Security by Default - Sind vollständig integrierte Sicherheitsarchitekturen Ihr Trauma oder Ihr Traum?

Andreas Schindler, Director Market Unit Cybersecurity & Compliance

HERZLICHEN DANK,
dass Sie dabei sind!

Referent

Andreas Schindler
Director & Executive Cloud Architect
Market Unit Cybersecurity & Compliance

All for One Group SE
Rita-Maiburg-Straße 40
70794 Filderstadt-Bernhausen
all-for-one.com

andreas.schindler@all-for-one.com

Moderator

Michael Bauer
Transformation Architect

All for One Group SE
Rita-Maiburg-Straße 40
70794 Filderstadt-Bernhausen
all-for-one.com

T: +49 211 550 26 315
M: +49 151 571 68 636
E: michael.bauer@all-for-one.com

Kurzvorstellung

Thementag 1
Cybersecurity & Compliance

- Während der Präsentation sind die Mikrofone stumm geschaltet
- Bitte stellen Sie Ihre Fragen im Chat, die Fragen werden am Ende der Session beantwortet
- Nach dem Vortrag auf der Bühne besteht die Möglichkeit sich mit dem Experten auszutauschen – siehe *Meet the Expert*
- Gerne bieten wir Ihnen auch individuelle Folgegespräche an

Cybersecurity & Compliance

Unser Werteversprechen

„Wir befreien Unternehmen in einer digitalen, vernetzten Welt von der Sorge um Cyberangriffe und Datenverlust und unterstützen bei der Einhaltung von Compliance-Anforderungen."

Unsere Leistungen

- Ganzheitliche Sicherheit über alle Ebenen einer Unternehmensorganisation
- Trusted Security Partner für Governance & Technologie sowie Single-Point of Contact
- Beratung und Implementierung moderner Cloud-First und Cybersecurity-Design-Grundlagen

Technologische Partner

ConSecur [security and consulting]
gemalto a Thales company
Lookout
Omada DO MORE WITH IDENTITY
ITing quality
SEC Consult
SECUDE

Strategische Partner

Microsoft
SAP

In Zeiten fortschreitender **Digitalisierung** verlagert sich die Wertschöpfung in Unternehmen weiter in den virtuellen Raum – damit wird das Thema **IT-Sicherheit** zugleich immer bedeutender.
Die Relevanz von IT-Risiken steigt für Unternehmen jeder Größenordnung und unabhängig vom Geschäftsmodell.

… daher ist es Ihre erste Pflicht, sich um ein funktionierendes IT-Risiko- und Sicherheitsmanagement zu kümmern. Nicht nur, weil Sie damit die Zukunftsfähigkeit Ihres Unternehmens sichern, sondern auch weil Sie damit beweisen, dass Sie Ihrer **Sorgfaltspflicht** als Geschäftsleiter nachkommen.
Hierfür ist die Geschäftsleitung verantwortlich, da sie laut Aktiengesetz und GmbH-Gesetz den Fortbestand des Unternehmens zu sichern hat.

Art. 5 DSGVO Dieser schreibt vor, dass personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen. Des Weiteren legt Art. 5 DSGVO dem Verantwortlichen die Pflicht auf, die Einhaltung dieser Vorgabe nachweisen zu können (sog. **Rechenschaftspflicht**). Art. 24 DSGVO spricht explizit von der Erfordernis technischer und organisatorischer Maßnahmen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung personenbezogener Daten gemäß der DSGVO erfolgt.

Prägende Cyberangriffe 2019 – Bundeslagebild 2019

JAN

Ein Tochterunternehmen der deutschen Kreditbank (DKB) wird von einem **DDoS**-Angriff getroffen – die Online-Dienste sind zeitweise nicht mehr verfügbar.

FEB

Kunden verschiedener Banken werden Opfer von SIM-Swapping[3] und anschließendem TAN-Abfang.

MRZ

Die **Ransomware** *LockerGoga* befällt den Internationalen Industriekonzern NorskHydro. *GandCrab* erpresst mehrere Unternehmen in Deutschland

APR

Verschiedene DAX-Unternehmen sollen mit Hilfe der **Malware** *Winnti* ausspioniert worden sein.

MAI

Ein Eine Welle der **Malware** *Emotet* trifft u.a. diverse Finanzämter.

JUN

Die IT-Systeme des internationalen Forensik-Dienstleisters Eurofins werden durch eine **Ransomware** verschlüsselt. Partner von Eurofins beenden daraufhin die Kooperation.

JUL

Die **Ransomware** *Sodinokibi* infiziert mehrere Einrichtungen des Deutschen Roten Kreuzes.

AUG

Die **Ransomware** *GermanWiper* verbreitet sich im Inland. Selbst nach Zahlung des Lösegeldes bleiben die verschlüsselten Daten unbrauchbar.

SEP

Die Systeme der Rheinmetall-Automotive-Gruppe werden mit **Malware** infiziert.

OKT

Während die **Malware** *Emotet* die Arbeit des Kammergerichts Berlin massiv beeinträchtigt, verschlüsselt eine **Ransomware** die Systeme der Universität Regensburg.

