Acht Gründe, warum Ihre Nutzer ein größeres Risiko darstellen als Hacker

So schützen Sie Ihre Unternehmensdaten

Die wahre Bedrohung für Ihre Informationssicherheit

Wenn Sie an die Gründe für Datenschutzverletzungen denken, was kommt Ihnen da in den Sinn? Ein Team von internationalen Hackern, die Daten stehlen, um Unternehmen zu erpressen? Ein Insider, der Ihrem Unternehmen übel gesinnt ist? Statistisch gesehen ist der wahrscheinlichste Grund jedoch ein ganz einfacher: z. B. einer Ihrer Vertriebsmitarbeiter, der sein Tablet im Flugzeug liegengelassen hat. 54 Prozent aller Unternehmen halten Fehler ihrer eigenen Mitarbeiter für die größte Bedrohung für ihre vertraulichen Daten, und nicht externe Hacker (30 Prozent) oder böswillige Insider (21 Prozent).[1]

Damit Ihre Mitarbeiter an jedem Ort produktiv arbeiten können, benötigen sie einen zuverlässigen, schnellen Zugriff auf wichtige Dateien und Daten. Aber wenn Ihre Daten an vielen verschiedenen Orten gespeichert sind und zahlreiche Anwender über ihre privaten Endgeräte auf sie zugreifen, wird die „Angriffsfläche" für Sicherheitsrisiken größer denn je. In diesem Fall benötigen Sie eine Content Collaboration Lösung, die Ihre wichtigen Daten schützt und gleichzeitig den Zugriff für Ihre Mitarbeiter vereinfacht.

Hier sind die acht Gründe, warum eine mangelhafte Absicherung von Nutzern eine Bedrohung ist und wie Sie die Content Collaboration angemessen schützen.

59 %

aller Unternehmen halten Fehler ihrer eigenen Mitarbeiter sowie Systemfehler für die größte Bedrohung für ihre vertraulichen Daten.[1]

1. Ungenügende Verschlüsselung

Jeden Tag versenden Ihre Mitarbeiter über Ihr Netzwerk unzählige Dateien mit unterschiedlichen Endgeräten. Ohne eine wirksame Verschlüsselung können Unbefugte viel einfacher auf Ihre vertraulichen Daten zugreifen – z. B. auf geistiges Eigentum Ihres Unternehmens oder vertrauliche Kundendaten. 54 Prozent aller Unternehmen nannten diese Faktoren als Hauptgründe für die Nutzung von Verschlüsselungstechnologie.[2]

Wie sieht eine wirksame Verschlüsselung aus?

- Sie muss leistungsstark sein und dem von der US-Regierung genutzten Advanced Encryption Standard entsprechen, mit einer Schlüssellänge von 256 Bits.
- Ihre Daten müssen sowohl im gespeicherten Zustand als auch während der Übertragung im Netzwerk geschützt sein.
- Sie müssen die volle Kontrolle behalten und in Ihrem gesamten Cloud-Speicher Ihre eigenen Verschlüsselungs-Keys managen können.

2. Die Nutzung externer Speichermedien, die leicht verlorengehen können

Ihre Mitarbeiter erstellen große Dateien wie Videos und andere grafikintensive Dateitypen. Die Dateigrößenbeschränkung beim E-Mail-Versand könnte sie in Versuchung bringen, Dateien über USB-Sticks und andere portable Speichermedien mit Kollegen und Kunden zu teilen. Jedes dieser externen Speichermedien stellt jedoch ein Sicherheitsrisiko dar. Ein Mitarbeiter muss lediglich einen USB-Stick im Café liegenlassen und schon können Ihre privaten Informationen vom Finder eingesehen werden.

Aufgrund dieses Risikos ist es notwendig, dass Sie Ihre Dateien in einer sicheren Private Cloud speichern. Sie möchten einen standort- und endgeräteunabhängigen sicheren Zugriff auf große Dateien bereitstellen, ganz gleich, ob Dateien in Ihrem lokalen Rechenzentrum oder in der Cloud gehostet werden. So können Ihre Mitarbeiter an jedem beliebigen Ort zusammenarbeiten,

ohne dass sie das Risiko eingehen müssen, Dateien auf einem USB-Stick aufzubewahren, der leicht verlorengehen kann.

