

# Security Services

**Erhöhung der Widerstandsfähigkeit** der bestehenden **IT-Infrastruktur** gegen **Cyber-Angriffe** und Vermeidung von **Datenverlust**

## 1. Analyse

### **Security Assessment**

Überprüfung der bestehenden IT-Infrastruktur auf Schwachstellen für erfolgreiche Cyber-Angriffe und Datenverlust, Risiko-Analyse

### **Penetration Tests**

simulierte Cyber-Angriffe auf die bestehende IT-Infrastruktur, um Schwachstellen für erfolgreiche Cyber-Angriffe sowie Datenverlust oder Datenmanipulation herauszufinden

## 2. Behebung

### **Security Support** und **Engineering**

Auflisten, Beheben und Schliessen von analysierten Sicherheitslücken der bestehenden Infrastruktur sowie Backup-Prozesse

## 3. temporäre Überwachung

### **vorübergehendes Monitoring** und **Reporting**

Erkennen von Auffälligkeiten, Massnahmen, Behebung, Ergänzung

### **Risk Operation Center**

## 4. permanente Überwachung

### **dauerhaftes Überwachen** und **Berichten**

Überwachung auf Auffälligkeiten, Erkennen von Angriffen, Abwehr und Beheben von Schwachstellen

### **Security Operation Center**



# Anwendung

---

- **Überwachung**
  - auffälliges, nicht übliches Verhalten der IT (lange Lade- oder Speicherzeiten, etc.), Datenmanipulation, fehlerhafte Datenwiederherstellung
- **Erkennung**
  - meist werden Cyber-Angriffe von langer Hand vorbereitet, daher frühzeitiges Entdecken solcher Versuche notwendig
- **Überprüfen**
  - simulierte, kontrollierte Angriffe; Schwachstellenanalyse und -Behebung
- **Risikoeinschätzung**
  - relativ einfach:  
Wie lange dauert es, eine Produktion wieder anlaufen zu lassen nach einem Fabrikbrand?
  - schwieriger:  
Und wie lange nach einem Cyber-Angriff?  
Wie hoch ist das Risiko des Datenverlustes?
- verschiedene **Service-Module** im Rahmen der **flexcloud® by diso** zur **Überwachung** von **Auffälligkeiten**,
  - zur **Erkennung** von **Angriffsversuchen** oder
  - zum **Austesten** von **Schwachstellen** zur Stärkung der **Widerstandsfähigkeit** gegen Cyber-Angriffe und **manipulationssicherem** Speichern von **Daten**



# Nutzen

---

- Cyber **Resilience** statt Cyber **Security**
  - Steigerung der **Widerstandsfähigkeit** der **Unternehmens-IT** gegen **Cyber-Angriffe (Immunität)**
  - **Vorbeugen** ist besser als **Heilen!**
  - denn: **100%-ige Sicherheit** gibt es **nie!**
  - keine Frage, **OB**, sondern **WANN** kommt der Cyber-Angriff
  - je **höher** die Immunität, umso **schneller** wird man wieder arbeitsfähig nach dem Cyber-Angriff
  - **manipulationssichere** Datenspeicherung (Backup) sorgt für „saubere“ Daten im disaster recovery (**Wiederherstellung**)
  - **Massnahmen** dienen der Früherkennung und Verhinderung von Cyber-Angriffen, der Datenmanipulation oder des Datenverlustes, die das Unternehmen enorm schädigen (Datendiebstahl, Produktionsausfall, Reputation, etc.)
- Die **flexible** Lösung für mehr **Sicherheit**: *flexCloud*® by diso
  - **flexibler** Baukasten aus **Cloud-Applikation**, **Datenspeicherung** und **Security Services**
  - **sicherer** virtueller Arbeitsplatz in der **eigenen** (privaten) Cloud (on premise) für **systemkritische** Anwendungen und Daten
  - **unveränderbare** und **manipulationssichere** Datenspeicherung mittels **object storage** über **S3-Protokoll**



The image features a large, stylized blue padlock on the right side, overlaid with a glowing blue circuit board pattern. To the left of the padlock, the logo for 'diso' is displayed. The logo consists of a blue 'd' followed by a grey arrow pointing to the right, and the lowercase letters 'diso' in a light blue, sans-serif font below it.

# Vorteile

---

- **IT-Infrastruktur** ist heute **Produktionsfaktor** wie **Kapital, Material, Personal**
- **Daten** sind inzwischen **wertvollstes** Wirtschaftsgut
  - ➔ **Immunität** der Unternehmens-IT **steigert Unternehmenserfolg**
  - ➔ **Minimierung** der **Risiken** durch Cyber-Angriffe, Datenmanipulation oder Datenverlust
  - ➔ **Reduzierung** von **Unterbrüchen** (ERP-System, Produktion, Kommunikation, etc.) durch **schnelles** disaster recovery (**Wiederherstellung** des **arbeitsfähigen** Zustandes durch „sauberes“ Daten-Backup)
- Bei Cyber-Versicherung: **Reduzierung** der **Schadens-** und **Prämien-Einstufung**



d >  
diso

# Abhängigkeiten

- Bei temporärer oder permanenter Überwachung: **externes** Monitoring



# Preis

---

- Je nach **Service-Module, Dauer** und **Anzahl end points** bzw. **Nutzer**



# diso

weil Ihre Daten wertvoll sind