NOV

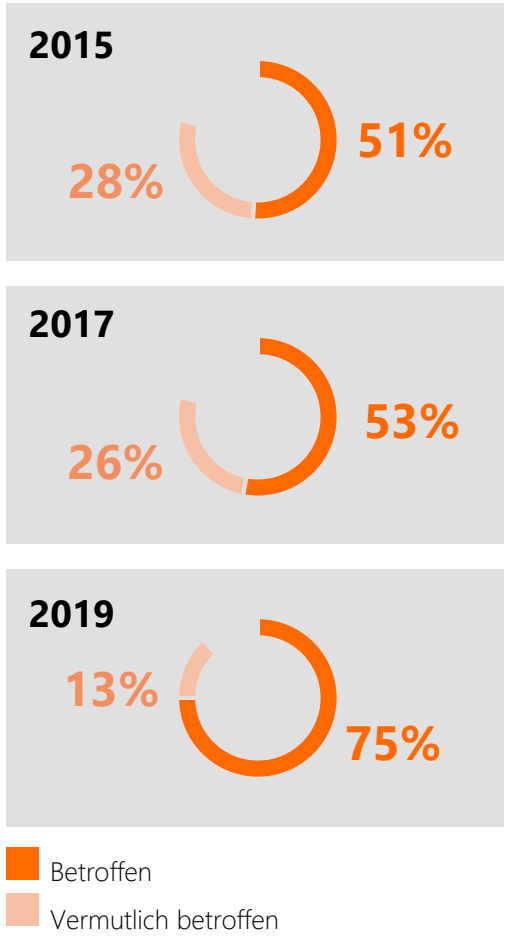
Die Pilz GmbH wird gezwungen, ihren Betrieb zeitweise einzustellen. Anlass ist eine **Ransomware**.

DEZ

Zum Jahresende tritt wieder verstärkt *Emotet* auf: Sowohl das Klinikum Fürth, die Stadt Frankfurt/Main als auch die Stadt Homburg werden von dem Trojaner infiziert. Zudem wird die Universität Gießen Opfer eines **Ransomware**-Angriffs.

Autor: Bundeskriminalamt

Prägende Cyberangriffe 2019 – Bundeslagebild 2019



Autor: Bundeskriminalamt

Diebstahl digitaler Identitäten

- „Handelsware der Underground Economy
- Jede gestohlene digitale Identität ist Nährboden für weitere kriminelle Aktivitäten.

Malware

- *Emotet* bleibt größte Malware-Bedrohung – v.a. im Verbund mit *TrickBot* und *Ryuk*
- Anzahl der Malware-Familien steigt stetig an
- Professionelles Crypting, das die Malware gegenüber AV-Scannern unsichtbar werden lässt

Ransomware

- Die primäre, existenzielle Bedrohung für Unternehmen
- Systeme werden nicht mehr nur verschlüsselt – Akteure drohen mit der Veröffentlichung der kryptierten Daten.

DDoS

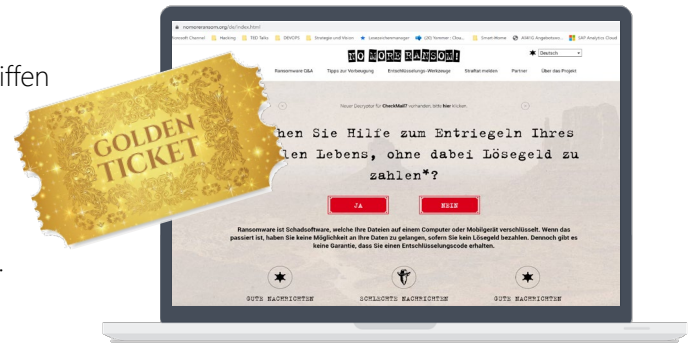
- Sowohl Quantität als auch Qualität steigend
- Vermehrter Nutzen von IoT und Clouds zur Verstärkung von DDoS-Angriffen

Underground Economy

- Arbeitsteilige, hochspezialisierte Wirtschaft
- Basiert auf neun Säulen – jede mit ihrem eigenen Fachgebiet
- Jede Säule sorgt für den reibungslosen Ablauf von kriminellen Aktivitäten.

Angriffe auf Unternehmen

- APT-ähnliches Verhalten durch kriminelle Organisationen
- Schaden durch z.B. einen Ransomware-Angriff liegt im mind. 6-stelligen Bereich

