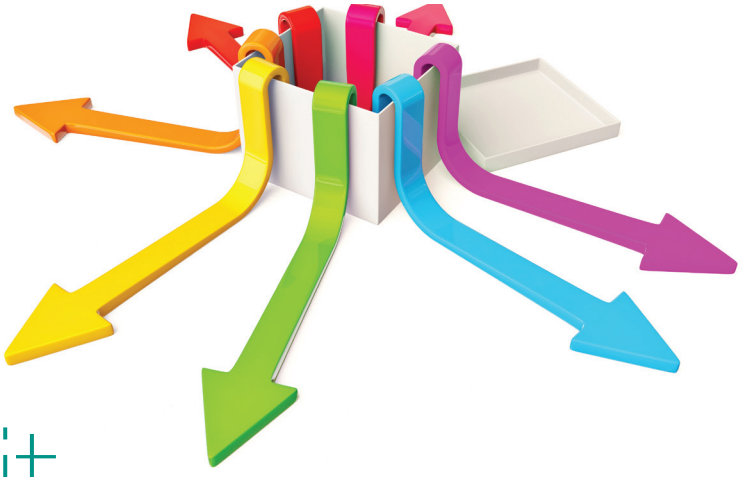
SOPHOS



Probleme mit Dropbox?

Die richtige Datenschutzstrategie schafft Abhilfe

Autoren: **Chris Pace**, Product Marketing Manager,
und **Barbara Hudson,** Product Marketing Manager

Schätzungen zu Folge wurden bereits über 50 Millionen Dateien über öffentliche Cloud Storage-Dienste ausgetauscht. Die Kehrseite der freien Zugänglichkeit und Benutzerfreundlichkeit solcher Angebote besteht jedoch darin, dass IT-Richtlinien zur Übertragung vertraulicher Daten häufig ins Hintertreffen geraten. Zur Bewältigung zunehmender Datenvolumen im Unternehmen benötigen IT-Manager eine erschwingliche und sichere Speicherlösung. In unserem White Paper wird in drei einfachen Schritten erläutert, wie Sie Ihre Anwender beim Zugriff auf die Cloud unterstützen können, ohne dabei Ihre Daten oder Ihr Unternehmen zu gefährden.

Daten sind überall

Was bedeutet eigentlich „Cloud Computing“ oder „die Cloud“? Die Cloud, ein viel diskutiertes Schlagwort in den Medien, bezeichnet eine externe, virtuelle Speicherlösung der nächsten Generation. Im IT-Bereich lassen sich hiermit immense Datenvolumen erfassen, speichern, umverteilen und verwalten. Benutzern bietet die Cloud die Möglichkeit, eigene Daten zu speichern oder unternehmensextern auszutauschen.

Dank Cloud Storage-Diensten, wie Dropbox (mit über 25 Millionen Benutzern im April 2011), Egnyte oder SkyDrive von Microsoft kann von überall und mit beliebigen Geräten auf Dateien zugegriffen werden. Doch wie wirkt sich dies auf die Datensicherheit aus? Da Mitarbeiter heutzutage häufig von unterwegs arbeiten, muss Ihre Datenschutzlösung standortunabhängig immer die gleiche Sicherheit bieten. Erschwerend kommt hinzu, dass Unternehmen in aller Welt immer wieder aufgrund von Datendiebstahl in Negativschlagzeilen geraten.

Dem Datendiebstahl-Report von Verizon 2011 zufolge wurden im Jahre 2010 über 4 Millionen Datensätze kompromittiert. Dabei gingen mehr als 92 % der Übergriffe nicht etwa von abtrünnigen Mitarbeitern oder Geschäftspartnern, sondern von Hackern aus. Auch die finanziellen Einbußen durch Datenlecks steigen immer mehr an. Aus einem aktuellen Report des Ponemon Institute in den USA geht hervor, dass die Kosten pro missbrauchtem Datensatz im Schnitt bei 214 USD (ca. 160 EUR) und pro Datenschutzverletzungsvorfall bei 7,2 Millionen USD liegen.[1]

Es ist daher wichtiger denn je, Laptops und Laufwerke sowie Dateien auf Servern, in der Cloud und auf Mobilgeräten befinden, zu sichern. Womöglich nutzen Ihre Mitarbeiter die Cloud bereits ohne Ihr Wissen oder Ihre Zustimmung. Bei der Ausarbeitung Ihrer Sicherheitsstrategie für die Cloud sollten Sie stets bedenken, was Daten für Ihr Unternehmen bedeuten.

