

PLATTFORM WASSER BURGENLAND

Interessengemeinschaft
burgenländischer
Wasserversorger

INFOTAG PLATTFORM WASSER BURGENLAND 2019



KRYPTO - Trojaner

This computer and all of it's files have been locked! Send an email to redboot@emeware.net containing your ID key for instructions on how to unlock them. Your ID key is 79E7794CEE8BDF34EE595914D968AAAD2E355904_



MASSNAHMEN GEGEN CYBERATTACKEN beim WLNVNB

5 „Tibeter“ des Multibarrierenkonzepts zur Erhöhung der Cybersicherheit

1. Identifizieren

- Asset Management - Anlagenverwaltung
- Risikobewertung

2. Schützen

- physischer Zugangsschutz der Anlagen & Büros
- Zugangskontrolle
- Schutz des Fernwirknetzwerkes

3. Erkennen

- Bestimmen Sie die Auswirkungen möglicher Events
- Sicherstellen, dass Aktivitäten von externen Dienstleistern überwacht werden

5 „Tibeter“ des Multibarrierenkonzepts zur Erhöhung der Cybersicherheit

4. Reagieren

- Ergreifen von Maßnahmen gegen einen eingetretenen Cybersicherheitsvorfall

5. Wiederherstellen

- Wiederherstellungsplanung
- Backups

IKT oder Strom AUS bedeutet „NICHT sofort“ Wasser AUS !!

5 „Tibeter“ des Multibarrierenkonzepts zur Erhöhung der Cybersicherheit

Identifizieren

- Asset Management - Anlagenverwaltung
- Risikobewertung

Asset Management

Richtfunk Begas
Anbindung Heuberg
Line 8 IEC-870-S-101
Line 7 Seab 1F - TCP/IP

Serial/Ethernet Converter

Analoger Funk



WIKIPEDIA
Die freie Enzyklopädie

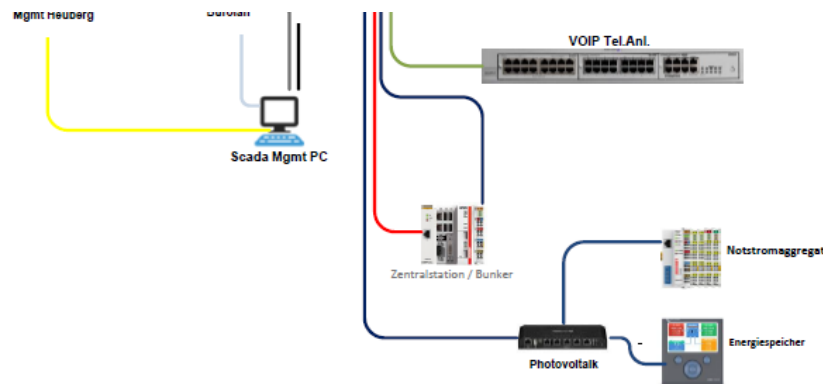
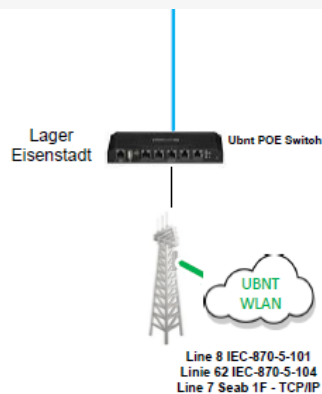
Hauptseite
Themenportale
Zufälliger Artikel

Artikel Diskussion

Asset-Management

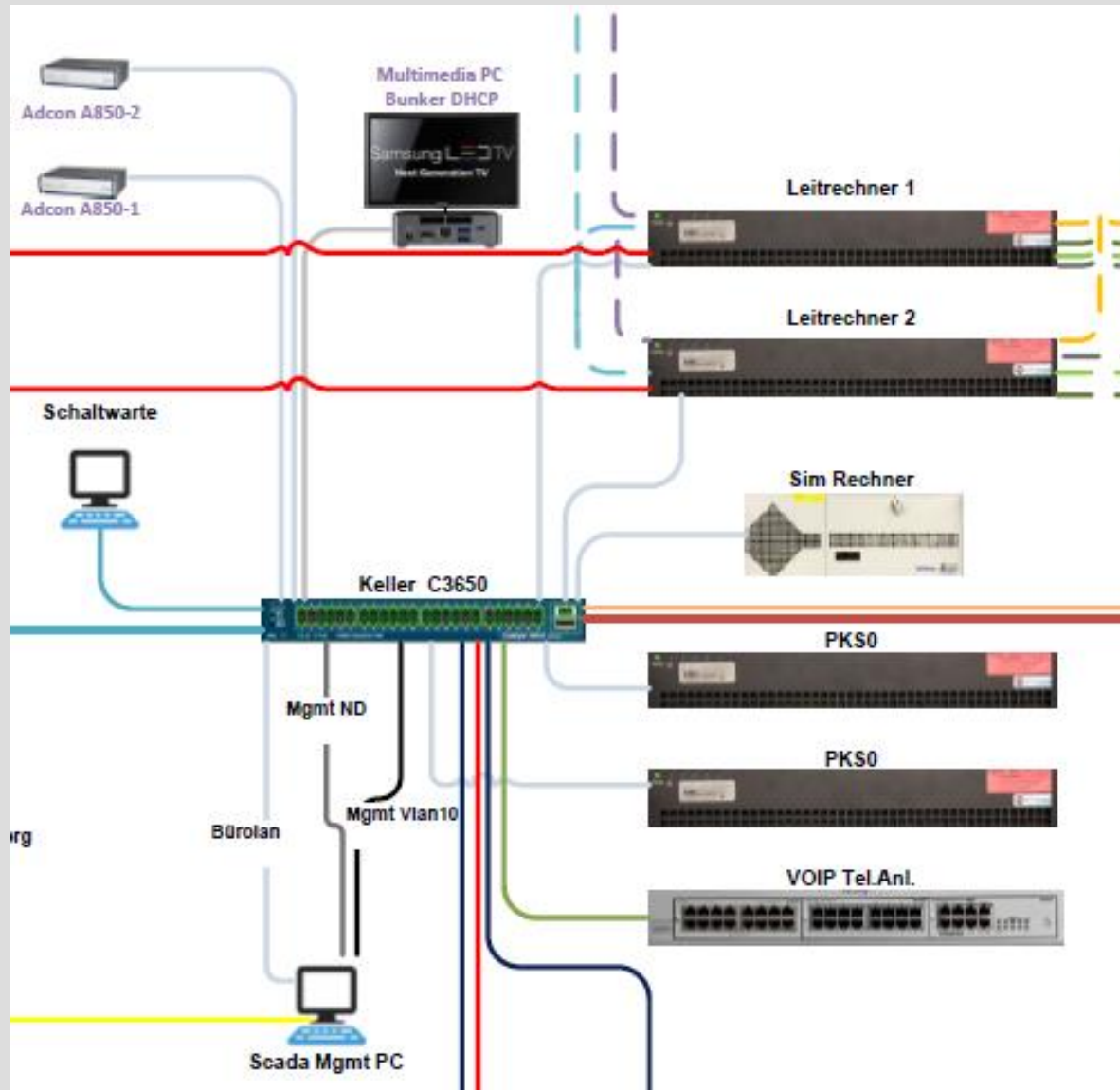
Der englische Begriff **Asset-Management** steht für

