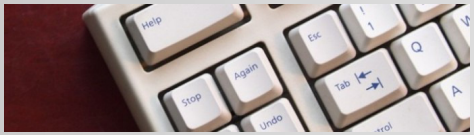
Ihr Zugang zum digitalen Puls der Zeit

IT-Sicherheit in der Gebäudeautomation

Praktisch und wirtschaftlich lösen

04.04.2019

So soll es nicht sein



Ihr Zugang zum digitalen Puls der Zeit

heidelberg24.de

02.10.2018

Kokelnder Sandwich-Maker verursacht „nur“ 10.000 Euro Schaden

Am Dienstagmorgen hört eine 22-jährige Mieterin gegen 09.15 Uhr in einem …

F-Secure Presseraum

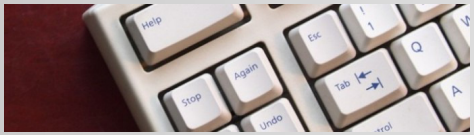
25.04.2018

Schwachstelle: Millionen Hotelzimmer lassen sich hacken

Schlüsselkarten int. Hotelketten und Hotels können gehackt werden – damit steht der Zugang …

Wie verhindern/ vorbeugen?

Proaktive Sicherheit



Ihr Zugang zum digitalen Puls der Zeit

Einfache allgemeingültige Grundregeln aufstellen

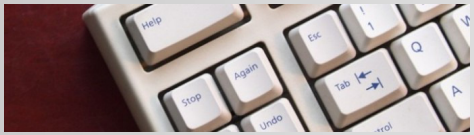
- An Gefahrenstellen (Herd) darf nichts gelagert werden (z.B. einen brennbaren Sandwich Maker) und es dürfen nur geeignete Werkzeuge (Topf und Pfanne) verwendet werden.
- Systeme gelten auch bei scheinbar harmlosen Vorfällen (abgelaufene Schlüsselkarten nicht zerstört in den Müll werfen) als kompromittiert.

Ihr Zugang zum digitalen Puls der Zeit

Wie plant man Sicherheit?

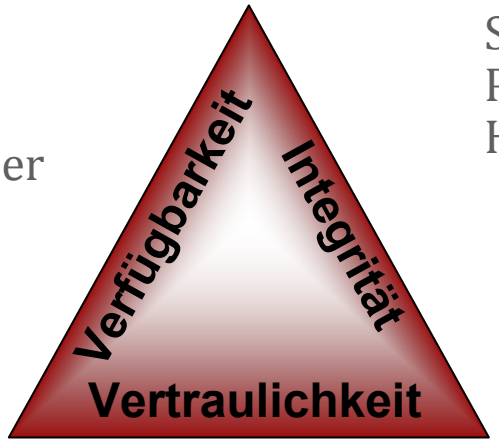
In der Informationstechnologie, der Gebäudeleittechnik und dem Prozessmanagement

1. Was wollen wir erreichen?
CIA Prinzip



Ihr Zugang zum digitalen Puls der Zeit

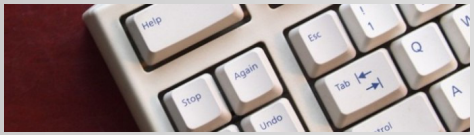
- SHKL soll 24/7 funktionieren
- Dachfenster sollen geschlossen werden bei Regen
- Brandmelder sollen immer meldebereit sein



- Abrechnung von Strom, Gas, Wasser soll korrekt sein
- Parameter der Gewerke (z.B. Steilheit und Parallelverschiebung der Heizkurve) soll immer stimmen

- Anwesenheiten sollen nicht bekannt werden
- Persönliche Gewohnheiten (z.B. Duschzeiten/ Toilettengänge) sollen privat bleiben

2. Was kann passieren?
Risikomatrix



Ihr Zugang zum digitalen Puls der Zeit

Schadensschwere

Eintrittswahrscheinlichkeit

	keine Folgen	Bagatell-folgen	mäßig schwere Folgen	irreparable Folgen	tödliche Folgen
fast gewiss					
zu erwarten					
durchaus möglich					
vorstellbar					
praktisch unmöglich					

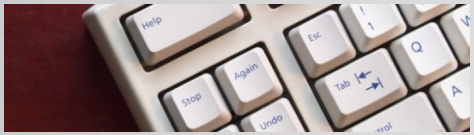
akzeptabel

akzeptabel mit Schadens-minderung

inakzeptabel

Beispiel: Netzwerkausfall – Wo einordnen?

