VORTRAG

Anforderungen an ein IAM für kritische Infrastrukturen

Martin Kuppinger

Principal Analyst | KuppingerCole Analysts

Kritische Infrastrukturen im Fokus von Angreifern

Tatsächliche Angriffe und realistische Angriffsszenarien

Ransomware-Attacken

Der Cyberangriff auf die US-Pipeli Warnschuss für Deutschland

Onlinekriminelle haben die Betreiberfirma der größten US-Pipeline ang Folgen? Und wie bedrohlich ist Erpressersoftware für deutsche Firmer wichtigsten Fragen.

Von **Markus Böhm** und **Matthias Kremp**
10.05.2021, 15.41 Uhr

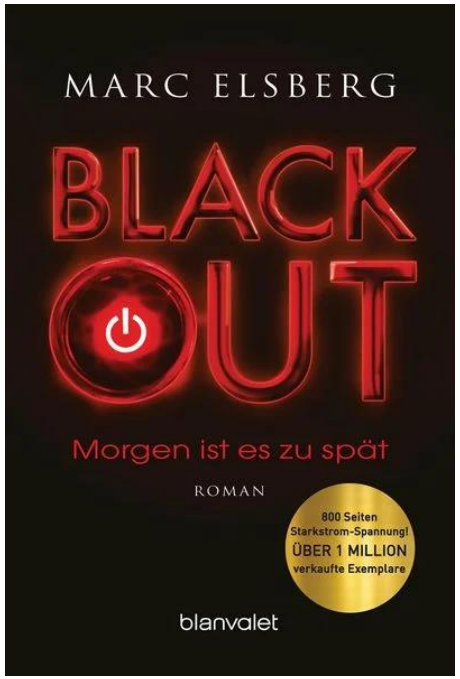
CYBERKRIMINALITÄT

Todesfall nach Hackerangriff auf Uni-Klinik Düsseldorf

Eine Patientin stirbt, nachdem ihr Rettungswagen wegen einer Cyberattacke umgeleitet werden musste. Der Fall illustriert die wachsenden IT-Risiken.

Christof Kerkmann Lars-Marten Nagel

18.09.2020 - 13:05 Uhr • Kommentieren • 14 x geteilt



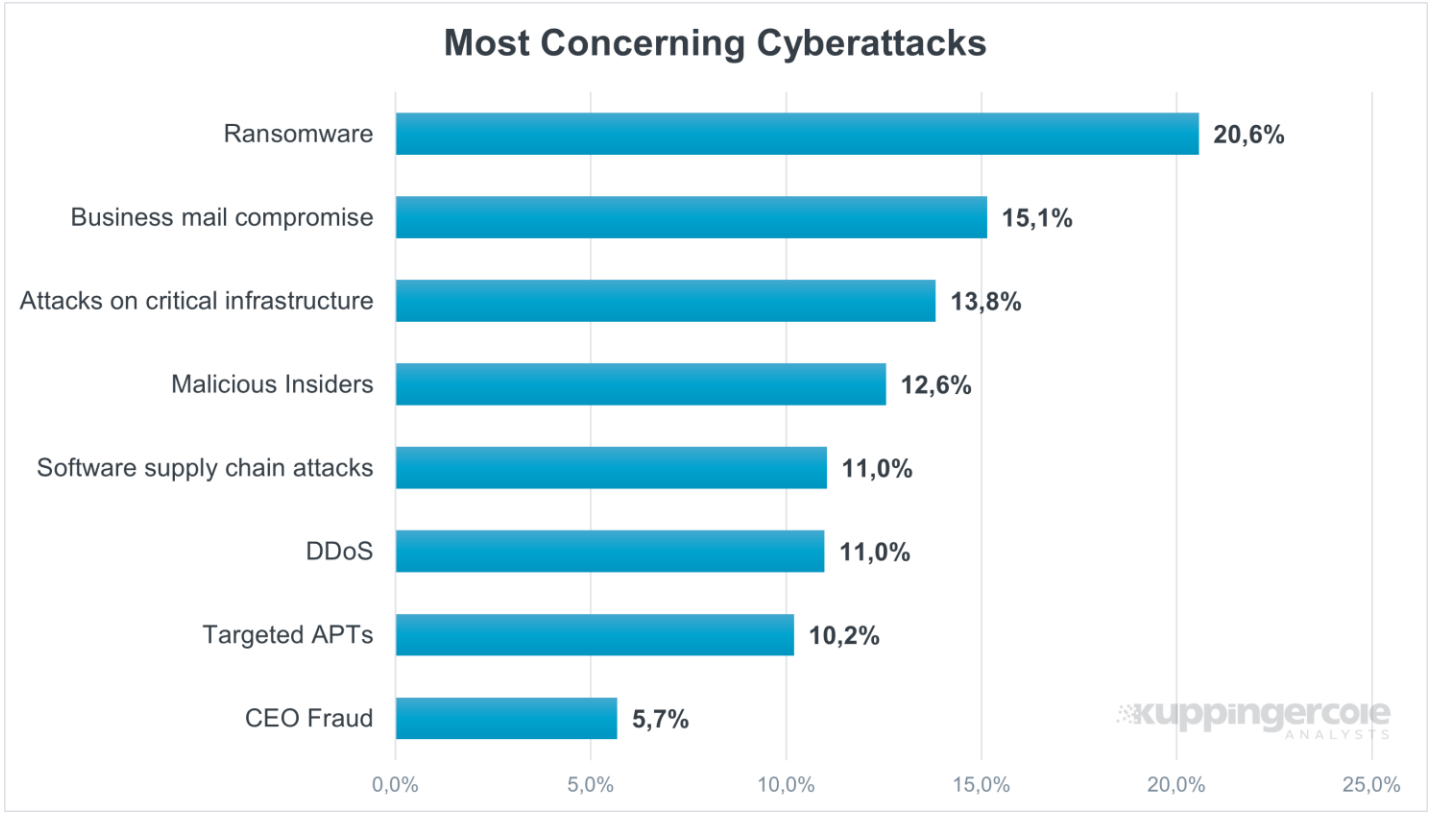
Die Zahlen sind deutlich: Identität als Angriffsvektor

