AUCONET
Beta Systems Group

Was Du nicht kennst, kannst Du nicht beschützen

Gerd Gruner, Auconet GmbH
Head of Presales and Support

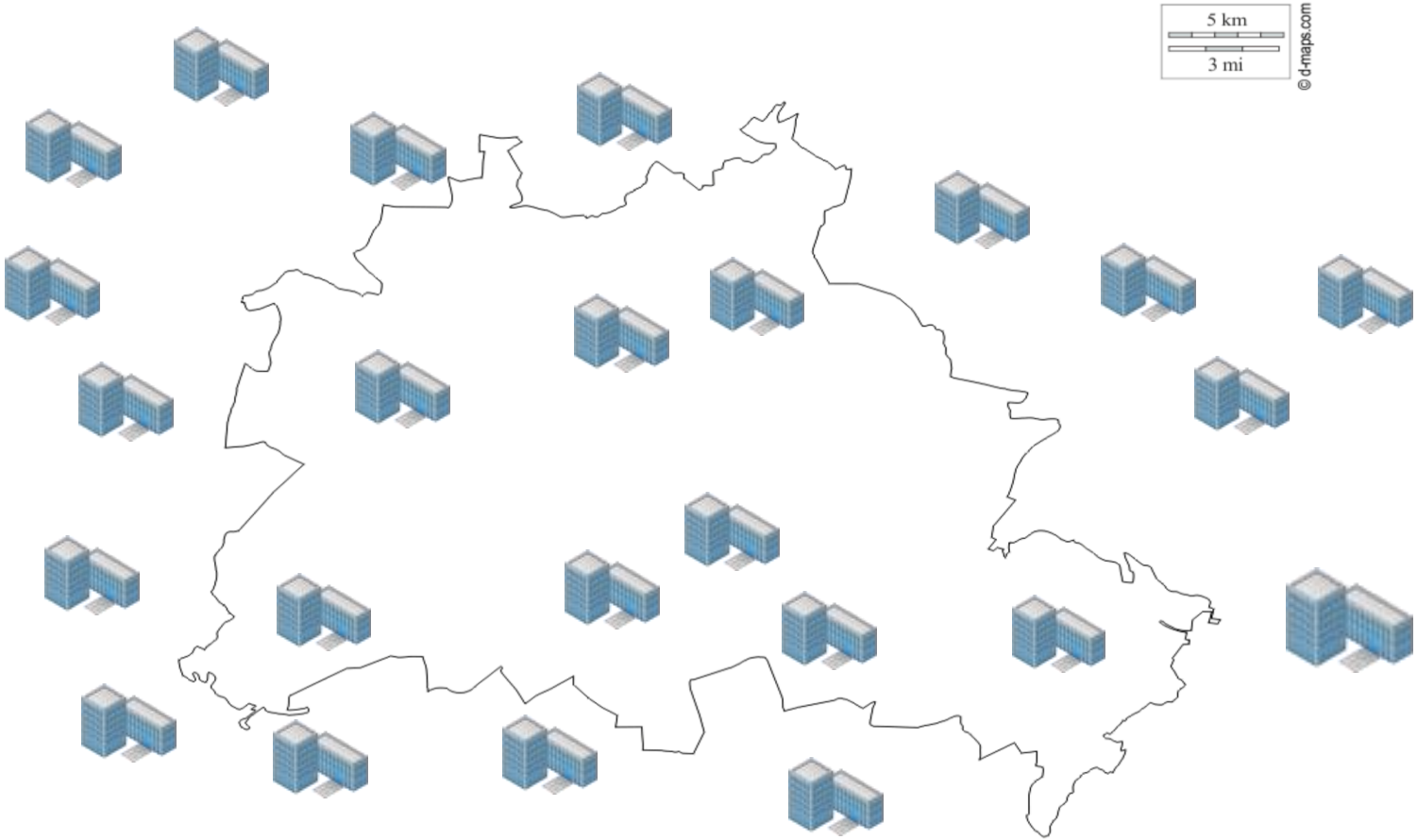
Projekt - Historie

Projektstart 2005, Unternehmen mit industriellen Hintergrund

Ausgangssituation

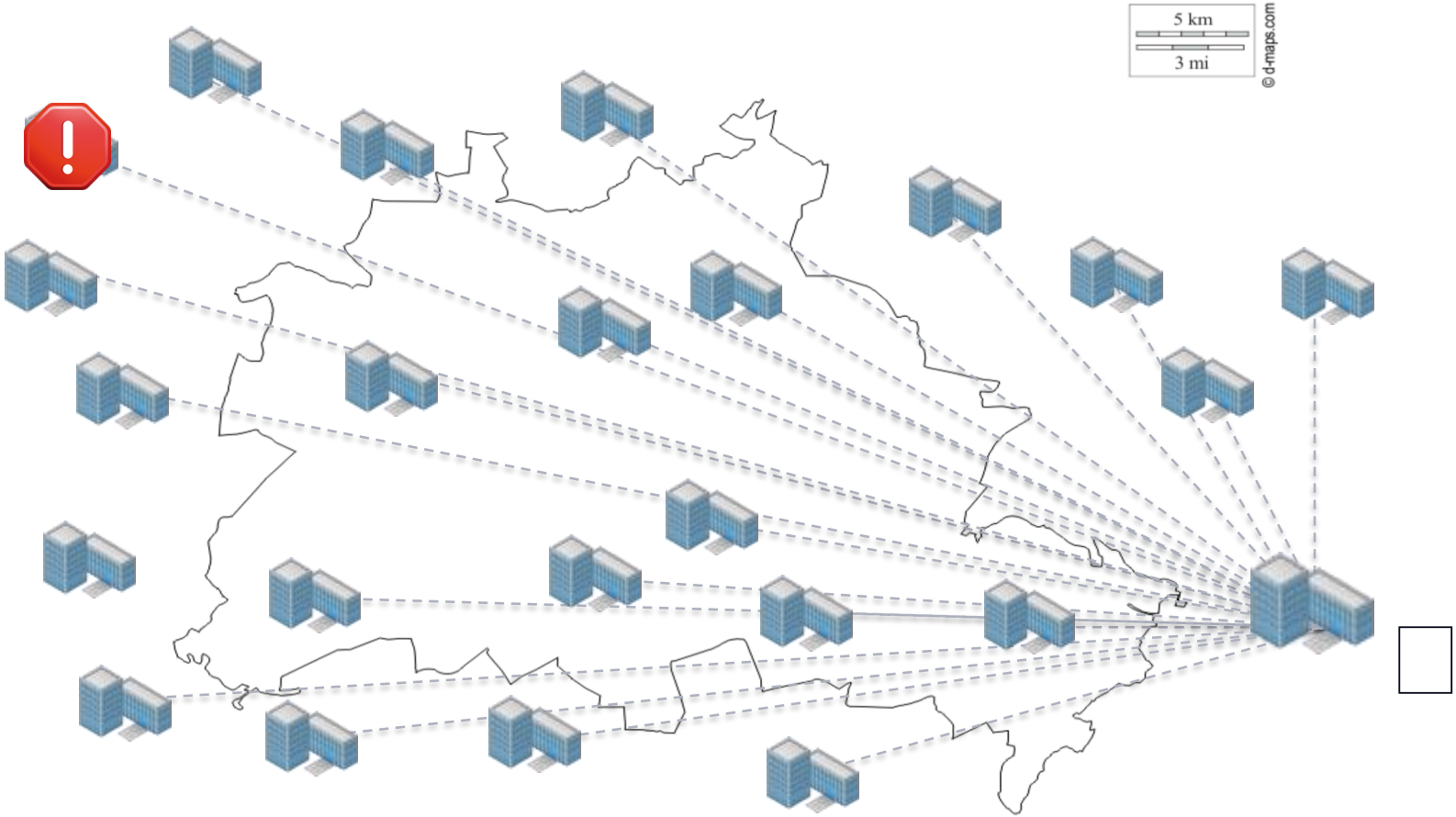
- Ca. 25 Standorte in Berlin und Umgebung
- Standorte sind untereinander mit eigenen Leitungen verbunden (IP-basiertes WAN)
- teilweise Backupverbindungen per ISDN
- Infrastruktur in den Standorten:
  - LAN (Ethernet)
  - Feldbussysteme (ProfiBus)
  - Prozessleitsystem (SCADA-Server, Clients, Drucker)