3. Was können wir schützen?
Netzwerk als unterste Ebene



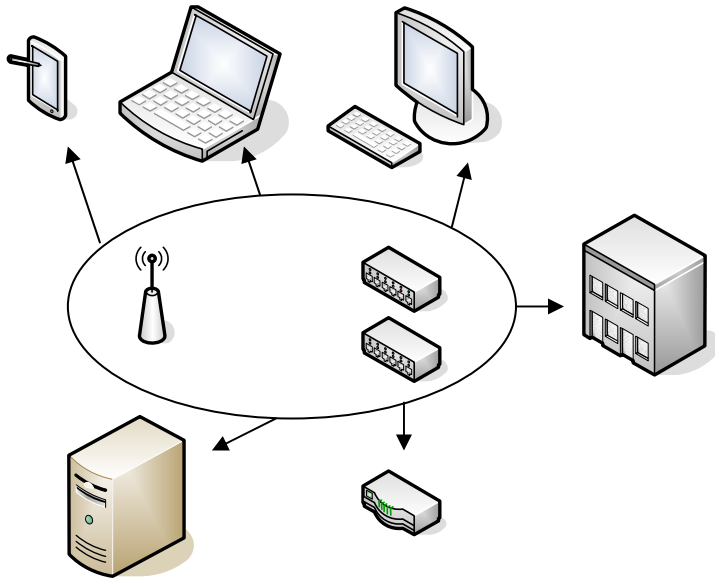
Ihr Zugang zum digitalen Puls der Zeit

Information Security Management (ISM)

Endpunkte
- Endpoint Detection & Response (EDR) – Avira, Panda Security
- Forensic State Analysis (FSA) - Infocyte
- …

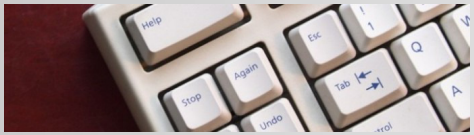
Netzwerk

Server/ Internet
- Unified Threat Managment (UTM) – Rhode&Schwarz, TuxGuard
- …



Gebäudeleit-technik BUS-Systeme

Das arme Netzwerk



Ihr Zugang zum digitalen Puls der Zeit

- Das Netzwerk verbindet inzwischen alle Bereiche (s.a. ModbusTCP, KNX over IP, u.v.m.)
- Das Netzwerk erhält am wenigstens Schutz: *„wenn der (Netzwerk)Stecker passt wird es schon funktionieren“*.

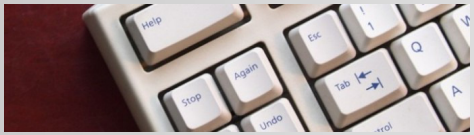
→ IT-Sicherheit in der Gebäudeautomation ist Netzwerksicherheit

Ihr Zugang zum digitalen Puls der Zeit

Sicherheit durch richtige Konzeption

Frameworks verwenden – Beispiel FCAPS

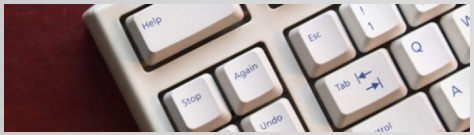
FCAPS



Ihr Zugang zum digitalen Puls der Zeit

- Fault Management
  - Wenn Fehler Auftreten wie findet und behebt man sie?
- Configuration Management
  - Was ist eigentlich eingestellt und wo haben wir es aufgeschrieben?
- AAA – Accounting, Authorization, Administration Management
  - Wer/ welches Gerät darf eigentlich was und können wir es in Rechnung stellen?
- Performance Management
  - Warten auf Antwort …
- Security Management
  - Was könnte passieren?

Fault Management



Ihr Zugang zum digitalen Puls der Zeit

Physikalisch

- Leitungspläne vorhalten, zumindest Patchfeld Zuordnung
- Kabel geschützt verlegen
- Netzwerk Hardware zugänglich aber geschützt verbauen
- Hardware regelmäßig reinigen (Wärmeabfuhr der Geräte selbst **und!** der Mehrfachsteckdosen)

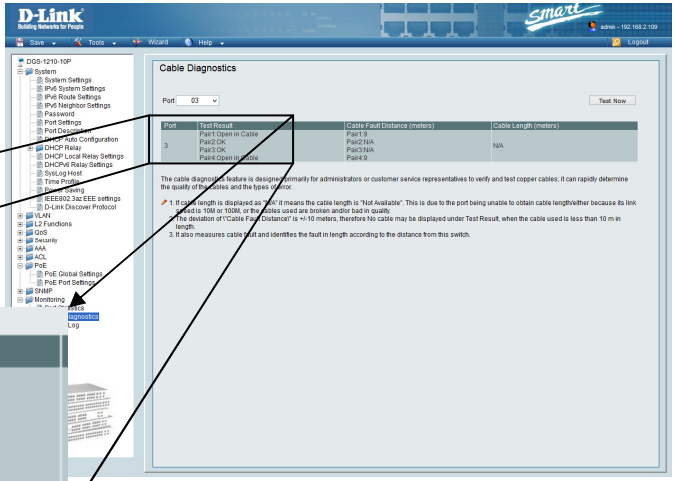
Administrativ

- Planen: Zuständigkeiten klären und vorhalten

  → Ansprechpartner Netzwerk und Gebäudeverkabelung
- Wartungspflichten, z.B. VDE 701/702

