NIS2

Prüfungsvorgehen anhand eines fiktiven Unternehmens

LIMES SECURITY

Wer sind wir

- Experten für Cybersecurity, OT Security & Secure Product Development
- Herstellerunabhängiges Cybersecurity-Beratungsunternehmen
- Eigentümergeführtes europäisches Unternehmen
- 20+ hochqualifizierte Cybersicherheitsexperten
- 160+ Jahre praktische Erfahrung aus anspruchsvollen Industrial Security Projekten

Womit wir Ihnen helfen

Assessments

Wir führen technische und organisatorische Sicherheitsbewertungen auf höchstem Niveau durch und verwenden modernste Hacking-Techniken, um reale Cyberangriffe zu simulieren.

Consulting & Engineering

Wir unterstützen Ihr Team dabei, relevante Cybersicherheitsrisiken zu verstehen und wirksame technische Gegenmaßnahmen zu entwickeln und umzusetzen.

Ausbildung & Zertifizierung

Wir ermöglichen Ihnen den Aufbau und die Integration von Sicherheitskompetenzen in Ihrem Unternehmen durch erstklassige Security-Trainings und die Zertifizierung Ihrer Mitarbeiter


Island
Schweden
Norwegen
Russland
Kanada
Irland
Belarus
Polen
Ukraine
Frankreich
Kasachstan
Mongolei
Italien
Spanien
Portugal
Griechenland
Türkei
Usbekistan
Kirgisistan
Turkmenistan
China
Südkorea
Japan
Syrien
Irak
Iran
Afghanistan
Pakistan
Nepal
Indien
Myanmar (Birma)
Thailand
Vietnam
Philippinen
Marokko
Tunesien
Algerien
Libyen
Ägypten
Westsahara
Saudi-Arabien
Oman
Jemen
Mauretanien
Mali
Niger
Tschad
Sudan
Burkina Faso
USA
Mexiko
Kuba
Puerto Rico
Guatemala
Nicaragua

Limes Security ist eine qualifizierte Stelle (QuaSte) nach NIS-Gesetz

- Limes Security ist laut Bescheid befugt, sowohl technische als auch organisatorische Prüfungen nach NISG für alle Branchen durchzuführen. Hierfür wurden insgesamt 5 Prüfer akkreditiert.
- Über den NIS-Scope hinaus bieten wir zusätzlichen Mehrwert durch optionale integrierte Pentests, detaillierte OT-Security-Assessments, ganzheitliche Risikobewertungen und Reifegradmodellierungen.
- Limes Security verfügt über langjährige Erfahrung in den Bereichen Kritische Infrastrukturen, OT-Systeme, ISMS und OSMS. Wir gestalten unsere Dienstleistungen sinnvoll, ganzheitlich und umfassend für Ihren maximalen Mehrwert.
- Limes Status als ***unabhängige Stelle mit unabhängigen Prüfern*** wird angestrebt.

DI (FH) Bernhard Lorenz

IT/OT Security Specialist

- Expertise:
  - Information Systems Auditing
  - Penetration Testing
  - Application Security
  - IT/OT Security Consulting
- Mehrere Jahre PCI QSA & ASV, nach wie vor PCIP
- Akkreditierter NIS Prüfer
- Limes NIS Prüfprozess & Prüfplan mitentwickelt

Inhalt

- 1. Überblick und Status NIS2
- 2. Pflichten von Einrichtungen
- 3. Ablauf der Prüfung
- 4. Beispiele Prüfungssituationen in fiktiven Unternehmen
- 5. Fragen und Antworten

NIS2 Status

- NIS2: Adressiert Shortcomings aus NIS, erweiterter Scope, Änderungen Schwellenwerte
- Zuvor ca. 200 BwD, jetzt 900 wesentliche bzw. etwa 2500 wichtige Einrichtungen
  - Untersch. Prüfpflicht '*ex ante*' vs. '*ex post*'
- Status: Gesetzesentwurf, aber noch nicht verabschiedet (ev. Q4 2025)
  - Keine Übergangsfrist geplant
    - https://www.parlament.gv.at/dokument/XXVII/ME/326/fname_1621118.pdf
- Beschreibung der Risikomanagementmaßnahmen für Betreiber recht vage
  - Praktische Abhilfe durch Durchsetzungsverordnung *2024/2690*
    - https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202402690&qid=1736332059214#anx_1
  - Cybersecurity Hygienemaßnahmen

- Unsere fiktive Situation für heute:
  - Wir sind wesentliche Einrichtung. Was jetzt?

