Identitätskrisen im Dschungel der Berechtigungen

Daniel Timmann, Consultant Cybersecurity & Compliance
Christian Lechner, Senior Cybersecurity Architect

HERZLICHEN DANK,
dass Sie dabei sind!

Referent

Daniel Timmann

Consultant Cybersecurity & Compliance

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

T: +49 711 788 07-140
M: +49 176 341 70 155
E: daniel.timmann@all-for-one.com

Referent

Christian Lechner

Senior Cybersecurity Architect

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

T: +49 7131 3940 497
M: +49 151 616 98 819
E: christian.lechner@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

Agenda

1 IT-Sicherheit: Status Quo

2 Willkommen im Dschungel

3 Identity Access Management & Governance

4 Wie Sie konkret mit uns starten können

1

Typischer Cyberangriff

Wie läuft ein Angriff typischerweise ab?

Typischer Cyberangriff: Timeline & Beobachtungen

Erste digitale Identität kompromittiert

Domain Admin kompromittiert

Research & Preparation — **24-48 Stunden** — **Daten Exfiltration** (Angreifer unbemerkt) **8+ Monate** — **Angriff erkannt**

Raffinesse des Angriffs
Angreifer wird jede Schwachstelle ausnützen Wichtige und interessante Informationen liegen auf jedem Gerät oder in jedem Service

Exploiting Credentials
On-premises Active Directory regelt Zugang zu Business Assets. Angreifer attackieren fast immer das AD und den IT Admin

Angriff unerkannt
Aktuelle Lösungen erkennen einen Angriff häufig nicht Konzentration liegt ausschließlich auf dem Permimeter und AntiVirus

Reaktion & Wiederherstellung
Reaktion auf einen Angriff erfordert teure Experten und Tools.
Es ist kostspielig und schwierig, sich erfolgreich davon zu erholen.

Ernüchternde Zahlen

Eine kompromittierte digitale Identität ist ausreichend

01

Eine **kompromittierte digitale Identität** ist ausreichend

I am convinced that there are only two types of companies: Those that have been hacked and those who don't know. – *Robert Miller (FBI)*

2

Willkommen im Dschungel….

Wie kann es soweit kommen?

Wie kann es soweit kommen? – Der Dschungel….

Bequemlichkeit

„Als Mitarbeiter möchte ich so schnell wie möglich und ohne Unterbrechungen all meinen Arbeiten nachgehen können – egal ob ich mich organisatorisch verändere oder nicht“. „Es dauert schon lange genug, wenn ich zusätzliche Rechte beantrage. Noch komplexere Prozesse will ich nicht!“

Historie

„Accounts und Berechtigungen hat bei uns schon immer die IT genehmigt und verwaltet.“ „Bei uns funktioniert Identity und Access Management einwandfrei – in der IT betreiben wir Active Directory und verwalten dort Gruppen und Berechtigungen.“

Komplexität von IT Landschaften & Schatten-IT

„Diese Berechtigungen und Accounts bitte nicht löschen – wir wissen nicht wo diese verwendet werden und wollen keinen Produktionsausfall.“
„Eine komplett dokumentierte IT Landschaft haben wir nicht. Viele Abteilungen betreiben zusätzliche Services, die nicht von der IT verwaltet werden.“

Fehlende Ressourcen

„Wir hab das Thema „IAM“ schon seit Jahren auf der Roadmap, aber bis jetzt sind wir noch nicht dazugekommen.“
„Der Aufwand in unserer jetzigen IT Landschaft neue Prozesse und Tools einzuführen ist zu groß.“

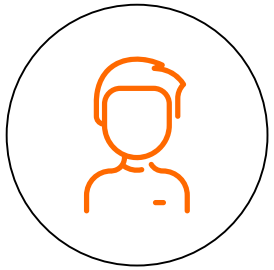
Falsche Sicherheit / Selbstbewusstsein

„Uns greift niemand an, wir sind zu klein / zu sicher / zu vorbereitet.“
„Natürlich wissen wir wer in unserem Unternehmen welche Zugriffe hat!“

