SICHERE KOMMUNIKATION MIT

MOBIVISOR

Über uns

Die IOTIQ GmbH stellt seit 2017 innovative Softwarelösungen für verschiedene Anwendungsbereiche bereit. Unser Anliegen ist es, Unternehmen aller Branchen und Größen darin zu unterstützen, den Weg in Richtung Digitalisierung mit den richtigen Werkzeugen an der Hand und dem richtigen Partner an der Seite zu beschreiten.
In einer Welt, die mobil ist und stetig mobiler wird, steht die Sicherheit nach wie vor an oberster Stelle.
Um diese zu sichern, haben wir MobiVisor entwickelt - das Mobile Device Management System, dass genau zu Ihnen passt.

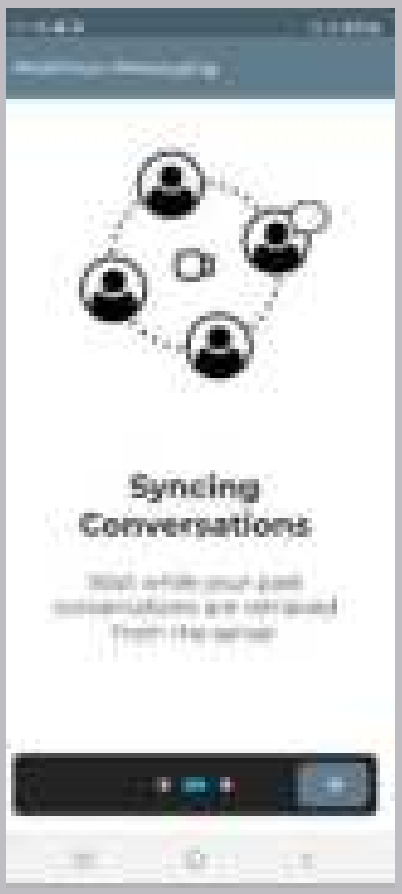
IOTIQ

Smartly Done.

ZU BERÜCKSICHTIGENDE FAKTOREN

In der Regel nutzen Unternehmen öffentliche Chat-Netzwerke wie SMS, MMS, WhatsApp, Skype, Telegram, WeChat, Line oder Social-Media-Anwendungen wie Facebook oder LinkedIn, um mit ihren Mitarbeiter*innen in Kontakt zu bleiben. Ein großes Sicherheitsrisiko besteht darin, dass die Daten in diesen Anwendungen meist auf amerikanischen Servern gehostet werden. In den USA gelten nämlich weniger Datenschutzvorschriften als in anderen Ländern, beispielsweise in der EU.

Darüber hinaus bieten die oben aufgeführten, allgemein bekannten Apps keinen ausreichenden Schutz für die Nutzenden. Sie erlauben es den Nutzer*innen, mit jedem in ihrer persönlichen Kontaktliste zu kommunizieren und ignorieren dabei die Vorsicht des Unternehmens. Sie bieten keine unternehmensspezifische Kontaktliste für die Teamarbeit. Intern sollte eine Richtlinienliste erstellt werden, die festlegt, welche Apps von wem und in welchen Zeiträumen genutzt werden können. Auch wenn Apps wie Instagram und Facebook vor allem bei kreativen Aufgaben als Inspiration dienen können, ist die Wahrscheinlichkeit groß, dass eine Vielzahl von Kontakten mit beliebigen Personen Mitarbeitende ablenkt und ihre Konzentration auf geschäftsrelevante Themen beeinträchtigt. Hier bietet Ihnen MobiVisor mit seiner Erweiterung MobiVisor Messenger die Möglichkeit, Direkt- und Gruppennachrichten im Unternehmen zu unterstützen.



Wenn Sie Ihr Gerät wechseln und MobiVisor Messenger auf das neue Gerät herunterladen, müssen Sie sich keine Sorgen um Ihre vergangenen Konversationen machen. Sie werden gesichert und können auch auf dem neuen Gerät angezeigt werden.

Wenn Sie feststellen, dass etwas mit der App nicht stimmt und einige Funktionen nicht reibungslos funktionieren, finden Sie in den Fehlerberichten Hinweise darauf, wo das Problem liegt und wie es behoben werden kann.

Dies ist ein Beispiel dafür, wie der Nachrichtenbildschirm aussieht. Sie können alle Arten von Medien, Dokumenten, Videos und Audiodateien senden und empfangen.

Der MobiVisor Messenger ist besonders zuverlässig, da er die Nachrichten mit einer verschlüsselten Infrastruktur über SSL/TLS sichert. Im Gegensatz zu anderen Chat-Apps können Bilder, Dateien, Texte und Dokumente eingeschränkt werden, da dann niemand diese Elemente kopieren und einfügen oder weiterleiten kann. Selbst wenn ein Gerät verloren geht, kann der Inhalt von Nachrichten aus der Ferne gelöscht werden, so dass niemand sie sehen kann, wenn das Gerät gefunden oder angesehen wird. Da das Gerät in den Verlustmodus versetzt werden kann, wird verhindert, dass Fremde es vollständig nutzen und auf Unternehmensdaten zugreifen können.

