Accellion

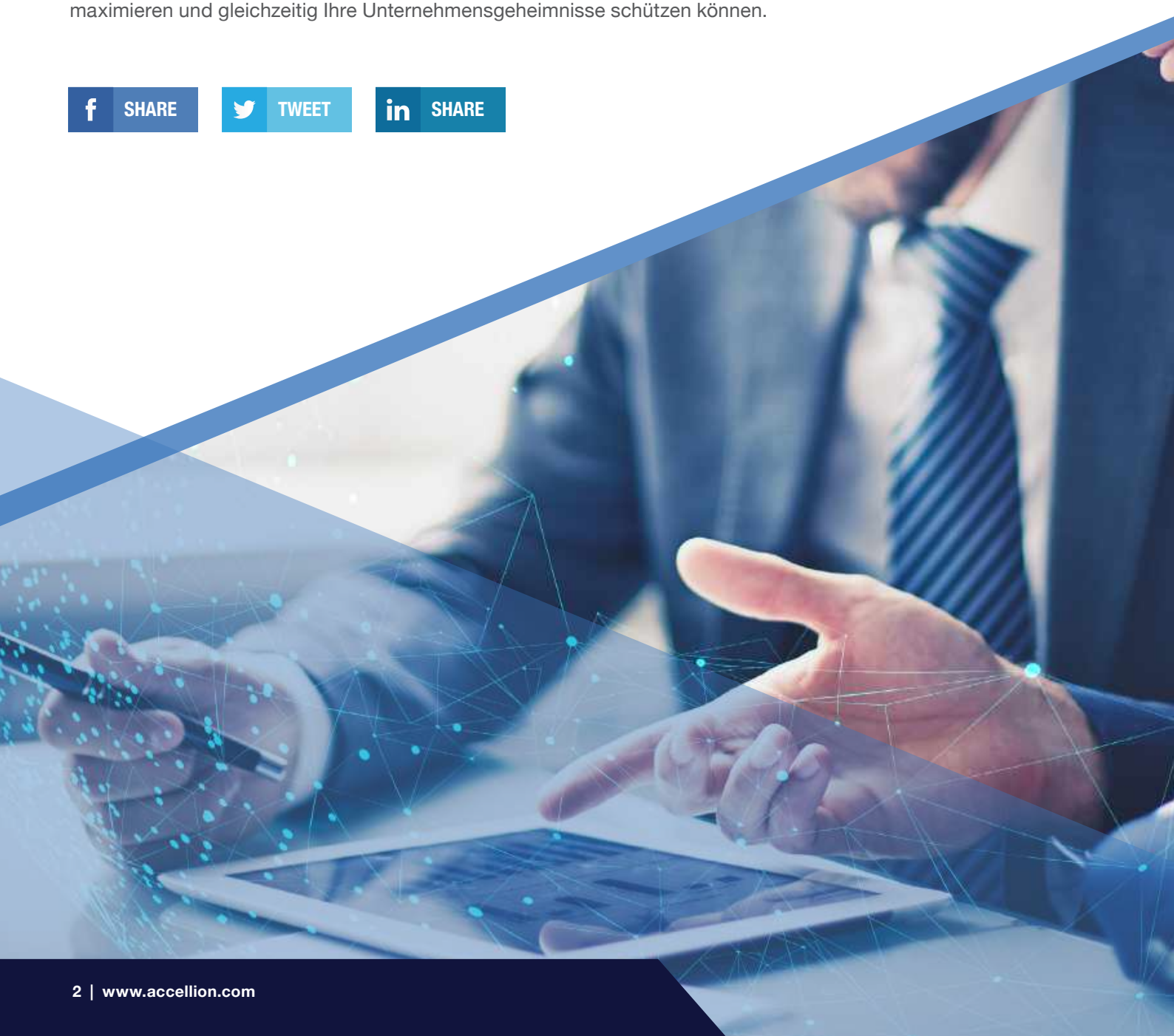
Risikofreies mobiles Arbeiten für Führungskräfte