- Laden Ihre Mitarbeiter Dateien in die Cloud hoch?
- Welche Dienste werden genutzt und in welcher Form?
- Enthalten die Dateien sensible Unternehmensdaten?
- Werden die Dateien verschlüsselt?
- Wo werden Ihre Daten archiviert?

1. Ponemon Institute, „Second Annual Cost of Cyber Crime Study: Benchmark Study of US Companies“, August 2011

Die Cloud ist überall

Tatsächlich erhalten Cloud-Speicheranbieter Vollzugriff auf Ihre Daten und kontrollieren, wo diese gespeichert werden. Der Standort eines Managed Service Providers für die Cloud ist zwar oft bekannt, doch meist werden Benutzer nicht im Detail über die Infrastruktur oder Sicherheitsmechanismen des MSPs informiert. Werden Ihre Daten etwa in einem mehrinstanzenfähigen oder einem isolierten Container archiviert? Werden SAS-70 oder Umgebungssteuerungen verwendet? Auch in Zusammenhang mit der Einhaltung von Datenschutzrichtlinien wirft Cloud Storage Probleme auf. Unter Umständen werden die Daten in einem anderen Land gespeichert. Für Auditoren, die die Datensicherheit und Überwachungskette in Ihrem Unternehmen bewerten, kann dies problematisch sein. Mangelnde Kontrollen und Prozesse bergen zudem das Risiko, dass Unbefugte auf nicht hinreichend abgesicherte Daten zugreifen, für die besondere Sicherheitsvorkehren gelten.

Laut einer Umfrage von Ernst & Young aus dem Jahr 2011 nutzen oder testeten bereits 61 % der befragten Unternehmen Cloud Storage. In 52 % der Unternehmen wurden jedoch noch keine Kontrollmechanismen zur Abschwächung des Risikos eingeführt.[2]

Vor nicht allzu langer Zeit wurden statt Cloud Storage noch USB-Laufwerke und statt Diensten wie Dropbox noch VPN zum Speichern von Daten genutzt.
Der Zugriff auf und die Speicherung von Daten haben sich aufgrund der sogenannten Consumerization der IT und der schnellen Internetverbindungen am Arbeitsplatz, zu Hause sowie auf Mobilgeräten grundlegend geändert.

Die Benutzer sind jetzt wesentlicher unabhängiger und flexibler. In den meisten Fällen wählen sie Dienste aus, mit denen sie vertraut sind. IT-Richtlinien im Unternehmen bleiben hierbei jedoch häufig unbeachtet. Zu viel Kontrolle für die Endbenutzer birgt Risiken.

4,0

Millionen verunreute Datensätze

allein im Jahr 2010 (Quelle: Verizon 2011 Data Breach Investigation Report).

7,2

Millionen US-Dollar pro pro Datenschutzverletzungsvorfall

Die Kosten pro missbrauchtem Datensatz liegen im Schnitt bei 214 USD.

92

Prozent aller Datenbrüche wurden von externen Hackern verübt

und nicht von ehemaligen Mitarbeitern oder Geschäftspartnern.

2. 2011 Ernst & Young Global Information Security Survey

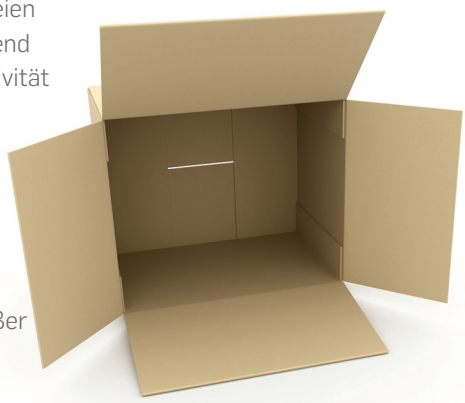
Risiken nachlässiger Sicherheitsvorkehrungen

Ohne klar abgegrenzte Richtlinien, Mitarbeiterschulungen und offiziell genehmigte Mechanismen zum Datenaustausch greifen Endbenutzer nicht selten auf komfortable Alternativen zurück und lassen Sicherheit und Compliance außer Acht. Zu solchen Alternativen zählen verbrauchernahe Dropbox-Lösungen, nichtgewerbliche FTP-Server, die Übertragung von Dateien als E-Mail-Attachments sowie intern entwickelte Anwendungen und Skripts.

