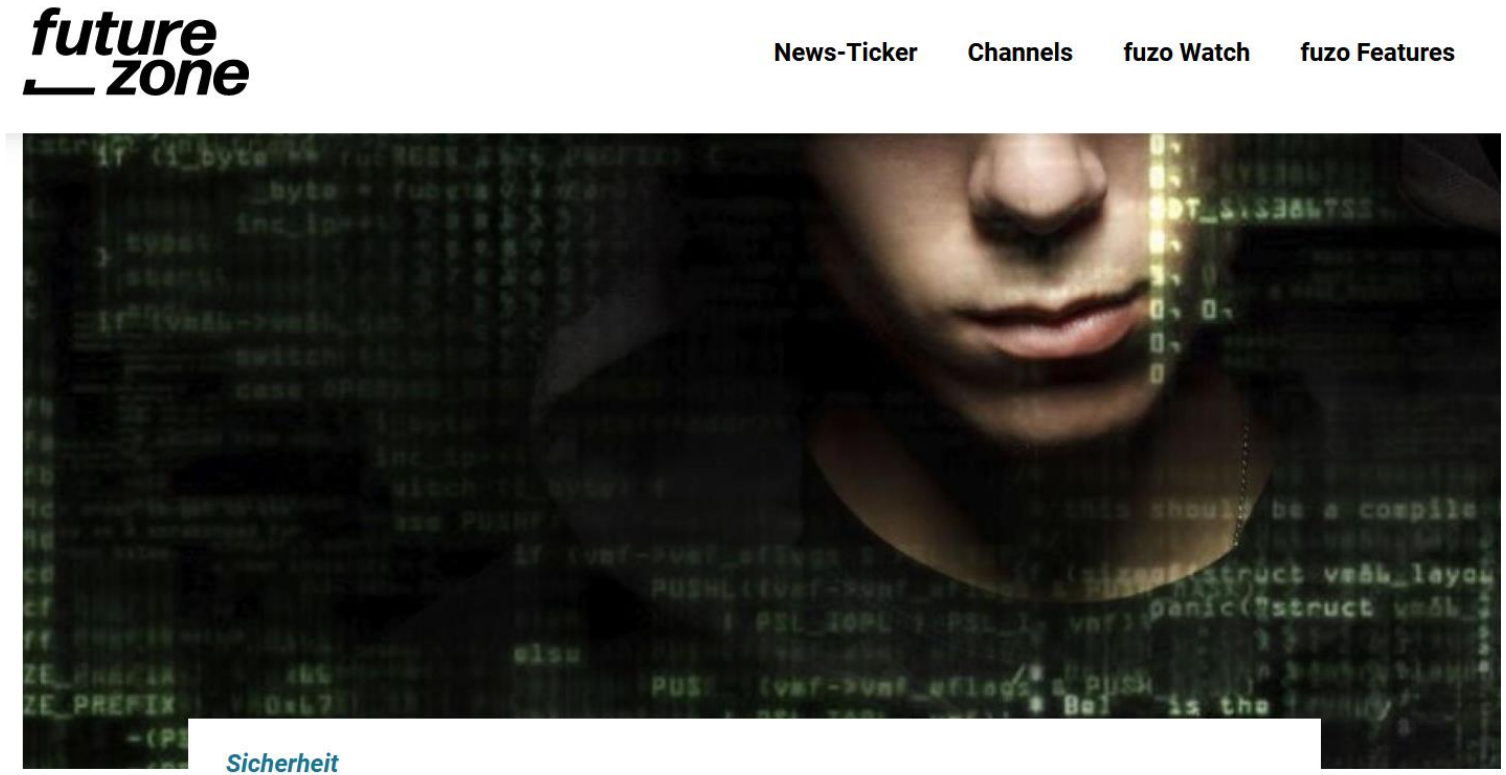
Alles unter eigener Kontrolle?

