oneconsult
together against cyberattacks

IoT Security

Tales from the real world

Erfahrungsbericht über Verwundbarkeiten, Fehler und Schutzmassnahmen

Jan Alsenz, Head of Innovation , 7. März 2023

Jan Alsenz

Head of Innovation

Oneconsult AG

Principal Penetration Tester,
Security Consultant & Researcher

MSc ETH CS

OPST & OPSA

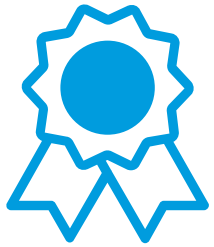
Oneconsult
Über uns

2'000+
Cybersecurity-Projekte

Oneconsult-Unternehmensgruppe:
Oneconsult International AG (Holding),
Oneconsult AG,
Oneconsult Deutschland AG,
Oneconsult New Zealand Limited

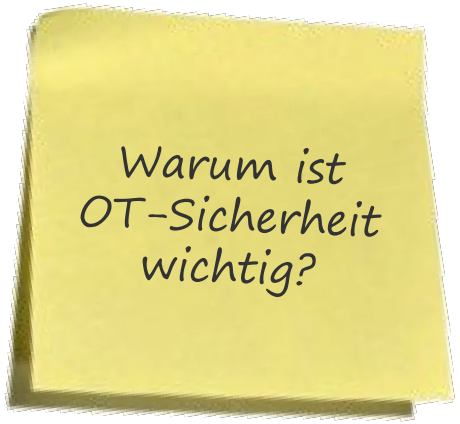
100+
Red-Teaming-Projekte

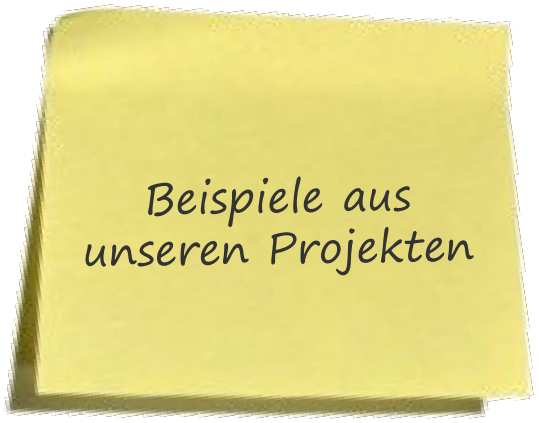
250+
Incident-Response-Einsätze

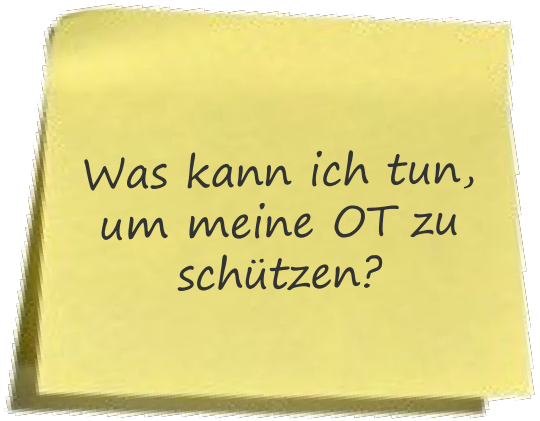


Inhabergeführt seit 2003

Erwartungen

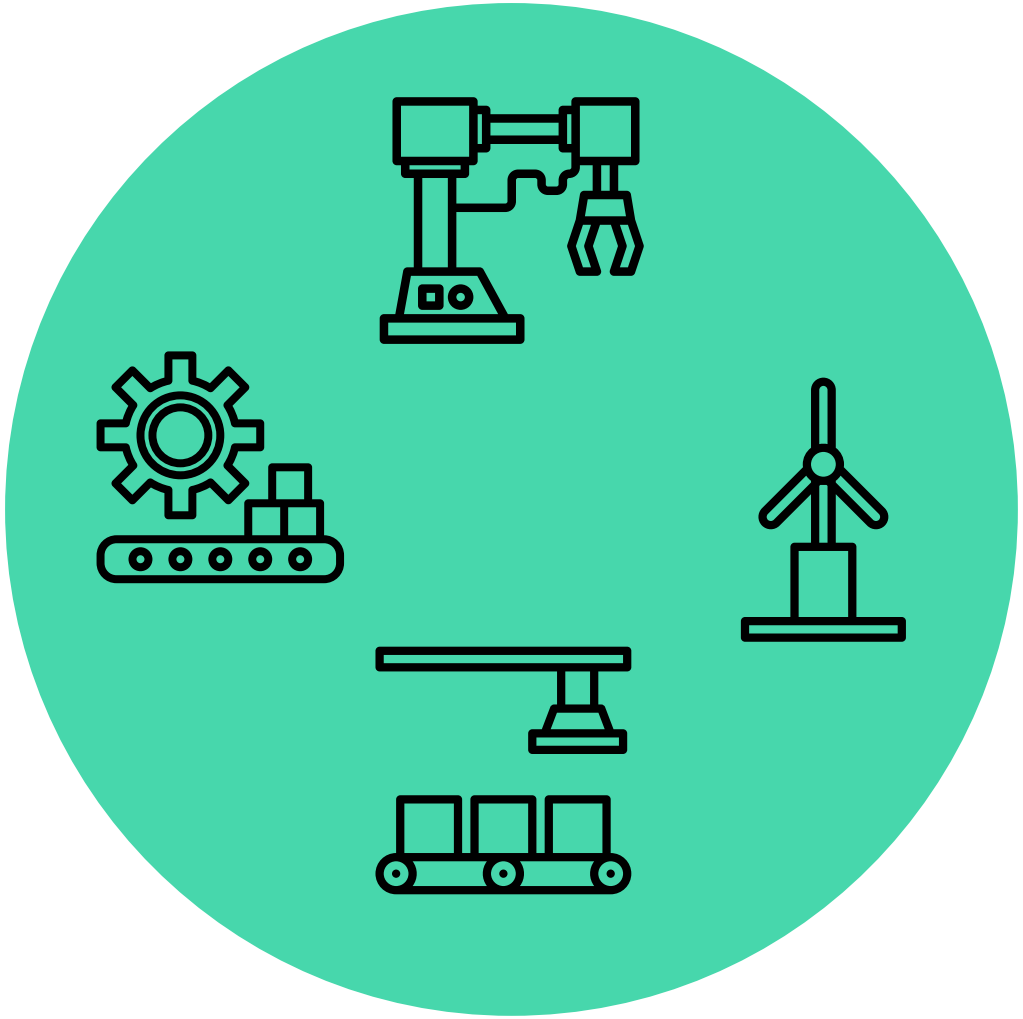






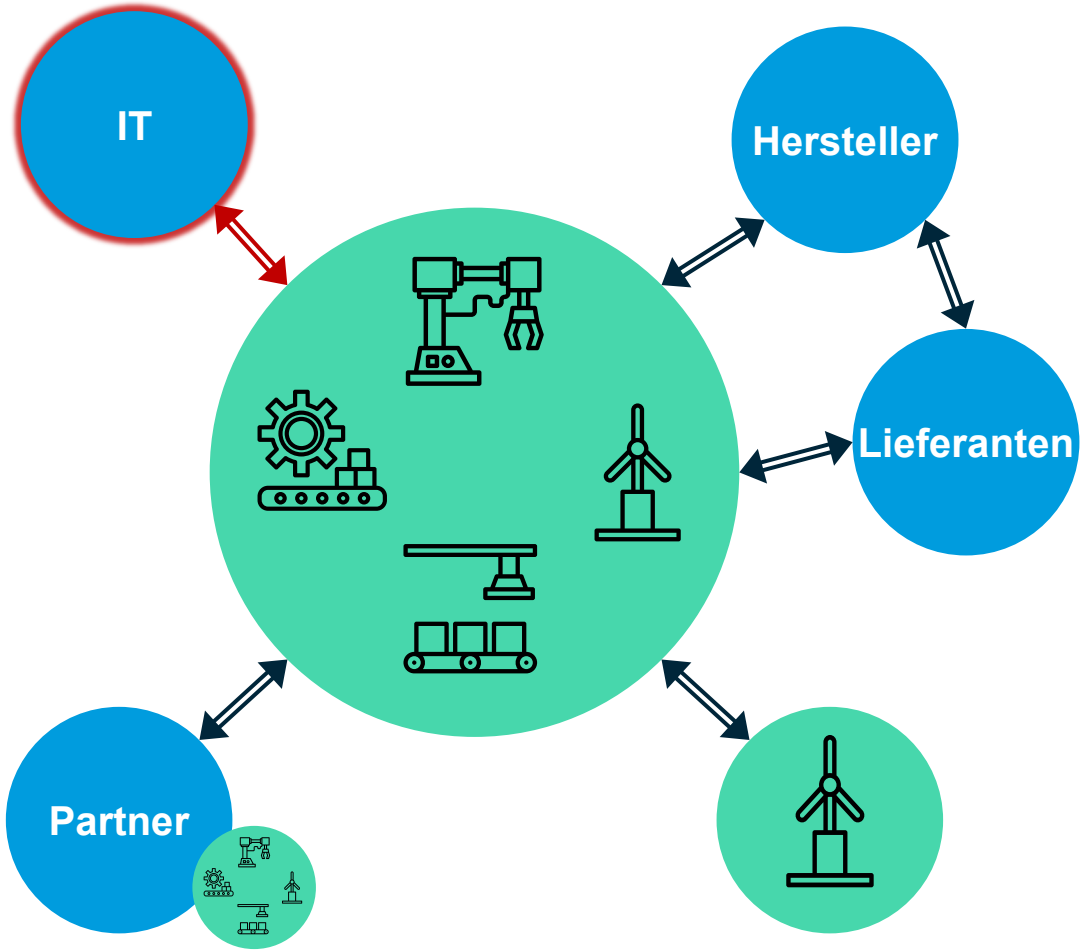
OT Sicherheit in der Praxis
Was sind die Risiken?

