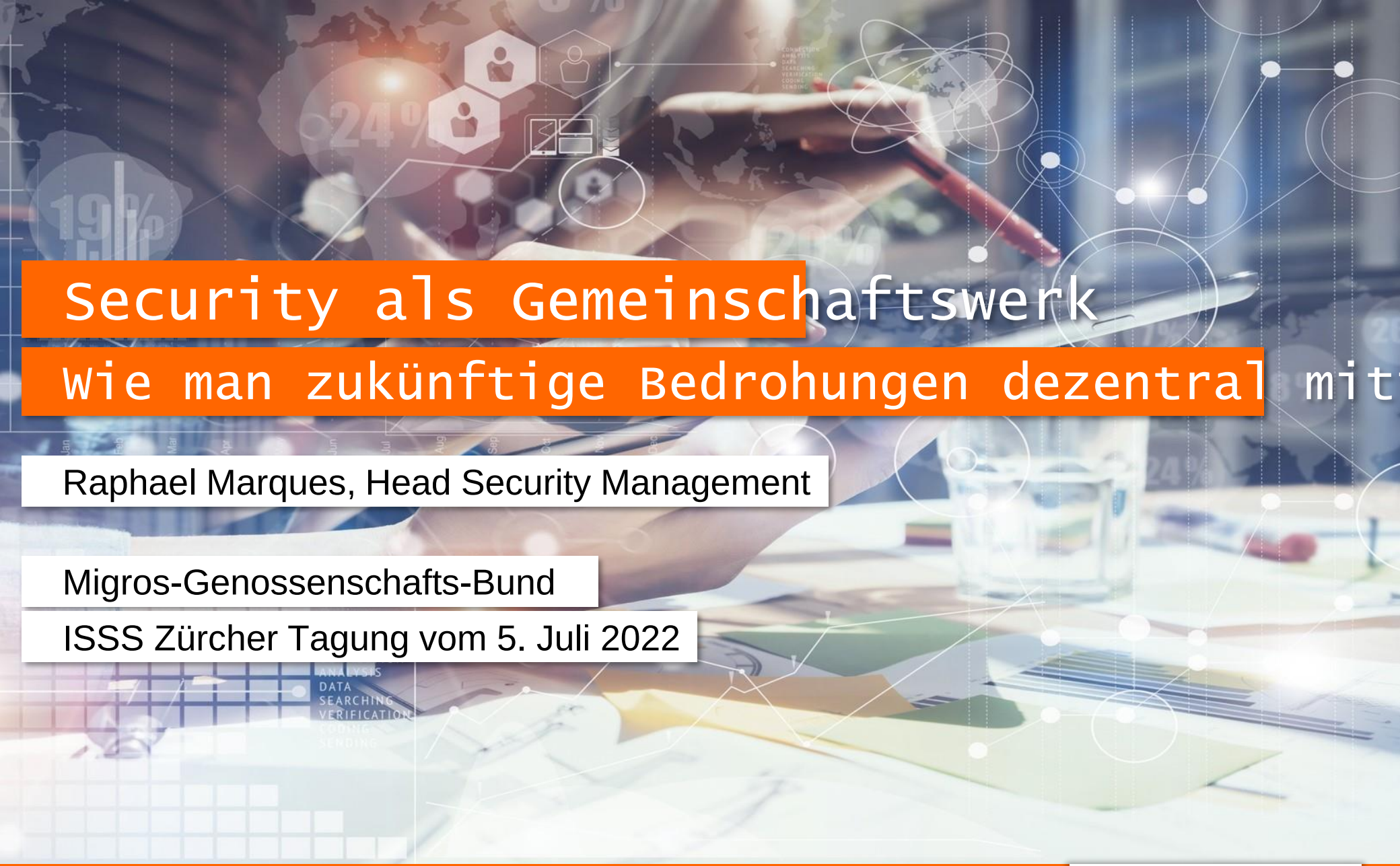


Security als Gemeinschaftswerk

Wie man zukünftige Bedrohungen dezentral mit

Raphael Marques, Head Security Management

Migros-Genossenschafts-Bund

ISSS Zürcher Tagung vom 5. Juli 2022

MIGROS

Referent - Raphael Marques

Head Security Management

Ausbildung & Zertifikate:

- CISSP Zertifiziert
- Bachelor of Science in Informatik Züricher Hochschule für angewandte Wissenschaften (ZHAW)