- **Vermögensverwaltung**, die Betreuung eines Finanzportfolios
- **Anlagenwirtschaft**, die Verwaltung der Anlagen eines Unternehmens
- **Software-Lizenzmanagement**, Software Asset-Management in Unternehmen

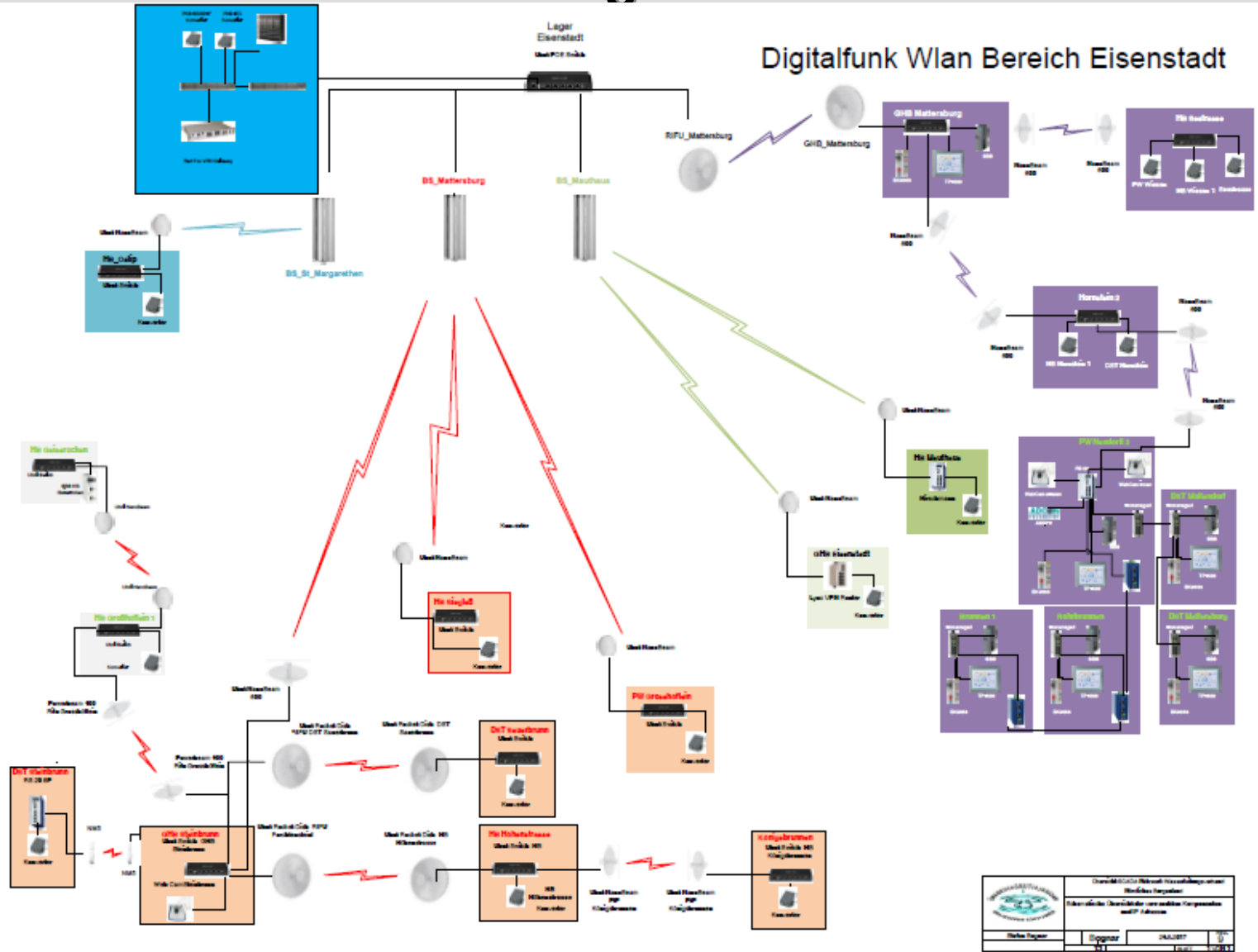


Bunker

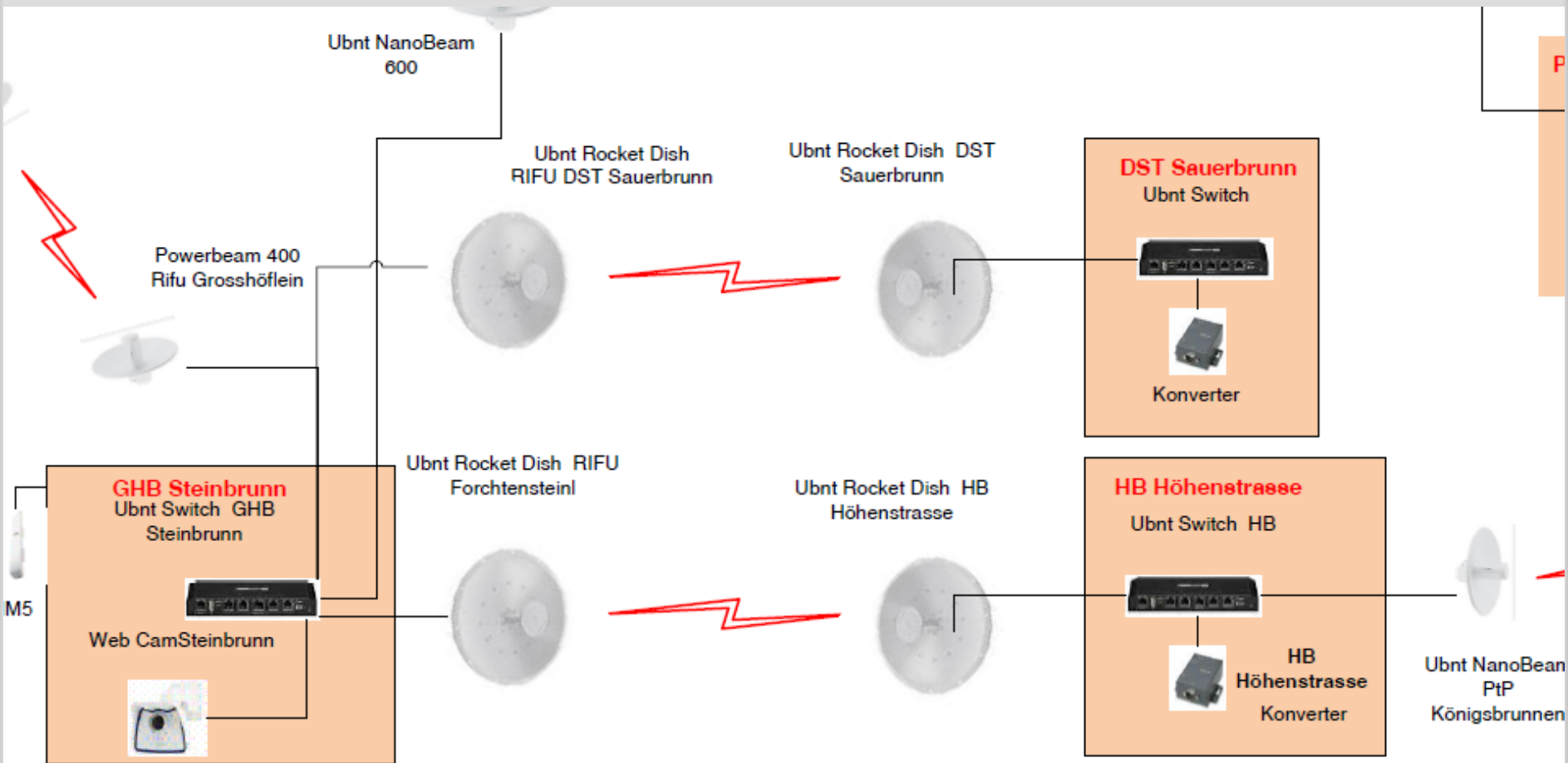
Asset Management



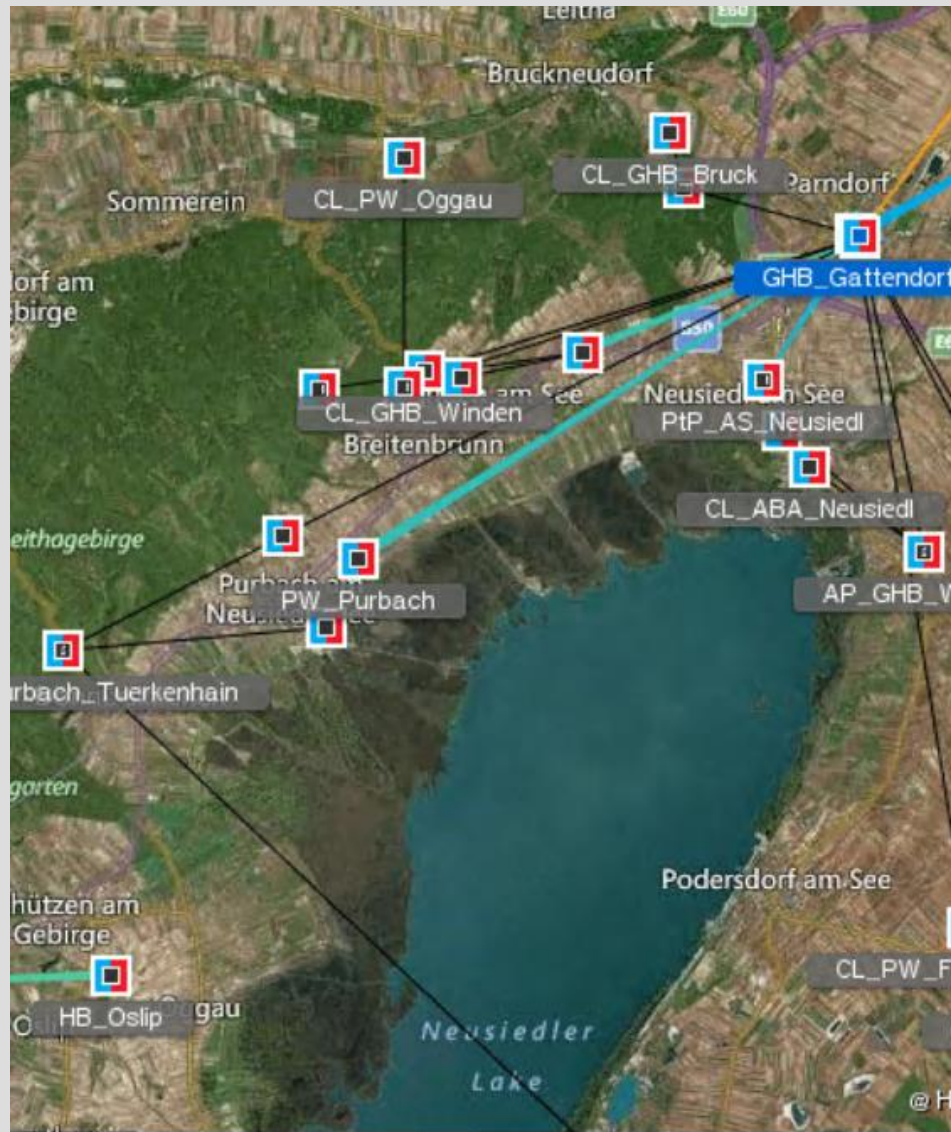
Asset Management



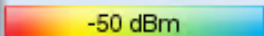
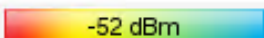
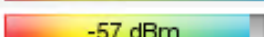
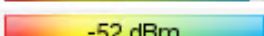
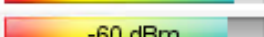
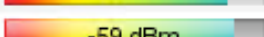
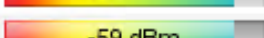
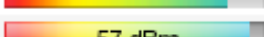
Asset Management



Asset Management



Asset Management

Device Name	Device Status	CCQ	Signal Strength	Frequency	Firmware Ve
