Public (Öffentlich)

BT SCHÜTZEN

Unser Standard für Drittanbieter-Sicherheitsmaßnahmen

Version: 1.1 **Eigentümer:** Mark Tilston

Mit diesem Standard werden die grundlegenden Sicherheitsmaßnahmen für unsere Drittanbieter festgelegt.

Er wird veröffentlicht und an alle betroffenen Parteien kommuniziert und wird mindestens einmal jährlich von den „Subject Matter Expert's“ (Fachexperten) überprüft, um sicherzustellen, dass er weiterhin den Anforderungen der interessierten Parteien und unseren Geschäftszielen, wie sie im ISMS von BT beschrieben sind, entspricht.

Der Standard gilt für alle Drittanbieter, die für die oder im Auftrag der BT Group einschließlich Openreach, EE und PlusNet tätig sind.

Der Einfachheit halber verwenden wir für das restliche Dokument die Bezeichnung „BT“.

Wenn eine Aktivität von einem BT-Stakeholder durchgeführt werden muss, ist sie grau markiert.

Einführung

BT verpflichtet sich, ein sicheres Umfeld zu schaffen, dem unsere Kunden und Mitarbeiter vertrauen können. Unser Ziel ist es, alle unsere Informationen und Systeme vor versehentlicher oder böswilliger Zerstörung, Beschädigung, Veränderung oder Offenlegung zu schützen. Wir erreichen dies, indem wir sicherstellen, dass wir die richtigen Sicherheitsmaßnahmen für Drittanbieter vorgeben und so die Vertraulichkeit, Integrität und Verfügbarkeit unserer Informationen und Systeme schützen.

Für wen gilt der Standard?

Dieser Standard gilt für alle Drittanbieter, die für BT tätig sind oder im Auftrag von BT mit BT-Informationen oder -Daten in Kontakt kommen, auf sie zugreifen, sie verarbeiten, speichern oder verteilen. Wir können diesen Standard von Zeit zu Zeit ändern, vorbehaltlich der vereinbarten internen Konsultationsverfahren.

Begriffsdefinition:

Begriff	Erklärung
muss/müssen	Dieser Begriff oder die Begriffe „ERFORDERLICH“ oder „MUSS/MÜSSEN“ bedeuten, dass die Definition absolut verpflichtend sind.
dürfen nicht	Dieser Begriff oder der Begriff „DÜRFEN NICHT“ bedeutet, dass die Definition absolut verpflichtend sind.
kann/können	Dieser Begriff und das Adjektiv „OPTIONAL“ bedeuten, dass etwas wirklich optional ist.
sollte/sollten	Dieses Wort/diese Wörter oder das Adjektiv „EMPFOHLEN“ bedeutet, dass es in bestimmten Situationen einen triftigen Grund gibt, etwas Bestimmtes zu ignorieren, die Auswirkungen davon aber vollständig verstanden und sorgfältig bewertet werden, bevor eine andere Option gewählt wird.
sollte/sollten nicht	Dieser Begriff oder der Begriff „NICHT EMPFOHLEN“ bedeutet, dass alle Anstrengungen unternommen werden, um die Anforderungen einer Kontrolle zu erfüllen, aber dass die beschriebene Aktion nicht immer und in allen Fällen vermieden werden kann. Wenn die Anforderungen einer Kontrolle nicht erfüllt werden können, werden die Folgen bewertet und voll verstanden.

Geltungsbereich:

Dieses Dokument beschreibt auf hohem Niveau die Mindestsicherheitsmaßnahmen, die für das Sicherheitsmanagement innerhalb der Drittanbieter-Lieferkette von BT erforderlich sind.

Die Mitarbeiter von BT finden auf der Security-Website unterstützende Standards sowie die Grundlagen, Prozessdokumente und Richtlinien, die die Umsetzung der Maßnahmen beschreiben, die in Verbindung mit diesem Standard gelesen werden müssen.

BT-Stakeholder, die eine Ausnahme von diesem Standard für einen Drittanbieter wünschen, müssen eine Anfrage über den Ausnahme-Prozess stellen

Was beinhaltet dieses Dokument?

1. Rollen und Verantwortlichkeiten.

Alle Drittanbieter müssen die Anforderungen dieses Standards kennen und verstehen und sind dafür verantwortlich, dass alle Personen, die an der Erbringung eines Dienstes für BT beteiligt sind, mit den relevanten Anforderungen dieses Standards vertraut sind und diese erfüllen.

BT-Stakeholder sind dafür verantwortlich, die Compliance mit diesem Standard zu überwachen und mit dem Drittanbieter zusammenzuarbeiten, um die Compliance zu verbessern und bei festgestellten Lücken Abhilfemaßnahmen zu ergreifen.

Die Manager von BT sind dafür verantwortlich, sicherzustellen, dass ihre Mitarbeiter mit diesem Standard und den damit verbundenen Richtlinien und Standards vertraut sind und diese einhalten.

2. Governance

2.1. Der Drittanbieter muss über einen etablierten und konsistenten Industriestandard-Sicherheitsrahmen für die Informations- und Cybersicherheits-Governance verfügen, der die folgenden Komponenten umfasst:

- Angemessene Informations- und Cyber-Sicherheitsrichtlinien und -verfahren, die genehmigt und mitgeteilt werden
- Eine Informationssicherheitsstrategie
- Einschlägige gesetzliche und regulatorische Anforderungen in Bezug auf Informations- und Cybersicherheit (einschließlich Datenschutz), die verstanden und verwaltet werden
- Governance- und Risikomanagementprozesse, die sich mit Informations- und Cybersicherheitsrisiken befassen

2.2. Der Drittanbieter muss sicherstellen, dass angemessene Rollen und Verantwortlichkeiten für die Informations- und Cybersicherheit definiert und umgesetzt werden. Dies umfasst Folgendes:

- Ein in Vollzeit beschäftigter "Chief Information Security Officer" (oder in vergleichbarer Position), der eine ausreichend hochrangige Position hat und die Verantwortung für das Informationssicherheitsprogramm trägt.
- Eine hochrangige Arbeitsgruppe, ein Ausschuss oder ein gleichwertiges Gremium unter dem Vorsitz eines entsprechend hochrangigen Mitarbeiters, welches die Aktivitäten im Bereich der Informationssicherheit beim gesamten Drittanbieter koordiniert und sich regelmäßig trifft
- Eine spezialisierte Informationssicherheitsfunktion mit geeigneten und definierten Rollen und Verantwortlichkeiten

2.3. Der Drittanbieter muss sicherstellen, dass es eine individuelle Verantwortung für Informationen und Systeme gibt, indem er dafür sorgt, dass es ein angemessenes Eigentumsrecht an kritischen Geschäftsumgebungen, Informationen und Systemen gibt und dass diese fähigen Personen zugewiesen wird.

2.4. Der Drittanbieter muss sicherstellen, dass er BT (schriftlich) benachrichtigt, sobald er rechtlich dazu in der Lage ist, wenn der Drittanbieter Gegenstand einer Fusion, Übernahme oder eines anderen Eigentümerwechsels ist.

3. Incident Management (Vorfallmanagement)

3.1. Der Drittanbieter muss über ein etabliertes und konsistentes Rahmenwerk für das Incident Management verfügen, um sicherzustellen, dass Vorfälle angemessen gehandhabt, eingedämmt und gemildert werden, und das die folgenden Komponenten umfasst:

- Sicherstellen, dass die Mitarbeiter, wenn eine Reaktion erforderlich ist, ihre Rollen und die Reihenfolge der Abläufe kennen
- Sicherstellen, dass Vorfälle nach den festgelegten Kriterien gemeldet werden
- Sicherstellen, dass die Auswirkungen von Vorfällen verstanden werden
- Sicherstellen, dass die nachträgliche Untersuchungen und Analysen, wenn nötig, entweder intern oder durch eine Fachfunktion durchgeführt wird
- Sicherstellen, dass die aus den Vorfällen gezogenen Lehren in die bewährten Methoden einfließen
- Sicherstellen, dass Informationen, die sich auf einen Vorfall beziehen, der eine Auswirkung auf BT hat, als „vertraulich“ behandelt werden.

