VISION consulting

ZERO TRUST

Der 5-Schritte-Plan mit Architektur-Artefakten nach TOGAF, Künstlicher Intelligenz und ITIL-Prozessen der VISION Consulting GmbH

Enterprise Architect: M.Sc. Sebastian Kämper

Zero Trust – die Grundlagen

Die zunehmende Digitalisierung und die damit einhergehenden Cyberbedrohungen stellen die Öffentliche Verwaltung vor erhebliche Herausforderungen. Traditionelle Sicherheitsansätze wie IT-Grundschutz, die auf Vertrauen in interne Netzwerke setzen, erweisen sich gegenüber modernen, durch künstliche Intelligenz unterstützten Angriffsmethoden als unzureichend. Der Zero-Trust-Ansatz bietet hier eine zeitgemäße Lösung, indem er das Prinzip verfolgt, keinem Nutzer oder Gerät standardmäßig zu vertrauen, unabhängig von dessen Standort innerhalb oder außerhalb des Netzwerks. So weit, so klar.

Das eigentliche Thema ist der sehr zögerliche Umgang mit modernen Frameworks oder Technologien. Daher beleuchtet dieser Artikel die Grundlagen von Zero Trust, die Beiträge von NIST, Forrester und CISA zu diesem Thema und präsentiert den 5-Schritte-Plan der VISION Consulting zur Implementierung einer Zero-Trust-Architektur in der Öffentlichen Verwaltung. Zudem wird die Bedeutung von Sicherheits-Frameworks wie der MITRE ATT&CK Matrix sowie der Einsatz von Künstlicher Intelligenz (KI) bei der Entwicklung von Sicherheitsrichtlinien und der Identifizierung von IT-Schwachstellen diskutiert. Bei der Einführung einer Zero-Trust-Architektur sollte die Organisation bestenfalls ein etabliertes Enterprise Architecture Management (EAM) betreiben, um bei der Erhebung der Assets nicht bei Null anzufangen. Warum?

Grundlagen des Zero-Trust-Ansatzes

Zero Trust hat eine definierte Architektur, bestehend aus fünf Rollen, die im Zusammenspiel Ihre Sicherheit gewährleisten. Der Policy Enforcement Point (PEP) hat die Aufgabe, Zugriffe eines Subjekts (z. B. Antragsteller) auf eine Ressource (z. B. Online-Dienst) festzustellen. Er leitet jeden identifizierten Zugriffsversuch an den Policy Decision Point (PDP) weiter, welcher über ein definiertes Set an Regeln über den Zugriffsversuch entscheidet. Hierzu werden Informationen benötigt, welche durch den PDP bei sogenannten Policy Information Points (PIP) abgefragt werden (z. B. bei einem Servicekonto). Dieses Zusammenspiel wird durch den Policy Administration Point (PAP) konfiguriert. Verschiedene Technologien stehen bereit, die Aufgaben dieser Rollen zu übernehmen. Um Zero-Trust-Architekturen einzuführen, benötigen Sie einen EAM-Ansatz im Haus, da Bedrohungen heutzutage über ein Werkzeug gemeinsam strukturiert, gepflegt und modelliert werden. Die Bedrohungsmodellierung ersetzt meterlange, konjunktive Betrachtungen in Sicherheitskonzepten mit fingierten Situationen, die ein Risiko darstellen könnten.

Denn Zero Trust basiert auf dem Grundsatz „Vertraue niemandem, überprüfe alles". Das bedeutet, dass weder internen noch externen Entitäten ohne vorherige Verifizierung Zugriff gewährt wird. Jede Anfrage wird unabhängig von ihrer Herkunft geprüft und der Zugriff nur auf Basis strenger Authentifizierungs- und Autorisierungsmechanismen gewährt. Dieses Paradigma stellt einen Paradigmenwechsel gegenüber traditionellen Sicherheitsmodellen dar, die oft davon ausgehen, dass alles innerhalb des Netzwerks vertrauenswürdig ist.

Das National Institute of Standards and Technology (NIST) hat mit der Veröffentlichung der Special Publication 800-207 "Zero Trust Architecture" einen umfassenden Leitfaden zur Implementierung von Zero-Trust-Prinzipien bereitgestellt. Dieses Dokument definiert Zero Trust als eine Reihe von sich entwickelnden Cybersicherheitsparadigmen, die Verteidigungsstrategien von statischen, netzwerkbasierten Perimetern hin zu einem Fokus auf Benutzer:innen, Assets und Ressourcen verlagern.

