IKARUS security software

IKARUS mobile.management

Datenblatt

Mobility-Lösung für Firmenumgebungen

IKARUS mobile.management löst die komplexen Anforderungen an den flexiblen Einsatz mobiler Endgeräte in Firmenumgebungen. TÜV-geprüft, in unabhängigen Audits getestet und ausschließlich in Europa entwickelt und gehostet, entspricht die Software allen Richtlinien des Europäisches Datenschutzes sowie allen Anforderungen modernen und ortsunabhängigen Arbeitens.

IKARUS mobile.management ist eine hochprofessionelle Komplettlösung mit Mobile Device Management (MDM), Mobile Application Management (MAM), Mobile Content Management (MCM) und Mobile Security Management (MSM). Der besonders flexible Cloud-Service verwaltet und schützt Smartphones, Tablets oder auch Notebooks vor Bedrohungen durch Malware, Datenverlust und unberechtigte Daten- und Systemzugriffe.

Flexibles Arbeiten, unabhängig von Orten und Endgeräten

Die Digitalisierung und Vernetzung unserer Kommunikationswege bringen nicht nur Vorteile, sondern öffnen auch attraktive neue Angriffsflächen – vor allem im Unternehmensbereich, wo es um Firmengeheimnisse genauso wie um persönliche Daten geht. Mitarbeiter*innen sollen mit dem Einsatz von Laptops und Smartphones in ihrer Mobilität und Produktivität unterstützt werden. Gleichzeitig müssen Datensicherheit, die Einhaltung von Unternehmensrichtlinien und rechtliche Rahmenbedingungen gewährleistet sein. Der Spagat zwischen strikten Vorgaben und flexibler Nutzung erfordert eine intelligente Lösung.

Datenschutzpflichten erfüllen und Kontrolle gewinnen

Alle Unternehmen, die mit Daten von EU-Bürger*innen arbeiten, müssen nachweislich sicherstellen, dass auch an Mobilgeräten geeignete organisatorische und technische Sicherheitsvorgaben nach Stand der Technik eingehalten werden. Laptops, Smartphones oder Tablets müssen daher verschlüsselt werden und es sind Backups zu erstellen. Es gilt zusätzliche Einfallstore, beispielsweise durch Berechtigungen am Gerät installierter Apps, abzusichern. Es dürfen nur entsprechend zertifizierte Apps installiert werden und im Zweifelsfall müssen alle Firmendaten via Fernzugriff gelöscht werden können.

Private Daten und Apps sind von Unternehmensdaten zu trennen, beispielsweise mittels Container-Lösungen. Denn nur so können unerlaubte Datenzugriffe und unbefugte Offenlegung vollständig und nachweislich unterbunden werden. Zugleich können die Container die Verschlüsselung der Unternehmensdaten und der Kommunikation zwischen mobilem Endgerät und IT-Abteilung sicherstellen. Alle Risiken und Sicherheitsvorkehrungen müssen zudem regelmäßig überprüft, bewertet und dokumentiert werden.

Ein geeignetes Mobile Management-System bietet auf einen Blick eine detaillierte Übersicht über alle Geräte mit Zugriff auf Unternehmensressourcen. Geräte und Applikationen können zentral verwaltet und inventarisiert werden. Auch die Softwareverteilung inklusive dem Ausrollen von Updates und Lizenzen sollte zentral steuerbar sein – selbstverständlich inklusive eines leistungsfähigen Malwareschutzes, Remote Control Features und automatischen Aktionen im Fall von Sicherheitsverletzungen.

Umfassender Schutz, zentrale Übersicht, einfache Steuerung

Mit **IKARUS mobile.management** erhalten Sie Übersicht und Kontrolle über den mobilen Zugriff Ihrer Anwender*innen auf die Unternehmensressourcen. Individuelle Zugriffsregeln sowie Remote-Konfiguration und Remote-Steuerung der Mobilgeräte ermöglichen die zuverlässige Umsetzung Ihrer Firmen-Policies über alle Systeme hinweg, schützen Geräte wie Daten durch ungeplante und ungewollte Fremdzugriffe und Verlust von Daten, Wissen und Firmengeheimnissen. In einem zentralen anpassbaren Dashboard können flexible Richtlinien definiert und der Status der Systeme und Geräte überwacht werden. Werden Unternehmensvorgaben oder Sicherheitsrichtlinien verletzt, können automatisiert vordefinierte Aktionen ausgeführt werden.