OT Netze sind unsicher



- Lange Lebensdauer
- Zertifizierung & Safety
- Hersteller & Lieferanten
  - Fehlendes Bewusstsein
  - Alte Plattformen
  - Keine Security Prozesse
- Verfügbarkeitsanforderungen
- Rückwärts-Kompatibilität
- Historische Strukturen
  - Elektrik & Elektronik vs. IT
  - Keine Sicherheitsanforderungen

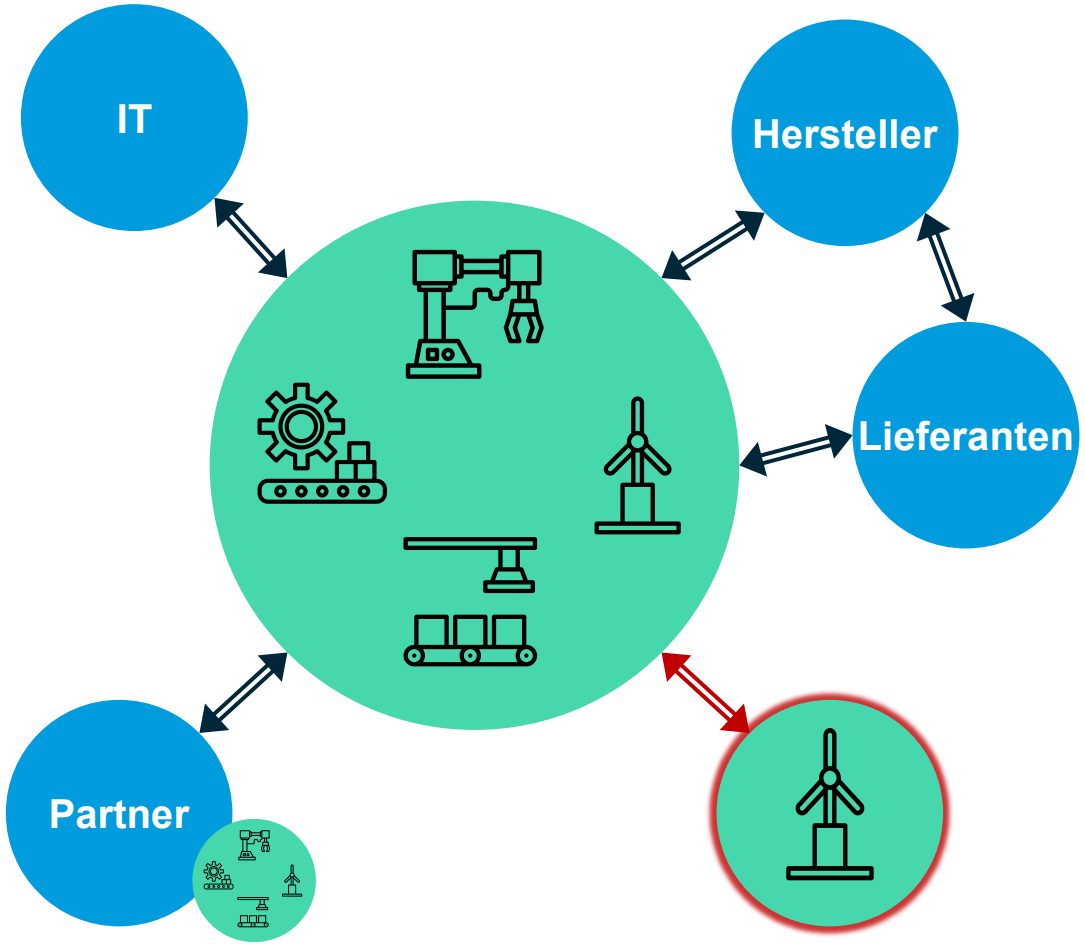
OT Netze sind verbunden



IT:

- ERP / EWM
- Datenaustausch
- Wartung & Betrieb
  - Updates
  - Administration
  - Fernzugriff
- Geteilte Systeme
  - VoIP Telefone
  - Alarmanlage
  - Videoüberwachung
  - Schliesssysteme
  - Drucker