Fünf Best Practices für die mobile Sicherheit von Geschäftsleitung und Vorstand

Kurzfassung

Geschäftsführer und leitende Angestellte von Unternehmen senden und empfangen täglich vertrauliche Unternehmensinformationen an den gefahrenträchtigsten Orten und verwenden dabei die riskantesten Geräte: ihre Mobiltelefone und Tablets. Sie sind auf diese Geräte angewiesen, um trotz eines anspruchsvollen Reiseplans produktiv zu bleiben, wenn sie Kunden, Lieferanten, Partner und Niederlassungen besuchen. Schließlich kann der Betrieb nicht stillstehen, während sie unterwegs sind oder in Meetings stecken. Tag für Tag versenden Mitarbeiter Besprechungsunterlagen, Präsentationen, Beschaffungsanträge und Projektstatusberichte. Führungskräfte arbeiten mit Vorstand und Anwälten zusammen oder überprüfen die neueste Version eines Vertrags - und das alles in wenigen Minuten freier Zeit an Flughäfen, in Hotels und Bürofluren. Dieser Produktivitätsgewinn birgt jedoch das Risiko, dass vertrauliche Informationen - vorläufige Finanzergebnisse, M&A-Unterlagen, Klagen oder Geschäftsgeheimnisse - mit potenziell unternehmensbeeinflussenden Folgen unbeabsichtigt preisgegeben werden. Verringern Sie dieses Risiko, indem Sie fünf Best Practices befolgen, mit denen Sie die mobile Produktivität Ihrer Führungskräfte und Vorstandsmitglieder maximieren und gleichzeitig Ihre Unternehmensgeheimnisse schützen können.

SHARE TWEET SHARE



BEST PRACTICE #1:

Schützen Sie Produktivität und Sicherheit Ihrer Führungskräfte

Einfache und sichere mobile E-Mail-Funktionalität

CEOs nutzen ihre mobilen E-Mail-Clients den ganzen Tag über, um Finanzpläne mit Vorstandsmitgliedern zu teilen, vertraulichen juristischen Rat von ihren Anwälten einzuholen oder andere sensible Informationen auszutauschen. Wenn sie jedoch E-Mails und Anhänge mit Standardanwendungen senden, können diese leicht durch Mobilfunkanbieter, staatliche Stellen oder gar Kriminelle ausspioniert werden. Wenn etwas schief geht, haben Sie keinen Audit-Trail, um nachzuweisen, wer Zugriff auf welche Dateien hatte. Schließlich ist Ihre wichtige eingehende Kommunikation im Spam vergraben, was ihre Reaktionszeiten verlangsamt. Verhindern Sie dieses Szenario, indem Sie ein sicheres End-to-End-E-Mail-System für Ihre Führungskräfte auf Ihre Unternehmens-E-Mails packen. Unterstützen Sie die Akzeptanz durch eine benutzerfreundliche Bedienung und einen sicheren Zugriff auf wichtige Dateispeicher des Unternehmens. Verschlüsseln Sie alle Dateien und Nachrichten, die übertragen werden, auch die auf dem Gerät gespeicherten Offlinedateien. Entfernen Sie Spam, indem Sie unbekannte Absender herausfiltern. Stellen Sie darüber hinaus sicher, dass Führungskräfte immer up-to-date sind: Lassen Sie sie direkt benachrichtigen, wenn der Empfänger ein Dokument herunterlädt oder eine Antwort sendet. Vervollständigen Sie die Lösung, indem Sie den Inhalt beim Empfänger sichern, unabhängig davon, wie unsicher dessen Unternehmens-E-Mail-System ist. Bieten Sie diesen externen Parteien eine einfache und sichere Möglichkeit, Nachrichten anzuzeigen, Anhänge herunterzuladen und ihre Antworten automatisch zu verschlüsseln, ohne Software installieren zu müssen.

