Sicherheitsanforderung

Externes Hosting

Deutsche Telekom Gruppe

Version	2.3
Datum	07.11.2017
Status	Freigegeben

Impressum

Herausgeber
Deutsche Telekom AG
Vorstandsbereich Datenschutz, Recht und Compliance
Group Security Policy
Friedrich-Ebert-Allee 140, 53113 Bonn
Deutschland

Dateiname	Dokumentennummer	Dokumententyp
	3.08	Sicherheitsanforderung

Version	Stand	Status
2.3	07.11.2017	Freigegeben

Telekom Security	Gültigkeitsdauer	Freigegeben von
https:/ / security.telekom.com	07.11.2017 - 06.11.2022	Markus Schmall, Leiter SEC-AST

Zusammenfassung
Externes Hosting

Inhaltsverzeichnis

1. Einleitung

Dieses Dokument wurde auf Basis der Vorgaben aus der Konzernrichtlinie IT-/NT-Sicherheit erstellt.Die Sicherheitsanforderung dient u.a. als Grundlage zur Freigabe im PSA-Prozess. Sie dient darüber hinaus als Umsetzungsempfehlung für Vorgaben der KRL IT-/NT-Sicherheit in Einheiten, die nicht am PSA-Verfahren teilnehmen. Diese Anforderungen müssen bereits während der Planungs- und Entscheidungsprozesse berücksichtigt werden. Bei der Umsetzung der Sicherheitsanforderung ist das jeweils vorrangige nationale, internationale und supranationale Recht zu beachten.

2. Anforderungen an das externe Sicherheitsmanagement

Req 1	Der Hosting Provider/SaaS Provider muss einen entscheidungsbefugten Ansprechpartner für alle Sicherheitsfragen zur Verfügung stel-len.

Der Ansprechpartner sollte hier auch Schnittstelle für Meldungen aus dem Schwachstellenmanagement der jeweiligen Landesgesellschaft sein. Der Ansprechpartner muss für technische/nicht technische Aspekte zur Verfügung stehen.

Motivation: Im Fall eines Sicherheitsvorfalls muss schnell und kompetent gehandelt werden können. Zur Vermeidung vermeidbarer Verzögerungen ist ein Ansprechpartner unumgänglich.

ID: 3.08-1/2.3

Req 2	Der Hosting Provider/SaaS Provider muss eine telefonische 7x24 Stunden-Erreichbarkeit für alle Sicherheitsthemen sicherstellen. Der HostingProvider/SaaS Provider muss diese Erreichbarkeit mindestens während der üblichen Geschäftszeiten sicherstellen, sofern nicht explizit anders im SLA vereinbart.

Motivation: Im Fall eines Sicherheitsvorfalls muss unverzüglich gehandelt werden können. Eine ständige Erreichbarkeit ist daher unumgänglich.

ID: 3.08-2/2.3

Req 3	Der Hosting Provider/SaaS Provider muss ein jährlich aktualisiertes Security Framework / Sicherheitsprozeß besitzen, umsetzen und dieses auf Nachfrage des Auftraggebers oder einer vom Auftraggeber benannten Stelle vorlegen.

Motivation: Durch die Umsetzung eines Security Frameworks wird eine strukturierte und nachvollziehbare Herangehensweise in Sicherheitsfragen sicher gestellt.

ID: 3.08-3/2.3

Req 4	Der Hosting Provider/SaaS Provider muss Prozesse und Prozessdokumentation etablieren, um schnell und effizient auf Sicherheitsschwächen und Sicherheitsvorfälle zu reagieren und diese auf Nachfrage auf Nachfrage des Auftraggebers oder einer vom Auftraggeber benannten Stelle vorlegen.

Motivation: Im Fall eines Sicherheitsvorfalls muss schnell und kompetent gehandelt werden können. Zur Vermei-dung unnötiger Verzögerungen ist eine Prozessbeschreibung inkl. Training der Prozesse unumgäng-lich.

