IT-Sicherheit im Umfeld ständig wachsender Angriffe

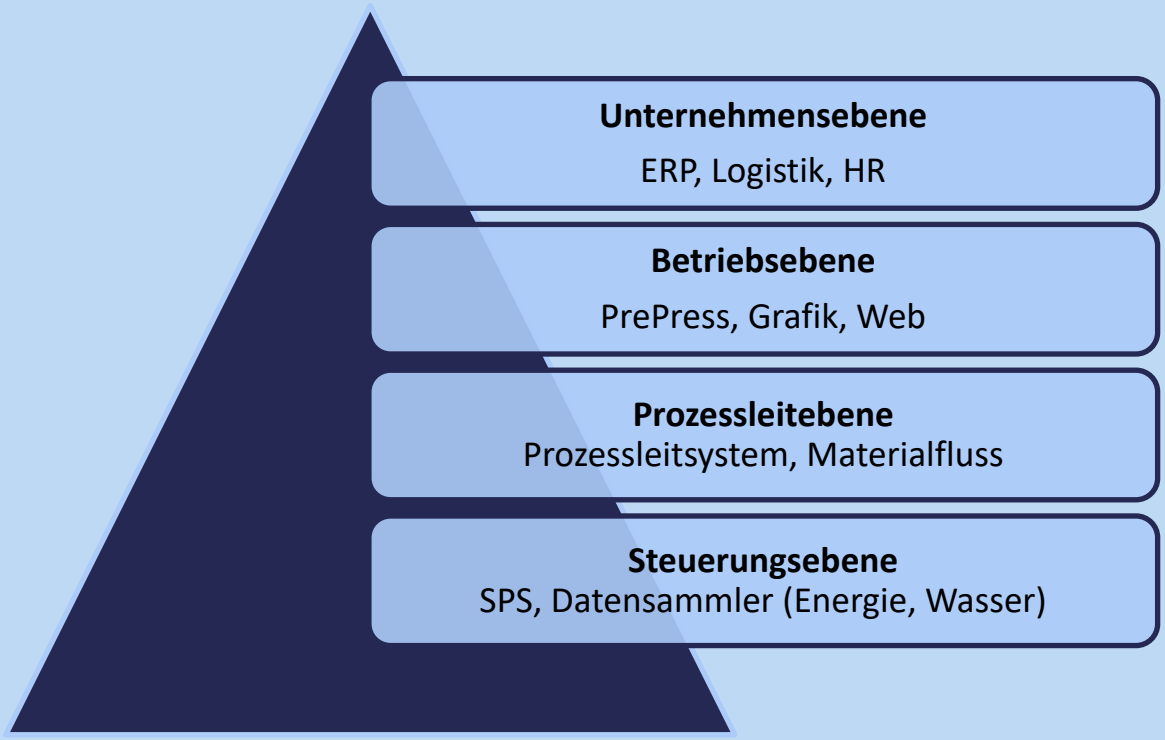
Prof. Ulf Glende – GLENDE.CONSULTING GmbH & Co. KG

Prof.
Ulf Glende

Geschäftsführer
GLENDE.CONSULTING
GmbH & Co. KG

- Studium Informatik, Dipl. Ing. (FH)
- u.a. Lehrgebiet „Technischer Datenschutz“ im Studiengang IT-Forensik
- Datenschutzbeauftragter/Data Protection Officer
- IT-Sicherheitsbeauftragter/Information Security Officer gemäß ISO/IEC 27001 und BSI IT-Grundschutz
- Auditor ISO/IEC 27001 und 27701
- Prüfverfahrens-Kompetenz §8a (3) BSIG – IT-Sicherheitsaudits bei KRITIS-Unternehmen
- externer Datenschutzbeauftragter von Unternehmen, Verbänden und Körperschaften des öffentlichen Rechts
- Beratung und Auditierung im Bereich der Informationssicherheit