Hobbies

- Reisen, Fotografie, Squash

Leitung Security Management der MGB

- ISMS Aufbau
- Control Management Aufbau
- Security Regelwerk Aufbau
- Verantwortlicher Enterprise Security Architektur
- Verantwortlicher Security Consulting

Erfahrungen

- Consulting im Bereich Security
  - Umsetzung Security Projekte
  - Durchführung Security Assessments
  - Strategieberatung in der Informationssicherheit
- Security Spezialist (Analyst, Developer, Architekt) in einer Grossbank

Agenda

1. Die Anatomie eines föderalistischen Unternehmens
2. Herausforderung Security
3. Grundlagen für eine effektive Informationssicherheit
4. Etablierung «Security als Gemeinschaftswerk»
5. Erhöhung Reaktionsfähigkeit
6. Fragen

Die Anatomie eines föderalistischen Unternehmens

Die Migros – ein grosser Mischkonzern

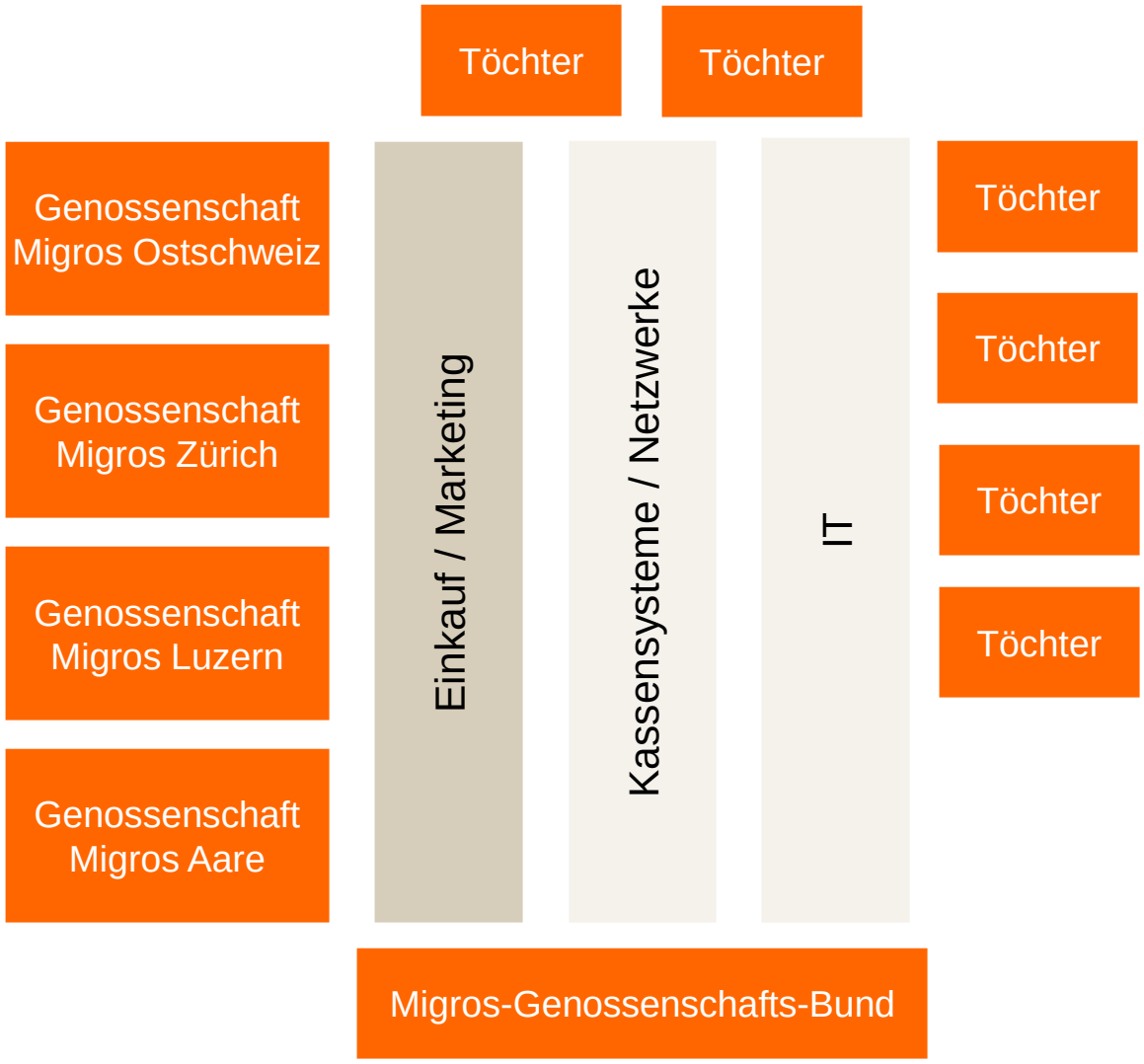
- Die Migros ist ein systemrelevanter Retailer der Schweiz
- Besitzt mehr als 3’500 Läden in der Schweiz
- Hat eine globale Präsenz von Kalifornien bis Japan