Standorte



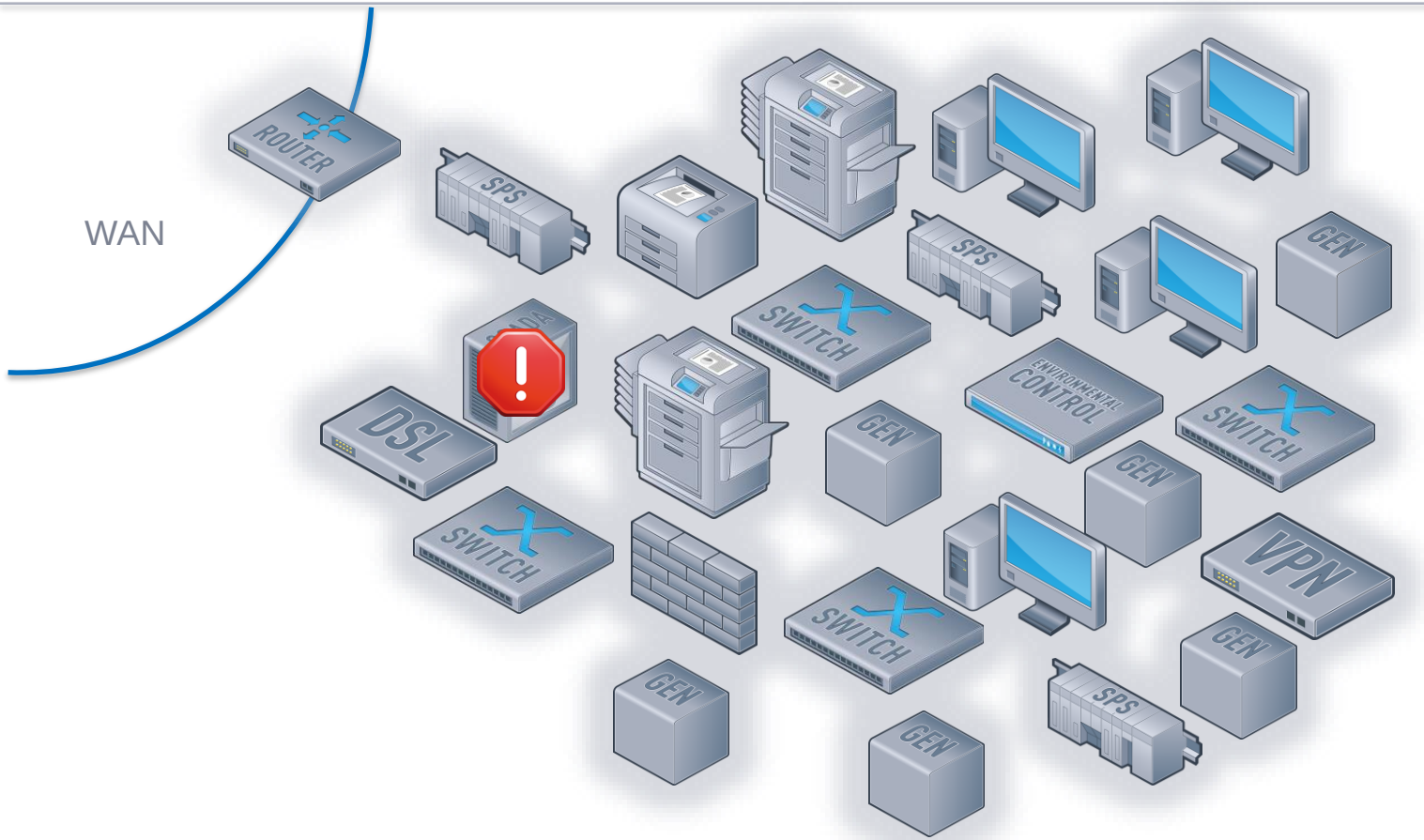
Standorte - Überwachung

AUCONET
Beta Systems Group



LAN eines Standorts

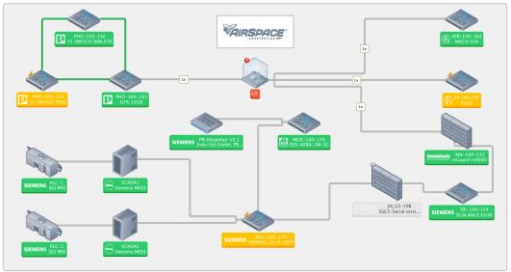
AUCONET
Beta Systems Group



Projekt - Historie

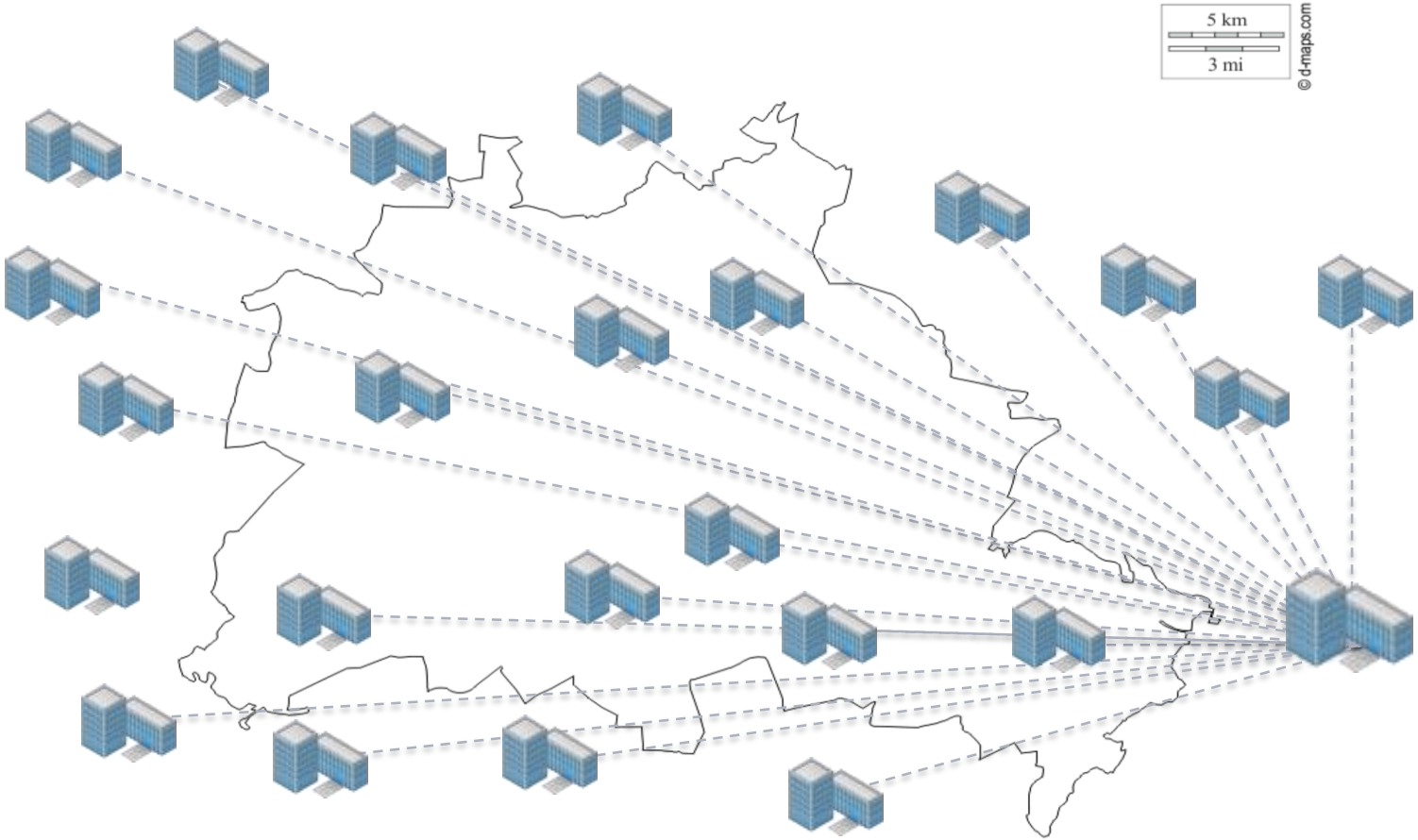
Ziele

- Schaffung von Transparenz sowohl im WAN als auch im LAN
- Einrichtung einer zentralen Alarm- und Eventkonsole
- Grafische Darstellung der aktuellen Systemtopologie
- Monitoring aller WAN- und LAN-Komponenten von einer zentralen Stelle
- Überwachung der SCADA-Server und Clients mit Fehlerkorrektur (soweit möglich)
- Einrichtung einer Testumgebung mit allen relevanten Systemkomponenten



