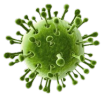
Entscheider-Zyklus 2022

Ergebnisveranstaltung, November 2022:

Gruppe 1

ENTSCHEIDERFABRIK

Teilnehmer



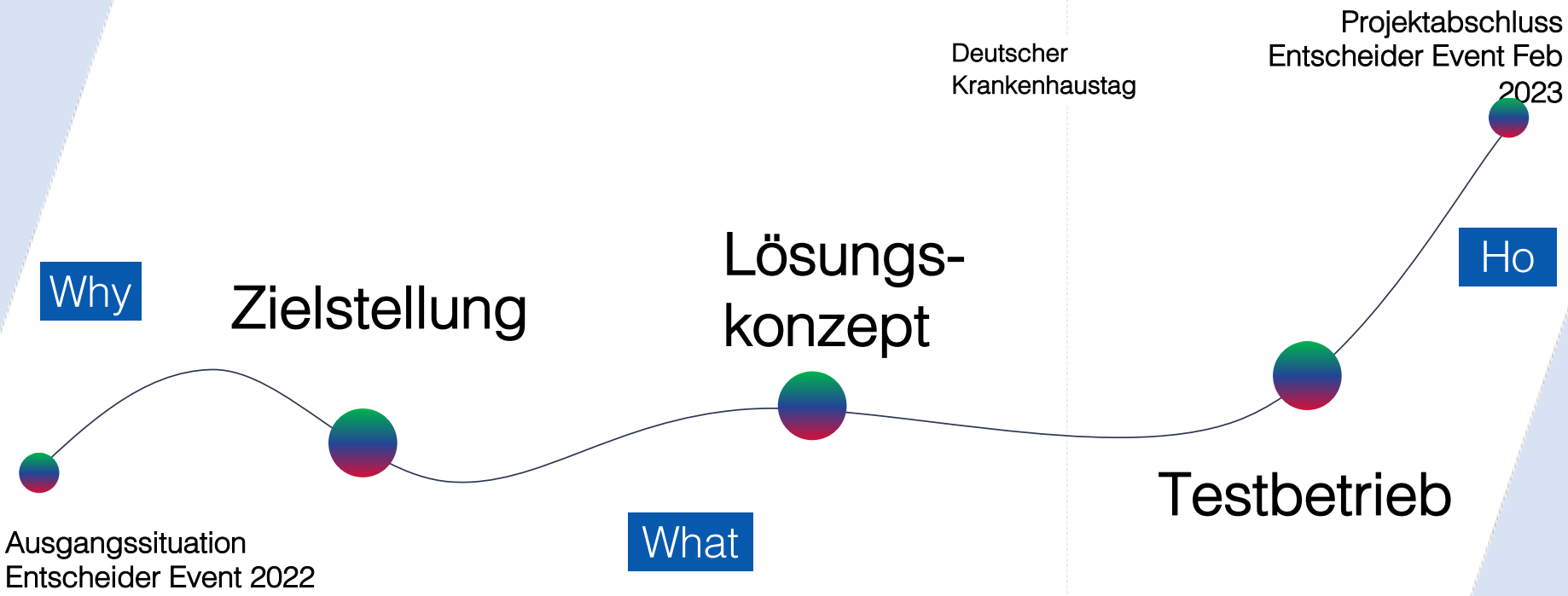
terraconnect
healthcare | it-management

MARIEN KRANKENHAUS

Westpfalz-Klinikum GmbH

secunet

Projektpfad



ENTSCHEIDERFABRIK

Unsere Publikation

Projekt 3: Sichere Anbindung vernetzbarer Systeme in lokalen Wirkungskreisen

Sicherer Fernzugang im digitalen Zeitalter

Im Projekt soll ein zuverlässiger Fernwartungszugang konzipiert werden, der nicht nur einschlägige Standards der Informationssicherheit berücksichtigt, sondern auch kosteneffizient ist. Im Einsatz ist dafür ein Edge-Computing-Ansatz, der ein Höchstmaß an Sicherheit erlaubt.

Die immer größer werdende Zahl an zu wartenden Medizingeräten im Krankenhaus stellt zunehmend ein Sicherheitsproblem dar. Änderungen wie Sicherheitsupdates können heute leider oft nicht (zeitnah) durchgeführt werden. Daher sind diese Geräte – aus Sicht der IT-Sicherheit – häufig veraltet und verfügen über bekannte Schwachstellen, was sie angreifbar macht. Die langen Laufzeiten bzw. Lebenszyklen verschärfen die Situation zusätzlich. Einen Fernzugang zu erlauben, ohne angemessene Vorkehrungen hinsichtlich der IT-Sicherheit getroffen zu haben, ist riskant.

Angriffsfläche reduzieren

Diese Herausforderung kann mit dem sogenannten Edge-Computing-Ansatz gelöst werden. Das heißt, dass mit kleinen IT-Komponenten wichtige (IT-Sicherheits-) Funktionen nachgerüstet werden. Diese Komponenten werden entweder in der Netzwerkperipherie („Edge") direkt am Medizingerät oder in einem Netzwerksegment mit mehreren Medizingeräten platziert. So kann die Angriffsfläche erheblich reduziert werden.

Lösungsansatz im Projekt

Mit dem Konzept „medical connect" (secunet AG) wird es möglich, ein Höchstmaß an IT-Sicherheit bei der Anbindung zu realisieren. Eine Besonderheit ist die system- und netzwerkseitige Isolation der unterschiedlichen Applikationen, die auf medical connect betrieben werden.