- **Ist einer der grössten Retailer der Schweiz physisch, wie auch online**

- Die Migros operiert in verschiedensten Feldern: vom Banking, Datenanalysen, Logistik, Medizinal Services, Fitness, Reisen, Detailhandel, Industrie und vieles mehr

Die Anatomie eines föderalistischen Unternehmens

Mehrwert durch Synergien

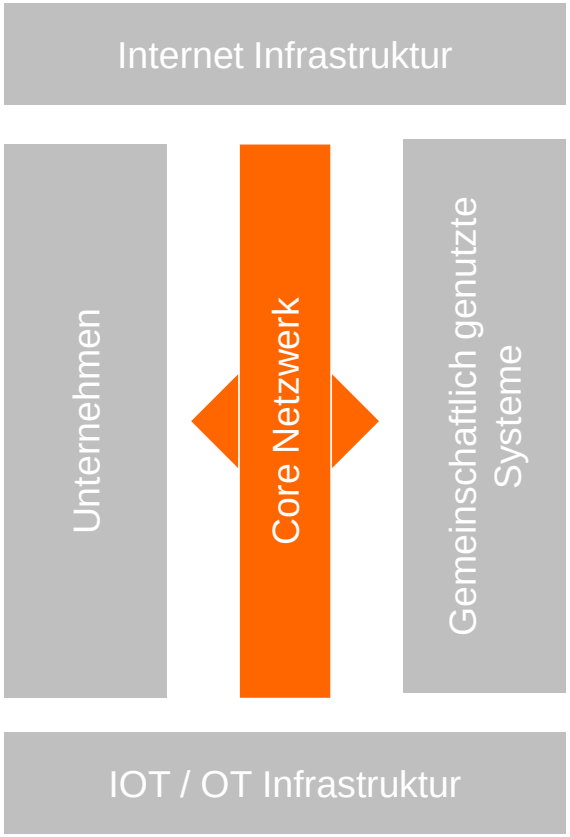


* 4 Genossenschaften stellvertretend für alle Genossenschaften

- Die Migros Gemeinschaft ist ein regional organisierter Verbund von Unternehmen
- Die Genossenschaften der Migros agierten in der Vergangenheit sehr autonom
- Durch die Nutzung von Synergien konnten die Genossenschaften Effizienz und Mehrwert schaffen - zuerst im Einkauf und dem Marketing und in den letzten Jahren in der Technologie
- Auch Töchter nutzen diese Synergien – sofern für sie sinnvoll

Die Anatomie eines föderalistischen Unternehmens

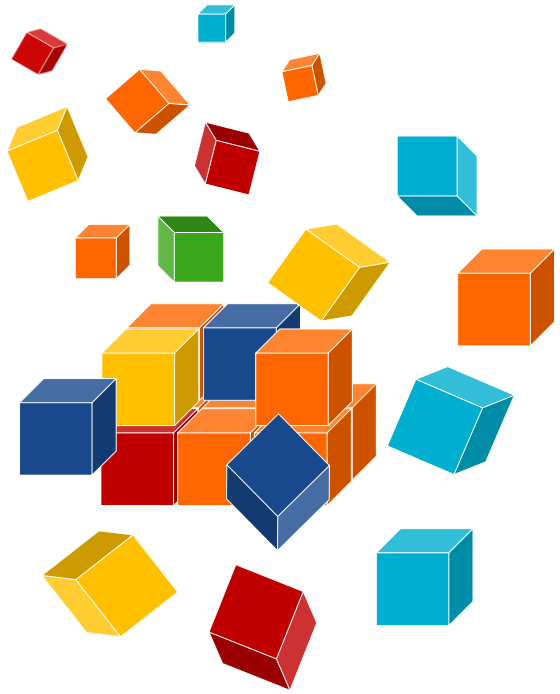
Komplexität Netzwerk



- Durch das Verbinden der einzelnen Unternehmen entstand ein «Core Netzwerk»
- Dieses «Core Netzwerk» dient zum Transit von von diversen Daten aus diversen IT-Systemen in der ganzen Migros Gemeinschaft
- Das «Core Netzwerk» ist an sehr unterschiedliche Netze mit unterschiedlichen Sicherheitsstufen angebunden
- Hunderte Entitäten sind am Core-Netzwerk angeschlossen und diese sind per Firewall mit einem Basisschutz versehen
- Die Unternehmensnetzwerke haben anschliessend eigene Infrastrukturen, unterschiedliche IOT/ OT Netze, usw.