Die meisten Cyberangriffe sind auf die eine oder andere Weise mit Identitäten verbunden

Beispiele:

- Phishing als initialer Angriffsvektor, um Anmeldeinformationen zu erhalten
- Interne Angreifer, die übermäßige Berechtigungen missbrauchen
- Advanced persistent threats (APTs), bei denen sich Angreifer immer mehr Rechte verschaffen und zu kritischen Systemen hinbewegen

Es geht immer um Identitäten und Berechtigungen. IAM ist essentiell für Cybersicherheit.



Identitätsbezogene Bedrohungsszenarien

Szenarien und Auslöser, die risikoerhöhend wirken

Privilegierte Benutzerkonten

- Dienstkonten
- Server-Administratoren
- Netzwerk-Administratoren
- Endgeräte-Administratoren
- Anwendungs-konten

Schlecht verwaltete Benutzerkonten

- Gruppenkonten
- Konten & Administratoren in der Schatten-IT
- Konten für Fernzugriffe
- Schwache Authentifizierung
- Überhöhte Berechtigungen
- Fehlendes Identity Lifecycle Management (verwaiste Benutzerkonten)
- Nicht verwaltete Legacy-Systeme und OT-Lösungen

Exponierte Anmeldedaten

- Dark Web
- Klartext-Kennwörter in Skripten und Dateien
- Tokens, Cookies, Hashes
- In-memory
- Unsichere, offene RDP-Sitzungen

Ungenügend geprüfte Identitäten

- Auftragnehmer
- Neue Mitarbeiter / BYOD (eigene Endgeräte)
- Zugriff von Partner und Lieferanten

Wie Identitäten von Angreifern genutzt werden

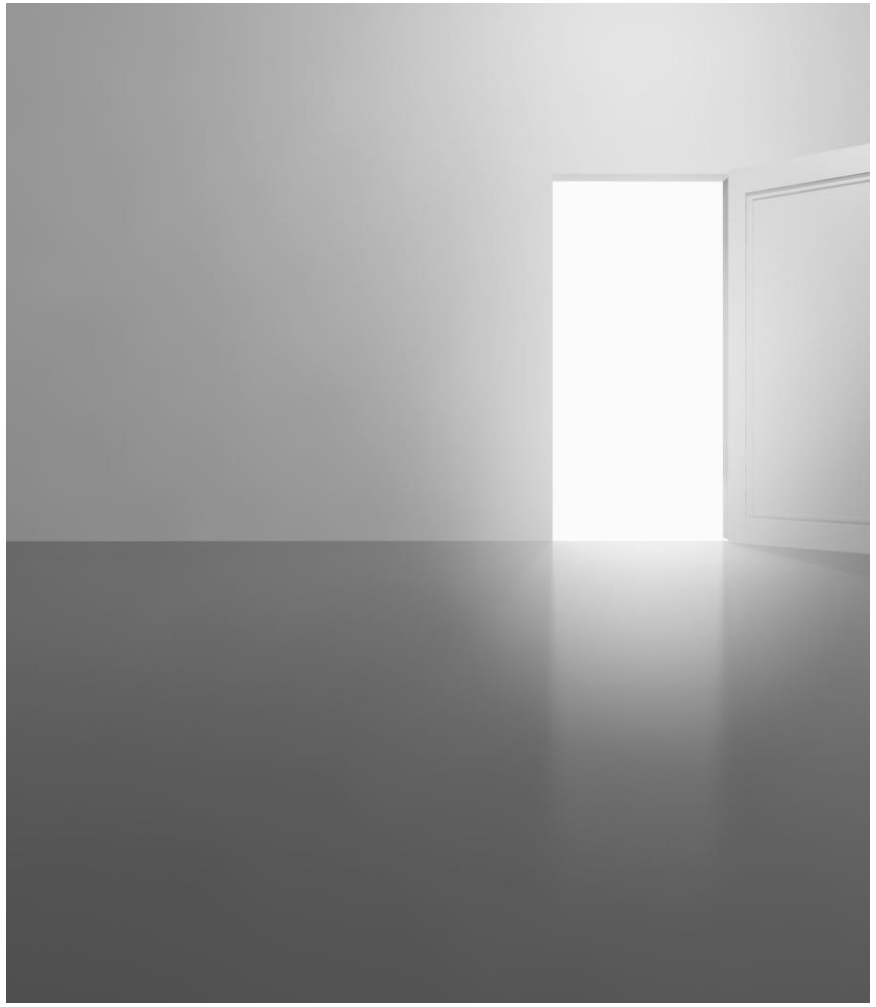
Identitäten sind ein Schlüsselfaktor für erfolgreiche Angriffe