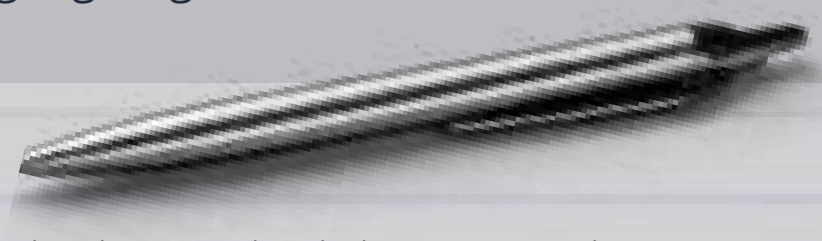
KOMMUNIKATIONSSCHWIERIGKEITEN

Datenmissbrauch

Das Weiterleiten von Nachrichten oder das Kopieren und Einfügen von Text in einen anderen Chat kann bereits ein Datenmissbrauch sein. Meistens gehören Daten und Informationen, die im Zusammenhang mit Unternehmens-aufgaben erstellt werden, dem Unternehmen und nicht dem Mitarbeitenden. Dieser Unterschied ist wichtig, denn eine so kleine Handlung wie das Senden von Informationen an eine private E-Mail-Adresse, auf die man später zurückgreifen möchte, kann einen Verstoß gegen die Datenstrategie des Unternehmens darstellen.

Unbefugter Zugriff

Es muss klar sein, dass Nachrichten innerhalb bestimmter Abteilungen, zwischen Mitarbeiter*innen oder zwischen dem Unternehmen und externen Parteien vertraulich sind. Es darf nicht sein, dass diese Nachrichten von Anderen eingesehen werden können. Dies geschieht leichter, als die meisten von uns sich vorstellen können: Sie brauchen nur zu vergessen, den Praktikanten aus dem Gruppenchat zu entfernen oder ihm den Zugang zu gemeinsamen Dateien zu entziehen.



Die **Endpunktsicherheit** besteht aus vielen Schichten:

1. **Signatur-Vergleiche**: Testet die Signatur (Code) jedes Virus und vergleicht sie mit einer Reihe bekannter Viren.
2. **Verifizierung durch maschinelles Lernen**: Bereitet das Verhalten des Systems auf die Abwehr von Cyber-Bedrohungen vor.
3. **Verhaltensanalyse**: Entdeckt jedes ungewöhnliche Verhalten im System und bestimmt, ob es bösartig ist.

Undefinierte Kontaktliste

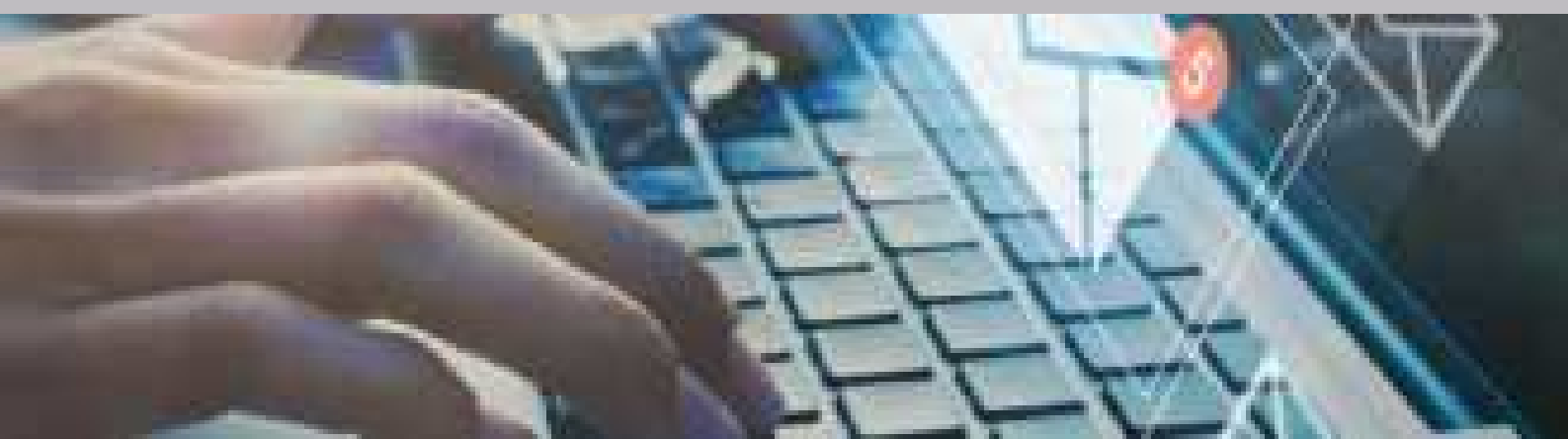
Manchmal werden die E-Mail-Konten von Mitarbeitern durch Werbung, Anwendungsbenachrichtigungen und mehr terrorisiert. Dies liegt daran, dass fast alle kommerziellen Websites und Anwendungen E-Mail-Konten erfordern, um eine Mitgliedschaft zu erstellen. Deren unnötige E-Mails können als Bedrohung angesehen werden, solange sie im zentralen Posteingang auftauchen.