Neben den Vorteilen aus Sicht der IT-Sicherheit (z.B. Mikroseparierung von System, Netzwerken und Medizingeräten), können sich auch wirtschaftliche Vorteile ergeben. So können Kosteneinsparungen entlang des Lebenszyklus damit erreicht werden, dass medical connect als Appliance ausgeliefert wird, was die Integrations- und Betriebskosten der Lösung erheblich reduziert.

Im Kontext der Entscheiderfabrik haben sich das Marienkrankenhaus Hamburg, das Westpfalz-Klinikum Kaiserslautern, die IT-Management-Beratung terraconnect aus Notuln und secunet in einem Pilotprojekt zusammengeschlossen, um ein Lösungskonzept zu entwickeln.

Das Lösungskonzept auf Basis von medical connect setzt auf einen Protokollagnostizismus, was es universal für unterschiedliche Hersteller und Protokolle einsetzbar macht. Anders als bei z.B. klassischen VPN-basierten Fernzugangslösungen, werden bei medical connect nicht komplette Netzwerke miteinander verbunden. Vielmehr lassen sich eine Mikroseparierung umsetzen und Fernzugangsverbindungen differenziert freischalten.

Detailsicht auf IT-Sicherheit

Die Lösung verfolgt, neben der IT-Sicherheit, unterschiedliche Design-Ziele:

- Entlastung der IT,
- der Aufwand zur Freischaltung von Fernzugängen reduziert sich für die IT auf ein Minimum,
- Befähigung der Endanwender,
- die Lösung lässt sich auch von Endanwendern bedienen,
- volle Kontrolle liegt bei Krankenhäusern,
- durch die eingebaute Audit-Funktion lassen sich Fernzugänge und Änderungen am System jederzeit nachvollziehen,
- Individualisierbarkeit,
- die Lösung bietet die Möglichkeit die Arbeitsumgebung auf die individuellen Bedürfnisse anzupassen.

> „Die Mitarbeitenden berichten von erheblichen Arbeitserleichterungen."
>
> Prof. Gregor Hülsken

Um die eine einheitliche und regelkonforme Fernzugangslösung bereitzustellen, sind unterschiedlichste Komponenten erforderlich. Die Abbildung rechts zeigt die grobe Lösungsarchitektur sowie den „Workflow" des sicheren Fernzugangs.

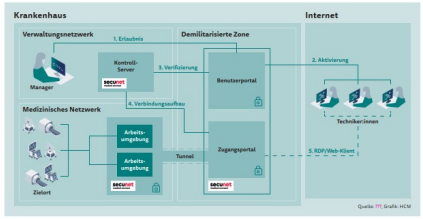
Das sagen die Pilotkliniken

Aus dem Marienkrankenhaus Hamburg heißt es: „Die Anzahl der Geräte mit Fernwartungsbedarf in den Bereichen Labor, Pathologie, Intensivmedizin und der Robotik-assistierten Chirurgie steigt deutlich an. Standardisierte und skalierbare Lösungsansätze wie der hier beschriebene sind geeignet, um die zunehmende Anzahl an Geräten mit Fernwartungsbedarf zu betreiben. Die technischen Administratoren können durch die Dashboard-Funktionalität so eine Vielzahl von einzelnen Fernwartungsverbindungen entlang eines standardisierten Managementprozesses monitoren, steuern und bei Bedarf eingreifen. Die Akzeptanz in den Fachbereichen steigt spürbar, da die organisatorische Freigabe der Fernwartungszugriffe aus den klinischen Prozessen heraus gesteuert und in die Tagesroutine integriert werden kann. Tiefere technische Vorkenntnisse bei den Geräteanwendern sind nicht mehr erforderlich."

Seitens des Westpfalz Klinikum Kaiserslautern wird folgendes Ziel festgelegt: maßgeschneiderte technische Lösungen für die Fragestellungen des Hauses zu erarbeiten und zusammen mit den Partnern ein spannendes und kurzweiliges Projekt etablieren und umsetzen.

Moderne Konzepte ermöglichen es trotz komplexer Netzwerkstrukturen und unterschiedlichsten Anforderungen der Servicepartner, ein Höchstmaß an IT-Sicherheit bei der Anbindung zu realisieren. Neben den Vorteilen aus Sicht der IT-Sicherheit zeigten sich im Projekt auch wirtschaftliche Vorteile. Eine der überraschendsten Erkenntnisse war das Feedback der Mitarbeitenden und Servicepartnerschaften. Sie berichteten von erheblichen Arbeitserleichterungen im Zusammenhang mit Fernzugangstätigkeiten. Durch die auf diesen Zweck ausgerichtete Benutzeroberfläche hat sich die Zufriedenheit spürbar steigern lassen.

Prof. Dr. Gregor Hülsken, Kontakt: gregor.huelsken@ahime.eut.de



Quelle: FPT, Grafik: HCM

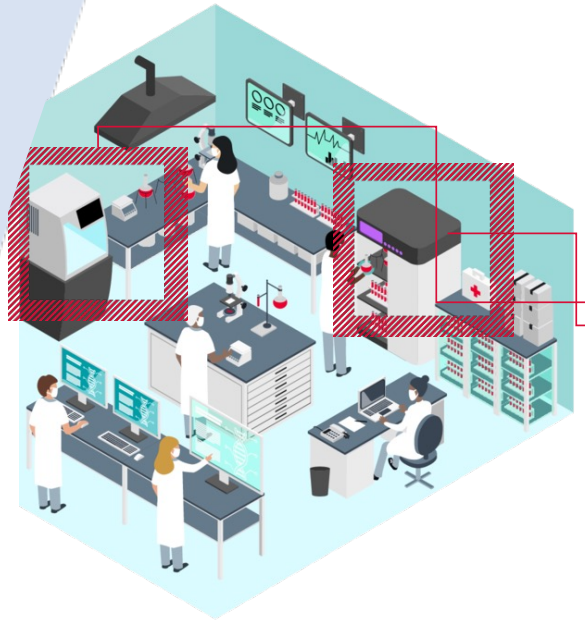
Vernetzte Systeme sicher angebunden

Klinikpartner
Katholisches Marienkrankenhaus gGmbH Hambur, Westpfalz-Klinikum GmbH Kaiserslautern
Industriepartner
secunet Security Networks AG
Projektleitung
Prof. Dr. Gregor Hülsken, terraconnect GTmbH & Co. KG
Projektteam
Markus Habetha, Katholisches Marienkrankenhaus Hamburg, Frank Ebling und Peter Förster, Westpfalz-Klinikum, Markus Wolf, secunet Security Networks AG und Prof. Dr. Gregor Hülsken, terraconnect