3.2. Der Drittanbieter unternimmt alle angemessenen Schritte, um sicherzustellen, dass eine geeignete Person oder geeignete Personen als Ansprechpartner für Sicherheitsrisiken, Incident Management und Compliance Management bestimmt und dafür verantwortlich gemacht werden. Der Drittanbieter teilt dem BT Stakeholder die Kontaktdaten der Person(en) mit und informiert die zuständige(n) Person(en) ebenfalls, wenn sich diese ändern. Die Kontaktdaten sollten Folgendes enthalten: Name, Zuständigkeit, Rolle und Gruppen-E-Mail-Adresse und/oder Telefonnummer.

3.3. Der Drittanbieter informiert den BT Stakeholder innerhalb eines angemessenen Zeitraums nach Bekanntwerden eines Vorfalls, der sich auf die Dienste für BT oder BT-Informationen auswirkt, auf jeden Fall aber spätestens zwölf (12) Stunden, nachdem der Vorfall dem Drittanbieter zur Kenntnis gelangt ist.

3.4. Der Drittanbieter ergreift ohne unangemessene Verzögerung angemessene und rechtzeitige Korrekturmaßnahmen, um alle Risiken und Auswirkungen im Zusammenhang mit dem Vorfall zu mindern und dadurch die Schwere und Dauer des Vorfalls zu verringern.

3.5. Der Drittanbieter legt dem BT Stakeholder einen Bericht über jeden Vorfall vor, der sich auf die Dienste für BT oder die BT-Informationen auswirkt. Dieser Bericht sollte mindestens das Folgende beinhalten:

- Datum und Uhrzeit
- Ort
- Art des Vorfalls
- Auswirkung
- Klassifizierung der Informationen, auf die der Vorfall sich auswirkt (Siehe Datenklassifizierungs- und Datenverarbeitungsstandard für Drittanbieter)
- Status
- Ergebnis (einschließlich der Lösungsempfehlungen und der zu ergreifenden Maßnahmen)

3.6. Wenn ein Viertanbieter für die Erbringung der Dienste eingesetzt wird und dieser BT-Informationen speichert oder verarbeitet, muss der Drittanbieter vom BT Stakeholder genehmigen lassen, welche Informationen geteilt werden dürfen. Der Drittanbieter muss sicherstellen, dass er eine vertragliche Beziehung mit dem Viertanbieter hat und dass der Viertanbieter über einen Sicherheitsrahmen nach Industriestandard verfügt.

4. Änderungsmanagement

4.1. Der Drittanbieter muss sicherstellen, dass alle IT-Änderungen vor der Implementierung genehmigt, protokolliert und getestet werden, einschließlich der Rücknahme fehlgeschlagener Änderungen, um eine Unterbrechung des Dienstes oder Sicherheitsverletzungen zu verhindern. Der Drittanbieter muss ebenfalls sicherstellen, dass es einen Prozess für die kontrollierte Durchführung von Notfall-Updates gibt.

4.2. Der Drittanbieter muss sicherstellen, dass die Änderungen in den Produktions- und DR-Umgebungen berücksichtigt werden.

4.3. Der Drittanbieter muss BT unverzüglich über alle wesentlichen Änderungen des Dienstes (wie z. B. Änderungen der Zugangsmethode durch die Firewalls, einschließlich der Bereitstellung der Netzwerkadressübersetzung) informieren.

4.4. Der Drittanbieter muss sicherstellen, dass die Wartung und Reparatur von Vermögenswerten des Unternehmens mit genehmigten und kontrollierten Werkzeugen durchgeführt und protokolliert wird.

4.5. Der Drittanbieter muss sicherstellen, dass die Fernwartung von Vermögenswerten des Unternehmens genehmigt, protokolliert und so durchgeführt wird, dass ein unbefugter Zugriff verhindert wird.

5. Cyber-Risiko- und Bedrohungsmanagement

5.1. Der Drittanbieter muss sicherstellen, dass es einen fortlaufenden Rahmen für die Bewertung von Risiken und Bedrohungen der Cybersicherheit gibt, um sicherzustellen, dass das Risikoprofil der Cybersicherheit für den Betrieb, die Vermögenswerte, die Räumlichkeiten und die Personen des Unternehmens verstanden und verwaltet wird:

- Bewertung der Vermögensschwachstellen
- Identifizierung von internen und externen Bedrohungen
- Sensibilität der Informationen/Daten im Geltungsbereich
- Abschätzung der potenziellen geschäftlichen Auswirkungen
- Werden Bedrohungen, Schwachstellen, Wahrscheinlichkeiten und Auswirkungen zur Bestimmung des Risikos herangezogen?
- Sicherstellen, dass der Rahmen für das Management von Cyberrisiken und -bedrohungen auf einer geeigneten Ebene im Unternehmen vereinbart wird.

5.2. Der Drittanbieter muss sicherstellen, dass alle Risiken und Bedrohungen, die im Rahmen der Bewertung der Risiken und Bedrohungen der Cybersicherheit identifiziert wurden, nach Priorität geordnet und entsprechende Maßnahmen ergriffen werden, um die Risiken in einem geeigneten Zeitrahmen zu mindern.

5.3. Der Drittanbieter muss dem BT Stakeholder mitteilen, wenn er nicht in der Lage ist, wesentliche Risikobereiche, die sich auf die zu erbringende Dienste auswirken könnten, zu beheben oder zu reduzieren.

6. Identitätsmanagement und Zugangskontrolle

6.1 Der Drittanbieter muss über einen etablierten und konsistenten Rahmen verfügen, um sicherzustellen, dass Identitäten und Berechtigungen von autorisierten Mitarbeitern sicher verwaltet werden:

- Gewährung, erneutes Aktivieren, Ändern und Deaktivieren von Zugriffsrechten nur auf Grundlage dokumentierter und autorisierter Genehmigungen.
- Sicherstellen, dass unbenutzte Konten deaktiviert werden.
- Deaktivieren der Konten von Mitarbeitern, die nicht mehr beim Unternehmen tätig sind.
- Regelmäßige Überprüfungen der Zugangsrechte, um sicherzustellen, dass die Zugangsrechte zweckmäßig sind.
- Nutzerkonten werden mindestens einmal im Jahr und privilegierte Konten vierteljährlich rezertifiziert.

6.2 Der Drittanbieter muss sicherstellen, dass der Fernzugriff so verwaltet wird, dass nur zugelassene Personen eine Fernverbindung zu den Systemen des Drittanbieters herstellen können, und dass die Verbindungen sicher sind und Datenverluste verhindert werden und dass eine angemessene Zugangskontrolle, wie z. B. eine Multi-Faktor-Authentifizierung, vorhanden ist.

Eine Zwei-Faktor-Authentifizierung sollte mit einer Nutzer-ID, einem Passwort und einer der folgenden Methoden erreicht werden:

- Ein Einmal-Passwortgenerator, der eine nutzerspezifische PIN/ein nutzerspezifisches Passwort benötigt, um das Einmal-Passwort anzuzeigen.
- Eine Smartcard mit einem ISO 7816-konformen Chip und dem dazugehörigen Kartenleser und der dazugehörigen Software. Kontaktlose Chipkarten sind nicht erlaubt.
- Zertifikatsbasierte Authentisierung, die in Übereinstimmung mit Ihrer eigenen Informationssicherheitsrichtline für Zertifikate ausgestellt wurde.

Um Zweifel zu vermeiden, wenn ein privilegierter Zugang für den Support über Fernzugriff gewährt wird, muss dieser über eine sichere Verbindung erfolgen und eine 2-Faktor-Authentifizierung verwenden.

6.3 Der Drittanbieter muss sicherstellen, dass die Zugriffsrechte und -berechtigungen für alle Systeme (einschließlich Tools, Anwendungen, Datenbanken, Betriebssysteme, Hardware usw.) nach den Grundsätzen der geringsten Privilegien und der Aufgabentrennung verwaltet werden.

6.4 Der Drittanbieter muss sicherstellen, dass jede Transaktion auf eine einzige, eindeutig identifizierbare Person zurückgeführt werden kann und, falls Benutzerkonten von mehreren Personen verwendet werden, dass es angemessene zusätzliche Sicherheitsmaßnahmen gibt (einschließlich „Break Glass Procedure“).

6.5 Der Drittanbieter muss sicherstellen, dass Authentifizierungen entsprechend dem Risiko der Transaktion gesteuert werden, d. h. angemessene Passwortlänge und -komplexität, Häufigkeit von Passwortänderungen, Multi-Faktor-Authentifizierung, sichere Verwaltung der Passwortzugangsdaten oder andere Sicherheitsmaßnahmen.