Herausforderung Security

Heterogenität der Gemeinschaft



01 Die Migros Gemeinschaft betreibt nahezu alle IT-Systeme mehrfach – es gibt nicht «einen» Workplace oder Serverbuild.

02 Die verschiedenen Unternehmen in der Gemeinschaft sind sehr unterschiedlich fortgeschritten im Reifegrad der Sicherheit.

03 Verschiedene Unternehmen haben sehr unterschiedliche Use Cases – von einer Bank bis zu einer Bäckerfiliale. Es gibt keinen «One Size Fits All»-Approach.

04 Es gibt keine einheitlichen Betriebsmodelle oder Change-Prozesse.

Grundlagen für eine effektive Informationssicherheit

Verankerung in der Gemeinschaft

Explizite Definition des Geltungsbereiches

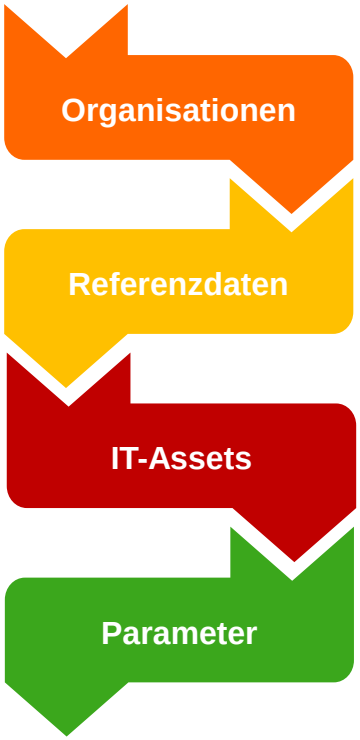
Definition des Frameworks wie Regeln der Security aufgestellt werden (Regelwerk)

Definition der Aufgaben Kompetenzen und Verantwortlichkeiten der Security Organisation

Definition der Disziplinen Risiko und Sicherheits-Management

Grundlagen für eine effektive Informationssicherheit

Know your assets



1. Um Transparenz in der Organisation herzustellen ist es essenziell, den Scope der Organisation genau auszuleuchten. Wer sind die Organisationen im «Scope»? Hat die Organisation Töchter? Ab welchem Beteiligungsgrad ist die Organisation in Scope?

2. Für die Organisationen im Scope müssen Referenzdaten erfasst werden. Wie gross ist die Organisation? Was sind die wichtigsten Prozesse der Organisation? Auf was für «Spezialitäten» muss man achten?

3. Basierend auf dem Scope müssen alle IT-Assets erfasst werden: Applikationen, IT-Systeme, Middleware, Netzwerkkomponenten, Domänen, …

4. Versionen und Parameter der Assets müssen für spezifische Cases erfasst und gepflegt werden.

Ohne die Assets zu kennen ist Security nicht effektiv möglich!

Etablierung «Security als Gemeinschaftswerk»