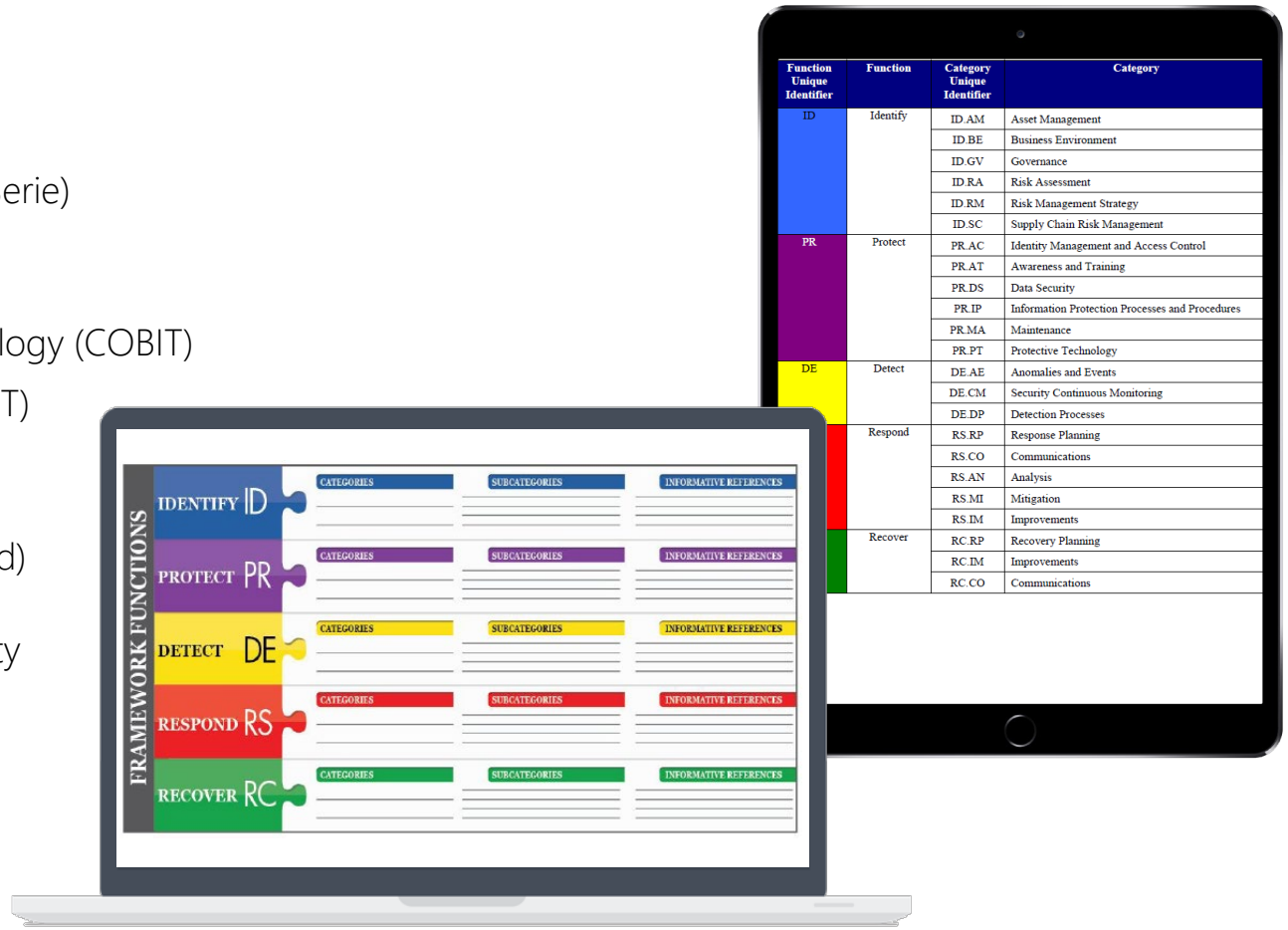


www.nomoreransom.org

WIE entwickelt man eine vollständig integrierte Sicherheitsarchitektur?

IT-Sicherheits-Frameworks

- IT-Grundschutz/Grundschutzkataloge des BSI
- International Standards Organisation (ISO/IEC-27000-Serie)
- Sarbanes-Oxley Act (SOA)
- Control Objectives for Information and Related Technology (COBIT)
- US National Institute of Standards and Technology (NIST)
- CIS Critical Security Controls
- PCI DSS (Payment Card Industry Data Security Standard)
- IEC 62443 internationale Normenreihe für Cybersecurity in der Industrieautomatisierung

