A1 Digital

Man kann nur schützen, was man kennt!

Risikomanagement und Schwachstellenerkennung für IoT Systeme

it-sa 2024

Holger Hartwig

A1 Digital

Arne Trittelvitz

asimily

Was ist IoT?

IoT | Internet der Dinge | Allesnetz | Web of Things | M2M | Industrial Internet | ...

Technologien, die es ermöglichen,
Objekte miteinander zu vernetzen
und sie durch Informations- und
Kommunikationstechniken
zusammenarbeiten zu lassen.

(Wikipedia)

asimily

Nutzen und Risiken

Aus Anwendersicht

- Schneller, einfacher Einsatz
- Für spezifische Aufgaben
- Einfacher Netzwerkzugang
- Wenig Konfiguration nötig

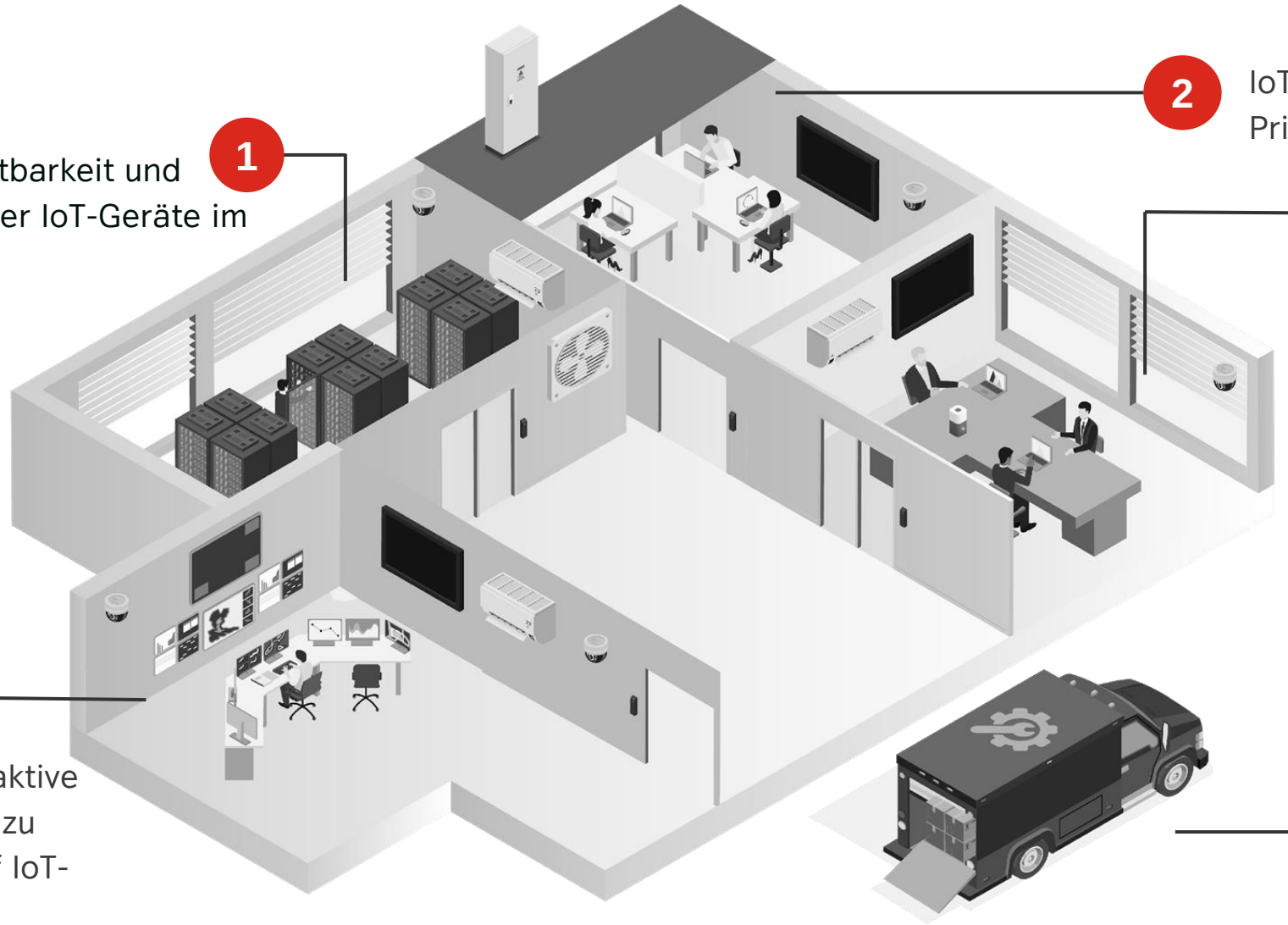
Aus Sicht der Security

- Oft ohne Wissen der IT
- Keine vollständige Asset-Verwaltung
- Keine aktive Überwachung
- Verändertes Verhalten wird nicht erkannt

Auch IoT-Geräte haben Schwachstellen, die Angreifer ausnutzen können, um Angriffe auf das gesamte Netzwerk auszuführen. **Damit sind IoT-Geräte ein ernstes Sicherheitsrisiko.**

A1 Digital

Anforderungen durch IoT Einsatz



1 Fehlende Sichtbarkeit und Transparenz der IoT-Geräte im Netzwerk

2 IoT-Geräte besitzen keine Priorität in der IT

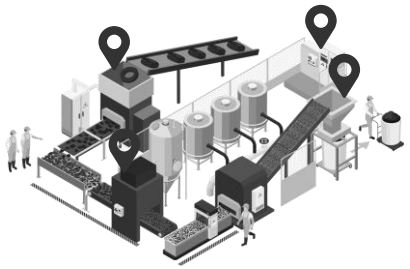
3 Das Risiko durch IoT ist schwer zu definieren und zu messen