Grundlegende Organisation der Security

CU Security&Risk

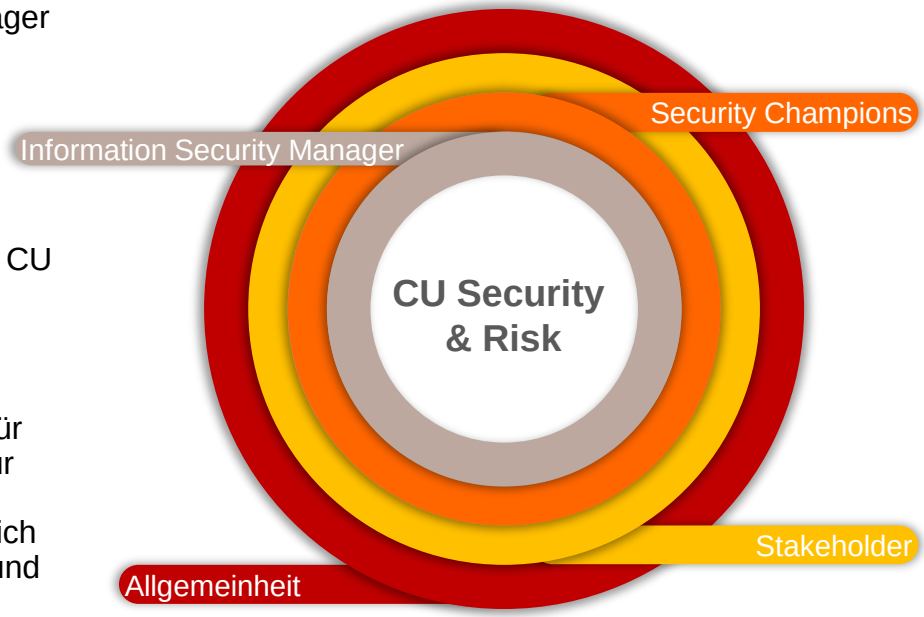
Die CU Security & Risk ist die zentrale Abteilung, welche alle Tätigkeiten koordiniert und die Inhalte für die dezentralen Stakeholder erarbeitet und diese unterstützt in der Umsetzung. Die restlichen Rollen sind alle lokal in den Unternehmen.

Information Security Manager

Die Information Security Manager (ISM) sind der Rückgrat einer effektiven Security. Die Information Security Manager koordinieren die Informationssicherheit im jeweiligen Unternehmen und arbeiten eng mit der zentralen CU Security&Risk zusammen

Allgemeinheit

Alle Mitarbeiter sind relevant für die Security. Jeder, der sich für Security interessiert soll sich aktuell halten können. Zusätzlich wird grossflächig Awareness und Security-Kultur gefördert.



Security Champions

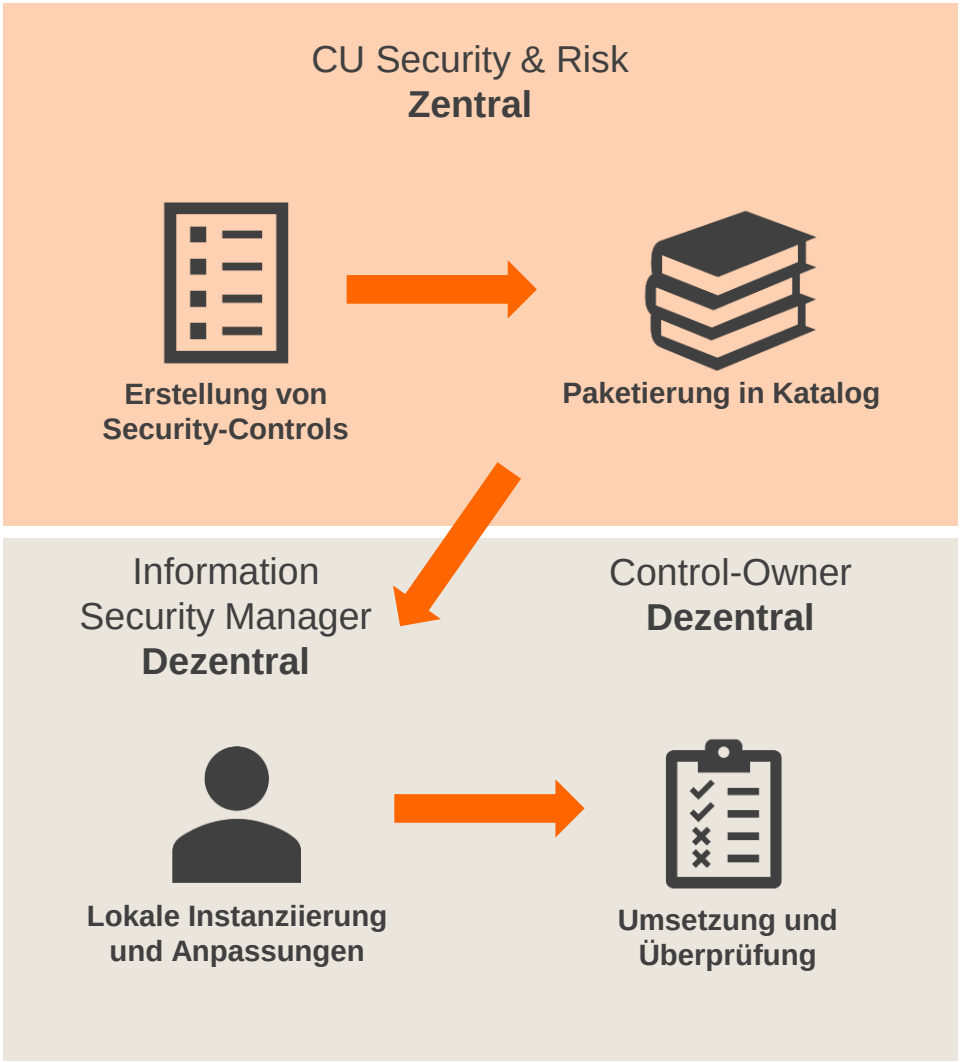
Die Security Champions sind Mitarbeiter mit spezieller Security Verantwortung. Hierzu zählen zum Beispiel Solution Architekten, Engineers, Netzwerk Spezialisten usw.. Diese Personen haben einen grossen Impact auf die tatsächliche Sicherheit.