Ebenen IT-gestützter Systeme



Grundlage der IT-Sicherheit

Asset Management

- Netzwerkplan
- IT Hardware
- IT Software
- Prozesssteuerungssysteme
- Infrastruktur
- Personen

Bewertung der Asset nach den Schutzzielen

- Vertraulichkeit, Integrität und Verfügbarkeit

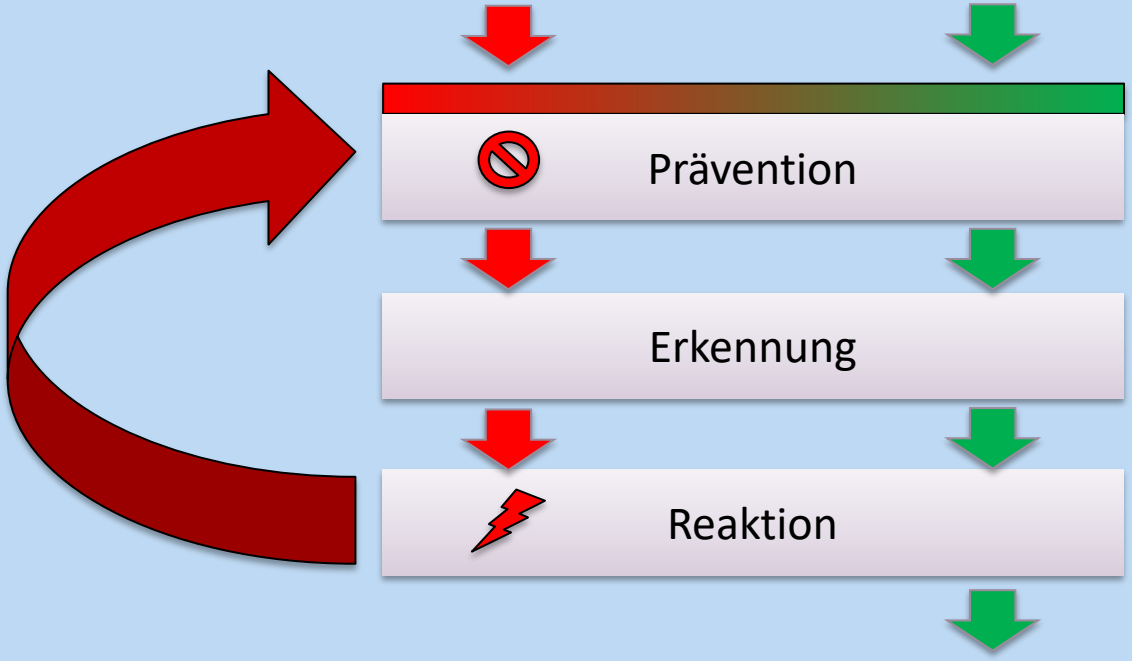
Risiken IT-Sicherheit

BEDROHUNG

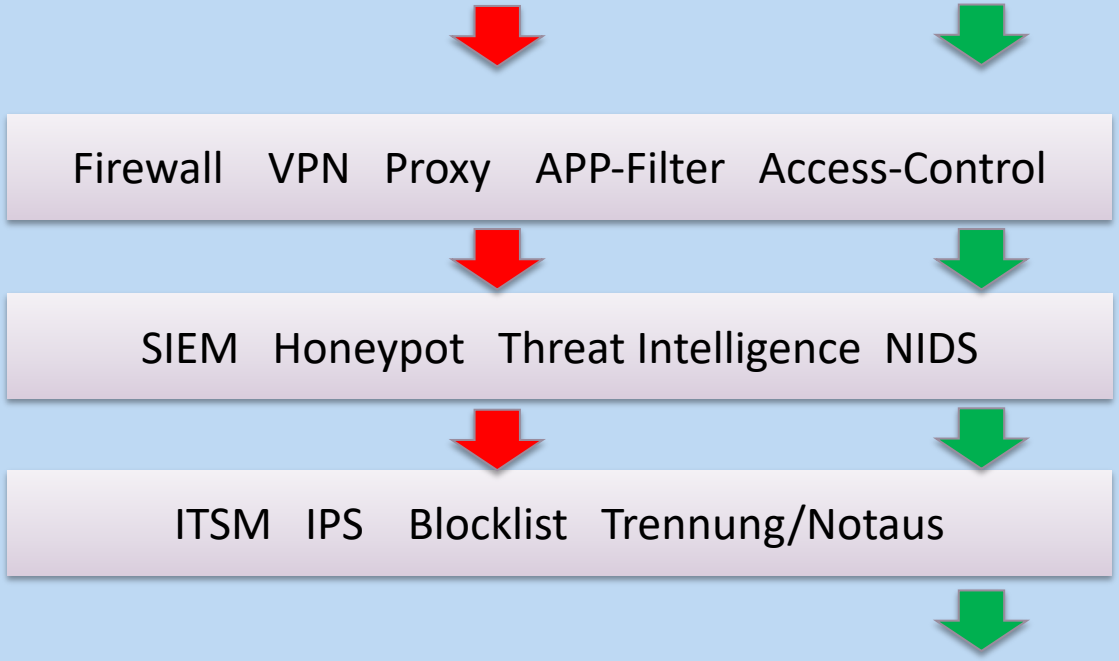
GEFÄHRDUNG

SCHWACHSTELLE

Vorfallbehandlung



Beispiele technische Umsetzung



BCM

Business Continuity Management (BCM)

- Business-Impact-Analyse (BIA)
- Schadenszenarien und -kategorien
- Bewertung (Beispiel BSI)
- Notfallvorsorgekonzept
- Notfallhandbuch
- Geschäftsfortführungsplan
- Wiederanlauf- / wiederherstellungsplan
- Übungskonzept
- Lieferketten und Outsourcing

Informationssicherheit

1. **Informieren**

   sicherheitsrelevante Informationen an alle betroffenen Akteure innerhalb des Unternehmens und seiner Lieferkette weiterzugeben

2. **Verstehen der Technologiearchitektur**

   die Richtung erkennen, in die sich die Sicherheitstechnologie entwickelt, und die Fähigkeit des Unternehmens, die geeignete Technologie entsprechend auszuwählen

Informationssicherheit

3. **Sicherheit einfach und transparent machen**

   Sicherheitsregeln und -technologien so darzustellen und implementieren, dass jeder, auch ein Laie, genau weiß, warum sie existieren und wie sie zu verwenden sind