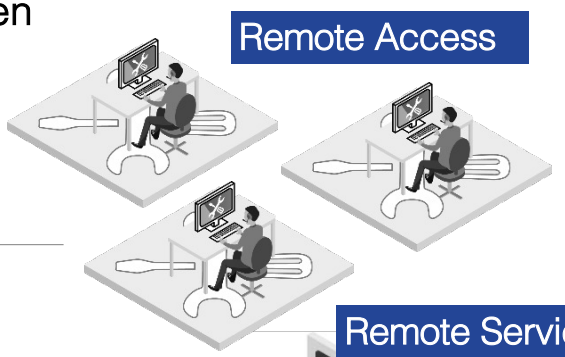
ENTSCHEIDERFABRIK

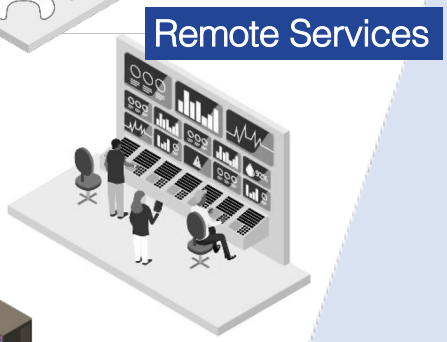
Digitalisierungsprojekt 2022

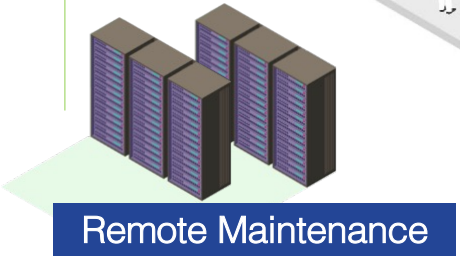
! Best Practices bilden
! Knotenpunkte vereinheitlichen
! Komplexität reduzieren
! Einfache Integration