Pflichten

- Registrierung bei der Cybersicherheitsbehörde
  - mit konkreten Angaben innerhalb von drei Monaten nach Inkrafttreten des Gesetzes
  - Name, Anschrift, wo werden Dienste erbracht, …
  - Kontaktdaten
- Umsetzen von ***verhältnismäßigen technische***, ***operative*** und ***organisatorische*** Risikomanagementmaßnahmen im Bereich der Cybersicherheit
  - Ziel: Auswirkungen von Cybersicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten

Pflichten

Risikomanagementmaßnahmen im Bereich der Cybersicherheit

§ 32. (1) Wesentliche und wichtige Einrichtungen haben geeignete und verhältnismäßige technische, operative und organisatorische Risikomanagementmaßnahmen in den Bereichen der Anlage 3 umzusetzen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Cybersicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

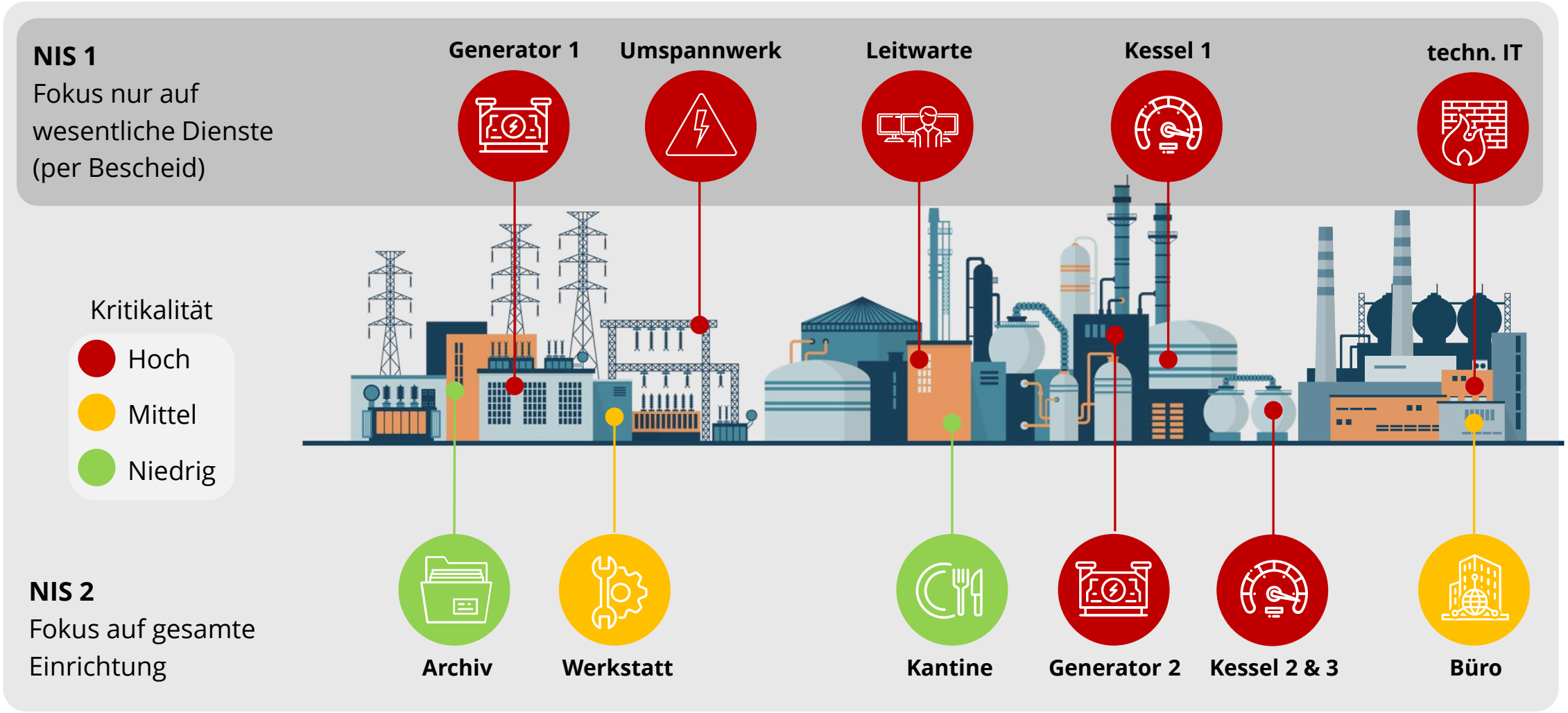
(2) Diese Risikomanagementmaßnahmen haben

1. ein dem bestehenden Risiko angemessenes Cybersicherheitsniveau zu gewährleisten, unter Berücksichtigung
   a. des Stands der Technik und gegebenenfalls der einschlägigen nationalen, europäischen und internationalen Normen sowie Best-Practices sowie
   b. der Kosten der Umsetzung;
2. auf einem gefahrenübergreifenden Ansatz zu beruhen, der auf den Schutz von Netz- und Informationssystemen und deren physischer Umwelt vor Cybersicherheitsvorfällen abzielt sowie
3. zur Sicherheit der Lieferketten
   a) die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter, die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Dienstanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse sowie
   b) die Ergebnisse der gemäß Art. 22 Abs. 1 NIS-2-Richtlinie durchgeführten koordinierten Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten,

gebührend zu berücksichtigen.

Kernstück Risikomanagement

Umsetzung mit vorbeugenden und reaktiven Maßnahmen



Pflichten

- Registrierung bei der Cybersicherheitsbehörde
  - mit konkreten Angaben innerhalb von drei Monaten nach Inkrafttreten des Gesetzes
  - Name, Anschrift, wo werden Dienste erbracht, …
  - Kontaktdaten
- Umsetzen von ***verhältnismäßigen technische***, ***operative*** und ***organisatorische*** Risikomanagementmaßnahmen im Bereich der Cybersicherheit
  - Ziel: Auswirkungen von Cybersicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten
- Nachweis der Wirksamkeit von Risikomanagementmaßnahmen erbringen
  - Aufforderung der Cybersicherheitsbehörde zur Übermittlung der Aufstellung umgesetzter Risikomanagementmaßnahmen (Selbstdeklaration) innerhalb von **sechs Monaten**
  - Effektivität der Risikomanagement Maßnahmen ist innerhalb von **drei Jahren** durch ***unabhängige Stellen und unabhängige Prüfer*** nachzuweisen

Berichtspflichten

Frühzeitige Warnung an das CSIRT nach Bekanntwerden eines Vorfalls.