ID: 3.08-4/2.3

Req 5	Der Hosting Provider/SaaS Provider muss sicherstellen, dass der Auftraggeber, ggf. auch das zuständige Sicherheitsmanagement, unverzüglich nach Bekanntwerden eines Sicherheitsvorfalls/einer schwerwiegenden Sicherheitsschwäche mit Relevanz für Systeme der Deutschen Telekom Gruppe informiert wird.

Motivation: Um schnellstmöglich auf Anfragen von Kunden / Partnern / Presse reagieren zu können ist eine zeitnahe Informationspolitik notwendig.

ID: 3.08-5/2.3

Req 6	Der Hosting Provider/SaaS Provider muss technisch sicherstellen, dass die Daten des Auftraggebers auf Anforderung des Auftraggebers oder des zuständigen Sicherheitsmanagements innerhalb von einer Stunde in der Applikation nicht mehr verfügbar/nutzbar sind.

Die komplette Abschaltung / Netztrennung ist bei dediziert aufgebauten Systemen für die Deutsche Telekom z.B. eine angemessene Lösung.
Die Festlegung, wer Anforderer der Nutzung dieser Maßnahme sein darf, ist individuell pro System zu bestimmen.

Motivation: Im Fall eines Sicherheitsvorfalls muss es möglich sein, korrumpierte Systeme schnell zur Vermeidung von weiterem Schaden und für forensische Analysen zu isolieren.

ID: 3.08-6/2.3

Req 7	Der Hosting Provider/SaaS Provider muss vom Auftraggeber benannte Deutsche Telekom Gruppe interne Sicherheitseinheiten das Recht einräumen, eigene Audits in der von ihr (mit)genutzten Hosting-infrastruktur durchzuführen (Lieferantenaudits).

Der Hosting Provider hat den Auftraggeber und von ihm benannte Sicherheitseinheiten der Deutschen Telekom Gruppe bei der Durchführung zu unterstützen. Eine Unterstützung im Detail heißt, dass

- Testaccounts zur Verfügung gestellt werden,
- Relevante Sicherheitsdokumentation einsehbar ist und
- Zugänge (technisch/physisch) zur Verfügung gestellt werden.

Motivation: Durch die Verwendung von unterschiedlichen Auditoren wird ein Vier-Augen Prinzip abgedeckt.

ID: 3.08-7/2.3

Req 8	Der Hosting Provider/SaaS Provider muss nachweislich alle 12 Monate ein Sicherheitsreview seiner Hostingumgebung durchführen und auf Nachfrage die Ergebnisse dem Auftraggeber und von diesem benannten Einheiten der Deutschen Telekom Gruppe zur Verfügung stellen.

Im Scope des Audits sollte mindestens die Netzwerkinfrastruktur und die Basisapplikationen wie z. B. Apache oder Oracle sein.
Neben der Überprüfung auf Basis von Portscannern und Versionsscannern (wie z. B. Nikto) ist die Kommuni-kation auf Anomalien hin zu überprüfen.

Motivation: Im Fall eines nicht entdeckten Sicherheitsvorfalls kann dieser durch ein Review entdeckt werden. Weiterhin ermöglicht die zyklische Überprüfung der Systeme eine Anpassung an neue Entwicklungen und Problembereiche, die bisher nicht erkannt worden sind.

ID: 3.08-8/2.3

Req 9	Um die Nachhaltigkeit von Sicherheitsreviews/Auditmaßnahmen sicherzustellen muss der Hosting Provider/SaaS Provider im Anschluss an die Maßnahme einen Zeitplan zur Behebung der erkannten Schwachstellen dem Auftraggeber oder einer vom Auftraggeber benannten Stelle vorlegen.

Im Scope des Audits müssen mindestens die Netzwerkinfrastruktur und die Basisapplikationen wie z. B. Apache oder Oracle sein.Neben der Überprüfung auf Basis von Portscannern und Versionsscannern (wie z. B. Nikto) ist die Kommunikation auf Anomalien hin zu überprüfen.