CL_GHB_Gattendorf_Mast	 online	78 %	 -47 dBm	5675 MHz	6.1.9 (XW)
HB_Rosalia	 online	87 %	 -48 dBm	5520 MHz	6.1.9 (XW)
AP_RIFU_ND_PARNDORF	 online	97 %	 -47 dBm	5640 MHz	6.1.9 (XW)
WLV_RIFU_OST_AP	 online	80 %	 -50 dBm	5675 MHz	6.1.9 (XW)
CL_RIFU_GHB_ZAGERSDORF	 online	90 %	 -52 dBm	5540 MHz	6.1.9 (XW)
AP_RIFU_GHB_ZAGERSDORF	 online	99 %	 -52 dBm	5540 MHz	6.1.9 (XW)
CL_Quelle_Winden	 online	99 %	 -53 dBm	5635 MHz	6.1.9 (XW)
CL_PW_T@@rkenhain	 online	85 %	 -54 dBm	5600 MHz	6.1.9 (XW)
GHB_WEIDEN	 online	58 %	 -54 dBm	5650 MHz	6.1.9 (XW)
GHB_STeinbrunn	 online	99 %	 -55 dBm	5205 MHz	6.1.9 (XW)
PW_Frauenkirchen	 online	62 %	 -57 dBm	5650 MHz	6.1.9 (XW)
AP_ABA_Gols	 online	74 %	 -52 dBm	5635 MHz	6.1.9 (XW)
Ap_Rifu_Pw_T@@rkenhain	 online	94 %	 -59 dBm	5600 MHz	6.1.9 (XW)
RIFU_ASND_Client	 online	97 %	 -60 dBm	5640 MHz	6.1.9 (XW)
ptp_ABA_ND	 online	70 %	 -59 dBm	5500 MHz	6.1.9 (XW)