3

Identity Access Management & Governance

Identitäten im Identity & Access Management



Natürliche Identität

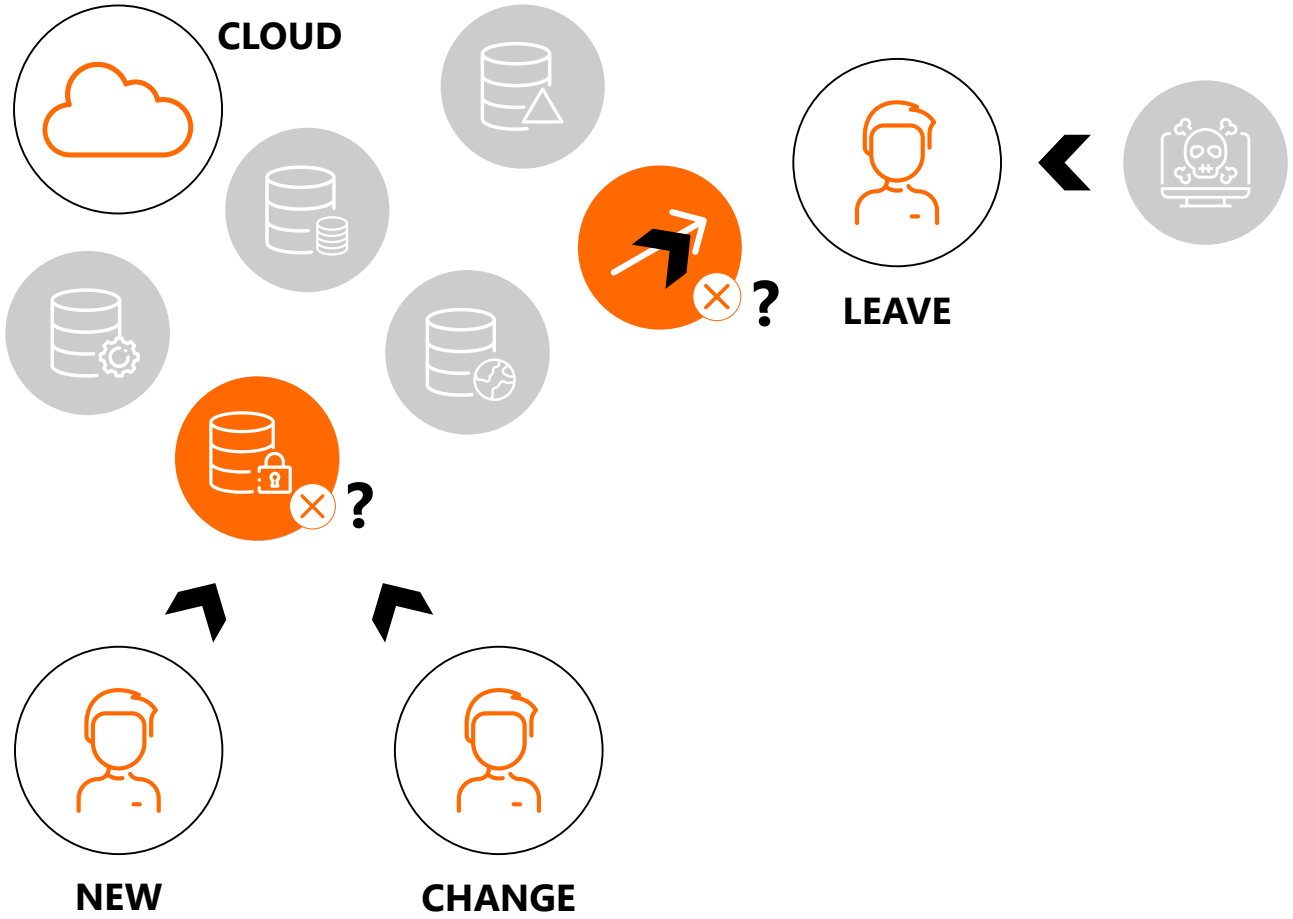
Ein Mensch.

VS.