Welches Wissen rund um Assets wichtig für die Cybersicherheit ist

Thomas Roßmann

Cyberversicherung – Der Allheilsbringer?



www.futurezone.at am 2. November 2015

Cyberversicherung – Die Gegenwart

BearingPoint

ÖVIA

Cyberversicherung: Boom wird auf Eis gelegt

www.versicherungswirtschaft-heute.de am 2. September 2021

Cyberversicherer in der Verlustzone

www.versicherungsmagazin.de am 12. September 2022

GDV: Cyberversicherer machen auf jeden eingenommenen Euro 1,24 Euro Verlust

www.cash-online.de am 7. September 2022

Attackierte Branchen der letzten Jahre

BearingPoint

ÖVIA

Sector	Ranking 2019	Ranking 2020	Ranking 2021
Manufacturing	**8**	**2**	**1**
Finance and Insurance	1	1	2
Professional and business services	5	5	3
Energy	9	3	4
Retail and wholesale	2	4	5
Healthcare	10	7	6
Transportation	3	9	7
Government	6	6	8
Education	7	10	9
Media	4	8	10

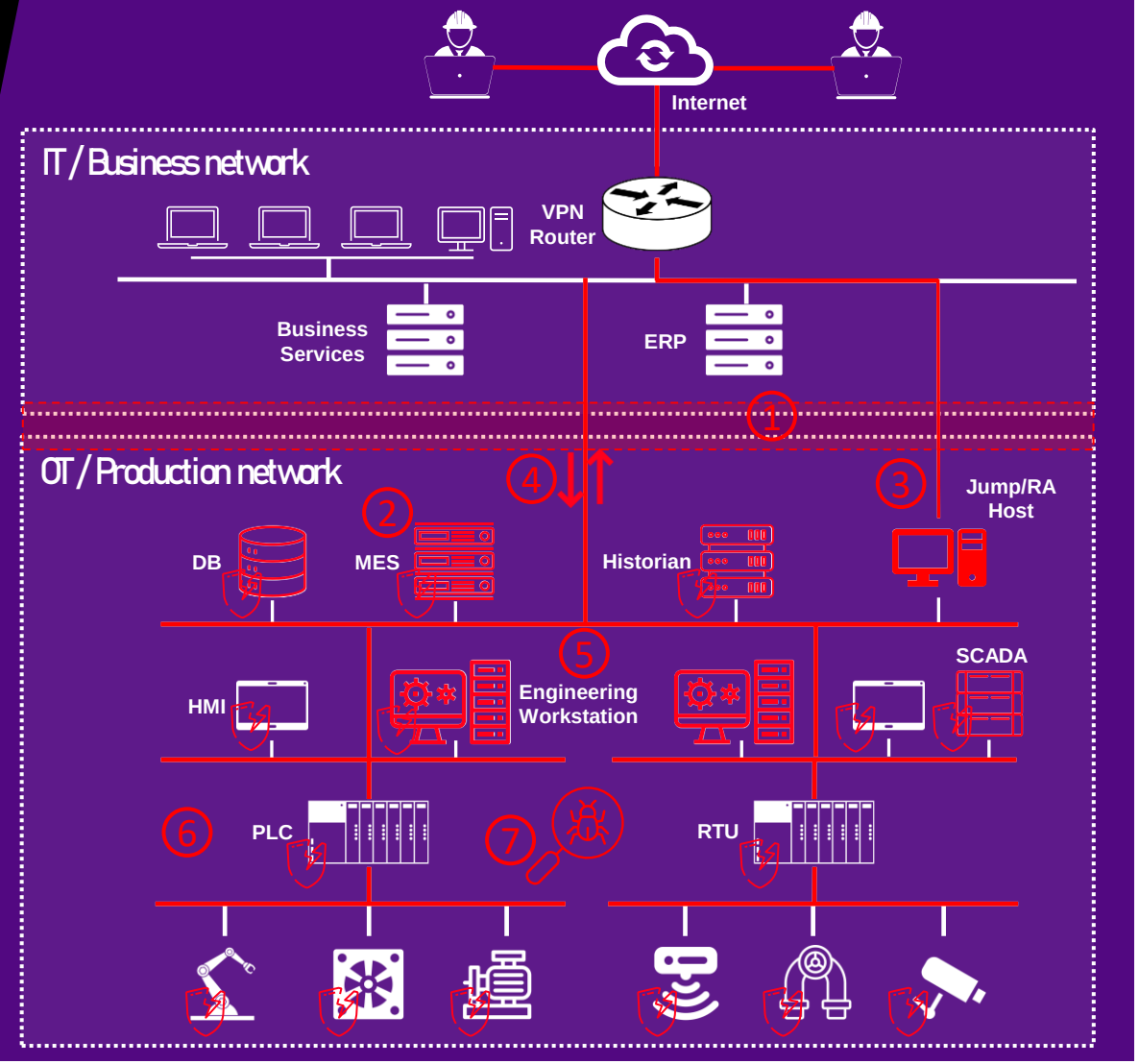
Top 10 most attacked industries – Source: IBM Security X-Force