Die meisten Cyberangriffe, Datenverluste und –diebstähle und Cybercrime-Vorfälle nutzen Schwächen im Umgang mit digitalen Identitäten.

Benutzernamen, Anmeldeinformationen, Tokens, Tickets, Hashes, Vertrauensbeziehungen etc., sogar MFA haben Schwachstellen, die von Angreifern gezielt ausgenutzt werden.

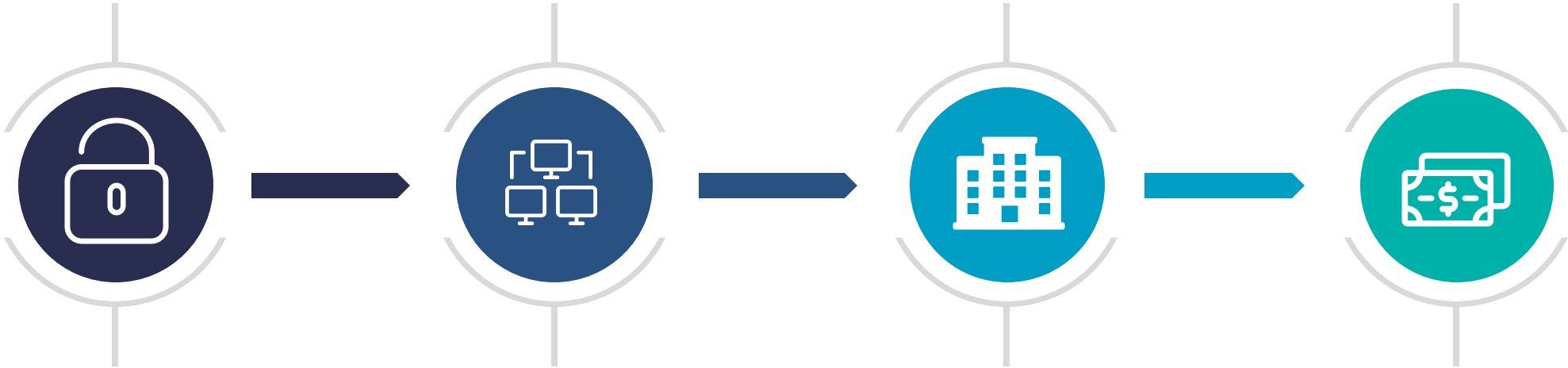
Angreifer haben viele Möglichkeiten, um an Anmeldeinformationen zu gelangen:

- Brute force
- Ausspähung
- Dark web
- Zwischensysteme
- Insider



Zugriffsrisiken sind Unternehmensrisiken

Das Management von Zugriffsrisiken ist essentiell für die Reduktion kritischer Unternehmensrisiken



ZUGRIFFSRISIKO

Missbräuchlicher Zugriff kann zu signifikanten finanziellen und regulatorischen Risiken ebenso wie Datenlecks führen.

IT-RISIKO

IT benötigt einen Ansatz, der alle IT-Risiken ganzheitlich betrachtet: Zugriffsrisiken, Cloud-Risiken, BCM etc.

BUSINESS-RISIKO

IT-Risiken haben einen Einfluss auf das Geschäft, z.B. Finanzen und Reputation. Sie müssen sichtbar gemacht werden.

