15:55 – 16:15 Uhr

Gemanagte Security für KMUs

Maximilian Munker

Agenda

1. **Bedrohungslage**
2. **Aktuelle Herausforderungen für KMUs**
3. **Wie gehen wir die Herausforderungen an?**
4. **Wie kann Bechtle Sie im Mittelstand unterstützen**

1

Bedrohungslage

bechtle

Auszug aus dem BSI-Lagebericht

Weiterhin die größte Bedrohung:

Ransomware

2 **Ransomware-Angriffe** auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat erkannt.

68 Erfolgreiche **Ransomware-Angriffe auf Unternehmen** wurden bekannt.

15 Davon richten sich gegen **IT-Dienstleister.**

Mehr als **2.000** Schwachstellen in Softwareprodukten (**15% davon kritisch**) wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24%**.

66% aller **Spam-Mails** im Berichtszeitraum waren Cyberangriffe:

34 % Erpressungsmails,
32 % Betrugsmails

Eine Viertelmillion neue **Schadprogramm-Varianten** wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.

84% aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken oder Sparkassen

Top 3

Bedrohungen je Zielgruppe

Gesellschaft
Identitätsdiebstahl

Sextortion
Phishing

Wirtschaft
Ransomware

Abhängigkeit innerhalb der IT-Supply-Chain Schwachstellen, offene oder falsch konfigurierte Onlineserver

Staat und Verwaltung
Ransomware

ATP, Schwachstellen, offener oder falsch konfigurierter Onlineserver

Prominente Opfer von Cyber-Angriffen in der Schweiz

RG Realgymnasium Rämibühl Zürich
ZURICH
Universität Zürich[UZH]
SWISS POST
SBB CFF FFS
NZZ Mediengruppe
BERNINA
BOSShard bekennt Farbe
schlatter

Halbjahresbericht 2024 / 1
Bundesamt für Cybersicherheit (BACS)

Die Bedrohung im Cyberraum **ist so hoch wie noch nie** zuvor.

Aktuelle Herausforderungen für KMU´s

2

bechtle

Welche Herausforderungen treffen wir vor allem im Mittelstand?

Angesichts der sich entwickelnden Cyberangriffe, des regulatorischen Drucks und der zunehmenden Komplexität von IT-Umgebungen muss Cybersicherheit als strategische Investition betrachtet werden. Es ist unerlässlich, das Unternehmen vor operativen, finanziellen, rechtlichen und Reputationsrisiken zu schützen.

Zunehmende Bedrohungen

Gezielte Angriffe

Explosion von Ransomware

Künstliche Intelligenz

Fragmentierung der Umgebung

Hybride Infrastrukturen

Multicloud

(SaaS-Verbreitung

BYOD, IoT, Schatten-IT)