(Einige) technische Herausforderungen in OT Umgebungen

BearingPoint

ÖVIA

1. Fehlende/schwache Trennung IT/OT
2. Veraltete Systeme / Software (end of life), kein Patching möglich oder verfügbar
3. Unsichere Fernzugriffe
4. Unreglementierter Datenverkehr
5. Keine/unzureichende Segmentierung
6. Kein Asset/Vulnerability Management
7. Kein Monitoring und keine Anomalieerkennung



Cyberversicherung – Die Konsequenzen

- Steigende Prämien
- Technische Schutzmaßnahmen müssen gegeben sein
- Mitarbeiterschulungen werden vorgeschrieben
- Nachweispflicht über umgesetzte Maßnahmen für Versicherte
- Fristen zur Umsetzung von Abwehrmaßnahmen
- Kündigung von Policen bei Nichterfüllung von Auflagen

Probleme bei der Umsetzung von Maßnahmen

Die fatalen Ausgangspositionen

- **Kein Verantwortlicher zum Themengebiet Cybersicherheit**
- **Kein geregelter Betrieb von IT-Hardware die im OT-Umfeld eingesetzt wird**
- **Mangelndes Wissen über die eigenen Assets**
  „Fiktive“ Aussagen bei Befragungen:
  - „Wurde damals von irgendeiner Elektro-Firma aufgebaut“
  - „Kann sein, dass da noch ein paar ältere Windows Systeme sind, vielleicht Windows NT?“
  - „Ich denke dass könnte Herr Mayer wissen, der ist aber letztes Jahr in Pension gegangen“
  - „Die Daten für die Produktionsaufträge kommen irgendwie über das Netzwerk daher“
  - „Möglich dass unser Zulieferer da irgendeinen Zugriff darauf hat“
  - „Zum Erfassen aller Assets fehlt uns die Zeit und das Personal“
  - „Wie man den Automatisierungsrechner neu aufsetzen kann ist eine gute Frage“

Hilfestellungen zur Erhöhung der Cybersicherheit

Normenreihen, Leitfäden, Empfehlungen, etc.

Sämtliche dieser angeführten Publikationen umfassen das Thema Cybersicherheit sehr detailliert. Deren Umsetzung ist jedoch zumeist mit sehr großen Aufwand verbunden!

