# **Asset-Inventar**

## **Übersicht des Asset-Inventars**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Asset-ID** | **Asset-Typ** | **Beschreibung** | **Core Asset** | **Verant-wortlicher** | **Standort** | **Status** | **Priorität** |
| A001 | Server | Produktionsserver für ERP-System | ✅ | IT-Leiter | Rechenzentrum 1 | Aktiv | Hoch |
| A002 | Datenbank | Kundendatenbank | ✅ | Datenbank-administrator | Rechenzentrum 2 | Aktiv | Hoch |
| A003 | Workstation | Sekretariats-PC | ❌ | Sekretariat | Büroetage 1 | Aktiv | Mittel |
| A004 | Netzwerk-Switch | Backbone-Switch | ✅ | Netzwerk-administrator | Serverraum 1 | Aktiv | Hoch |
| A005 | Endpoint | Laptop Geschäftsführer | ✅ | Geschäfts-führung | Büro GF | Aktiv | Hoch |
| A006 | Firewall | Perimeter-Firewall | ✅ | IT-Sicherheits-beauftragter | Rechenzentrum 1 | Aktiv | Hoch |
| A007 | Backup-System | Cloud-Backup für kritische Daten | ✅ | Backup-Administrator | Cloud (AWS) | Aktiv | Hoch |
| A008 | Software | Buchhaltungssoftware | ❌ | Buchhaltung | Büroetage 2 | Aktiv | Mittel |
| A009 | Drucker | Netzwerkdrucker | ❌ | Facility Management | Büroetage 1 | Aktiv | Niedrig |
| A010 | Zugangs-kontrolle | RFID-Zugangssystem | ✅ | Sicherheits-abteilung | Firmengebäude | Aktiv | Hoch |

## **2. Beschreibung der Kategorien**

**Core Assets**

• **Definition:** Core Assets sind geschäftskritische Ressourcen, deren Ausfall erhebliche Auswirkungen auf den Betrieb, die Vertraulichkeit, Integrität oder Verfügbarkeit haben könnte.

• **Beispiele:**

• ERP-Systeme

• Datenbanken mit sensiblen Kundendaten

• Firewalls und Netzwerk-Switches

• Backup-Systeme und Sicherheitslösungen

**Nicht-Core Assets**

• Assets, die unterstützende Funktionen haben und deren Ausfall keine sofortige Unterbrechung der Kernprozesse verursacht.

• Beispiele:

• Arbeitsstationen (außer für Schlüsselrollen)

• Drucker

• Software für nicht-geschäftskritische Prozesse

## **3. Details zu Core Assets**

**Core Asset: A001 – Produktionsserver**

• **Beschreibung:** Hält die ERP-Daten und gewährleistet den reibungslosen Betrieb der Produktionskette.

• **Sicherheitsmaßnahmen:**

• Tägliche Backups.

• Zugriffskontrolle mit MFA.

• Regelmäßige Schwachstellenanalysen.

• **Risiko:** Hoch, da ein Ausfall den gesamten Produktionsprozess lahmlegen würde.

**Core Asset: A002 – Kundendatenbank**

• **Beschreibung:** Speichert personenbezogene Daten (PII) von Kunden.

• **Sicherheitsmaßnahmen:**

• Verschlüsselung der Daten (AES-256).

• Wöchentliche Schwachstellen-Scans.

• Zugriff nur für autorisierte Personen (Zero-Trust-Prinzip).

• **Risiko:** Sehr hoch, da ein Datenleck gravierende DSGVO-Bußgelder nach sich ziehen könnte.

**Core Asset: A006 – Perimeter-Firewall**

• **Beschreibung:** Schützt das interne Netzwerk vor externen Angriffen.

• **Sicherheitsmaßnahmen:**

• Tägliche Log-Analysen und Intrusion Detection.

• Segmentierung von Netzwerken.

• Regelmäßige Patching-Updates.

• **Risiko:** Hoch, da ein Ausfall das gesamte Netzwerk ungeschützt lassen würde.

**Core Asset: A007 – Backup-System**

• **Beschreibung:** Sichert kritische Daten und ermöglicht schnelle Wiederherstellung im Notfall.

• **Sicherheitsmaßnahmen:**

• Verschlüsselung aller Backups.

• Georedundanz in verschiedenen Rechenzentren.

• Regelmäßige Tests der Wiederherstellbarkeit (Disaster Recovery Übungen).

• **Risiko:** Hoch, da ein fehlendes Backup zu Datenverlust führen könnte.

## **4. Wartungs- und Überwachungsplan**

|  |  |  |
| --- | --- | --- |
| **Asset-Typ** | **Wartungsintervall** | **Überwachungsmaßnahmen** |
| Server | Monatlich | Patching, Schwachstellenscans, Log-Analysen |
| Datenbanken | Wöchentlich | Backup-Überprüfung, Zugriffskontrolle |
| Firewalls | Täglich | Intrusion Detection, Konfigurations-Checks |
| Netzwerk-Switches | Monatlich | Firmware-Updates, Performance-Monitoring |
| Backup-Systeme | Wöchentlich | Wiederherstellungstests, Verschlüsselungskontrolle |

## **5. Fazit**

Ein gut gepflegtes Asset-Inventar mit klar hervorgehobenen Core Assets ermöglicht eine gezielte Ressourcenplanung und Risikoabwehr. Durch regelmäßige Wartung und Überwachung dieser kritischen Systeme wird die Sicherheit und Kontinuität des Unternehmens gewährleistet.