all for one Group

MITTELSTANDSFORUM 2020

Next-Generation Cyber-Defense: Wie Sie der wachsenden Bedrohung durch Cyberangriffe mit modernen Technologien begegnen.

Philipp Hilgers Senior Consultant Cybersecurity & Compliance
Oliver Filbert Senior Consultant Cybersecurity & Compliance

HERZLICHEN DANK,
dass Sie dabei sind!

Referent

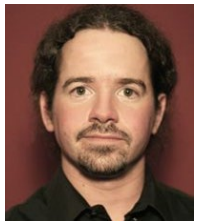
Philipp Hilgers
Senior Consultant
Cybersecurity & Compliance

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

T: +49 89 149 0226 443
M: +49 151 240 76 506
E: philipp.hilgers@all-for-one.com

Referent

Oliver Filbert
Senior Consultant
Cybersecurity & Compliance



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

T: +49 89 149 0226 16
M: +49 151 448 93 791
E: oliver.filbert@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

01 Einleitung – Status Quo

02 Heutige Herausforderungen

03 SIEM Tools (Cloud/On-Premises)

04 Projektphasen SOC / SIEM

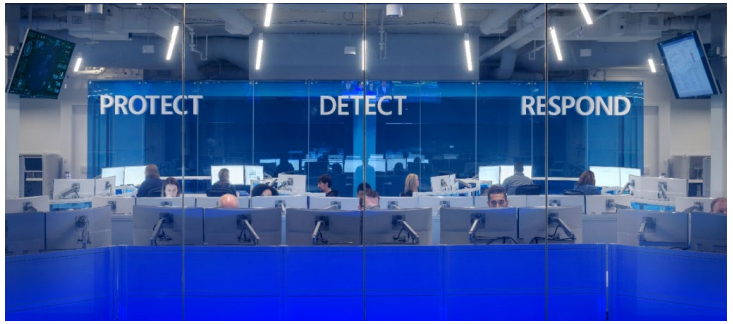
05 Exkurs - Tactics & Technics der Angreifer

01

Einleitung – Status Quo

Begriffsdefinitionen

- **SIEM** = **S**ecurity **I**nformation **E**vent **M**anagement System vereint
- **SIM** = **S**ecurity **I**nformation **M**anagement bzw. Log Management
- **SEM** = **S**ecurity **E**vent **M**anagement
  (Korrelation von Logs anhand definierter Richtlinien)
- **SOAR** = **S**ecurity **O**rchestration, **A**utomation and **R**esponse
- **SOC** = **S**ecurity **O**peration **C**enter
  Zentrale Überwachung von IT-Ressourcen und Daten, der Suche nach Anzeichen für Angriffe und der Steuerung von Reaktionen auf Cyber-Bedrohungen
- **CDC** = **C**yber **D**efence **C**enter (SOC 2.0)



Ernüchternde Zahlen

- Eine kompromittierte digitale Identität ist ausreichend
- Durchschnittliche Kosten pro Datendiebstahl – $3.8 Mio.
- Durchschnittliche Zeit bis ein Angreifer im Netzwerk erkannt wird – 146 Tage
- Geschätzt mehr als 100 Milliarden Euro Schaden pro Jahr allein bei deutschen Unternehmen.

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

Typische Attacke: Timeline & Beobachtungen

Erste digitale Identität kompromittiert

Domain Admin kompromittiert

Research & Preparation — **24-48 Stunden** — **Daten Exfiltration** (Angreifer unbemerkt) **+8 months** — **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 und Wiederherstellung
Reaktion auf einen Angriff erfordert teure Experten und Tools.
Es ist kostspielig und schwierig, sich erfolgreich davon zu erholen.

