MITARBEITER*INNEN-ZUFRIEDENHEIT MIT MDM

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.

BRING DEIN EIGENES GERÄT ZUR ARBEIT

Mobile Geräte wie Laptops und Smartphones werden in großem Umfang für private und geschäftliche Zwecke genutzt. Vor allem mit der COVID-19-Pandemie und der zunehmenden Arbeit von zu Hause aus hat auch die Bedeutung der Nutzung mobiler Geräte zugenommen. Mitarbeiter*innen begannen, ihre eigenen Geräte zu verwenden, verbanden sie aber mit dem Unternehmensnetzwerk oder griffen aus der Ferne auf Unternehmensdaten zu. Diese Situation blieb auch dann noch bestehen, als das Arbeitsleben zur "neuen Normalität" zurückkehrte. Die meisten Unternehmen fanden vorteilhaft, wenn ihre Mitarbeitenden ihre eigenen Geräte mitbrachten und damit arbeiteten. Aber wie jede technologische Entwicklung birgt natürlich auch die Nutzung eigener Geräte durch Angestellte nicht nur Vorteile, sondern auch Risiken.

Bring Your Own Device (BYOD) zum Beispiel ist eine Richtlinie, die es den Mitarbeitenden eines Unternehmens erlaubt, ihre eigenen Geräte zu benutzen. Unternehmen definieren eine Reihe von Richtlinien, die es ihren Mitarbeiter*innen erlauben, ihre eigenen Geräte für den Zugriff auf E-Mails, Unternehmensanwendungen und -daten sowie für die Verbindung mit Unternehmensnetzwerken zu nutzen.

Es gibt auch Alternativen zu BYOD-Modellen, beispielsweise COBO-Geräte (company-owned/business-only) oder COPE-Geräte (company-owned/personally-enabled). Diese beiden Optionen bedeuten, dass das Unternehmen die mobilen Geräte kauft und besitzt und ihren Angestellten die Möglichkeit gibt, auf Unternehmensinformationen und -anwendungen zuzugreifen. Das Hauptaugenmerk dieses Infopapers liegt jedoch auf dem BYOD-Modell, das gemeinhin mit der IT-Consumerization in Verbindung gebracht wird.

Da BYOD-Modelle Angestellten den Zugang zu Unternehmensinformationen ermöglicht, ist es für Unternehmen von entscheidender Bedeutung, eine gut definierte BYOD-Richtlinie zu haben, um die Gefahr von Cyber-Bedrohungen wie Ransomware, Hacking und Datenschutzverletzungen zu vermeiden.

EINRICHTUNG EINER BYOD RICHTLINIE

Eine BYOD-Richtlinie wird im Allgemeinen in einem Dokument mit einigen Anforderungen erstellt, deren Umsetzung die Arbeitnehmer*innen akzeptieren. Diese Anforderungen können sein:

- Arten von mobilen Geräten, die von der IT-Abteilung zur Nutzung zugelassen sind
- Eine klare Definition der Kündigungsrichtlinien
- Sicherheitsmaßnahmen wie z.B. Passwortanforderungen
- Verantwortlichkeiten der Benutzer in Bezug auf das Gerät und seinen Zugang zum Netz
- Anreize oder Kostenerstattungen für die Nutzung persönlicher Datenpläne für arbeitsbezogene Aktivitäten
- Software, die installiert werden muss, um ein Gerät zu sichern, z.B. ein MDM-Tool
- Ein Ausstiegsplan für den Fall, dass Mitarbeitende ihre persönlichen Geräte nicht mehr nutzen möchten

WARUM BYOD?

Zufriedenheit der Mitarbeitenden

Das BYOD-Modell ist in den letzten Jahren immer beliebter geworden, vor allem während der COVID-19-Pandemie, da es den Mitarbeitern ermöglicht, von zu Hause oder unterwegs auf das Netzwerk und die Daten ihres Unternehmens zuzugreifen. Mit Hilfe des BYOD-Modells können die Menschen wählen, wo sie arbeiten und sich unabhängig bewegen, da sie die Möglichkeit haben, ihre eigenen Geräte überallhin mitzunehmen. Vor allem junge Menschen suchen sich gerne aus, wo sie leben wollen, und wollen nicht an einen Arbeitsplatz an einem bestimmten Ort gebunden sein, was ein BYOD-Modell für diese Arbeitskräfte attraktiver macht.

Warum sollten Mitarbeiter*innen ihre eigenen Geräte verwenden?