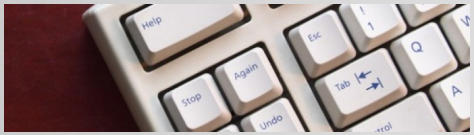
Technisch

- Smart Switches verwenden (Ausnahmen im Bereich des Access Netzwerks), z.B. für die Kabeldiagnose



Port	Test Result
3	Pair1:Open in Cable Pair2:OK Pair3:OK Pair4:Open in Cable

Configuration Management



Ihr Zugang zum digitalen Puls der Zeit

Physikalisch

- Informationen sicher und verfügbar verwahren

Masterzugang zum ISP nicht zu den Rechnungen heften sondern an (mehreren Beauftragten) bekanntem Ort wegschließen

Administrativ

- Zuständigkeiten: Wer darf Konfiguration ändern?

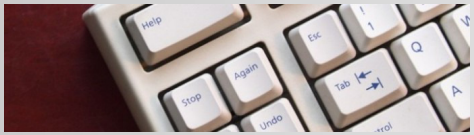
  → nur geschultes Personal, Änderungen dokumentieren und abzeichnen lassen

Viele Hersteller bieten die Schulungen für ihre Netzwerk Hardware kostenlos mit an, bzw. können über den Planer vermittelt werden → Fachpersonal selbst vorhalten

Technisch

- Management System verwenden oder Config-Dateien speichern
- Config-Dateien versionieren

Accounting, Authorization, Administration



Ihr Zugang zum digitalen Puls der Zeit

Physikalisch

- Switche, Wireless Access Points, u.a. Infrastruktur vor Zugriff schützen

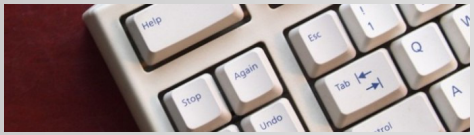
Administrativ

- Wer braucht worauf Zugriff?
  - getrennte Speicher
  - unzugängliche Komponenten
- Gastzugriffe einrichten oder keine Gäste zulassen