Da diese Lösungen meist gratis genutzt werden können und von den gängigsten Plattformen unterstützt werden, haben sie in Unternehmen aller Größen Einzug gehalten und wurden nicht selten in kritische Workflows eingebunden.

Risiken verbrauchernaher Dropbox-Lösungen und intern entwickelter Programme

- **Nicht unterstützte Infrastruktur:** Aller Wahrscheinlichkeit nach werden verbrauchernahe Lösungen den Anforderungen von Unternehmen nicht gerecht. Die Entwickler interner Programme und Skripts sind unter Umständen bereits aus dem Unternehmen ausgeschieden.
- **Missachtung von Richtlinien:** Da sich die Programme an den Bedürfnissen der Endverbraucher orientieren und sich interne Entwicklungsstandards ändern können, wird den Sicherheits- und Compliance-Anforderungen im Unternehmen nicht immer Rechnung getragen.
- **Ignorierte Gefahr:** Die Risiken in Unternehmen, in denen Mitarbeiter weiterhin Dateien über nicht unterstützte Umgebungen austauschen, werden mitunter nicht hinreichend analysiert. Der alt bekannte Konflikt zwischen Unternehmensrichtlinie und Produktivität der Endbenutzer kommt in diesem Bereich besonders zum Tragen.



Risiken der Dateienübertragung als E-Mail-Attachments

- Größe von Attachments: In der Regel werden E-Mail-Attachments in Unternehmen auf 10 MB beschränkt.
- Performance: E-Mail-Programme wurden nicht für die Verarbeitung besonders großer Dateien konzipiert.
  So werden E-Mails mitunter nicht rechtzeitig oder überhaupt nicht zugestellt.
- Speicher: Der freie Speicher wird schnell durch große Attachments (mitunter mehrere Kopien) aufgebraucht. Gleiches gilt für kleine Attachments, die an viele Empfänger weitergeleitet werden.
- Sicherheit und Compliance: Nur allzu häufig wird bei der Richtlinienumsetzung auf die Entscheidungen einzelner Benutzer statt auf automatisierte Enforcement-Lösungen von Spezialisten vertraut.

Quelle: Aberdeen Group, Januar 2012.

Ausarbeitung einer Datenschutzstrategie für die Cloud

Die folgenden Erwägungen sollten in Ihre strategische Planung einfließen:

- Wer verwaltet Ihre Daten?
- Behalten Sie die Kontrolle über Ihre Daten?
- Welche Konsequenzen drohen im Falle einer Datenschutzverletzung?
- Wie wahrscheinlich sind Datenlecks?
- Können Sie die Sicherheit Ihrer Daten garantieren?

Wenn Ihre Mitarbeiter Cloud Storage ohne Ihr Wissen bzw. Ihre Zustimmung und unter Missachtung von Verschlüsselungsrichtlinien nutzen, können Sie diese Fragen nicht immer beantworten. Wenn Sie den Benutzerzugriff auf Storage und Anwendungen in der Cloud nicht kontrollieren und nicht alle sensiblen Daten verschlüsseln, sollten Sie umgehend entsprechende Mechanismen implementieren.

In nur drei einfachen Schritten können Sie den verantwortungsbewussten Umgang mit Cloud-Diensten gewährleisten und gleichzeitig den Datenschutz im Unternehmen optimieren.

1. Implementieren webbasierter Richtlinien mit URL-Filterung

Mit der URL-Filterung, einem Feature zur Kontrolle aufgerufener Websites im Unternehmen, können Sie den Zugriff auf Seiten wie „Dropbox.com“ regulieren. Dank multipler Profileinstellungen können Sie außerdem den Zugriff je nach Sachlage auf ausgewählte Benutzer beschränken.

2. Kontrolle von Anwendungen mit Application Control

Mit Application Control-Funktionen können Sie die Nutzung bestimmter Anwendungen allen Mitarbeitern oder ausgewählten Gruppen gestatten bzw. verweigern. Im Falle von Dropbox werden mit Application Control etwa die Installation und Ausführung der Anwendung verhindert und die ausführbare Datei wird blockiert.