KOSTEN

Zugriffsrisiken können den Erfolg eines Unternehmens und seinen Wert gefährden und bis hin zur Insolvenz führen.

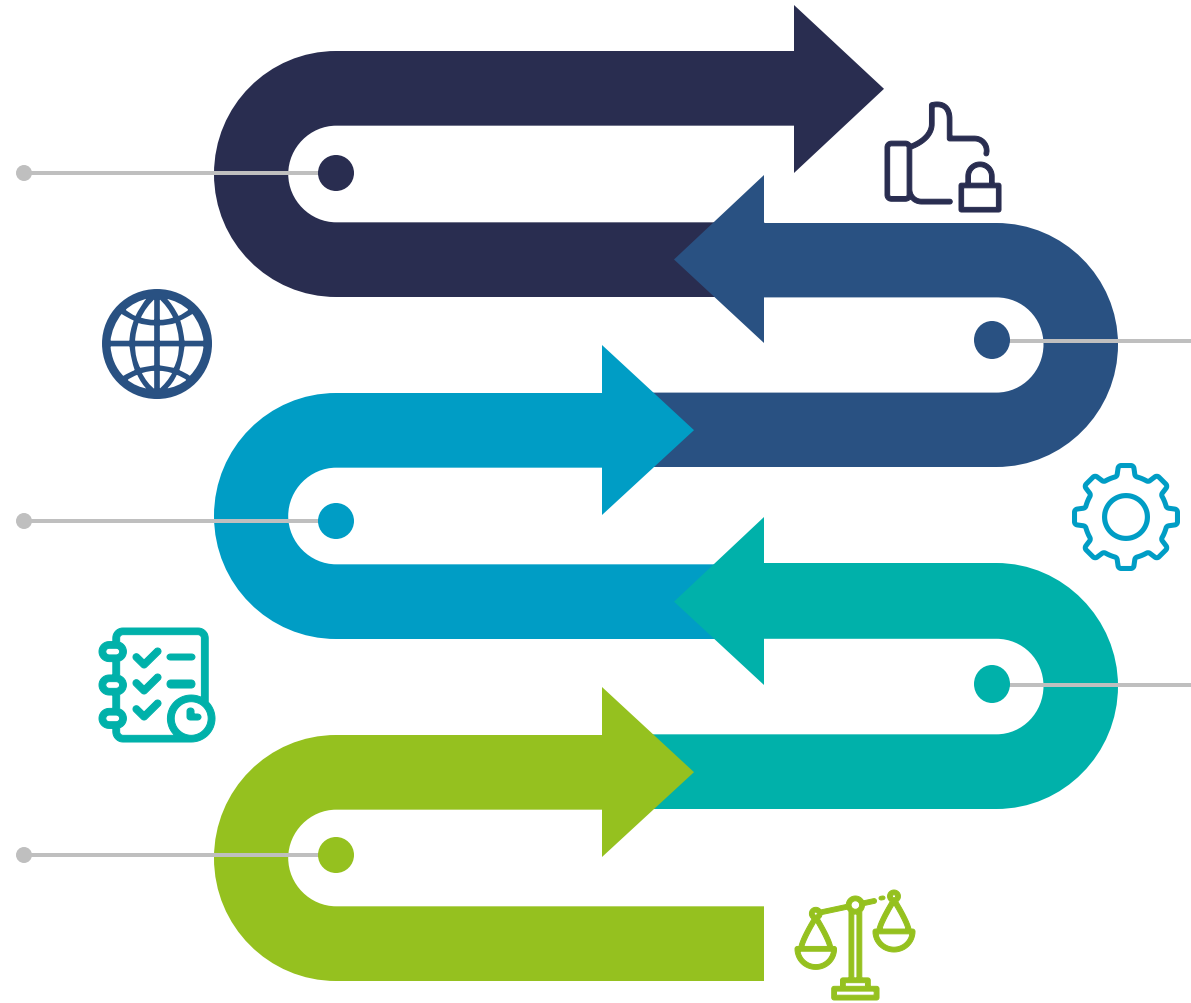
Compliance ≠ Audit ≠ Sicherheit

Es geht darum, die richtigen Maßnahmen zu ergreifen für mehr Sicherheit!

SICHERHEIT
Weder Compliance noch Audit führen zur Sicherheit – es sind die richtigen Maßnahmen.

MASSNAHMEN
Was wirklich gemacht wird, nicht was dem Auditor erzählt wird.

COMPLIANCE
Die Erfüllung von Gesetzen und Regularien.



GANZHEITLICHER ANSATZ
Compliance, Audit und Maßnahmen sind eng verbunden – sie müssen als Ganzes betrachtet werden.

AUDIT
Die Fähigkeit zu beweisen, dass man wirklich macht, was man behauptet zu tun.