CL_GHB_M@@nchhof	 online	66 %	 -59 dBm	5650 MHz	6.1.9 (XW)
CL_HB_Marz	 online	98 %	 -60 dBm	5630 MHz	6.2.0 (XW)
AP_DST_Illmitz-M@@rb	 online	99 %	 -57 dBm	5330 MHz	6.1.9 (XW)
Halbturn	 online	62 %	 -60 dBm	5650 MHz	6.1.9 (XW)

Asset Management

Summary Config Software Performance Uptime Location Events

Asset type: Windows

Last user: Bernhard Hanifl

OS: Windows 10 Pro (64 bit)

Build: 10.0.17763.805

Version: 1809

Domain: WLVNB

Manufacturer: Lenovo

Model: ThinkCentre M900

SKU: LENOVO_MT_10FL_BU_LENOVO_FM_ThinkCentre M900

Memory: 16 GB

Processor: Intel Core i7-6700T CPU @ 2.80GHz

Motherboard: LENOVO 30D0

Graphics: Intel(R) HD Graphics 530 1 GB

Audio: Intel(R) Display-Audio
 Realtek High Definition Audio

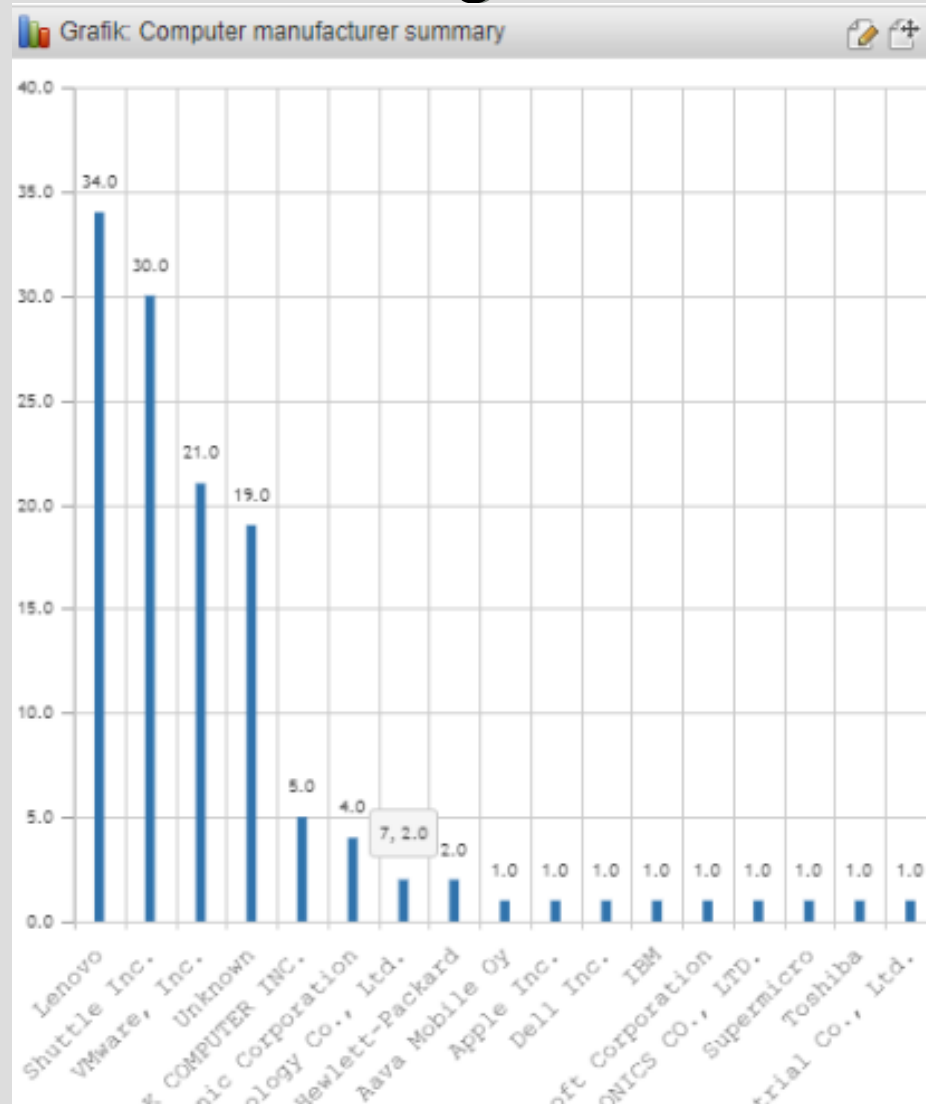
Antivirus: Traps™ Advanced Endpoint Protection **Enabled & Up To Date**
 Windows Defender **Disabled & Up To Date**