Motivation: Auf Basis eines Maßnahmenplans inkl. Zeitlinien ist ein Tracking der Vorgänge möglich und es wird sichergestellt, dass temporär geduldete Systemzustände in verabredeten Zeiten behoben werden.

ID: 3.08-9/2.3

Req 10	Der Hosting Provider/SaaS Provider muss sicherstellen, dass durch die Deutsche Telekom Gruppe oder auf deren Veranlassung hin überlassene interne Informationen unter Beachtung des Prinzips „Need-to-know“ nur einem kleinen, für die Auftragsdurchführung unbedingt notwendigen Personenkreis, zugänglich sind.

Motivation: Die Eingrenzung der Daten auf einen kleinstmöglichen Adressatenkreis minimiert das Risiko einer Weitergabe von Daten.

ID: 3.08-10/2.3

Req 11	Der Hosting Provider/SaaS Provider muss Informationen im Kontext der gehosteten Anwendungen der Deut-schen Telekom Gruppe stets aktuelle Informationen über Hardware, Betriebssystem, Software, Architektur, Ansprechpartner, Härtung und Eskalationsmöglichkeiten auf Anfrage dem Auftrag-geber unentgeltlich zur Verfügung stellen.

Motivation: Ein hohes Sicherheitsniveau kann nur sichergestellt werden, wenn alle Beteiligten im Prozess nach den gleichen Maßstäben arbeiten und diese auch bekannt sind.

ID: 3.08-11/2.3

Req 12	Der Hosting Provider muss sicherstellen, dass redundante Systeme auf Anforderung der Deut-schen Telekom Gruppe in getrennten Brandabschnitten untergebracht sind.

Motivation: Redundante Systeme in getrennten Brandabschnitten zu betreiben bietet Schutz gegen physika-lische Schäden wie Wasser, Feuer etc..

ID: 3.08-12/2.3

Req 13	Der Hosting Provider muss sicherstellen, dass für zuvor durch die Deutsche Telekom Gruppe als relevant bezeichnete Anwendungen (Systeme) Sicherheitsmaßnahmen wie z. B. abschließbare Rechnerschränke zum sicheren Betrieb des Hosting zur Verfügung gestellt werden. (nicht relevant für SaaS)

Motivation: Eine Aufteilung der Sicherheitszonen ermöglicht es, für besonders zu schützende Systeme ein höheres Sicherheitsniveau zu etablieren, ohne das pauschal alle Systeme kostenintensiv zu schützen sind.

ID: 3.08-13/2.3

Req 14	Der Hosting Provider muss sicherstellen, dass Anwendungen des Auftraggebers logisch getrennt von Anwendungen anderer Kunden betrieben werden. Der SaaS Provider muss sicherstellen, dass Daten des Auftraggebers logisch getrennt von Daten anderer Kunden betrieben werden. Wenn die Art der Applikation es zulässt, muss die Anwendung/Daten auch physisch getrennt von Anwendungen/Daten anderer Kunden betrieben werden.

Motivation: Durch die Trennung der Systeme nach Auftraggeber wird das Risiko minimiert, dass sich die Systeme untereinander beeinflussen und ein geringeres Sicherheitsniveau des Systems eines anderen Kunden des Hosting Providers ein System der Deutschen Telekom Gruppe gefährdet.

ID: 3.08-14/2.3

Req 15	Der Hosting Provider/SaaS Provider muss sicherstellen, dass MZ-Systeme nicht direkt aus dem Internet erreich----bar sind.

MZ steht hierbei für „militarisierte Zone“, d. h. die Zone mit geschäftskritischen Backend-Systemen, die nur über den Umweg von Systemen in der „entmilitarisierte Zone“ (DMZ) von externen Quellen angesprochen werden dürfen.

Motivation: Die Terminierung von allem Verkehr in der DMZ ermöglicht einen weitergehenden Schutz aller MZ-Systeme.

ID: 3.08-15/2.3

Req 16	Der Hosting Provider/SaaS Provider muss sicherstellen, dass die eigentliche Datenhaltung einer Anwendung immer in nicht aus dem Internet erreichbaren Zonen geschieht.

