Kiteworks

Eliminieren Sie die Risiken, die mit der mobilen Arbeit Ihrer Führungskräfte verbunden sind

5 Best Practices für Vorstand und Aufsichtsrat im Umgang mit der Kommunikation sensibler Inhalte

Zusammenfassung

Täglich versenden und empfangen Geschäftsführer und leitende Angestellte vertrauliche Unternehmensinformationen an den risikoreichsten Orten und mit den risikoreichsten Geräten: ihren Mobiltelefonen und Tablets. Sie sind auf diese Geräte angewiesen, um trotz anspruchsvoller Reisepläne produktiv zu bleiben, wenn sie Kunden, Investoren und Niederlassungen besuchen..

Schließlich können sie ihre Arbeit nicht unterbrechen, wenn sie auf Reisen sind oder sich in einer Reihe von Besprechungen befinden. Täglich versenden Mitarbeiter Briefingunterlagen, Präsentationsfolien, Genehmigungsanträge für Einkäufe und Projektstatusberichte. Manager müssen mit dem Vorstand und den Anwälten zusammenarbeiten oder die neueste Version eines Vertrags prüfen - und das alles in den wenigen freien Minuten, die sie auf Flughäfen, in Hotels und auf Bürofluren verbringen.

Diese Produktivitätssteigerung birgt jedoch auch das Risiko, dass vertrauliche Informationen, wie vorläufige Finanzergebnisse, Fusionen und Übernahmen, Verhandlungen, Rechtsstreitigkeiten oder Geschäftsgeheimnisse, versehentlich offengelegt werden, was sich negativ auf das Unternehmen auswirken kann. Reduzieren Sie dieses Risiko, indem Sie die folgenden fünf Best Practices befolgen, um die mobile Produktivität Ihrer Führungskräfte und Vorstandsmitglieder zu maximieren und gleichzeitig Ihre Geschäftsgeheimnisse zu schützen.

Best Practice #1:

01 Gewährleisten Sie die Sicherheit und Produktivität von Führungskräften unterwegs

Einfacher und sicherer mobiler E-Mail-Dienst

CEOs nutzen ihre mobilen E-Mails den ganzen Tag über, um Finanzpläne mit Vorstandsmitgliedern zu teilen, sich von ihren Anwälten beraten zu lassen oder andere vertrauliche Mitteilungen zu machen. Wenn sie jedoch E-Mails und Anhänge mit Standard-Apps versenden, sind sie anfällig für das Scannen durch Anbieter von Mobilgeräten, staatliche Behörden und gar Kriminelle. Sollte etwas schief gehen, haben sie keinen Audit-Trail, um nachzuweisen, wer auf welche Dateien Zugriff hatte. Am Ende werden womöglich ihre wichtigen eingehenden Mitteilungen noch unter Spam begraben, was ihre Antworten verlangsamt.

Vermeiden Sie dieses Szenario, indem Sie ein sicheres End-to-End-E-Mail-System für Ihre Führungskräfte auf Ihren Unternehmens-E-Mail-Dienst aufsetzen. Fördern die Akzeptanz, indem sie die Benutzerfreundlichkeit auf ein für Konsumenten übliches Niveau anheben und einen sicheren Zugriff auf wichtige Dateispeicher in der Zentrale ermöglichen. Verschlüsseln Sie alle Dateien und Nachrichten während der Übertragung sowie die auf dem Gerät gespeicherten Offline-Dateien. Vermeiden Sie Spam, indem Sie unbekannte Absender herausfiltern. Stellen Sie sicher, dass Ihre Führungskräfte keine wichtigen Aktionen verpassen: Lassen Sie sie sofort benachrichtigen, wenn der Empfänger ein Dokument herunterlädt oder eine Antwort sendet.

Vervollständigen Sie die Lösung, indem Sie den Inhalt beim Empfänger schützen, unabhängig davon, wie unsicher dessen E-Mail-System ist. Bieten Sie diesen externen Parteien eine sichere und einfache Möglichkeit, Nachrichten zu lesen, Anhänge herunterzuladen und ihre Antworten automatisch zu verschlüsseln, ohne Software installieren zu müssen.