6.6 Es müssen angemessene Sicherheitsmaßnahmen vorhanden sein, um mit fehlgeschlagenen Authentifizierungen umzugehen, einschließlich Bildschirmbenachrichtigungen, Protokollierung von Fehlern und Nutzersperrung.

6.7 Es müssen Prozesse und Sicherheitsmaßnahmen vorhanden sein, um Gäste- und Servicekonten zu verwalten und zu autorisieren.

7. Verwaltung von Informationsgut

7.1. Der Drittanbieter muss über ein Bestandsverzeichnis des Informationsguts verfügen (das gegebenenfalls auch alle BT-Geräte in den Räumlichkeiten des Drittanbieters umfasst) und sicherstellen, dass jährlich mindestens ein Test durchgeführt wird, um die Aktualität, Vollständigkeit und Richtigkeit des Bestandsverzeichnisses des Informationsguts zu überprüfen.

7.2. Der Drittanbieter muss sicherstellen, dass in dem Bestandsverzeichnis des Informationsguts die folgenden Komponenten inventarisiert oder katalogisiert sind:

- Physikalische Geräte und Systeme, Software-Plattformen und Anwendungen, externe Informationssysteme.
- Ressourcen (z. B. Hardware, Geräte, Daten, Zeit und Software) werden auf der Grundlage ihrer Klassifizierung, ihrer Kritikalität und ihres Geschäftswerts priorisiert.
- Unternehmens- und Kommunikationsdatenflüsse, einschließlich externer/Drittanbieter-Flüsse.
- Manuelle Prozesse, die mit Daten von BT oder Daten von Kunden von BT umgehen.

8. Zugriff auf BT-Systeme

8.1 Der Drittanbieter soll sich an die betreffenden Anweisungen halten, die ihm hinsichtlich des Zugriffs auf und der Nutzung von BT-Systemen mitgeteilt wurden.

8.2 Der Drittanbieter ist dafür verantwortlich, BT innerhalb von 24 Stunden zu informieren, wenn ein Mitarbeiter des Drittanbieters keinen Zugang mehr benötigt.

8.3 Der Drittanbieter stellt sicher, dass Nutzeridentifikation, Passwörter, PINs, Token und Konferenzzugang für einzelne Mitarbeiter des Drittanbieters bestimmt sind und nicht gemeinsam genutzt werden. Zugangsdaten müssen sicher und getrennt von dem Gerät, das für den Zugriff verwendet wird, aufbewahrt werden. Wenn ein Passwort einer anderen Person bekannt ist, muss es sofort geändert werden.

System-zu-System-Konnektivität

8.4 Inter-Domain-Linking zu BT-Systemen ist nicht zulässig, es sei denn, es wurde ausdrücklich von BT genehmigt und autorisiert.

8.5 Der Drittanbieter muss alle angemessenen Anstrengungen unternehmen, um sicherzustellen, dass keine Viren oder bösartige Programme (so wie das in der Computerindustrie allgemein verstanden wird) in BT Systeme eingeführt werden.

8.6 Besteht eine Verbindung zwischen den Systemen des Drittanbieters und den Systemen von BT, so erfolgt die Verbindung über sichere Verbindungen, die durch Verschlüsselung gemäß den Sicherheitsmaßnahmen im **Abschnitt 11 Kryptographie** geschützt sind.

8.7 Der Drittanbieter stellt sicher, dass die verwendeten Systeme und die Infrastruktur in ein dediziertes logisches Netzwerk eingebunden sind. Dieses Netzwerk darf nur aus den Systemen bestehen, die für die Bereitstellung einer sicheren Kundendatenverarbeitungsmöglichkeit bestimmt sind.

9. Physische Sicherheit in den Räumlichkeiten von Drittanbietern

9.1 Der Drittanbieter muss über ein Verfahren für den physischen Zugang verfügen, das die Zugangsmethoden und -berechtigungen zu den Räumlichkeiten des Drittanbieters (Standorte, Gebäude oder interne Bereiche) umfasst, in denen Dienstleistungen erbracht werden oder in denen BT-Informationen gespeichert oder verarbeitet werden. Die Zugriffsmethode sollte einen oder mehrere der folgenden Punkte umfassen:

- Ein autorisierter Ausweis des Drittanbieters mit Foto, das ein eindeutiges und ein wahres Abbild der Person darstellt.
- Eine autorisierte elektronische Zugangskarte für den Zutritt zu den entsprechenden Bereichen der Räumlichkeiten.
- Einen Sicherheitszugang über ein Tastenfeld, der über Verfahren verfügen muss für die Autorisierung, die Verbreitung von Codeänderungen (die mindestens monatlich erfolgen müssen) und Ad-hoc-Codeänderungen.
- Biometrischer Erkennung

9.2 Der Drittanbieter muss über Prozesse und Verfahren zur Kontrolle und Überwachung von Besuchern und anderen externen Personen einschließlich Drittanbietern verfügen mit physischem Zugang zu Sicherheitsbereichen oder zum Zweck der Wartung im Rahmen der Umgebungskontrolle, der Wartung von Alarmsystemen und Reinigungsmitteln.

9.3 Sichere Bereiche in Räumlichkeiten von Drittanbietern, die für die Bereitstellung des Dienstes genutzt werden (z. B. Netzwerkkommunikationsräume), sind von allgemeinen Zugangsbereichen zu trennen und durch geeignete Zugangskontrollen zu schützen, um sicherzustellen, dass nur autorisierten Personen der Zugang gestattet wird. Der Zugang zu diesen Bereichen muss regelmäßig überprüft werden und es muss mindestens jährlich eine Bewertung der Wiedererteilung der Zugangsrechte zu diesen Bereichen durchgeführt werden.

9.4 Der Drittanbieter muss über Videoüberwachungssysteme an den Orten verfügen, an denen BT-Informationen gespeichert oder verarbeitet werden.

9.5 Die Aufzeichnungen der Videoüberwachung müssen mindestens 20 Tage lang aufbewahrt werden. Dieser Zeitraum kann jedoch in den folgenden Situationen verlängert werden:

- wenn CCTV-Videobeweise für einen Vorfall oder eine strafrechtliche Untersuchung aufbewahrt werden müssen; oder
- wenn dies als notwendige Voraussetzung für die Einhaltung der Gesetzgebung angegeben ist.

9.6 Alle Videoaufzeichnungen und Aufnahmegeräte müssen sicher verwahrt werden, um eine Änderung, Löschung oder das „beiläufige“ Betrachten der zugehörigen Bildschirme zu verhindern. Der Zugang zu den Aufzeichnungen muss kontrolliert und auf autorisierte Personen beschränkt werden.

9.7 Der Drittanbieter muss geeignete Maßnahmen zur Gewährleistung der physischen Sicherheit in Bezug auf folgende Punkte getroffen haben:

- Maßnahmen zur Brandverhütung, unter anderem Alarm-, Erkennungs- und Unterdrückungseinrichtungen.
- Klimatische Bedingungen unter Berücksichtigung von Temperatur, Feuchtigkeit und statischer Elektrizität und das damit verbundene Management, die Überwachung und die Reaktion auf extreme Bedingungen (wie z. B. automatische Abschaltung, Alarme).
- Kontrollausrüstung wie Klimaanlagen und Wassererkennung.
- Verhinderung von Wasserschäden, Lage der Wassertanks, Leitungen usw. innerhalb des Geländes.

9.8 Der Drittanbieter muss sicherstellen, dass der physische Zugang zu den Bereichen, in denen BT-Information untergebracht sind, mit Smart- oder Proximity-Karten (oder gleichwertigen oder besseren Sicherheitssystemen) erfolgt. Und der Drittanbieter muss monatliche Kontrollen durchführen, um sicherzustellen, dass nur relevante Personen diesen Zugang erhalten.

9.9 Der Drittanbieter muss sicherstellen, dass das Fotografieren und/oder die Bildaufnahme von BT-Informationen verboten ist. Wenn eine geschäftliche Notwendigkeit besteht, solche Bilder zu erfassen, muss eine schriftliche Bestätigung des BT Stakeholders eingeholt werden.

Bereitstellung einer Hosting-Umgebung für BT-Geräte.