Motivation: Durch die Nichterreichbarkeit datenhaltender Systeme aus dem Internet wird das direkte Angriffsrisiko mi-ni-miert.

ID: 3.08-16/2.3

Req 17	Die gewählte Architektur muss den Industry Best Practices entsprechen und auch eine Separierung der funktionalen Blöcke sicherstellen.

Eine Separierung der funktionalen Blöcke (d.h. Datenbank und Webserver nicht auf einer logischen Instanz) ist notwendig, um die Auswirkung der Übernahme einer Softwarekomponente so gering wie möglich zu halten.

Motivation: Durch die Verwendung von Industriestandards kann die Verfügbarkeit, Skalierbarkeit und Sicherheit von Anwendungen effizient / effektiv sichergestellt werden.

ID: 3.08-17/2.3

Req 18	Der Hosting Provider/SaaS Provider muss Maßnahmen/Werkzeuge zur Angriffserkennung vorhalten und nutzen.

Geeignete Maßnahmen an dieser Stelle können sein:

- Tools zur Logfileananalyse (z. B. Access/Error Logs) jenseits eines reinen Texteditors
- Firewall Systeme
- Intrusion Detection Systeme
- Netzwerkmonitore

Intrusion Prevention Systeme sind aus aktueller Techniksicht nicht zwanghaft einzusetzen.

Motivation: Durch eine frühzeitige Erkennung von Angriffen kann Schaden abgewendet werden.

ID: 3.08-18/2.3

Req 19	Der Hosting Provider/SaaS Provider muss geeignete Maßnahmen und Prozesse zur Abwehr von Angriffen wie z.B. DoS / Brute Force Login Versuche, die aus dem Internet auf die Systeme/Plattformen durchgeführt werden, vorhalten und dokumentieren.

Geeignete Maßnahmen an dieser Stelle können sein:

- Router mit Traffic Shaping,
- Firewall Mechanismen oder

- mehrere Peering Points.
- Captchas für Eingabeseiten
- Teergruben

Motivation: Nur basierend auf vorbeugenden Maßnahmen und einer zeitnahen Reaktion kann Schaden verhindert bzw. minimiert werden.

Umsetzungsbeispiel: Ein Beispiel für eine geeignete Segmentierung ist die Verwendung eines eigenen VLANs.

ID: 3.08-19/2.3

Req 20	Der Hosting Provider/SaaS Provider muss den Aufbau einer DMZ/MZ durch Verwendung von geeigneten akti-ven Netzelementen (mindestens Paketfilter) sicherstellen.

Eine Demilitarized Zone (DMZ, auch ent- oder demilitarisierte Zone) bezeichnet ein Computernetz mit sicher-heits-technisch kontrollierten Zugriffmöglichkeiten auf die daran angeschlossenen Server. Einzig auf Systeme der DMZ darf aus dem externen Netz/Internet direkt zugegriffen werden.

Motivation: Die Etablierung von DMZ-/MZ-Zonen ohne Verwendung von aktiven Netzelementen bietet keinen zusätzlichen Schutz.

ID: 3.08-20/2.3

Req 21	Der Hosting Provider/SaaS Provider muss sicherstellen, dass ein administrativer Zugang zu Hostingsystemen mit Anwendungen/Daten der Deutschen Telekom Gruppe nur über anerkannt zuverlässig arbeitende ver-schlüsselte Zugänge/Protokolle, wie z. B. SSH, erfolgen kann.

Motivation: Das Risiko eines Mitlauschens von administrativen Kennungen wird durch die Verwendung von verschlüsselten Protokollen deutlich verringert.

ID: 3.08-21/2.3

Req 22	Administrativer Zugänge erfolgen über Administrationsnetze bzw. via Hopping Stations (VPN basiert).

Motivation: Das Risiko eines Mitlauschens von administrativen Kennungen wird durch die Verwendung von verschlüsselten Protokollen deutlich verringert.