Zero Trust

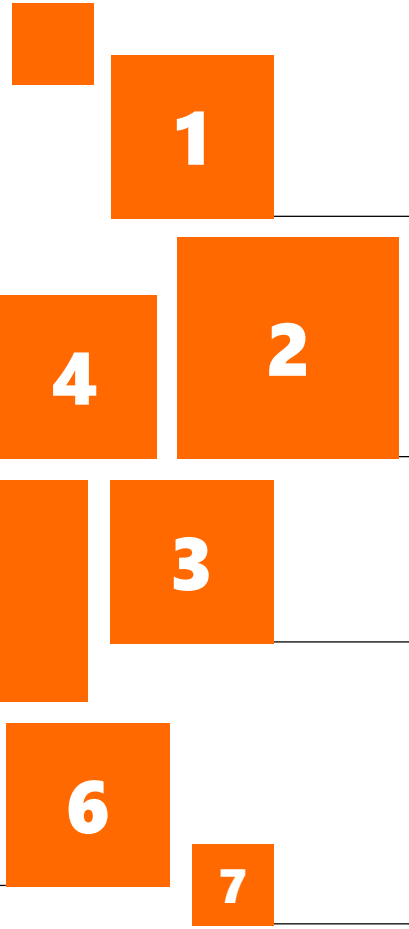
„Traditional perimeter-based network defense is obsolete“

- Defense in Depth
- Focus on Monitoring & Detection
- Incident & Response

02

Heutige Herausforderungen

Herausforderungen



Komplexität – Hybride Landschaften

im Design, Aufbau und Betrieb (SOC/CDC)

Intelligenz

für die Auswertung der Logs

Skalierung

bei wachsender/m Infrastruktur und Datenvolumen

PPP

Processes, Product, People!

Schnittstellen & Kompatibilität

für verschiedenste Quellen von Logs

Kosten

für die Verarbeitung und Aufbewahrung der Logs.