Stakeholder

Weiter gibt es verschiedenste andere Stakeholder die – auch dezentral – abgeholt werden müssen. Hierzu gehören das Management, Kommunikation, Enterprise Architektur, Finanzen, usw.

Etablierung «Security als Gemeinschaftswerk»

Sicherstellung von Transparenz mit einem Control Management und ISMs



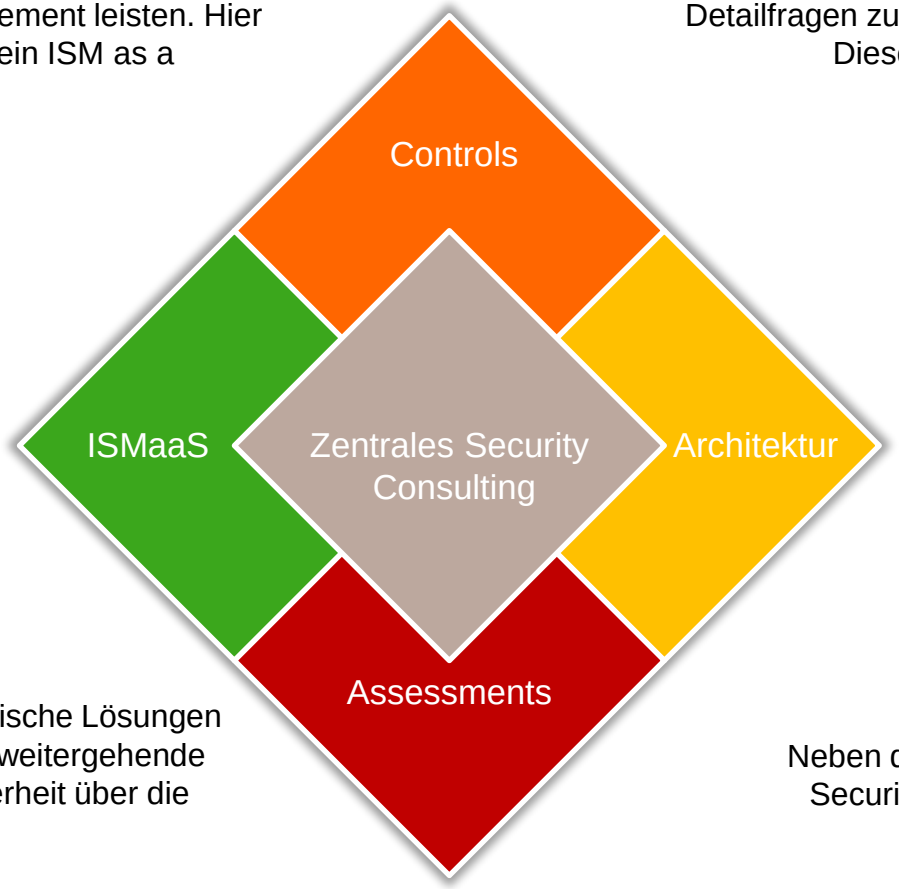
- Die CU Security & Risk erstellt zentral die Inhalte in Form von Controls und paketiert diese in Kataloge (z.B. ITGC, Grundschutz, ISMS, …)
- Der Information Security Manager übernimmt die Kataloge lokal und hat die Möglichkeit den Katalog anzupassen für das jeweilige Unternehmen
- Der Information Security Manager definiert die Control-Owner pro Control, welche im Anschluss diese umsetzen und überprüfen
- Optional kann ein separater Control Assessor eingesetzt werden um die umgesetzten Controls zu überprüfen

Etablierung «Security als Gemeinschaftswerk»

Unterstützung durch Consulting

ISM as a Service
Kleine Unternehmen können sich keine dedizierte Ressource für Security Management leisten. Hier bietet das zentrale Consulting ein ISM as a Service Angebot an.