3. Verschlüsseln von Daten

Lassen Sie die Daten automatisch vor dem Hochladen in die Cloud von allen verwalteten Endpoints verschlüsseln. Über ein Kennwort können die Benutzer so weiterhin von überall auf allen beliebigen Geräten auf verschlüsselte Dateien zugreifen.

Mit einer Verschlüsselungslösung behalten Sie die Kontrolle über Ihre Daten

Dank einer umfassenden Lösung zur direkten Verwaltung der Verschlüsselung von lokal oder in der Cloud gespeicherten Dateien können Benutzer ihre eigenen Schlüssel zum Absichern bestimmter Dateien festlegen und verwalten. Hiermit können die Benutzer jederzeit auf Dateien hinter der Firewall oder in der Cloud zugreifen. Zudem werden stets einheitliche Verschlüsselungsstandards umgesetzt. So werden mit SafeGuard Encryption für Cloud Storage etwa sämtliche Dateien verschlüsselt, egal ob sie auf ein anderes Laufwerk, Netzwerk oder Gerät kopiert bzw. verschoben werden.

Da die Dateien immer verschlüsselt werden und Ihre Mitarbeiter stets über ihre eigenen Schlüssel verfügen, steht den Benutzern die Wahl eines Cloud Storage-Dienstes frei. Darüber hinaus erfolgt die Verschlüsselung vor der Synchronisierung von Daten auf dem Client, so dass Sie die vollständige Kontrolle über die Sicherheit Ihrer Daten behalten. Über Sicherheitslecks beim Cloud Storage-Anbieter müssen Sie sich keine Gedanken mehr machen.

Autorisierte Benutzer oder Gruppen greifen über zentrale Schlüssel auf Dateien zu, die für andere verschlüsselt bleiben. Sollte ein Web-Schlüssel abhanden kommen, weil ein Benutzer beispielsweise sein Kennwort vergessen hat, kann der Sicherheitsbeauftragte im Unternehmen die Schlüssel abrufen und so den autorisierten Mitarbeitern Zugriff auf die Datei gewähren.

Zudem können Sie Konten bei Dropbox.com für die einzelnen Geschäftseinheiten erstellen. So können beispielsweise alle bei Dropbox gespeicherten Dateien der Personalabteilung mit einem Kennwort verschlüsselt werden, das nur den relevanten Mitarbeitern bekannt ist. Wenn Mitarbeiter der Personalabteilung die Dateien auf einem Unternehmens-Laptop öffnen, verfügen sie bereits über den Schlüssel und können Dateien je nach Bedarf aufrufen und mit Kollegen austauschen.

SafeGuard Encryption für Cloud Storage bietet standortunabhängigen Schutz – egal, ob Sie von Ihrem privaten PC, dem Unternehmens-Lapotop oder (ab 2012) einem Dateileser für iOS- (z.B. iPhone, iPad) oder Android-Geräte auf Daten zugreifen. Beachten Sie bitte, dass verschlüsselte Inhalte auf diesen Geräten zwar aufrufen, jedoch nicht ändern können.

Case-Study zum Thema Datensicherheit: Diebstahl durch Mitarbeiter

Das folgende Szenario zeigt auf, wie fatal die Folgen vernachlässigter Datenverschlüsselung sein können: Die Geschäfte laufen gut. Als jedoch Gerüchte aufkommen, dass mögliche Gehaltszuschlagszahlungen ausfallen, wendet sich eine Mitarbeiterin Ihrer Vertriebsabteilung an die Konkurrenz. Sie möchte ihre Kunden- und Interessentendatenbank herunterladen, weiß jedoch, dass die IT-Abteilung über Downloads auf ihrem Computer informiert werden.

Nach kurzer Internetrecherche findet sie eine kostenlose App für das iPad für den Remote-Zugriff auf ihren Arbeitscomputer. So kopiert sie heimlich alle vertraulichen Daten, die sie über die Jahre angesammelt hat. Sie präsentiert die gesammelten Daten ihrem potenziellen neuen Arbeitgeber. Als sie schließlich kündigt, weiß die IT-Abteilung nicht, dass vertrauliche Daten aus dem sicheren Netzwerk gestohlen wurden.[3]

3. Quelle: Sheehan Phinney Bass + Green PA, www.sheehan.com.

Machen Sie sich mit der Cloud vertraut

Daten sind nicht statisch: Sie unterliegen ständigen Veränderungen und wirken sich entscheidend auf den gegenwärtigen und zukünftigen Unternehmenserfolg aus. Daher müssen Datensicherheit, -schutz und -vertraulichkeit stets gewährleistet werden. Daten müssen ausgetauscht werden – mit Mitarbeitern, Partnern, Management, Vorstand und anderen Investoren.