Schlüsselfertig und erprobt ermöglicht **IKARUS mobile.management** den einfachen und schnellen Aufbau einer passgenauen Lösung für das effiziente Management Ihrer mobilen Geräte, Anwendungen und Daten. Der Cloud-Service passt für Kleinunternehmen genauso wie für Enterprises – die Abrechnung erfolgt per User und es gibt keine Obergrenze an Endgeräten. Das Plus an Sicherheit: Alle Daten werden nur auf in Österreich stehenden Servern im ISO-zertifizierten Rechenzentrum Interxion in Wien verarbeitet (ISO27001 und BS25999). Es gelten zur Gänze die österreichischen sowie EU-Datenschutzgesetze.

Mobile Lösungen werden auch in Zukunft eine tragende Rolle in unserem privaten und beruflichen Leben spielen. Daher empfiehlt es sich, in eine zukunftsfähige Lösung zu investieren: Professionelle Konzepte, einfache Handhabung und zuverlässige Methoden lohnen sich. Nicht zuletzt in Anbetracht der empfindlichen Strafen im Falle einer Nicht-Compliance: Wer seine Datenschutzpflichten vernachlässigt, muss mit hohen Strafgeldern kalkulieren.

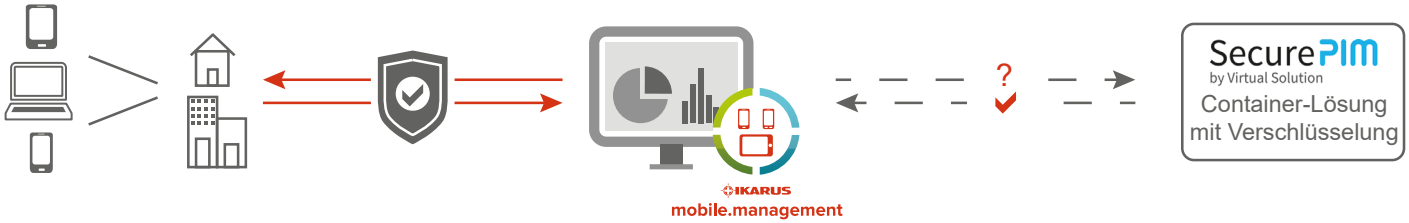

Abb. 1 - Zentrales Mobile Management-System für die sichere und kontrollierte Nutzung mobiler Geräte in Firmenumgebungen

Vorteile

- TÜV Zertifizierung - einzigartig in Europa seit Einführung der EU-DSGVO
- Vollständige Abdeckung aller führenden Plattformen (Android, Android for Work, Samsung KNOX, iOS, Windows 10, Windows 8 Phone, Symbian) über eine einzige Benutzeroberfläche
- Höchste Datensicherheit und Datenschutz nach EU-DSGVO
- BYOD-geeignet:
  Trennung geschäftlicher und privater Daten

Features

- Mobile Device Management (MDM) mit Asset Management, Integration in die zentrale Nutzerverwaltung, Konfiguration durch automatisierte Regeln und Remote-Zugriff sowie Monitoring über ein Web-Interface und konfigurierbare Berichte
- Mobile Application Management (MAM) mit App Security mit Datenbankzugriff auf sicherheitsrelevante App-Bewertungen, Android Mobile Security zum Schutz vor Malware aus Apps und Internet, Container-Support für Passwortschutz und Trennung von geschäftlichen und privaten Daten sowie einen eigenen Enterprise App Store.
- Mobile Content Management (MCM) mit Secure Access Gateway für ein flexibles Management der Zugriffsmöglichkeiten auf Unternehmensressourcen inkl. Firewall, Datenzugriffs per VPN für dedizierte Apps, DSGVO-konformes BYOD-Management & Self Service Portal
- Mobile Security Management (MSM) mit Schutz vor unberechtigtem Zugriff, Sicherheitsmanagement, Virus- und Malware-Scanner für Android, Ausrollen und Verwalten von Templates und Richtlinien, Überwachung der Einstellungen und Richtlinien, automatisierte Aktionen im Fall von Non-Compliance.