Digitale Identität

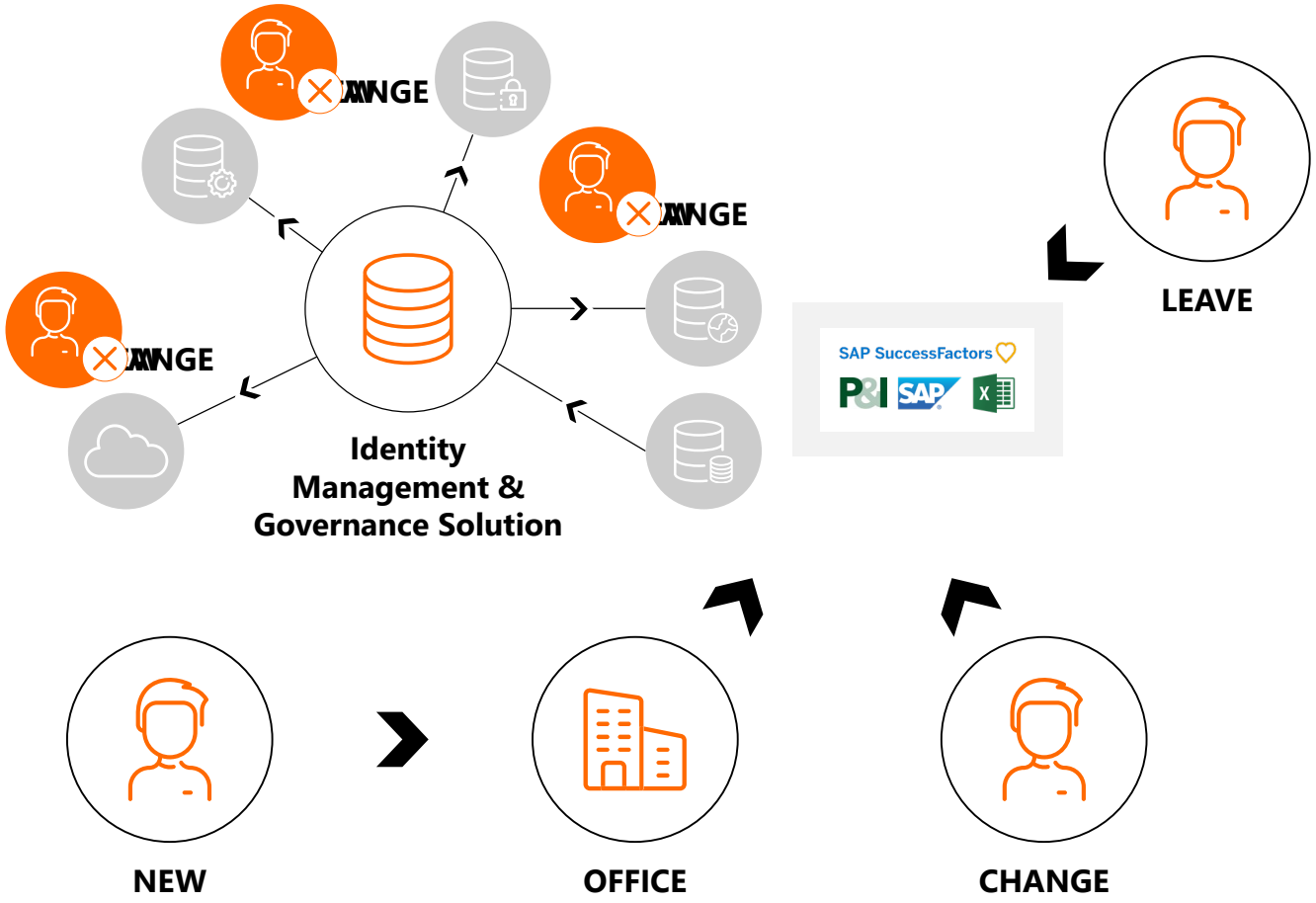
Eine Reihe persönlicher Attribute, die in Computersystemen gespeichert sind und dafür verwendet werden können, um eine Entität wie eine Person, Organisation, Anwendung oder ein Gerät eindeutig zu identifizieren.