Innerhalb 24 Stunden

Innerhalb 72 Stunden

Meldung des Vorfalls an das CSIRT, einschließlich einer ersten Klassifizierung

Endbericht an das CSIRT.

Innerhalb eines Monats

Ein **Sicherheitsvorfall** gilt als erheblich, wenn er

a) **schwerwiegende Betriebsstörungen** der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder

b) wenn er **andere** natürliche oder juristische Personen durch **erhebliche materielle oder immaterielle Schäden beeinträchtigt** hat oder beeinträchtigen kann

Konkreter Ablauf bei einer Prüfung

Initialisierung
NDA/PTA, Austausch der Dokumente, Aufklärung zum Umgang mit den Daten

Aktivitäten

Planung und Informationsgewinnung	Organisatorische (ISMS) Prüfung	Technische Prüfung	Prüfbericht
▪ Kennenlernen des Unternehmens ▪ Erheben der wesentlichen Abläufe ▪ Definition des Prüfumfangs und Planung der Prüfungstätigkeiten	▪ kontrollbasierter Prüfansatz, welcher sich auf das interne Kontrollsystem, Prozesse, Vorgaben und Richtlinien der Einrichtung stützt	▪ technische, meist systembasierte, Prüfungshandlungen (z.T. Vulnerability Scanning) ▪ Bestehende Prüfberichte können herangezogen werden werden wenn Scope und Qualität ausreichend sind	▪ nachvollziehbare Darstellung der geprüften Kontrollen, Prüfungshandlungen, Prüfergebnisse, Stichproben und zugeordneten geprüften Systemkomponenten ▪ Kein Zertifikat

Was ein NIS Prüfer NICHT darf

- Prüfer MÜSSEN die Effektivität von Maßnahmen feststellen, aber dürfen NICHT…
  - … Durchführen eigenständiger, nicht vereinbarter Prüfungsvorgehen
    - Beispiel: Eigenständiges, nicht vereinbartes Hantieren an HMIs
  - … Umsetzung von Maßnahmen fordern
  - … konkrete Hersteller oder Produkte verlangen
  - … Administrative Rechte verlangen und selbständig verwenden
  - … Ändern von Konfigurationen und Einstellungen
  - … Management-Entscheidungen treffen oder beeinflussen
  - … Bei der Umsetzung oder dem Betrieb von Sicherheitsmaßnahmen beteiligt sein

Beispiel 1: Risikomanagement Zutrittslösung

Server/Infra	Domain	OS	DR	CPU Cores	Memory	Storage	Purpose	Note	Verfügbarkeit
SEA-Server1	internal	Windows Server 2019 Standard	no	2	8 GB	60 GB	Karten-Programmierung	vm	1
SEA-Server2	internal	Windows Server 2012 R2 Standard	no	2	16 GB	120 GB	AD	phyisch	1
SEA-Server3	internal	Windows Server 2012 R2 Standard	yes	4	16 GB	256 GB	Applikations-Server	vm	2
SEA-Server4	DMZ	Windows Server 2012 R2 Standard	yes	4	16 GB	120 GB	Terminal Server		2
SEA-Server5	internal	CENTOS 8	yes	4	32 GB	1 TB	FS		1
SEA-Server6	Management	CENTOS 8	yes	4	8 GB	120 GB	Logging & Monitoring		3

Beispiel 1: Risikomanagement

Schutzbedarfs Feststellung 2

Servernamen 1

Server/Infra	Domain	OS	DR	CPU Cores	Memory	Storage	Purpose	Note	Verfügbarkeit
-Server1	internal	Windows Server 2019 Standard	no	2	8 GB	60 GB	Karten-Programmierung	vm	1
-Server2	internal	Windows Server 2012 R2 Standard	no	2	16 GB	120 GB	AD	phyisch	1
SEA-Server3	internal	Windows Server 2012 R2 Standard	yes	4	16 GB	256 GB	Applikations-Server	vm	2
SEA-Server4	DMZ	Windows Server 2012 R2 Standard	yes	4	16 GB	120 GB	Terminal Server		2
SEA-Server5	internal	CENTOS 8	yes	4	32 GB	1 TB	FS		1
SEA-Server6	Management	CENTOS 8	yes	4	8 GB	120 GB	Logging & Monitoring		3

Performance Daten 3

Jetzt sind Sie gefragt!

Auf der abgebildeten Tabelle sind verschiedene technische Details zu den Servern und deren Konfigurationen aufgeführt. Welcher dieser Bereiche würde einem Prüfer schnell ins Auge fallen, was denken Sie?