Network: Intel(R) Ethernet Connection (2) I219-LM - 00:23:24:DC:C7:E7
10.241.200.82 CA3560_LA.wlvnb.net ↔ 10108 | GigabitEthernet0/8 (Gi0/8)
25/10/2019 09:50:57

Harddisk: C: 171,4 GB free of 237,2 GB

OU: CN=Computers, DC=wlvnb, DC=net

Asset Management

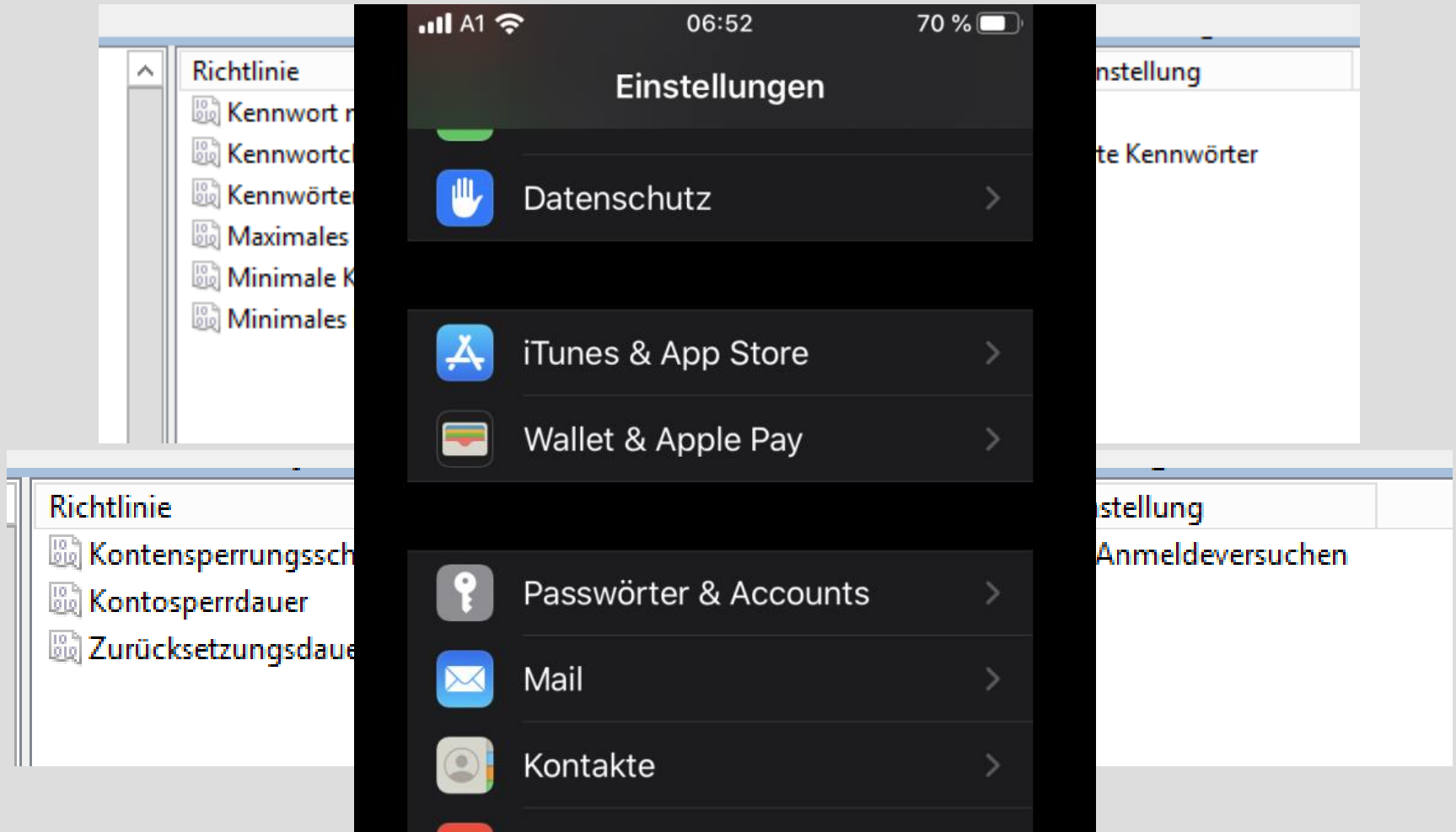


5 „Tibeter“ des Multibarrierenkonzepts zur Erhöhung der Cybersicherheit

Schützen

- physischer Zugangsschutz der Anlagen & Büros
Sicherheitstüren Anlagen, Büros versperren
- Zugangs – Zugriffskontrolle, Feststellen der Identität, Besucher
- End – Point Echtzeit Security „Palo-Alto Traps“
- Wechseldatenträger

