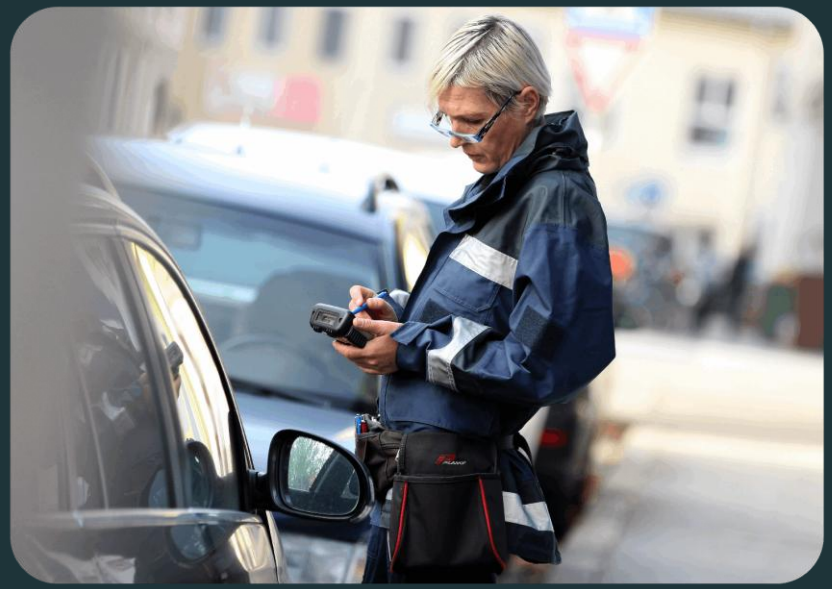
GEMA

Digitale Selbstbestimmung beginnt am Endgerät

Souveränes Device Management in der Praxis

Endgeräte bestimmen den Alltag im öffentlichen Sektor



Ein vereinheitlichtes Verwaltungs-system über alle Endgeräte und Betriebssysteme

2 Komponenten für behördliches Device Management

Wahrung des Datenschutzes; Compliance durch klare Zugriffs-rechte und souveräne Systeme

Digitale Souveränität

Bedeutet uneingeschränkte Kontrolle über alle Daten, Systeme und Betriebsprozesse, ohne Abhängigkeit von ausländischen Herstellern oder Dienstleistern

Diese Kontrolle beginnt unmittelbar an den Endpunkten der IT-Infrastruktur: den Endgeräten

3 zentrale Aspekte der Souveränität

Datensouveränität

- Datenhoheit ohne externe Abhängigkeiten
- Datensicherheit durch starke Identitätskontrollen und Ver-schlüsselungsmechanismen

Betriebssouveränität

- Schutz vor Abschaltung kritischer Komponenten
- Betrieb durch sicherheitsüberprüftes, zertifiziertes österreichisches & europäisches Personal

Technische Souveränität

- Physische Isolation der Hardware
- Besitz und Kontrolle der Technologien
- Nutzung eigener kryptographischer Schlüssel

Souveränität in Gefahr

CLOUD Act

Erlaubt US-Behörden Zugang zu Daten, die bei US-Dienstleistern gespeichert sind – unabhängig vom Speicherort

FISA (Foreign Intelligence Surveillance Act)

Nationale Sicherheit kann Zugriffsrechte auf Kommunikationsdaten gewähren

National Intelligence Law (Art. 7)

Verpflichtet chinesische Unternehmen zur Zusammenarbeit mit Geheimdiensten

Strafgerichtshof: Microsofts E-Mail-Sperre als Weckruf für digitale Souveränität

Microsoft hat nach Trump-Sanktionen das Mail-Konto des Chefanklägers des Internationalen Gerichtshofs blockiert. Kritiker: "Wir brauchen dringend Alternativen."

749

Eingriffe von außen sind Realität.

Strafgerichtshof: Microsofts E-Mail-Sperre als Weckruf für digitale Souveränität

Microsoft hat nach Trump-Sanktionen das Mail-Konto des Chefanklägers des Internationalen Gerichtshofs blockiert. Kritiker: "Wir brauchen dringend Alternativen."

749

Wie können wir uns schützen?

(und trotzdem moderne Software nutzen)

Architektur am Beispiel
Workspace ONE®

Device Management

User & Device Management wie gehabt
durch Kunde oder Service Partner

Unified Endpoint Management Software

Control Plane

Plattform-Betrieb durch lokalen, zertifizierten Anbieter, in Österreich durch GEMA Austria

Ohne Datenverbindung zum Hersteller

Infrastruktur exakt nach Herstellervorgaben

Im Rechenzentrum oder Bring Your Own Infrastructure

Sicherheitsmechanismen

Tenant Kontext:
Logische Trennung und sichere Isolation von Mandantendaten

Service-to-Service-Authentifizierung:
Sichere und verschlüsselte Kommunikation zwischen Diensten

Row-Level Security:
Granulare Zugriffsbeschränkungen auf Datenbankebene

Bring Your Own Key (BYOK):
Kunden behalten volle Kontrolle über die Verschlüsselung

Einige Vorteile von Omnissa™ Workspace ONE®

Desired State & Declarative Management

- Schnelle Verteilung und konsistente Umsetzung von Richtlinien auf Endgeräten durch Desired State & Declarative Management
- Überwachung und Durchsetzung von Sicherheits- und Compliance-Vorgaben mit Werkzeugen für Compliance & IT Policy Enforcement

Echtzeit-Monitoring

- Echtzeitüberwachung von Geräten und Anwendungen mit automatischer Erkennung von Compliance-Verstößen und dynamischer Anpassung von Richtlinien zur sofortigen Risikominimierung

Automatisierung komplexer Workflows

- Automatisierte Gerätebereitstellung und Konfiguration zur schnellen und konsistenten Inbetriebnahme neuer Endgeräte
- Orchestrierung von Sicherheits- und Compliance-Prüfungen sowie automatisches Reagieren auf Richtlinienverstöße

Sehr hohe Systemabdeckung und Verwaltung aller gängigen Endgeräteklassen

- Windows + Windows Server
- Apple inkl. DDM
- Android inkl. Management API
- Linux
- Rugged Devices, z.B. Zebra OTA

Michèl Bohlig
michel.bohlig@thegema.eu

Martin Cornelius
martin.cornelius@thegema.eu

Konrad Hannig
konrad.hannig@thegema.eu

GEMA Austria

- Spezialist für Device Lifecycle Management und Mobile Device Management Systeme
- Seit über 15 Jahren in Österreich tätig direkt vor Ort in Wien
- BBG gelistet
- C5 Testat nach BSI-Kriterienkatalog

thegema.at