»Mobile Lösungen spielen jetzt und in weiterer Zukunft eine tragende Rolle in unserem privaten und beruflichen Leben. Daher empfiehlt es sich, in eine zukunftsfähige Lösung zu investieren: Professionelle Konzepte, einfache Handhabung und zuverlässige Methoden lohnen sich.«

Christian Fritz - COO IKARUS Security Software

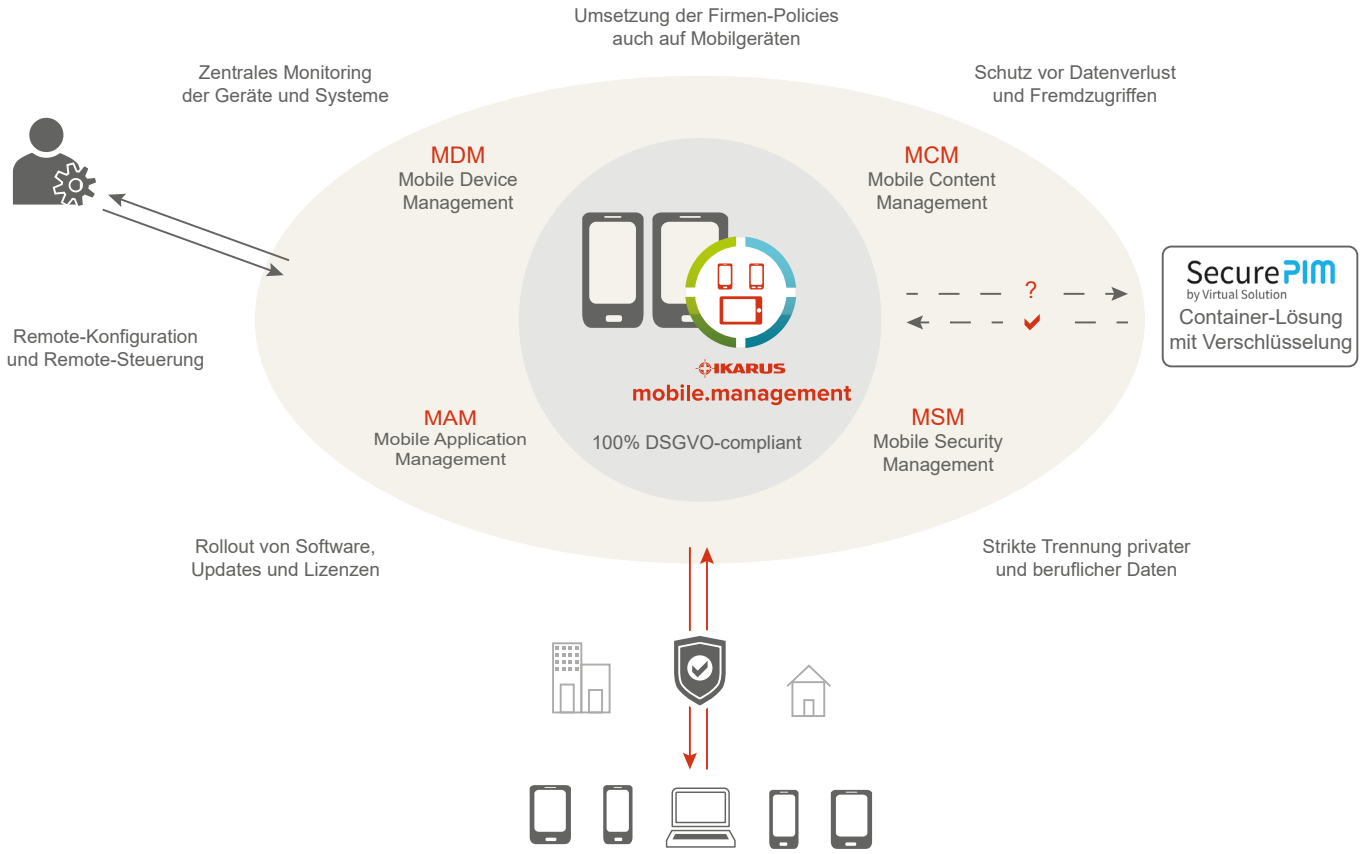

Abb. 2 - **IKARUS mobile.management** ermöglicht die zentrale Verwaltung, Sicherung und Steuerung mobiler Endgeräte und erfüllt alle Anforderungen der EU-DSGVO.

IKARUS mobile.management: TÜV Trusted App

Die MDM-Lösung **IKARUS mobile.management** ist das Ergebnis einer Entwicklungspartnerschaft von **SEVEN PRINCIPLES AG** und **IKARUS Security Software GmbH.**

7P ist der führende deutsche Hersteller von Enterprise-Mobility-Lösungen zur sicheren Verwaltung Ihrer Smartphones und Tablets.

