Kriterium	Dienstleisterhinweise	ja	nein	Bemerkung
Organisation				
Der Dienstleister bietet an, eine **Schutzbedarfsanalyse** für die Systeme des Kunden durchzuführen, sowie daraus gemeinsam mit dem Kunden ein **Sicherheitskonzept** abzuleiten.	Es geht dabei darum, die Kronjuwelen des Anwenders zu identifizieren, und mit ihm gemeinsam passende Maßnahmen auszusuchen.	☐	☐	
Die Auswahl der technischen Sicherungsverfahren und die Organisation der IT-Sicherheit werden in Abstimmung mit dem Kunden auf der Basis der Best Practices der **ISO 27002** (oder vergleichbar) abgestimmt.	Es geht dabei darum, die Kronjuwelen des Anwenders zu identifizieren, und mit ihm gemeinsam passende Maßnahmen auszusuchen.	☐	☐	
Der Dienstleister **berichtet** monatlich über den sicherheitsrelevanten Status der Kundensysteme und gibt **Handlungsempfehlungen**.	Es geht dabei darum, die Kronjuwelen des Anwenders zu identifizieren, und mit ihm gemeinsam passende Maßnahmen auszusuchen.	☐	☐	
Der Dienstleister ist bei Vertragsabschluss bereit, für alle **Subunternehmer** die hier aufgeführten Anforderungen ausgefüllt dem Kunden vorzulegen.	Geben Sie den Stab weiter – auch Ihre Subunternehmer können risikant handeln.	☐	☐	
Der Dienstleister erklärt sich bereit, **Security Audits** durch geeignete Dritte mit einer angemessenen Vorlaufzeit zu akzeptieren.	Geben Sie den Stab weiter – auch Ihre Subunternehmer können risikant handeln.	☐	☐	
Prävention				
Der Dienstleister gewährleistet eine definierte **Mindestverfügbarkeit** pro Monat für alle für den Kunden relevanten Systeme (Service Level Agreement - „SLA“).	Die Mindestverfügbarkeit muss zu Ihrem Kunden passen. Richten Sie ihre internen Dienste darauf aus.	☐	☐	
Der Dienstleister bietet an, für alle für den Kunden relevante Systeme **Backups nach Stand der Technik** durchzuführen und auf Anforderung des Kunden testweise rückzusichern.	Sehen Sie geeignete Prozesse für das Rückspielen vor.	☐	☐	
Der Dienstleister ist in der Lage, eine **Inventarisierung** aller für den Auftraggeber relevanten Anwendungen und Systeme zu dokumentieren.	Eine kundenspezifische CMDB sollte Pflicht sein, wenn Sie IT-Sicherheitsaufgaben für Kunden übernehmen.	☐	☐	
Es gibt einen **dokumentierten Prozess**, um Änderungen an Systemen zu erfassen und die Sicherheitsauswirkungen bewerten zu können, bevor die Änderungen durchgeführt werden.	Der Prozess sollte durch Sie definiert, dokumentiert und gesteuert werden.	☐	☐	
Eine Fernwartung geschieht ausschließlich über nach dem Stand der Technik **verschlüsselte Leitungen** mit angemessen starker **Authentifizierung**.	Verwenden Sie für versichedene Kunden niemals identische Passwörter!	☐	☐	

Kriterium	Dienstleisterhinweise	ja	nein	Bemerkung
Reaktion				
Der Dienstleister bietet an, Vorkehrungen zu treffen, um **Hacker-Angriffe** auf alle für den Kunden relevanten Systeme zu erkennen.	Dies kann manuell geschehen (z.B. Logfile-Analyse) oder automatisch (z.B. Einsatz von SIEM-Lösungen).	☐	☐	
Sicherheitswarnungen/-meldungen zu allen mit dem Kunden vereinbarten Betriebssystemen, IT-Systemen und Software-Anwendungen werden **beobachtet**.	Dafür gibt es standardisierte Informationsangebote. Voraussetzung ist in der Regel eine aktuelle CMDB.	☐	☐	
Sicherheitsvorfälle und -warnungen mit **hoher Kritikalität** werden sofort an den Kunden kommuniziert und es wird unverzüglich (entsprechend der vereinbarten SLAs) in Abstimmung mit dem Kunden ein sicherer Zustand wieder hergestellt.	Etablieren Sie einen Notfall-Prozess zur Information der Kunden bei kritischen Vorfällen und Warnungen!	☐	☐	
Sicherheitsvorfälle und –warnungen mit **normaler Kritikalität** werden am gleichen Tag an den Kunden kommuniziert und in Abstimmung mit dem Kunden ein sicherer Zustand wieder hergestellt.	Seien Sie transparent bei der Festlegung der Kriterien für Kritikalität.	☐	☐	