BEST PRACTICE #2:

Unterstützen Sie Mitarbeiter bei der Betreuung von Führungskräften

Sichere Übertragung von Inhalten auf mobile Geräte

Die Kommunikation nach innen ist genauso wichtig wie die Interaktionen nach außen. Wenn Führungskräfte unterwegs zu Meetings sind, müssen ihre Mitarbeiter sie mit den entsprechenden Tagesordnungen, Besprechungsunterlagen und Präsentationen versorgen. Sie müssen die Dokumente direkt in die Themenordner legen, sodass sie sich bereits auf den mobilen Geräten befinden, wenn die Manager einen Moment Zeit haben, die Dateien durchzusehen und zu beantworten. Ermöglichen Sie Ihren Führungskräften, die Dateien offline zu öffnen, da die Zeit während eines Fluges möglicherweise die einzige freie Zeit ist, um einen komplexen Vorschlag oder ein PDF eines Vertrags zu überprüfen und zu kommentieren.

BEST PRACTICE #3:

Digitalisierung und Koordination der Kommunikation von Vorstand und Gremien

Sichere Zusammenarbeit mit externen Partnern

Ihre größten Risiken beim Informationsaustausch sind häufig verbunden mit Dritten, wie Aufsichtsräten, Anwälten und Bankern, Private Equity-Firmen und M&A-Beratern. Fast alles, was Sie mit externen Parteien teilen, kann Mitbewerber auf den Plan rufen oder Sie in Konflikt mit den Gesetzen zur Offenlegung von Finanzdaten bringen, wenn diese durchsickern. Viele dieser externen Parteien nutzen, wie Ihre Führungskräfte, Mobiltelefone und Tablets, um unterwegs Zugriff auf notwendige Informationen zu haben.

Bewahren Sie diese sich ständig ändernden Informationen konsequent in entsprechend sicher freigegebenen Ordnern auf. Legen Sie die Berechtigungen für jeden Ordner so fest, dass nur befugte Parteien den Ordner sehen können und nur diejenigen, die Eingaben vornehmen müssen, den Ordner ändern können. Stellen Sie bei solchen sensiblen Informationen sicher, dass Sie einen unveränderlichen Audit-Trail und ein automatisches Ablaufdatum implementieren.

Unterstützen Sie die Zusammenarbeit externer Gremien in Projekten, an Verträgen, Übernahmen oder Finanztransaktionen. Bieten Sie eine einfache, benutzerfreundliche Möglichkeit Dateien in Microsoft Word-, Excel- und PowerPoint-Anwendungen zu bearbeiten oder PDFs zu kommentieren und freizugeben. Speichern Sie die Änderungen automatisch wieder im sicheren Kollaborationsordner. Unabhängig davon, ob der externe Empfänger einen Browser oder eine mobile App verwendet, sollten Sie Benachrichtigungen bereitstellen, alle Dateiversionen verfolgen und den Audit-Trail dokumentieren.

BEST PRACTICE #4:

Mobile Inhalte sichern

Schützen Sie Dateien End-to-End auf jedem mobilen Gerät

Mithilfe von Commodity-Cloud-Dateifreigaben und E-Mails können Ihre Führungskräfte heute jederzeit mit Mitarbeitern und externen Parteien in Kontakt bleiben. Öffentliche Cloud-Anbieter für diese Tools können jedoch die Metadaten Ihrer Datenübertragungen scannen, wodurch sich Ihre Risiken erhöhen. Wenn sie eine Vorladung erhalten, sind diese Anbieter in der Lage und verpflichtet, Ihre vertraulichen Daten ohne eine entsprechende Vollmacht herauszugeben. Reduzieren Sie die Risiken mobiler E-Mails und freigegebener Ordner mit einer erstklassigen Sicherheits- und Compliance-Lösung. Implementieren Sie den Service auf einem gehärteten, skalierbaren Server-Cluster und verschlüsseln Sie Informationen während der Übertragung und im ruhenden Zustand auf dem Gerät oder Server mit von der IT-Abteilung verwalteten Schlüsseln. Kontrollieren Sie, wer Zugriff auf Ihre Daten hat, indem Sie diesen Service mithilfe von On-Premise, FedRAMP oder privater Cloud-Infrastruktur bereitstellen. Da externe Benutzer sich nicht unter Ihrer Kontrolle befinden, sollten Sie die App für einen sicheren Betrieb auf ihren persönlichen Geräten schützen.