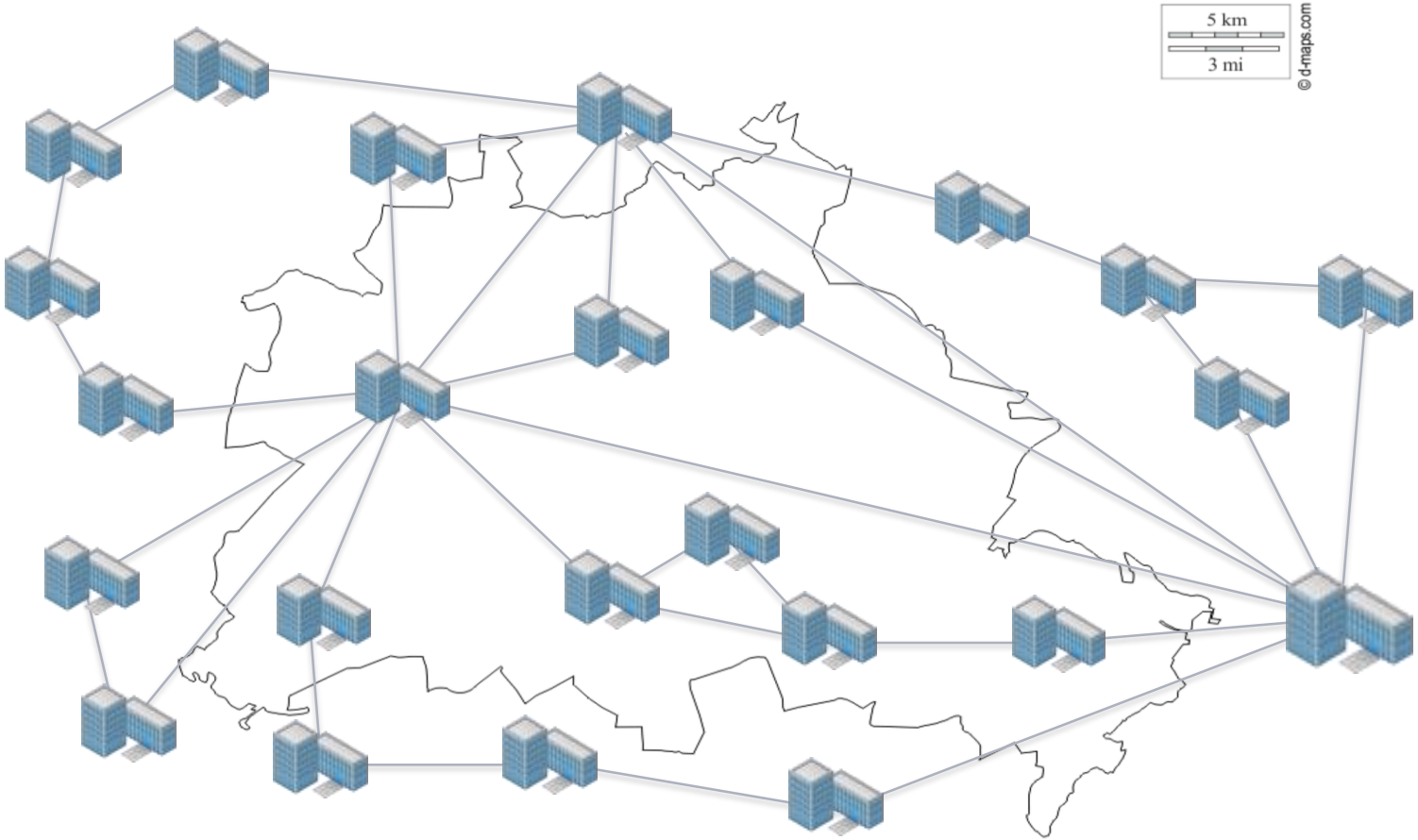
Monitoring - WAN

AUCONET
Beta Systems Group



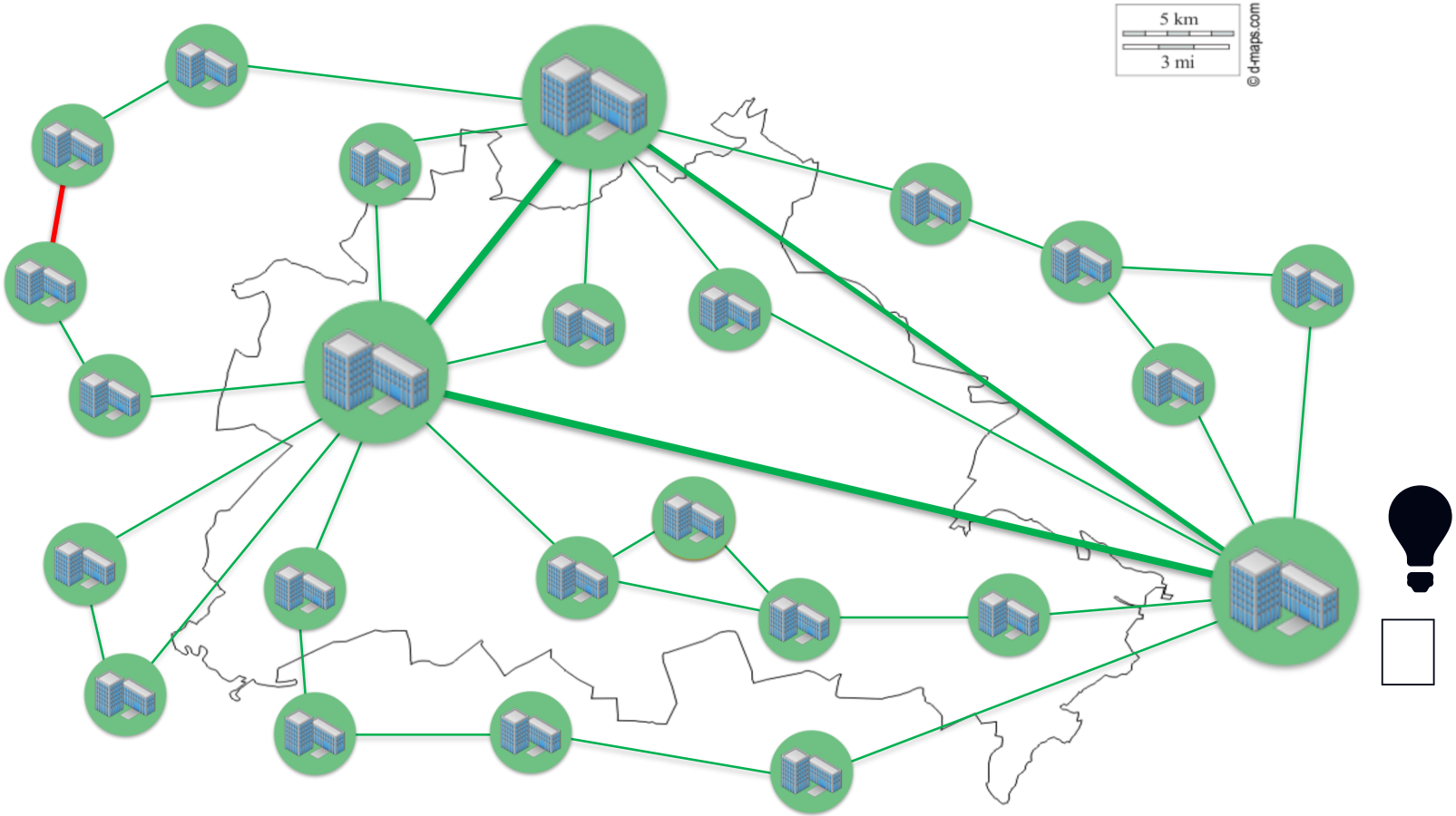
Monitoring - WAN

AUCONET
Beta Systems Group

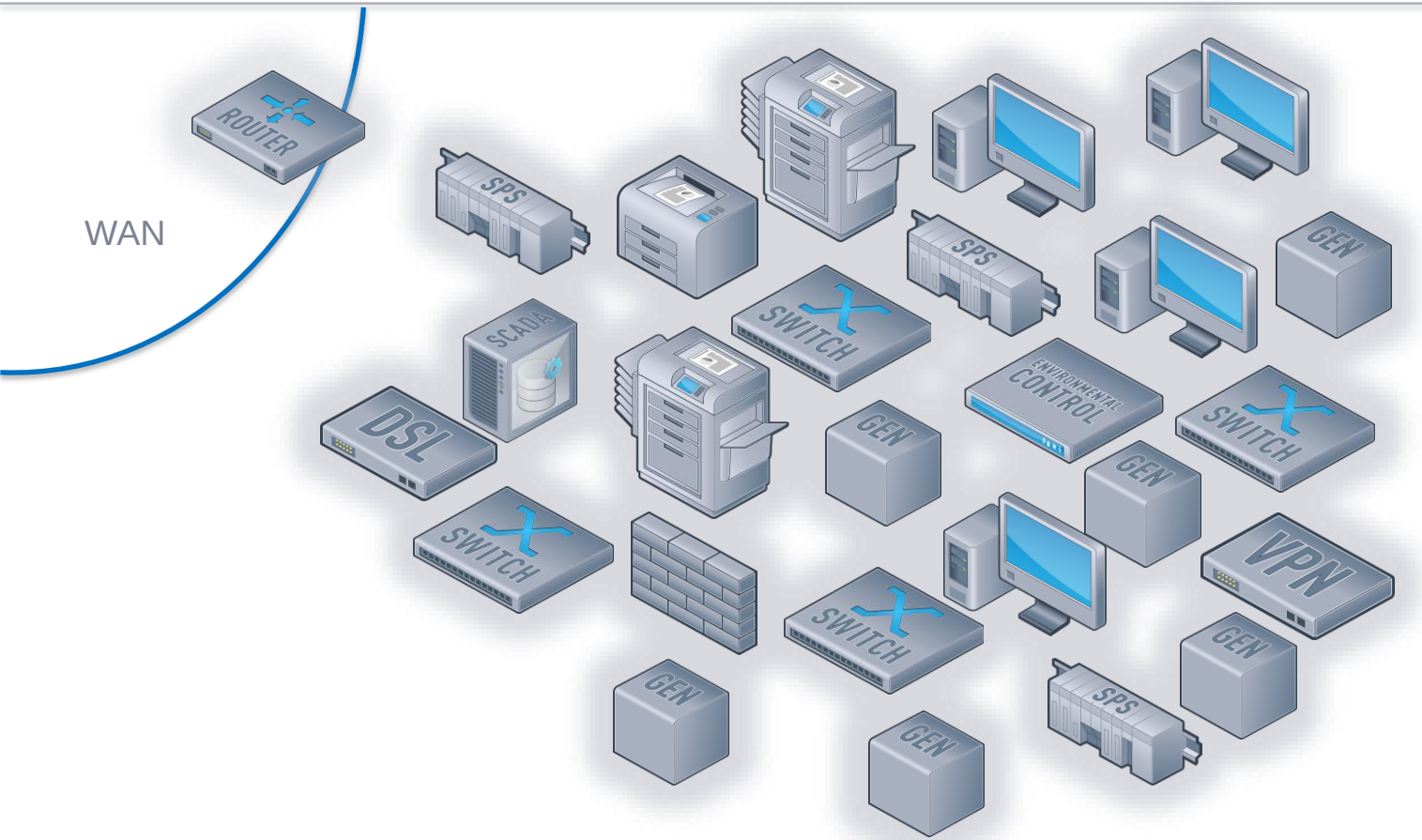


Monitoring - WAN

AUCONET
Beta Systems Group

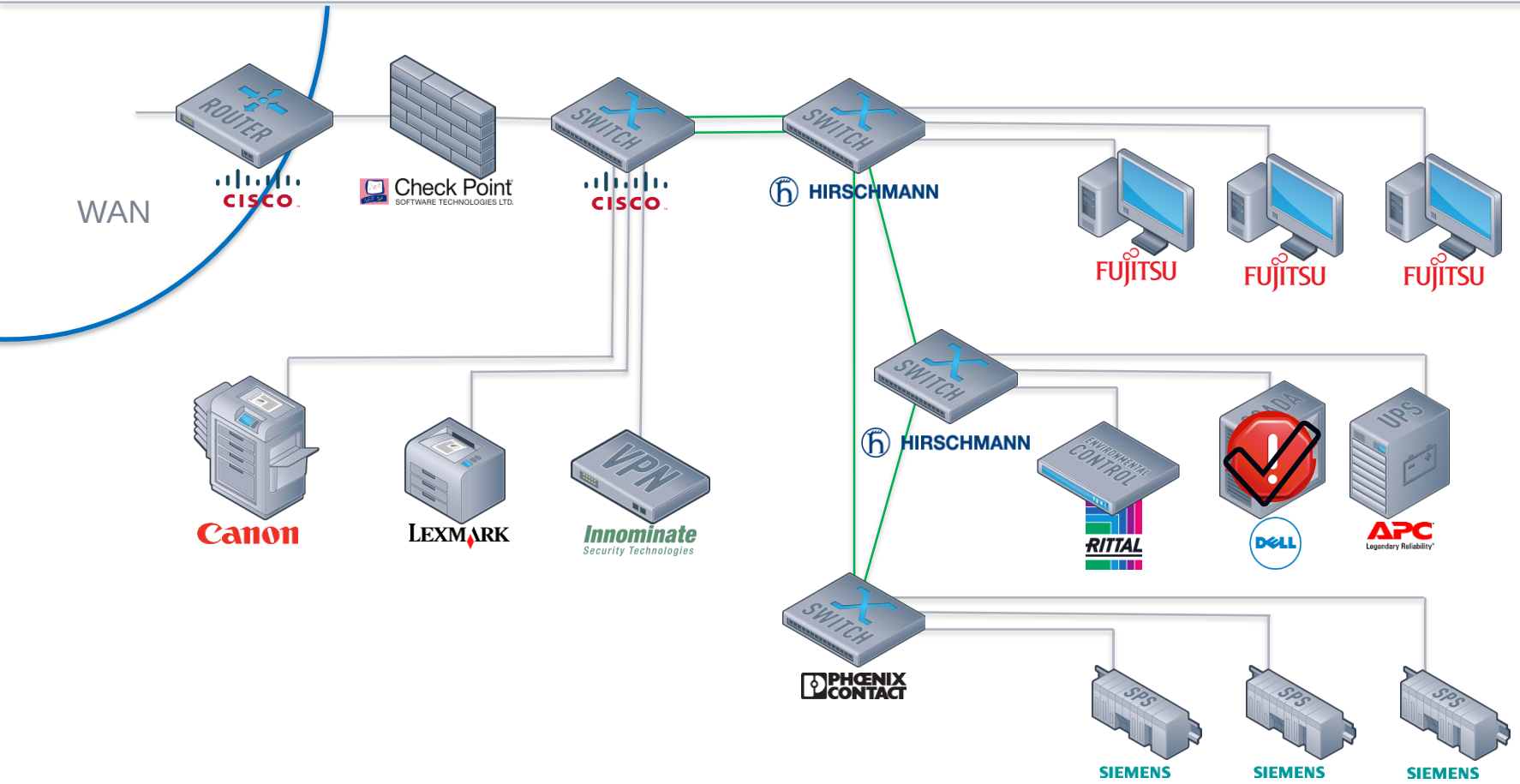


LAN eines Standorts



LAN eines Standorts

AUCONET
Beta Systems Group



2010 Stuxnet

AUCONET
Beta Systems Group

COMPUTERWORLD UNITED STATES INSIDER

NEWS

