

**CHECKLISTE für die Auswahl eines Internet Service Providers für Unternehmen**

Diese Checkliste soll Ihnen als Gedankenstütze dienen, um über Ihre eigenen Anforderungen und die Qualifikation Ihres derzeitigen oder künftigen Internet Service Providers zu reflektieren.



**Natürlich dürfen Sie dieses Dokument auch an einen ISP zur Beantwortung weiterleiten.**

**Internet Service Provider**

- |   |   |
|---|---|
| <p>1. Welche Zertifizierungen besitzt der ISP (z.B. ISO-27001, ...)?<br/>Tipp: Ein ISP muss branchenübliche Standards erfüllen, welche regelmässig überprüft werden</p>   | <p>-----</p> <p>-----</p>   |
| <p>2. Wurde das ISP-Netz auditiert? Wenn Ja, von wem?<br/>Tipp: Kann der ISP nachweisen, dass auch sein Netz auditiert wurde?<br/>Risiko: Nur der ISP als Firma wurde überprüft, nicht aber das Netz durch eine unabhängige Stelle (Carrier-Grade)</p>  | <p><input type="checkbox"/> Ja <input type="checkbox"/> Nein</p> <p>-----</p> |
| <p>3. Betreibt der ISP ein eigenes Network Operation Center 24x7 inkl. Hotline?<br/>Tipp: Benötigen Sie den Service rund um die Uhr oder nur während der Arbeitszeit?<br/>Kann der ISP im Störfall auch nachts reagieren?<br/>Risiko: Bei Störungen wird nicht in angemessener Zeit reagiert</p>  | <p><input type="checkbox"/> Ja <input type="checkbox"/> Nein</p>              |
| <p>4. Bietet der ISP für die Internet-Anschlüsse einen DDoS-Schutz an?<br/>Info: Bei einer Distributed-Denial-of-Service-Attacke kommt es zu einer Überlastung der Internetanbindung eines Unternehmens. Mehrere GBit an Datenverkehr werden meist durch viele infizierte Geräte generiert und Richtung Opfer adressiert.<br/>Risiko: Angreifer könnten einen Betrieb durch einen DDoS-Angriff vom Netz nehmen und die Geschäftsprozesse womöglich stark beeinträchtigen.<br/>Mögliche Folgen: Umsatzverlust, Reputationsschäden, ...</p> | <p><input type="checkbox"/> Ja <input type="checkbox"/> Nein</p>              |
| <p>5. Werden Business-Anschlüsse gegenüber privaten Haushalten priorisiert?<br/>Risiko: Beeinträchtigung des Netzes durch massives Download-Verhalten von privaten Haushalten - auch ausgelöst durch DDoS-Angriffe auf Gamer</p>  | <p><input type="checkbox"/> Ja <input type="checkbox"/> Nein</p>              |
| <p>6. Priorisiert der ISP Telefonie-Gesprächsdaten gegenüber anderen Internet-Daten, sodass für Gespräche immer ausreichend Bandbreite zur Verfügung steht?<br/>Risiko: Keine Notrufe möglich, bei ausgelasteter Bandbreite</p>   | <p><input type="checkbox"/> Ja <input type="checkbox"/> Nein</p>              |
| <p>7. Können Bandbreiten garantiert werden?<br/>Tipp: Welche Anwendungen betreiben Sie im Unternehmen?<br/>Benötigen Sie dazu eine konstante Bandbreite, die nicht schwankt?<br/>Risiko: tägliche Arbeit wird beeinträchtigt, wenn die Bandbreite schwankt (Video-Konferenzen, ...)</p>   | <p><input type="checkbox"/> Ja <input type="checkbox"/> Nein</p>              |