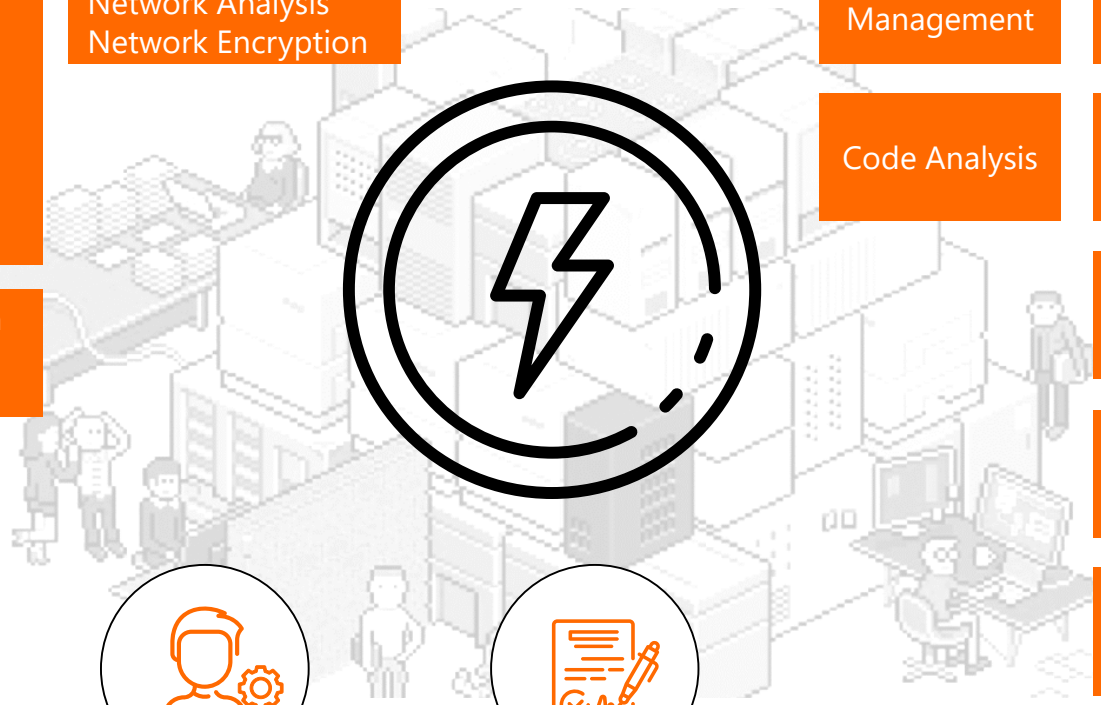


Dezentral + viele Lösungen + keine übergeordnete Steuerung = „Flickenteppich“

Firewalls
Client Firewall
Server Firewalls
Intrusion Detection
Reverse Proxy
DNS Security
E-Mail Security
Internet-Proxy

NAC-Systems
Network Analysis
Network Encryption

Malware Protection
Drive Encryption
System Encryption



Certificate Management
Code Analysis

Access Management
Web Application Firewall
Log Analytics
Multi-Factor-Authentication
Data Classification
Role Based Access Management
IoT Security
Privileged Access Management
Data Encryption
Container Security

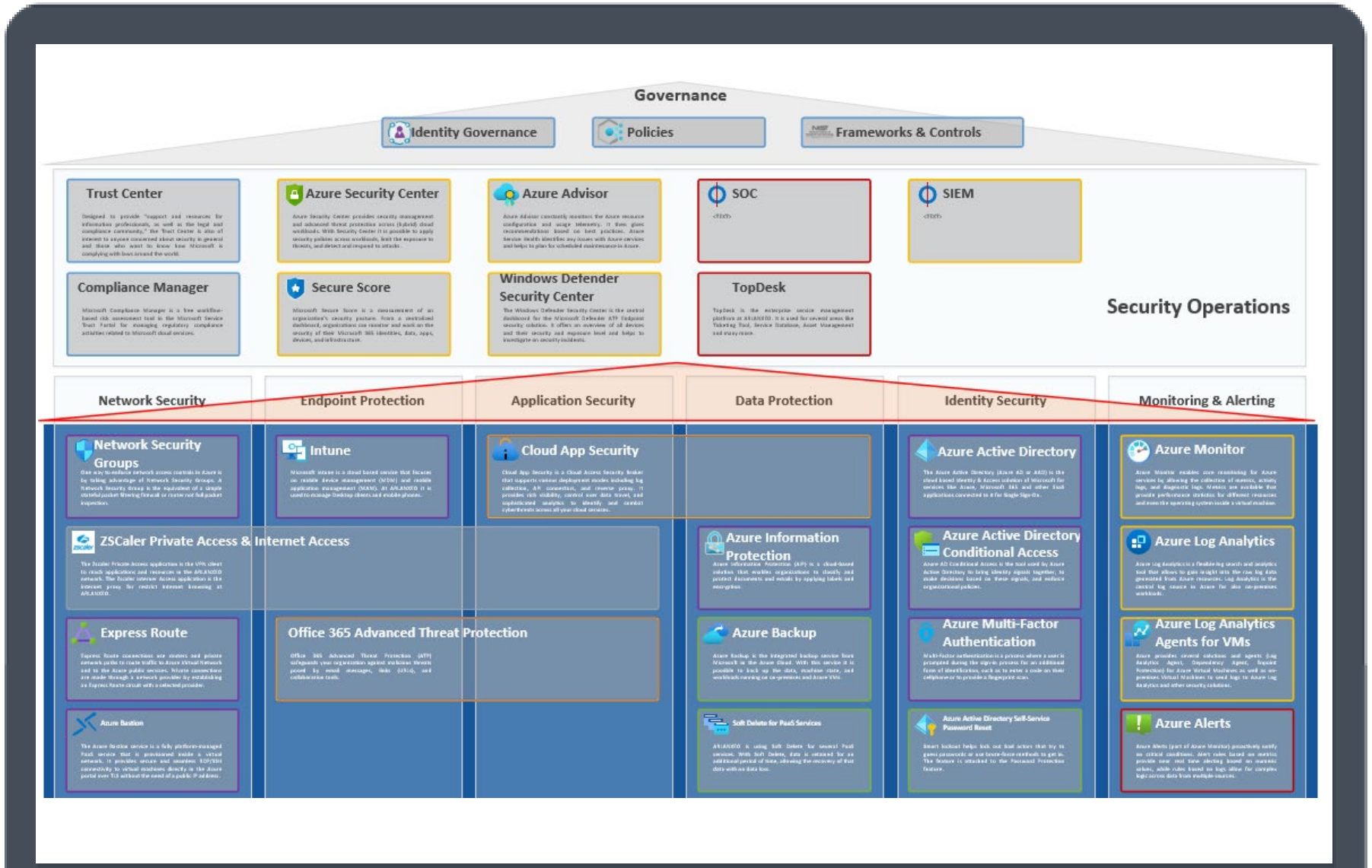
SAP Cloud Connector
Web Application Gateway

