinnvoll, die Entscheidung über die Vertraulichkeit bestimmter Daten vom IT-Team treffen zu lassen.

**Schritt 4: Wissen, wo sich die Daten befinden**

Die Antwort auf die Frage nach dem Speicherort Ihrer Daten ist nicht so offensichtlich, wie es im ersten Moment scheint. Sie denken natürlich sofort an Dateiserver, Datenbanken und die einzelnen Computer. Was ist aber mit Sicherungslaufwerken, USB-Speichermedien, Smartphones und anderen persönlichen Geräten, die Ihre Mitarbeiter mit ins Büro bringen? Und was ist mit den Systemen, die sie zuhause nutzen? Denken Sie dabei nicht nur an die Geräte, die Ihr Unternehmen offiziell an Mitarbeiter verteilt hat. Sie müssen genau wissen, wer auf diese persönlichen Systeme und Geräte zugreifen kann.

**Schritt 5: Festlegung offizieller Regeln zur Erstellung und Änderung von Richtlinien**

Wahrscheinlich werden zahlreichen Personen daran beteiligt sein, die Richtlinien zum Schutz der Daten in Ihrem Unternehmen zu definieren. Denken Sie darüber nach, wie Ergänzungen und Änderungen der Richtlinie vorgeschlagen, vermittelt und umgesetzt werden können. Auf diese Weise lassen sich Unterbrechungen der normalen Geschäftsabläufe vermeiden.

**Schritt 6: Einrichtung von Mechanismen zur Warnung und Durchsetzung**

Für eine effiziente Sicherheitsstrategie benötigen Sie immer auch Mechanismen, nach denen bei Bedrohungen Meldungen ausgegeben und in Echtzeit Maßnahmen getroffen werden können. Die Benachrichtigungen, die an die IT-Administratoren sowie an Verantwortliche für Personalfragen, Rechtsfragen und Compliance gesendet werden, sind zweifellos wichtig. Wenn jedoch die Endbenutzer ebenfalls Warnungen erhalten, erreichen Sie damit, dass Ihre Mitarbeiter im richtigen Umgang mit vertraulichen Daten geschult werden und ihr Verhalten anpassen können.

Die Umsetzung der Richtlinien kann darin bestehen, dass E-Mail-Benachrichtigungen über eine Datenschutzverletzung versendet werden. Sie kann aber auch proaktive Maßnahmen umfassen, damit vertrauliche Daten vor dem Verlassen des Unternehmens immer verschlüsselt werden. Sie können ebenso festlegen, dass Zugriff auf Webmail-Dienste wie Google Mail und Yahoo! Mail sowie öffentliche Instant-Messaging-Dienste wie Windows Live Messenger und Yahoo! Messenger blockiert werden, da dies typische Kanäle für Datenschutzverletzungen sind.

**Schritt 7: Delegierung von Kontrollen und Verantwortungsbereichen**

Bisher haben wir uns damit befasst, wie wichtig es ist, Risiken zu kennen und Richtlinien und Mechanismen zum Schutz vertraulicher Daten einzurichten. Der nächste Schritt besteht darin, die Kontrolle über Richtlinien zu delegieren und die Verantwortungsbereiche für den Fall einer Datenschutzverletzung festzulegen.

Es ist offensichtlich, dass diese Personen unterschiedliche Zugriffsrechte auf Daten und Richtlinien zum Schutz dieser Daten benötigen. So müssen Sie wahrscheinlich ein oder zwei Mitarbeiter benennen, die vertrauliche Daten identifizieren, Richtlinien definieren und schließlich sicherstellen, dass diese Informationen entsprechend geschützt werden.

Erheblich wichtiger ist jedoch die Delegierung von Maßnahmen, die bei einem Sicherheitsvorfall erforderlich sind. Sollen die Mitarbeiter, deren Daten kompromittiert wurden, selbst eine Behebung versuchen oder sich an einen Compliance-Beauftragten wenden? Was ist zu tun, wenn der Desktop-Computer eines Endbenutzers neu konfiguriert werden muss und das Eingreifen von IT-Mitarbeitern erforderlich ist? Was ist zu tun, wenn Benutzerschulungen notwendig sind? Und wie soll die Behebung von Problemen durchgeführt und bis zum erfolgreichen Abschluss überwacht werden? Für solche Fälle brauchen Sie festgelegte Workflow-Prozeduren. Noch wichtiger: Ihr Unternehmen muss sicherstellen, dass die betroffenen sensiblen Daten geschützt und nur wenigen berechtigten Benutzern und Managern zugänglich sind.