Identity - Security

IAM schafft Sicherheit

Administrative Effizienz

Workflows, Automatisierung, Self Service

Management und Kontrolle

Einheitliche Administration aller Identitäten auf allen Systemen in der hybriden Realität der Digitalen Transformation

Sicherheit und Vertrauen

Absicherung der Identitäten, Zugänge und Berechtigungen mit starker Authentifizierung

Compliance und Governance

Wer hat auf was Zugriff, wer sollte Zugriff haben, und wie wird dieser Zugriff benutzt?

IAM muss sich weiterentwickeln: Neue Anforderungen

IAM muss liefern, von der Kostenoptimierung bis hin zur Unterstützung von Zukunftsthemen

IAM ist nicht statisch.

Anforderungen verändern sich.

Beispiele für veränderte Anforderungen:

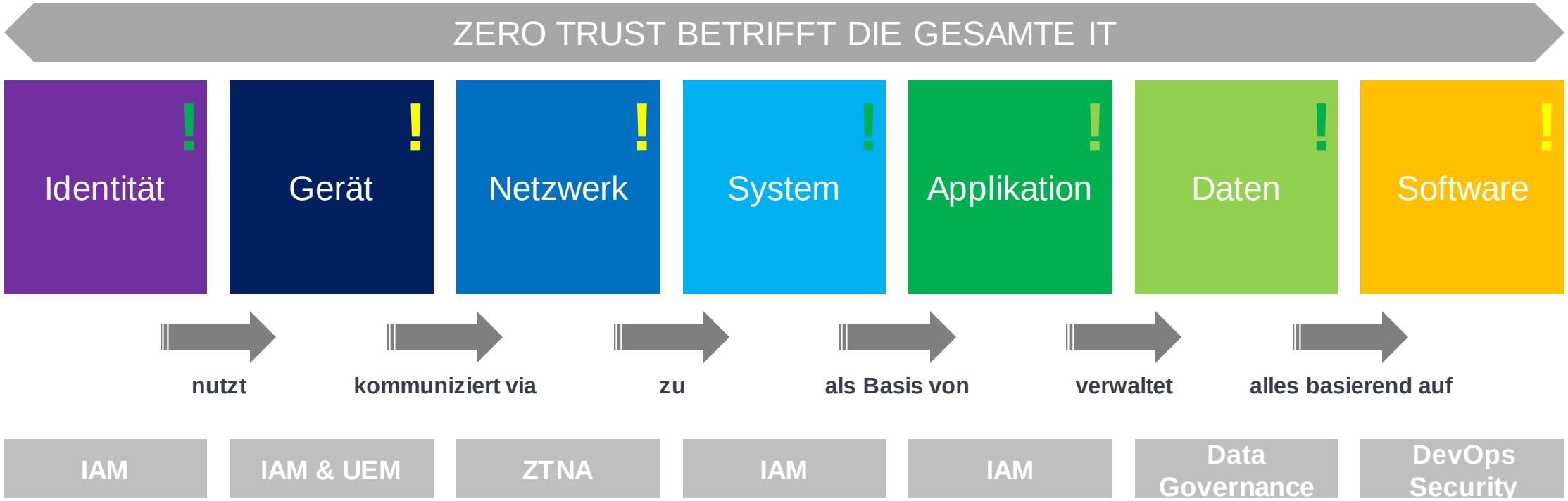
- Work from anywhere
- Cloud
- Digitale Dienste und die Notwendigkeit, die Identitäten von Kunden und Dingen zu unterstützen

Neue Herausforderungen am Horizont:

- Web3
- Metaverse
- Dezentrale Technologien/Identitäten

Warum Identity Security für Zero Trust?

Identity Security ist der zentrale Baustein für Zero Trust.



IAM: Identity & Access Management
UEM: Unified Endpoint Management
ZTNA: Zero Trust Network Access