Regulatorischer Druck

Lokaler & internationaler Rechtsrahmen

Audits & Kontrollen

Anforderungen der Kunden

Unzureichende Kapazität

Fachkräftemangel

Mehrere Rollen zur Gewährleistung der Sicherheit

Notwendigkeit der Automatisierung

Steigende Kosten

Multiplikation von Lösungen

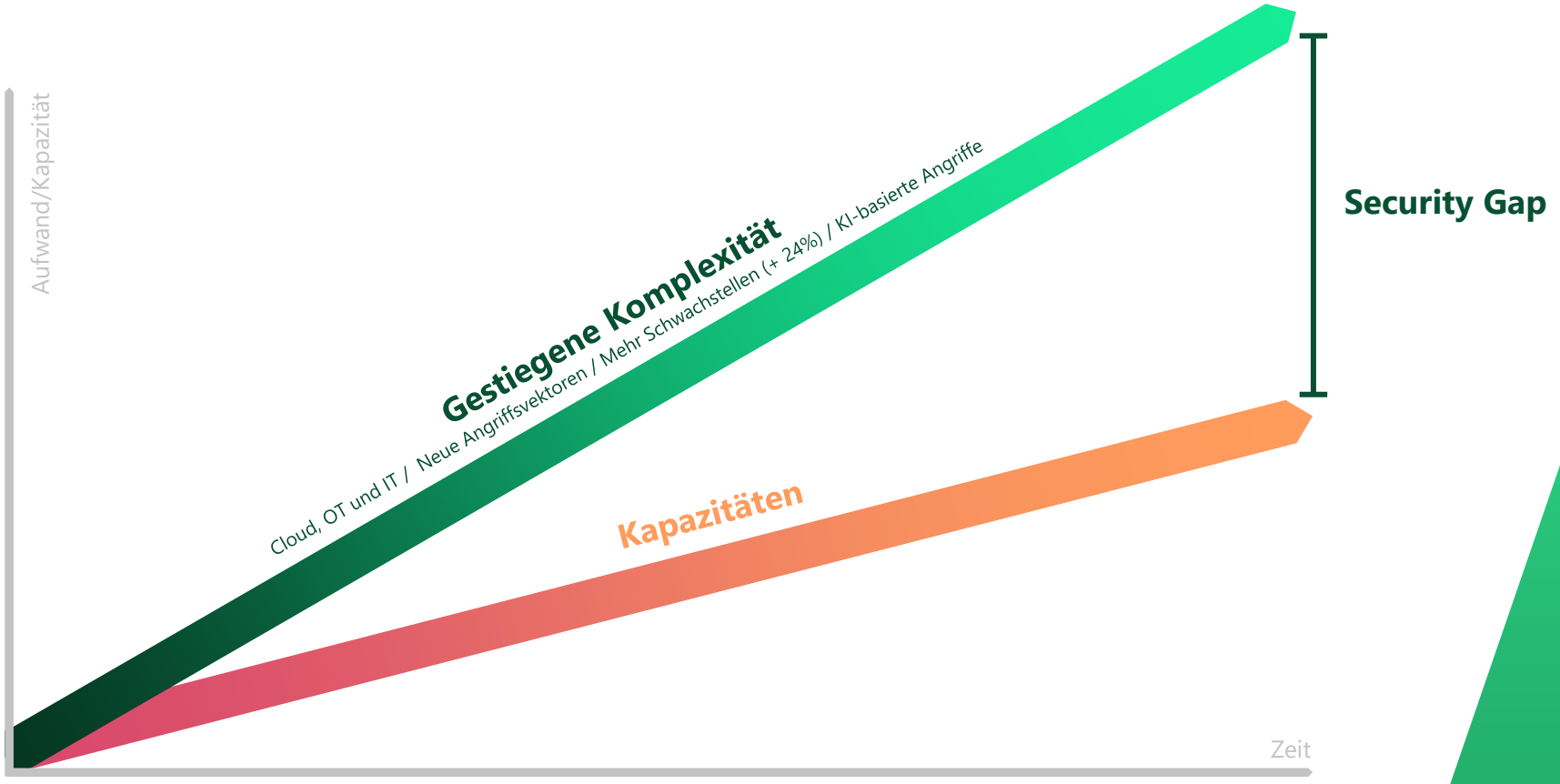
Komplexität technologischer Entscheidungen

Wie genau sollen alle diese Handlungsfelder durch ein kleines IT Team bewerkstelligt werden?

Zwangsläufig steigt die Risikodisposition, da nicht alle Themenbereiche adressiert werden können.

Aktuelle Herausforderungen für KMU´s

Das Security Gap.