Data Management Gateway
Tenant-Security
SIEM
Zone Model
Identity Management
CASB (Cloud Access Security Broker)

Unternehmensweite Nutzung und Integration

Administrations-aufwendungen

Vertragsmanagement und Kosten


Governance
Identity Governance
Policies
Frameworks & Controls
Trust Center
Azure Security Center
Azure Advisor
SOC
SIEM
Compliance Manager
Secure Score
Windows Defender Security Center
TopDesk
Security Operations
Network Security
Endpoint Protection
Application Security
Data Protection
Identity Security
Monitoring & Alerting
Network Security Groups
Intune
Cloud App Security
Azure Active Directory
Azure Monitor
ZSCaler Private Access & Internet Access
Azure Information Protection
Azure Active Directory Conditional Access
Azure Log Analytics
Express Route
Office 365 Advanced Threat Protection
Azure Backup
Azure Multi-Factor Authentication
Azure Log Analytics Agents for VMs
Azure Bastion
Soft Delete for PaaS Services
Azure Active Directory Self-Service Password Reset
Azure Alerts

ZERO Trust Sicherheitsmodell

Legacy:

Daten und Systeme sind sicher solange sie sich innerhalb des Unternehmensnetzwerkes befinden.

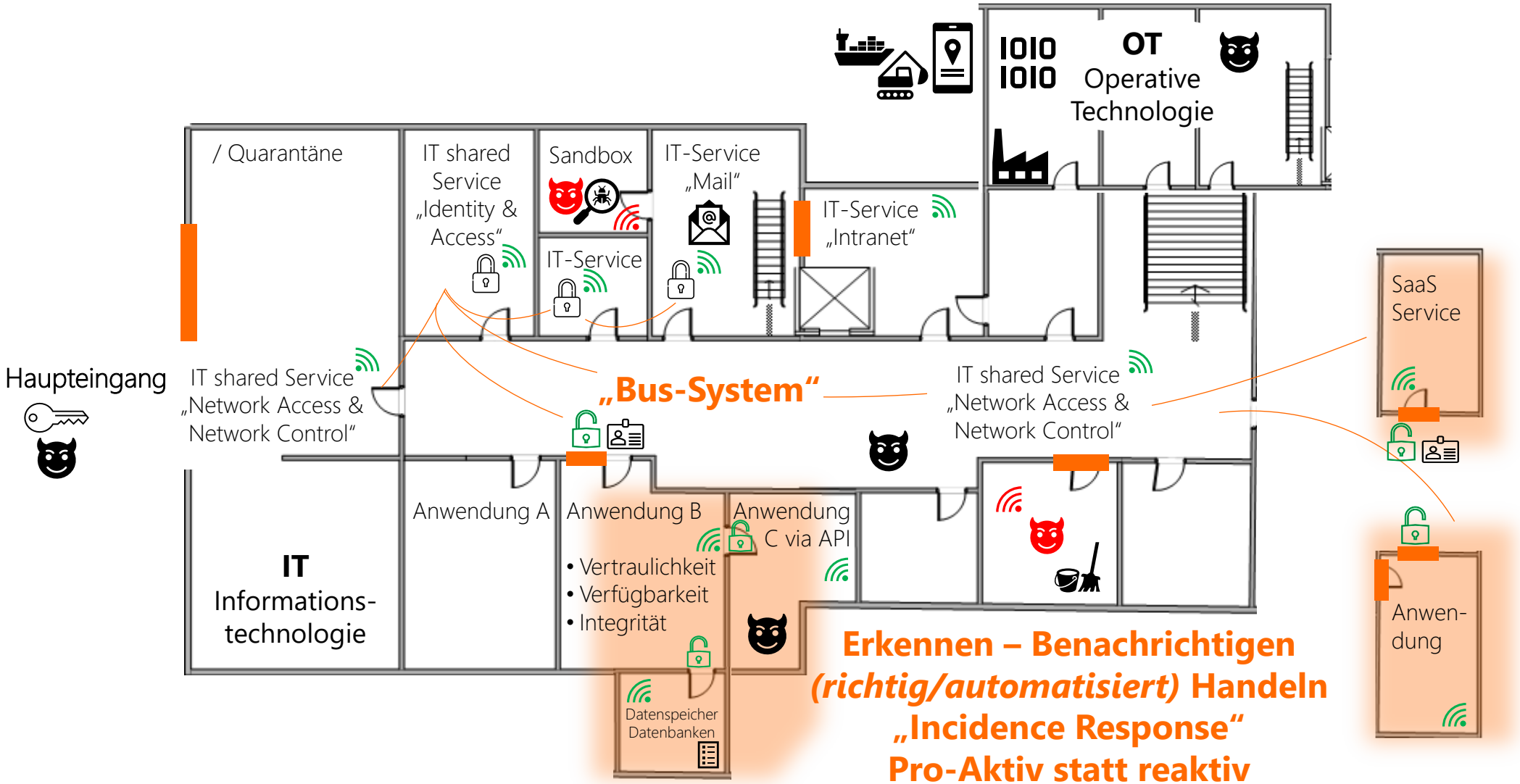
„Blindes" Vertrauen innerhalb des Unternehmensnetzwerkes. Externe Zugänge via VPN.