Manuelle Identitäts- und Berechtigungsverwaltung



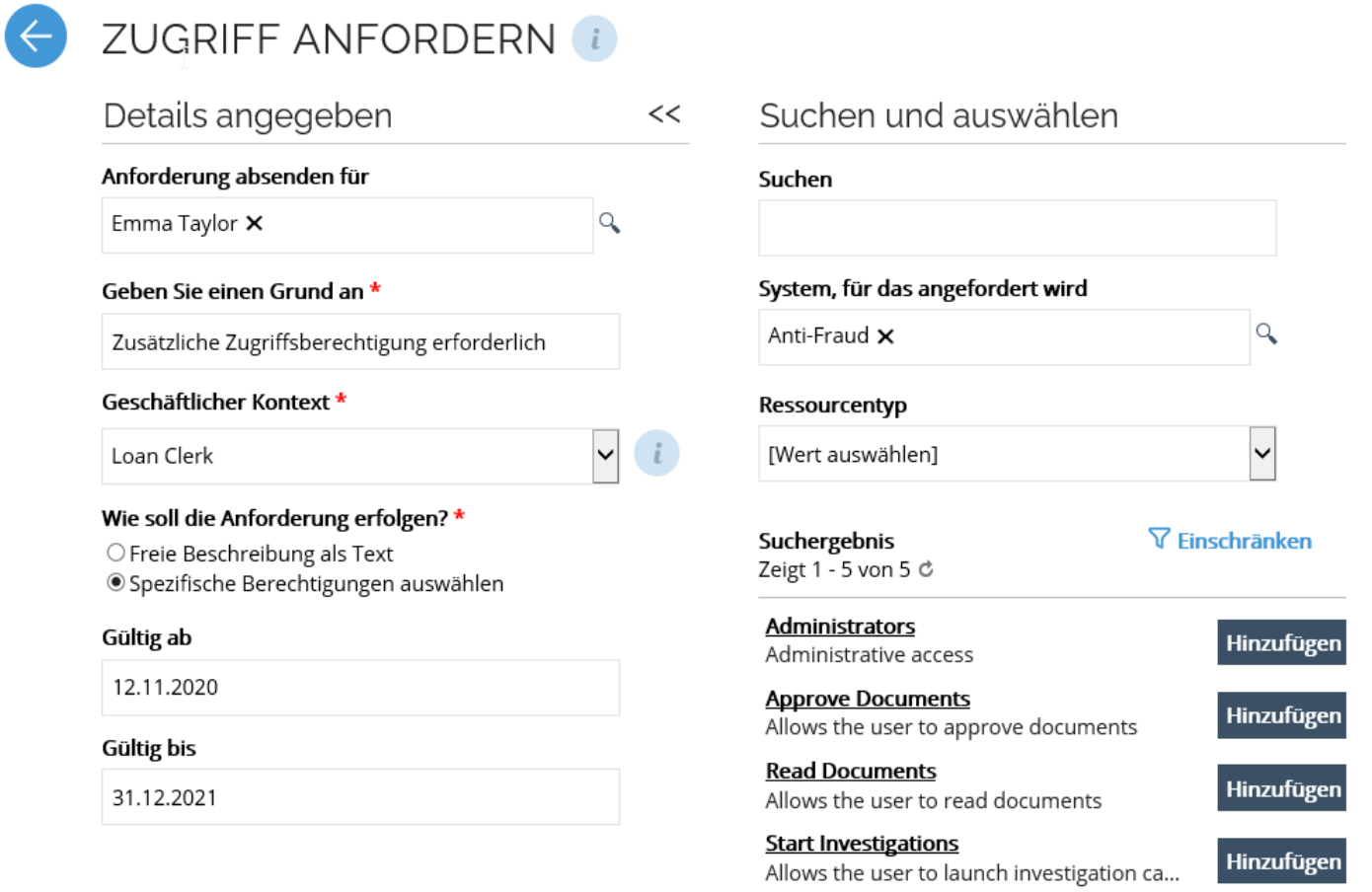
- Zu viele Rechte
- Accounts ohne Identität
- Leichtes Angriffsziel für Hacker
- Hoher administrativer Aufwand
- Keine Absicherung privilegierter Konten
- Keine Aussagefähigkeit wer wann welche Berechtigungen besitzt
- Keine klar definierten Eintritts- und Austrittsprozesse
- Langwierige Berechtigungsprozesse

Identity Access Management & Governance



- … Umsetzung von z.B. **Segregation of Duty** und Absicherung privilegierter Konten (MFA, **Zero Standing Access**)
- … wissen wer wann welche Rechte besitzt (**Reporting / Auditing**)
- … **reduzierter administrativer Aufwand** und erhebliche Kostenersparnis
- … schnelle und effiziente **Berechtigungs- und Genehmigungsprozesse**
- … zentrale Verwaltung von Identitäten und **automatisiertes Berechtigungsmanagement**
- … User-Benefits wie **Single-Sign-On** oder **Self-Service Password-Reset**