Best Practice #2:

02 Helfen Sie Mitarbeitern bei der Vorbereitung und Unterstützung reisender Führungskräfte

Sichere Übertragung von Inhalten auf mobile Geräte

Die interne Kommunikation ist ebenso wichtig wie die Interaktion mit der Außenwelt. Wenn ein Manager zu einer Reihe von Besprechungen reist, müssen ihre Mitarbeiter ihn mit Tagesordnungen, Briefing-Unterlagen und Präsentationsdateien vorbereiten. Diese Dokumente müssen automatisch in seinen Themenordner verschoben werden, damit sie auf ihrem Gerät verfügbar sind, wenn er sie lesen und beantworten kann. Erlauben Sie ihm, die Dokumente offline zu öffnen, denn ein internationaler Flug kann für eine Führungskraft die einzige freie Zeit sein, um ein komplexes Angebots- oder Vertrags-PDF durchzusehen und zu kommentieren.

Die interne Kommunikation ist genauso wichtig wie die Interaktion mit der Außenwelt.

Best Practice #3:

03 Digitalisierung und Verwaltung der Kommunikation des Aufsichtsrats und weiterer Gremien

Stellen Sie sichere Collaboration-Ordner bereit

Die größten Risiken bei der Weitergabe von Informationen bestehen oft bei externen Beteiligten wie Ihren Aufsichtsratsmitgliedern, Anwälten und Bankern, Private Equity-Firmen und M&A-Beratern. Fast alles, was Sie mit diesen Personen teilen, kann Konkurrenten auf den Plan rufen oder gegen Gesetze bezüglich der Offenlegung von Finanzdaten verstoßen, wenn es durchsickert. Viele dieser externen Parteien konsumieren - wie Ihre Führungskräfte - Informationen unterwegs über Mobiltelefone und Tablets.

Verwalten Sie diese sich ständig ändernden Informationen mit Hilfe von gemeinsamen Ordnern. Legen Sie die Berechtigungen für jeden Ordner so fest, dass nur Personen, die diese Informationen kennen müssen, sie sehen können und nur Personen, die Daten eingeben müssen, sie ändern können. Achten Sie bei solch sensiblen Informationen darauf, dass Sie einen unveränderlichen Audit-Trail und Richtlinien für das automatische Verfallsdatum einführen.

Unterstützen Sie die Zusammenarbeit mit externen Gremien, um gemeinsam an Projekten wie Verträgen, Übernahmen oder Finanztransaktionen zu arbeiten. Ermöglichen Sie die einfache und nahtlose Bearbeitung in Microsoft Word-, Excel- und PowerPoint-Anwendungen oder das Kommentieren und Unterzeichnen von PDFs, wobei die Änderungen automatisch im sicheren Collaboration-Ordner gespeichert werden. Unabhängig davon, ob der externe Empfänger einen Browser oder eine mobile App verwendet, können Sie Benachrichtigungen bereitstellen, alle Dateiversionen nachverfolgen und den Audit-Trail stets auf dem neuesten Stand halten.

Best Practice #4:

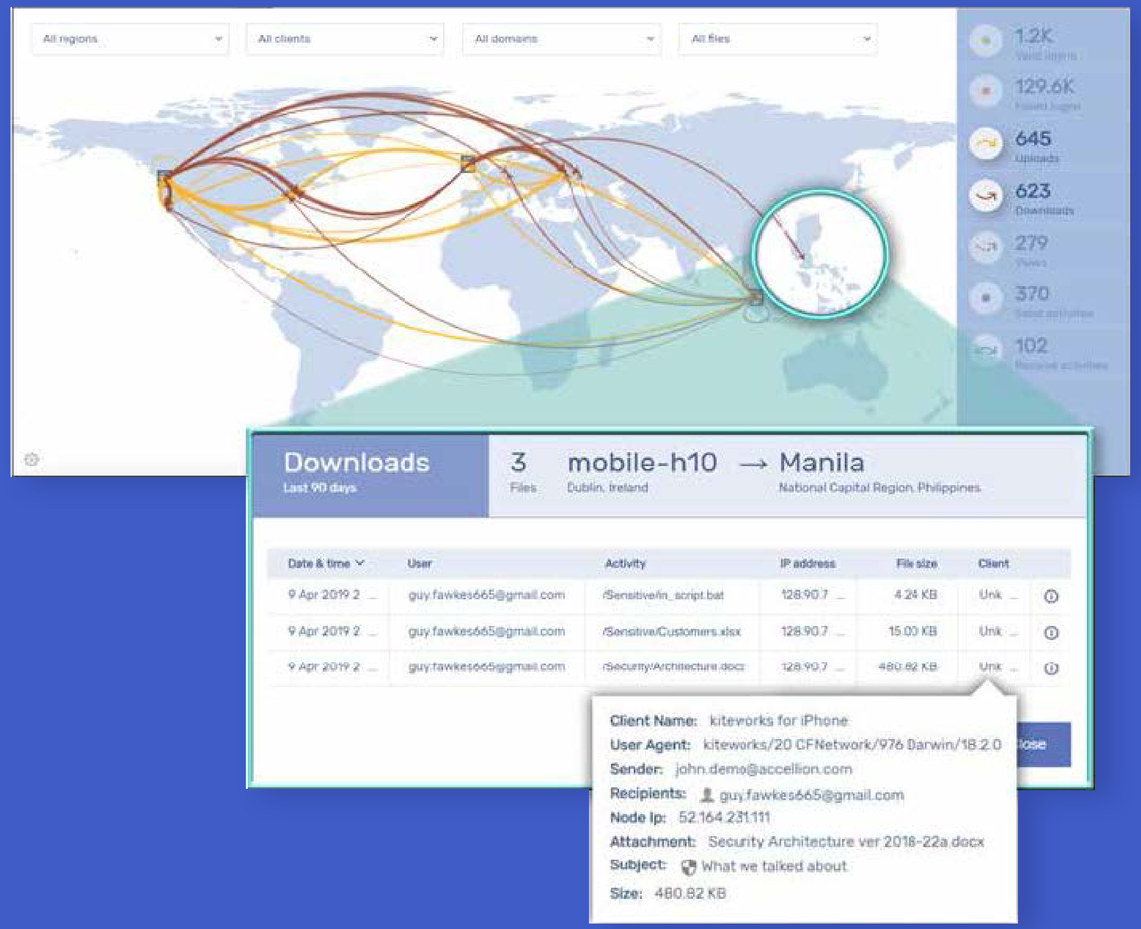
04 Schützen Sie Ihre mobilen Inhalte

Sichere Dateien End-to-End auf jedem mobilen Gerät

Vielleicht nutzen Ihre Führungskräfte gegenwärtig Standard-Cloud-Dateifreigaben und E-Mail, um mit ihren Mitarbeitern und externen Parteien in Kontakt zu bleiben. Die Public-Cloud-Anbieter dieser Tools sind jedoch in der Lage, die Metadaten Ihrer Datenübertragungen zu scannen, was Ihr Risiko erhöht. Im Falle einer Vorladung haben diese Anbieter die Möglichkeit und die Pflicht, Ihre vertraulichen Daten ohne Durchsuchungsbefehl herauszugeben.

Reduzieren Sie die Risiken mobiler E-Mails und freigegebener Ordner mit einer erstklassigen Sicherheits- und Governance-Plattform. Implementieren Sie den Service auf einem gehärteten, skalierbaren Server-Cluster und verschlüsseln Sie die Informationen während der Übertragung und bei der Speicherung auf dem Gerät oder Server mit von der IT verwalteten Schlüsseln. Kontrollieren Sie, wer auf Ihre Daten zugreifen kann, indem Sie den Service in einer lokalen, FedRAMP- oder privaten Cloud-Infrastruktur bereitstellen. Da sich externe Benutzer Ihrer Kontrolle entziehen, sollte die App so gehärtet sein, dass sie auf deren privaten Geräten sicher ausgeführt werden kann.

Ermöglichen Sie Administratoren die rollenbasierte Kontrolle von Richtlinien, die Verwaltung von Benutzern mobiler Geräte, das Hinzufügen von unterstützenden Anwendungen wie Microsoft Word zur Whitelist und Sicherheitsintegrationen wie LDAP/AD und MDM. Eliminieren Sie das Risiko von Unternehmensdaten auf einem fremden oder gestohlenen Gerät, indem Sie das Gerät remote löschen, ohne die persönlichen Inhalte des Benutzers zu verändern.



Best Practice #5:

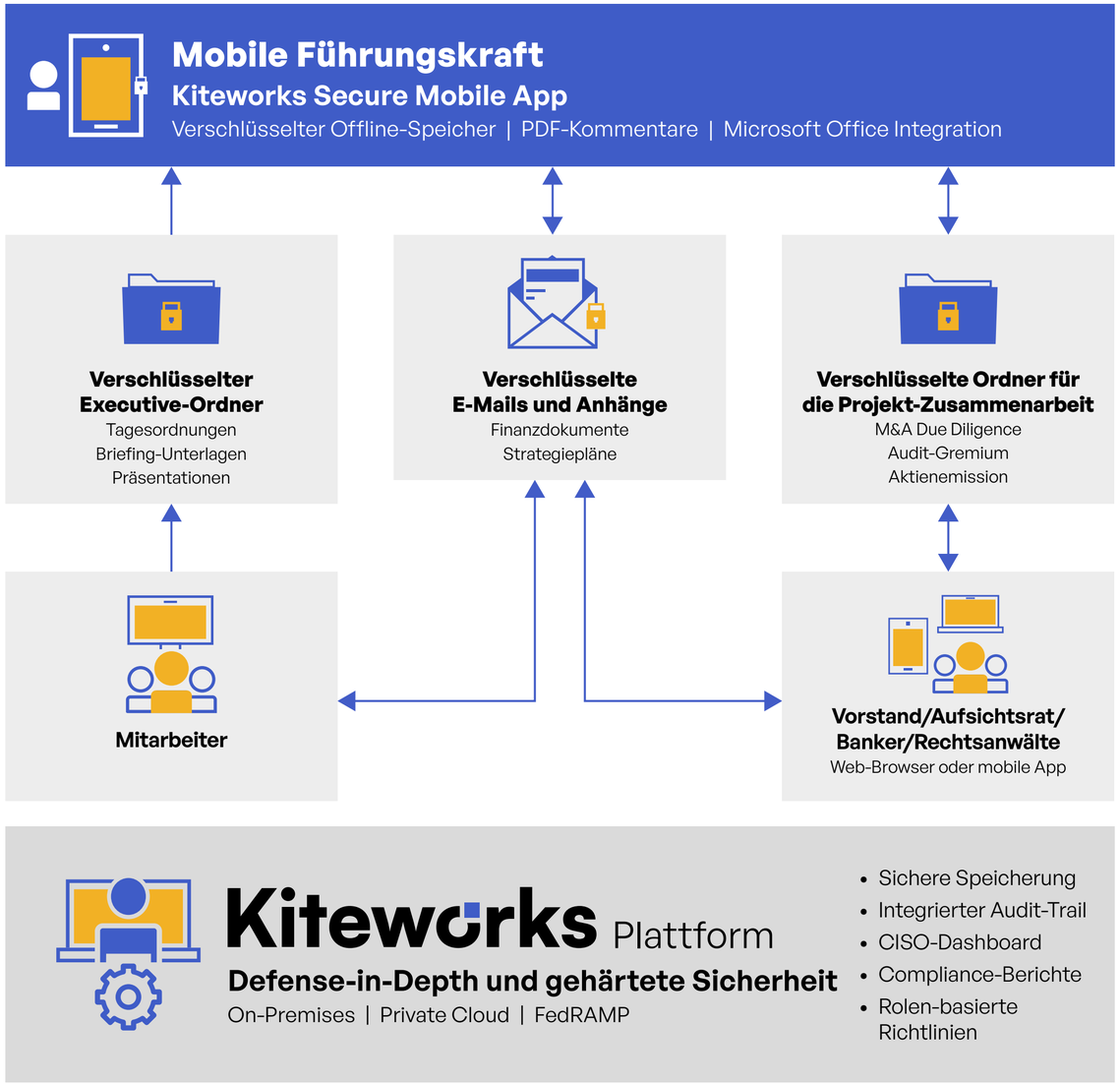
05 Verhindern Sie Datenschutzverletzungen

Transparenz bei jeder mobilen Dateiübertragung

Um sich vor Bedrohungen zu schützen, die von internen und externen Personen bei der mobilen Kommunikation mit Managern und Vorstandsmitgliedern ausgehen, müssen Sie genau wissen, welche Dateien über mobile Geräte in Ihr Unternehmen gelangen und es verlassen. Beginnen Sie mit der Implementierung eines konsolidierten Audit-Trails für alle mobilen Übertragungen zwischen Ihrem Unternehmen und diesen reisenden oder externen Parteien. Sobald Sie über diese Metadaten verfügen, können Sie klare und vollständige Echtzeit-Visualisierungen erstellen, die die wichtigsten Sicherheitsfragen in Bezug auf die Informationen beantworten, die das Unternehmen erreichen und verlassen. Woher kommen sie? Wohin gehen sie? Wer sendet sie? Wer empfängt sie? Sind sie vertraulich? Ist die Transaktion normal oder stellt sie eine Bedrohung dar?

Kiteworks Private Content Network

Verhindern Sie Sicherheits- und Compliance-Verstöße durch Führungskräfte auf Dienstreise.



Kiteworks

www.kiteworks.com

Juli 2022