4 Es gibt keine aktive Überwachung zu Anomalien auf IoT-Geräten

5 IoT-Geräte von Dritten im eigenen Netzwerk

asimily

Was sich verbessern muss



Bestandsaufnahme

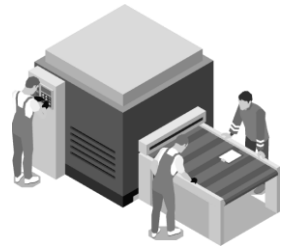
Detaillierte Informationen über IoT-Geräte und ihre Eigenschaften in Echtzeit

Risikoverringerung

Schwachstellenerkennung und Modellierung der kleinsten Risikos

Sicherheitsvorfälle

Anomalien erkennen und schnell und zielgerichtet reagieren



Verwaltung

Wirtschaftlichen Nutzen und Auslastung der IoT-Geräte optimieren

Asimily – der bessere Weg

Vollständige Transparenz zu Geräten und Risiken

Effizientes Schwachstellen-management

Agile Reaktion auf Sicherheitsvorfälle

- Automatische Ermittlung des tatsächlichen Gerätebestandes inkl. Klassifizierung
- Verkürzt Sicherheitsüberprüfungen, durch Best-Practice Empfehlungen zur Härtung
- Alle früheren und aktuellen CVEs, Konfigurationen und Angriffe, werden zur Priorisierung verwendet
- Intelligente Priorisierung zur Beseitigung der größten Risiken von den wichtigsten Geräten
- Kontinuierliche Überprüfung auf Richtlinienverstöße basierend auf jede erkennbare Interaktion
- Reduziert Kosten, Aufwand und Zeit für die Bearbeitung von Sicherheitsvorfällen