Forrester Research hat das Zero Trust eXtended (ZTX) Ecosystem entwickelt, das über die reine Netzwerksegmentierung hinausgeht und Bereiche wie Workforce Security, Device Security, Workload Security, Network Security, Data Security, Visibility and Analytics sowie Automation and Orchestration umfasst. Dieses erweiterte Modell betont die Notwendigkeit einer ganzheitlichen Sicherheitsstrategie, die alle Aspekte der IT-Infrastruktur berücksichtigt.

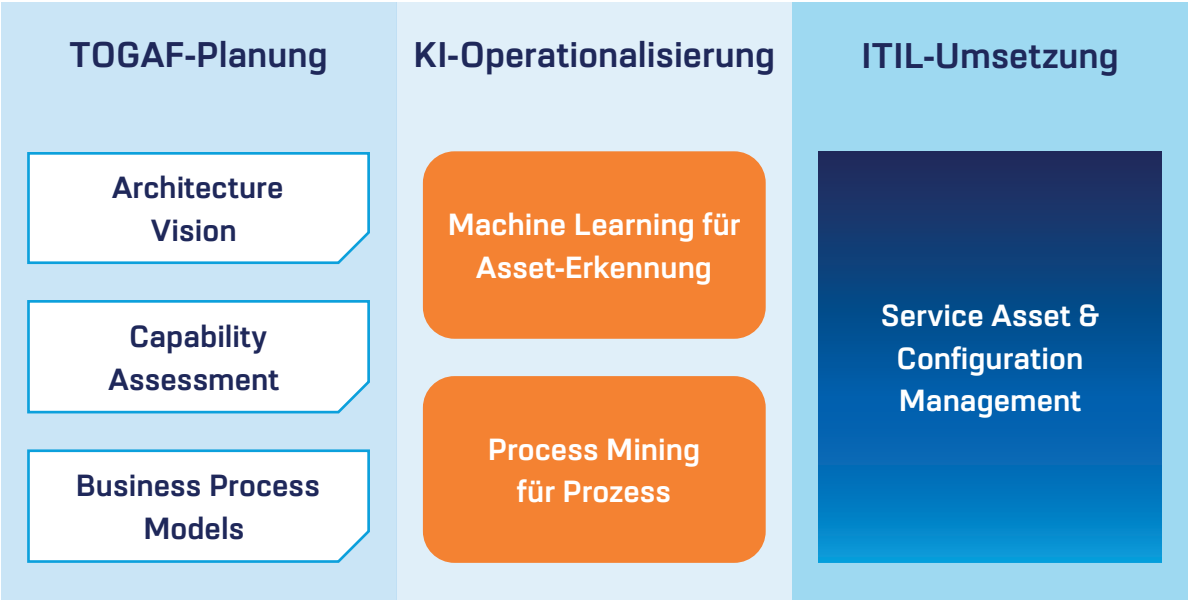
Die Cybersecurity and Infrastructure Security Agency (CISA) hat das Zero Trust Maturity Model (ZTMM) entwickelt, das Organisationen dabei unterstützt, ihre Zero-Trust-Strategien zu entwickeln und umzusetzen. Das Modell umfasst fünf Säulen: Identität, Geräte, Netzwerk, Anwendungen und Workloads sowie Daten. Es bietet einen Reifegradansatz, der es Organisationen ermöglicht, stetige Fortschritte bei der Implementierung von Zero-Trust-Maßnahmen zu erzielen.

Auf Basis eines EAM-Ansatzes nach TOGAF wird die neue Zero-Trust-Architektur geplant und in den Betrieb überführt. Die neuen Zero-Trust-Rollen und deren Zusammenspiel beeinflussen die ITIL-Prozesse, die den Betrieb der Dienste sicherstellen. Um die wissensintensiven Prozesse der Inventur sowie Aktualisierung der Daten, Systeme und Prozesse zu gewährleisten, werden KI-Technologien eingesetzt. In den folgenden fünf Schritten wird dargestellt, wie die Einführung, einer Zero-Trust-Architektur methodisch und technologisch unterstützt werden kann, um diese erfolgreich abzuschließen.