Geben Sie Administratoren die Möglichkeit, rollenbasierte Richtlinien zu implementieren, die Verwaltung von Benutzern mobiler Geräte zu übernehmen, Hilfsprogramme wie Microsoft Word auf die Whitelist zu setzen und Sicherheitsintegrationen wie LDAP/AD und MDM zu integrieren. Beseitigen Sie schließlich das Risiko, das von Unternehmensdaten auf einem externen oder einem gestohlenen Gerät ausgeht, indem Sie diese per Remote Wipe löschen, ohne den persönlichen Inhalt des Benutzers zu beeinträchtigen.

BEST PRACTICE #5:

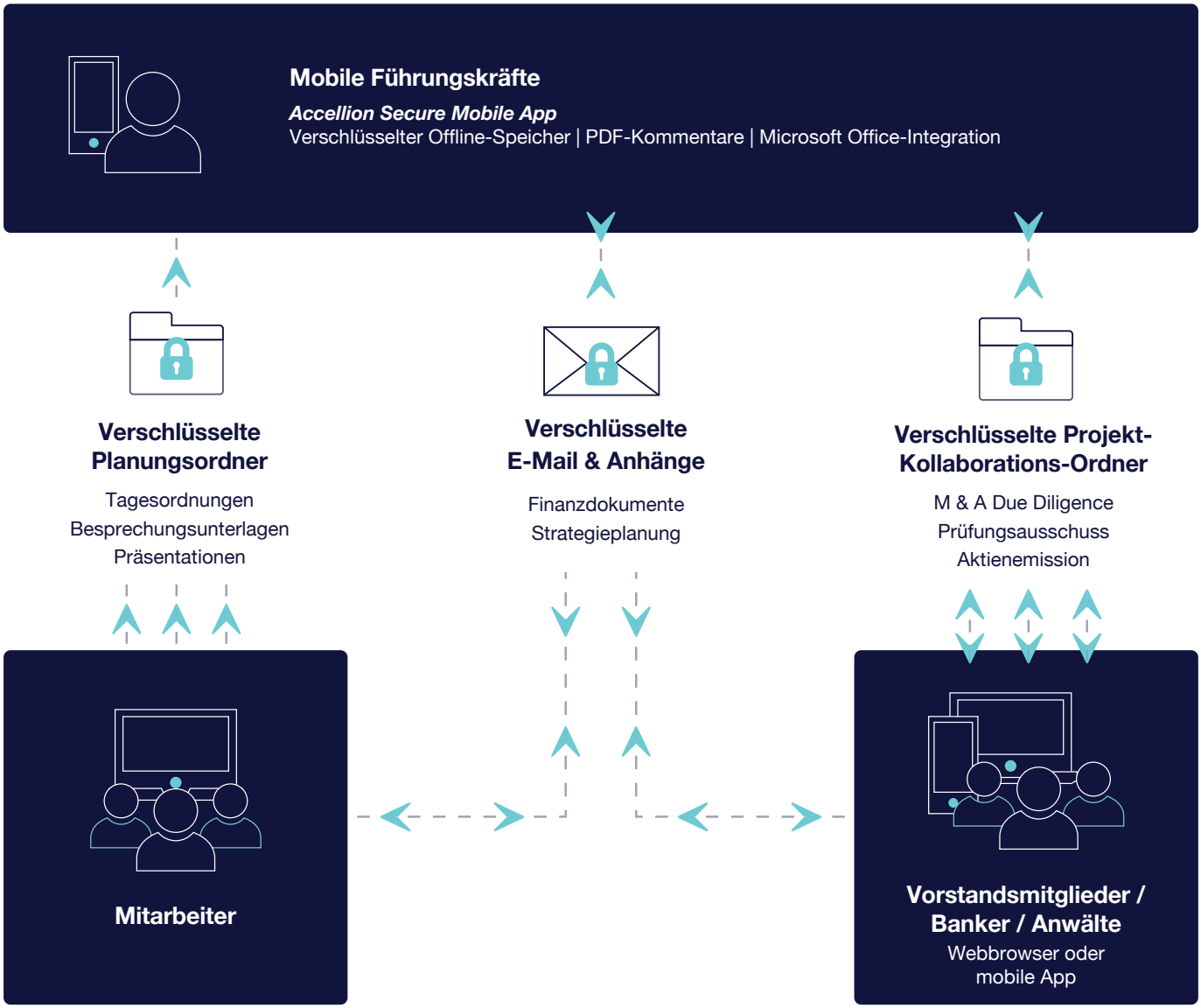
Vermeiden Sie Datenschutzverletzungen

Transparenz bei jedem mobilen Dateitransfer

Um die Kommunikation Ihrer mobilen Führungskräfte und Vorstandsmitglieder gegen In- und Outsider-Bedrohungen zu schützen, müssen Sie alle Dateien, die über mobile Geräte in Ihr Unternehmen gelangen oder es verlassen, im Auge behalten. Beginnen Sie mit der Implementierung eines konsolidierten Audit-Trails für alle mobilen Dateitransfers zwischen Ihrem Unternehmen und den Reisenden oder dritten Parteien. Wenn Sie über diese Metadaten verfügen, erstellen Sie eine klare und vollständige Echtzeit-Ansicht, die die wichtigsten Sicherheitsfragen zu den in Ihrem Unternehmen ein- und ausgehenden Informationen beantwortet. Woher stammen diese Informationen? Wohin werden die Daten verschickt? Wer hat sie gesendet? Wer ist der Empfänger? Sind die Daten vertraulich? Ist die Transaktion normal oder als eine Bedrohung einzustufen?

