IT-Sicherheitscheckliste

Checkliste zur Überprüfung der IT-Sicherheit Ihres IT-Dienstleisters

livtec cloud provider

1 Wir sind für Sie da (KOSTENLOS)!

Wenn Sie diese Checkliste verwenden, um Ihren aktuellen IT-Partner zu überprüfen, zeigen Sie bereits ein verantwortungsbewusstes Engagement für die IT-Sicherheit Ihrer IT-Infrastruktur. Ihre Daten und Systeme sind von entscheidender Bedeutung, und es ist wichtig sicherzustellen, dass Sie die bestmöglichen Sicherheitsvorkehrungen getroffen haben.

Wir wissen, dass das Thema IT-Sicherheit komplex sein kann und es manchmal schwer sein kann, die richtigen Fragen zu stellen. Deshalb möchten wir betonen, dass wir hier sind, um Ihnen zu helfen. Unabhängig davon, ob Sie bereits unser Kunde sind oder nicht, bieten wir Ihnen unsere Unterstützung und Beratung völlig kostenlos an.

Unsere Expertise ist die IT-Sicherheit, und wir möchten einen positiven Beitrag dazu leisten. Wenn Sie Fragen zur IT-Sicherheit Ihres aktuellen IT-Infrastruktur haben, Unsicherheiten ausräumen müssen oder Unterstützung bei der Bewertung der Sicherheitspraktiken Ihres aktuellen IT-Partners benötigen, zögern Sie nicht, uns zu kontaktieren. Wir sind hier, um Ihnen mit unserem Fachwissen und unserer Erfahrung zu unterstützen.

Kontaktdaten:
Livtec AG
Poststrasse 1
6343 Rotkreuz

support@livtec.cloud
+41 41 244 70 70

Termin vereinbaren unter:
crm.livtec.cloud/meetings/livtec/beratung

livtec

2 Checkliste für IT-Sicherheitsfragen

1. Netzwerksicherheit:

- Verfügt Ihre Cloud-Lösung über ein dediziertes Netzwerk, das unabhängig von anderen Kunden betrieben wird?
- Wie wird die Netzwerktrennung sichergestellt, um potenzielle Angriffsvektoren zu minimieren?

2. Firewall-Schutz:

- Besitzt Ihre Infrastruktur eine eigene individualisierte Firewall pro Kunde, um externe und interne Bedrohungen proaktiv abzuwehren?
- Wie wird sichergestellt, dass unbefugter Zugriff auf die Firewall und somit auf die Daten verhindert wird?

3. Server-Infrastruktur:

- Werden eigene dedizierte Server pro Kunde eingesetzt, um höchste Datenschutz- und IT-Sicherheitsstandards zu gewährleisten?
- Werden für verschiedene Serverrollen eigene dedizierte Server eingesetzt, um die IT-Sicherheit weiter zu erhöhen?
- Werden die Daten zusätzlich verschlüsselt, so dass die Datensicherheit und Datenintegrität gewährleistet ist?

4. Active Directory (Benutzer- und Serververwaltung):

- Verfügt Ihre Cloud-Lösung über ein eigenes, dediziertes Active Directory pro Kunde, um eine isolierte und sichere Benutzerverwaltung gewährleisten zu können?
- Wie werden Angriffe auf das Active Directory und somit auf die Konten der Benutzer verhindert?

5. Sicherheits-Benchmarks:

- Welche spezifischen Sicherheitsstandards oder Benchmarks werden von Ihrer Lösung in Bezug auf Betriebssystemhärtung erfüllt?
- Wie wird sichergestellt, dass diese Standards kontinuierlich eingehalten werden?

6. Security Operation Center (SOC):

- Besitzt Ihre Cloud ein eigenes Security Operation Center mit Anomalie Erkennung, um potenzielle Bedrohungen in Echtzeit zu identifizieren?
- Wie reagiert Ihr Security Operation Center auf erkannte Anomalien, um proaktiv auf mögliche Sicherheitsverletzungen zu reagieren?

7. Multi-Faktor-Authentifizierung (MFA) und Single Sign-On (SSO):

- Bietet Ihre Cloud-Lösung Multi-Faktor-Authentifizierung (weiterer Schutzfaktor zusätzlich zum Passwort) und Single Sign-On (ein abgesichertes Login für alle Dienste) als zusätzliche Sicherheitsebene für Benutzerkonten für jegliche Zugriffe?
- Werden Zugriffe und Zugriffsversuche protokolliert und Anomalien erkannt und automatisch gesperrt?
- Wie werden Identitätsdiebstahl und nicht autorisierte Zugriffe durch diese Funktionen verhindert?

livtec

8. Patch-Management:

- Wie häufig und zuverlässig werden Sicherheitspatches und Updates für Betriebssysteme und Anwendungen eingespielt?
- Wie schnell wird auf akute Sicherheitslücken reagiert, um potenzielle Exploits zu minimieren?