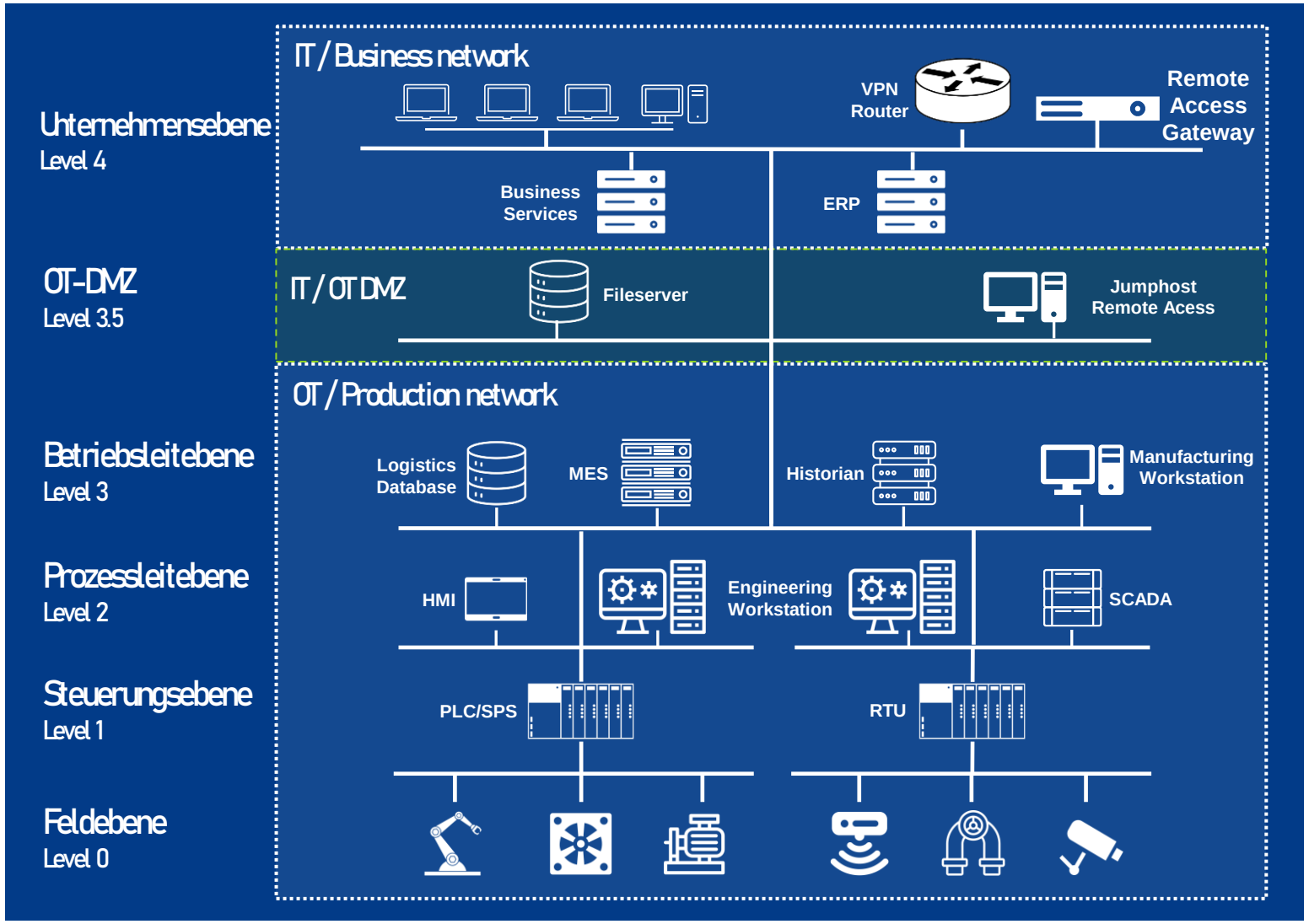
- **ISO/ IEC 27000**
  Reihe zur Informationssicherheit
- **CIS Controls**
  Handlungsempfehlung für Cybersicherheit
- **IEC 62443**
  Normenreihe zur Absicherung von automatisierten Systemen
- **VDI/ VDE – Richtlinie 2182**
  Informationssicherheit in der industriellen Automatisierung.
- **BSI IT-Grundschutz**
  Kompendium vom deutschen Bundesamt für Sicherheit in der Informationstechnik