Heute/Morgen:

Das „Böse" wird generell überall vermutet.

Es wird kein Unterschied zwischen Diensten, Anwendern und Geräten innerhalb oder außerhalb des eigenen Netzwerks gemacht. Sämtlicher Verkehr muss geprüft werden und alle Anwender oder Dienste müssen sich authentifizieren.

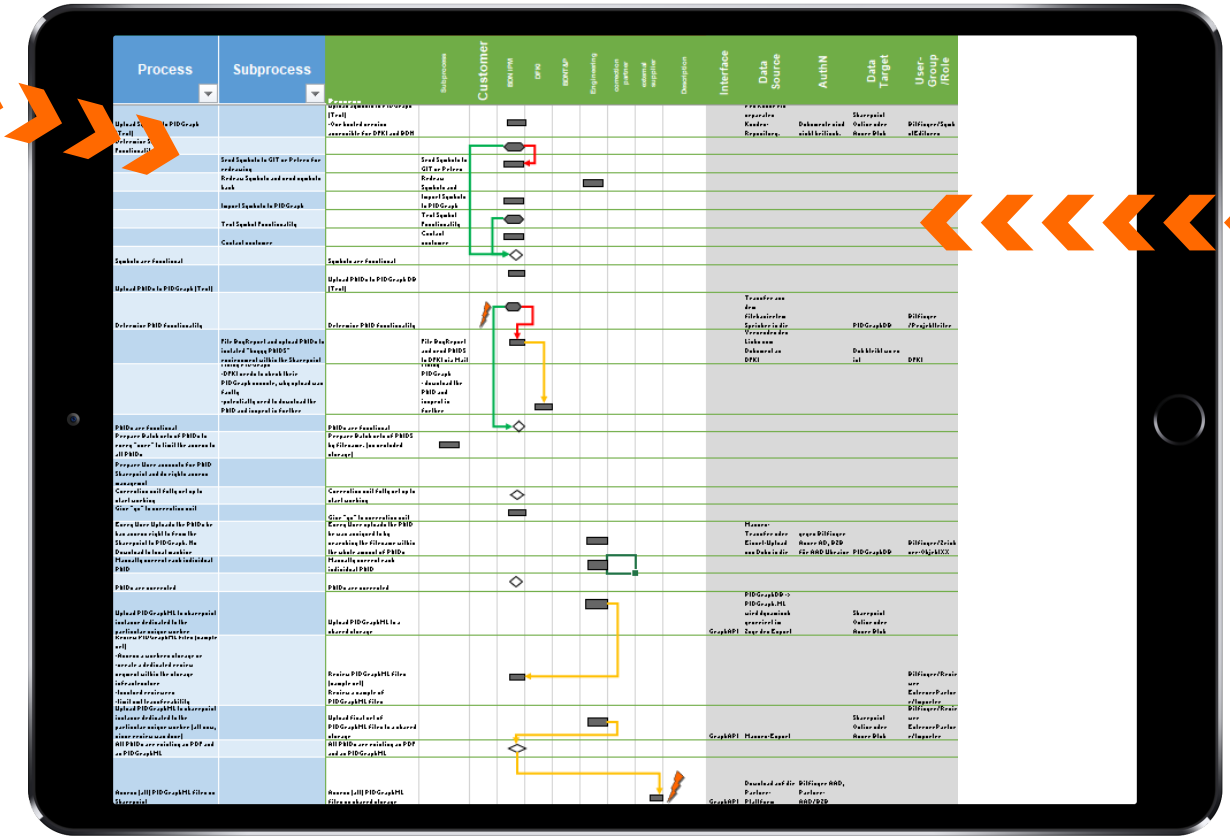
Zero Trust


OT
Operative
Technologie
/ Quarantäne
IT shared
Service
„Identity &
Access“
Sandbox
IT-Service
IT-Service
„Mail“
IT-Service
„Intranet“
SaaS
Service
Haupteingang
IT shared Service
„Network Access &
Network Control“
„Bus-System“
IT shared Service
„Network Access &
Network Control“
Anwendung A
Anwendung B
• Vertraulichkeit
• Verfügbarkeit
• Integrität
Anwendung
C via API
IT
Informations-
technologie
Datenspeicher
Datenbanken
Anwen-
dung
Erkennen – Benachrichtigen
(richtig/automatisiert) Handeln
„Incidence Response“
Pro-Aktiv statt reaktiv

