PASSION4IT

OPTIMALE SICHERHEIT FÜR CLOUD- UND ONLINEANWENDUNGEN

Webinar zur Überprüfung von IT-Sicherheitsstandards

Florian Laumer | 27.09.2023 |

FLORIAN LAUMER

PASSION4IT

+49 151 11676 502

Florian.laumer@passion4it.de

https://www.linkedin.com/in/florianlaumer/

www.passion4it.de

- ✓ 25 Jahre Leidenschaft für IT, Digitalisierung, digitale Transformation und Innovation
- ✓ Hands On Mentalität
- ✓ ITQ-Auditor (Informationssicherheit)
- ✓ LEAD Digital Transformation Analyst (LEADing Practice)
- ✓ Certified SAFe 6 Agilist
- ✓ ICO ISMS Security Officer according to ISO/IEC 27001:2022

ICO-CERT International Certification Organization

VORTEILE VON CLOUDANWENDUNGEN

- ✓ **Kostenersparnis:** Cloud-Anwendungen reduzieren die Notwendigkeit teurer Hardware und Wartungskosten.
- ✓ **Skalierbarkeit:** Cloud-Anwendungen ermöglichen es Mittelstandsunternehmen, ihre IT-Ressourcen bei Bedarf schnell und einfach zu skalieren.
- ✓ **Flexibilität und Mobilität:** Mitarbeiter können von überall auf Cloud-Anwendungen zugreifen.
- ✓ **Automatisierung und Effizienz:** Cloud-Anwendungen bieten oft automatisierte Updates, Sicherheitspatches und Daten-Backups.
- ✓ **Zugang zu modernen Technologien:** Cloud-Anbieter investieren kontinuierlich in die Entwicklung neuer Technologien und Dienste.

GEFAHREN NACH DEM BSI

PASSION4IT

- G 0.9 Ausfall oder Störung von Kommunikationsnetzen
- G 0.11 Ausfall oder Störung von Dienstleistern
- G 0.14 Ausspähen von Informationen (Spionage)
- G 0.15 Abhören
- G 0.18 Fehlplanung oder fehlende Anpassung
- G 0.19 Offenlegung schützenswerter Informationen
- G 0.22 Manipulation von Informationen
- G 0.25 Ausfall von Geräten oder Systemen
- G 0.26 Fehlfunktion von Geräten oder Systemen
- G 0.29 Verstoß gegen Gesetze oder Regelungen
- G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
- G 0.32 Missbrauch von Berechtigungen
- G 0.35 Nötigung, Erpressung oder Korruption
- G 0.40 Verhinderung von Diensten (Denial of Service)
- G 0.45 Datenverlust

Bundesamt
für Sicherheit in der
Informationstechnik

BETROFFENE FACHVERFAHREN NACH BSI

- IT-Administration
- Unternehmensleitung
- Datenschutzmanagement
  - Datenschutzbeauftragte (DSB)
- Informationssicherheitsmanagement
  - Informationssicherheitsbeauftragte (ISB)

Bundesamt
für Sicherheit in der
Informationstechnik

SCHUTZKLASSEN

Welche Informationen sind betroffen?

- Schutzklasse 1: Öffentliche Informationen
  - Beispiel: Marketingmaterialien
- Schutzklasse 2: Interne Informationen
  - Beispiel: Standardbetriebsverfahren
- Schutzklasse 3: Geschäftskritische Informationen
  - Beispiel: Verträge
- Schutzklasse 4: Hochsensible Informationen
  - Beispiel: personenbezogene Daten
- Schutzklasse 5: Streng vertrauliche Informationen
  - Beispiel: Geschäftsgeheimnisse

SCHWERPUNKTE

PASSION4IT

1.

STANDORT UND BETRIEB DER CLOUD-ANWENDUNG

2.

ROBUSTE ZUGANGS- UND DATENABSICHERUNG

3.

DATENSCHUTZ, BACKUPS UND VERSCHLÜSSELUNG

1. STANDORT UND BETRIEB DER CLOUD-ANWENDUNG

PASSION4IT

Auswirkungen auf die Sicherheit

Geografischer Standort

- Datenschutzgesetze variieren je nach Land
  - Der Standort der Cloud-Anwendung kann Auswirkungen auf die Einhaltung dieser Gesetze (DSGVO) haben
- Nähe zu Rechenzentren kann Latenzzeiten beeinflussen

1. STANDORT UND BETRIEB DER CLOUD-ANWENDUNG

PASSION4IT

Auswirkungen auf die Sicherheit

Rechenzentrumssicherheit

- Die physische Sicherheit des Rechenzentrums, in dem die Daten gehostet werden, ist entscheidend
- Zugriffskontrollen, Überwachung und Schutz vor Naturkatastrophen sind relevante Faktoren
- Gebäudesicherheit (Brandsicherung, Wasser, Biometrie)
- Strom- und Klimaversorgung / Ausfallsicherheit (Transformatoren, Generatoren)