5-Schritte-Plan mit Architektur-Artefakten nach TOGAF, Künstlicher Intelligenz und ITIL-Prozessen

1. Bestandsaufnahme und Risikobewertung

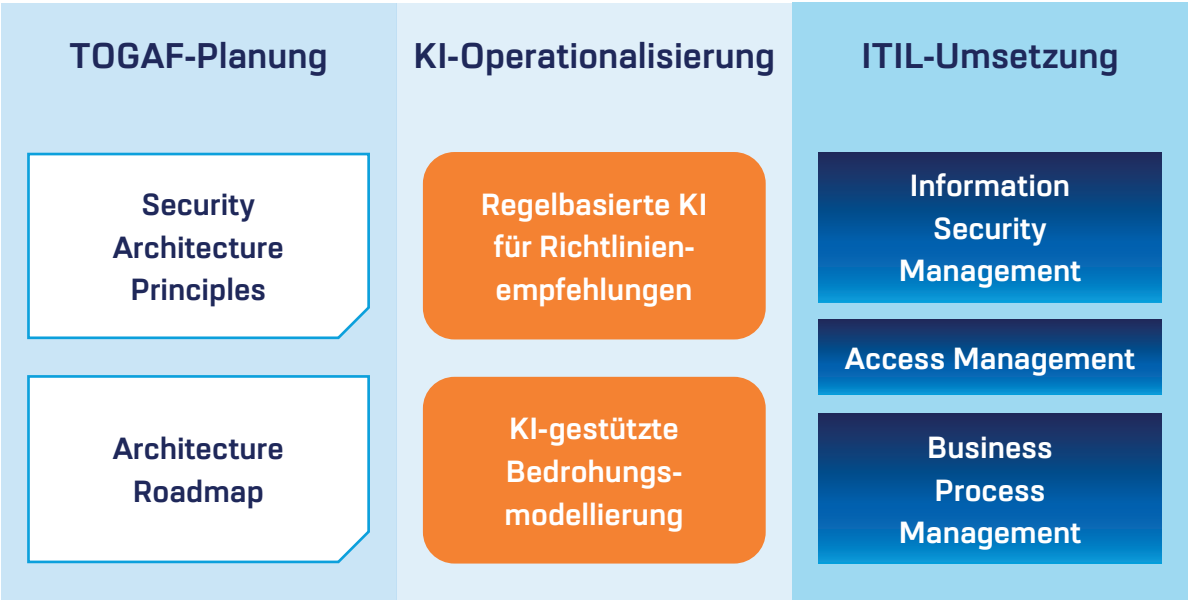
Zu Beginn sollte eine umfassende Bestandsaufnahme aller IT-Ressourcen, einschließlich Benutzer, Geräte, Anwendungen und Daten durchgeführt werden. Ebenso wichtig ist die Analyse der bestehenden Geschäfts- und IT-Prozesse, um potenzielle Schwachstellen in Abläufen zu ermitteln. KI-gestützte Systeme helfen dabei, Assets automatisch zu identifizieren und zu kategorisieren. Prozess-Mining-Technologien analysieren Arbeitsabläufe und erkennen ineffiziente oder unsichere Prozesse, während NLP eingesetzt wird, um bestehende Sicherheitsrichtlinien und Dokumentationen zu analysieren.



Die strukturierte Vorgehensweise

2. Definition von Sicherheitsrichtlinien und -kontrollen

Basierend auf den Ergebnissen der Bestandsaufnahme sollten klare Sicherheitsrichtlinien entwickelt werden, die den Zugriff auf Ressourcen streng regeln. Neben der technischen Sicht müssen auch prozessuale Schwachstellen adressiert werden. KI kann hier auf Basis bekannter Bedrohungsmuster automatisierte Richtlinienvorschläge generieren. Bedrohungsmodellierungs-KI unterstützt bei der Vorhersage möglicher Angriffswege und hilft, präventive Maßnahmen zu definieren.



3. Implementierung von Überwachungs- und Analysemechanismen

Die kontinuierliche Überwachung des Netzwerkverkehrs und der Benutzeraktivitäten ist unerlässlich, um Anomalien frühzeitig zu erkennen. Dabei sollten auch Prozessabweichungen betrachtet werden, da verdächtige Aktivitäten oft durch unerwartete Verhaltensänderungen sichtbar werden. Machine-Learning-Modelle analysieren Datenströme in Echtzeit und identifizieren verdächtige Aktivitäten. KI-gestützte SIEM-Systeme (Security Information and Event Management) helfen bei der automatischen Korrelation von Bedrohungsinformationen.