ID: 3.08-22/2.3

Req 23	Der Hosting Provider/SaaS Provider muss, in Abhängigkeit von der Ausprägung des gehosteten Dienstes und der verarbeitenden Daten, sicher-stel-len, dass seine Mitarbeiter auf die Einhaltung der landespezifischen Datenschutz- und Fern-mel-de-geheim-nisse der jeweiligen Legal-Einheit verpflichtet sind.

Im Falle des Hostings von personenbezogenen Daten und in Abhängigkeit des nationalesn Datenschutzgesetzes ist dieses Requirement durch eine Auftragsdatenverarbeitungsvereinbarung zu erfüllen.

Motivation: Um den Schutz der an den Hosting Provider weitergegebenen oder für diesen zugreifbaren Daten sicherzustellen, müssen die Beschäftigten angemessen auf die Schutzbedürftigkeit der Daten hingewiesen und (wenn gesetzlich erforderlich) auf deren Beachtung verpflichtet werden.
Für Kundendaten aus Deutschland bedeutet dies z. B. den Abschluss eines Vertrages zur Auftragsdaten-verar-beitung und die Verpflichtung der Beschäftigten auf das Fernmeldegeheimnis und das Bundesdaten-schutz-gesetz.

ID: 3.08-23/2.3

Req 24	Der Hosting Provider/SaaS Provider muss sicherstellen, dass das Einrichten, Ändern, Löschen, Freischalten, Sperren und Einsehen von Benutzern auf dem System nur durch hierfür unter Beachtung des Prinzips „Need-to-know“ berechtigte Administratoren/Systemprozesse erfolgen kann.

Motivation: Eine Eingrenzung bestimmter kritischer Funktionen auf einzelne Mitarbeiter verringert das generelle Missbrauchsrisiko.

ID: 3.08-24/2.3

Req 25	Der Hosting Provider/SaaS Provider muss sicherstellen, dass ein Administrator bzw. jedweder Benutzer in der Applikation nie mehr Rechte vergeben können darf, als er entsprechend seiner Rolle selbst besitzt.

Motivation: Eine Eingrenzung bestimmter kritischer Funktionen auf einzelne Mitarbeiter verringert das generelle Missbrauchsrisiko.

ID: 3.08-25/2.3

Req 26	Der Hosting Provider/SaaS Provider muss sicherstellen, dass für die Deutsche Telekom Gruppe betrie-bene Systeme mit technischen Möglichkeiten frei von Schadsoftware gehalten werden (z.B. aktuellen Virenscannern).

Im Kontext von Webanwendung mit Uploadfunktion heißt dies, dass entsprechend geuploadete Dateien durch das System automatisch geprüft werden.

Motivation: Schad-Software stellt für den Betrieb ein großes Risiko dar, da z. B. durch diese Software Zugriff auf weitere Systeme nicht ausgeschlossen werden kann.

ID: 3.08-26/2.3

Req 27	Der Hosting Provider /SaaS Provider muss durch regelmäßige (d. h. mindestens einmal pro Monat) Überprü-fun-gen sicherstellen, dass auf den für die Deutsche Telekom Gruppe betriebenen Systemen nur die vom Hosting Provider/ SaaS Provider definierte, unbedingt notwendige Software installiert/aktiviert ist.

Diese Anforderung muss im Kontext der beauftragten Leistung betrachtet werden, so ist diese Anforderung nicht zutreffend für Managed Services, da hier der Dienstleister für den Service zuständig ist.

Motivation: Regelmäßige Überprüfungen können dazu beigetragen, dass das Sicherheitsniveau auf einem bekannten Level bleibt und unnötige Software als weitere Gefahrenquelle ausgeschlossen werden kann.

ID: 3.08-27/2.3

Req 28	Der Hosting Provider/SaaS Provider muss durch regelmäßige (d. h. mindestens einmal pro Monat) Überprü-fun-gen sicherstellen, dass auf für die Deutsche Telekom Gruppe betriebenen Systemen nur die vom Hosting Provider/SaaS Provider definierten, not-wendigen Dienste und Services laufen.

Diese Anforderung muss im Kontext der beauftragten Leistung betrachtet werden, so ist diese Anforderung nicht zutreffend für managed Services, da hier der Dienstleister für den Service zuständig ist.