9. Überwachung (Monitoring):

- Welche Art von Überwachungssystemen sind implementiert, um verdächtige Aktivitäten oder Datenverkehr zu identifizieren?
- Wie werden Kunden über Bedrohungen oder Vorfälle informiert, und wie erfolgt die Zusammenarbeit bei der Bewältigung dieser Vorfälle?

10. Physische Sicherheit:

- Wie wird die physische Sicherheit Ihrer Rechenzentren und Serverräume sichergestellt, um unbefugten Zugriff zu verhindern?
- Gibt es Überwachungskameras, Zugangskontrollsysteme und Alarme, um die physische Sicherheit zu gewährleisten?
- Welche (ISO-) Zertifizierungen oder internationale Standards werden eingehalten und sind zertifiziert?

11. Datenschutz und Compliance:

- Welche Datenschutzrichtlinien und Compliance-Standards sind in Ihrer Cloud-Lösung implementiert, insbesondere in Bezug auf DSG, FINMA, SAV, HIPAA oder andere relevante Vorschriften?
- In welchem Land werden die Server betrieben und wo werden Daten und Backups aufbewahrt? (Jede Applikation einzeln, abfragen)
- Werden Dienste von amerikanischen Firmen verwendet, welche vom Cloud Act betroffen sein können?

12. Backup und Wiederherstellung:

- Wie werden regelmässige Backups Ihrer Daten durchgeführt, um Datenverlust im Falle eines Ausfalls oder Angriffs zu verhindern?
- Wie oft werden Sicherungen durchgeführt und wie lange werden diese aufbewahrt?
- Werden Sicherungen an mehreren Standorten aufbewahrt?
- Ist mindestens ein Backup an einem anderen Standort aufbewahrt?
- Wie sind die Sicherungen vor Cyber Angriffen geschützt? Können die Sicherungen gelöscht oder manipuliert werden?
- Gibt es ein Testverfahren, um die Machbarkeit der Wiederherstellungsprozesse zu überprüfen, um sicherzustellen, dass die Sicherungen funktionsfähig sind?

13. Incident Response:

- Wie ist der Prozess zur Erkennung und Bewältigung von Sicherheitsvorfällen strukturiert?
- Welche Schritte werden unternommen, um die Auswirkungen von Sicherheitsvorfällen zu minimieren und Kunden zu informieren?

14. DDoS-Schutz (Schutz vor Distributed Denial of Service-Angriffen):

- Welche Massnahmen haben Sie ergriffen, um sich vor Distributed Denial of Service-Angriffen zu schützen und die Verfügbarkeit Ihrer Dienste aufrechtzuerhalten?

15. Verschlüsselung:

- Wie werden Daten in Ihrer Cloud-Lösung verschlüsselt, sowohl im gespeicherten Zustand als auch während Übertragungen?
- Welche Verschlüsselungsalgorithmen und Schlüsselverwaltungsmethoden werden verwendet?

16. Security Awareness und Schulungen:

- Gibt es ein Angebot von Schulungen und Schulungsmaterialien für Kunden, um das IT-Sicherheitsbewusstsein und das Verständnis zu erhöhen?
- Wie werden Kunden über bewährte IT-Sicherheitspraktiken und potenzielle Bedrohungen auf dem Laufenden gehalten?

17. Notfallplanung:

- Haben Sie oder Ihr IT-Dienstleister einen Notfallplan für den Umgang mit Cyber-Angriffen, Naturkatastrophen, Systemausfällen oder anderen unvorhergesehenen Ereignissen?
- Verfügt Ihr IT-Dienstleister über einen alternativen Kommunikationskanal oder einen Dienst/Webseite, um über Ausfälle oder Störungen zu informieren?
- Wie werden Kunden bei der Notfallwiederherstellung unterstützt?

18. Zugriffsrechte und Berechtigungen:

- Wie werden Zugriffsrechte und Berechtigungen für Benutzer und Administratoren verwaltet, um den Prinzipien des geringsten Privilegs zu entsprechen?
- Wie wird sichergestellt, dass ehemalige Mitarbeiter oder Dienstleister keine Zugriffsberechtigungen behalten?
- Werden Zugriffe auf sämtliche Dateien und Systeme auditiert und Anomalien ausgewertet?