**Dienstleister-Bewertung IT-Sicherheit**

Die folgende Bewertungsmethodik soll Ihnen helfen, Ihren aktuellen Dienstleister im Hinblick auf seine IT-Sicherheits-Kompetenz zu bewerten bzw. einen neuen, geeigneten Dienstleister auszuwählen.

Wählen Sie pro Kriterium aus, ob der Dienstleister zu der entsprechenden Zusage bereit ist / in der Lage ist, diese Zusage zu liefern.

Die Gesamtbewertung besteht aus der Summe der JA-Antworten, und ist eine Zahl zwischen 0 und 20. Je besser diese Zahl, desto besser ist der Dienstleister geeignet, die IT-Sicherheitsanforderungen zu erfüllen. Idealer Weise sind alle Kriterien erfüllt.

| Nr | Kriterium | Ja / Nein |
| --- | --- | --- |
| 1 | Der Dienstleister sichert eine Mindestverfügbarkeit von 99% pro Monat für alle für den Kunden relevanten Systeme zu |  |
| 2 | Der Dienstleister ist in der Lage, Hacker-Angriffe zu erkennen |  |
| 3 | Sicherheitswarnungen von allen verwendeten Betriebssystemen, IT-Systemen und Software-Anwendungen werden beobachtet |  |
| 4 | Sicherheitsvorfälle und -warnungen mit hoher Kritikalität werden unverzüglich an den Kunden kommuniziert und es wird unverzüglich ein sicherer Zustand wieder hergestellt |  |
| 5 | Sicherheitsvorfälle und -warnungen mit normaler Kritikalität werden am gleichen Tag an den Kunden kommuniziert und es wird innerhalb einer Woche ein sicherer Zustand wieder hergestellt |  |
| 6 | Personenbezogene Daten von deutschen Mitarbeitern des Kunden werden nach den gesetzlichen Vorgaben verarbeitet. |  |
| 7 | Auf Ausscheiden eines Mitarbeiters des Dienstleisters wird das Benutzerkonto deaktiviert, Passwörter geändert und alle Unterlagen, die den Kunden betreffen, eingezogen. |  |
| 8 | Die personelle Ausstattung mit angemessener Kompetenz ist auch bei Sicherheitsvorfällen ausreichend gegeben. |  |
| 9 | Der Dienstleister hat eine Risikoanalyse durchgeführt und hat geeignete Notfallpläne und risikosenkende Maßnahmen im Einsatz |  |
| 10 | Es gibt einen dokumentierten Prozess, um Änderungen an Systemen zu erfassen und die Sicherheitsauswirkungen bewerten zu können, bevor die Änderungen durchgeführt werden. |  |
| 11 | Alle für den Kunden relevante Systeme sind in einer „Configuration Management DataBase“ (CMDB) aktuell dokumentiert. |  |
| 12 | Der Dienstleister hat ein Computer Emergency Response Team im Einsatz. |  |
| 13 | Eine Fernwartung geschieht ausschließlich über verschlüsselte Leitungen mit starker Authentifizierung. |  |
| 14 | Die für den Kunden relevanten Systeme werden nach den Best Practices der ISO 27002 gesichert. |  |
| 15 | Der Dienstleister führt regelmäßig Sicherheits-Sensibilisierungen bei seinen Mitarbeitern durch. |  |
| 16 | Der Dienstleister führt für alle relevanten Systeme Backups. Diese werden gesichert gelagert (auch eine Kopie außer Haus) und regelmäßig testweise rückgesichert. |  |
| 17 | Der Dienstleister erklärt sich bereit, Security Audits durch den Kunden mit einer Vorlaufzeit von 7 Tagen zu akzeptieren. |  |
| 18 | Der Dienstleister berichtet monatlich über sicherheitsrelevante Ereignisse und Informationen. |  |
| 19 | Die Mitarbeiter des Dienstleisters sind nachweislich angemessen zu Sicherheitsthemen qualifiziert. |  |
| 20 | Wenn Subunternehmer eingesetzt werden, so haftet der Dienstleister unbeschränkt gegenüber dem Kunden. |  |
|  | **Anzahl JA-Antworten** |  |