**CHECKLISTE für die Auswahl eines Internet Service Providers für Unternehmen**

8. Bietet der ISP gewisse Service Level Agreements an?  Ja  Nein  
Tipp: Wie schnell muss Ihre Internetanbindung bei einem Ausfall wieder verfügbar sein? Führen Sie eine Kosten/Nutzen Analyse durch.  
Risiko: Bei einem Ausfall wird nicht schnell genug reagiert und es kommt zu längeren Unterbrechungen
9. Bietet der ISP die Möglichkeit den Internetanschluss mit einer mobilen Backup-Verbindung auszustatten (Kleinunternehmen)?  Ja  Nein  
Risiko: Es kommt zu einem Ausfall im Core-Netz bei Ihrem ISP und es wird nicht automatisch auf mobiles Internet umgeschaltet – Unterbrechung
10. Redundanz-Optionen  
Tipp: Ist für Ihr Unternehmen eine unterbrechungsfreie Internetanbindung essentiell (z.B. bei Cloud-First-Strategien von grösseren Unternehmen)? Wenn ja, sollten Sie einen ISP wählen, der Ihnen die Hardwarekomponenten redundant installiert und im Fehlerfall eine automatische Umschaltung garantiert, sodass ein Anschluss immer verfügbar ist. Führen Sie periodisch Redundanztests durch.
- a. Ermöglicht der ISP einen redundanten Firewall-Betrieb?  Ja  Nein  
Risiko: Firewall ist defekt oder muss gewartet werden - Unterbrechung
- b. Netzabschluss-Geräte-Redundanz durch ISP möglich?  Ja  Nein  
Risiko: Ihr ISP-Router/Switch erleidet einen Defekt - Unterbrechung
- c. Bietet der ISP eine Option auf getrennte Trassenführung an?  Ja  Nein  
Risiko: Glasfaserleitungen zum Gebäude werden beschädigt - Unterbrechung
11. Betreibt der ISP mehrere eigene Rechenzentren, um Ihnen georedundante Backups durch eine Kombination von Standortvernetzung und Housing zu ermöglichen?  Ja  Nein  
Info: Unvorhersehbare Ereignisse, wie Brand, Einbruch und Diebstahl können zu einem Datenverlust bei einem Unternehmen führen. Mit einer redundanten Standortstrategie wird das Risiko eines kompletten Verlusts der Daten minimiert.
12. Sind die Rechenzentren des ISPs an unterschiedliche Stromnetze angeschlossen?  Ja  Nein  
Risiko: Stromausfälle können zu Netzausfällen führen – Unterbrechung
13. Wird die Stromversorgung des ISPs zusätzlich durch ein Dieselaggregat oder Batterie-Backup abgesichert?  Ja  Nein  
Risiko: Stromausfälle können zu Netzausfällen führen – Unterbrechung
14. Hat das eingesetzte Equipment des ISPs redundante Netzteile?  Ja  Nein  
Risiko: Netzausfall durch ein defektes Netzteil (Stromversorgung)

**CHECKLISTE für die Auswahl eines Internet Service Providers für Unternehmen**

15. Steht neben den Vertriebsmitarbeitern des ISPs auch ein direkter technischer Ansprechpartner für die Umsetzung des Projektes und spätere technische Anfragen zur Verfügung?  
Risiko: Koordinationsprobleme bei der Umsetzung des Projekts, «Stille Post»  Ja  Nein
16. Ist die Sicherheit der Daten gegeben?  
Risiko: Ihre rechtlichen Vorgaben werden nicht komplett eingehalten  
Info: Wo werden meine Daten gespeichert (lokal beim ISP oder in der Cloud)?  
Sind die Leitungen des ISPs verschlüsselt?  Ja  Nein
17. Hat der ISP die Möglichkeit eine lückenlose Überwachung des Betriebszustandes des Netzes anzubieten und können Geschäftskunden ihr Netz selbst überwachen?  
Info: Verbindungsprobleme können verschiedene Ursachen haben und eine aktive Überwachung hilft bei der schnellen Identifikation  Ja  Nein
18. Betreibt der ISP sein Netz selbst (also nicht über Dritte)?  
Wann wurde die Hardware vom Kern-Netz erneuert?  
Info: In der Regel werden ISP-Netze alle 5 Jahre erneuert.  
Risiko: Abhängigkeit eines ISPs von Dritten kann zu Verzögerungen bei der Identifikation und Behebung von Problemen führen  Ja  Nein
- 
19. Hat der ISP Erfahrungen mit komplexen Business-Anbindungen/Anwendungen und betreibt er derzeit ähnliche Lösungen bei anderen Kunden?  
Beispiel mit Referenzen?  
Risiko: ISP bietet nicht notwendige Konfigurationen für Ihre IT-Strategie (z.B. Cloud-First, high-availability, ...)  Ja  Nein
- 
20. Bietet der ISP eine gewisse Flexibilität bei seinem Internet-Produkt?  
Kann der ISP die Bandbreite ohne grossen Aufwand erhöhen / verringern?  
Risiko: Standard-Produkte sind in Stein gemeisselt und es gibt keinen Spielraum für Sonderlösungen (Kompatibilität, ...)  Ja  Nein
21. Verfügt der ISP über genug Ressourcen, um Ihre Wachstumsstrategie abzudecken?  
Risiko: Sie sind vertraglich noch lange gebunden, jedoch kann der ISP nicht auf Ihre neuen Anforderungen eingehen  Ja  Nein
22. Wie viele Anwender teilen sich welche Bandbreite?  
Info: max. 16 Teilnehmer teilen sich 2.5Gbit bei nicht garantierter Bandbreite  
Risiko: Schwankungen können die Betriebsprozesse beeinflussen oder die Kommunikation stören  Ja  Nein
- 
23. Wie viele Mitarbeiter beschäftigt der Internet-Service-Provider (ISP)?  
Tipp: Die Auswahl des richtigen ISP ist für ein Unternehmen eine strategische Entscheidung. Man benötigt einen zuverlässigen Partner, der dabei unterstützt, die Unternehmensziele zu erreichen. Daher ist es sehr wichtig, dass der ISP ausreichend kompetentes Personal beschäftigt – auch im Bereich Security.  
Risiko: Personalfluktuaton bei ISP, Know-How-Verlust, Qualitätseinbrüche  Ja  Nein
-