Nutzung öffentlich zugänglicher Chat-Apps

Apps wie WhatsApp, Line, WeChat und Telegram können im Hinblick auf den Datenschutz schädlich sein. Von der Nutzung von Express-Mail-Diensten wie Gmail, Outlook usw. ist ebenfalls abzuraten. Wie bereits erwähnt, speichern sie die Daten meist auf amerikanischen Servern, die weniger strenge Datenschutzgesetze haben.

Internes Weiterleiten

Manchmal kommt es vor, dass Mitarbeiter Dokumente versehentlich oder absichtlich an die falsche Person weiterleiten, wenn zum Beispiel Daten über Kosten, Leistungen und Gehälter eigentlich an die Finanzabteilung des Unternehmens geschickt werden sollen, einige Mitarbeiter*innen sie jedoch an die Marketingabteilung weiterleiten.



Haftung für Emails

Unternehmen können Viren, Würmer oder jegliche Art von Malware über E-Mails an andere Unternehmen weitergeben. Manchmal verbreiten sie sie unbeabsichtigt, wenn ein anderes Unternehmen ihnen zuvor einen Virus übermittelt hat und sie sich dessen nicht bewusst sind.

Spam

Wenn Nachrichten an jeden in der persönlichen Kontaktliste gesendet werden können und wenn keine spezielle Kontaktliste für Firmenangelegenheiten erstellt wird, kann der Inhalt des Kommunikationsnetzes durchgesickert sein. Eine Trennung zwischen Arbeitskontakten und persönlichen Kontakten kann durch Containerisierung erreicht werden (die Aufteilung zwischen Arbeitsprofil und privatem Profil auf einem Gerät).

Lösungen

- Festlegung klarer Datenschutzrichtlinien für die Kommunikation, damit jeder Mitarbeitende die Regeln befolgt.
- Verschlüsselung von schriftlichen Texten und Videokonferenzen mit komplexen Passwörtern, einschließlich Touch ID, Face ID usw.
- Schulungen spielen eine wichtige Rolle, um das Sicherheitsbewusstsein von Arbeitnehmern, Arbeitgebern und Unternehmen zu verbessern.
- Cloud-Computing, d. h. Datensicherungen, retten Sie im Falle eines gestohlenen/verlorenen/gebrochenen Geräts.
- Die Überwachung von Apps hält Mitarbeiter*innen davon ab, sich in öffentlichen Chat-Netzwerken wie WhatsApp, WeChat usw. zu engagieren und persönliche Kontakte mit Personen außerhalb des Büros zu knüpfen.

- Die Kontrolle der E-Mail-Verteilung spielt eine wichtige Rolle, um sicherzustellen, dass die Daten direkt an den richtigen Empfänger geschickt werden.
- Sicherung von E-Mails über SSL (Secure Socket Layer), d. h. eine verschlüsselte Verbindung zwischen einem Client und einem Server.
- Blockieren des E-Mail-Zugriffs von nicht autorisierten Geräten.
- Beschränkung des E-Mail-Zugangs auf vom Unternehmen zugelassene Geräte.
- Aufdecken von nicht verwalteten Geräten, die versuchen, auf Unternehmens-E-Mails zuzugreifen.
- Eine qualifizierte elektronische Signatur ist rechtsverbindlich und gültig in Bezug auf die sichere Kommunikation über Papierkram, wenn Dokumente grenzüberschreitend ausgetauscht und unterzeichnet werden müssen. Eine digitale Signatur kann in E-Mails, Installationspaketen, Anwendungsupdates usw. verwendet werden.

Sie wollen mehr erfahren?

Haben Sie Fragen zur Funktionsweise von MobiVisor und unseren Erweiterungen oder sind Sie unsicher, ob MobiVisor MDM zu Ihrem Unternehmen und dessen Herausforderungen passt?

Wir stehen Ihnen gerne mit Rat und Tat zur Seite! Kontaktieren Sie uns einfach per Telefon oder E-Mail.
Gerne vereinbaren wir auch einen persönlichen Präsentationstermin mit Ihnen und stellen Ihnen eine unverbindliche Testumgebung von MobiVisor zur Verfügung.

Toni Voß
toni@iotiq.de
+49 1578 3020995

Saskia Riechers
saskia@iotiq.de
+49 176 1500 6080