Der Dienstleister bietet **IT-Notfall-Dienstleistungen** an.	Dies sollte auch für alle Systeme angeboten werden, für die nicht im SLA benannt sind.	☐	☐	
Lieferant				
Der Dienstleister führt bzgl. seines eigenen Geschäftes und seiner Infrastruktur regelmäßig eine **Risikoanalyse** durch und hat geeignete Notfallpläne und **risikosenkende Maßnahmen** im Einsatz.	Ihre internen Prozesse müssen sich an den Schutzbedarfen Ihrer Kunden ausrichten.	☐	☐	
Die **Mitarbeiter** des Dienstleisters sind nachweislich angemessen zu Sicherheitsthemen **qualifiziert**. Auch bei Sicherheitsvorfällen ist eine ausreichende personelle Ausstattung mit **nachgewiesener Kompetenz** (z.B. Herstellerzertifikat) für alle für den Kunden relevante Systeme gegeben.	Ihre internen Prozesse müssen sich an den Schutzbedarfen Ihrer Kunden ausrichten.	☐	☐	
Der Dienstleister dokumentiert seine regelmäßigen **Sicherheits-Sensibilisierungen und -Schulungen** bei seinen Mitarbeitern und gewährt den Kunden Einblick in die Dokumentation.	Die Sensibilisierungen Ihrer Mitarbeiter sollte den Schutzbedarf der Kunden mit berücksichtigen.	☐	☐	
Auf **Ausscheiden eines Mitarbeiters** des Dienstleisters wird das Benutzerkonto deaktiviert, Passwörter geändert und alle Unterlagen, die den Kunden betreffen, eingezogen.	Es empfiehlt sich für IT-Dienstleister, aus Selbstschutz ein Privileged Access Management einzusetzen.	☐	☐	
Personenbezogene Daten von Mitarbeitern des Kunden werden in die Schadenspotenzianalyse im Rahmen des **Datenschutzmanagements** des Dienstleisters mit einbezogen.	Es empfiehlt sich für IT-Dienstleister, aus Selbstschutz ein Privileged Access Management einzusetzen.	☐	☐	

Kriterium	Anwenderhinweise	Notizen
Organisation 		
Der Dienstleister bietet an, eine **Schutzbedarfsanalyse** für die Systeme des Kunden durchzuführen, sowie daraus gemeinsam mit dem Kunden ein **Sicherheitskonzept** abzuleiten.	Der Dienstleister soll damit nachweisen, dass er die Kompetenz hat, die richtigen Dinge zu tun, um den Anwender optimal zu schützen.	
Die Auswahl der technischen Sicherungsverfahren und die Organisation der IT-Sicherheit werden in Abstimmung mit dem Kunden auf der Basis der Best Practices der **ISO 27002** (oder vergleichbar) abgestimmt.	Oder vergleichbar: z.B. VDS 3473, IT-Grundschutz, Basis-Absicherung nach 200-2.	
Der Dienstleister **berichtet** monatlich über den sicherheitsrelevanten Status der Kundensysteme und gibt **Handlungsempfehlungen**.	Es kann, muss kein physischer Termin sein. Ist man eingespielt, reichen oft ein kleiner Bericht und ein Telefonat.	
Der Dienstleister ist bei Vertragsabschluss bereit, für alle **Subunternehmer** die hier aufgeführten Anforderungen ausgefüllt dem Kunden vorzulegen.	Die gleichen Anforderungen müssen auch für Subunternehmen gelten.	
Der Dienstleister erklärt sich bereit, **Security Audits** durch geeignete Dritte mit einer angemessenen Vorlaufzeit zu akzeptieren.	Geeignete Dritte sind etwa Wirtschaftsprüfer, Steuerberater, Gutachter, beauftragte Vertreter der Kammern, oder andere, geeignet qualifizierte Personen.	
Prävention 		
Der Dienstleister gewährleistet eine definierte **Mindestverfügbarkeit** pro Monat für alle für den Kunden relevanten Systeme (Service Level Agreement - „SLA“).	Die Mindestverfügbarkeit muss zu Ihrem Bedarf passen. Oft ist 99% der Arbeitszeit ausreichend.	
Der Dienstleister bietet an, für alle für den Kunden relevante Systeme **Backups nach Stand der Technik** durchzuführen und auf Anforderung des Kunden testweise rückzusichern.	Für die testweise Rücksicherung müssen Sie mitarbeiten; ein eingespielter Prozess kann große Schäden vermeiden.	