Labor-Umgebung / Medtec Netzwerk





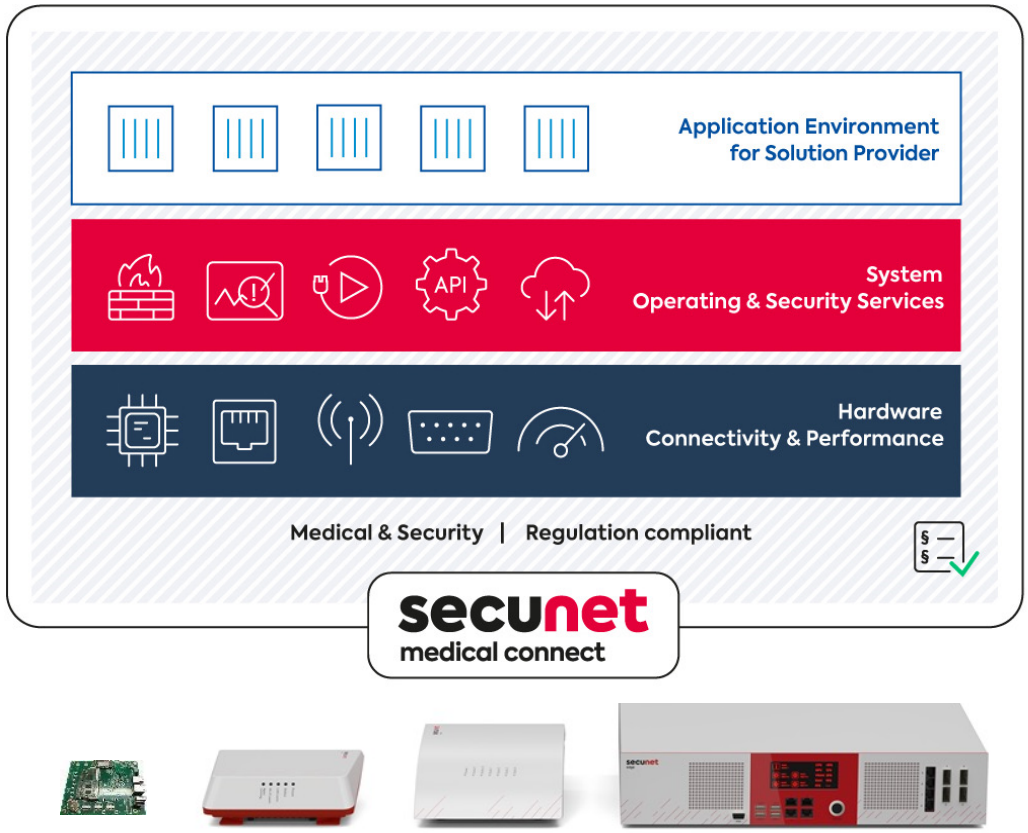


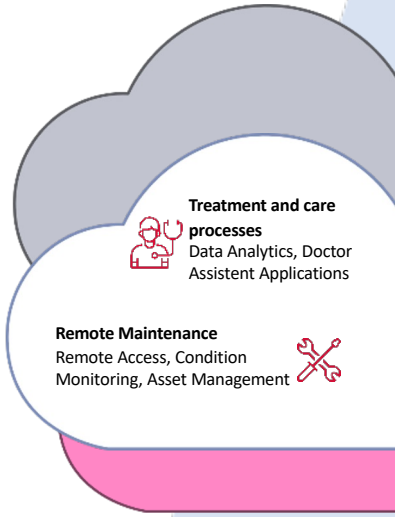
Problemstellung

MARIEN KRANKENHAUS

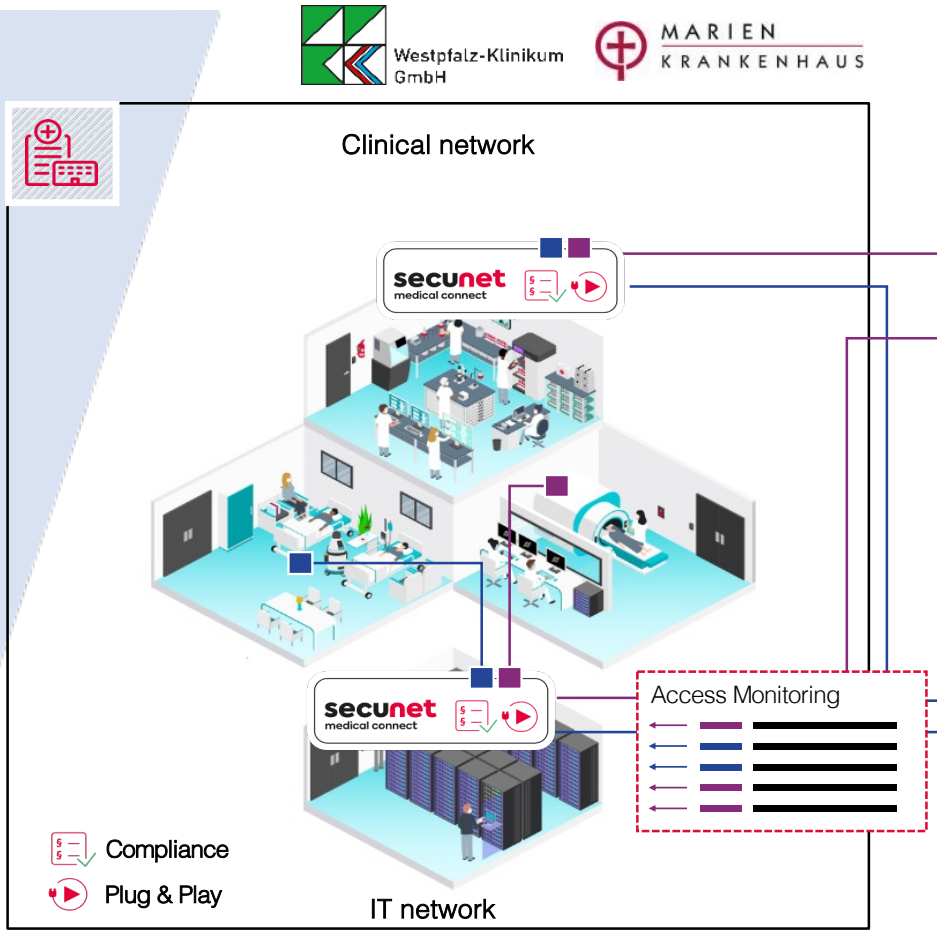
„Die Anzahl der Geräte mit Fernwartungsbedarf in den Bereichen Labor, Pathologie, Intensivmedizin und der Robotik-assistierten Chirurgie steigt deutlich an.“