9.10 Der Drittanbieter muss, wenn der Drittanbieter in seinen Räumlichkeiten einen sicheren Zugangsbereich für das Hosting von Geräten von BT oder das Hosting von Geräten von Kunden von BT zur Verfügung stellt:

- BT einen Grundriss des zugewiesenen Platzes im gesicherten Bereich der Räumlichkeiten zur Verfügung stellen.
- Sicherstellen, dass die Schränke von BT und BT-Kunden in den Räumlichkeiten verschlossen bleiben und nur von autorisierten BT-Mitarbeitern, zugelassenen BT-Vertretern und relevanten Mitarbeitern von Drittanbietern zugänglich sind.
- Einen sicheren Schlüsselverwaltungsprozess implementieren.

9.11 BT muss dem Drittanbieter Folgendes zur Verfügung stellen:

- Ein Verzeichnis der physischen Vermögenswerte von BT und/oder der Kunden von BT, die sich in den Räumlichkeiten des Drittanbieters befinden.
- Einzelheiten zu den Mitarbeitern, Subunternehmern und Agenten von BT, die Zugang zu den Räumlichkeiten des Drittanbieters benötigen (kontinuierlich aktualisiert).

10. Datenklassifizierung und Datenschutz

10.1 Der Drittanbieter muss über ein etabliertes und konsistentes Rahmenwerk/Schema für die Klassifizierung und Handhabung von Daten/Informationen verfügen (ausgerichtet an der Good Industry Practice/den Anforderungen von BT), das die folgenden Komponenten enthält:

- Richtlinien zum Umgang mit Informationen.
- Die Informationen werden entsprechend dem zugewiesenen Geheimhaltungsgrad geschützt.
- Es muss sichergestellt werden, dass sich alle Mitarbeiter bewusst sind, dass die BT-Informationen nicht für andere Zwecke als den, für den sie bereitgestellt wurden, verwendet werden dürfen.
- Die Informationen von BT sollten nach dem Datenklassifizierungs- und Datenverarbeitungsstandard für Drittanbieter behandelt werden.

11. Kryptographie

11.1 Der Drittanbieter muss sicherstellen, dass, wenn das Risikoniveau eine Verschlüsselung erfordert, solche Daten angemessen verschlüsselt werden (während der Übertragung und im Ruhezustand) und wenn kryptographische Schlüssel verwendet werden, dass diese so entworfen und implementiert werden, dass sie die Sicherheitsanforderungen des NIST-Standards FIPS 140-2 auf Stufe 2 oder höher erfüllen.

11.2 Kryptographische Schlüssel müssen die folgenden Mindestlängen erfüllen oder überschreiten:

- Symmetrische Schlüssel (z. B. AES) müssen eine Schlüssellänge von mindestens 256 Bit haben.
- Asymmetrische Schlüssel (z. B. RSA) müssen eine Schlüssellänge von mindestens 2048 Bit haben.
- Elliptische Kurvenschlüssel müssen eine Schlüssellänge von mindestens 224 Bit haben.

11.3 Wenn das NIST bekannt gibt, dass ein Kryptoalgorithmus nicht mehr sicher ist, darf er nicht für neue Einsätze verwendet werden. Bestehende Implementierungen müssen die weitere Verwendung veralteter Kryptoalgorithmen überprüfen und einen Migrationsplan vorlegen, um von veralteten Kryptoalgorithmen zu etwas Sichererem überzugehen.

11.4 Für die symmetrische Verschlüsselung sind die folgenden Algorithmen nicht zulässig: 3DES-168 (sofern nicht durch einen internationalen Standard vorgeschrieben), 3DES-112, Blowfish, Twofish, RC4, IDEA, Camellia, Seed und ARIA.

11.5 Salted Hashes müssen verwendet werden, um die Daten im Speicher, d. h. die Passwörter, zu schützen. Hashing kann auch zur Anonymisierung von Daten vor der Verarbeitung verwendet werden, z. B. MSISDNs oder Zahlungen. Die folgenden Hashing-Algorithmen sind nicht zulässig: MD2, MD4, MD5 und SHA-1.

11.6 Schlüsselverwaltung - Erstellung und Inbetriebnahme

- Sitzungsschlüssel und Nonces müssen mit einem sicheren Pseudo-Zufallszahlengenerator erstellt werden. Dies muss mit mindestens so vielen Bits Entropie, wie die Anzahl der effektiven Sicherheitsbits, die der Algorithmus, der den Schlüssel verwendet, bietet.
- Es ist verboten, einen kürzeren Schlüssel von 64 Bits zu verwenden und auf nicht kryptographische Weise mit demselben Schlüssel von 64 Bits zu kombinieren, um 128 Bits zu erhalten.
- Alle Bits des Schlüssels müssen von dem Algorithmus verwendet werden.
- Auffüllungen oder andere vom Algorithmus verwendete Bits zählen nicht zur Schlüssellänge

11.7 Schlüsselverwaltung - Zufälligkeit

- Bei der Erzeugung von Sitzungsschlüsseln zur Verwendung in den symmetrischen Teilen der hybriden Kryptographie oder zur Erzeugung von Salts oder Initialisierungsvektoren muss eine robuste Quelle von Zufallsdaten verwendet werden.
- Pseudo-Zufallszahlengeneratoren (PRNG) können verwendet werden, aber um als sicher zu gelten, darf ein PRNG einem Angreifer nicht ermöglichen, Folgendes zu tun:
  - die zukünftige Leistung des Generators zu erraten, wenn die vorherige Leistung bekannt ist
  - die vorherigen Zustände des Generators bei Kenntnis des aktuellen Zustands errechnen
  - die Ausgabe des PRNG von echter Zufälligkeit unterscheiden. (Die Verwendung von Rand() ist nicht erlaubt.

11.8 Schlüsselverwaltung - Schlüsselaustausch

- Sitzungsschlüssel, die zur Verwendung mit einem symmetrischen Algorithmus generiert werden, müssen mit einem sicheren Schlüsselaustauschprotokoll ausgetauscht werden.

11.9 Schlüsselverwaltung - Schlüsselspeicherung

- Wenn Schlüssel zum Schutz von Data at Rest verwendet werden, muss der Datenverschlüsselungs-Schlüssel (DEK) mit einem Schlüssel-Verschlüsselungs-Schlüssel (KEK) geschützt werden, der auf einem separaten Server oder in einem Trusted Platform Module (TPM) gespeichert werden muss.
- Wenn der KEK auf einem separaten Server gespeichert ist, muss er während der Übertragung zu dem Server, der die Daten beherbergt, geschützt werden.

11.10 Schlüsselverwaltung - Schlüsselrotation (Regeneration)

- Es muss möglich sein, während des Schlüssel-Lebenszyklus den Schlüssel entsprechend Industry Best Practices zu erneuern.
- Es muss möglich sein, die zu schützenden Daten mit dem regenerierten Schlüssel erneut zu verschlüsseln.
- Es muss möglich sein, eine Ad-hoc-Neugenerierung des Schlüssels und eine erneute Verschlüsselung der Daten durchzuführen, wenn der Verdacht besteht, dass der ursprüngliche Verschlüsselungsschlüssel kompromittiert wurde.
- Bei AES GCM darf die Wahrscheinlichkeit, dass die authentifizierte Verschlüsselungsfunktion jemals mit derselben IV und demselben Schlüssel bei zwei (oder mehr) unterschiedlichen Eingabedatensätzen aufgerufen wird, nicht größer als 232 sein

11.11 Schlüsselverwaltung - Hardware-Sicherheitsmodule (HSMs)

- Kryptographische Schlüssel müssen mit Hilfe von Chipkarten auf ein HSM geladen werden.
- Chipkarten müssen eine PIN benötigen, um den Zugang zu ermöglichen.
- Die PINs müssen in Übereinstimmung mit der Zugangskontrollpolitik gewählt werden.
- Die PINs und Chipkarten müssen in einem Safe aufbewahrt werden, der von Ihrem eigenen Informationssicherheits-Team überprüft wurde.
- Es darf nicht möglich sein, kryptographische Schlüssel aus einem HSM zu extrahieren.
- HSMs müssen die in ihnen gespeicherten kryptographischen Schlüssel zerstören, wenn versucht wird, das Gehäuse zu öffnen.
- Bei HSMs, die hochsensible Schlüssel enthalten, dürfen die PINs und Smart Cards, die zu ihrem Schutz verwendet werden, nur von Mitarbeitern des technischen Sicherheitspersonals konfiguriert und gespeichert werden.
- Wenn der HSM zum Schutz hochsensibler Daten eingesetzt werden soll, muss für Änderungen am HSM ein Mindestquorum von 2 Chipkarten und den dazugehörigen PINs erforderlich sein. Die Mitglieder des Quorums müssen auf der Ebene der erweiterten Überprüfung sicherheitsüberprüft werden.