- Höhere Produktivität der Mitarbeiter: Wenn sie nicht zwischen den Geräten wechseln müssen, können Mitarbeiter*innen schneller auf die Arbeit zugreifen
- Mehr Komfort: Die Mitarbeiter fühlen sich wohler, wenn sie ihre eigenen Geräte nutzen, als wenn sie lernen müssen, wie man mit neuen Geräten umgeht.
- Neueste Technologien werden in den Arbeitsplatz integriert: Ohne IT-Ausgaben für Hardware, Softwarelizenzen oder Gerätewartung
- Höhere Mitarbeiterzufriedenheit durch Unterstützung flexibler Arbeitsregelungen
- Bessere allgemeine Benutzererfahrung, da die Geräte bekannt sind
- Weniger Geräte, die die Mitarbeiter mit sich führen müssen

Warum sollten Unternehmen das BYOD Modell übernehmen?

- Vereinfachtes Onboarding und Offboarding: Mit der Verwendung von MDM und dem BYOD-Modell kann der Zugang zum Unternehmensnetzwerk aktiviert/deaktiviert werden
- Kostenersparnis: Die Nutzung des BYOD-Modells verringert die Unternehmensressourcen, die nachverfolgt, ausgegeben, verwaltet oder aufgerüstet werden müssen.
- 59% der Unternehmen haben BYOD eingeführt
- 67 % der Arbeitnehmer nutzen ihre eigenen Geräte bei der Arbeit
- 87 % der Unternehmen sind darauf angewiesen, dass ihre Mitarbeiter von ihrem Smartphone aus auf mobile Geschäftsanwendungen zugreifen können

Unternehmenssicherheit

Mit der zunehmenden Verbreitung des BYOD-Modells wird die Gewährleistung der Sicherheit immer wichtiger. Um diese zu gewährleisten, sollten die IT-Abteilungen der Unternehmen ein Mobile-Device-Management-System (MDM) einsetzen, um Gefahren und Risiken zu minimieren und Zugriffe und Berechtigungen verwalten zu können.

Darüber hinaus können Unternehmen, die BYOD-Modelle einführen, auch bestimmte Sicherheitsrichtlinien für jedes Gerät sicherstellen. Die Richtlinie sollte Folgendes beinhalten:

- Sicherheitskontrollen einschließlich: Datenverschlüsselung und Passwortstärke
- Welche Software zur Verwaltung mobiler Geräte (MDM) muss auf BYOD-Geräten installiert werden?
- Ob das Unternehmen befugt ist, aus der Ferne zu kontrollieren, und einzugreifen, wenn ein Verstoß gegen die Richtlinien festgestellt wird
- Welche Websites sind verboten, wenn sie mit Unternehmensressourcen, dem Unternehmensnetzwerk oder VPN verbunden sind?.
- Auf welche Unternehmensanwendungen und -daten kann von Benutzergeräten aus zugegriffen werden, z. B. auf E-Mail, Kalender, Nachrichten, Kontakte usw.

Sicherheit der Mitarbeiter*innen

Das **Bring Your Own Device (BYOD)-Modell** ermöglicht den Zugriff auf Unternehmensdaten, aber die Mitarbeiter*innen sind besorgt, dass auch ihre privaten Informationen preisgegeben werden. Durch ein MDM kann dies verhindert und das BYOD-Modell abgesichert werden.
Mit einem MDM können Unternehmen nicht auf die persönlichen Daten des Gerätebesitzers zugreifen, diese kontrollieren oder überwachen.

Ein MDM wird nur für die Sicherheit von Unternehmensinformationen und unternehmensbezogenen Transaktionen verwendet. Daher fordert es Zugang zu Informationen, die diese Sicherheit gewährleisten. Bei diesen Informationen handelt es sich um technische und gerätespezifische Informationen wie die Seriennummer und den Namen des Gerätemodells. Es gibt keine Funktion wie die Verfolgung des Suchverlaufs oder den Zugriff auf persönliche Notizen. MDM dient in erster Linie nicht der Kontrolle, sondern der Verwaltung.

In diesem Zusammenhang ist die erste und wichtigste Vorsichtsmaßnahme zur Gewährleistung der Sicherheit der Mitarbeiter im BYOD-Modell die Verwendung eines MDM.