DevSECOps – gelebte Applikationsmodernisierung: Sicherheit in Geschäftsprozessen

Prozessschritte

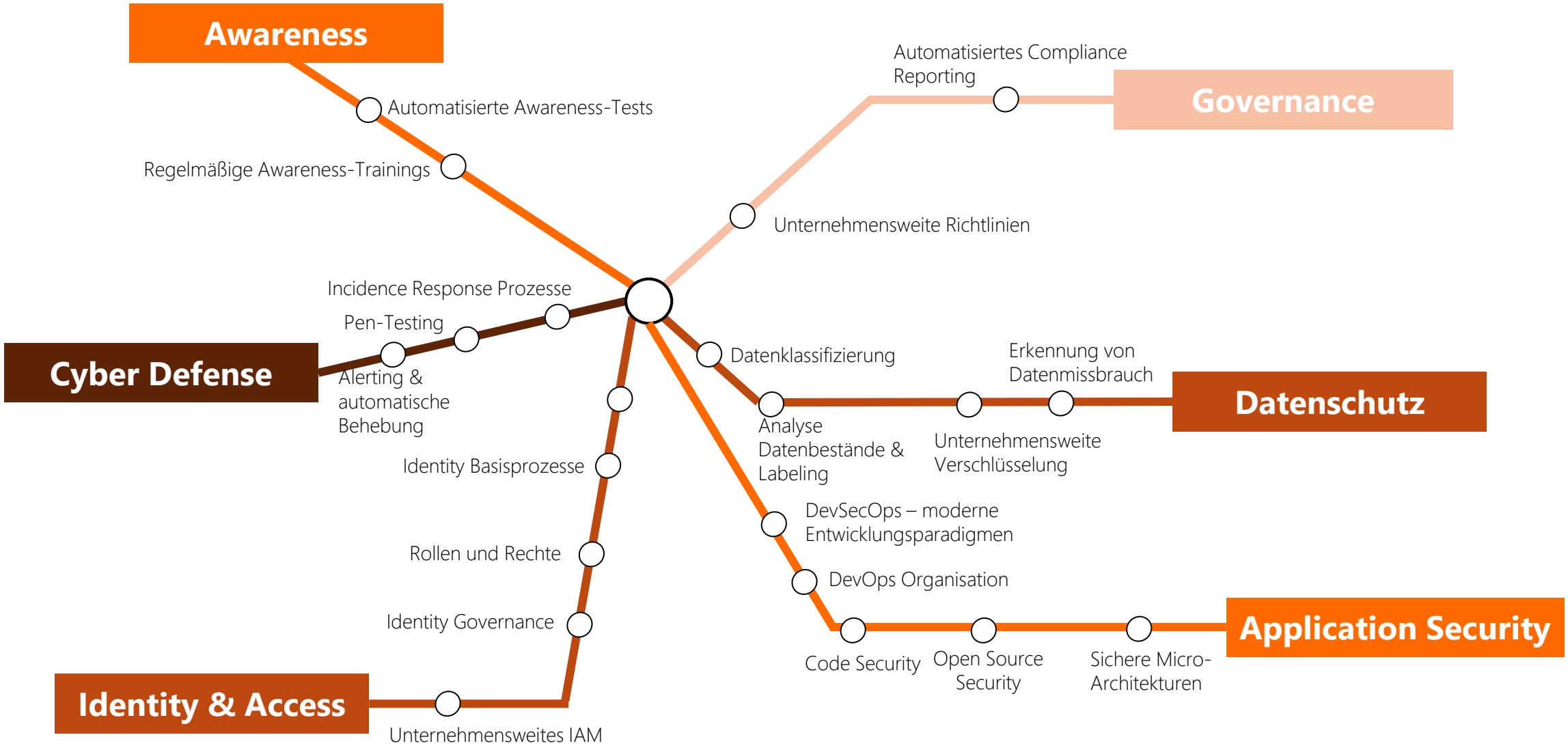
Datenfluss
Datenzugriff



Antworten auf:

- Welche Daten werden verarbeitet?
- Wo werden Daten gespeichert?
- Wie wird einem Datenverlust vorgebeugt?
- Nur die richtigen Menschen haben Zugriff auf die nötigen Informationen.

Ihr Weg zum Ziel



Key Takeaways

Digitalisierung & Sicherheit sind Chefsache

50% Organisationsentwicklung / 50% Technologie

Awareness ist wichtig – genauso wichtig wie die technologische Sicherstellung

Reduzieren Sie Komplexität sowohl in der IT-Infrastruktur als auch Security. Verstehen Sie Cloud als Enabler.