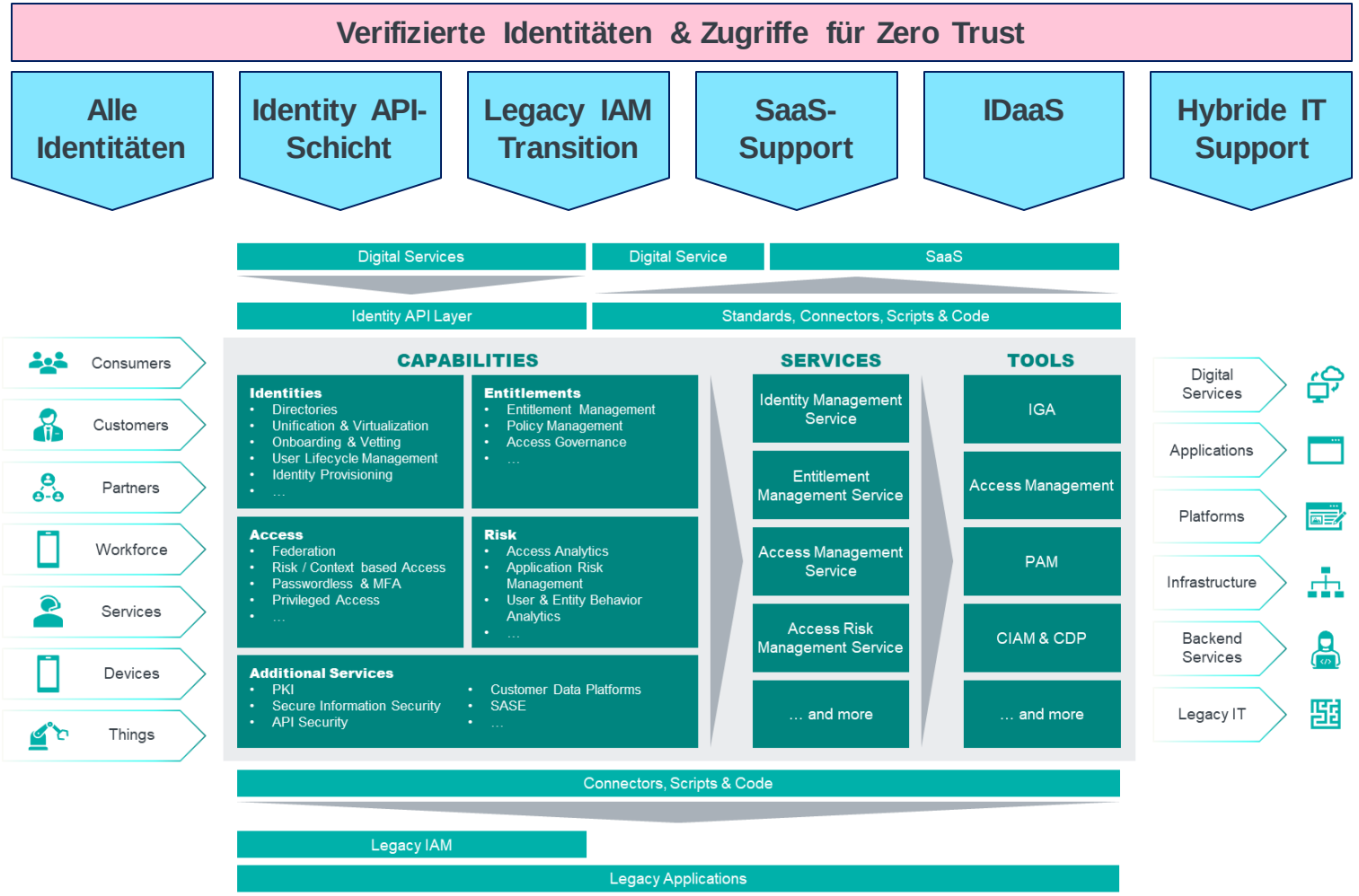
IAM weiterentwickeln, Zero Trust unterstützen, IDaaS

IAM ist nicht statisch, sondern entwächst dem traditionellen Mitarbeiterfokus: Identity Fabrics

Identity Fabrics sind ein grundlegendes Paradigma: Eine integrierte Sicht über alle Bereiche von IAM, mit denen reibungsloser, aber dennoch sicherer Zugriff von allen Identitäten auf alle Ressourcen und Dienste bereitgestellt wird. Modular, flexibel, adaptiv.

- Unterstützung aller Identitäten: Menschen, Dinge, Geräte.
- Unterstützung für die Verwaltung von Diensten und die Bereitstellung von Diensten: Identity API-Schicht.
- Einbindung und Erweiterung des Legacy-IAM für eine reibungslose Transition.
- Unterstützung von modernen SaaS- (und IaaS/PaaS-) Infrastrukturen.
- Bereitstellung als SaaS-Dienst.
- Gebaut für die hybride Realität der heutigen IT-Infrastrukturen.