Einsatz einer Gateway Platform

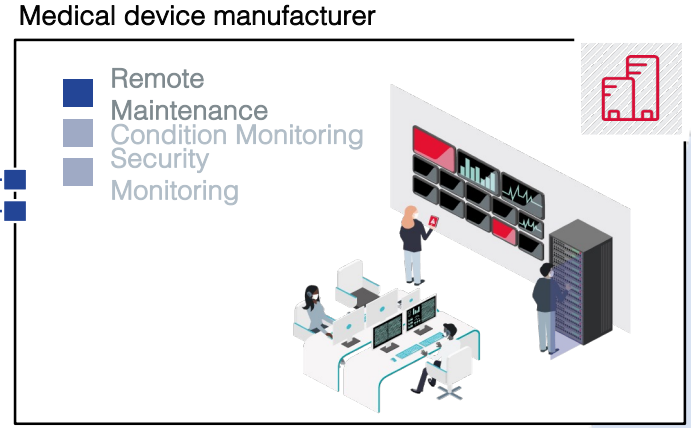




Projektziel

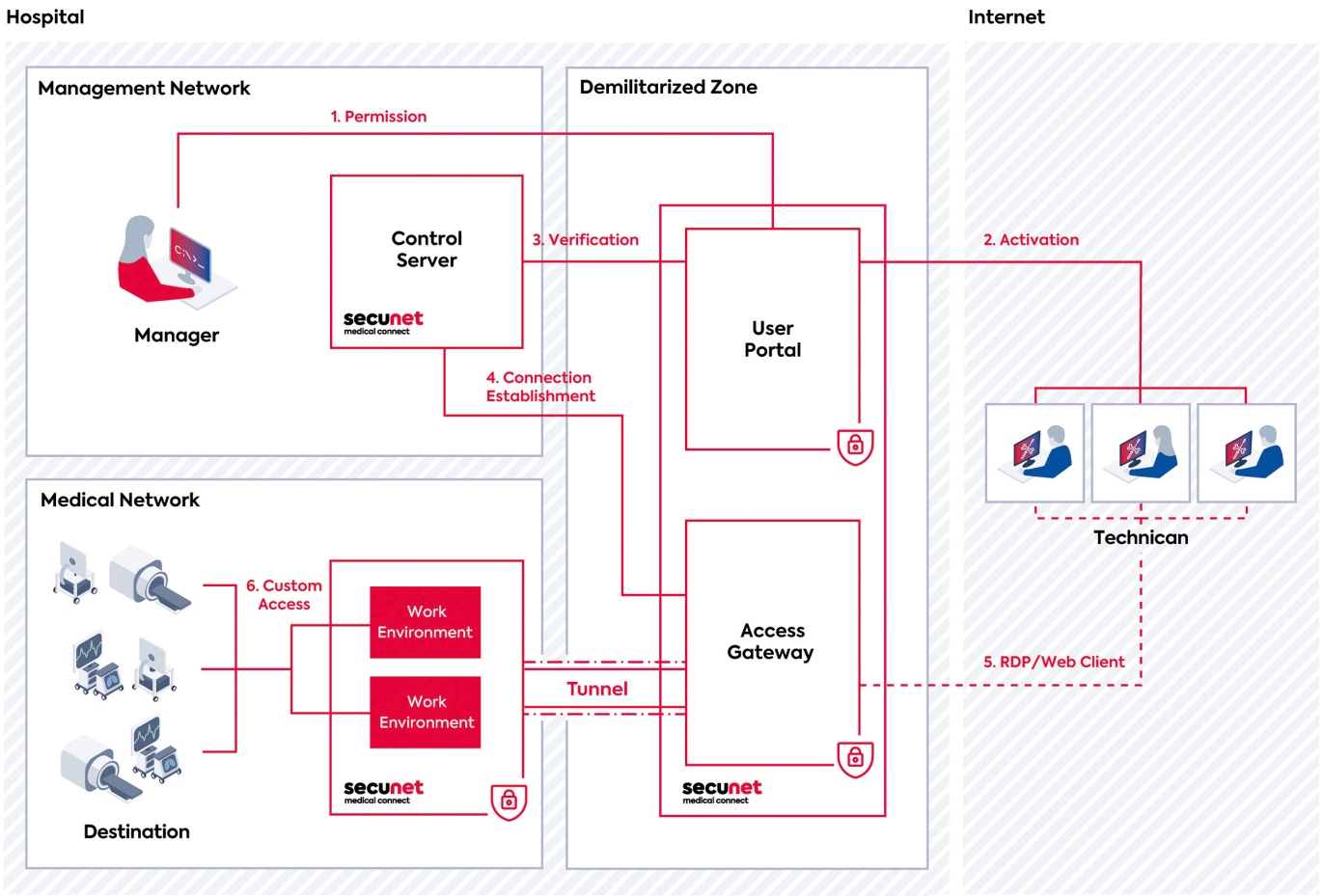


- Isolation von „medtec Netzwerken“ mit einer Secure Gateway Platform
- Integration Lösung „Remote Access“ in KH-Infrastruktur
- Selbstständiges Fernzugangs-Management durch Fachbereich → Entlastung der IT-Administration
- Ggf. Integration von Hersteller-eigenen Fernzugangs-Möglichkeiten (z.B. via TeamViewer oder PTC ThingWorx)



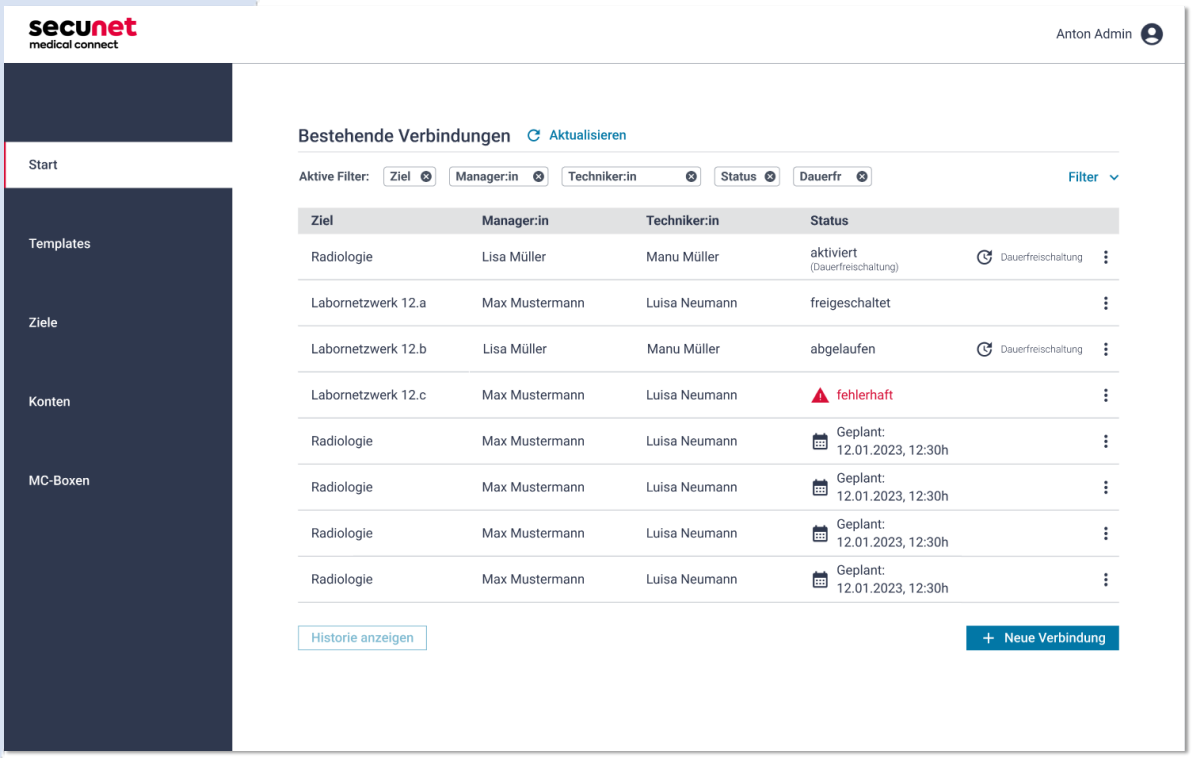
ENTSCHEIDERFABRIK

Ziel-Architektur Bild (Anwendungs-Schicht)