4. Segmentierung des Netzwerks und Schutz der Workloads

Die Netzwerksegmentierung reduziert die Angriffsfläche, indem sie das Netzwerk in kleinere, isolierte Abschnitte unterteilt. Neben technischer Segmentierung ist es essenziell, auch Arbeitsabläufe so zu strukturieren, dass sensible Prozesse voneinander getrennt bleiben. KI kann hier eingesetzt werden, um Zugriffsregeln dynamisch anzupassen und sich verändernde Bedrohungslagen in Echtzeit zu berücksichtigen. Automatisierte KI-Systeme können Workloads basierend auf deren Risikoprofil optimal absichern.

5. Kontinuierliche Verbesserung und Anpassung

Da sich Bedrohungslandschaften ständig weiterentwickeln, ist es wichtig, die Zero-Trust-Strategie regelmäßig zu überprüfen und anzupassen. Predictive Analytics hilft dabei, neue Bedrohungen frühzeitig zu erkennen, während KI-gesteuerte Automatisierung für regelmäßige Systemaktualisierungen und Compliance-Überprüfungen sorgt. Durch den Einsatz von KI-gestütztem Process Mining können ineffiziente oder riskante Prozesse kontinuierlich verbessert werden.

Fazit

Die Implementierung einer Zero-Trust-Architektur erfordert eine strukturierte Vorgehensweise. Die Kombination von TOGAF, KI-Technologien und ITIL-Prozessen ermöglicht eine effiziente und nachhaltige Sicherheitsstrategie, die sowohl technische als auch organisatorische Risiken berücksichtigt.

Bedeutung von Sicherheits-Frameworks wie der MITRE ATT&CK Matrix

Die MITRE ATT&CK Matrix ist ein wertvolles Framework, das bekannte Taktiken, Techniken und Verfahren (TTPs) von Angreifern dokumentiert. Sie dient als Referenz für die Identifizierung von Bedrohungen und die Entwicklung von Abwehrstrategien. In einer Zero-Trust-Umgebung kann dieses Framework genutzt werden, um Angriffsvektoren zu analysieren und Sicherheitsrichtlinien entsprechend anzupassen. Durch den Abgleich von Netzwerkaktivitäten mit den in der MITRE ATT&CK Matrix dokumentierten Angriffstechniken können Sicherheitsverantwortliche Bedrohungen frühzeitig erkennen und darauf reagieren.

Ein konkretes Beispiel ist die Erkennung von anomalen Benutzeraktivitäten: Wenn ein legitimer Benutzer plötzlich auf Daten zugreifen möchte, die außerhalb seines normalen Verhaltensmusters liegen, kann ein Zero-Trust-System dies mit Hilfe der MITRE ATT&CK Matrix als potenzielle Bedrohung einstufen und entsprechende Gegenmaßnahmen einleiten. Das Metamodell der Mitre Attack Matrix wurde in das Architekturwerkzeug integriert und konnte folgendermaßen genutzt werden:

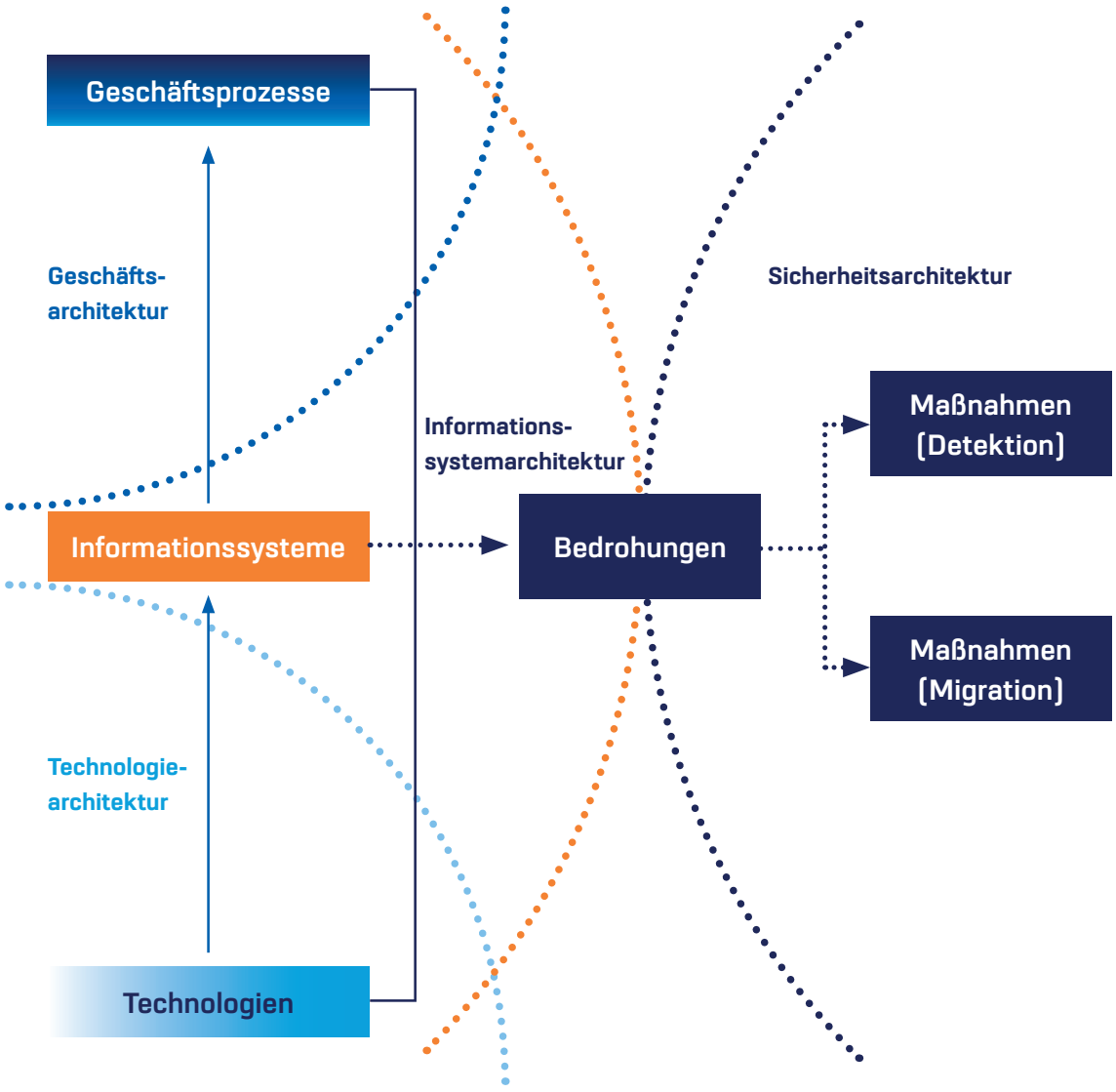


Abbildung 1: Metamodell Bedrohungsmodellierung

Der Vorteil der Bedrohungsmodellierung ist die schnelle Verfügbarkeit von Informationen. Der IT-Architekt wählt z. B. während der Konzeption die Technologien aus, benötigt jedoch nicht Kenntnis über die Risiken. Die Zuordnung, welche Technologie welcher Bedrohung ausgesetzt ist, ist Aufgabe des Sicherheitsarchitekten. Sind die Risiken gut gepflegt, können direkt im Anschluss an die Informationssystemarchitektur diejenigen Maßnahmen dargestellt werden, die zur Mitigation der bekannten Risiken nötig sind.

Vorteile von Künstlicher Intelligenz bei der Entwicklung von Sicherheitsrichtlinien

Um diese Zuordnungen auf dem neuesten Stand zu halten, können KI-Technologien dazu dienen, „Inventuren" durchzuführen, um Abläufe, Systeme und Technologien zu erfassen. Durch selbstlernende Mechanismen werden neue Beziehungen zwischen diesen Elementen identifiziert. Das Sprachmodell findet sich in der Architektur wieder. Daher spielt Künstliche Intelligenz (KI) eine immer wichtigere Rolle in der Cybersicherheit. In einer Zero-Trust-Architektur kann KI genutzt werden, um Sicherheitsrichtlinien dynamisch anzupassen, Bedrohungen zu erkennen und automatisierte Reaktionsmaßnahmen einzuleiten.

