

DIE ILLUSION DER 100% IT-SICHERHEIT

„100%ige IT-Sicherheit
kann es nicht geben.“

Markus Richter, Bundes-CIO
Quelle: <https://glm.io/169596>

Der Mythos der 100%igen IT-Sicherheit

- Komplexität der IT-Landschaft (IT-Systeme, Software, Hardware etc.) entwickelt sich stetig weiter
→ Folge: neue Lücken und Schwachstellen tun sich regelmäßig auf
- demnach darf man sich nicht auf der aktuellen Momentaufnahme ausruhen
- der technische Status Quo sagt nur etwas über den aktuellen Moment aus und nichts über die Zukunft

Schritt für Schritt zu mehr Informationssicherheit

- **1. Schritt:** Was möchte man schützen?
- **2. Schritt:** Werden die Schutzziele der Informationssicherheit (Integrität, Authentizität, Vertraulichkeit, Verfügbarkeit) berücksichtigt?
- **3. Schritt:** Schutzmaßnahmen nach und nach planen, ausführen, prüfen und gegebenenfalls korrigieren

Wie kann man sich den 100% IT-Sicherheit annähern?

- Informationssicherheit nach dem **Matrjoschka-Prinzip:** Jede noch so kleine Schutzmaßnahme bildet eine Schutzschicht um das zu schützende Objekt und erhöht damit die IT-Sicherheit.
- Je mehr Schutzschichten man aufgestellt hat, desto länger dauert es, zu dem schützenswerten Kern vorzudringen
- **Wichtig!** Regelmäßig Maßnahmen auf Wirksamkeit überprüfen und gegebenenfalls korrigieren
→ **Merke:** Informationssicherheit ist ein stetiger Prozess!!!

Konkrete Maßnahmen für mehr Informationssicherheit?

- Datensicherheitskonzepte erstellen
- Authentifizierungsstrategien erarbeiten und entsprechende Verfahren einführen
- Systematische W-LAN-Gestaltung und Netzwerksegmentierung vornehmen
- Update- und Firmware-Management
- Backup- und Disaster-Recovery-Strategie entwickeln/umsetzen
- Notfallmanagement und Notfallkonzepte etablieren



SAFER SEC

DER IT-SICHERHEITS-PODCAST FÜR UNTERNEHMEN UND DIE ÖFFENTLICHE VERWALTUNG.



Unsere Security-Experten
erreicht ihr hier:

it-security@kupper-it.com

NICHT
VERGESSEN &
ABONNIEREN!



DIE MATRJOSCHKA DER IT-SICHERHEIT

- In unserem **Matrjoschka-Prinzip** gehen wir auf verschiedene Maßnahmen ein, die aus unserer Sicht die **Grundlagen** und **Must-haves** der IT-Sicherheit sind.
- Die einzelnen Maßnahmen werden wir in den kommenden Episoden unseres **Podcast Safer Sec** näher beleuchten.
- Darüber hinaus gibt es viele weitere Sicherheitsmechanismen die das Niveau eurer IT- und Informationssicherheit weiter anheben.

Das Geschäftsgeheimnis / die Geschäftskritischen Daten

Daten / Informationen / Knowhow / Patente / Software

Erste Puppe: Datensicherheitskonzepte entwickeln, um den Kern zu schützen.

Zweite Puppe: Authentifizierungsstrategien und entsprechende Zugriffsverfahren zur Sicherung der Daten.

Dritte Puppe: Systematische W-LAN-Gestaltung und Netzwerksegmentierung, um die Sicherheits Ebenen zu erhöhen.

Vierte Puppe: Update- und Firmware-Management, um Sicherheitslücken zu schließen und Daten zu schützen.

Fünfte Puppe: Backup- und Disaster-Recovery-Strategien, um im Notfall Daten wiederherstellen zu können.

Sechste Puppe: Notfallmanagement und Notfallkonzepten, um den Geschäftsbetrieb auch in Krisensituationen aufrechtzuerhalten.