Siemens: Stuxnet worm hit industrial systems

By Robert McMillan
IDG News Service | SEP 14, 2010 1:17 PM PST

A sophisticated worm designed to steal industrial secrets and disrupt operations has infected at least 14 plants, according to Siemens.

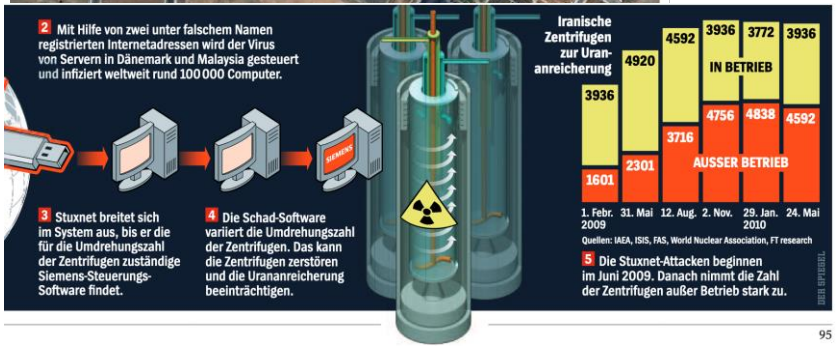
Ausland

SPIEGEL

CYBERKRIEG

Die Zauberwaffe

Der Virus „Stuxnet“, mit dem der Mossad das iranische Atomprogramm attackierte, ist das erste digitale Kampfgerät von geopolitischer Bedeutung.



