File-Sharing-Security: Kontrolle über kritische Daten behalten

Cloud-Storage- und File-Sharing-Anwendungen bringen Unternehmen aufgrund ihrer Skalierbarkeit und komfortablen Nutzung viele Vorteile. Wird File Sharing jedoch nicht ordnungsgemäß verwaltet, kann dies schwerwiegende Auswirkungen auf die Datensicherheit haben. Jedes Mal, wenn Mitarbeiter Technologien zum Dateienaustausch verwenden, ist dies mit Risiken wie Malware-Infektionen, Verlust oder Offenlegung sensibler Informationen verbunden. Ohne geeignete Sicherheitsmaßnahmen können die Nachteile durch File Sharing deutlich überwiegen, wenn kritische Unternehmensdaten wie Kunden-, Finanzinformationen, Geschäftsgeheimnisse und geistiges Eigentum zusätzlichen Bedrohungen ausgesetzt sind.

Maßnahmen für die File-Sharing-Sicherheit
Um Datensicherheitsrisiken zu minimieren, sollten Unternehmen einige Security-Maßnahmen bei der Nutzung von File-Sharing ergreifen. Hierzu gehören:

1. Aufklärung über Schatten-IT

Der erste Schritt für eine effektive File-Sharing-Security besteht darin, alle Mitarbeiter über die Risiken aufzuklären, insbesondere im Hinblick auf Schatten-IT – heißt, die Nutzung von IT-Lösungen, die nicht offiziell von der IT-Abteilung implementiert und genehmigt wurden. File Sharing per Schatten-IT beinhaltet die Nutzung privater E-Mail-Konten, kostenloser Cloud-Storage-Dienste und anderer File-Sharing-Systeme für Privatanwender. Diese entsprechen möglicherweise nicht den Sicherheitsstandards des Unternehmens und liegen in vielen Fällen außerhalb der bestehenden Sicherheitskontrollen.

2. File-Sharing-Richtlinien implementieren

Neben der Aufklärung der Mitarbeiter über die Risiken durch Schatten-IT, schafft die Umsetzung einer formalen File-Sharing-Richtlinie Klarheit. Die IT- und Security-Teams sollten die Nutzung und Sicherheit von Filesharing-Systemen bewerten. So können sie entscheiden, ob sie eine Verwendung zulassen oder nicht, sowie Sicherheitsmaßnahmen ergreifen, falls ein System zugelassen wird. Zudem sollten Unternehmen die Entwicklung und Implementierung einer allgemeinen Richtlinie für die Nutzung von Dateien erwägen, die speziell für die Verwendung aller File-Sharing-Methoden gilt – einschließlich der Cloud-basierten und der, die zwischen Dateisynchronisierungs- und Datenfreigabe-Anwendungen eingesetzt werden.

3. Anwendungs- und Datentransparenz sowie Datenkontrolle

Wichtig ist, dass die IT-Abteilung einen vollständigen Überblick über alle File-Sharing-Anwendungen hat, die von den Mitarbeitern für die gemeinsame Nutzung von Daten verwendet werden. Zudem sollte das IT-Team in der Lage sein, den Benutzerzugriff auf sensible Unternehmensdaten zu verwalten und zu kontrollieren. Auch müssen Mitarbeiter speziell über die Risiken von Datenverlust oder Diebstahl durch File Sharing aufgeklärt sowie über die Einhaltung der geltenden Vorschriften informiert werden. Zusätzlich helfen regelmäßig Audits, um die File-Sharing-Praktiken des Unternehmens zu analysieren und Sicherheitsrisiken zu identifizieren.

4. Datensicherheitslösungen für die File-Sharing-Security

Die letzte Verteidigungslinie der File-Sharing-Security ist eine Datensicherheitslösung, die vor Datenverlust und Diebstahl durch File Sharing schützt. Data-Loss-Prevention-Technologien (DLP) bieten Sicherheit für File-Sharing-Anwendungen und Cloud-Storage durch eine Kombination aus Zugriffs- und Anwendungskontrolle, Endgerätesteuerung, Netzwerksicherheits-Appliances und anderen proaktiven Maßnahmen, die den Austausch sensibler Unternehmensdaten für nicht autorisierte Anwendungen, Endgeräte und Benutzer wirksam verhindern. Zu den Vorteilen der Einführung einer Datensicherheitslösung für die Sicherheit von File Sharing gehören:

- Kontinuierliche Überwachung und Transparenz für alle Dateninteraktionen mit Web- und Cloud-Speicheranwendungen
- Granulare Steuerung der Dateibewegung basierend auf Browser- und Betriebssystemereignissen, die Webanwendungen wie SharePoint, Dropbox und Google Apps betreffen
- Automatische Klassifizierung und richtlinienbasierter Schutz von Daten, die von Webanwendungen heruntergeladen werden
- Forensische Ereignisprotokolle für eine effektive Alarmierung, Berichterstattung und Richtlinienerstellung
- Automatische Verschlüsselung sensibler Daten vor dem Austritt
- API-Integration mit führenden File-Sharing-Anwendungen, um die Erweiterung der Datensicherheitsmaßnahmen des

Unternehmens auf die Cloud zu ermöglichen

Mit der zunehmenden Verbreitung von Cloud Computing kann es für Unternehmen eine große Herausforderung sein, die Nutzung von Cloud Storage und File Sharing durch Mitarbeiter effektiv zu blockieren. Mit der richtigen Kombination aus Mitarbeiterschulungen, umfassenden Sicherheitsrichtlinien für den Dateiaustausch sowie Data-Loss-Prevention-Technologien können Unternehmen jedoch die Vorteile von Cloud Computing und File Sharing nutzen und gleichzeitig Datensicherheitsrisiken minimieren.