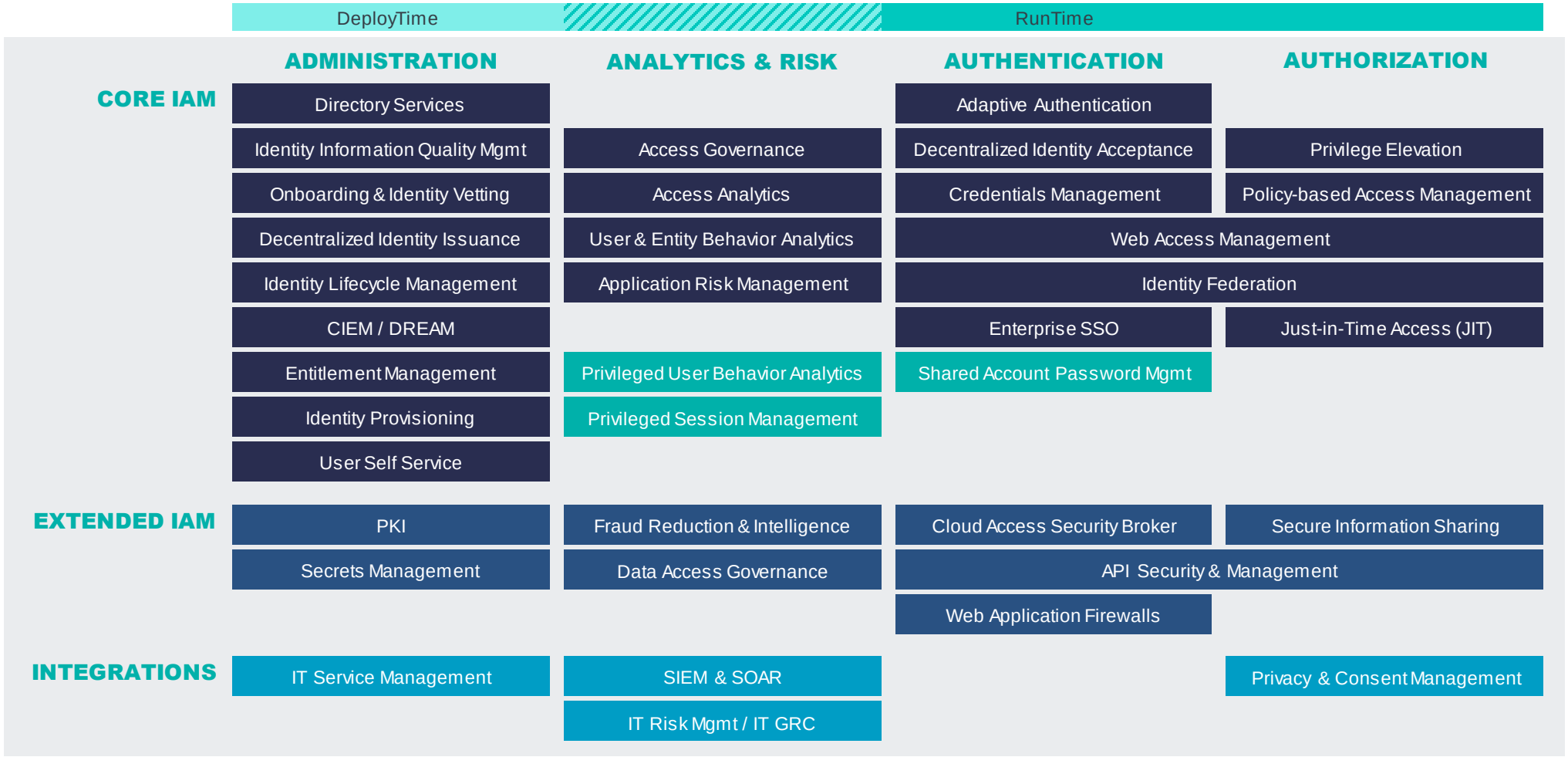
Kernbaustein von Zero Trust: Verifizierte Identitäten.



KuppingerCole Identity Fabrics Model

Identity & Access Management ist mehr als nur IGA

KuppingerCole IAM Reference Architecture: Kernbausteine für IAM



Funktionale Anforderungen: 20 Kernfunktionen

Kritische Infrastrukturen brauchen ein gutes IAM – und mehr

Funktionale Breite	Authentifizierungs-funktionen	Benutzer-provisionierung	Identity Lifecycle Management (ILM)	Repository/Directory	Directory-Synchronisation
Zentrale administrative UI	Benutzer-Self-Service	Granulare Autorisierung	Access Governance	Berechtigungs-anforderung	Access Analytics
AI-/ML-basierte Analysten	Review/ Rezertifizierung	Unterstützung hybrider Zielsysteme	API-Unterstützung	Standardprotokoll-unterstützung	Reports
		Dashboards	OT-Unterstützung (Operational Technology)		