Rollen- und kontextbasierte Berechtigungsvergabe

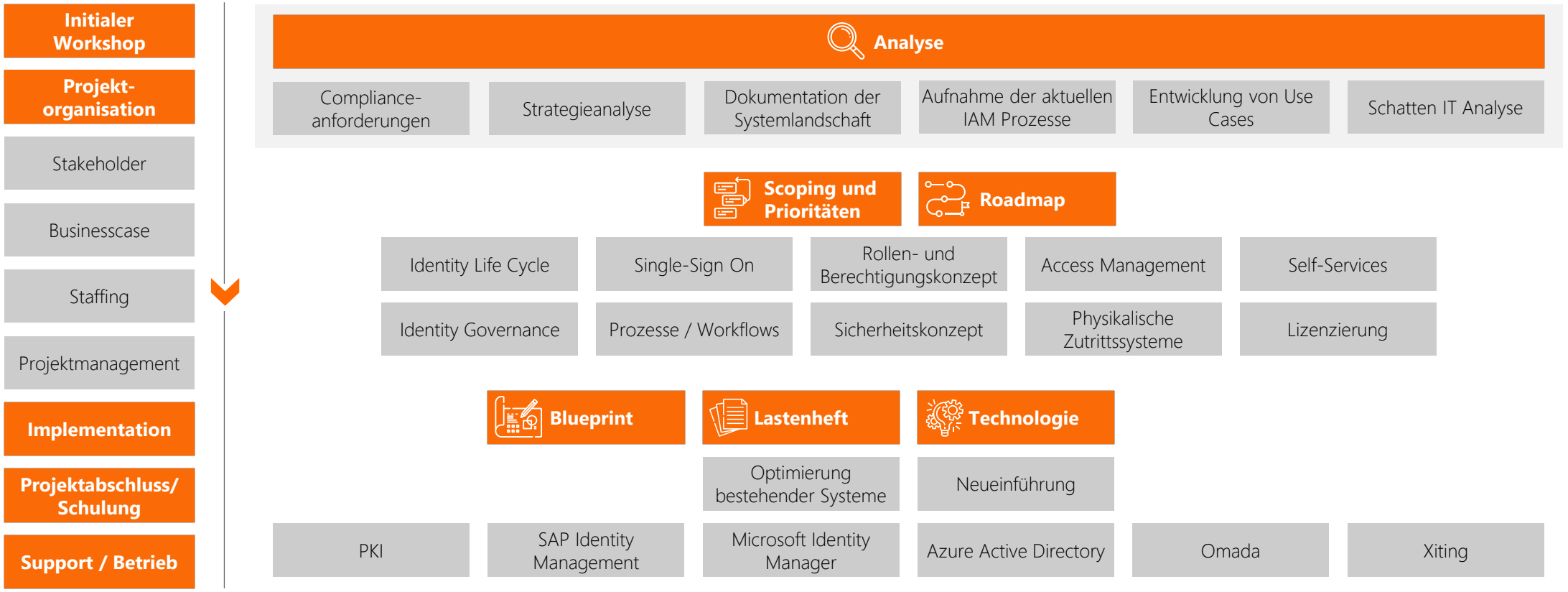


- Iterativer Modellierungsprozess für Rollen und Kontexte
- Automatische Rollenvergabe mit oder ohne Genehmigungsprozess
- Self-Service Berechtigungsvergabe
- Self-Service Account Unlock
- Self-Service Passwort Reset
- Gesteigerte Produktivität und schnelle Arbeitsfähigkeit der Mitarbeiter

4

Wie Sie konkret mit uns starten können

Individuelle Vorgehensweise: Je nach Situation & Zielbild



Erfolgreiche und nachhaltige Optimierung Ihrer Arbeitswelt!

Zusammenfassung – die wichtigsten Punkte

- Jedes Unternehmen kann Opfer einer Cyberattacke werden.
- Manuelle Prozesse führen in den Dschungel. Finden sie mit uns den Weg aus dem Dschungel.
- Überlassen sie Entscheidungen über notwendige Berechtigungen dem Benutzer und der Fachabteilung.
- Setzen sie auf Self-Services und reduzieren dadurch administrative Aufwände.
- Schaffen sie Transparenz durch Dokumentation und Auditierbarkeit ihrer Berechtigungsvergabe und ihres User Managements.