Join at menti.com | use code 6609 6879

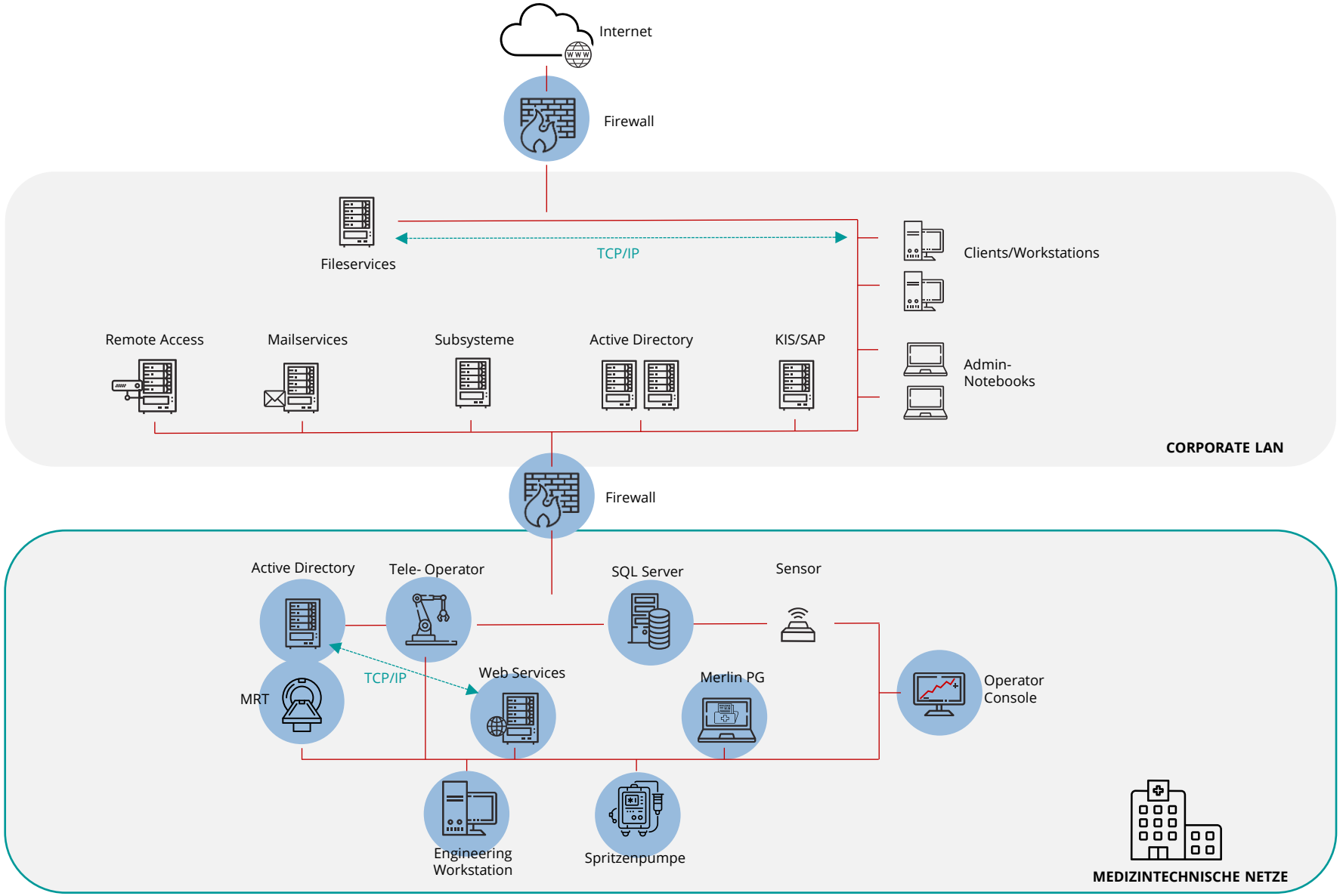
Auflösung Beispiel 1

- Schutzbedarfsfeststellung nur auf Basis von Verfügbarkeit?
- Insbesondere bezüglich Karten Programmierung wären hohe Anforderungen an die Vertraulichkeit zu erwarten gewesen.

Schutzbedarfs Feststellung 2

Storage	Purpose	Note	Verfügbarkeit
60 GB	Karten-Programmierung	vm	1
120 GB	AD	phyisch	1
256 GB	Applikations-Server	vm	2
120 GB	Terminal Server		2
1 TB	FS		1
120 GB	Logging & Monitoring		3