Zugriffsschutz - Passwörter

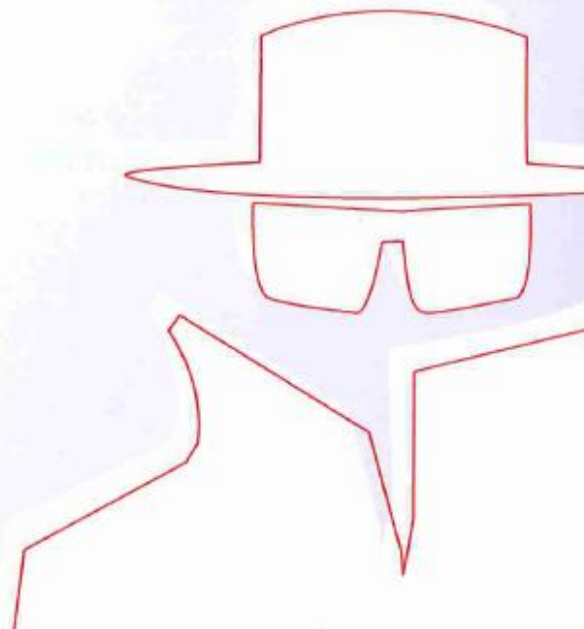


 **Bundesministerium
Inneres**

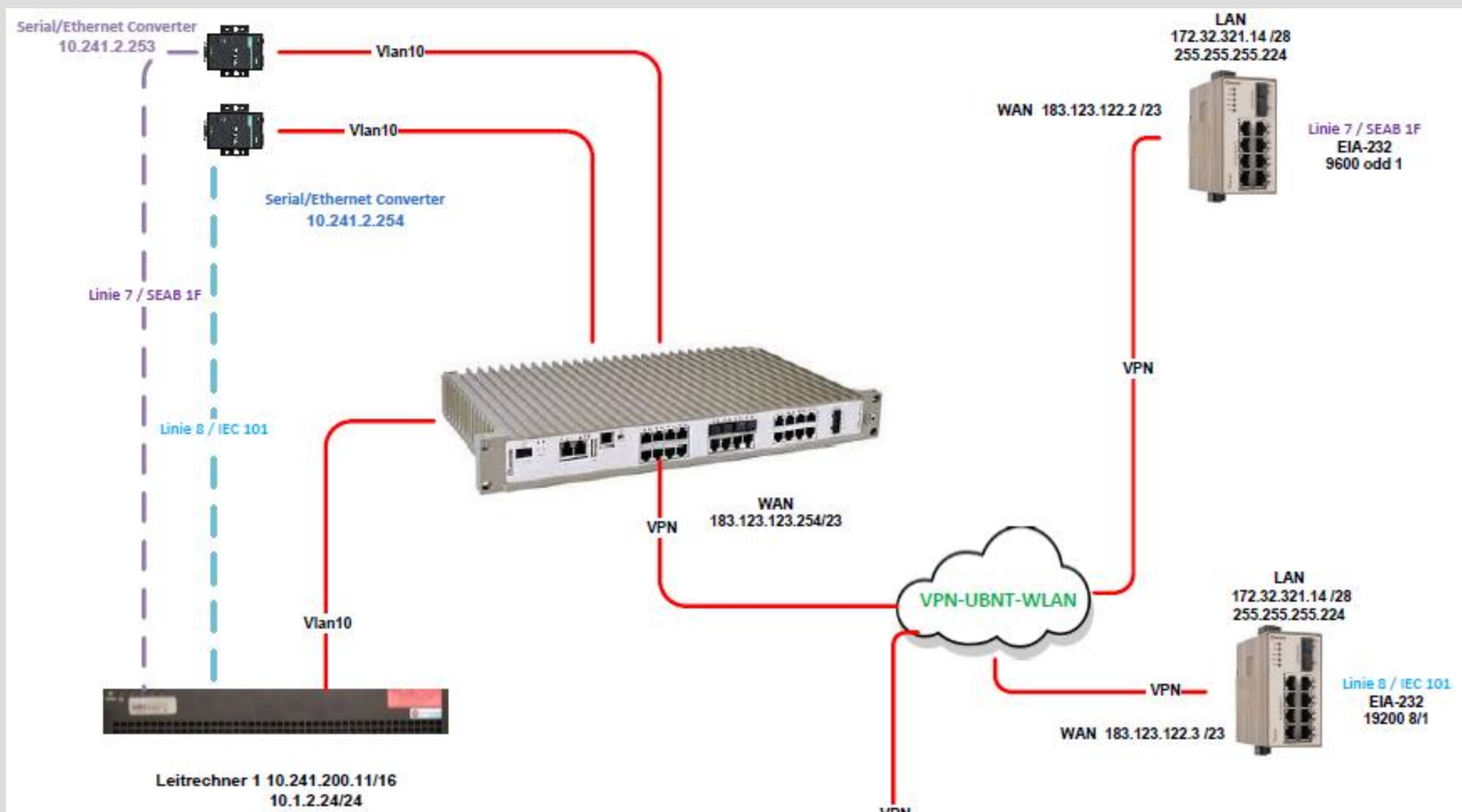
Bundesamt für Verfassungsschutz
und Terrorismusbekämpfung