3. Schwache Passwörter und keine Zwei-Faktor-Authentifizierung

Zu viele Anwender nutzen einfache Passwörter, die leicht einzugeben sind, und verwenden sie auf mehreren Websites. Dies macht sie zu einem beliebten Ziel für Hacker. Sie sollten Ihre Mitarbeiter davon überzeugen, stärkere Passwörter zu verwenden, die keine persönlichen Informationen oder geläufigen Phrasen enthalten. Ein starkes Passwort besteht aus mindestens zehn Zeichen, darunter Zahlen, Symbole, Groß- und Kleinbuchstaben. Oder noch besser: Mitarbeiter sollten sich eine Passphrase ausdenken, die aus zufälligen aneinandergereihten Wörtern, Zahlen und Symbolen besteht, die schwierig für einen Hacker zu erraten wären. Ein einfacher, sinnfreier Satz wäre zum Beispiel: „Meine erste Wohnung befand sich in der Musterstraße 34 und die Miete war 500 Euro pro Monat.“ Aus diesem Satz könnten Sie nun eine Passphrase machen, indem Sie die ersten Zeichen jedes Wortes aneinanderreihen. Somit wäre das Passwort „MeWbsidM34udMw5€pM.“

Es ist auch wichtig, dass Ihre Mitarbeiter verschiedene Passwörter für jede Website und Anwendung nutzen, die sie für die Arbeit verwenden. Sie können hierbei zur Unterstützung einen Passwortmanager wie LastPass verwenden, um starke, einzigartige Passwörter für alle wichtigen Logins zu erstellen. Sie sollten auch eine Content Collaboration Lösung wählen, die regelmäßige Passwortänderungen verlangt (z. B. alle 60 Tage) und Zwei-Faktor-Authentifizierung unterstützt – besonders wenn sich ein Nutzer über ein neues Endgerät einloggt.

4. Das Teilen vertraulicher Informationen auf privaten Endgeräten

Der Umgang mit Kundendaten wird durch zahlreiche Gesetze und Richtlinien reguliert. Wenn ein Mitarbeiter diese vertraulichen Daten auf ein nicht genehmigtes Endgerät herunterlädt, könnte das Unternehmen aufgrund einer Compliance-Verletzung verklagt und mit einer Geldstrafe belegt werden. Sie müssen sicherstellen, dass nur berechtigte interne und externe Anwender auf private Informationen zugreifen können.

Daher ist es unumgänglich, den Dateiaustausch in Ihrer gesamten Organisation zu kontrollieren. Sie müssen Maßnahmen zum Schutz vor Datenverlust (Data Loss Prevention, DLP) einrichten, um Unbefugte daran zu hindern, heruntergeladene Dateien in nicht genehmigten Anwendungen zu öffnen. Ihre Content Collaboration Plattform sollte sich zudem in die Lösungen von Cloud Access Security Brokern wie Skyhigh und Avanan integrieren lassen, damit Sie DLP-Richtlinien auf Dateien in der Cloud anwenden können.

5. Screenshots vertraulicher Informationen

Um vertrauliche Daten zu schützen, bedarf es mehr als die Absicherung der Dateien selbst. Manchmal machen Anwender Screenshots von vertraulichen Dateien, um Informationen zu notieren, und senden diese Screenshots anschließend ohne Genehmigung weiter. Daher müssen Sie sicherstellen, dass der beabsichtigte Empfänger der Daten keine Screenshots anfertigen und diese Informationen mit Unbefugten teilen kann.

Die Antwort ist eine Content Collaboration Lösung, die die Verwaltung von Informationsrechten (Information Rights Management, IRM) unterstützt. Vertrauliche Daten werden geschützt, indem ein digitales Wasserzeichen angezeigt

wird, dass den Namen des Empfängers, seine E-Mail- und IP-Adresse enthält. IRM verringert also das Risiko nicht autorisierter Bildschirmaufnahmen, indem nur Anwendern mit Wasserzeichen die entsprechenden Dokumente angezeigt werden.

6. Verlorene oder gestohlene mobile Endgeräte

Wenn Sie Ihren Mitarbeitern erlauben, von überall und mit jedem beliebigen Endgerät zu arbeiten, steigt die Wahrscheinlichkeit, dass jemand ein Endgerät verliert, auf dem sich vertrauliche Informationen befinden. Dies ist noch schlimmer als der Verlust eines externen Speichermediums mit vertraulichen Daten, da gestohlene Smartphones oder Tablets von böswilligen Anwendern auch dazu genutzt werden können, auf Ihr Netzwerk zuzugreifen.