Im Zuge der zunehmenden Nutzung von Smartphones und Tablets hat sich die Zusammenarbeit grundlegend verändert. Mitarbeiter, die solche Geräte nutzen oder ihre eigenen Geräte mitbringen („Bring Your Own Device“ oder „BYOD“), können komfortabler und produktiver arbeiten.

Mehr Mobilität geht jedoch nur dann mit Produktivitäts- und Flexibilitätssteigerungen einher, wenn die richtigen Tools zum Einsatz kommen. Cloud Storage zählt zu den Tools für die Zusammenarbeit im Unternehmen. Sofern Ihre Unternehmens-Cloud keine klaren Alternativen bietet, kann sich das Sperren dieser Dienste negativ auf den Erfolg ihrer Strategie für Mobilgeräte auswirken.

Doch bleiben Sie wachsam und kritisch. Externe Dienste zum Zugriff auf und Austausch von Daten werden aller Wahrscheinlichkeit nach nicht allzu schnell von der Bildfläche verschwinden. Meist nutzen Anwender solche Dienste zur Produktivitätssteigerung. In Einzelfällen wird hierbei jedoch versucht, strenge Schutzmechanismen zu umgehen.

So führen Benutzer etwa an, dass Dropbox-Dienste weniger aufwändig als VPN oder E-Mails sind. Noch riskanter ist der Rückgriff auf unverschlüsselte, ungeschützte USB-Sticks.

Ermitteln Sie, wie und wo Datenaustausch stattfindet. Sie legen fest, ob Daten immer, nur eingeschränkt oder überhaupt nicht in der Cloud gespeichert werden dürfen und für welche Benutzergruppen besondere Regeln gelten.

Fallbeispiel: Sichere Datenspeicherung in der Cloud

Nehmen wir an, bei Ihrem Unternehmen handelt es sich um einen amerikanischen Zulieferer für ein international agierendes Unternehmen. Von Ihrem Team erstellte Grafiken sind zu groß, um an die Niederlassung in Europa übertragen zu werden, und Ihre FTP-Server unterstützen keine Verschlüsselung. Zudem kann die vollständige, fehlerfreie Übertragung nicht geprüft werden. Wenn Sie die Datei vor dem Hochladen in Dropbox mit SafeGuard Enterprise 6 verschlüsseln, können Mitarbeiter in Europa über das Dropbox-Konto problemlos auf die Grafiken zugreifen und die Budgets für Produkt- und Herstellungskosten ermitteln.

SafeGuard Encryption für Cloud Storage

Dank **SafeGuard Encryption für Cloud Storage** können Sie darauf vertrauen, dass Ihre Mitarbeiter die richtigen Entscheidungen treffen. So müssen die Benutzer ihre Gewohnheiten nicht ändern – mit Hilfe von Richtlinien und Lösungen können Sie sicherstellen, dass IT-Nutzungsrichtlinien und Standards eingehalten werden. Hierzu zählt:

Schutz von Daten in der Cloud. Sie behalten die Kontrolle über Ihre Verschlüsselungsschlüssel. Und nur Personen, die über einen Schlüssel verfügen, erhalten Zugriff auf Ihre Daten.

Sicherer Austausch vertraulicher Daten innerhalb einzelner Abteilungen. Sogar der Datenaustausch mit Dritten ist möglich, ohne die Sicherheit zu gefährden.

Transparante Verschlüsselung im Hintergrund, damit Ihre Anwender reibungslos arbeiten können.

Einsatz bewährter Datenverschlüsselungsalgorithmen, um Ihnen beste Sicherheit und Performance bereitzustellen.

Nahtloser Datenschutz für Daten auf Festplatten, Flash-Laufwerken, File Shares und in der Cloud.

So funktioniert's

Fordern Sie jetzt eine kostenlose Testversion von SafeGuard Encryption für Cloud Storage an.

Sales DACH
Deutschland, Österreich, Schweiz
Tel: +49 (0) 611 5858-0
+49 (0) 721 255 16-0
E-Mail: sales@sophos.de

Boston, USA | Oxford, UK

Sophos Whitepaper 3.12v1.dNA

SOPHOS