Motivation: Durch regelmäßige Überprüfung kann dazu beigetragen werden, Dienste und Services, die für administrative oder Support-Zwecke gebraucht wurden, als unnötige Gefahrenquelle auszuschließen.

ID: 3.08-28/2.3

Req 29	Der Hosting Provider/SaaS Provider muss sicherstellen, dass System/Applikations/Middleware Härtungen basierend auf Best-Practice-Ansätzen für die im Auftrag oder auf Veranlassung der Deutschen Telekom Gruppe betriebenen Systeme durchgeführt werden.

Best practice Haertungsvorgaben sind unter anderem bei www.cisecurity.org zu finden.

Motivation: Jedes gehärtete System erhöht die Absicherung des gesamten Rechnenzentrums.

ID: 3.08-29/2.3

Req 30	Der Hosting Provider/SaaS Provider muss nachweislich einen dokumentierten und implementierten Prozess zum Patch-manage-ment sicherstellen.

Motivation: Ständig auf einem aktuellen Patchstand gehaltene Systeme bieten weniger Angriffsfläche für externe/interne Angreifer. Ein aktueller Patchstand stellt damit einen elementaren Bestandteil eines sicheren Systems dar.

ID: 3.08-30/2.3

Req 31	Der Hosting Provider/SaaS Provider muss nachweislich sicherstellen, dass Anwendungen/Betriebssysteme immer einen aktuellen, stabilen, für den Betrieb geeigneten Patchstand aufweisen.

Motivation: Ständig auf einem aktuellen Patchstand gehaltene Systeme bieten weniger Angriffsfläche für externe/interne Angreifer. Ein aktueller Patchstand stellt damit einen elementaren Bestandteil eines sicheren Systems dar.

ID: 3.08-31/2.3

Req 32	Der Hosting Provider/SaaS Provider muss nachweislich einen Backup- und Recovery-Prozess etablieren, leben und testen.

Motivation: Backups und Recoveryverfahren ermöglichen im Schadensfall eine schnelle Wiederaufnahme des Wirkbetriebs und tragen somit zur Betriebsqualität bei.

ID: 3.08-32/2.3

Req 33	Der Hosting Provider/SaaS Provider muss sicherstellen, dass nur durch den Lieferanten/Hersteller/ Entwick-ler aktiv betreute Software eingesetzt wird.

Motivation: Sollte es in einer Softwarekomponente zu einem Fehler kommen, so ist nur bei einer aktiv gepflegten Softwareliste sichergestellt, dass Patches innerhalb eines kurzen Zeitraums zur Verfügung gestellt werden können.

ID: 3.08-33/2.3

Req 34	Der SaaS Anbieter stellt sicher, dass die Webanwendungen nach Best Practices entwickelt und gehärtet wurden (z.B. durch Abwehr aller OWASP Top 10 Angriffe und einer robusten Input Validierung).

Motivation: Durch die Verwendung von Industriestandards / Best practices kann die Verfügbarkeit, Skalierbarkeit und Sicherheit von Anwendungen effizient / effektiv sichergestellt werden.

ID: 3.08-34/2.3

Req 35	Die Härtung der etwaig eingesetzten Datenbanksysteme muss den Industrie Best Practices entsprechen.

Die Härtung umfaßt u.a. die Aspekte

- bei mehreren Datenbankinstanzen pro System muss der gleiche Betreiberkreis sichergestellt sein
- nicht benötige Pakete / Funktionen sind zu löschen
- Default Passwörter / Datenbnaken / Rollen sind zu löschen
- Datenbanken sind mit minimal notwendigen Rechten zu betreiben

Motivation: Durch die Verwendung von Industriestandards bzw. Best Practices kann die Verfügbarkeit, Skalierbarkeit und Sicherheit von Anwendungen effizient / effektiv sichergestellt werden.