Beispiel 2: HealthCare Network Architecture

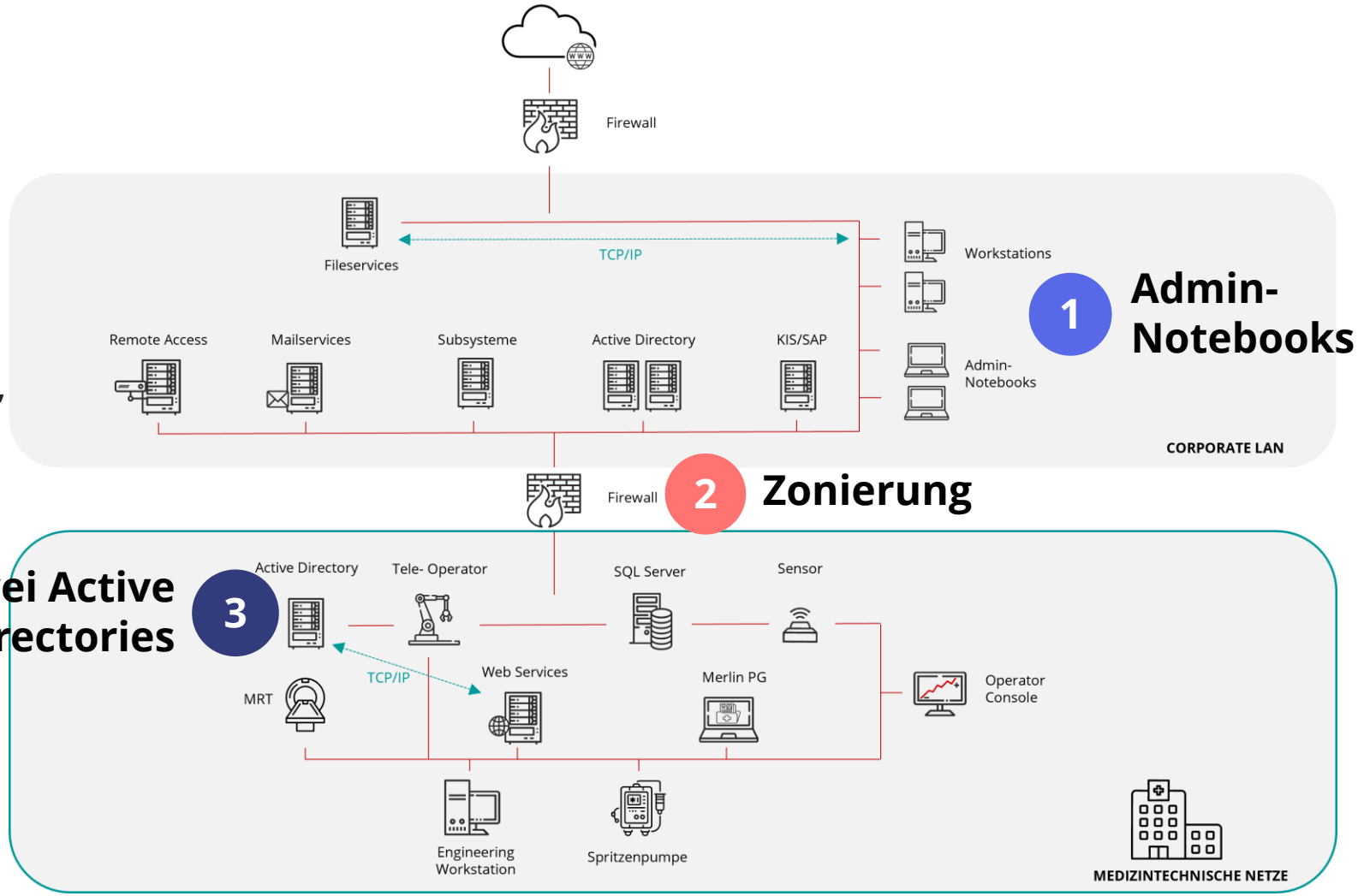


Healthcare Network Architecture

Jetzt sind Sie gefragt!

Auf der abgebildeten Netzwerkgrafik sind drei verschiedene Bereiche markiert. Welcher dieser Bereiche denken Sie, würde einem Prüfer sofort ins Auge fallen?

