

1 Hintergrund

Im Programm „Sicherheit für den Mittelstand“ stellt die T-Systems drei standardisierte, aufeinander aufbauende IT-Sicherheitsbausteine zur Verfügung: Basissicherheit, Standardsicherheit, Professionelle Sicherheit. Diese Leistungsbeschreibung präzisiert die Leistungen für den Baustein „Standardsicherheit“.

2 Baustein „Standardsicherheit“

Zusätzlich zu den Leistungen aus dem Baustein „Basissicherheit“ (siehe entsprechende Leistungsbeschreibung) werden folgende Leistungen erbracht:

- Durchführung von Offsite-Penetrationstests nach Absprache mit dem Kunden.
- Durchführung eines Sicherheitsaudits vor Ort beim Kunden.
- Vergabe eines Siegels „Sicherheit für den Mittelstand“ mit der Möglichkeit, dieses als Nachweis der Sicherheitsbemühungen (auch zu Werbezwecken) zu verwenden.

Der Baustein „Standardsicherheit“ wird in Form eines Abonnements angeboten: Der Kunde beauftragt für jeweils ein Jahr die Nutzung der Leistungen aus diesem Baustein. Solange nicht mindestens 3 Monate vor Ablauf eines Abonnementsjahres gekündigt wird, verlängert sich die Nutzung jeweils um ein weiteres Jahr.

3 Leistungsbeschreibung

Die Leistungsbeschreibung des Bausteins „Basissicherheit“ ist mit allen Leistungen und Bedingungen auch Gegenstand des Bausteins „Standardsicherheit“, ohne dass dies im Folgenden explizit beschrieben wird.

3.1 Offsite-Penetrationstests

Für max. drei IP-Adressen des Kunden werden Offsite-Penetrationstests durchgeführt. Entsprechende Tests für weitere IP-Adressen können gegen Aufpreis vereinbart werden.

Die Offsite-Penetrationstests werden in der Reihenfolge des Eingangs der Aufträge und nach terminlicher Absprache mit dem Kunden durchgeführt. Die Testergebnisse werden im Auditbericht (s. 3.2) dokumentiert.

3.2 Audit vor Ort

Am zentralen Standort des Kunden wird ein ca. eintägiges Audit zum IT-Sicherheitsmanagement durchgeführt. Falls nach vorheriger Absprache und sachlicher Notwendigkeit weitere Standorte einbezogen werden müssen, wird ein Aufpreis erhoben. Das Audit wird in Anlehnung an den Standard ISO/IEC 27001 durchgeführt, und zwar anhand einer Checkliste und unter Nutzung des ausgefüllten Fragebogens (s. Baustein „Basissicherheit“). Die Ergebnisse des Audits werden normgerecht dokumentiert (Auditbericht) und dem Kunden übergeben.

Eventuell beim Audit festgestellte Sicherheitsdefizite sind vom Kunden zeitnah zu beseitigen, sofern eine Siegelvergabe (s. 3.3) erfolgen soll; die Beseitigung wird vom Kunden schriftlich angezeigt und beim nächsten Audit vom Auditor begutachtet.

3.3 Siegelvergabe

Sobald der Kunde die Beseitigung eventueller im Auditbericht aufgeführter Defizite schriftlich mitgeteilt hat, erhält er ein Prüfsiegel „Sicherheit für den Mittelstand“ in elektronischer Form.

Der Kunde ist berechtigt, dieses Siegel in eigenen Dokumenten (z.B. Briefbögen) oder auch auf dem eigenen Web-Server zu verwenden. Diese Gestattung gilt für die Dauer des Abonnements des Bausteins „Standardsicherheit“ und solange nicht in Folgeprüfungen (s. 3.4) Sicherheitsdefizite festgestellt werden, die vom Kunden nicht zeitnah behoben werden.

Die Siegelvergabe erfolgt durch die Zertifizierungsstelle der T-Systems. Die Zertifizierungsstelle arbeitet auf der einschlägigen Grundlage der DIN EN 45011.

3.4 Folgeprüfungen

Im Rahmen des Abonnements werden jährliche Folgeprüfungen durchgeführt. Bestandteil der Folgeprüfungen sind die erneute Durchführung der Offsite-Penetrationstests (s. 3.1) und ein Wiederholungs-Audit. Zur Vorbereitung des Wiederholungs-Audits sendet der Kunde den erneut ausgefüllten Fragebogen - unter Berücksichtigung eingetretener Veränderungen.

Für das Wiederholungs-Audit gelten die gleichen Bedingungen und der gleiche Ablauf wie beim Erstaudit (s. 3.2).

4 Zusätzliche Leistungen

Zu den zusätzlichen Leistungen gegen Aufpreis gehören

- Penetrationstests für weitere IP-Adressen (s. 3.1),
- Auditierung weiterer Standorte (s. 3.2),
- Ausstellung besonderer Sicherheitsbestätigungen (z.B. für Aufsichtsbehörden, Kreditinstitute).

5 Sonstiges

Der Baustein "Standardsicherheit" wird über Vertriebs- und Leistungspartner des Programms „Sicherheit für den Mittelstand“ angeboten., kann jedoch auch direkt bei der Zertifizierungsstelle bestellt werden.

Mit der Bestellung dieses Bausteins stimmt der Kunde der Übermittlung seiner Daten an ggf. zu beteiligende Leistungspartner zu. Die Vertriebs- und Leistungspartner haben sich verpflichtet, alle Informationen des Kunden vertraulich zu behandeln und nur zum Zwecke der Leistungserbringung zu verwenden.

Die Durchführung aller Prüfungen erfolgt in der Reihenfolge des Eingangs der Aufträge und nach terminlicher Absprache mit dem Kunden.

Die Offsite-Penetrationstests werden mit der gebotenen Sorgfalt und auf der Basis langjähriger Erfahrungen durchgeführt; jedoch kann keine Gewähr für die Vollständigkeit und Richtigkeit der Testergebnisse übernommen werden.

Es wird darauf hingewiesen, dass Penetrationstests zu Betriebsstörungen und Ausfällen führen können. Hieraus kann der Kunde keine Ansprüche an die T-Systems bzw. ihre Vertriebs- und Leistungspartner ableiten. Jegliche Haftung ist insoweit ausgeschlossen.

Für die Durchführung des Audits vor Ort gewährt der Kunde den Auditoren der Initiative Zugang zu den relevanten Liegenschaften, Räumlichkeiten und Unterlagen. Wird der Zugang ganz oder teilweise verwehrt, besteht seitens des Kunden kein Anspruch auf Vollständigkeit und Richtigkeit der Ergebnisse.

Es gelten die Allgemeinen Geschäftsbedingungen der T-Systems GEI GmbH.