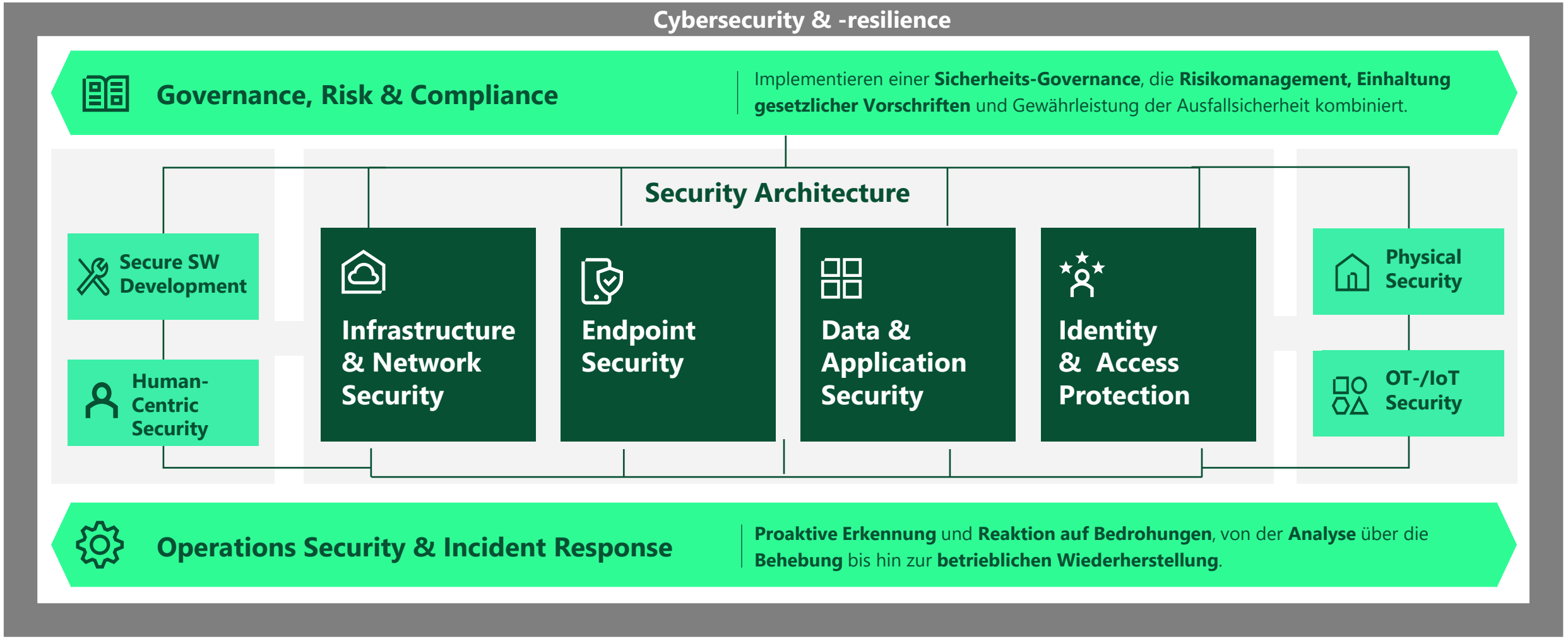


Wie gehen wir die Herausforderungen an?

3

bechtle

Wie würde eine vollumfängliche IT Sicherheitsstrategie aussehen?



Wer stellt dies denn alles sicher?

bechtle

Welche Optionen haben wir mit dem „Security Gap“ umzugehen ?

Mehr interne Ressourcen

- Aufbau von Fachkompetenz
- Aufbau eigener organisatorischer / technischer Sicherheitslösungen
- Betriebsverantwortung /Risikoverantwortung
- Benötigt eine gewisse Zeit, um den Themenbereich vollumfänglich zu beherrschen

Security Gap ignorieren

- Risikodisposition steigt signifikant (Cybervorfälle)
- „Best Effort“ IT
- Unkalkulierbares Risiko und mögliche monetäre Konsequenzen

Themenbereiche auslagern durch externe Unterstützung

- Verantwortlichkeiten sowie Service Level Agreement definiert
- Planbare Kosten
- „Mietbare“ Fachkompetenz
- Signifikante Verringerung des Risikos
- Schnell buchbar und einsatzbereit

Wie kann Bechtle Sie im Mittelstand unterstützen?

4

bechtle

Security Journey.

Unklare oder fehlende Security-Strategie oder (stark) veränderte Bedrohungslage

Sicherheitsstrategie/-ziele, Etablierung Rollen, Verantwortlichkeiten; Definition Richtlinien, Standards, Governance-Framework

Assessment

Strategie & Governance

Asset- und Bedrohungsanalyse; Risiko-Analyse/-Bewertung; Risikostrategie

Risiko-Assessment

Regulatorien

Wie reduziere ich die Risiken?

Policies, SLA
Firewall, IAM, EDR, DLP, SASE, …
Patch-Management, Backup

Planung & Umsetzung

Auswahl und Umsetzung Schutzmassnahmen; Planung/Umsetzung technische und organisatorische Massnahmen

Kontinuierliche Verbesserung

Wie hat sich die Bedrohungslage geändert? Welche Optimierungen sind erforderlich?

Wie stelle ich den laufenden Betrieb und das Monitoring sicher?

Wie reagiere ich bei Sicherheits-vorfällen und stelle die Geschäfts-kontinuität sicher?