11.12 Digitale Zertifikate

- Zertifikate müssen das Certificate Revocation List Distribution Point (CDP) Attributset haben.
- Zur Bestimmung des Zertifikatsstatus muss das Online Certificate Status Protocol (OCSP) oder die Zertifikatsperrliste (CRL) verwendet werden.
- Zertifikatseigentümer müssen die Gültigkeit und den Ablauf der Zertifikate, die sie besitzen, überwachen, um sicherzustellen, dass erwartete Ablaufereignisse keinen Systemausfall verursachen.
- Zertifikatskonsumenten (Kunden) müssen die Gültigkeit und den Ablauf der verwendeten Zertifikate überwachen, um sicherzustellen, dass erwartete Ablaufereignisse keinen Systemausfall verursachen.

- Die Gültigkeitsdauer des Zertifikats muss entsprechend dem Zweck des Zertifikats gewählt werden.
- Die Gültigkeitsdauer des Zertifikats muss vor der Ausstellung festgelegt werden.
- Verwendung der Standard-Identität (Client, Server) 1024 nicht erlaubt

11.13 Data in Transit (Daten während der Übertragung)

- Die Verschlüsselung von Data in Transit wird in der Regel durch Transport oder Payload Encryption (Message oder Selective Field) erreicht. Zu den Transportverschlüsselungsmechanismen gehören unter anderem
- Transport Layer Security (TLS)
- Secure Tunnelling (IPSec)
- Secure Shell (SSH)
- Für die Transportverschlüsselung muss die symmetrische Komponente mit Abschnitt 12.14 dieses Standards im Einklang stehen.
- Transportsicherheitsprotokolle müssen so konfiguriert werden, dass die Aushandlung schwächerer Algorithmen und/oder kürzerer Schlüssellängen verhindert wird, wenn beide Endpunkte die stärkere Option unterstützen.
- Das SSL-Protokoll darf nicht verwendet werden, da es mehrere bekannte Schwachstellen gibt, die auf dieses Protokoll gerichtet sind.
- Die Initialisierungsvektoren für Stromchiffrierungen und AES im CBC-Modus dürfen nicht vorhersehbar sein.
- Die IV/Nonce im AES GCM muss die folgende „Eindeutigkeits“-Anforderung erfüllen:
  - Die Einhaltung dieser Anforderung ist entscheidend für die Sicherheit des GCM
  - Transportsicherheitsprotokolle müssen so konfiguriert werden (z. B. durch Verwendung von Richtungsbits), dass bekannte Klartext-Angriffe durch bekannte Nachrichten verhindert werden, die z. B. zurückgesendet werden „nichts zu berichten“.
  - Bei der Einrichtung des Transports muss eine gegenseitige Identitätsprüfung durchgeführt werden.
  - Bei sensiblen Daten kurzer Länge, die eine Verschlüsselung der Nutzlast erfordern (Verschlüsselungsschlüssel, Passwörter, Zahlungskarteninformationen), asymmetrische Verschlüsselung unter Verwendung mindestens der in diesem Dokument beschriebenen Mindestschlüssellängen und Algorithmen.
  - Systemverwaltungsdaten müssen bei der Übertragung verschlüsselt werden.
  - Die folgenden TLS-Optionen sind nicht zulässig: TLS v1.0, TLS v1.2, v6.0, TLS v6.1 und SSL (alle Versionen)
  - Die folgenden SSH (SFTP)-Optionen sind nicht zulässig: SSH v1
  - Die folgenden IPSec-Optionen sind nicht zulässig: IKE Version 1

11.14 Data at Rest (Daten im Ruhezustand)

- Zu den Data at Rest gehören Daten, die in Dateien, Datenbanken, temporären und Auslagerungsspeichern und auf jedem beliebigen Gerät gespeichert sind, unter anderem auf PCs, Laptops und anderen tragbaren Geräte, Servern, Bändern, SANs, USB, CDs, DVDs, Disketten und anderen Wechselspeicherlösungen.
- Daten, die als vertraulich oder höher definiert sind und im nichtflüchtigen Speicher eines beliebigen Geräts gespeichert werden, müssen verschlüsselt werden.
- Zahlungskarteninformationen, die auf einem beliebigen Gerät im nichtflüchtigen Speicher gespeichert sind, müssen verschlüsselt werden.
- Wenn symmetrische Schlüsseldaten durch einen asymmetrischen Schlüssel geschützt gespeichert werden, muss der asymmetrische Schlüssel, gemessen an den Sicherheitsbits, die gleiche Stärke wie der symmetrische Schlüssel selbst aufweisen.

- Die Systemdokumentation muss die Datenklassifizierung und die vom System gespeicherten Datenmengen darlegen.
- Die zur Entschlüsselung verwendeten Schlüssel dürfen nicht zusammen mit den zu entschlüsselnden Daten gespeichert oder gesichert werden. Die Software muss vor dem Einsatz in Produktionssystemen vollständig getestet werden.

12. Verhinderung von Datenlecks

12.1 Der Drittanbieter muss über einen etablierten und konsistenten Rahmen verfügen, um sicherzustellen, dass ein Schutz gegen unangemessene Datenlecks besteht, wobei der Schutz auch (aber nicht nur) die folgenden Vektoren umfasst:

- E-Mail
- Internet / Web-Gateway (einschließlich Online-Speicher und Webmail)
- USB, optische und andere Formen von Anschlüssen / tragbare Speichergeräte usw.
- Mobile Computing und BYOD
- Remote Access Services
- Mechanismen zur gemeinsamen Nutzung von Dateien und sozialen Medien

Bitte beachten: Wechseldatenträger/tragbare Geräte sollten standardmäßig deaktiviert und nur aus legitimen geschäftlichen Gründen aktiviert werden. Alle Daten, die auf Wechselmedien oder tragbaren Geräten gespeichert sind, müssen entsprechend dem Risiko verschlüsselt werden. Nicht autorisierte Geräte dürfen nicht an das Netzwerk angeschlossen werden (weder an das Unternehmensnetzwerk des Verkäufers noch an die Systeme/das Netzwerk von BT) oder für den Zugriff auf nicht-öffentliche Informationen verwendet werden. Nähere Informationen zur Handhabung von Wechselmedien finden Sie im Datenklassifizierungs- und Datenverarbeitungsstandard für Drittanbieter

13. PCI DSS

13.1 Der Drittanbieter muss sicherstellen, dass der Drittanbieter, wenn er im Bereich der Zahlungskartendaten tätig ist, den PCI DSS Standard in angemessener Weise erfüllt.

14. Cloud / Online-Computing.

14.1. Der Drittanbieter muss nach der neuesten Version von ISO27017 zertifiziert sein oder über ein etabliertes und konsistentes Rahmenwerk verfügen, um sicherzustellen, dass die gesamte Nutzung der Cloud-Technologie und der in der Cloud gespeicherten nicht-öffentlichen Daten genehmigt ist und angemessenen Sicherheitsmaßnahmen unterliegt, die der neuesten Version der Cloud Security Alliance, Cloud Controls Matrix (CCM) entspricht.

14.2. Netz- und Infrastruktur-Service-Level-Vereinbarungen (intern oder extern) müssen die Sicherheitsmaßnahmen, die Kapazitäten und Service-Level sowie die Geschäfts- oder Kundenanforderungen klar dokumentieren.

14.3. Der Drittanbieter muss Sicherheitsmaßnahmen in allen Aspekten des zu erbringenden Dienstes umsetzen, so dass die Vertraulichkeit, Verfügbarkeit, Qualität und Integrität gewährleistet sind, indem die Möglichkeit, dass unbefugte Personen (z. B. andere Cloud-Kunden) Zugang zu BT-Informationen und den von BT genutzten Diensten erhalten, minimiert wird.