Masterplan + Veränderung in kleinen Schritten

! Menschen + Prozesse + Technologien = Erfolg und unternehmensweite Kultur

Steigen Sie ein: „IT Security Assessment“ Workshop

UNSERE UMFASSENDE SICHERHEITSANALYSE

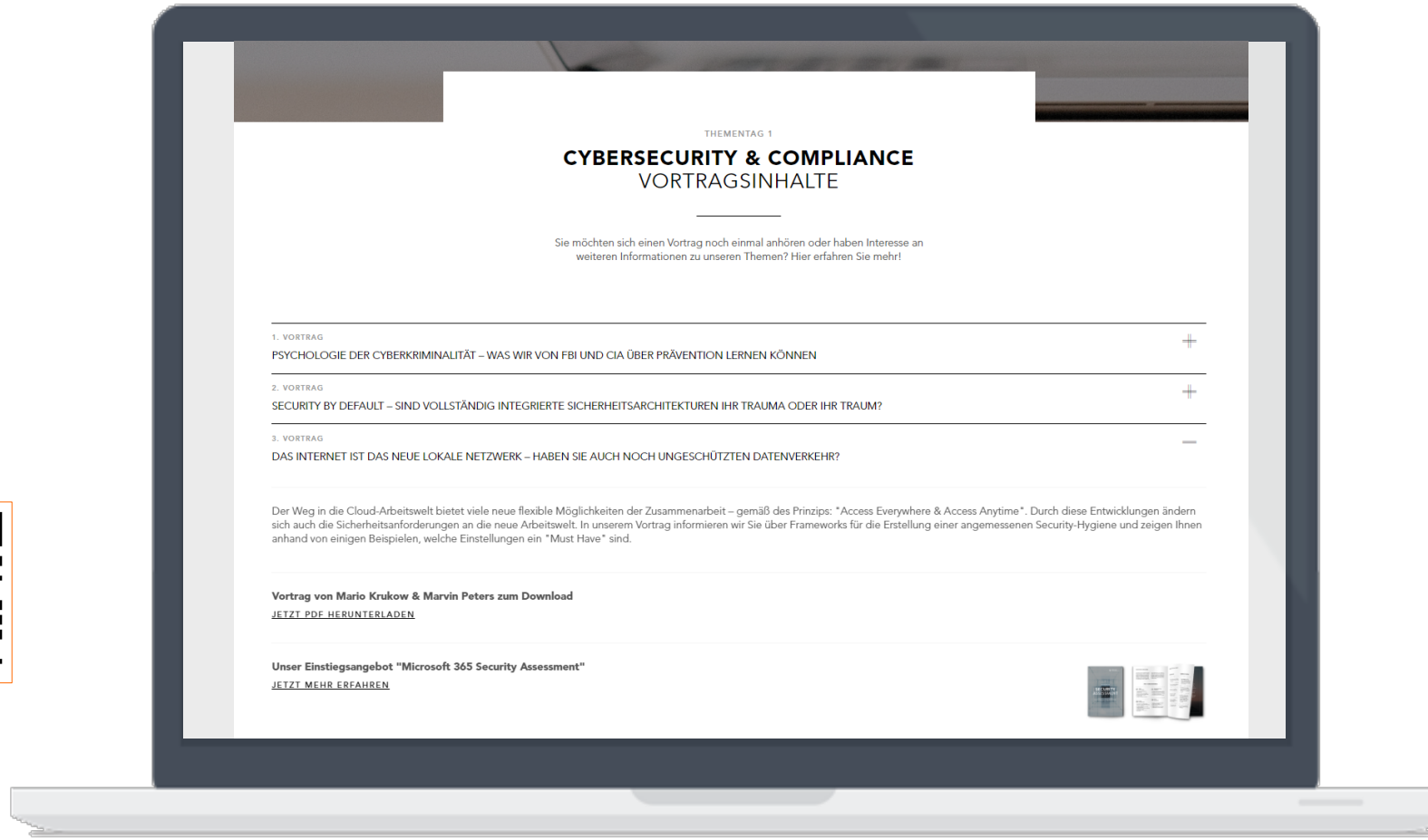
Alles zum gegenwärtigen Zustand erfahren, ihn bewerten, konkrete Handlungsfelder aufzeigen und geeignete Maßnahmen für mehr Sicherheit finden.

Mehr erfahren und Kurzcheck machen:
info.all-for-one.com/mifo2020-cybersecurity

Jetzt QR-Code scannen oder auf Link im Chat klicken!

Sie finden dort auf unserer Website:

- Diesen Vortrag zum Download
- Informationen zum o.g. Workshop



HABEN SIE FRAGEN?

Jetzt QR-Code scannen
oder auf Link im Chat klicken!

Sie finden dort auf unserer Website:

- Diesen Vortrag zum Download
- Informationen zum Workshop

Ihre Ansprechpartner bei Cybersecurity & Compliance

Andreas Schindler
Director & Executive Cloud Architect

+49 151 587 77 408
andreas.schindler@all-for-one.com

Willi Prosen
Head of Sales Microsoft

+49 175 48 176 71
willi.prosen@all-for-one.com

Roland Dühring
Senior Sales Manager

+49 151 526 42 338
roland.duehring@all-for-one.com

one idea ahead

Disclaimer

Die Informationen in diesen Unterlagen sind vertraulich und dürfen nicht ohne vorherige schriftliche Genehmigung durch All for One Group SE bekannt gegeben werden. Alle Texte, Bilder und Grafiken unterliegen dem Urheberrecht und anderen Gesetzen zum Schutz des geistigen Eigentums. Alle Rechte an diesen Unterlagen sind der All for One Group SE vorbehalten.
All for One Group SE stellt diese Unterlagen ohne jegliche Verpflichtung, Gewährleistung oder Garantie, weder ausdrücklich noch stillschweigend, zur Verfügung. All for One Group SE übernimmt keine Verantwortung für Fehler oder Irrtümer in diesem Dokument, es sei denn, derartige Schäden beruhen auf Vorsatz oder grober Fahrlässigkeit.
Der Inhalt dieser Unterlagen kann von All for One Group SE jederzeit geändert werden. Diese Unterlagen dienen ausschließlich informativen Zwecken und dürfen in keinen Vertrag aufgenommen, für Handelszwecke weiterverwendet oder an Dritte weitergegeben werden, soweit sie nicht für eine solche Verwendung gekennzeichnet sind oder eine vorherige schriftliche Genehmigung von All for One Group SE vorliegt.