ENTSCHEIDERFABRIK

Perspektive Administration



(1) Zugänge konfigurieren

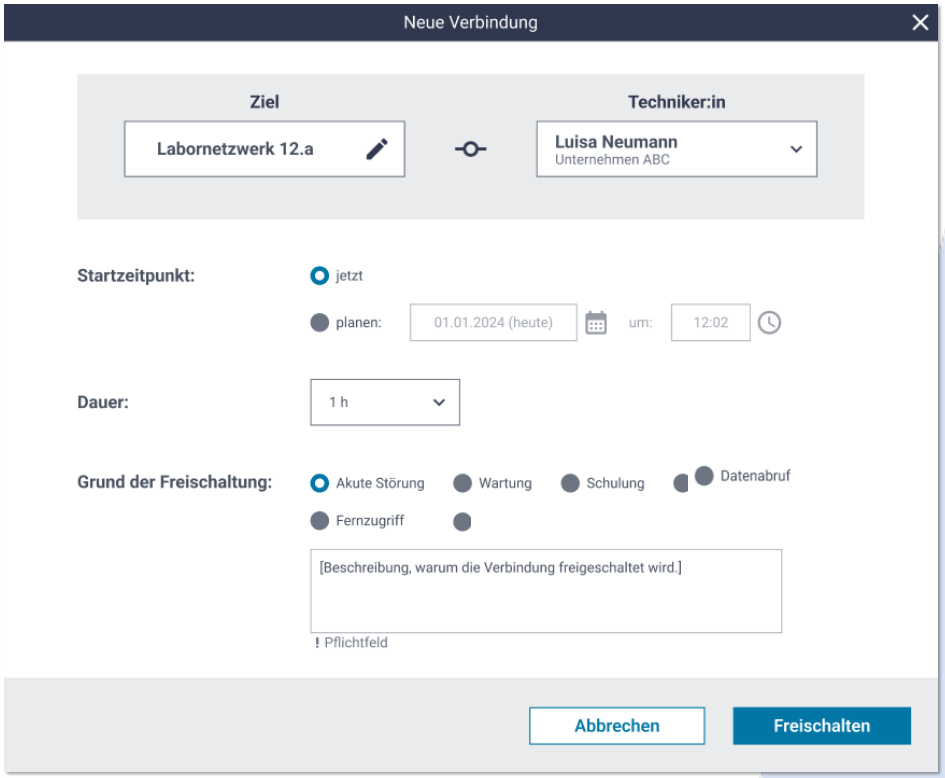
- Reduzierte Betriebsaufwände
- Volle Transparenz & Kontrolle
- Kein Fachwissen „IT-Sicherheit“ erforderlich

ENTSCHEIDERFABRIK

Perspektive Fachbereich

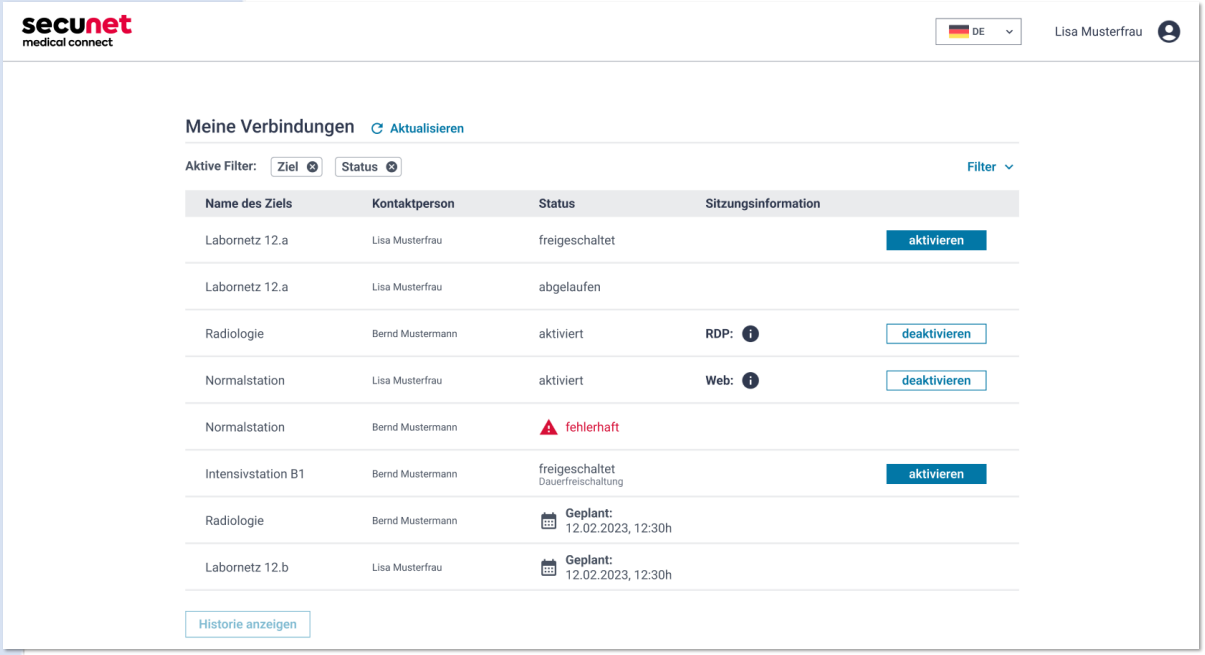
(2) Schaltungen vornehmen

- Selbstständig nutzbar
- Vereinfachte Dokumentation
- Kein Fachwissen „IT“ erforderlich