Herausforderung Betriebsmodell

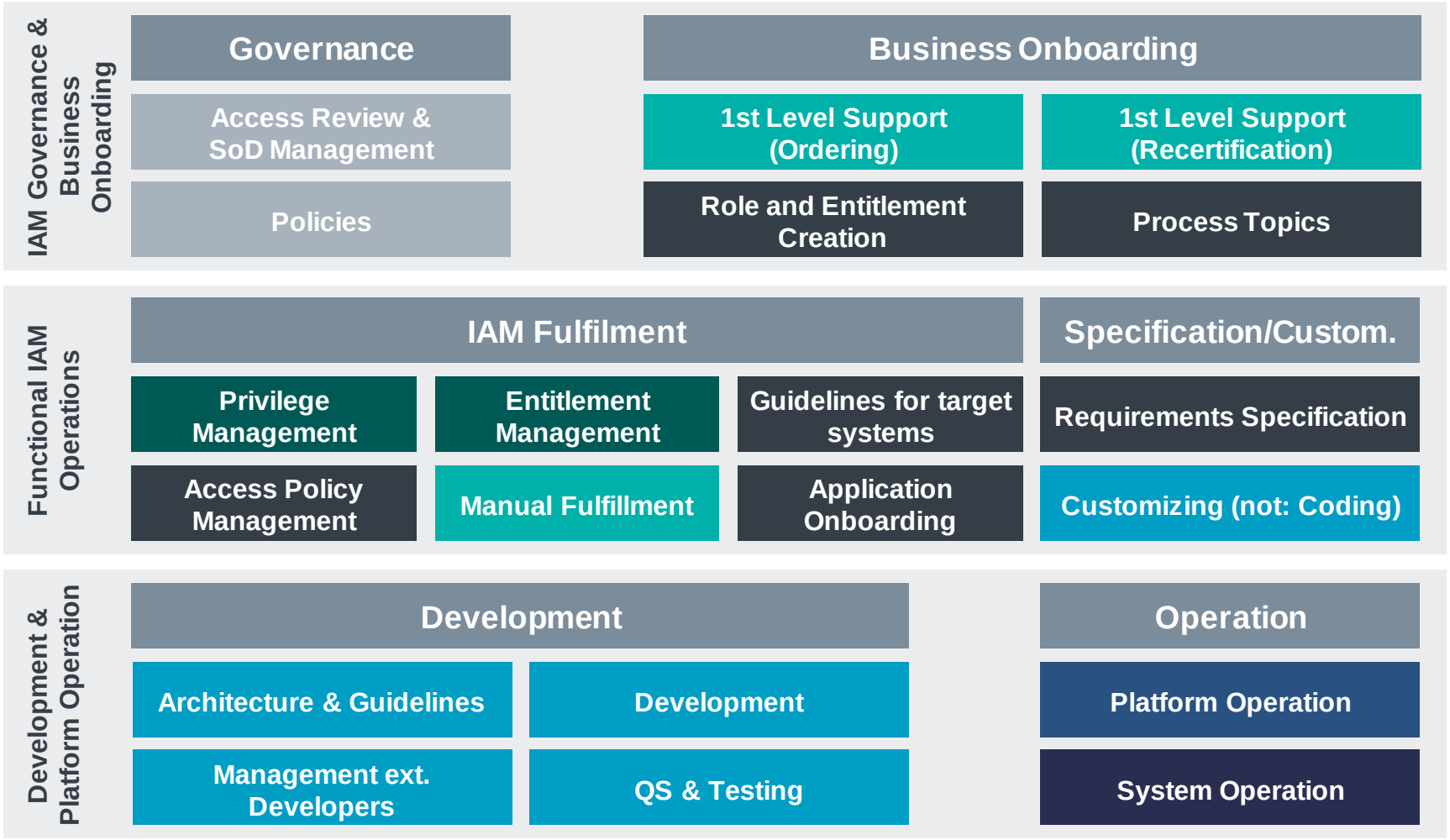
Kritische Infrastrukturen haben spezielle Anforderungen

Wo kann der Dienst laufen?

- On premises mit/ohne managed service
- As-a-service (regional) mit/ohne managed service

IAM braucht eine definierte Organisation

Target Operating Model (TOM): Organisation und Zuständigkeiten, intern und für Provider



Legende

Funktionale Target Operating Model (TOM) Kategorien

- Governance
- Process & Policy
- Operational Provisioning
- Support + Manual Fulfilment
- Development
- Platform Operation
- System Operation

10 häufige Stolpersteine in IAM-Projekten

Die Bereiche, auf die man achten sollte, um ein IAM-Projekt erfolgreich umzusetzen

Schlüsselfaktoren für den Erfolg von IAM-Projekten

Viele Faktoren bestimmen den Erfolg von IAM-Projekten

DANKE!

Fragen?

Bei Fragen können Sie sich jederzeit an mich wenden (mk@kuppingercole.com)!

KuppingerCole Analysts AG
Wilhelmstr. 20 - 22
65185 Wiesbaden | GERMANY

P: +49 | 211 - 23 70 77 - 0
F: +49 | 211 - 23 70 77 – 11

E: info@kuppingercole.com
www.kuppingercole.com