Risikomanagement mit

MOBIVISOR

Die Verwaltung eines Unternehmens ist mit vielen verschiedenen Herausforderungen verbunden. Von nun an ist das Risikomanagement dank MobiVisor nicht mehr schwierig!

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.

Wie MobiVisor Unternehmen bei der Bewältigung von Risiken hilft

RISIKEN

Sicherheitsrisiken

Wenn ein*e Mitarbeiter*in das Büro mit ihrem Gerät verlässt, kann dies zu Sicherheitsrisiken, Datenverlusten usw. führen.

Verlorene Geräte

Die Verwendung von Mobilgeräten an öffentlichen Orten birgt das Risiko, dass diese Geräte gestohlen werden.

Der Besitz von Daten

Durch die Bring Your Own Device-Methode am Arbeitsplatz werden Unternehmensdaten auf demselben Gerät gespeichert wie die privaten Daten des Mitarbeitenden. Private und Unternehmensdaten am selben Ort können gefährlich sein. Beispielsweise könnten Mitarbeitende versehentlich Unternehmensdaten auf ihrem eigenen Geräten versenden, oder ein mit Unternehmensdaten versehenes Gerät im Besitz eines Mitarbeitenden könnte verloren gehen oder gestohlen werden, was dann zu einem Datenverlust führt.

Unvertrauenswürdiges Mobilgerät

Die Verwendung eines Geräts einer nicht sehr bekannten Marke oder eines Modells, das zu alt ist, um mit einem MDM ausgestattet zu werden, kann bei Mitarbeitenden Zweifel wecken.

Verdächtige Apps

Einige bekannte Apps mögen auf den ersten Blick zuverlässig erscheinen, sind aber für Firmengeräte völlig ungeeignet. Sie sind öffentlich zugänglich und einige enthalten kleine Werbeanzeigen, die gefährlich sein können, wenn Sie darauf klicken - manchmal können Werbelinks Sie auf eine belanglose Seite leiten, die nach Ihren privaten Daten fragt, um diese zu stehlen. Auf diese Weise können Unternehmensdaten gestohlen werden.

Offene WLAN-Netzwerke

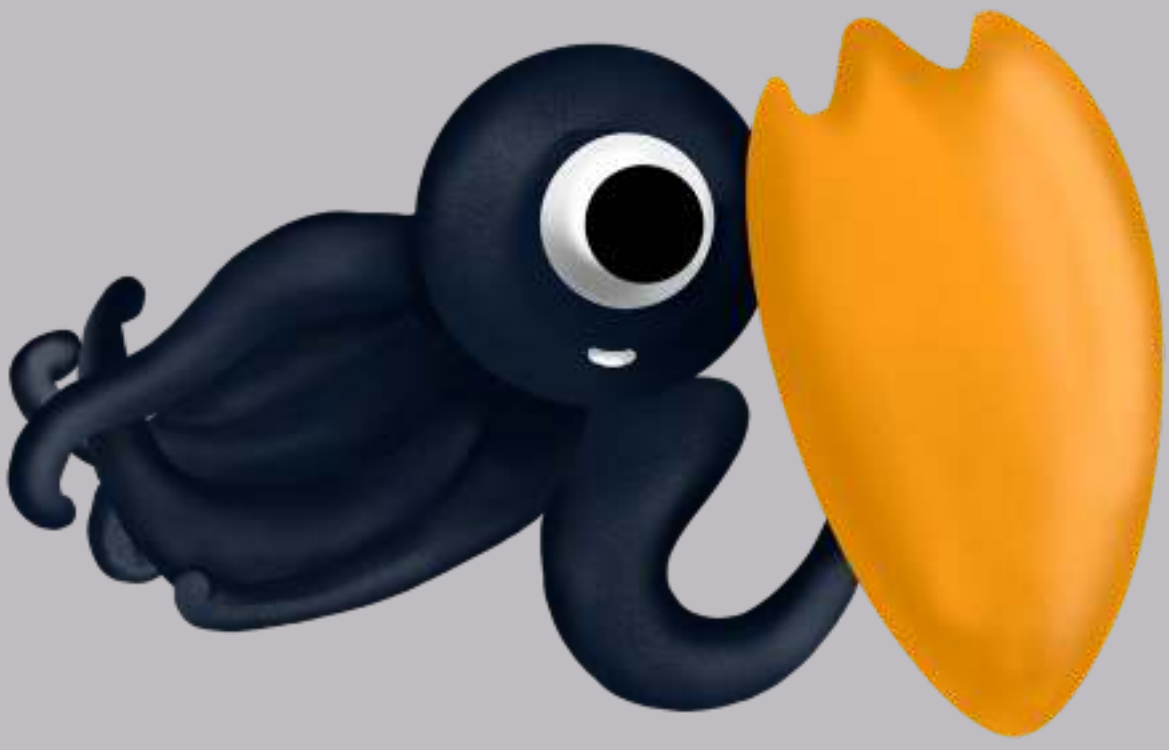
Eine WLAN-Verbindung, die kein Passwort hat oder von allen Personen im Firmengebäude genutzt wird, ist schlecht für die Sicherheit. Ein gemeinsames WLAN birgt das Risiko des Diebstahls von Unternehmensdaten, von Cyberangriffen, der Verbreitung von Malware und mehr.