Kein Stillstand

Security is an „ongoing battle“

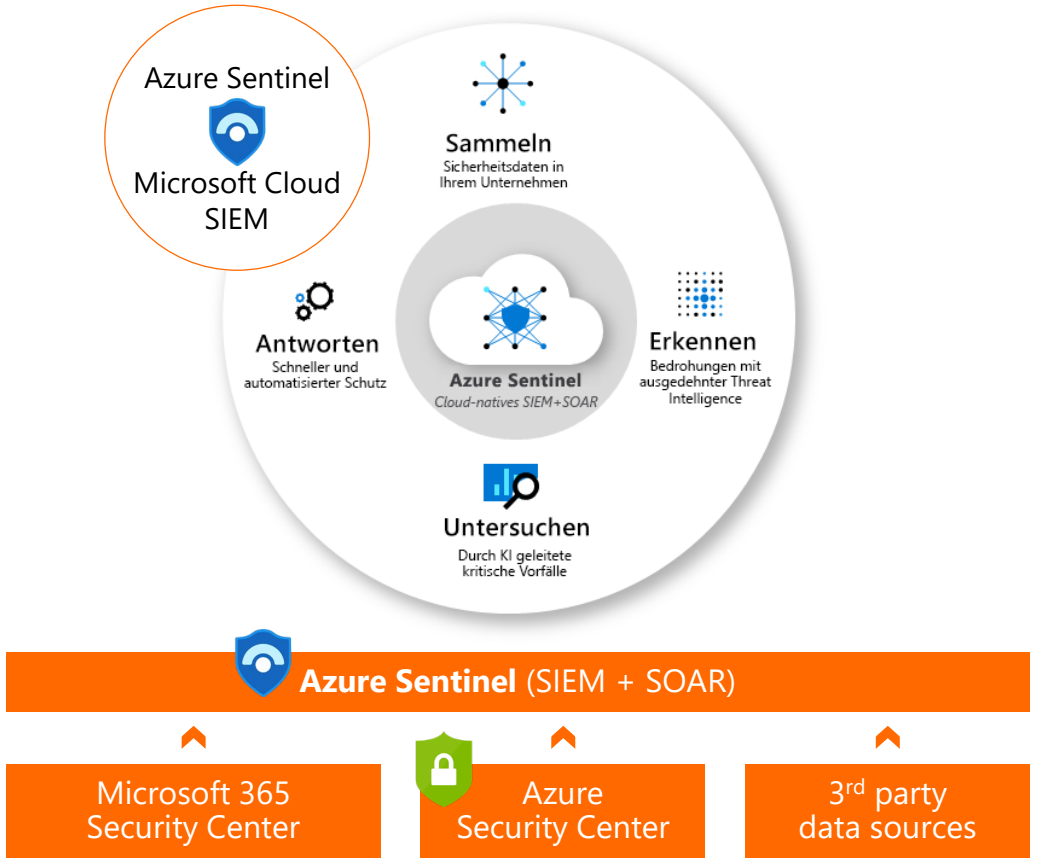
SIEM Tools – Cloud/On-Premises

03

Cloud-natives SIEM von Microsoft

- Cloud-natives SIEM – PaaS Service
- MITRE ATT&CK Framework integriert
- Community-Ansatz (Github Repos, Dashbaords usw.)
- Über 80 vordefinierte Use Cases
- Cloud-Vorteile - Geschwindigkeit und Skalierung
- Ausgeprägte SOAR-Funktionalität (Playbooks)
- ML / KI Unterstützung
  (User Behavioral Analytics)
- Azure & Microsoft 365 Datenintegration ist kostenfrei

Log-Plattform für mehr als 10 Petabyte / Tag



Projektphasen – SOC/SIEM

04

Projektphasen SIEM (Auszug)

01 Vorprojekt

- Klärung der Anforderungen des Kunden und die Definition des Ziels eines SIEMs
- Prioritäten werden definiert und durch einen Risikobasierten Ansatz/Strategie fundiert
- Was ist der Treiber für ein SIEM ? Compliance, Security .. ?
- Was sind die Unternehmswerte / Wo unterstützt die IT
- Definition von Logquellen
- Use Case Definitionen / Alarming
- Prozesse / Ticketsystem
- Auswahl des geeigneten SIEM Tools

02 Onboarding

- Onboarding der Logquellen
- Implementierung der Use Cases
- Anbindung / Integration der nachgelagerten SIEM Prozesse, z.B. Ticketsystem
- Justierung der Alarme – (false positives)
- Testen des Systems & der Prozesse

03 Betrieb

- SIEM geht live
- Use Case Lifecycle
- Incident Response Process
- Basis für SOC / CDC Betrieb
- Auswahl des SOC / CDC Providers (A41 hat hierfür Partner)

Bauchlandung verhindern – aus dem Nähkästchen

- Ohne Strategie und Ziel ein SIEM einführen
- Einführung eines SIEM ist KEINE TOP Down Entscheidung
- Einfach ALLE Logs einsammeln (bringt wenig)
- Nur mit „out of the Box“ Use Cases arbeiten
- Installiert und fertig – SIEM & Security ist ein andauernder Prozess
- SIEM Betrieb macht die IT nebenher mit (kann nur schief gehen)

! Wenn Sie ein SIEM Projekt planen oder eine bereits bestehende SIEM-Lösung betreiben, betrachten Sie SIEM ganz-heitlich. Ein „bisschen“ SIEM gibt es nicht.

05

Exkurs
Tactics & Technics der Angreifer

MITRE ATT&ACK – Was ist das?

ATT&ACK = Adversarial Tactics, Techniques and Common Knowledge

ATT&CK™

» Frei, Offen, Community getrieben Wissensdatenbank
(Weltweite Beobachtungen)