15. Soziale Medien

15.1. Der Drittanbieter muss über ein etabliertes und konsistentes Regelwerk für die akzeptable Nutzung von privaten und geschäftlichen sozialen Medien verfügen. Die folgenden Themen müssen abgedeckt werden:

- Sicherstellen, dass das Personal nichts Verleumderisches, Obszönes oder Beleidigendes über das Unternehmen, seine Kunden oder Auftraggeber veröffentlicht
- Verwendung von Unternehmens- oder Kundenlogos ohne vorherige Genehmigung
- Offenlegung nicht-öffentlicher Informationen von Unternehmen oder Kunden ohne vorherige Zustimmung
- Veröffentlichung von Meinungen über das Unternehmen, seine Kunden oder Auftraggeber, die vernünftigerweise als offizielle Stellungnahme des Unternehmens oder seiner Auftraggeber ausgelegt werden könnten
- BT-Informationen, die als „vertraulich“ oder „streng vertraulich“ gekennzeichnet sind, dürfen nicht veröffentlicht werden

16. Systemkonfiguration

16.1. Der Drittanbieter muss über ein etabliertes und konsistentes Regelwerk verfügen, um sicherzustellen, dass die Systeme angemessen konfiguriert sind (sowohl Systeme von Drittanbietern als auch Systeme, die BT zur Verfügung gestellt werden). Dies betrifft die folgenden Komponenten:

- Systeme und Netzwerkgeräte werden so konfiguriert, dass sie im Einklang mit den Sicherheitsprinzipien funktionieren (z. B. Konzept der geringsten Funktionalität und keine unautorisierte Software)
- Sicherstellen, dass die Geräte die korrekte und konsistente Zeit nutzen
- Die Systeme sind frei von bösartiger Software
- Es gibt geeignete Tests und Überwachungen, um die Integrität der Bauwerke/Geräte zu gewährleisten.

17. Sichere Software-Entwicklung

17.1. Der Drittanbieter muss sicherstellen, dass Produktions- und Nicht-Produktionsumgebungen angemessen gesichert sind, indem er dafür sorgt, dass die folgenden Komponenten vorhanden sind:

- Trennung von Produktions- und Nichtproduktionsumgebungen und Aufgabentrennung
- Es werden ohne die vorherige Zustimmung des Dateneigentümers im Test keine Live-Daten verwendet, und es werden dort dieselben Sicherheitsmaßnahmen eingesetzt, die auch in der Produktionsumgebung eingesetzt werden.
- Aufgabentrennung zwischen Produktions- und Nicht-Produktionsentwicklung

17.2. Der Drittanbieter muss über ein etabliertes und konsistentes Rahmenwerk für die Systementwicklung verfügen, um Sicherheitslücken und Cyber-Sicherheitsverletzungen zu verhindern. Dieses Rahmenwerk muss die folgenden Komponenten enthalten:

- Die Systeme werden in Übereinstimmung mit der den bewährten Methoden für sichere Entwicklung (z. B. OWASP) entwickelt.
- Der Code wird sicher gespeichert und unterliegt der Qualitätssicherung.
- Der Code ist vor unbefugten Änderungen angemessen geschützt, sobald die Testphase

abgeschlossen ist.

17.3. Wenn zum Schutz aller Parteien eine Escrow-Schema erforderlich ist, muss der Drittanbieter entweder für Erstanbieter- oder Drittanbieter-Escrow (d. h. für geistiges Eigentum/Quellcode, usw.) ein konsistentes und etabliertes Rahmenwerk haben, das die folgenden Komponenten umfasst:

- Ausführung des Escrow-Vertrags mit einem unabhängigen, neutralen und seriösen Escrow-Agenten
- Lieferung und laufende Aktualisierung des Quellcodes und anderer Materialien an den Escrow-Agenten, um sicherzustellen, dass die erforderlichen Informationen auf dem neuesten Stand sind
- Sichere Lagerung von Quellcode und anderen Materialien, bis die Freigabebedingungen erfüllt sind
- Geeignete Freigabebedingungen
- Laufende Aktualisierungen, angemessene Zahlungen und Überprüfungen des Escrow-Vertrags

18. Anti-Malware-Schutz

18.1. Vulnerability Management muss sicherstellen, dass der aktuellste Malware-Schutz für alle anwendbaren IT-Ressourcen verwendet wird, um eine Unterbrechung der Dienste oder Sicherheitsverletzungen zu verhindern und sicherzustellen, dass geeignete Verfahren zur Sensibilisierung der Nutzer implementiert werden.

Bitte beachten: Anti-Malware zur Erkennung von (nicht nur) unautorisiertem mobilen Code, Viren, Spyware, Key-Logger-Software, Botnets, Würmern, Trojanern usw.

19. Vulnerability Management (Schwachstellen-Management)

19.1. Vulnerability Management muss über ein etabliertes und konsistentes Rahmenwerk für das Vulnerability Management verfügen, das die folgenden Komponenten umfasst:

- Prozessrichtlinien und -verfahren
- Definierte Rollen und Verantwortlichkeiten
- Geeignete Werkzeuge wie Intrusion Detection Systeme und Schwachstellen-Scansysteme.

19.2. Das Rahmenwerk für das Vulnerability Management des Drittanbieters muss, um potenzielle Cyber-Sicherheitsereignisse zu erkennen, sicherstellen, dass Folgendes routinemäßig überwacht wird,

- Wichtige Systeme und Anlagen
- Unerlaubte Verbindungen
- Unerlaubte Software/Anwendungen
- Netzwerk-Aktivität.

19.3. Das Vulnerability Management des Drittanbieters muss sicherstellen, dass:

- Es gibt Prozesse, die eingerichtet wurden, um Schwachstellen, die der Organisation aus internen und externen Quellen (z. B. interne Tests, Sicherheitsbulletins oder Sicherheitsforscher) bekannt werden, zu erhalten, zu analysieren und darauf zu reagieren.
- Nur autorisierte Werkzeuge, Technologien und Nutzer sind erlaubt.
- Identifizierte Schwachstellen werden geschlossen oder als akzeptierte Risiken dokumentiert.

19.4. Der Drittanbieter muss sicherstellen, dass die neuesten Sicherheitspatches rechtzeitig auf

Systeme/Anlagen/Netzwerke/Anwendungen angewendet werden, um zu gewährleisten, dass:

- der Drittanbieter Patches verwendet, die er von folgenden Anbietern direkt für proprietäre Systeme erhält und Patches, die entweder (i) digital signiert oder (ii) durch die Verwendung eines Anbieter-Hashes (MD5-Hashes dürfen nicht verwendet werden) für das Update-Paket verifiziert werden, so dass der Patch als von einer seriösen Support-Community für Open-Source-Software stammend identifiziert werden kann.
- der Drittanbieter alle Patches auf Systemen testet, die die Konfiguration der Ziel-Produktionssysteme exakt repräsentieren, bevor der Patch auf die Produktionssysteme verteilt wird, und dass die korrekte Funktion des gepatchten Dienstes nach jeder Patch-Aktivität überprüft wird.
- alle zutreffenden Anbieter und andere relevante Informationsquellen auf Schwachstellenwarnungen überprüft werden.
- Wenn ein System nicht gepatcht werden kann, sind geeignete Gegenmaßnahmen zu ergreifen.

19.5. Der Drittanbieter muss sicherstellen, dass mindestens einmal jährlich eine unabhängige IT-Sicherheitsbewertung/Penetrationsprüfung der IT-Infrastruktur und der Anwendungen des Drittanbieters, die für die Bereitstellung von Diensten verwendet werden, einschließlich der Disaster-Recovery-Standorte, in Auftrag gegeben wird, um Schwachstellen zu ermitteln, die zur Verletzung von Daten/Diensten ausgenutzt werden könnten, und um Sicherheitsverletzungen durch Cyber-Angriffe zu verhindern. Der Drittanbieter muss BT auf begründeten Antrag Zugriff auf für die angebotenen Dienste relevanten Penetrationstestberichte gewähren.

19.6. Der Drittanbieter muss sicherstellen, dass der Zugang zu den Diagnose- und Verwaltungsanschlüssen sowie zu den Diagnosewerkzeugen gesichert ist.

19.7. Der Drittanbieter muss sicherstellen, dass der Zugang zu den Audit-Tools auf die entsprechenden Mitarbeiter des Lieferanten beschränkt ist und ihre Verwendung überwacht wird.

19.8. Der Drittanbieter muss sicherstellen, dass alle Server, die für die Bereitstellung des Dienstes verwendet werden, nicht ohne angemessene Sicherheitsmaßnahmen in nicht vertrauenswürdigen Netzwerken (Netzwerke außerhalb des Sicherheitsbereichs, die sich der administrativen Kontrolle entziehen, z. B. mit Internetanschluss) eingesetzt werden.