Umsetzungsbeispiel: Als Beispiel hierfür können die DTAG Härtungsvorgaben für gängige Datenbanksysteme gelten. Weitere gute Quellen sind die CIS Seiten (http://www.cisecurity.org) und die Seiten der eigentlichen Hersteller.

ID: 3.08-35/2.3

Req 36	Der Hosting Provider/SaaS Provider muss sicherstellen, dass Zugriffe/Zugang auf interne Systeme und Anwendungen protokolliert werden.

Eine Protokollierung sollte mindestens die letzten sieben Tage abdecken und die Zugriffe auf Accountmanage-ment/Systemverwaltungssysteme beinhalten.

Motivation: Die Protokollierung von Zugriffen auf interne Systeme ermöglicht eine effektive Klärung von Vorfällen jeglicher Art.

ID: 3.08-36/2.3

Req 37	Der Hosting Provider/SaaS Provider muss sicherstellen, dass nur personalisierte Accounts zur Durchführung interner Arbeiten verwendet werden.

Interne Arbeiten im Sinne dieser Anforderung sind u. a.:

- Einrichtung neuer Accounts,
- Erweiterung von Firewallregelen sowie
- jegliche Form von Netzwerkverwaltungsmaßnahmen.

Motivation: Eine Verwendung von Gruppenaccounts erlaubt im Schadensfall nicht, dass eine saubere Ermittlung durchgeführt werden kann.

ID: 3.08-37/2.3

Req 38	Der Hosting Provider/SaaS Provider muss nachweislich einen dokumentierten Accountmanagementprozess für interne Accounts implementiert haben.

Motivation: Nur durch einen etablierten Prozess ist es möglich, sicherzustellen, dass sowohl neu eingestellte als auch ausscheidende Personen keinen unberechtigten Zugriffe erhalten.

ID: 3.08-38/2.3

Req 39	Zugangskontroll- und Authentisierungsmechanismen müssen entsprechend den aktuellen Best Practices in der Industrie wie z.B. starken Passwort Policies aufgebaut/angewendet werden.

Motivation: Durch die Verwendung von Industriestandards / Best Practices kann eine ausreichende Sicherheit hergestellt werden.

ID: 3.08-39/2.3

Req 40	Der Hosting Provider/SaaS Provider muss sicherstellen, dass vertrauliche Informationen wie z. B. Zugangs-daten nur verschlüsselt (basierend auf den aktuellen Verschlüsselungsstandards) übertragen und gespeichert werden.

Die Verschlüsselung der Zugangs- und Nutzdaten auf der Festplatte sollte einer Stärke von AES 256 Bit entsprechen. Für die Übertragung ist TLS 1.1 mit bevorzugt PFS Cyper Suites zu verwenden.

Motivation: Eine Verschlüsselung der auf Datenträgern gespeicherten Daten erschwert Angreifern den Zugang zu kritischen Daten.

ID: 3.08-40/2.3

Req 41	Der Hosting Provider/SaaS Provider muss Backups derart absichern (technisch, physisch und organisato-risch), dass Unberechtigte keinen Zugriff auf die Daten erhalten können.

Motivation: Da Backups vertrauliche Informationen enthalten können und generell Rückschlüsse auf Abwehr-maßnahmen ermöglichen, ist eine Absicherung der Backups (z. B. durch Einschließen in einen Stahlschrank) zwingend notwendig, um die Informationen der Deutschen Telekom Gruppe lückenlos zu sichern.

ID: 3.08-41/2.3

Req 42	Der Hosting Provider/SaaS Provider muss einen Prozess zur sicheren Vernichtung von Datenträgern (Bänder) vorweisen, diesen in die Praxis umgesetzt haben und Nachweise über die Vernichtung von Datenträgern vorlegen können.

Motivation: Ohne sichere Löschung von Datenträger besteht ein immanentes Risiko des Datenverlusts, welches explizit klein gehalten werden muss.

ID: 3.08-42/2.3

Req 43	Der Integritätsschutz der verarbeiteten Daten muss den Industry Best Practices entsprechen.