» Beschreibt Gegnerisches Verhalten & deren Eindämmung

» Gemeinsame Sprache (Taxonomie) für Angriff und Verteidigung

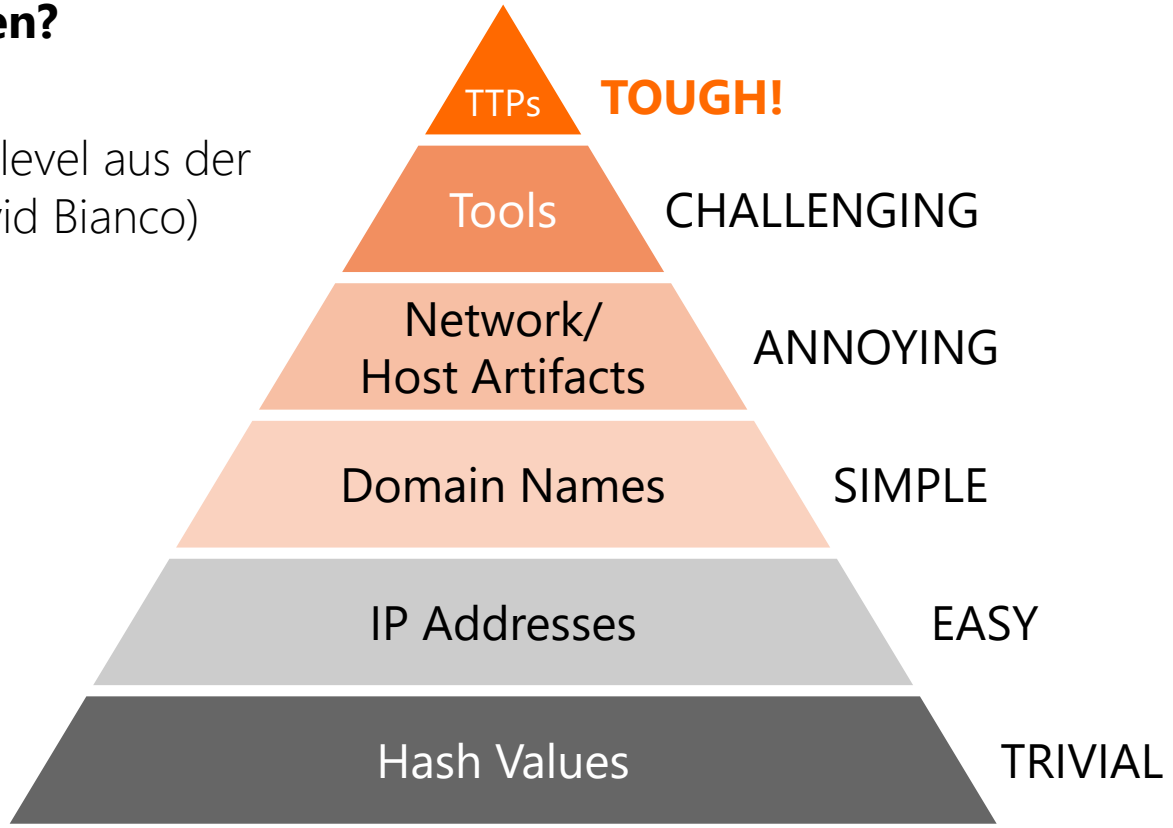
Taktik = Was versucht der Angreifer zu erreichen
Technik = Wie kann der Angreifer es erreichen

1. PRE-ATT&CK Matrix
2. Enterprise Matrix (Cloud, OS)

MITRE ATT&ACK

Was möchte MITRE lösen?

„Pyramid of Pain“ Schmerzlevel aus der Sicht eines Angreifers (David Bianco)



ATT&CK™

Quelle: http://2.bp.blogspot.com/-EDLbyYipz_E/UtnWN7fdGcI/AAAAAAAANns/4rBXaHarJ6o/s1600/Pyramid+of+Pain+v2.png

Next-Generation Cyber-Defense: Fazit

- Bedrohungslagen & Angriffsvektoren ändern sich fortlaufend –
  daher müssen auch Securityprozesse regelmäßig der Lage angepasst werden.
- Cybersecurity & Cyberdefense ist nichts was eine „Infrastruktur"-IT nebenher machen kann.
- Nicht nur Unternehmen mit Geschäftsgeheimnissen (z.B. Entwicklungsdaten, Patente) sind bedroht – Auch Systemausfälle können zu erheblichem wirtschaftlichem Schaden führen.
- Ein exzessives Einsammeln von Logs und Auditdaten hilft niemandem ohne
  das passende Analyse Know-how.

! Cyber-Defense & Cybersecurity ist nicht nur was für die großen Global Player.
IT und IT Security sind heutzutage untrennbar verbunden.

Steigen Sie ein: „Azure Sentinel SIEM“ Workshop

DER AZURE SENTINEL SIEM WORKSHOP

Initiale Entwicklung einer High-Level Designvariante und eines Architektur-Blueprints.