Neben der vorher beschriebenen DLP-Strategie sollte Ihre Lösung zudem eine Remote-Löschung von Inhalten auf Endgeräten ermöglichen. Ihre Daten werden vor Diebstahl geschützt, da Ihr IT-Team aus der Ferne den Zugriff auf die Content Collaboration Lösung sowie Dokumente auf den verlorenen mobilen Endgeräten entfernen kann. Mithilfe der Remote-Löschung können Sie auch sofort Mitarbeitern, die die Organisation verlassen, jeglichen Zugriff verwehren.

7. Unterschreiben ausgedruckter Dokumente

Vertriebsmitarbeiter haben Jahrzehnte lang abgeschlossene Geschäfte mit unterzeichneten Verträgen auf Papier besiegelt. Im digitalen Zeitalter stellen ausgedruckte Dokumente jedoch ein erhebliches Sicherheitsrisiko dar. Verträge auf Papier können verlorengehen, fotografiert oder auf unerlaubte Weise kopiert werden. Diese Risiken werden größer, je häufiger der Vertrag an Personen an anderen Orten weitergereicht wird.

Statt einen Vertrag auszudrucken und ihn diesen Risiken auszusetzen, sollten Sie eine Content Collaboration Lösung mit elektronischen Signaturen nutzen. Diese elektronische Verifizierung ist sowohl rechtlich bindend als auch sicherer als der Transport eines Dokuments in Papierform. Es gibt zwar Drittanbieter für elektronische Signaturen, jedoch können Sie die Administrationszeit um bis zu 93 Prozent verkürzen, wenn Sie eine Content Collaboration Lösung verwenden, die diese Funktion bereits unterstützt.

8. Ungenügendes Sicherheits-Auditing und mangelhafte Protokollierung

Wenn eine Datenschutzverletzung auftritt, dürfen Sie keine wertvolle Zeit mit der Suche nach der Ursache verschwenden. Sie müssen die Bedrohung sofort identifizieren und neutralisieren können. Daher ist es wichtig, die Aktivitäten Ihrer Anwender zu überwachen, sodass Sie wissen, wer welche Dateien in Ihrem Netzwerk herunterlädt oder sie versendet.

Die beste Art, um die Dateinutzung Ihrer Anwender zu überwachen, ist die Nutzung einer Content Collaboration Lösung mit Sicherheits-Auditing und Protokollierung. So können Sie die Anwenderaktivität überwachen, protokollieren und einen Audit Trail erstellen. Dadurch haben Sie einen besseren Überblick über die Datennutzung und können gesetzliche Vorgaben einfacher erfüllen. Und wenn Sie Benachrichtigungen aktivieren, stellen Sie sicher, dass verdächtige Aktivitäten sofort gemeldet werden, sodass Sie die entsprechenden Maßnahmen einleiten können.

Eröffnen Sie Ihren Anwendern neue Möglichkeiten, ohne die Informationssicherheit zu vernachlässigen

Nun, da Sie wissen, welches Sicherheitsrisiko Ihre Nutzer darstellen, ist es wichtig, dass Sie sie unterstützen, statt sie zu verdächtigen. Die beste Art, um dieses Risiko aufzufangen, ist nicht, alle Arbeitsplätze und Endgeräte von Anwendern von der Außenwelt abzuschotten, sondern ihnen eine Content Collaboration Plattform zu bieten, die es ihnen ermöglicht, mit maximaler Produktivität zu arbeiten. Mit der richtigen Lösung erhalten Ihre Anwender einen standort- und endgeräteunabhängigen Zugriff auf alle notwendigen Daten, während die Informationssicherheit gewahrt wird.

Weitere Informationen zu Content Collaboration erhalten Sie auf sharefile.com.

Quellen:

1. Dieser und andere Textbelege stammen von der 2019 Ponemon Global Encryption Trends Study. go.ncipher.com/rs/104-QOX-775/images/2019-Ponemon-Global-Encryption-Trends-Study-es-ar.pdf

2. 2019 Ponemon Global Encryption Trends Study

Vertrieb
Nordamerika | +1 800 441 3453
Weltweit | +1 408 790 8000

Standorte
Unternehmenszentrale | 851 Cypress Creek Road Fort Lauderdale, FL 33309, USA
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, USA