Join at menti.com | use code 6609 6879

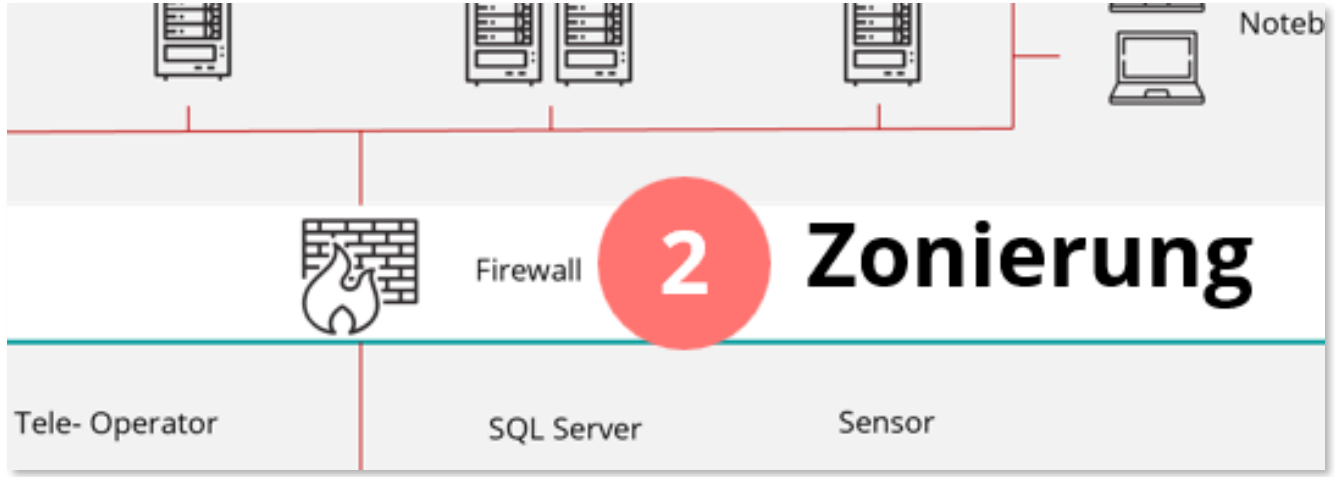


Auflösung Beispiel 2

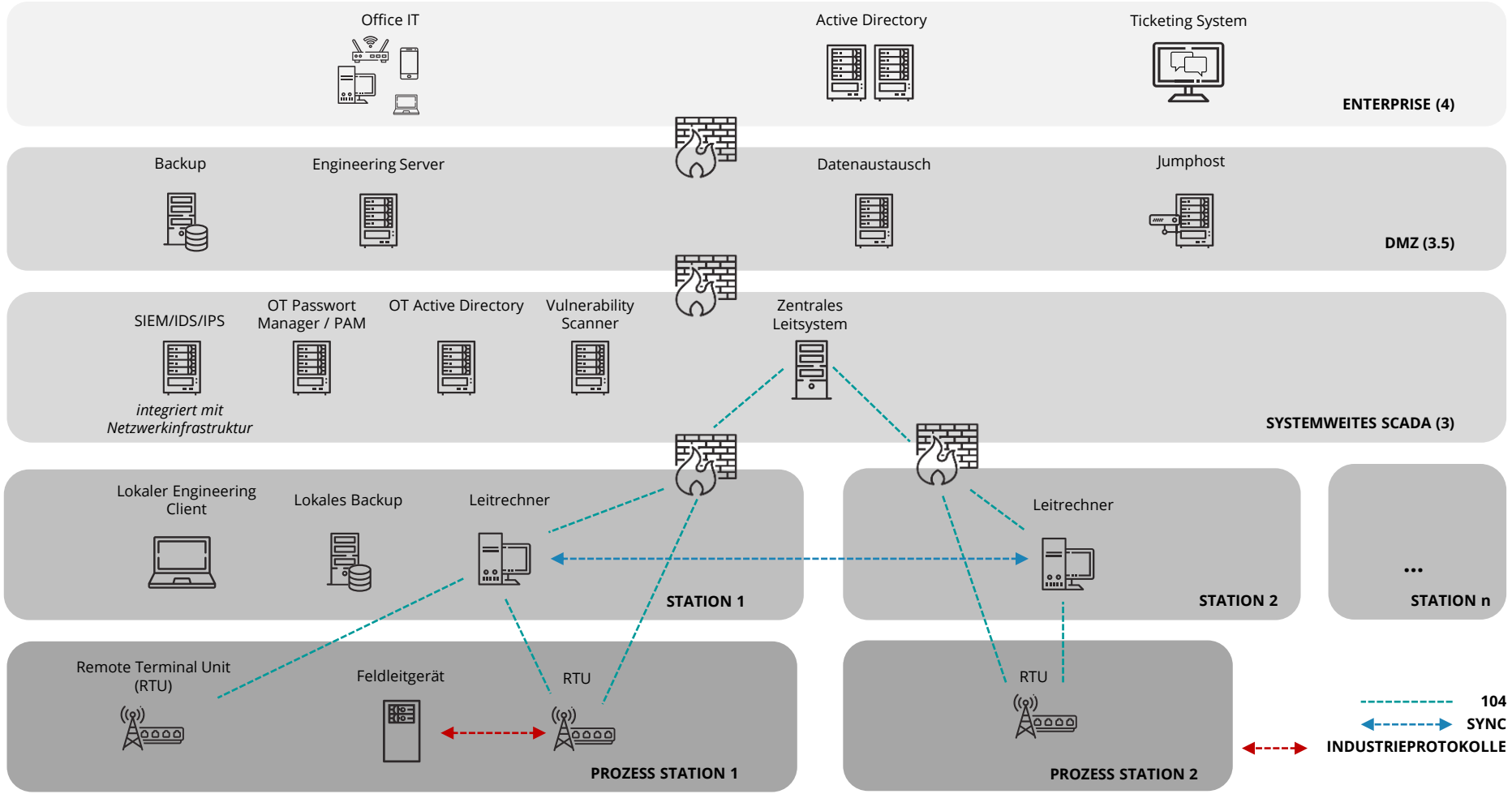
- Im Healthcare bzw. Krankenhaus-Umfeld gibt es viele unsichere Protokolle

  - *Bspl. HL7 oder DICOM*
  - *Insbesondere zw. Subsystemen und/oder KIS*
  - *Große Herausforderung den hohen Grad an Vernetzung zu beherrschen*
  - *KIS & Subsysteme in der*