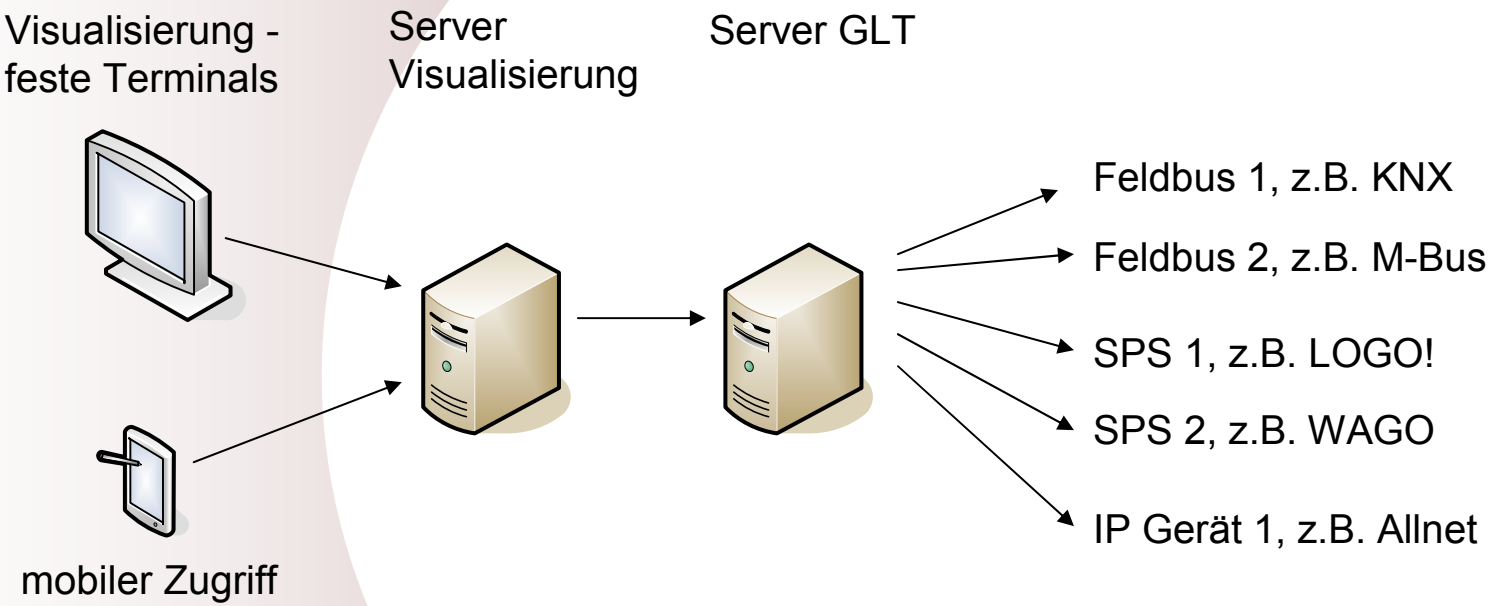
Technisch

- RADIUS, z.B. für **WPA2 Enterprise** im WLAN (bietet nahezu jeder moderne Wireless Access Point von Haus aus an)
- Subnetze und VLANs – virtuelle Trennung von Bereichen die physisch das Netz teilen müssen
  1. Management VLAN
  2. Gebäudeleittechnik (Prozesstechnik)
  3. Surveillance VLAN, VoIP
  4. *„Normale“* Clients

VLANs

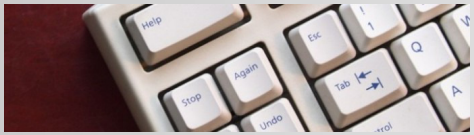


Ihr Zugang zum digitalen Puls der Zeit



1. nicht jedes Gerät muss mit jedem kommunizieren
2. nicht jedes Gerät muss mit dem Nutzer kommunizieren
3. alle Geräte sollen sich das Netzwerk (das Kabel) teilen

Performance Management



Ihr Zugang zum digitalen Puls der Zeit

Physikalisch

- Ausreichend „dicke“ und redundante Leitungen vorsehen
- Topologie planen
  - Link Aggregation (mehrere Netzwerkkabel verhalten sich wie eines)
  - Glasfaser verwenden (Splices vom Hersteller machen die Strecken günstig, ab ca. 2€/m)
  - Geräte auf zwei getrennten Wegen verbinden (z.B. Ring) – auch in kleinen Objekten

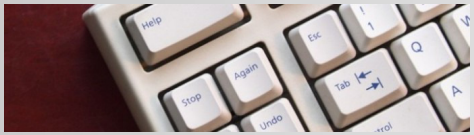
Administrativ

- Ressourcen Management betreiben – Budget vorsehen
- Kabelanlagen und Netzwerkinfrastruktur gehören zum Gebäude und benötigen Wartung und Ersatz wie alle anderen Gewerke auch

Technisch

- Smart Switches verwenden und konfigurieren (Spanning Tree, Ethernet Ring, Stacking)
- Flaschenhälse vermeiden und Hardware hierarchisch dimensionieren
  - Core Netzwerk
  - Aggregation Netzwerk
  - Access Netzwerk

Security Management



Ihr Zugang zum digitalen Puls der Zeit

Physikalisch

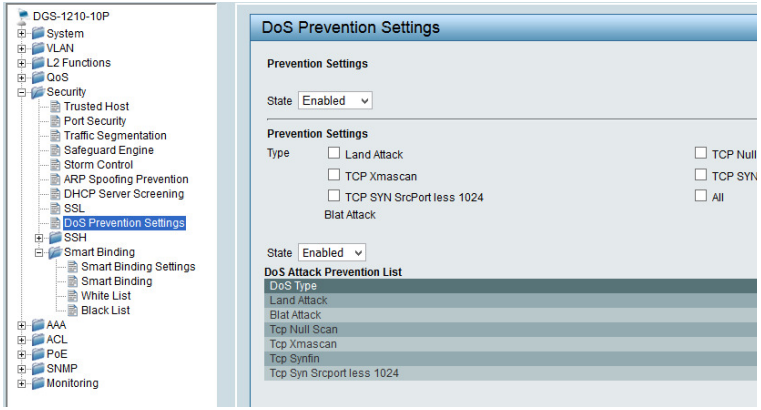
- Schutz vor Einbruchdiebstahl und Schadereignissen (Rohrbruch, Überspannung, Brand, Hitze, Kälte)

Administrativ

- Risikomanagement
- Awareness Trainings
- Regeln aufstellen (z.B. keine ausgetrockneten Dekopflanzen auf heiße Geräte legen)
- Regelmäßige Prüfung
  - Sichtprüfung von Kabeln und Geräten, Hotspots in Schaltschränken, Sichtung der Geräte Log-Dateien auf Auffälligkeiten

Technisch

- Sicherheit **einschalten**
- Whitelisting
  - erst alles sperren, dann freigeben wenn etwas gebraucht wird



Ihr Zugang zum digitalen Puls der Zeit

Danke für die Aufmerksamkeit

Fragen und Antworten