4. **Gleichgewicht zwischen Sicherheit und Geschäft**

   eine optimale Anzahl von Schutzmaßnahmen anwenden, die stark genug sind, um Sicherheitsrisiken zu bewältigen, und gleichzeitig so unauffällig sind, dass sie den regulären Betrieb nicht beeinträchtigen

Informationssicherheit

5. Verwaltung einer sicheren Lieferkette

Daten auch dann sicher halten, wenn diese Daten nicht unter der direkten Kontrolle des Unternehmens stehen

6. Prioritätensetzung

sich auf die wichtigsten IT-Sicherheitsaktivitäten und -produkte zu konzentrieren, um strategische Prioritäten zu erreichen

Informationssicherheit

7. Aufbau von Fachwissen

Cybersecurity-Know-how innerhalb des Unternehmens aufbauen, Entscheidung welches Fachwissen im Unternehmen vorhanden sein muss

8. Belohnung der Mitarbeiter

KPIs und andere Messmethoden zu nutzen, um sicherheitsrelevante Akteure zu motivieren

Informationssicherheit

9. Datenauswertung

Auswertung der vorhandenen Daten (z.B. Protokolle) um fundierte Sicherheitsentscheidungen zu treffen

10. Einbettung in Geschäftsabläufe

Mitarbeiter dazu bringen, Sicherheitsregeln und -technologien als Teil ihrer regulären täglichen Arbeit zu nutzen

Vielen Dank für Ihre Aufmerksamkeit.

Prof. Ulf Glende – glende-consulting.de