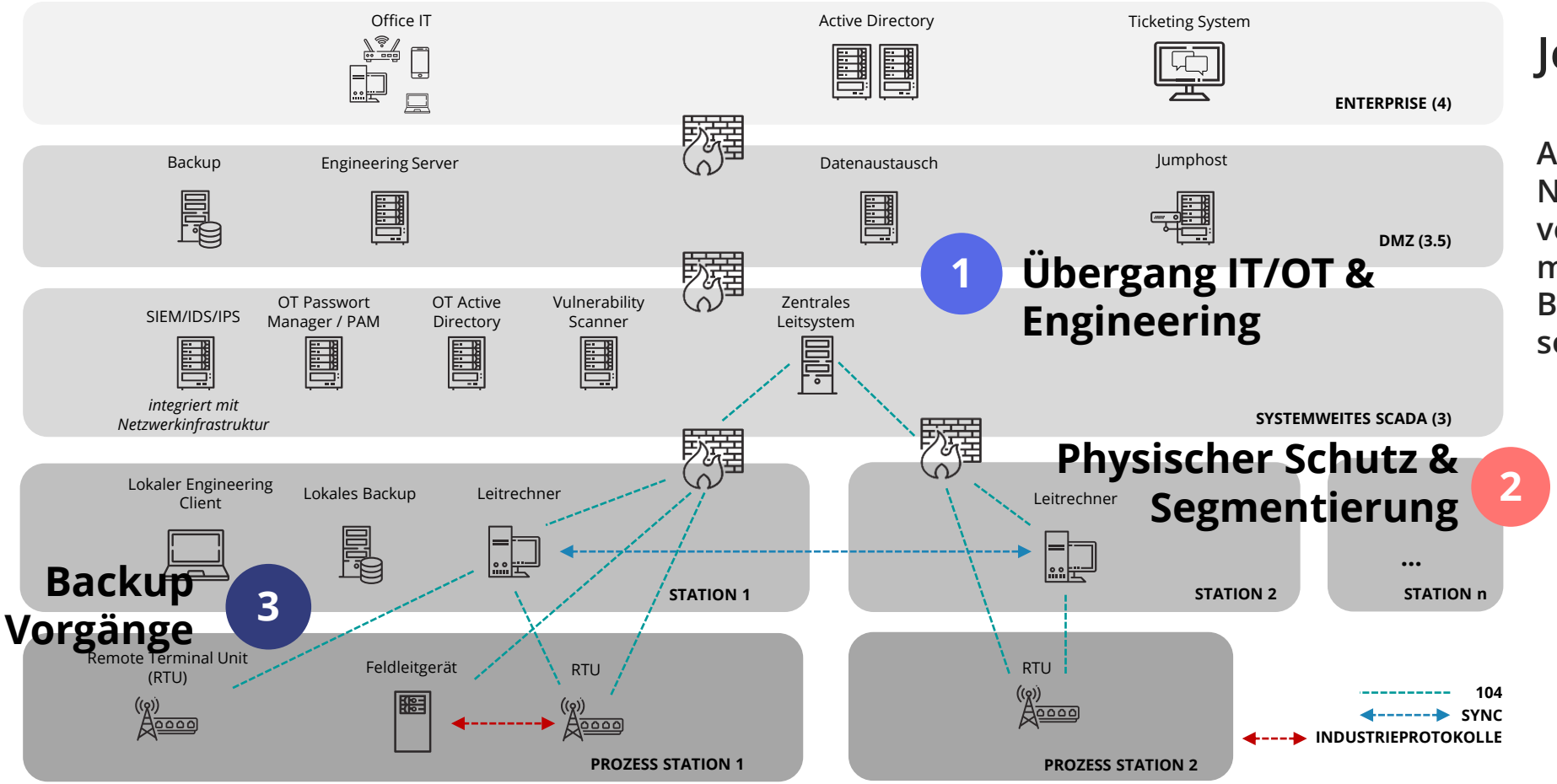
  Corporate Zone wirft viele Fragen auf



Beispiel 3: Energie-Netz Betreiber



Beispiel 3: Energie-Netz Betreiber



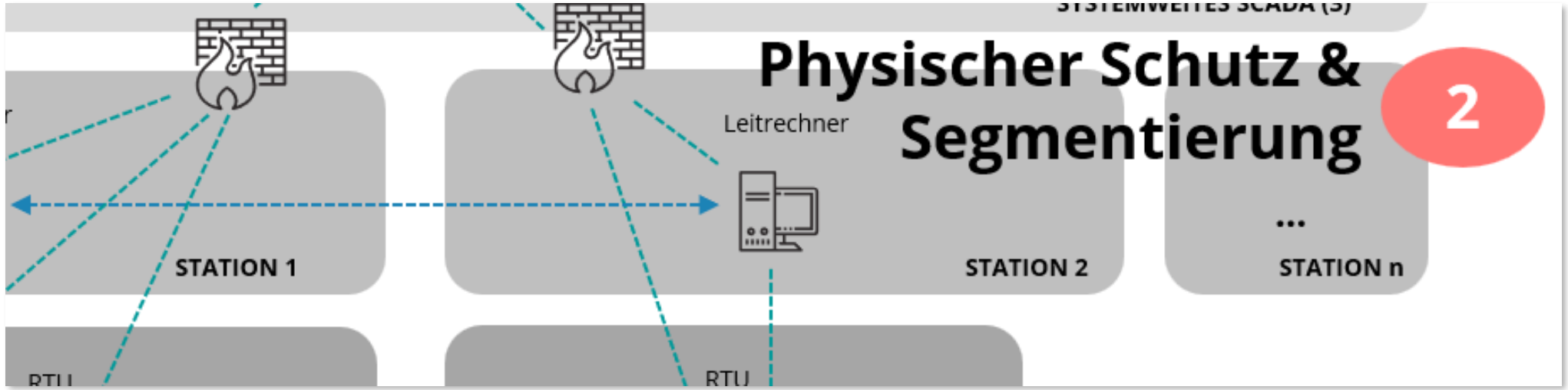
Jetzt sind Sie gefragt!