Security Services, Betriebs-unterstützung,

CISOaaS, DSBaaS

Incident Response

CIRT, Incident Manager, Forensik
Notfallpläne

Betrieb & Überwachung

Schwachstellen-Management, Hardening; SOC; Log-Management SIEM; Assessments, Tests, Audits, Compliance-Überwachung

Incident Management, Business Continuity & Desaster Recovery, Krisenbewältigung, Analyse & Forensik

Wie könnnte eine solche Reise mit uns aussehen? (Teil1)

Identify **Protect**

Unser Know-how in den Bereichen Infrastruktur und Sicherheit ermöglicht es uns, die Bedürfnisse unserer Kunden zu erkennen und ihre kritischen Assets effektiv zu schützen, um eine optimale Geschäftskontinuität zu gewährleisten.

1 Kennen Sie das Sicherheitsniveau und formalisieren Sie eine Roadmap

Durchführung eines organisatorischen und technischen **Cybersecurity Assessments.**

Kurz- , **mittel-** und **langfristiger** Fahrplan mit geschätzten Budgets und benötigten Ressourcen.

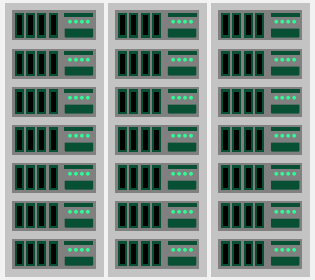
Unterstützung bei der Validierung **auf strategischer Ebene.**

2 Implementierung von Plänen für das Business Continuity Management

Untersuchung Ihrer Bedürfnisse durch eine **BIA** (Business Impact Analysis).

Formalisierung eines **BCP** (Plan zur Aufrechterhaltung des Geschäftsbetriebs).

Konzeption und Implementierung eines **DRP** (Disaster Recovery Plan).



3 Stärkung der Netzwerksicherheit

Prüfung und Überprüfung von **Firewall-Regeln sowie Netzwerk-Architektur (Zonierung/Segmentierung).**

Implementierung von **NAC** (Network Access Control).

Wie könnnte eine solche Reise mit uns aussehen? (Teil 2)

Detect **Response** **Recover**

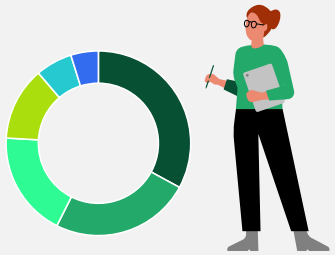
Unser Know-how in der Überwachung und im Betriebsmanagement ermöglicht es uns, Vorfälle zu erkennen, die für die Reaktion erforderlichen Akteure zu koordinieren und die Aktivität schnell wiederherzustellen und so eine optimale Resilienz zu gewährleisten.

4 Sichern und überwachen Sie alle Endpunkte

Untersuchung der Bedürfnisse und Regeln, die eingeführt werden sollen.

Bereitstellen und Konfigurieren der richtigen Lösungen wie **EDR**, **MDM** und **Firewall.**

Kontinuierliche Überwachung.

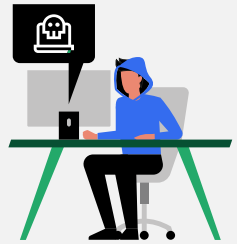


5 Profitieren Sie von kontinuierlicher IS-Überwachung und -Transparenz

Untersuchung des Bedarfs.

Bereitstellen eines **MDR-** oder **SOCaaS-Dienstes.**

Überwachung und **Berichterstattung** werden fortgesetzt.



6 Bewältigung einer Cyberkrise

Einrichtung eines **Krisenstabs.**

Verbindung mit einem vollständigen **CSIRT-Team** bis hin zum **Forensic Analyst.**

Rekonstruktion von Daten und Infrastruktur.

Härtung der Infrastruktur am Ende der Krise.

Wie können wir unsere Kunden im Mittelstand unterstützen?

bechtle

Bechtle Cybersecurity as a Service.

Kunde

Wir bieten ein komplettes Portfolio an Managed Security Services:
Unsere Expertise für Ihre Sicherheit – einfach, professionell, zuverlässig.