Veraltete Software

Älterer Software fehlt es an neuen Verbesserungen der Sicherheitsfunktionen und der Verschlüsselung durch den Hersteller. Dadurch werden Geräte leichter durch Malware infiziert.

Phishing

Phishing ist ein Versuch von Cyberkriminellen, das Vertrauen eines Opfers zu gewinnen, indem sie es dazu bringen, auf einen Link zu klicken oder sensible Informationen preiszugeben. Phisher versenden E-Mails, die wie die von offiziellen Banken und anderen bekannten Quellen aussehen. Sie erstellen auch Websites, die vertrauenswürdigen Websites ähneln oder diese nachahmen.



Lösungen mit MobiVisor

Zugriff deaktivieren

Arbeitgeber sollten den Zugang außerhalb der Bürozeiten begrenzen, um Sicherheitsverletzungen zu verhindern.

Passwort & Encryption

Das MDM kann komplexe Passwörter sowie Face-ID- und Touch-ID-Optionen aktivieren, die über einfache numerische Passcodes hinausgehen, um Ihr Gerät sicher zu halten.

Isolation

Unternehmen können ihre Daten von privaten Daten isolieren, indem sie ein spezielles Cloud-Computing-System verwenden. Auf diese Weise können unternehmens-bezogene Daten in einer bestimmten Cloud mit einem speziellen Passwort gesichert werden.

Einheitliche Geräte

Die Festlegung eines Standardgeräts (iPhone, iPad, Samsung, Casper etc. für alle Mitarbeitenden ist von Vorteil, um Probleme mit alten Geräten zu vermeiden.

App Monitoring:

Mit MobiVisor können Sie Apps auf Ihren Geräten aktualisieren, löschen oder sperren - alles, was mit Kontrolle und Verwaltung zu tun hat.

- Unternehmensspezifischer Appkatalog
- Installierte Apps aktualisieren
- Individuelle Freigabe und Sperrung von Apps
- Apps aus der Ferne installieren und löschen
- App-Schutz durch Backups

Per-App-VPN

Sie definieren bestimmte Apps und Internet-Domains. Wird auf eine definierte App oder Domain zugegriffen, aktiviert sich die VPN-Verbindung automatisch und Ihre Daten sind geschützt.

WLAN-Monitoring:

MDM-Lösungen ermöglichen es Administrator*innen, WLAN-Einstellungen und -Konfigurationen auf Geräten zu ändern, Geräte automatisch mit bestimmten WLAN-Netzwerken zu verbinden, Benutzern die Verbindung mit illegalen WLAN-Netzwerken zu untersagen und sie sogar daran zu hindern, die WLAN-Verbindung ganz abzuschalten.

Automatisierte Updates:

MDM sorgt dafür, dass Ihr Gerät immer auf dem neuesten Stand ist, anstatt Updates je nach den Interessen der Mitarbeitenden manuell zu bestätigen. Fortschritte bei den Datenschutzrichtlinien und der Cybersicherheit des Geräts helfen Ihnen, im Falle eines Virenangriffs oder eines Cyberschadens dynamisch zu bleiben.

Scam-Nummern blockieren:

Durch die Sperrung von Nummern, die z. B. mit 0850 beginnen, kann die MDM Cyberbetrügern, die wie Werbetreibende aussehen, an den Arbeitsplätzen eine Falle stellen. Darüber hinaus kann die MDM spezielle E-Mail-Server für Unternehmen bereitstellen, damit Mitarbeiter*innen nicht mit kommerziellen gefälschten E-Mails konfrontiert werden, deren Ziel Phishing ist.

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