1. STANDORT UND BETRIEB DER CLOUD-ANWENDUNG

PASSION4IT

Auswirkungen auf die Sicherheit

Netzwerk- und Datenübertragungssicherheit

Qualität der Netzwerksicherheit zwischen dem Benutzer und der Cloud-Anwendung beeinflusst die Möglichkeit von Man-in-the-Middle-Angriffen oder Datenlecks

- Verschlüsselung während der Datenübertragung ist unerlässlich (Integrität)
  - Nutzung von HTTPS (SSL/TLS) für sichere Datenübertragung
- Datenverschlüsselung im Ruhezustand, z.B., um sensible Dateien zu schützen
  - Starke Verschlüsselungsalgorithmen wie AES-256 verwenden
- Mandantentrennung

1. STANDORT UND BETRIEB DER CLOUD-ANWENDUNG

PASSION4IT

Auswirkungen auf die Sicherheit

Compliance und Zertifizierungen I

- Die Auswahl eines Cloud-Providers mit relevanten Compliance-Zertifizierungen (z.B. ISO 27001)
- Der Provider sollte transparente Informationen über Sicherheitspraktiken und Audits bereitstellen
- Auftragsdatenverarbeitung (ADV) klären

1. STANDORT UND BETRIEB DER CLOUD-ANWENDUNG

PASSION4IT

Auswirkungen auf die Sicherheit

Compliance und Zertifizierungen II

- ISO 27001: Internationale Standard für Informationssicherheitsmanagement
- BSI C5: Cloud Computing Compliance Controls Catalog (C5)
- TÜV-Zertifikate: Zertifizierungen und Prüfungen für eine Vielzahl von Branchen
- Datenschutzkonforme Cloud-Dienste: (GDPR) müssen deutsche Cloud-Anbieter sicherstellen
- IT-Grundschutz: Das BSI bietet ein umfassendes Framework für Informationssicherheit
- E-Rechnungsgesetz: Wenn ein Cloud-Anbieter E-Rechnungsdienste anbietet

Erstkontrolle gem. §11 BDSG durch den Kunden sollte möglich sein!

2. ROBUSTE ZUGANGS- UND DATENABSICHERUNG

PASSION4IT

Sicherung des Anwendungszugriffs

Zwei-Faktor-Authentifizierung (2FA)

- Die Implementierung von 2FA (oder MFA) erhöht die Sicherheit, indem sie sicherstellt, dass Benutzer sich zusätzlich zur Passworteingabe auf anderem Wege authentifizieren müssen
- Verwendung von komplexen (unterschiedlichen) Passwörtern.

2. ROBUSTE ZUGANGS- UND DATENABSICHERUNG

PASSION4IT

Sicherung des Anwendungszugriffs

Rollenbasierte Zugriffssteuerung (RBAC)

- RBAC ermöglicht Benutzerberechtigungen, sodass nur autorisierte Personen auf bestimmte Funktionen und Daten zugreifen können
- Regelmäßige Überprüfung und Aktualisierung von Benutzerzugriffsberechtigungen

2. ROBUSTE ZUGANGS- UND DATENABSICHERUNG

PASSION4IT

Sicherung des Anwendungszugriffs

Audit-Logging und Überwachung

- Protokollierung von Benutzeraktivitäten: die kontinuierliche Überwachung von Systemen ermöglichen die frühzeitige Erkennung von verdächtigem Verhalten
- Identifizierung von Sicherheitsvorfällen: Rasche Identifizierung von Sicherheitsvorfällen, wie zum Beispiel unbefugtem Zugriff auf sensible Daten oder ungewöhnlichem Verhalten von Benutzern oder Systemen

3. DATENSCHUTZ, BACKUPS UND VERSCHLÜSSELUNG

PASSION4IT

Aspekte für umfassende Sicherheit

Datenschutzrichtlinien (DSGVO)

- Klare Datenschutzrichtlinien sollten definiert sein, um sicherzustellen, dass personenbezogene Daten angemessen geschützt und verarbeitet werden
- Datenlokalisierung: Geographische Region
- Auftragsdatenverarbeitung (ADV) klären

3. DATENSCHUTZ, BACKUPS UND VERSCHLÜSSELUNG

PASSION4IT

Aspekte für umfassende Sicherheit

Regelmäßige Backups

- Regelmäßige automatisierte Backups sind wichtig, um Datenverlust durch versehentliches Löschen, Hardwarefehler oder Ransomware-Angriffe zu verhindern
- Offline Backups
- Wiederherstellungstests durchführen

3. DATENSCHUTZ, BACKUPS UND VERSCHLÜSSELUNG

PASSION4IT

Aspekte für umfassende Sicherheit

Sicherheitsupdates und Patch-Management

- Regelmäßige Updates und Patch-Management sind entscheidend, um Sicherheitslücken zu schließen
- Testen von Patches in einer isolierten Testumgebung, bevor sie in der Produktion eingespielt werden
- Integration von Sicherheitstests in den Entwicklungsprozess, einschließlich automatisierter Sicherheitsscans
  - Open Web Application Security Project (OWASP20)
- Beauftragung von externen Sicherheitsexperten für regelmäßige Sicherheitsbewertungen und Penetrationstests


PASSION4IT
VIELEN DANK FÜR IHRE
AUFMERKSAMKEIT!