### Schritt 8: Maximierung vorhandener IT-Investitionen

Im Laufe der letzten 15 bis 20 Jahre haben Unternehmen in erheblichem Maße in verschiedene Internettechnologien investiert. Durch den kontinuierlichen Ausbau der Unternehmensnetzwerke konnten neue Anwendungen für diese Netzwerke eingeführt und die Sicherheit immer weiter verbessert werden. Daher sollte der Schutz Ihrer sensiblen Daten den bestmöglichen Nutzen dieser Technologien ermöglichen – sowohl in Bezug auf ihre Funktionen als auch auf die Fähigkeiten Ihrer Mitarbeiter.

Beispielsweise sollte die ideale Lösung zur Richtlinienumsetzung vorhandene Infrastrukturelemente wie E-Mail-Gateways, Netzwerk-Switches, Webproxies und Verschlüsselungslösungen einbinden. Ebenso sollte die Datenschutzlösung Eindringungserkennungssysteme, Firewalls und Lösungen zur Schwachstellenbewertung nutzen. Auf diese Weise erreichen Sie eine bessere Transparenz der Netzwerkaktivitäten auf unterster Ebene und verbessern die Genauigkeit und allgemeine Effektivität der Datenschutzlösung.

### Schritt 9: Entscheidung für eine plattformbasierten Ansatz

Vergewissern Sie sich, dass alle eingesetzten Lösungen eine zentrale Verwaltung und genau die Art von Tools zur Bereitstellung, Umsetzung und Berichterstellung bieten, die den Anforderungen Ihres Unternehmens entsprechen. Der bislang übliche Einsatz der jeweils klassenbesten Lösungen kann schnell zu zahlreichen getrennten Lösungen unterschiedlicher Hersteller führen, die besonderer Aufmerksamkeit bedürfen und deren Sicherheit zu wünschen übrig lässt. Die Kosten eines solchen getrennten Ansatzes können schnell ansteigen, da Ihre Mitarbeiter für unterschiedliche Systeme ausgebildet werden müssen. Sie können keine unternehmensweite Berichterstellung nutzen, und die Kosten für die Schulung der Endbenutzer sind unnötig hoch. Zu schlechter Letzt wird im Falle eines Problems jeder Anbieter die anderen verantwortlich machen.

Unsere Kunden sind der Meinung, dass ein plattformbasierter Ansatz die bessere Wahl ist, und Studien belegen diese Einschätzung. Dank einer zentralen Plattform können Sie mit einer Lösung anfangen und weitere nach Bedarf hinzufügen – ohne dass Sie dabei die Infrastruktur replizieren oder umfangreiche neue Schulungen abhalten müssen. Der plattformbasierte Ansatz gewährleistet auch, dass die Bereitstellung problemlos erfolgt und Lösungen von Drittanbietern sich mithilfe bekannter Schnittstellen einklinken können.

### Schritt 10: Bedarfsgerechte Anpassung der Lösung

Viele Kunden legen Wert darauf, Probleme erst dann anzugehen, wenn sie auftreten. Sie können mit einem Laptop-Schutz, Dateiverschlüsselung, Verschlüsselung von Wechseldatenträgern oder einem Schutz vor Datenverlust beginnen, ganz wie es den aktuellen Bedürfnissen entspricht.

Der Ansatz von McAfee zum Datenschutz beginnt damit, dass Sie auswählen können, welche Lösung für Sie die sinnvollste ist. Bei Bedarf können Sie zu einem beliebigen Zeitpunkt Erweiterungen vornehmen. Mit dem McAfee-Ansatz können Sie schnell ein taktisches Problem lösen und dennoch für strategischen Erfolg gerüstet sein.

### Wählen Sie McAfee-Datenschutzlösungen

Nur McAfee bietet ein Portfolio mit Datenschutzlösungen in der Breite und Tiefe an, die für den umfassenden Schutz der wertvollsten Ressourcen in Ihrem Unternehmen notwendig ist: Ihrer Daten. Ganz gleich, ob Sie die McAfee® Data Loss Prevention-Lösungen (McAfee DLP) einsetzen oder Ihre Daten mit einer der McAfee-Verschlüsselungslösungen schützen möchten: Dank McAfee können Sie Daten auf Laptops und USB-Laufwerken schnell und einfach verschlüsseln, volle Transparenz über Daten erreichen, die Ihre Endgeräte verlassen, sowie Endgerätekontrollen durchsetzen. Und das Beste daran: Die Bereitstellung und Verwaltung kosten erheblich weniger Zeit, als Sie denken.

Sie verhindern Datenkompromittierung, bevor sie auftritt, gewährleisten Compliance mit Branchenrichtlinien und staatlichen Vorschriften und schaffen das, ohne die täglichen Geschäftsaktivitäten zu unterbrechen. Wenn Sie diese 10 Schritte zum Einsatz von McAfee DLP-Lösungen befolgen, werden Sie überrascht sein, wie einfach das ist.