20. Netzwerkintegrität

20.1. Der Drittanbieter muss sicherstellen, dass die Netzwerkintegrität hergestellt und aufrechterhalten wird, indem er dafür sorgt, dass die folgenden Komponenten angemessen implementiert werden:

- Externe Verbindungen zum Netzwerk werden dokumentiert, durch eine Firewall geleitet und vor dem Aufbau der Verbindungen verifiziert und genehmigt, um Datensicherheitsverletzungen zu verhindern.
- Das Netzwerk wird nach den Prinzipien der „Defense in Depth“ (Tiefenverteidigung) angemessen gestaltet, um sicherzustellen, dass Cyber-Sicherheitsverletzungen durch geeignete Sicherheitsmaßnahmen wie die „Netzwerksegmentierung“, die jeden gezielten Angriff verhindern, minimiert werden.
- Die Gestaltung und Umsetzung des Netzwerks werden mindestens jährlich überprüft.
- Jeder drahtlose Zugriff auf das Netzwerk unterliegt der Autorisierung, Authentifizierung, Segmentierung, und es werden Verschlüsselungsmechanismen eingesetzt, um Sicherheitsverletzungen zu verhindern.
- Verwendung sicherer Kommunikation zwischen den Geräten und Managementstationen.
- Sichere Kommunikation zwischen den Geräten, falls erforderlich; einschließlich der Verschlüsselung aller Administratorzugriffe (mit Ausnahme der Konsole);

- Verwendung eines starken Architekturdesigns, das in Schichten und Zonen mit effektiver Identitätsverwaltung und Betriebssystemkonfiguration unterteilt ist, die entsprechend gehärtet und dokumentiert werden müssen.
- durch die Deaktivierung (wo möglich) von Diensten, Anwendungen und Ports, die nicht genutzt werden.
- durch die Deaktivierung oder Entfernung von Gastkonten.
- durch die Vermeidung von Trust-Beziehungen zwischen Servern.
- durch die Anwendung des Best-Practice-Sicherheitsprinzips der „geringsten Privilegien“ zur Ausführung einer Funktion.
- durch die Gewährleistung geeigneter Maßnahmen zur Erkennung und/oder zum Schutz vor Eindringlingen.
- Gegebenenfalls Überwachung der Integrität von Dateien, um das Hinzufügen, Ändern oder Löschen von kritischen Systemdateien oder Daten zu erkennen.
- Änderung aller standardmäßig und vom Lieferanten gesetzten Passwörter, bevor die Netzwerkkomponenten in Betrieb genommen werden.

20.2. Das Netzwerk des Drittanbieters sollte alle gesetzlichen und regulatorischen Anforderungen erfüllen und

- sich nach besten Kräften bemühen, Unbefugten (z. B. Hackern) den Zugang zu dem/den Netzwerk(en) des Drittanbieters zu verwehren,
- sich nach besten Kräften bemühen, das Risiko eines Missbrauchs des/der Netzwerke(s) durch die zugangsberechtigten Personen zu verringern,
- sich nach besten Kräften bemühen, Sicherheitsverletzungen aufzudecken und eine rasche Behebung von Verstößen zu gewährleisten, dabei gleichzeitig die Personen identifizieren, die Zugang erhalten haben und bestimmen, wie sie den Zugang erhalten haben.

21. Minderung von Denial of Service

21.1. Der Drittanbieter muss sicherstellen, dass wichtige Systeme gegen Denial of Service (DoS)- und Distributed Denial of Service (DDoS)-Angriffe geschützt sind.

22. Sicherheit, kontinuierliche Protokollierung und Überwachung

22.1. Der Drittanbieter muss sicherstellen, dass es ein etabliertes und konsistentes Audit- und Log-Verwaltungssystem gibt, das gewährleistet, dass die wichtigen Systeme einschließlich der Anwendungen so eingestellt sind, dass sie wichtige Ereignisse (darunter auch solche mit privilegiertem Zugang und Personalaktivitäten) protokollieren. Diese Protokolle müssen mindestens 12 Monate lang aufbewahrt werden. Als Mindestanforderung muss der Drittanbieter sicherstellen, dass die Protokolle (soweit zutreffend) die folgenden Ereignisse enthalten:

- Start- und Stopppunkte des protokollierten Prozesses.
- Änderungen der Art der protokollierten Ereignisse entsprechend den Anforderungen der Prüfkette (z. B. die Startparameter und deren Änderungen).
- Systemstart und -abschaltung.
- Erfolgreiche Anmeldungen.

- Fehlgeschlagene Anmeldeversuche (z. B. falsche Nutzer-ID oder falsches Kennwort).
- Erstellen, Ändern und Löschen von Nutzerkonten.
- Auf welche Güter (z. B. Daten) greifen sie zu,
- Wo haben sie auf Güter zugegriffen (z. B. IP-Adresse),
- Wann (z. B. Zeitstempel).

22.2. Das Rahmenwerk für Audits und das Log-Management muss die folgenden Komponenten umfassen:

- Sicherstellen, dass die Protokolle der wichtigen Ereignisse mindestens monatlich von einer unabhängigen Funktion überprüft werden, um unbefugte Aktivitäten sowie Angriffsziele und -methoden aufzudecken.
- Vermerken von Ausnahmen und deren Untersuchung bis zur Lösung.
- Die Protokolle werden von mehreren Quellen und Sensoren gesammelt und korreliert und sicher und gegen Manipulationen geschützt gespeichert, um die Rekonstruktion solcher Ereignisse zu ermöglichen.
- Die Auswirkungen von Vorfällen werden anhand von Schwellenwerten für die Alarmierung bei Vorfällen ermittelt und es werden entsprechend der Kritikalität des Alarms rechtzeitig Maßnahmen ergriffen.

23. Schulung und Bewusstsein

23.1. Der Drittanbieter muss sicherstellen, dass alle seiner Kontrolle unterstehenden Mitarbeiter des Drittanbieters innerhalb eines Monats nach Eintritt in die Firma eine obligatorische Sicherheitsschulung zur Informationssicherheit absolvieren, die die bewährten Methoden der Cybersicherheit und den Schutz personenbezogener Daten umfasst und mindestens einmal im Jahr, gegebenenfalls auch in Form einer Auffrischung, durchgeführt wird:

- Privilegierte Nutzer
- Stakeholder des Drittanbieters (z. B. Subunternehmer, Kunden, Partner)
- Leitende Angestellte
- Physisches und Cyber-Sicherheitspersonal

23.2. Der Drittanbieter muss sicherstellen, dass es eine Testkomponente gibt, um zu überprüfen, ob der Nutzer die Schulung versteht und entsprechendes Bewusstsein hat.

24. Recht auf Überprüfung

24.1. Der Drittanbieter muss BT erlauben, eine Inspektion der Umgebung durchzuführen, in der die Dienstleistungen entwickelt, hergestellt oder bereitgestellt werden, um mindestens einmal jährlich (oder unmittelbar nach einem Zwischenfall) Prüfungen und/oder Bewertungen der Sicherheitskonformität durchzuführen.

24.2. Der Drittanbieter ist für die Kosten der Behebung der von BT festgestellten Sicherheitsschwächen innerhalb eines von beiden Parteien vereinbarten Zeitrahmens verantwortlich.

24.3. Im Falle eines schwerwiegenden Vorfalls arbeitet der Drittanbieter in vollem Umfang mit BT bei allen nachfolgenden Untersuchungen durch BT, eine Regulierungsbehörde und/oder eine Strafverfolgungsbehörde zusammen, indem er Zugang gewährt und Unterstützung leistet, soweit dies

für die Untersuchung des Vorfalls erforderlich und angemessen ist. BT muss möglicherweise verlangen, dass der Drittanbieters den Status/Stand aller relevanten Objekte, die dem Drittanbieter gehören, einfriert, um die Untersuchung zu unterstützen, und der Drittanbieter darf dieses Verlangen nicht unangemessen zurückweisen oder verzögern.

25. Physische Sicherheit - BT-Räumlichkeiten

25.1 Alle in BT-Räumlichkeiten arbeitenden Mitarbeiter von Drittanbietern müssen im Besitz eines von dem Drittanbieter oder BT zur Verfügung gestellten Ausweises sein und diesen an gut sichtbarer Stelle tragen. Der Ausweis muss ein Foto enthalten, das ein klares und wahrheitsgetreues Abbild des Mitarbeiters des Drittanbieters darstellt.

25.2 BT kann den Mitarbeitern eines Drittanbieters auch eine elektronische Zugangskarte und/oder eine zeitlich begrenzte Besucherkarte zur Verfügung stellen, die gemäß den örtlichen Verfahren verwendet werden müssen.