„Einfache“ Maßnahmen zur Erhöhung der Cybersicherheit

Unter anderem auch Vorgaben von Versicherungen

- **Trennung von IT- und OT-Bereichen**
  - Trennung von OT-Segmenten
  - In Anlehnung an das Purdue-Referenzmodell
- **Einsatz von aktueller Software**
  - Umgang mit nicht patchbaren Systemen
- **Sichere Authentifizierung und gesicherter Fernzugriff**
- **Backups und Wiederherstellbarkeit von kritischen Systemen**

Netztrennung in Anlehnung an das Purdue-Referenzmodell



Notwendige Asset-Informationen zur Netztrennung

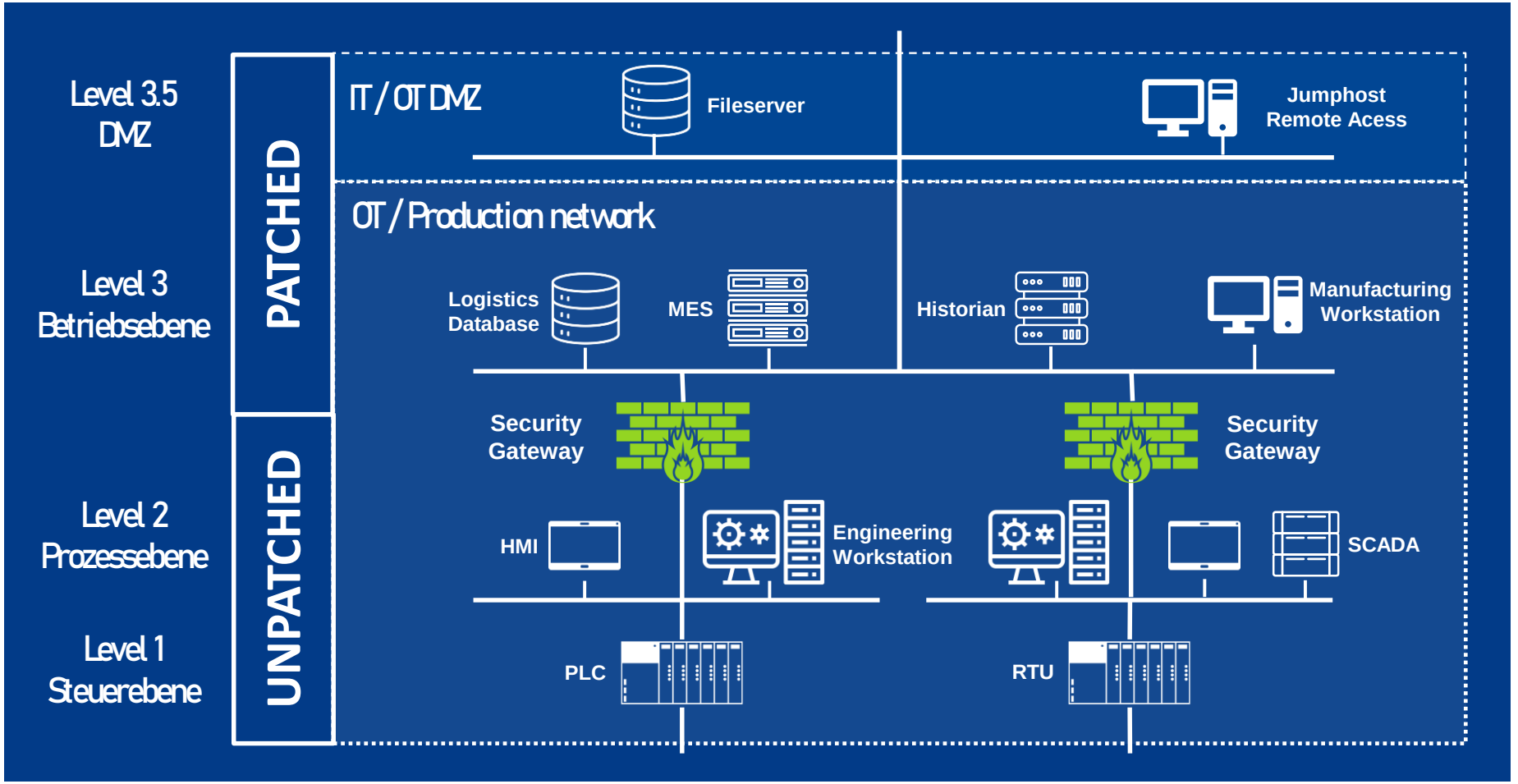
- **Welche Assets sind vorhanden?**
  - Ist die Liste der Assets vollständig?
- **Gibt es für jedes Asset eine Risikoabschätzung?**
- **Können die Assets in eine der Ebenen des Purdue-Referenzmodell zugeordnet werden?**
  - Sind ein und dieselben Assets für verschiedene Funktionen eingesetzt?
- **Kommunikation zwischen Assets**
  - Welche Daten werden zu meinen Assets übertragen?
  - In welche Richtung erfolgt die Verbindungsaufbau?
  - Mit welchen Protokollen erfolgt die Datenübertragung?
  - Erfolgt die Übertragung gesichert (Authentifizierung und Verschlüsselung der Verbindung)?