Accellion in Aktion

Verhindern Sie Datenschutzverletzungen und Compliance-Verstöße im mobilen Datenverkehr



Accellion PLATFORM

Gehärtete, skalierbare Accellion-Plattform

On-Premise | Private Cloud | FedRAMP

- Sichere Speicherung
- Integrierter Audit-Trail
- CISO-Dashboard
- Compliance-Berichte
- Rollenbasierte Richtlinien

Über Accellion

Die Enterprise Content Firewall von Accellion verhindert Datenschutzverletzungen und Compliance-Verstöße, die durch die Kommunikation mit Dritten und die damit verbundenen Risiken entstehen. Mit Accellion haben CIOs und CISOs die vollständige Transparenz, Compliance und Kontrolle über den Austausch von geistigem Eigentum, personenbezogenen Daten, Patienteninformationen und anderen sensiblen Inhalten über alle Kommunikationskanäle von Drittanbietern hinweg, einschließlich E-Mail, Datenfreigabe, Mobilgeräte, Business Applikationen, Webportale, SFTP und automatisierte geschäftsübergreifende Workflows.
Accellion-Lösungen schützen mehr als 25 Millionen Endbenutzer in mehr als 3.000 Unternehmen und Regierungsbehörden weltweit, darunter KPMG, Latham & Watkins, Linde Gas, NHS, das National Institute for Standards and Technology (NIST) sowie Pfizer und die Paul Hartmann AG. Für weitere Informationen besuchen Sie bitte www.accellion.com/de oder rufen Sie uns an unter +49 711 252861-0. Folgen Sie Accellion auf LinkedIn, Twitter und dem Accellion Blog.

© 2019 ACCELLION. Alle Rechte vorbehalten

SHARE TWEET SHARE