Ein zentraler Vorteil von KI ist die Möglichkeit, riesige Mengen an Sicherheitsdaten in Echtzeit zu analysieren. Machine-Learning-Modelle können Muster identifizieren, die auf böswillige Aktivitäten hindeuten, und Sicherheitsrichtlinien daraufhin automatisch anpassen. So können Organisationen schneller auf neue Bedrohungen reagieren, ohne dass manuelle Eingriffe erforderlich sind.

Beispielsweise kann KI erkennen, wenn ein Benutzerkonto kompromittiert wurde, indem es Login-Zeiten, Standortdaten und das Geräteprofil analysiert. Falls eine Unregelmäßigkeit festgestellt wird, kann das System automatisch die Zugriffsbeschränkungen verschärfen oder eine Multi-Faktor-Authentifizierung anfordern.

KI zur Entdeckung von IT-Schwachstellen

Neben der dynamischen Anpassung von Sicherheitsrichtlinien kann KI auch zur Identifizierung von IT-Schwachstellen eingesetzt werden. Herkömmliche Schwachstellen-Scans sind oft zeitaufwändig und erfassen nicht immer alle potenziellen Einfallstore. KI-gestützte Systeme können kontinuierlich Netzwerk- und Systemdaten analysieren, um Angriffsflächen frühzeitig zu identifizieren und zu beheben.

Ein praktisches Beispiel ist der Einsatz von KI in der sogenannten Threat Intelligence: Hierbei werden Bedrohungsdaten aus verschiedenen Quellen analysiert, um potenzielle Sicherheitslücken zu identifizieren. KI kann zudem simulierte Angriffe durchführen (automatisierte Penetrationstests), um zu testen, wie widerstandsfähig ein Netzwerk gegen bestimmte Angriffsmethoden ist.

Zusätzlich kann KI dazu beitragen, Zero-Day-Schwachstellen zu identifizieren, also Sicherheitslücken, die bisher noch nicht bekannt sind. Durch die Analyse von Benutzerverhalten, Netzwerkverkehr und Systemprotokollen kann KI Anomalien erkennen, die auf eine bislang unbekannte Schwachstelle hindeuten. Dies ermöglicht eine frühzeitige Absicherung, bevor Angreifer die Schwachstelle ausnutzen können.

Die effiziente Sicherheitsstrategie für Ihre Verwaltung

Fazit

Die Implementierung einer Zero-Trust-Architektur in der Öffentlichen Verwaltung ist ein komplexer, aber notwendiger Schritt zur Stärkung der Cybersicherheit, die eine strukturierte Vorgehensweise erfordert. Die Kombination von TOGAF, KI-Technologien und ITIL-Prozessen ermöglicht eine effiziente und nachhaltige Sicherheitsstrategie, die sowohl technische als auch organisatorische Risiken berücksichtigt.

Durch die Kombination eines Enterprise-Architecture-Management-Ansatzes zur Dokumentation und Analyse der Sicherheitsarchitektur, dem Einsatz von KI, um Geschwindigkeit zu gewinnen und der parallelen Implementierung in das Service Management kann die Einführung von Zero-Trust-Architekturen nachhaltig werden. Frameworks wie die MITRE ATT&CK Matrix unterstützen die Identifizierung von Bedrohungen und Angriffstechniken, während Künstliche Intelligenz eine entscheidende Rolle bei der dynamischen Anpassung von Sicherheitsrichtlinien und der Entdeckung von IT-Schwachstellen spielt.

Mit einem strukturierten 5-Schritte-Plan, der von der Bestandsaufnahme über die Definition von Sicherheitsrichtlinien bis hin zur kontinuierlichen Verbesserung reicht, wird die Öffentliche Verwaltung – gern auch gemeinsam mit der VISION Consulting – Zero-Trust-Architekturen erfolgreich umsetzen. Die Integration von KI und modernen Sicherheitsframeworks stellt sicher, dass sich die Verteidigungsmechanismen stetig an neue Bedrohungen anpassen können und eine resiliente IT-Sicherheitsstrategie entsteht.

Haben wir Ihr Interesse geweckt? Dann erweitern Sie Ihre Enterprise-Architektur um eine neue Organisationseinheit: VISION Consulting!

Ihr Enterprise Architect:
M.Sc. Sebastian Kämper

VISION Consulting GmbH
Telefon (+49) 30 206067-30
vertrieb@visionconsulting.de
www.visionconsulting.de