Auf der abgebildeten Netzwerkgrafik sind drei verschiedene Bereiche markiert. Welcher dieser Bereiche würden einem Prüfer sofort ins Auge fallen?

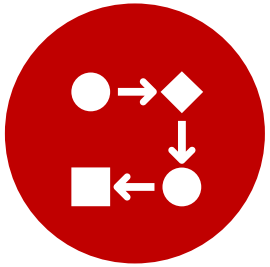
Join at menti.com | use code 6609 6879

Auflösung Beispiel 3

- Potenziell ungefilterte Verbindungsmöglichkeiten zwischen Stationen wirft Fragen bezüglich ausreichend effektiver Segmentierung und/oder physischer Zutrittskontrollen auf



Fallstricke bei Prüfungen



Unwirksame Prozesse

Lieferantenmanagement nicht risikobasiert

Unzureichende Netzsegmentierung

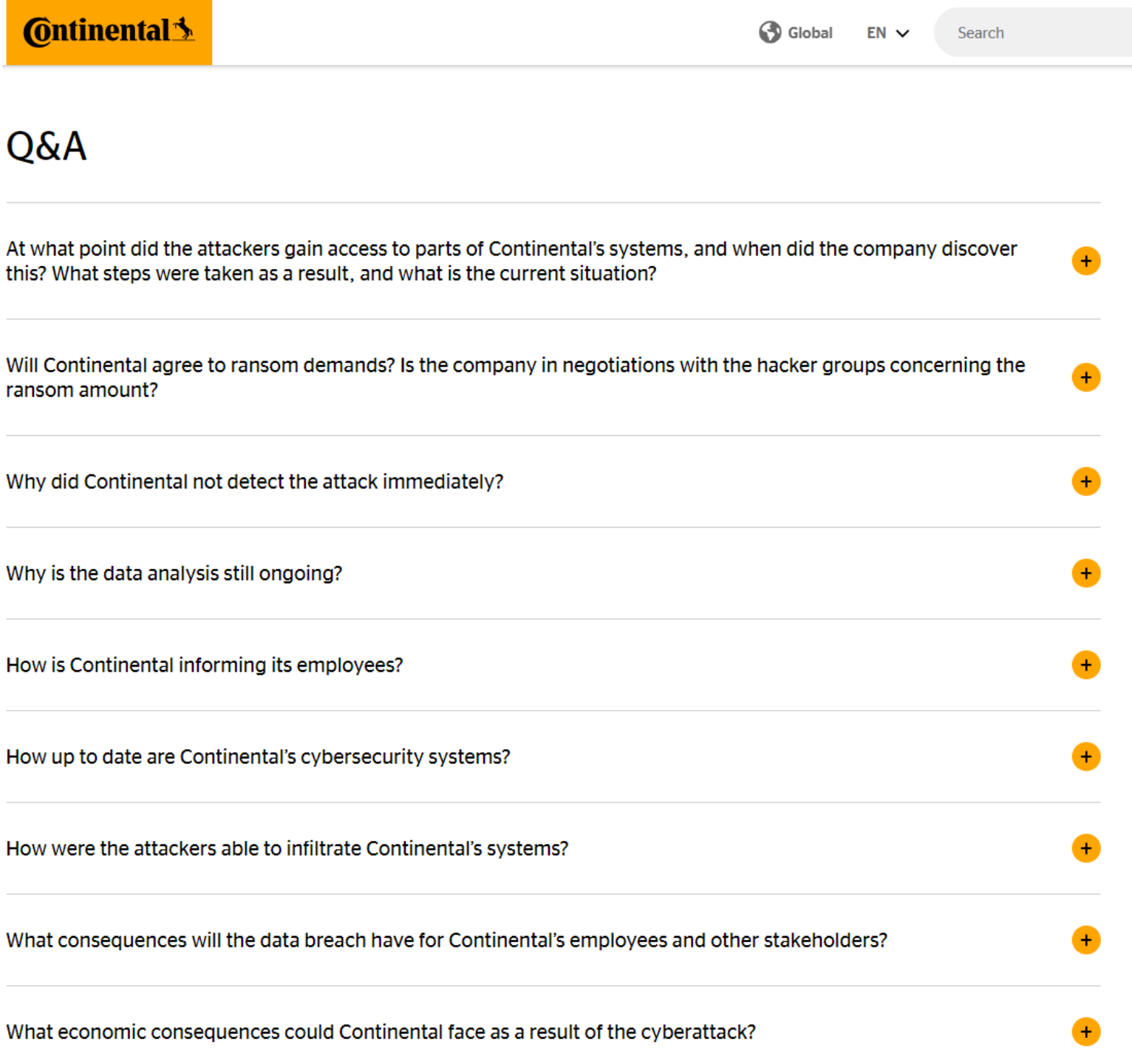
Systemhärtung fehlt

Fehlende Schulungen

Fehlende Ressourcen

Wenn ein Vorfall passiert, werden Sie gefragt wie das passieren konnte

12.05.2025



Vielen Dank!

LIMES
SECURITY

+43 720 510251

office@limessecurity.com