OT Netze sind verbunden



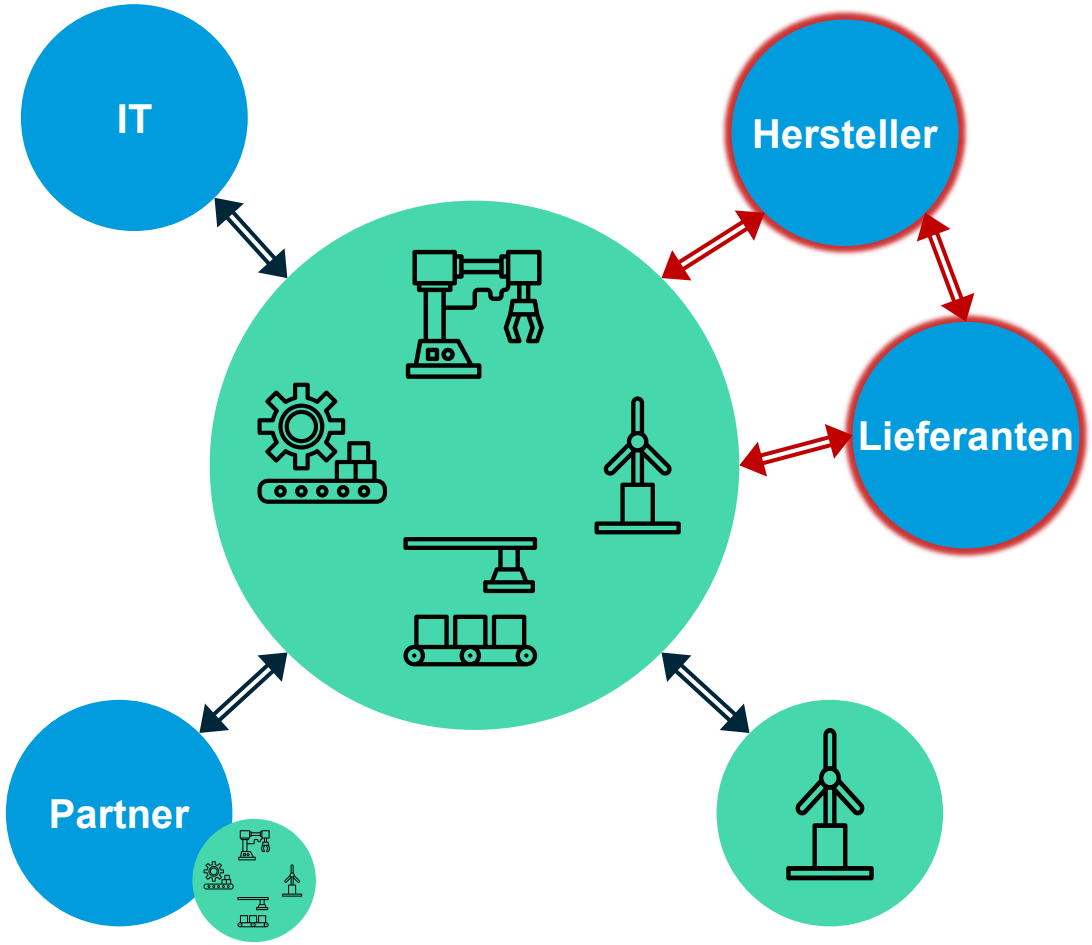
Verteilte Infrastruktur:

- Aussenstandorte
- Verteilte Anlagen

Verbindungen:

- Glasfaser
- Richtfunk
- (DSL-)Kabel

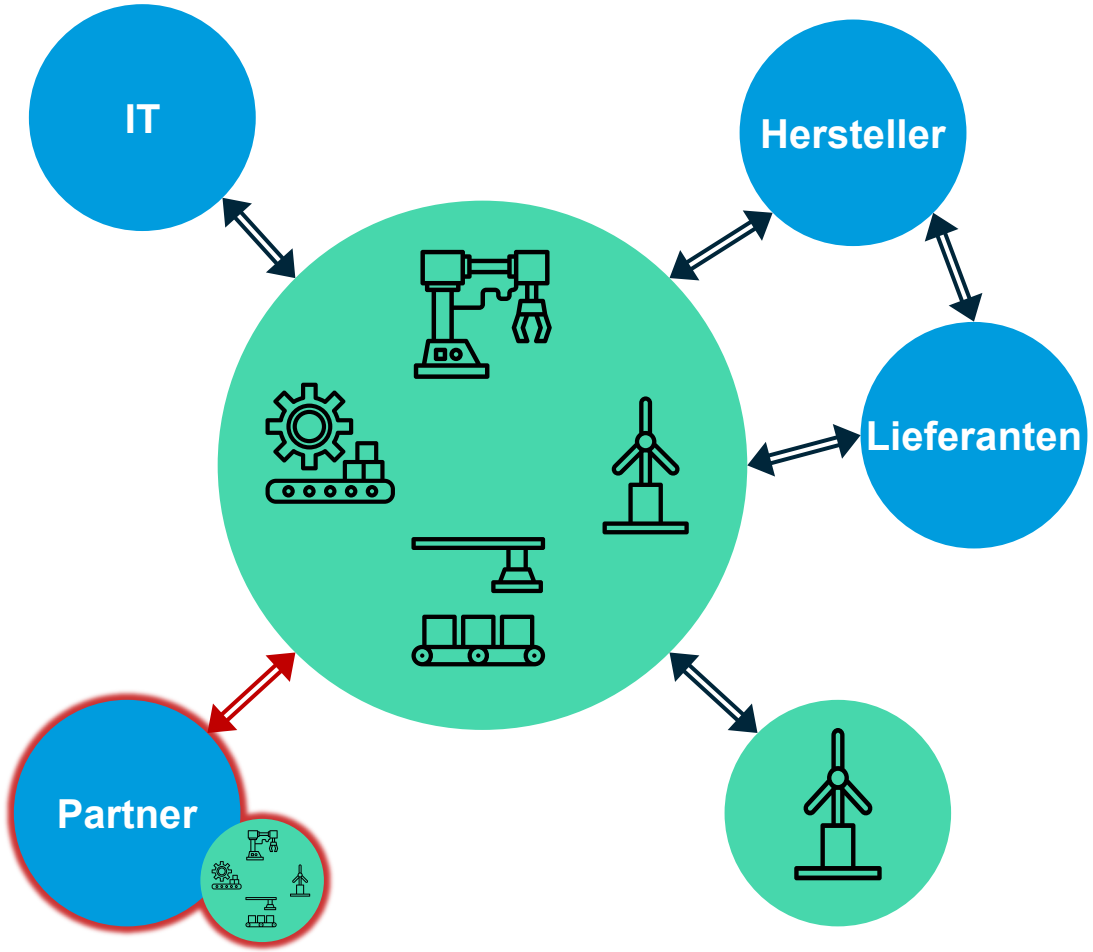
OT Netze sind verbunden



Hersteller & Lieferanten:

- Fernwartung
- Datenübermittlung
- Updates
- Techniker-Rechner

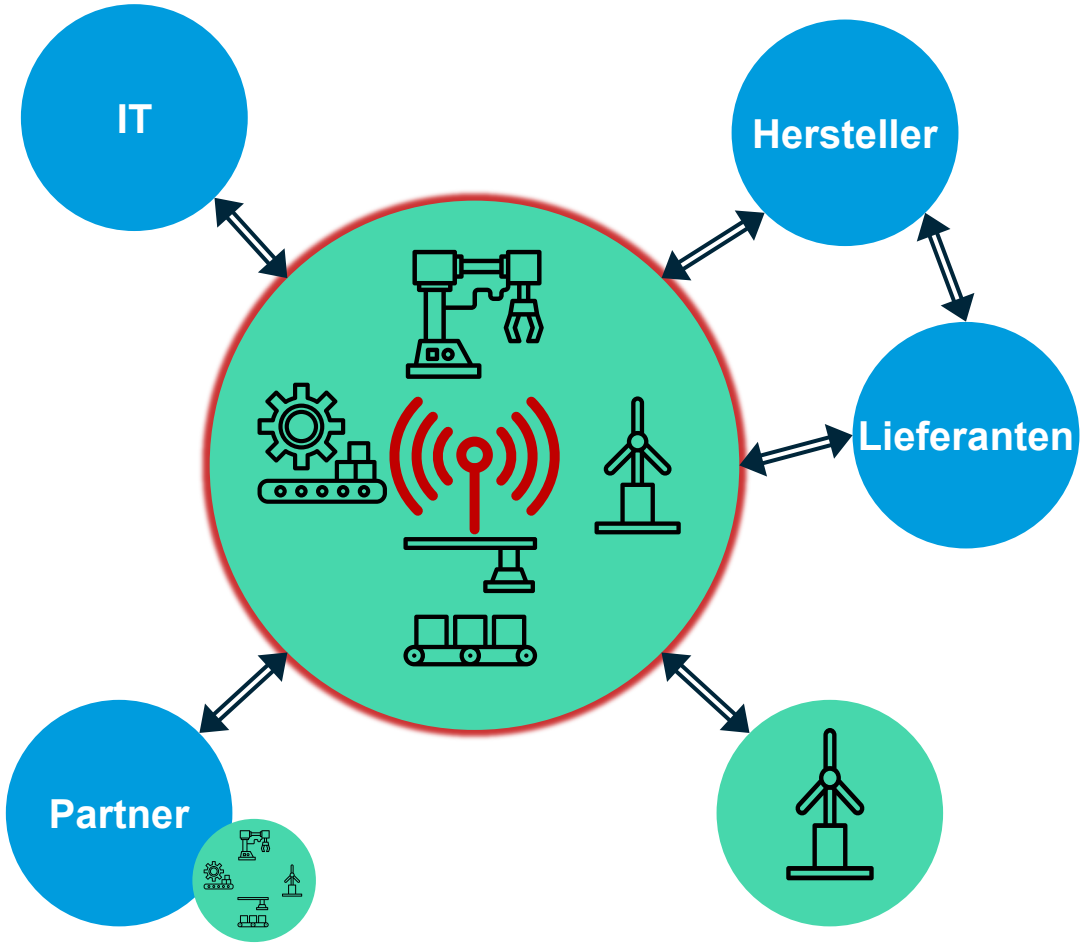
OT Netze sind verbunden



Partner:

- Verwandte Firmen
- Produkte-Zulieferer/-Abnehmer
- Aufsichts- / Kontrollbehörden
- Koordinationsstellen

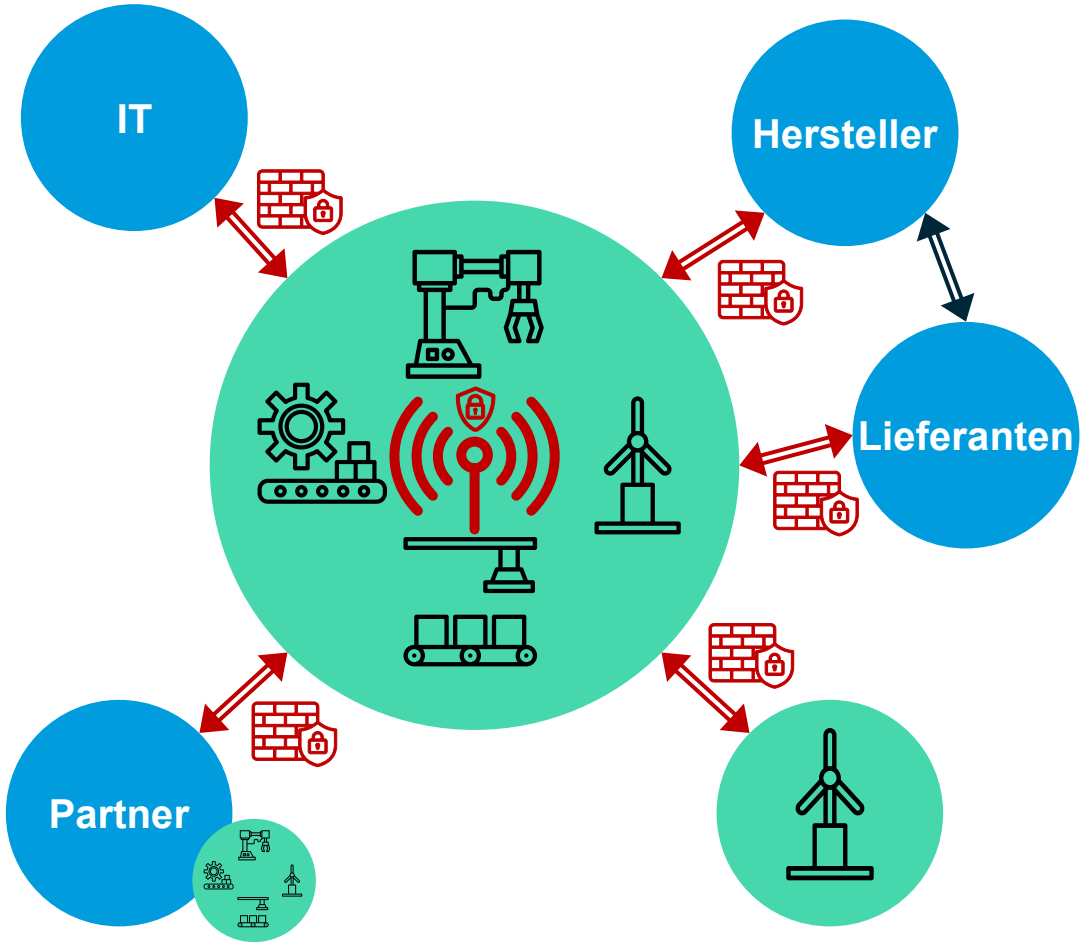
OT Netze sind auch in der Luft



- WLAN
  - Handhelds (z.B. Scanner)
  - Fahrende Roboter
  - Wartung / Laptops
- Andere
  - RFID
  - Funkfernsteuerungen
  - Betriebsfunk