Control Support
Bei der Controlumsetzung stellen sich oft Detailfragen zur Interpretation und Best Practices. Diese Unterstützung bietet das zentrale Consulting an.

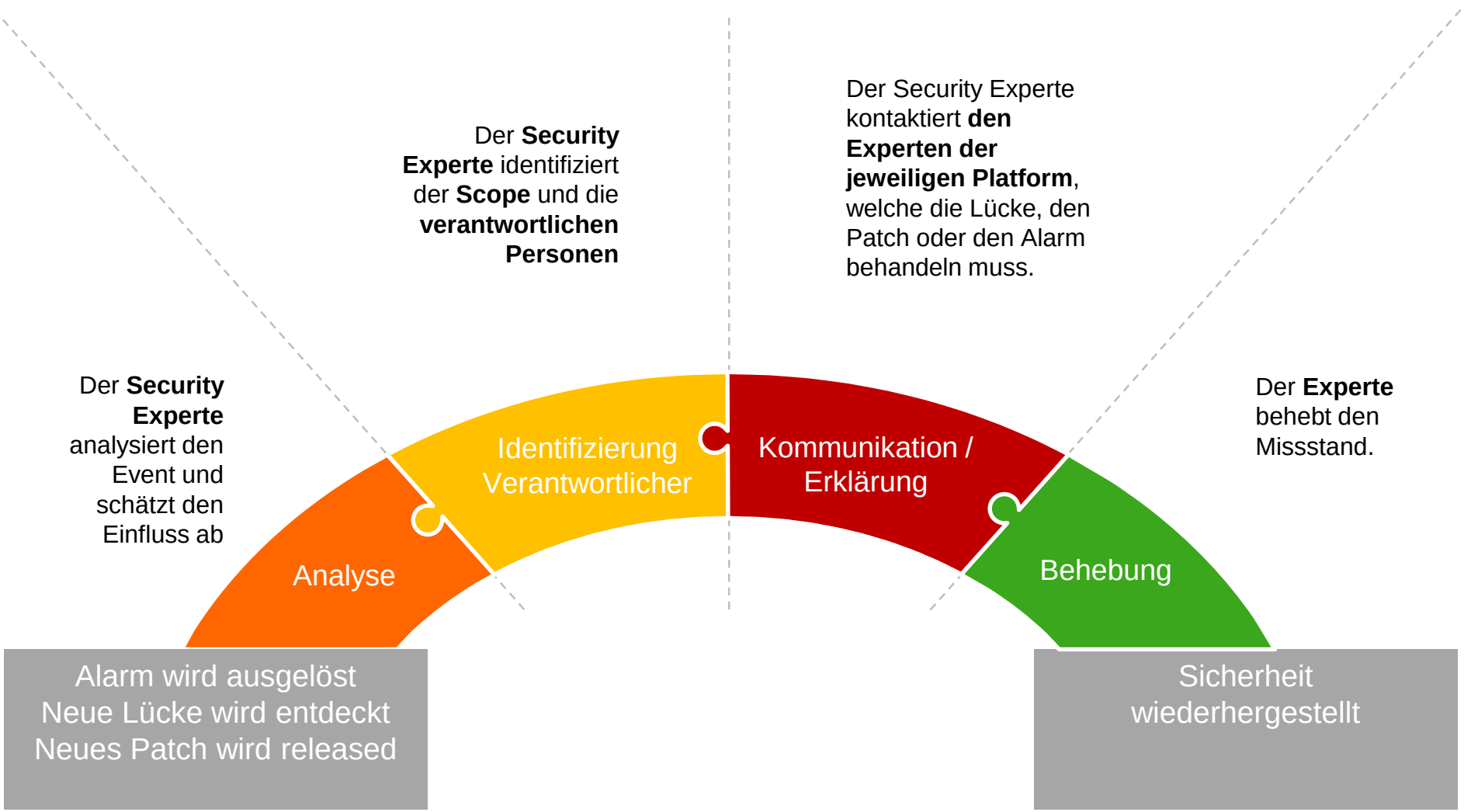


Assessments
Für sensitive oder businesskritische Lösungen bietet das zentrale Consulting weitergehende Unterstützung an um die Sicherheit über die Baseline sicherzustellen.