Der Dienstleister ist in der Lage, eine **Inventarisierung** aller für den Auftraggeber relevanten Anwendungen und Systeme zu dokumentieren.	Nur wenn alle Systeme bekannt sind, können auftretende Schwachstellen auch bezüglich ihres Risikos bewertet werden.	
Es gibt einen **dokumentierten Prozess**, um Änderungen an Systemen zu erfassen und die Sicherheitsauswirkungen bewerten zu können, bevor die Änderungen durchgeführt werden.	Lassen Sie sich den Prozess zeigen, damit Ihre Risikoaffinität dadurch abgebildet ist.	
Eine Fernwartung geschieht ausschließlich über nach dem Stand der Technik **verschlüsselte Leitungen** mit angemessen starker **Authentifizierung**.	Je nach Schutzbedarf reichen gute Passwörter - evtl. sind auch SMS-basierte Lösungen geboten.	

Kriterium	Anwenderhinweise	Notizen
Reaktion 		
Der Dienstleister bietet an, Vorkehrungen zu treffen, um **Hacker-Angriffe** auf alle für den Kunden relevanten Systeme zu erkennen.	Fragen Sie explizit nach, welche Angriffe der Dienstleister erkennt, und wann er Sie darüber informiert.	
Sicherheitswarnungen/-meldungen zu allen mit dem Kunden vereinbarten Betriebssystemen, IT-Systemen und Software-Anwendungen werden **beobachtet**.	Wichtig ist, der Dienstleister relevante Information für Ihre Systeme zeitnah bekommt - und natürlich verarbeitet.	
Sicherheitsvorfälle und -warnungen mit **hoher Kritikalität** werden sofort an den Kunden kommuniziert und es wird unverzüglich (entsprechend der vereinbarten SLAs) in Abstimmung mit dem Kunden ein sicherer Zustand wieder hergestellt.	Bei kritischen Vorfällen und Warnungen sollten Sie sich die Zeit nehmen, das für Sie entstehende Risiko (mit) zu bewerten.	
Sicherheitsvorfälle und –warnungen mit **normaler Kritikalität** werden am gleichen Tag an den Kunden kommuniziert und in Abstimmung mit dem Kunden ein sicherer Zustand wieder hergestellt.	Bei nicht-kritischen Vorfällen und Warnungen sollten Sie hin und wieder prüfen, ob Sie die Einschätzung der Kritikalität mitttragen.	
Der Dienstleister bietet **IT-Notfall-Dienstleistungen** an.	CERT-Dienstleistungen behandeln eingetretene Sicherheitsprobleme und helfen bei der Behebung – auch auf Anwender-Seite.	
Lieferant 		
Der Dienstleister führt bzgl. seines eigenen Geschäftes und seiner Infrastruktur regelmäßig eine **Risikoanalyse** durch und hat geeignete Notfallpläne und **risikosenkende Maßnahmen** im Einsatz.	Schwächen in diesem Bereich können Rickwirkungen auf Ihre Systeme und Daten haben.	
Die **Mitarbeiter** des Dienstleisters sind nachweislich angemessen zu Sicherheitsthemen **qualifiziert**. Auch bei Sicherheitsvorfällen ist eine ausreichende personelle Ausstattung mit **nachgewiesener Kompetenz** (z.B. Herstellerzertifikat) für alle für den Kunden relevante Systeme gegeben.	Bei Sicherheitsvorfällen sind meist mehrere oder alle Kunden betroffen. Gerade dann ist eine hohe Verfügbarkeit von kompetentem Personal wichtig.	
Der Dienstleister dokumentiert seine regelmäßigen **Sicherheits-Sensibilisierungen und -Schulungen** bei seinen Mitarbeitern und gewährt den Kunden Einblick in die Dokumentation.	Sie sollten in der Lage sein zu prüfen, ob die Sensibilisierung auch für Ihren Schutzbedarf angemessen erscheint.	
Auf **Ausscheiden eines Mitarbeiters** des Dienstleisters wird das Benutzerkonto deaktiviert, Passwörter geändert und alle Unterlagen, die den Kunden betreffen, eingezogen.	Biespielsweise kann ein Privileged Access Management den Zugang zu Systemen durch Administratoren kontrollieren – es werden Personen-spezifische Passwörter vergeben, so müssen die eigentlichen Admin-Passwörter nicht geändert werden.	
Personenbezogene Daten von Mitarbeitern des Kunden werden in die Schadenspotenzianalyse im Rahmen des **Datenschutzmanagements** des Dienstleisters mit einbezogen.	Dies ist im Rahmen der Auftragsdatenverarbeitung sowieso gefordert.	