ENTSCHEIDERFABRIK

Perspektive Hersteller

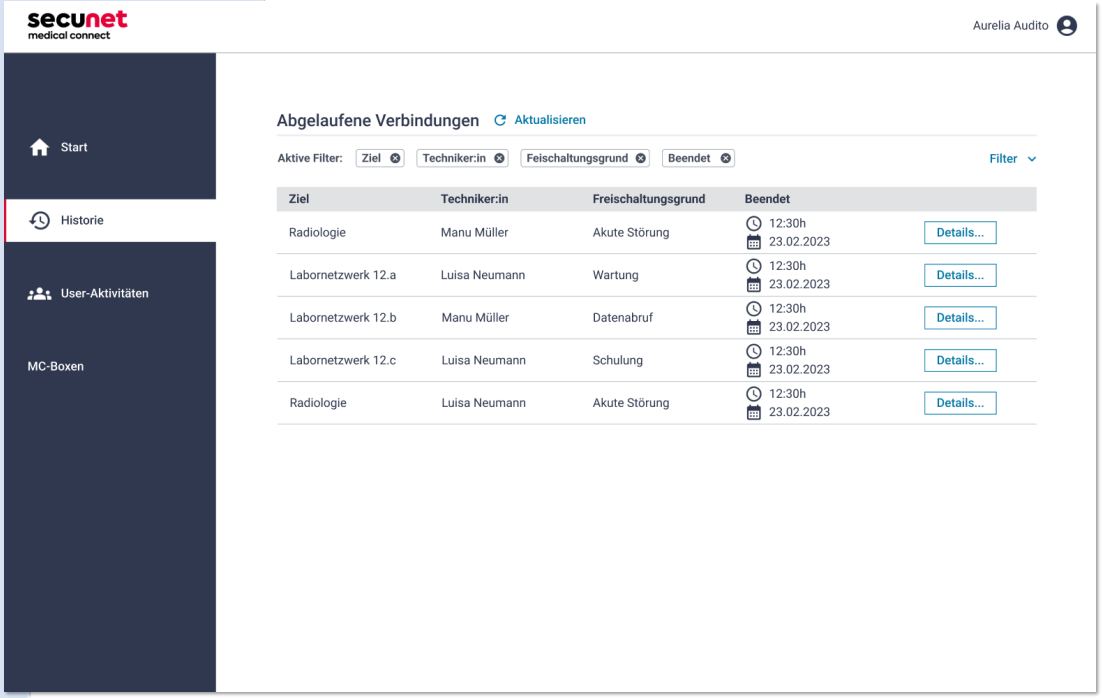


(3) Hinterlegte Zugänge nutzen

- Übersichtlich und einfach
- Selbstständig nutzbar
- Protokoll-unabhängig

ENTSCHEIDERFABRIK

Perspektive CISO



(4) Jederzeit den Überblick behalten

- Volle Transparenz der Zugänge
- Protokollierung sicherheits-relevanter Ereignisse
- IT-Sicherheit gem. BSI CS 108

ENTSCHEIDERFABRIK

Vergleich Lösungskonzepte

	secunet Appliance	Remote Access Lösung Software	„Classic VPN“ Software
Transparenz und Nachvollziehbarkeit	✓	✓	✗
Sichere Dateiübertragung („Schleuse“)	✓	✗	✗
Individuelle Arbeitsumgebung	✓	✓	✓
Erweiterte IT-Sicherheits-Maßnahmen (z.B. Mikro-Separierung, Norm-Konformität)	✓	✗	✗
Erweiterbarkeit (z.B. Anwendungsumgebung für andere kundenspezifische Anwendungsfälle)	✓	✗	✗
Öko-System (z.B. sichere IoT-/Cloud-Anbindung, Netzwerk-Sicherheits-Überwachung)	✓	✗	✗

ENTSCHEIDERFABRIK

Proof of Concept – Inhalte

Nutzer-Feedback
Praktische Anwendung der bereitgestellten Lösung

- Fachbereich
- Hersteller/Service-Partner
- Administratoren
- Auditoren
- CISO

Installation und Betrieb
Aufwände für ersten Aufbau und folgenden Betrieb der Lösung

- Installation Appliance
- Ersteinrichtung von Benutzern, Freigaben,...
- Einweisung/Schulung der Nutzer
- Stabilität/ Geschwindigkeit

IT-Sicherheit
Nutzbarkeit und Wirksamkeit der IT-Sicherheitsmaßnahmen

- Integrierbarkeit Architektur
- Netzwerkseparierung
- Ordnungsgemäße Verbindungsaufbauten
- Protokollierung

Kosten/Nutzen
Vergleich Leistung, Kosten und Aufwand alternativer Lösungskonzepte

- Mehrwerte und Nutzen
- Förderungsfähigkeit
- Betriebskonzept
- Gesamtkosten

ENTSCHEIDERFABRIK

Vom Konzept zur Lösung

Funktionale Anforderungen im Kundenumfeld

- Ableitung aus dem Use-Case
- Gespräche mit Anwendern
- Feedback aus den Evaluationen