Architektur
Neben der Erfüllung der Controls bietet die Security Architektur Unterstützung an um Security-By-Design sicherzustellen

Erhöhung Reaktionsfähigkeit

Informationsflüsse in einer traditionellen Security

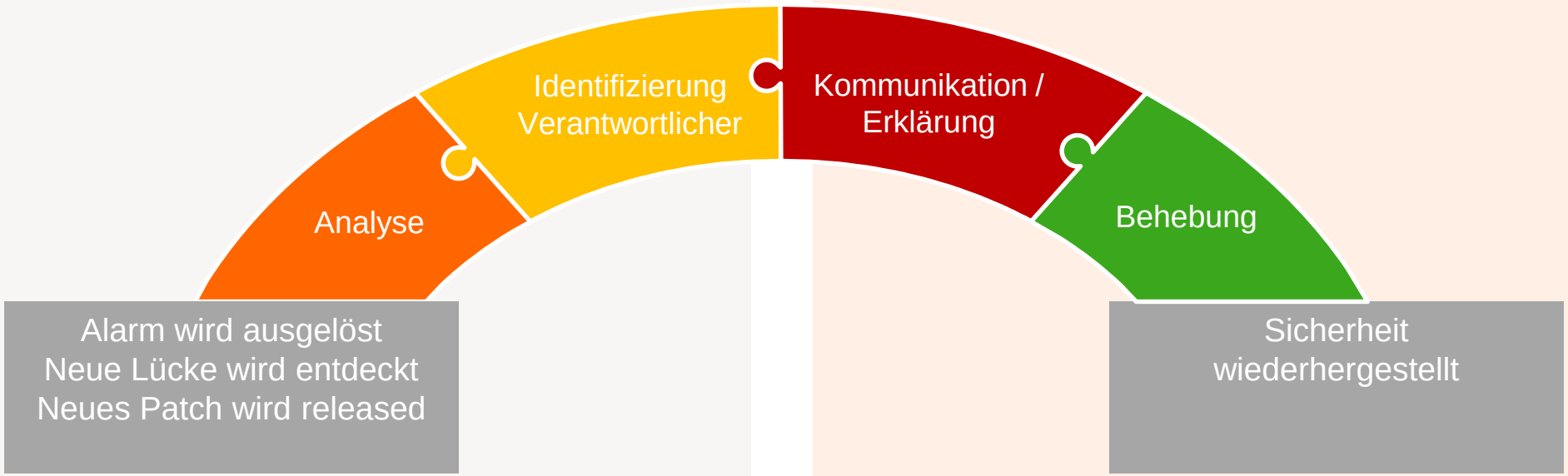


Erhöhung Reaktionsfähigkeit

Security Champions – die Schlüssel zum Erfolg

- Kann durch SOAR Automatisiert werden um schneller Informationen und Aktionen zu triggern
- Der Security Champion muss im Normalfall die Mitigation-Aktion ausführen
- Je direkter «Security Champions» Security Informationen konsumieren kann, desto schneller die Reaktion

- Durch Training und Schulung kann der Security Champion Informationen direkt konsumieren
- Aktionen können sofort dezentral umgesetzt werden
- Je besser das Training der Security Champions ist, desto schneller und wahrscheinlicher wird die richtige Aktion zur Behebung durchgeführt



Erhöhung Reaktionsfähigkeit

Training & Enablement von Security Champions

Engineers

- Know-How Verbesserung in Secure Coding
- Showcases von Exploits und Hacks um Awareness zu verbessern
- Verbesserung der Development Pipeline mit automatisierten Security-Checks
- Zugang zu Exploit Daten

System Operators

- Secure Operations und Deployment
- Produktspezifische Security Know-How Verbesserung
- Showcases von Hacks um Incidents besser zu identifizieren
- Schulung im Regelwerk
- Zugang zu Exploit & Incident Daten

Solution Architects

- Schulung im Regelwerk
- Security-By-Design Know-How
- Gemeinsame Erarbeitung von Security-Patterns und –Standards
- Schulung Security Konzepte (Zero-Trust, …)

Management

- Showcases von Hacks um Awareness zu verbessern
- Transparenz herstellen mit Reporting

Migros Security Awareness
Enablement für alle

Fragen?