Innentäter – Risiko für Unternehmen

Hintergründe &
Handlungsempfehlungen



Schutz Fernwirknetz - Trennung



Schutz Fernwirknetz - Risikobewertung



Risikobewertung je Anlage

Schutz Fernwirknetz

Ganzheitlicher Schutz vor Cyberangriffen in Produktionsanlagen



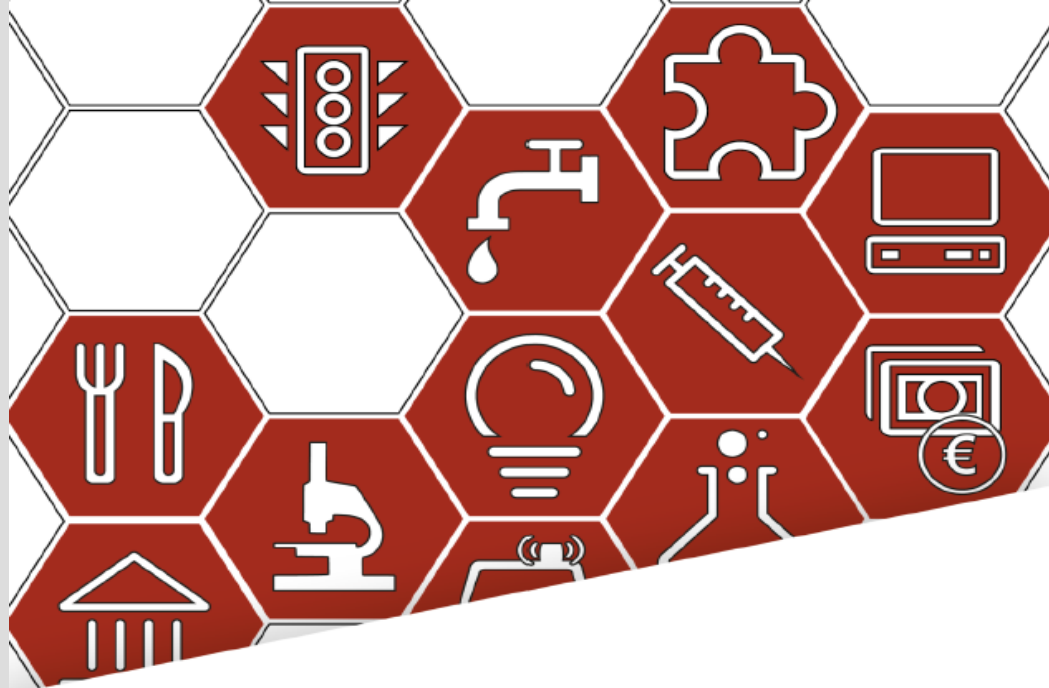
- Identifikation aller IT-Systeme in Produktionsanlagen
 - 360° Scan
 - passiv und ohne Aktivitäten im Industrial Ethernet
- Einfache Beurteilung im Risiko Management
 - Zentrale Analyse der Netzwerke und IT-Komponenten in MES, SCADA, SPS und PLC
- Kontinuität für den Überwachungsprozess
 - Automatisiert
 - integriert in das Alarmmanagement



Industrie Risiko Management Automatisierung

ZUGRIFFSKONTROLLE – iPhone & Co





März 2017

Sicherheitsratschläge zu iPhone & Co

20 Empfehlungen und präventive Maßnahmen

BM.I

REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
BUNDESAMT FÜR VERFASSUNGSSCHUTZ UND TERRORISMUSBEKÄMPFUNG





Inhalt

1.	Firmware-Updates	5
2.	Schutz gegen unbefugte Nutzung	6
3.	Deaktivieren von Sperrbildschirm-Benachrichtigungen	7
4.	Zwei-Faktor-Authentifizierung	7
5.	Deaktivieren von Siri auf dem Sperrbildschirm.....	8
6.	Deaktivieren der Synchronisierung mit der iCloud.....	8
7.	Verhindern automatischer WLAN-Verbindungen	8
8.	Verwendung eines VPN	9
9.	AirDrop deaktivieren	9
10.	WLAN und Bluetooth sicher nutzen.....	10
11.	Deaktivieren der Auto-Ausfüllen-Funktion in Safari	10
12.	Zugriffe von Apps auf private Daten verhindern	11
13.	E-Mail Sicherheit	11
14.	Bilder in E-Mails	12
15.	Mein iPhone suchen	13
16.	Ortungsdienste	13
17.	Jailbreak or not?	14
18.	WLAN-Passwort.....	14
19.	Schutz Ihrer Privatsphäre	15
20.	Regelmäßiges Backup	16

Schützen & Verwalten mobiler Geräte

- SOPHOS für Android & iOS
- Aktivierung Bitlocker auf allen Lap-Tops und Tablets
- Aktivierung BIOS Passwort auf allen Lap-Tops und Tablets
- Zugriff WLAN über Windows - Zertifizierung
- Fernzugriff nur über VPN – Tunnel bzw.
- Teamviewer
- Anwendung der Benutzer- und Gruppenrichtlinien



Geräte

- ✓ iOS, Android, Windows 10, macOS
- ✓ Konfiguration und Richtlinien
- ✓ Inventarverwaltung und Asset Management
- ✓ Detailliertes Reporting



Anwendungen

- ✓ Installation, Entfernung und Anzeige von Anwendungen
- ✓ Enterprise App Store
- ✓ App Control, Whitelist/Blacklist
- ✓ Verwaltung und Konfiguration von Office-365-Anwendungen



Inhalte

- ✓ E-Mail- und Dokument-Container
- ✓ Veröffentlichung von Inhalten
- ✓ Reine Container-Verwaltung
- ✓ Native Betriebssystem-Containerisierung



Sicherheit

- ✓ Compliance-Regeln und -Wiederherstellung
- ✓ Malware, Ransomware, PUAs
- ✓ Anti-Phishing
- ✓ Web Protection, Web-Filterung

5 „Tibeter“ des Multibarrierenkonzepts zur Erhöhung der Cybersicherheit

Erkennen

- Bestimmen Sie die Auswirkungen möglicher Events, kann Teil der Risikoanalyse lt. W88 sein
- Sicherstellen, dass Aktivitäten von externen Dienstleistern überwacht werden, 2 Faktor Authentifizierung
- Durchführung eines jährlichen Security – Checks
- Im NIS Bereich – alle 3 Jahre ein Audit