95

golem.de
IT-NEWS FÜR PROFIS

HOME TICKER VIDEOS VORGELESEN FORUM | ANMELDEN

Golem.de jetzt werbefrei lesen

TOP-THEMEN: Microsoft Security Klimakrise Auto

IT-KARRIERE: STELLENMARKT SEMINARE IT-KÖPFE GEHALTSCHECK | SERVICES: PREISVERGLEICH TOP-ANGEBOTE

STUXNET-WURM

Iranische Atomanlage infiziert

Der Stuxnet-Wurm hat die Rechner des iranischen Atomkraftwerks Buschehr infiziert. Das Hauptsystem der Atomanlage soll von dem Angriff nicht betroffen sein. Insgesamt seien 30.000 Computer der iranischen Regierung von Stuxnet befallen.

27. September 2010, 11:49 Uhr, Ingo Pakalski

AUCONET
Beta Systems Group

Paradigmenwechsel

Bisher: **„Wir sind sicher, wir haben ja keinen Internetzugang“**

Die Industriesteuerungen, die angegriffen wurden, hatten auch keine Verbindung zum Internet. Das sogenannte **„Air Gap“** konnte also überwunden werden. Hier durch einen manipulierten USB-Stick und durch „Zero-Day-Exploits“ im Betriebssystem Windows;
Aber auch andere Methoden sind denkbar, z. B. „Hinzufügen“ eines WLAN-AccessPoints an einem nicht benutzten Netzwerkport.

„Kann das auch bei uns passieren??“ – „JA“

„Was müssen wir tun, um dieses Risiko zu minimieren?“

Ab jetzt: **„Wir haben ein „Zero-Trust-Network“, es gibt keine sichere Zone mehr“**

Neue gesetzliche Vorschiften

2009 Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes (**BSI-Gesetz**)

2015 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (**IT-Sicherheitsgesetz**)

Definition kritischer Infrastrukturen (KRITIS)

Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teiledavon, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und
2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

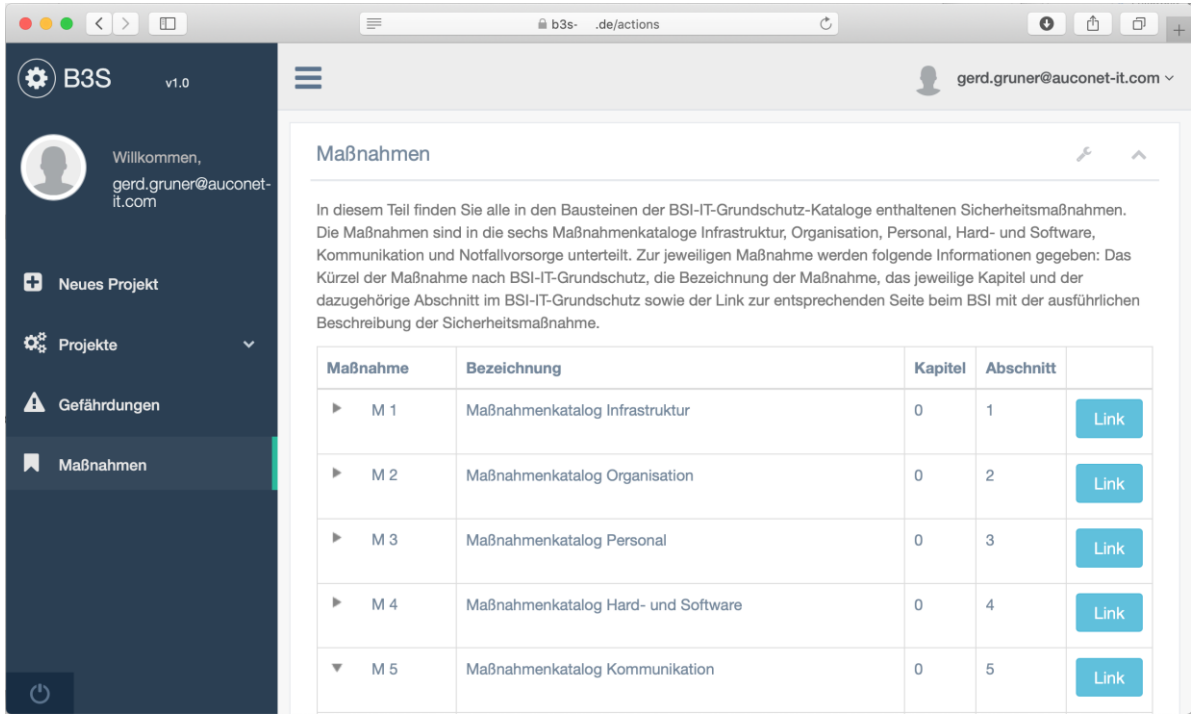
Neue gesetzliche Vorschriften

Was bedeutet das IT-Sicherheitsgesetz?

Schlagwort	BSIG	Beschreibung
Standards	§8a Abs. 1	Im BSIG Verweis auf „Stand der Technik“. Ausgestaltung durch DVGW im Rahmen UP-Kritis. Umsetzung innerhalb von 2 Jahren.
Audits	§8a Abs. 3	Mindestens alle 2 Jahre Nachweis der Erfüllung durch Audits, Prüfungen oder Zertifizierungen.
Meldepflicht	§8b Abs. 3	Meldung von erheblichen Störungen an das Bundesamt für Sicherheit in der Informationstechnik.
Erreichbarkeit	§8b Abs. 3	Jederzeit erreichbare Kontaktstelle ist einzurichten.
Unterstützung	§3 Abs. 3	BSI kann auf Ersuchen beraten und unterstützen