In der vernetzten Welt ändern sich Risiken permanent – aber auch die Abwehrtechniken.

Steigen Sie ein: „IDENTITY MANAGEMENT“ Workshop

DIE INITIALANALYSE

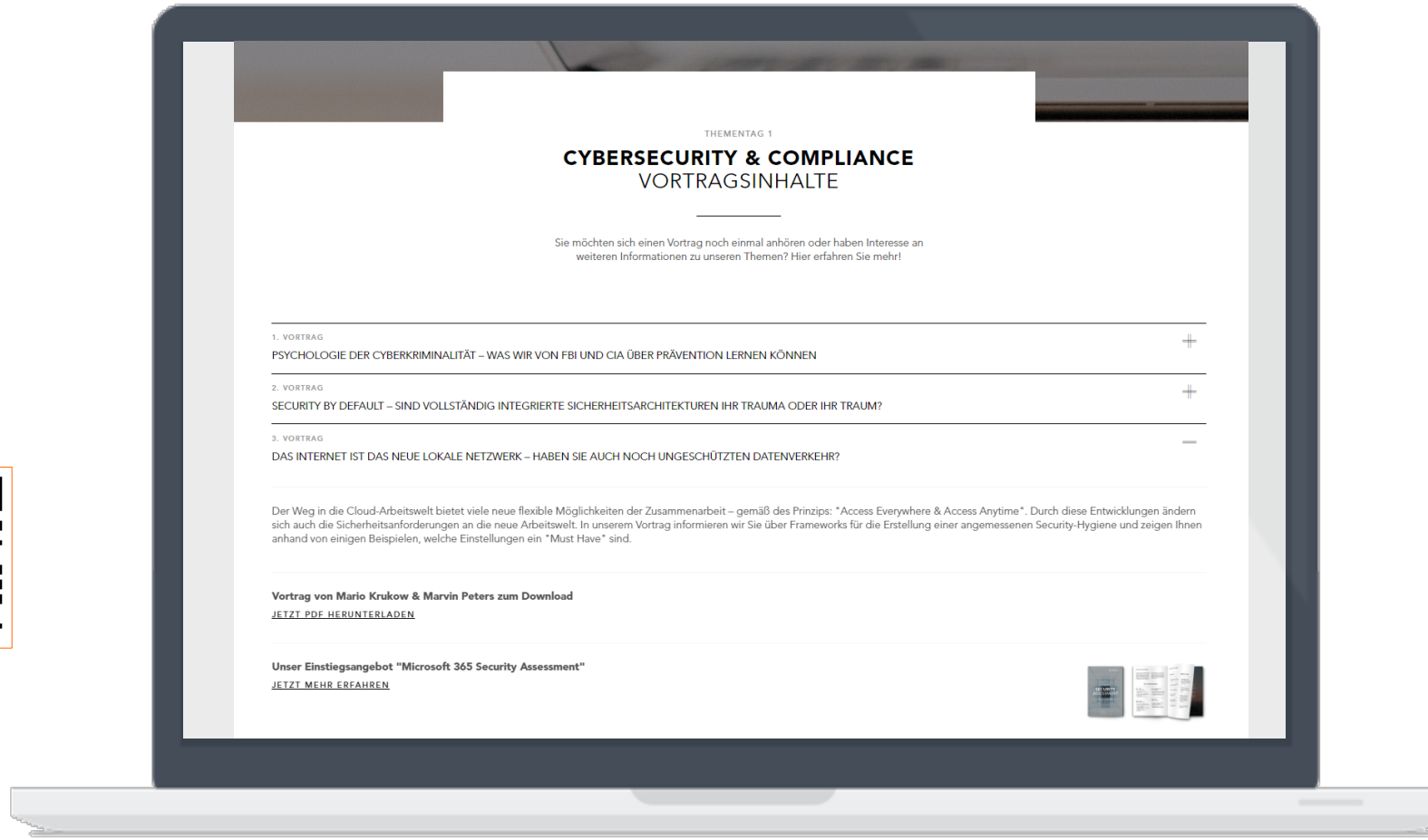
In vier Schritten zum individuellen Grobkonzept mit Handlungsempfehlungen.

Mehr erfahren und nächste Schritte planen:
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

Christian Lechner
Senior Cybersecurity Architect

+49 151 616 98 819
christian.lechner@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.