Nutzung der Sozialen Medien

Ein weiteres Thema, das mit der Einführung des BYOD-Modells kontrovers diskutiert wird, ist die Beeinträchtigung der Sicherheit und der Produktivität der Mitarbeiter durch die Nutzung Sozialer Medien.
Das BYOD-Modell bietet durch das MDM verschiedene Möglichkeiten, wie z. B. die Festlegung von Richtlinien, die sich auf Sicherheitsschwachstellen beziehen. Da Umsetzung der Richtlinien aus der Perspektive des Unternehmens erfolgt, ist die Existenz von Sicherheitsrichtlinien für die Sozialen Medien, die Mitarbeiter täglich auf ihren eigenen Geräten nutzen, natürlich umstritten. Daher sollten Unternehmen, die sich für das BYOD-Modell entscheiden, auch eine Richtlinie für Soziale Medien einführen und diese mit den Mitarbeiter*innen besprechen.

Sicherheits Bedenken:
Die Nutzung Sozialer Medien durch Mitarbeiter*innen im Rahmen des BYOD-Modells kann eine Gefahr für vertrauliche Geschäftsinformationen darstellen und Informationen über das Privatleben der Mitarbeiter preisgeben. Daher sollten Unternehmen bei der Einführung von BYOD-Richtlinien auch die Nutzung sozialer Medien durch ihre Mitarbeiter einschließen, und ihre Mitarbeiter im Hinblick auf die Umsetzung der Richtlinien und den Zugang zu Informationen schulen. Darüber hinaus sollten sie ein Mobile Device Management (MDM) einsetzen, um die Trennung zwischen persönlichen und Unternehmensdaten zu gewährleisten und den Zugriff auf Informationen im Rahmen dieser Trennung zu ermöglichen.

Was ein MDM erreichen kann:
Durch die Einrichtung eines sekundären Profils, das für die Arbeit verwendet wird, werden die Daten getrennt, indem private und berufliche Daten in unterschiedlichen Containern gesichert werden. Apps, die zB. nur im Arbeitsprofil verwendet werden, sind auf Android entsprechend gekennzeichnet. Das bedeutet, dass zwei Versionen der gleichen App existieren, die nicht miteinander verbunden sind und somit private und berufliche Daten trennen. Ein Transfer von Konten oder Daten aus den Profilen ist somit ausgeschlossen.

Produktivität der Mitarbeiter*innen

Erhöht die Verwendung eigener Geräte im Rahmen des BYOD-Modells die Nutzung sozialer Medien durch die Mitarbeiter? Wie wirkt sich das auf die Produktivität aus? Die Antworten auf diese Fragen variieren je nachdem, wofür die Mitarbeitenden die sozialen Medien nutzen.

Wird die Social-Media-Nutzung der Mitarbeitenden im Hinblick auf die Produktivität bewertet, muss unterschieden werden. Laut einer Studie erhöht sich die Arbeitszufriedenheit, wenn Arbeitnehmer*innen soziale Medien nutzen, um zwischen der Arbeit Kontakte zu knüpfen. Wenn sie jedoch soziale Medien aus arbeitsbezogener Motivation heraus nutzen, erhöht dies ihre Produktivität.

Das BYOD-Modell bietet Raum für beides. Die Mitarbeitenden können mit ihren eigenen Geräten in den sozialen Medien Kontakte knüpfen, ohne die Privatsphäre zu verletzen, ihre Produktivität steigern, indem sie Werbung machen und Entwicklungen verfolgen, die mit ihrer Arbeit zusammenhängen. Vor allem in Arbeitsbereichen, in denen Problemlösungskompetenz, Kreativität und das Bewusstsein für Entwicklungen und Trends wichtig sind, wie z. B. im Marketing, in der Geschäftsentwicklung oder im Vertrieb, kann die Nutzung sozialer Medien dazu beitragen, die Aktivitäten des Unternehmens weiterzuentwickeln, indem man sich von der Konkurrenz inspirieren lässt.

Die Studie zeigt auch:

- Die sozial orientierte Nutzung sozialer Medien ermöglicht es, den Kontakt zu bestehenden Freunden und Kunden zu pflegen.
- Soziale Medien haben erhebliche Auswirkungen auf die Kommunikation und das Management am Arbeitsplatz und in Unternehmen.
- Soziale Medien können das interne Wissensmanagement erleichtern und die Kommunikation und die Arbeitsleistung verbessern.

Auch wenn die **freiere und flexiblere Nutzung der mobilen Geräte** durch die Mitarbeitenden zunächst ein Risiko für die Produktivität zu sein scheint, ist es auch unbestritten, dass **die Zufriedenheit der Mitarbeitenden steigt,** wenn sie mehr Freiheiten haben.

Durch das **BYOD Modell** ist beides möglich. Mithilfe eines MDMs kann diese Nutzung zudem vollständig abgesichert 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