IKARUS ist der führende österreichische Anbieter von IT-/OT-Sicherheitslösungen und entwickelt auf Basis der IKARUS scan.engine richtungsweisende Security-Technologien.

Gemeinsam bieten wir Ihnen mit **IKARUS mobile.management** eine Komplett-Lösung zur Optimierung und Sicherung Ihrer mobilen Kommunikation und Arbeitsprozesse. DSGVO-Compliance und TÜV-Zertifizierung inklusive.

TÜV TRUST IT
TRUSTED APP
TÜV AUSTRIA Group

- ✓ geprüfter Datenschutz
- ✓ geprüfte Datensicherheit
- ✓ geprüfte Schutzmechanismen

DSGVO-Compliance: Sicherheit und Datenschutz To-Go

Die Digitalisierung und Vernetzung unserer Kommunikationswege bringen nicht nur Vorteile, sondern bieten auch attraktive neue Angriffsflächen. Dem trägt die heuer in Kraft getretene EU-DSGVO Rechnung, indem sie von Unternehmen im Umgang mit persönlichen Daten (von EU-Bürger*innen) einiges verlangt – nach Artikel 5 (**„Grundsätze für die Verarbeitung personenbezogener Daten“**) sind dies beispielsweise:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

*Der Verantwortliche ist nach Artikel 5 Absatz 2 für die Einhaltung der genannten Grundsätze verantwortlich und muss deren Einhaltung nachweisen können (**„Rechenschaftspflicht“**).*

IT-Abteilungen stehen vor neuen Herausforderungen. Unternehmen müssen nach Artikel 32 (**„Sicherheit der Verarbeitung“**) nachweislich sicherstellen, dass auch an Mobilgeräten geeignete organisatorische und technische Sicherheitsvorgaben nach Stand der Technik eingehalten werden, unter anderem:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten
- Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Laptops, Smartphones oder Tablets müssen daher ab sofort verschlüsselt werden und es sind Backups zu erstellen. Es gibt zusätzliche Einfallstore, beispielsweise durch Berechtigungen am Gerät installierter Apps, abzusichern. Es dürfen nur entsprechend zertifizierte Apps installiert werden und im Zweifelsfall müssen alle Firmendaten via Fernzugriff gelöscht werden können. Private Daten und Apps sind von Unternehmensdaten zu trennen, beispielsweise mittels Container-Lösungen. Denn nur so können unerlaubte Datenzugriffe und unbefugte Offenlegung vollständig und nachweislich unterbunden werden. Zugleich können die Container die Verschlüsselung der Unternehmensdaten und der Kommunikation zwischen mobilem Endgerät und IT-Abteilung sicherstellen.

Alle Risiken und Sicherheitsvorkehrungen müssen zudem nach Artikel 35 (**„Datenschutz-Folgenabschätzung“**) bewertet und dokumentiert werden, und auch Artikel 32 Absatz 1d) fordert „Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“. Ohne Einsatz eines Mobile Device Management-Systems sind auch diese Anforderungen kaum zu erfüllen.

Mobile Devices: flexible Nutzung trotz strikter Vorgaben

Ein geeignetes MDM-System bietet auf einen Blick eine detaillierte Übersicht über Geräte mit Zugriff auf Unternehmensressourcen. Geräte und Applikationen können zentral verwaltet und inventarisiert werden. Auch die Softwareverteilung inklusive dem Ausrollen von Updates und Lizenzen sollte zentral steuerbar sein – selbstverständlich inklusive eines leistungsfähigen Malwareschutzes, Remote Control Features und automatischen Aktionen im Fall von Sicherheitsverletzungen.

Mobile Lösungen werden auch in Zukunft eine tragende Rolle in unserem privaten und beruflichen Leben spielen. Daher empfiehlt es sich, in eine zukunftsfähige Lösung zu investieren: Professionelle Konzepte, einfache Handhabung und zuverlässige Methoden lohnen sich. Nicht zuletzt in Anbetracht der empfindlichen Strafen im Falle einer Nicht-Compliance: Wer seine Datenschutzpflichten vernachlässigt, muss mit Strafgeldern von bis zu 20 Millionen Euro bzw. vier Prozent des weltweit erzielten Jahresumsatzes kalkulieren (Artikel 83 Absatz 5 „Allgemeine Bedingungen für die Verhängung von Geldbußen“).

Fragen?

Wir beraten Sie gerne! Kontaktieren Sie uns unter sales@ikarus.at oder Tel. +43 1 58995-500.