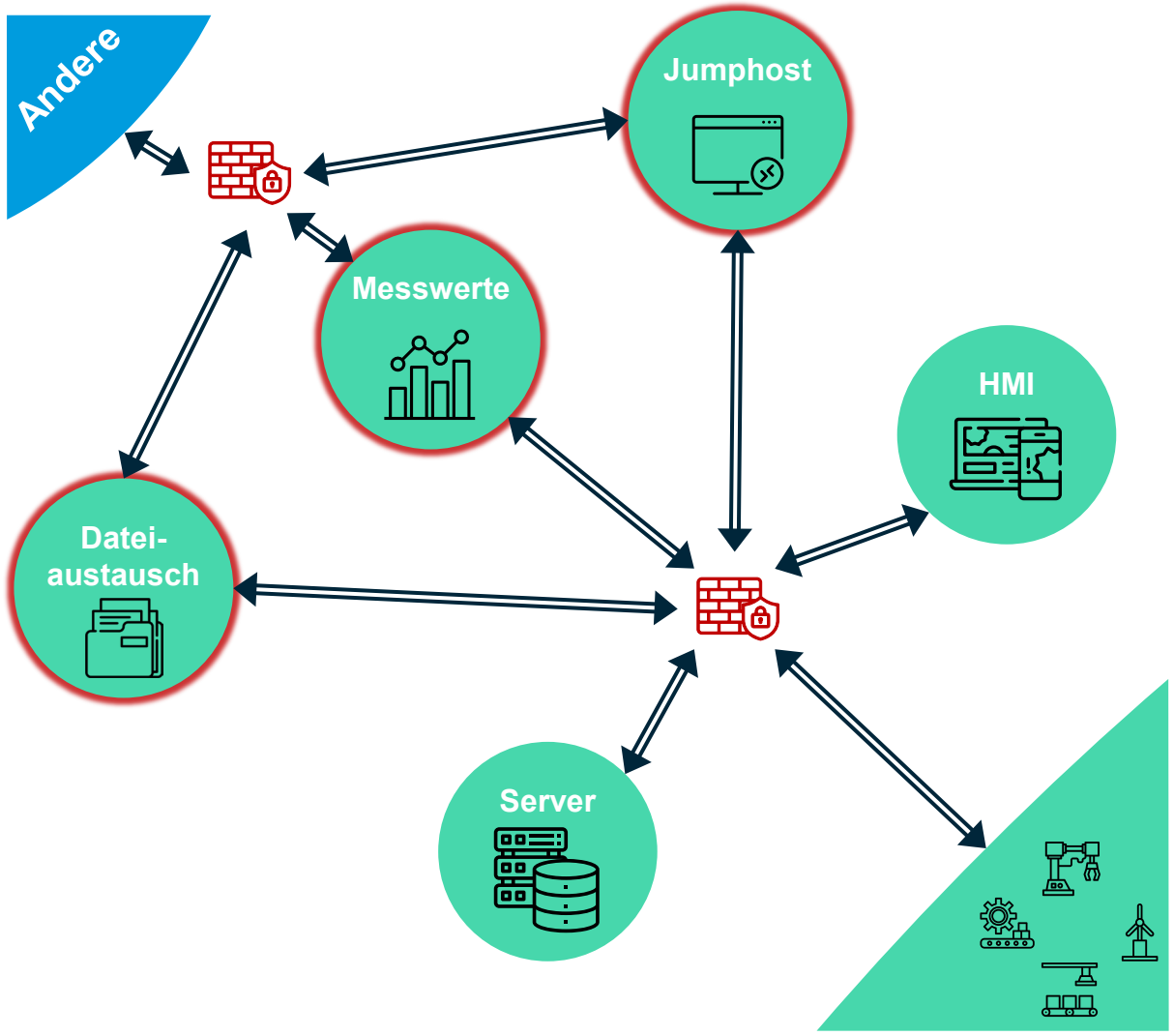
Schutzmassnahmen
aber richtig

Zugänge und Zugriffe schützen



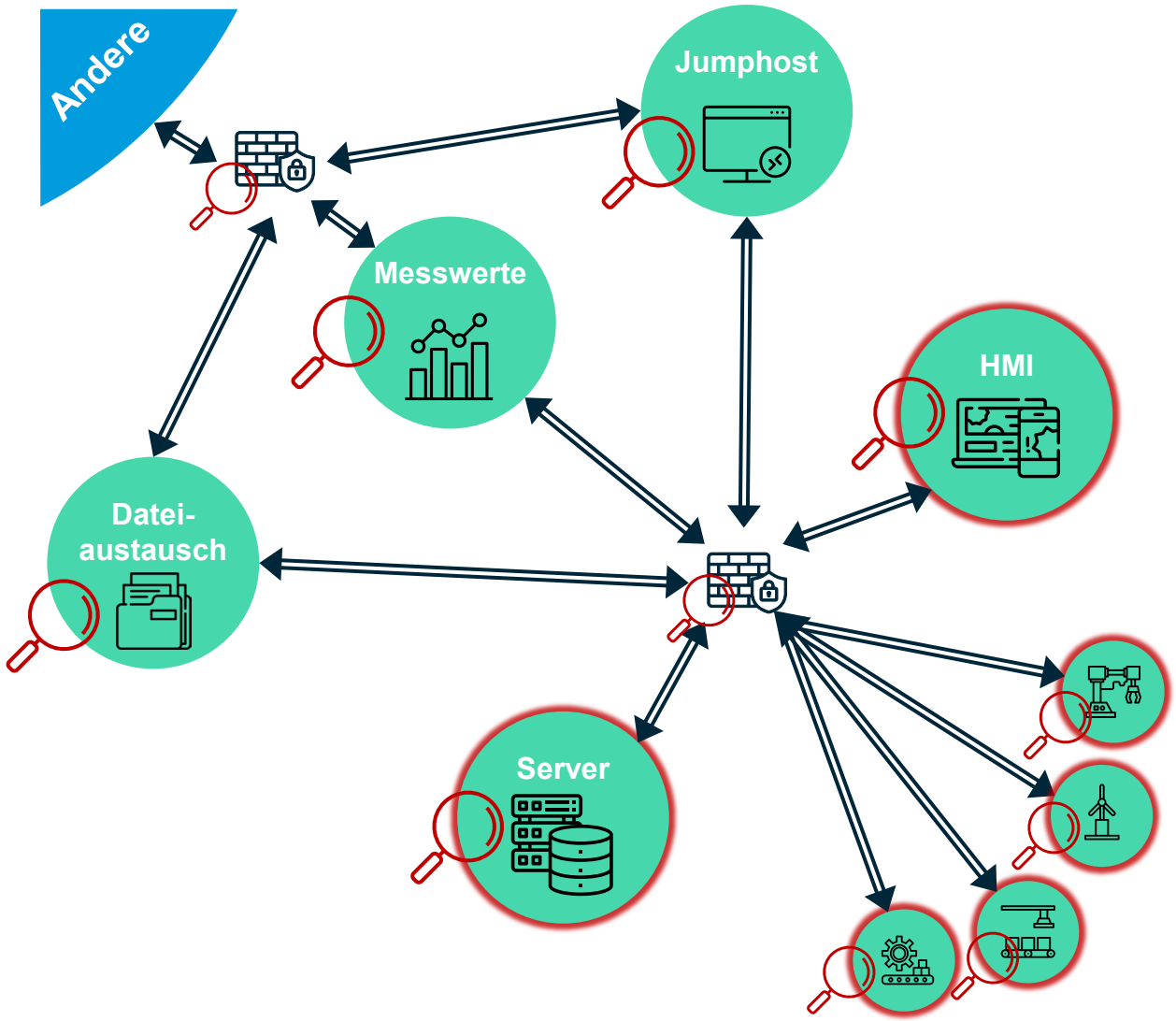
- Keine direkten Verbindungen aus dem Internet
- Wenn möglich keine direkten Verbindungen aus irgendwelchen anderen Netzwerken
- Alle Verbindungen über Firewalls unter eigener Kontrolle
- Überland Verbindungen nur verschlüsselt
- Keine nicht-standard Funkverbindungen
- Alle Standard Funkverbindungen verschlüsselt
  - WPA2+
    - EAP
    - mind. PSK mit zufälligem Passwort

Schützen – aber richtig



- OT-DMZ(s)
  - Protokollbruch
  - Jumphost
- Vorsicht bei Firewall-Auswahl (Verfügbarkeit!)
- Master muss OT sein
  - Administration
  - Berechtigungen
  - Authentisierung (2-Faktor)

Massnahmen innerhalb von OT



- (Micro) Segmentierung
- Überwachung
- Regelmässige Updates

Vielen Dank!

Jan Alsenz

Head of Innovation
Oneconsult AG

+41 43 377 22 30
jan.alsenz@oneconsult.com

Let's connect

www.oneconsult.com

/oneconsult-ag

/OneconsultAG

/oneconsult

Monatliche Cybersecurity News abonnieren:

Oneconsult Newsletter

Kontakt

Holding

Oneconsult International AG
Giesshübelstrasse 45
8045 Zürich
Schweiz

+41 43 377 22 22
info@oneconsult.com

Schweiz

Oneconsult AG
Giesshübelstrasse 45
8045 Zürich
Schweiz

+41 43 377 22 22
info@oneconsult.com

Oneconsult AG
Aarbergergasse 56
3011 Bern
Schweiz

+41 31 327 15 15
info@oneconsult.com

Deutschland

Oneconsult Deutschland GmbH
Agnes-Pockels-Bogen 1
80992 München
Deutschland

+49 89 248820 600
info@oneconsult.com

Neuseeland

Oneconsult New Zealand Limited
Level 3, 33-45 Hurstmere Road
Takapuna, Auckland 0622
New Zealand

+64 27 325 4299
info@oneconsult.com