Kundenbetreuung

- **Account Manager**
- **Service Manager**

+ Service Desk & Spezialisten-Unterstützung

- **360° firewall**
  Gesamtbetrieb standardisierte Firewall Infrastruktur
- **360° antivirus**
  Gesamtbetrieb Antivirenumgebung
- **360° iam**
  Plattform und Gesamtbetrieb Identity- und Accessmgmt
- **360° mdr**
  Managed Detection & Response
- **360° operation firewall**
  Betrieb Firewall Infrastruktur
- **360° awareness**
  Security Awareness Training & Phishing Simulation
- **360° dsb**
  Datenschutzbeauftragter as-a-Service
- **360° cirt**
  Incident Response Taskforce
- **360° IAM**
  Betriebs- & Supportleistungen
- **360° ciso**
  Informationssicherheits-beauftragter as-a-Service

- **SOC**
  Betrieb SOC/SIEM aus CDC Bechtle
- **Pentest**
  Pentesting durch Bechtle BISS
- **Attack Surface Management**
- **Schwachstellen-management**

- **Security Assessment**
  Analyse, Bewertung und Massnahmenempfehlung
- **Tenant Quick Check**
  Überprüfung M365 Azure-Identitäten & Online Services
- **Business Continuity Management**
  Ausarbeitung BCM-Konzept

Maximilian Munker

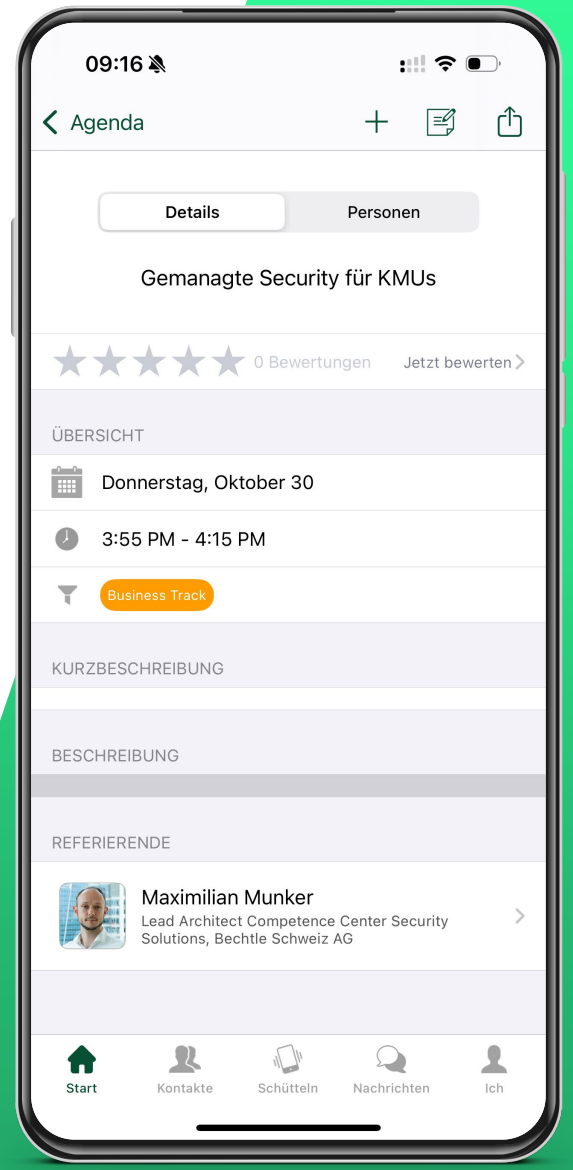
Gemanagte Security für KMUs

Ihr Feedback zählt

Jetzt in der App bewerten.

App Store

Play Store



16:20 bis 16:50 Uhr

Kaffee*pause*

16:50 - 17:10 Uhr

SCHMIEDE

Kundenreferenz Coop Pronto Shop
Andreas Weidner (Bechtle Schweiz)
Hasan Akzorba (Coop Pronto)
Beat Sommerhalder (HPE Aruba)

OFENHALLE

Cyberattacke: Was passiert, wenn der Ernstfall eintritt
Chris Bregenzer (Hawa Sliding Solutions AG)

STUBE

Quantencomputer und die Auswirkungen auf die digitale Sicherheit
Filip Vukadin (IBM Schweiz AG)

EVENTLOUNGE

Modern Meeting Demo-Center
Die neusten Lösungen, Trends & Technologien


bechtle