Einsatz von aktueller Software

- **Sind die Software-Stände meiner Assets bekannt?**
  - Version des Betriebssystem mitsamt Patch-Levels
  - Server-Dienste einschließlich Konfiguration
  - Eingesetzte Applikationen
- **Wie schnell können neue Sicherheits-Updates eingespielt werden?**
- **Welche Updates gefährden die Funktionalität meiner Assets?**
- **Für welche Assets erscheinen keine Sicherheits-Updates mehr?**
  - Gibt es für diese Assets bereits bekannte Sicherheitslücken?
  - Welche Maßnahmen wurden getroffen, um bekannte Sicherheitslücken unschädlich zu machen?

Nicht gepatchtes Systeme

Abschottung zum restlichen Netzwerk



Gesicherter Zugriff auf Assets

- **Wie erfolgt die Authentifizierung?**
  - Werden Standard-Passwörter eingesetzt?
  - Sind über mehrere Personen geteilte Administrator-Accounts im Einsatz?
  - Gibt es verschiedene Zugriffsberechtigungen?
  - Welcher Personenkreis hat Zugriff?
- **Wie erfolgt ein Fernzugriff?**
  - Auf welche Assets kann von der Ferne zugegriffen werden?
  - Über welche Protokolle findet der Fernzugriff statt?
  - Ist der Nutzerkreis für den Remote-Zugriff bekannt?
  - Erfolgt eine Netzkoppelung mit anderen Organisationen oder Geräten?
  - Sind die Tätigkeiten eines Remote-Zugriffs im Nachhinein nachvollziehbar?
  - Werden Remote-Access Lösungen von Lieferanten eingebracht?

Backups und Wiederherstellung von Assets

- **Gibt es Sicherungskopien für die Wiederherstellung von Assets?**
  - Betriebssysteme, Applikationen, Konfigurationen, etc.
- **Sind Sicherungskopien eigens geschützt (z. B. offline abgespeichert)?**
- **Ist das Wissen im Unternehmen vorhanden, um eine Wiederherstellung durchzuführen?**
  - Sind die Pläne zur Wiederherstellung verschriftlicht und für das notwendige Personal einsehbar?
- **Kann und wird die Wiederherstellbarkeit insbesondere von kritischen Assets regelmäßig geprüft?**
- **Ist die passende Hardware wie Speichermedien, etc. vorhanden, um die Wiederherstellung durchzuführen?**
- **Wie lange dauert die Wiederherstellung schlimmstenfalls?**

Alles unter eigener Kontrolle?

Welches Wissen rund um Assets wichtig für die Cybersicherheit ist

Thomas Roßmann

Kontakt: thomas.rossmann@bearingpoint.com