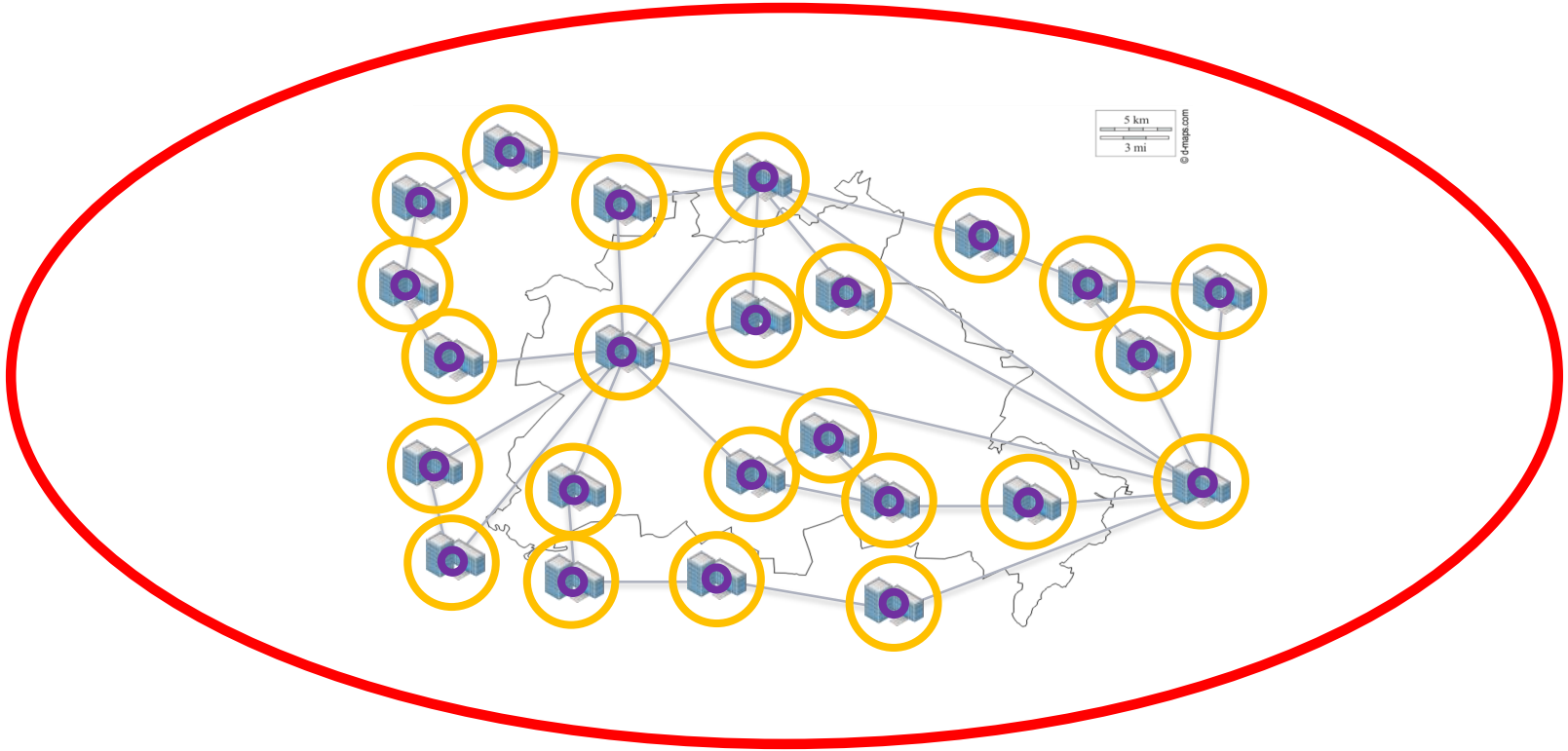
Neue gesetzliche Vorschriften

Branchenspezifischer Sicherheitsstandard (B3S)