Motivation: Durch die Verwendung von Industriestandards / Best Practices kann die Verfügbarkeit, Skalierbarkeit und Sicherheit von Anwendungen effizient / effektiv sichergestellt werden.

Umsetzungsbeispiel: Die Sicherheitsanforderungen der Deutschen Telekom AG (s. www.telekom.com/sicherheit) bieten gute Beispiele / Anhaltspunkte.

ID: 3.08-43/2.3

Req 44	Der Hosting Provider/SaaS Provider muss sicherstellen, dass abgestimmte Logfiles, die lediglich

	Daten bez. Accounts und/oder Nutzung durch End-Kunden in der Rolle als Geschäftspartner, Partner und Mitarbeiter der Deutschen Telekom Gruppe enthalten, auf Anfrage innerhalb von 24 Stunden an die Deutsche Telekom Gruppe verschlüsselt übergeben werden.

Die Grundannahme hier ist, dass die datenschutzrechtliche Klärung vorab innerhalb der Deutschen Telekom Gruppe stattgefunden hat und nur eine operative Umsetzung bei dem externen Partner erfolgt.

Eine Datenübertragung kann z. B. auf Basis verschlüsselter E-Mail-Kommunikation erfolgen.

Motivation: Im Falle einer Betriebsstörung muss zur Aufrechterhaltung des Betriebs kurzfristig reagiert werden können.

ID: 3.08-44/2.3

Req 45	Der Hosting Provider/SaaS Provider muss Logfiles revisionssicher gegen Verlust, Manipulation und Zugriff Unberechtigter schützen.

Motivation: Da Logfiles Rückschlüsse auf die Art des Angriffs und die Angreifer erlaubt, werden diese ein erstes Ziel der Angreifer sein. Eine Absicherung der Logfiles ermöglicht/vereinfacht daher die Täteridentifizierung.

ID: 3.08-45/2.3

Req 46	Industry Best Practices entsprechende Fraud Präventionsmechanismen müssen angemessen eingebaut / umgesetzt sein.

Motivation:
Durch die Verwendung von Industriestandards / Best Practices kann die Verfügbarkeit, Skalierbarkeit und Sicherheit von Anwendungen effizient / effektiv sichergestellt werden.

ID: 3.08-46/2.3

Req 47	Die Virtualisierungssoftware muss entsprechend der Härtungsvorschriften der jeweiligen Hersteller / Best Practices betrieben werden.

ID: 3.08-47/2.3

Req 48	Der Kommunikationskanal von virtueller Maschiene zum Virtualisierungsserver / - host und umgekehrt ist soweit wie möglich einzuschränken.

ID: 3.08-48/2.3

2.1. Rechtliche Aspekte

Req 49	Im Falle der Unterbeauftragung von Personen mit Zugriff auf vertrauliche Daten / personenbezogene Daten der Deutschen Telekom muss der Hosting Provider/SaaS Provider sich, sofern er für die Deutsche Telekom Gruppe vertrauliche Daten verarbeitet, den Einsatz von Unterauftragnehmern durch den Auftraggeber in der Deutschen Telekom Gruppe genehmigen lassen.

Motivation: Ein hohes Sicherheitsniveau kann nur sichergestellt werden, wenn alle Beteiligten im Prozess nach den gleichen Maßstäben arbeiten und dies auch vertraglich dokumentiert ist.

ID: 3.08-49/2.3

Req 50	Der Hosting Provider/SaaS Provider muss ein DTAG Non Disclosure Agreement (NDA) mit dem Auftraggeber unter-zeichnen, sofern der Hostingpartner/Provider durch die erbrachte Leistung geschäftliche Informationen der Deutschen Telekom Gruppe erlangen kann.

Ein NDA MUSS zwischen Auftraggeber und dem Hosting Provider abgeschlossen sein, um die Vertraulichkeit der weitergegebenen oder zugänglich gemachten Informationen sicherzustellen.

Motivation: Durch die Unterzeichnung eines NDA können schutzbedürftige Informationen des Konzerns unter Beachtung des Grundsatzes „Need-to-know" weitergegeben werden.

ID: 3.08-50/2.3