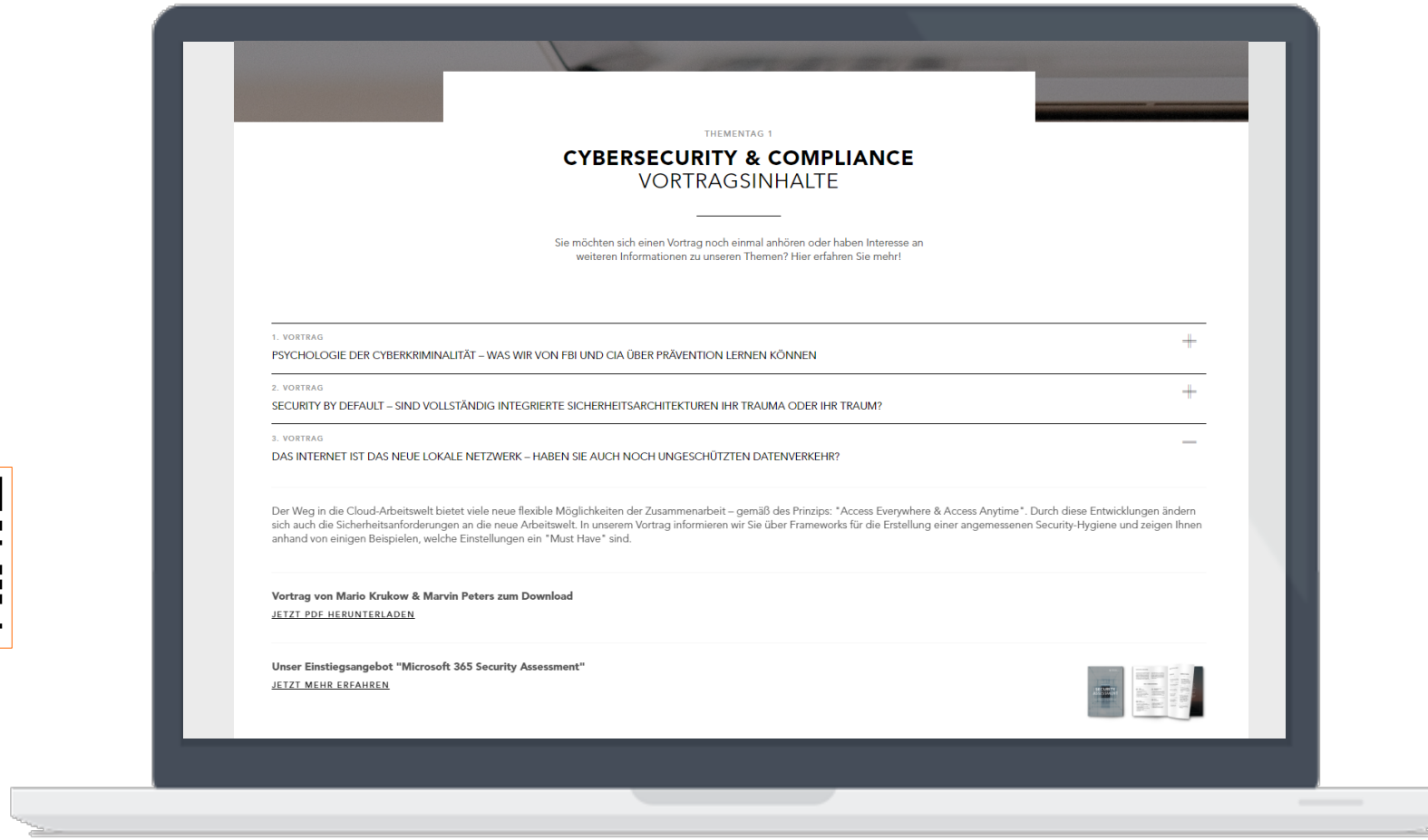
info.all-for-one.com/mifo2020-cybersecurity

Mehr erfahren und nächste Schritte planen:

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

Philipp Hilgers
Senior Consultant
Cybersecurity & Compliance

+49 151 240 76 506
philipp.hilgers@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.