Definition unterschiedlicher Schutzzonen

AUCONET
Beta Systems Group



Absicherung der WAN-Zugänge

Zwei Firewalls mit
„Split Responsibility“

Statistikdaten

Konzern-Netz

Produktionsnetz

VPN

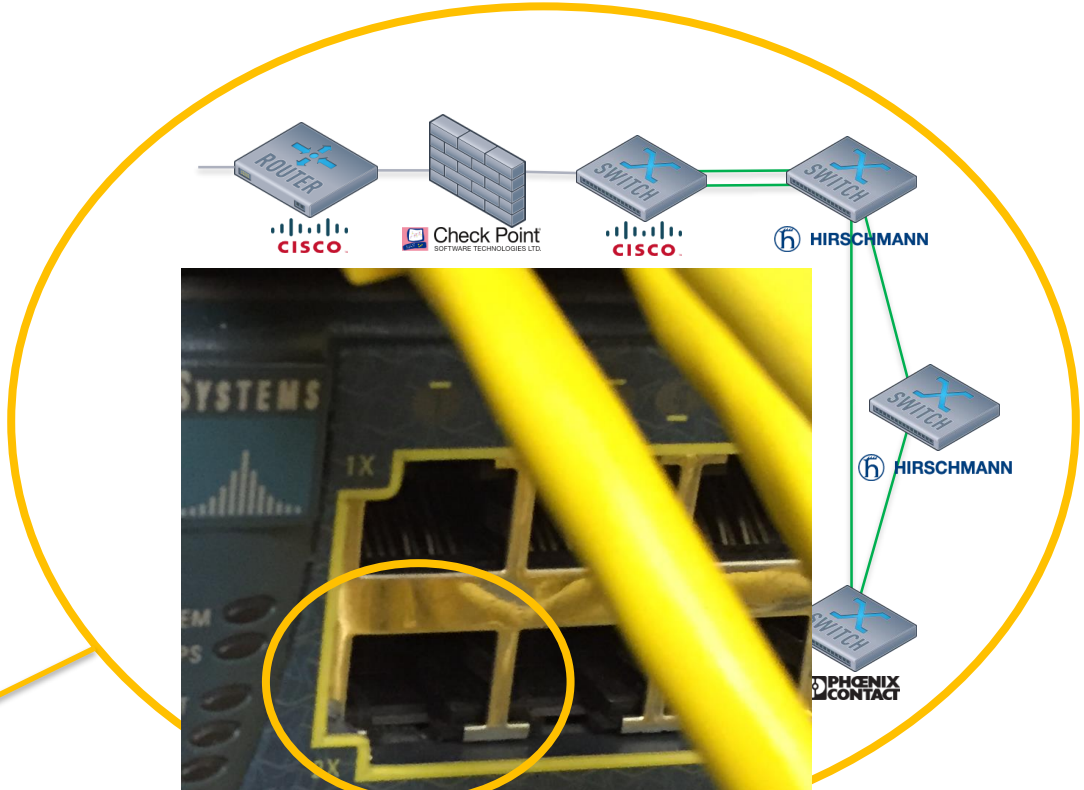
Zentraler
Fernwartungs-
zugang

Absicherung der LAN-Zugänge

Implementierung einer Netzzugangskontrolle

- MAC
- 802.1X

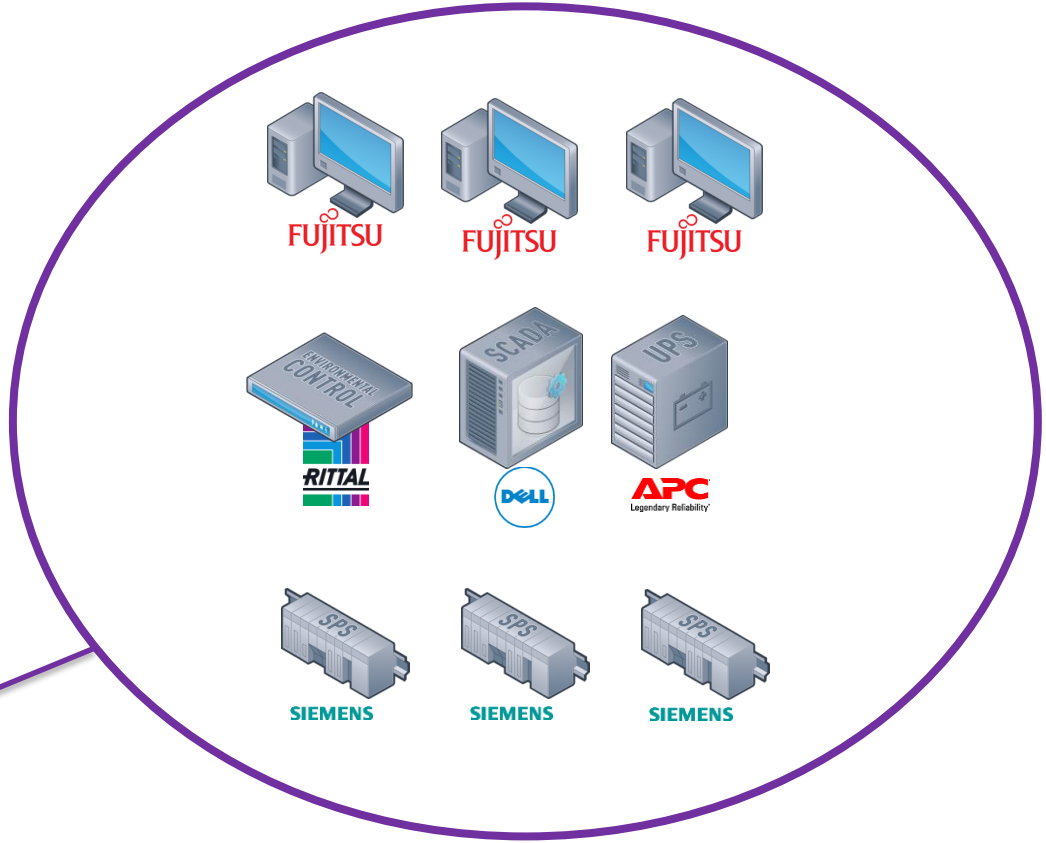
Kein Wi-Fi



Absicherung der Endgeräte

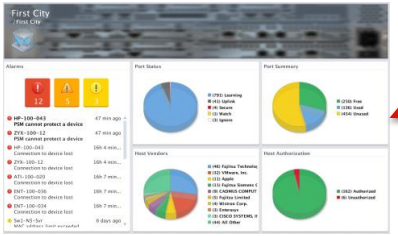
AUCONET
Beta Systems Group

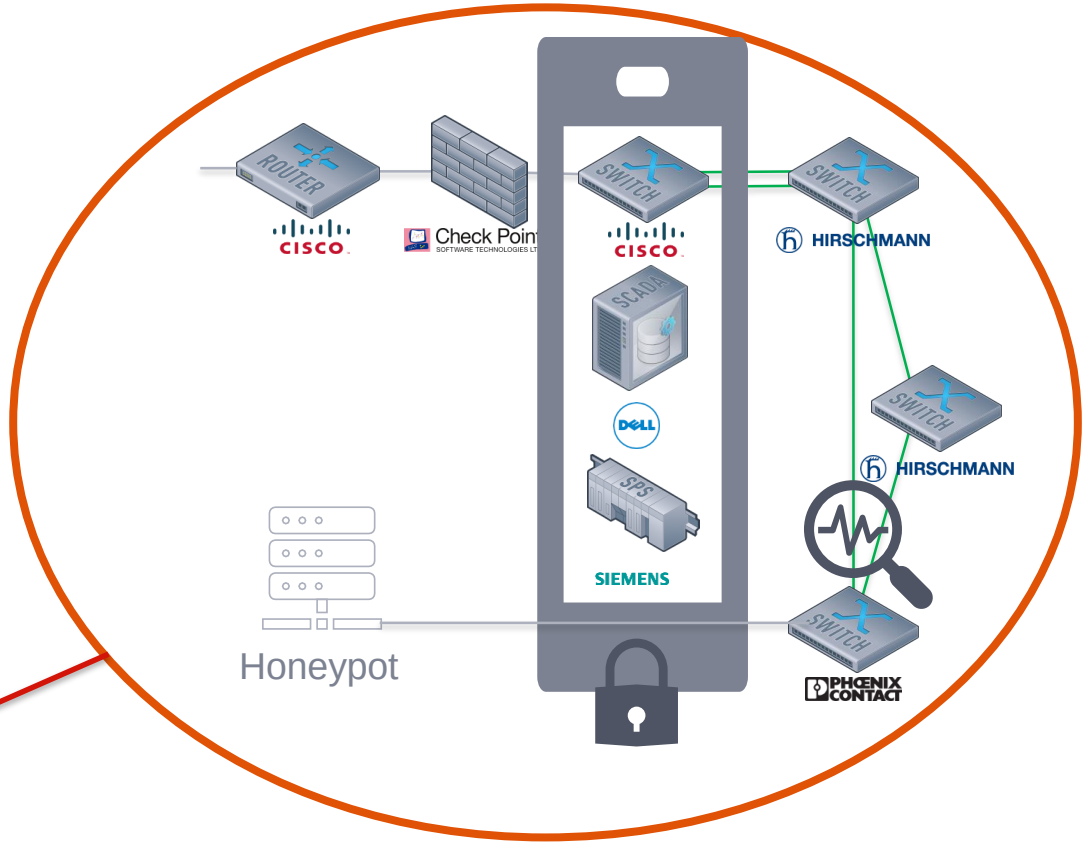
- USB-Port-Überwachung
- Zwei-Faktor-Authentifizierung
- Login-Überwachung
- Patchmanagement
- Konfigurationsüberwachung
- Einsatz von Antiviren-Software
- Überwachung von Serverdiensten (Whitelisting)



Weitere Sicherheitsmaßnahmen

- Anomalieerkennung
  - Per NetFlow
  - Spezielle Hardware
- Honeypot
- Einsatz von Schranküber-wachungssystemen
- Verwendung von verschlüsselter Kommunikation





Neue Herausforderungen

- Schrittweiser Ersatz der Feldbussysteme durch IP-basierte Systeme
- Ausbau von BICS in weiteren Konzernbereichen
- Einführung eines übergeordneten SIEM-Systems

AUCONET
Beta Systems Group

Vielen Dank für die Aufmerksamkeit

Gerd Gruner, Auconet GmbH