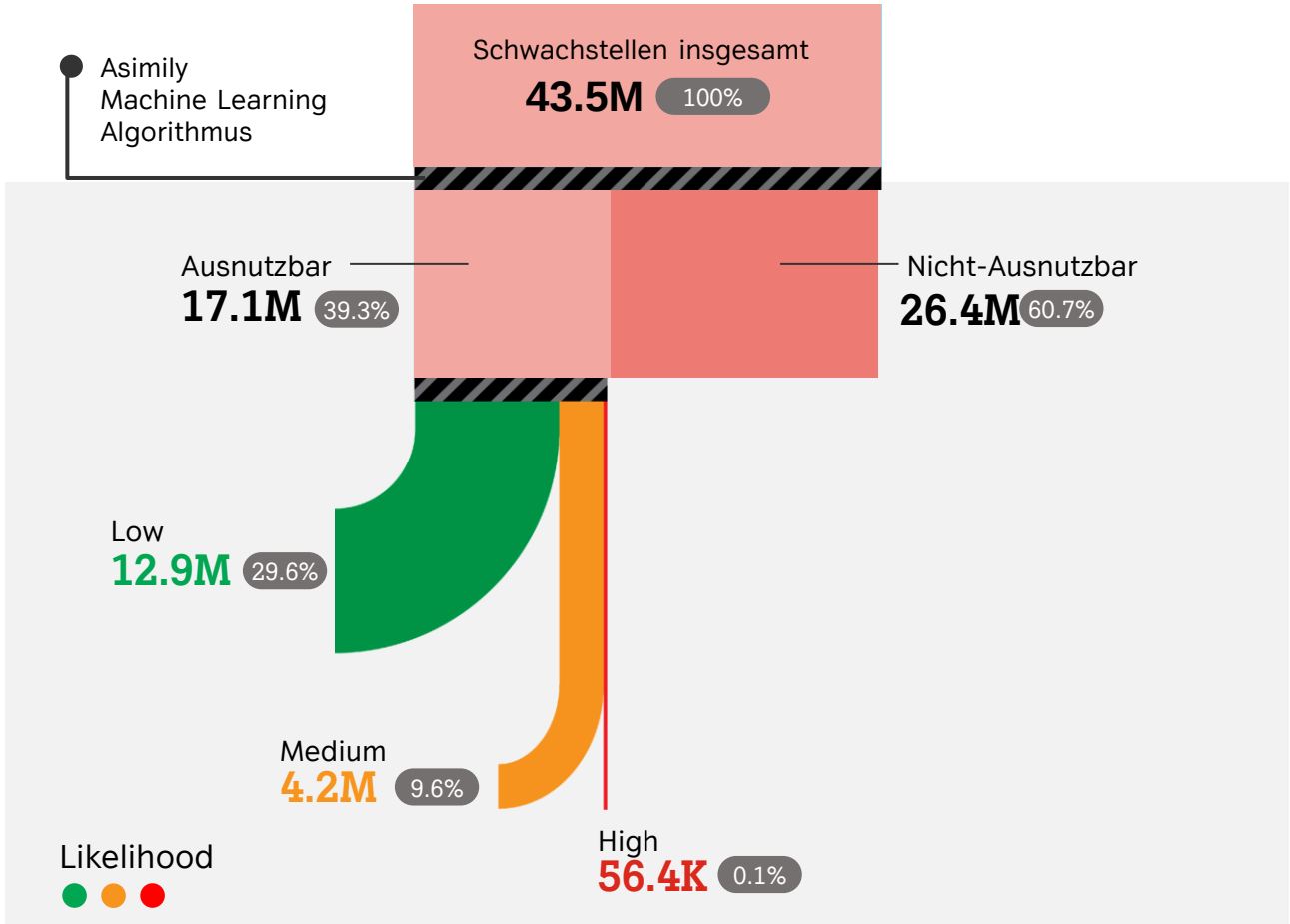
asimily A1

Schwachstellen priorisieren

Öffentliche Daten zur Anfälligkeit

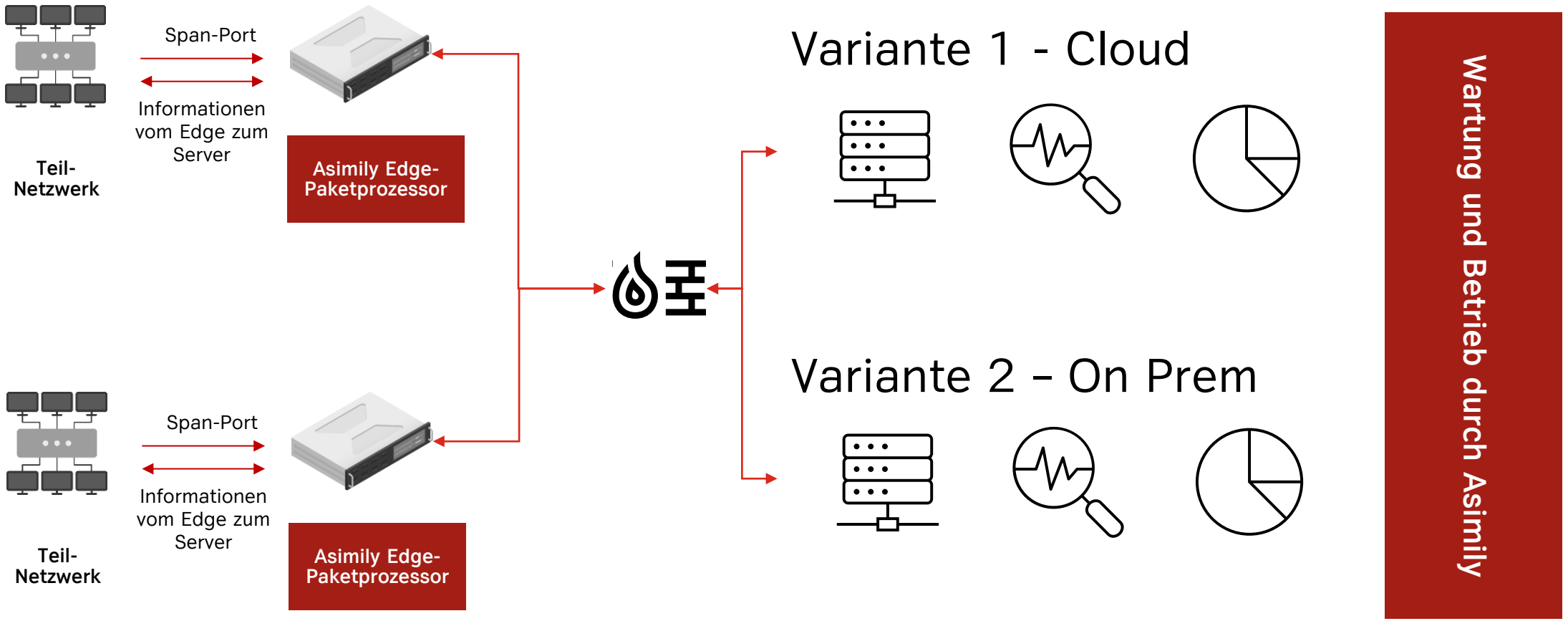
Asimilys patentierte Priorisierungs-Engine

+ MITRE ATT&CK Framework
+ MDS2
+ EPSS
+ SBOMs
+ Gerätekonfiguration in der Umgebung



A1 Digital

Einfach in Implementierung und Betrieb



Geschützte Daten verlassen niemals das Netzwerk des Kunden

asimily A1

Warum Kunden Asimily wählen

Risikominderung	Reaktion auf Vorfälle	Geräteverfügbarkeit
✓ Aussagekräftige Risikomatrix ✓ Priorisierung der Maßnahmen um Risiken schneller zu minimieren ✓ Simulation der Risiken von Geräten erhöht die Planbarkeit von Neubeschaffungen	✓ Anomalien erkennen und reagieren ✓ Für eigene IoT-Geräte und IoT-Geräte von Dienstleistern und Dritten ✓ Mit Richtlinien die Ausbreitung von Schadsoftware verhindern	✓ Details zu Nutzung, Auslastung, Verfügbarkeit und Zuverlässigkeit ✓ Optimaler Einsatz durch Nutzungsanalysen ✓ Höhere Lebensdauer durch gezielte Beseitigung von Schwachstellen

Danke für Ihre Aufmerksamkeit

A1 Digital

asimily

Besuchen Sie uns auf der it-sa

Stand 7-633
Halle 7A

Oder online unter

www.a1.digital