Sicherheitsrelevante Anforderungen

- Normenanalyse (B3S KH, BSI-CS 108, BSI-CS 054, OPS.1.2.5)
- Umsetzung flankierender Maßnahmen

Praktische Evaluation

- Prototyp im Labor
- Muster im Workshop
- Begleiteter Einsatz in Zielumgebung

Lösung für sicheres Remote Maintenance für medizinische Netzwerke

Konzeptvorteile - Sicht Marienkrankenhaus

Fokus-Zielgruppe(n): Hersteller & Fachbereich

MARIEN KRANKENHAUS

Konzeptvorteile

- Möglichkeit der (einfachen) Integration von Hersteller-individuellen und proprietären Lösungen
- Trotz Hersteller-Integration weiterhin volle Kontrolle beim Krankenhaus
- Akzeptanz und Zufriedenheit Fachbereich gegeben

Konzeptvorteile - Sicht Westpfalz-Klinikum

Westpfalz-Klinikum GmbH

Konzeptvorteile

- Spürbare Entlastung der IT-Administration nach erfolgter Initialisierung
- Einfacher Betrieb der Lösung durch Auslieferung als Appliance
- Hoheit über Netzwerk-Zugänge weiterhin bei der IT

Fokus-Zielgruppe(n):
IT-Administration

Roadmap

Dt. Krankenhaustag

EF Präsentation

Abstimmungen zu
- Zugangswegen / Protokollen
- Eingesetzten Tools
- Workflows
- Integrationsfragen
- Individuellen Anforderungen

- Vorbereitung der Hardware
- Vorkonfiguration der Lösung
- Ggf. Integration von herstellerspezifischen Containern
- Finalisierung Fragenkatalog
- Bereitstellung HW, SW, …

- Installation
- Konfiguration
- Einweisung
- Fachliche und technische Tests
- Fragenkatalog

Einbindung der Hersteller / Service-Partner | Vorbereitung der Teststellung | Testwoche(n)

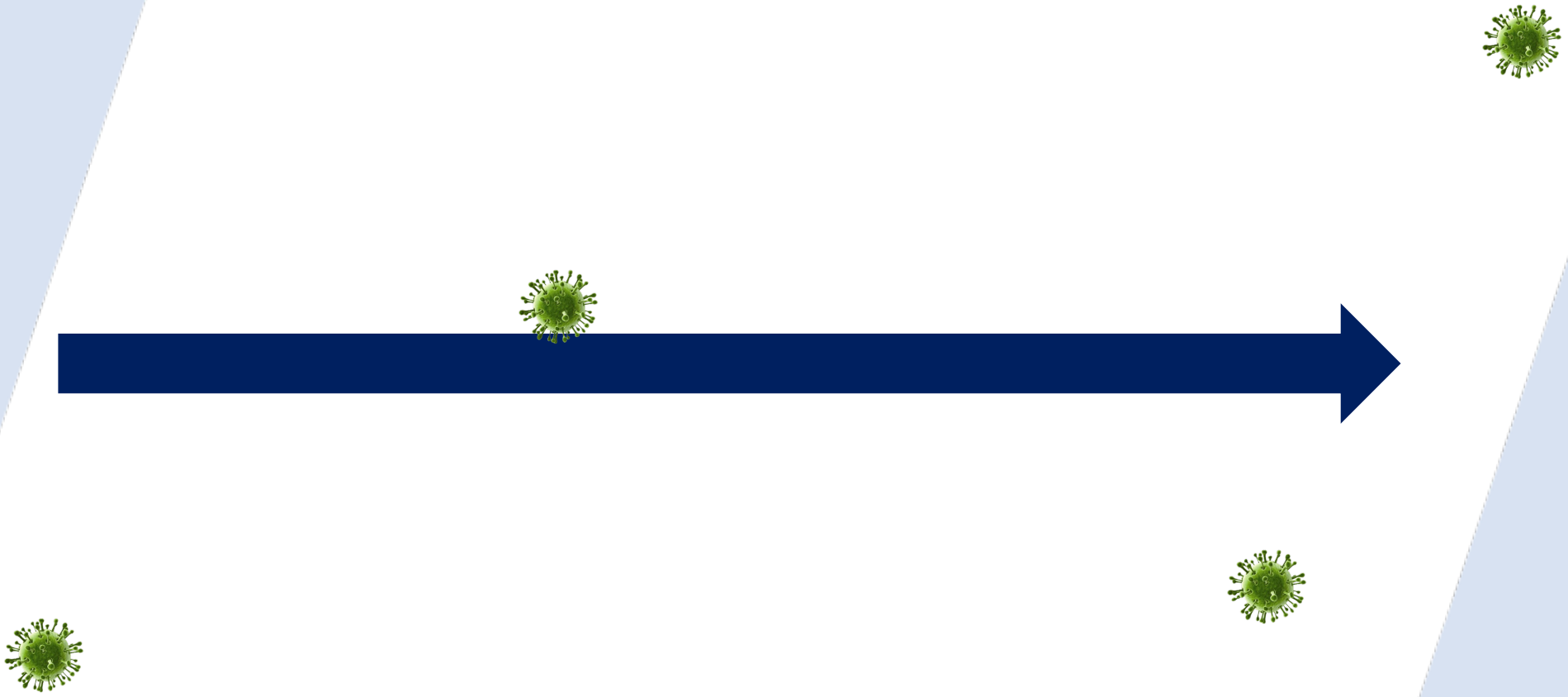
2022 | Q1 2023

Oktober | November | Dezember | Januar | Februar

secunet

ENTSCHEIDERFABRIK

Vorgehen im Projekt



ENTSCHEIDERFABRIK

FAZIT

DANKE FÜR IHRE AUFMERKSAMKEIT

Bleiben Sie gesund!