Erkennen

Ganzheitlicher Schutz vor Cyberangriffen in Produktionsanlagen

The interface displays a list of devices and their status:

Device	Status	Percentage
CL_HB_Marz	online	98 %
AP_DST_Illnitz-M@@b	online	99 %
Halbturn	online	62 %

Navigation tabs: Statistics, Charts, Events, Alerts, Configurations

Event Log (2019.10.23 (6)):

Event	Date	Device
LAN unplugged	2019.10.23 11:37:50	GHB_Gatte
LAN unplugged	2019.10.23 11:04:25	GHB_Gatte
geht online	2019.10.23 11:04:25	GHB_Gatte
Came back online	2019.10.23 11:04:24	GHB_Gatte
offline	2019.10.23 10:52:58	GHB_Gatte
Gone offline	2019.10.23 10:52:57	GHB_Gatte

This computer and all of it's files have been locked! Send an email to redboot@emcware.net containing your ID key for instructions on how to unlock them. Your ID key is 79E7794CEE8BDF34EE595914D968A0AD2E355904_



Website gemacht, auf der Sie Spaß

The control panel includes buttons for various components:

- Zentralstation (OK)
- Tankstelle (STÖRUNG)
- Notstromaggregat (STÖRUNG)
- USV-Anlage (STÖRUNG)

Additional status indicators:

- Quelle Winden (OK)
- BRUNNENFELD OPC-Kopplung (GESTÖRT)
- Brunnenfeld Neudörfel
- Wetterstationen

5 „Tibeter“ des Multibarrierenkonzepts zur Erhöhung der Cybersicherheit

Reagieren

- Ergreifen von Maßnahmen gegen einen eingetretenen Cybersicherheitsvorfall – Arbeitsanweisungen – Notfallhandbuch W74 – Notbedienebene
- AWARENESS („Bewusstsein“) Schulungen im Haus

**IKT oder Strom AUS
bedeutet „NICHT
sofort“ Wasser AUS !!**

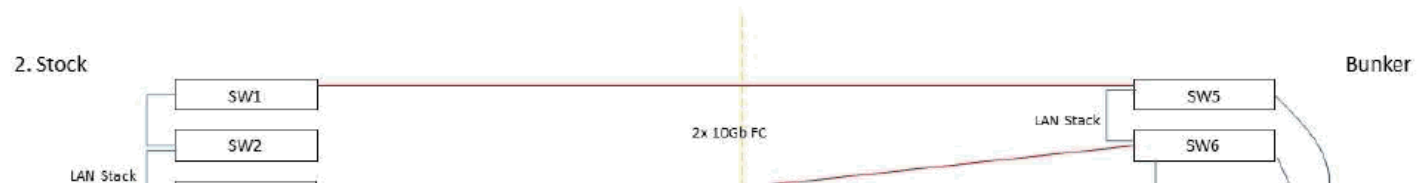
5 „Tibeter“ des Multibarrierenkonzepts zur Erhöhung der Cybersicherheit

Wiederherstellen & Backup

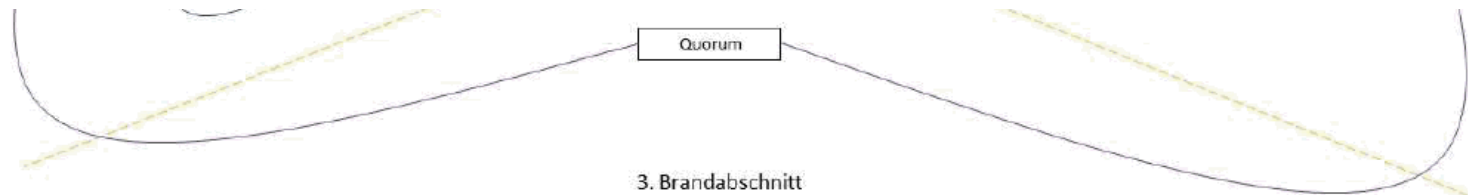
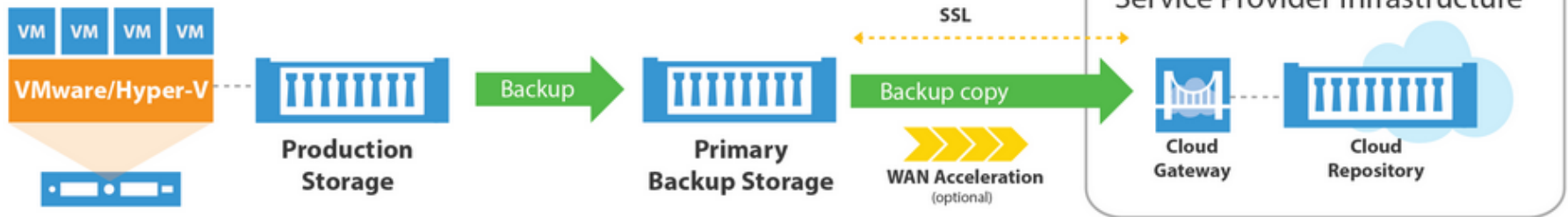
- Für Office & Fernwirk Systeme



Internes & externes Backup



Customer On-Premises Infrastructure



Recover - Dokumentation

Dateien zum Wiederherstellen auswählen

Daten zum Wiederherstellen auswählen

Auswählen aus Dateien ab Auftrag ▼

22.10.2019 ▼

Aktuellste/r/s ▼

Filter anzeigen

Ordner	Name	Größe	Änderungsdatum
D:\	☒ Verzeichnis_Rechtsbibliothek.xlsx	27 KB	04.07.2018 13:14
\$RECYCLE.BIN			
A0BEARB			
ALLGEMEIN			
BETRIEBSRAT			
DKM			
EXCEL			
File-Access-Log			
INTERN			
LOHN			
MOBILDAT			
ND			
SCAN			
SEKRETARIAT			
WLW			
Informationstech			
Personal			
Rechtsbibliothek			

Suchen

Elemente pro Seite

50 ▼

Seite

1 / 1 ▼

Die Polizeiliche Kriminalstatistik 2018

Österreich ist so sicher wie noch nie





Cyber Crime