25.3 Nur zugelassene von BT eingerichtete Server, BT Webtop-PCs und vertrauenswürdige Endgeräte können eine direkte Verbindung (Anschluss an einen LAN-Port oder eine drahtlose Verbindung) zu BT-Domänen herstellen. Drittanbieter dürfen ohne vorherige schriftliche Genehmigung von BT keine Geräte, die nicht von BT genehmigt sind, an eine BT-Domain anschließen.

25.4 Der physische Schutz und die Richtlinien für die Arbeit in den Räumlichkeiten von BT müssen eingehalten werden, einschließlich, aber nicht beschränkt auf die Begleitung des Personals von Drittanbietern und die Einführung geeigneter Arbeitspraktiken in sicheren Bereichen.

25.5 Wenn ein Drittanbieter berechtigt ist, seinen Mitarbeitern ungehinderten Zugang zu Bereichen innerhalb der BT-Räumlichkeiten zu gewähren; müssen sich der Unterzeichnungsberechtigte des Drittanbieters und die Mitarbeiter des Drittanbieters an den Verpflichtenden Sicherheitsleitfaden – Zugang zu den BT-Standorten halten.

Zusätzlich müssen sich der Unterzeichnungsberechtigte des Drittanbieters und die Mitarbeiter des Drittanbieters Sicherheitsüberprüfungen unterziehen.

26. Netzwerksicherheit – eigenes Netzwerk von BT

26.1 Der Drittanbieter muss dem BT-Sicherheitskontakt die Namen, Adressen (und alle anderen Einzelheiten, die BT verlangt) aller einzelnen Mitarbeiter des Drittanbieters mitteilen, die von Zeit zu Zeit direkt an der Bereitstellung, Wartung und/oder Verwaltung der Dienstleistung beteiligt sind, bevor diese jeweils mit der Bereitstellung, Wartung und/oder Verwaltung beauftragt werden.

26.2 In Bezug auf seine Unterstützungsaktivitäten im Vereinigten Königreich betreibt der Drittanbieter ein qualifiziertes Sicherheitsteam, dem mindestens ein britischer Staatsangehörigen angehört, der für die Verbindung mit dem BT-Sicherheitskontakt (oder seinen Beauftragten) zur Verfügung steht. Das Team nimmt an den Sitzungen teil, die der BT-Sicherheitskontakt von Zeit zu Zeit vernünftigerweise verlangt.

26.3 Der Drittanbieter stellt dem BT-Sicherheitskontakt eine (bei Bedarf aktualisierten) Aufstellung aller aktiven Komponenten der Dienstleistung und/oder der Dienstleistungen und ihrer jeweiligen Quellen zur Verfügung.

26.4 Der Drittanbieter stellt Einzelheiten zu seinen einzelnen Mitarbeitern zur Verfügung, die mit dem Vulnerability Management Team von BT (CERT) in Bezug auf Diskussionen über BT und von Dritten identifizierte Schwachstellen der Dienstleistung und/oder der Dienstleistungen in Verbindung stehen. Der Drittanbieter stellt BT rechtzeitig Informationen über Schwachstellen zur Verfügung und erfüllt (auf Kosten des Drittanbieters) die angemessenen Anforderungen in Bezug auf Schwachstellen, die von Zeit zu Zeit vom BT-Sicherheitskontakt gemeldet werden. Der Drittanbieter informiert BT über

alle Schwachstellen so rechtzeitig, dass Abhilfen angewendet oder installiert werden können, bevor der Drittanbieter die Schwachstellen öffentlich bekannt gibt.

26.5 Der Drittanbieter stellt sicher, dass alle sicherheitsrelevanten Komponenten, die von Zeit zu Zeit von oder für BT identifiziert werden, auf Kosten des Drittanbieters extern zur angemessenen Zufriedenheit von BT bewertet werden.

26.6 Der Drittanbieter muss dem BT-Sicherheitskontakt unverzüglich, auf jeden Fall aber innerhalb von 7 Werktagen, alle Einzelheiten zu allen Merkmalen und/oder Funktionalitäten des Dienstes (oder der in der Roadmap für den jeweiligen Dienst geplanten), die von Zeit zu Zeit zur Verfügung gestellt werden, mitteilen:

- von denen der Drittanbieter weiß oder von denen
- die BT-Sicherheits-Kontaktperson vernünftigerweise davon ausgeht und den Drittanbieter darüber informiert, dass sie für die rechtmäßige Überwachung oder jede andere Art der Überwachung des Telekommunikationsverkehrs vorgesehen sind oder verwendet werden könnten. Diese Angaben umfassen alle Informationen, die vernünftigerweise erforderlich sind, damit die BT-Sicherheits-Kontaktperson die Art, Zusammensetzung und den Umfang dieser Merkmale und/oder Funktionen vollständig verstehen kann.

26.7 Um den Zugang zu den BT-Netzwerken und/oder -Systemen aufrechtzuerhalten, muss der Drittanbieter BT unverzüglich über alle Änderungen seiner Zugangsmethode durch die Firewalls informieren, einschließlich der Bereitstellung einer Netzwerkadressübersetzung.

26.8 Der Drittanbieter darf keine Netzwerküberwachungswerkzeuge verwenden, die Anwendungsinformationen anzeigen können.

26.9 Der Drittanbieter muss sicherstellen, dass die in den Betriebssystemen enthaltene IPv6-Funktionalität auf Hosts (z. B. Endnutzergeräte oder Server), die eine Verbindung zum BT-Netzwerk herstellen, deaktiviert wird und dass die Domänen deaktiviert werden sollten, wenn dies nicht erforderlich ist.

26.10 Das Personal des Drittanbieters, der BT-Netzwerke oder Netzwerk-Güter aufbaut, entwickelt oder unterstützt, muss sicherstellen, dass sich alle Mitarbeiter des Drittanbieters vor der Einstellung mindestens L2-Prüfungen unterziehen. L3-Prüfungen vor der Einstellung sind für die vom BT-Sicherheitskontakt festgelegten Aufgaben erforderlich. Wenn der Drittanbieter nicht in der Lage ist, die Mitarbeiter des Drittanbieters im Rahmen von L3-Kontrollen direkt zu überprüfen, hilft BT auf Kosten des Drittanbieters bei der Einholung der Freigabe.

26.11 Der Drittanbieter muss die Hardware und Software gemäß den Spezifikationen des Herstellers warten.

26.12 Der Drittanbieter darf keine Wechselmedien (Disketten, USB-Laufwerke usw.), die für Support und Wartung bestimmt sind, für andere Zwecke verwenden

27. Glossar

Begriff	Definition
2-Faktor-Authentifizierung	Manchmal auch als zweistufige Verifizierung oder Zwei-Faktor-Authentifizierung bezeichnet, ist ein Sicherheitsprozess, bei dem der Nutzer zwei verschiedene Authentifizierungsfaktoren zur Verfügung stellt, um sich selbst zu verifizieren und so sowohl die Anmeldedaten des Nutzers als auch die Ressourcen, auf die der Nutzer zugreifen kann, besser zu schützen.
Drittanbieter	Personen, die für uns arbeiten, aber keine Mitarbeiter von BT sind
AES	Advanced Encryption Standard (AES), ist eine Spezifikation für die Verschlüsselung von elektronischen Daten, die vom U.S. National Institute of Standards and Technology (NIST) im Jahr 2001 festgelegt wurde.
ASG	Application Support Group

BT Group	BT Group bezieht sich auf alle CFUs & CUs innerhalb der BT Group, unter anderem Openreach, EE und Plusnet – für die Zwecke dieses Dokuments werden sie, sofern nicht anders angegeben, als „BT“ bezeichnet.
BT Stakeholder	Der BT-Mitarbeiter, der die Verantwortung für die Arbeit trägt, die dem Drittanbieter übertragen wurde.
CCTV	Steht für Close Circuit Television (Videoüberwachung)
DBA	Datenbank-Administrator
DC	Rechenzentrum
Defence in Depth (Tiefenverteidigung)	Ist ein Ansatz zur Cybersicherheit, bei dem eine Reihe von Abwehrmechanismen überlagert werden, um wertvolle Daten und Informationen zu schützen. Wenn ein Mechanismus versagt, tritt sofort ein anderer Mechanismus in Kraft, um einen Angriff zu vereiteln.
DR	Disaster Recovery (Wiederherstellung im Katastrophenfall)
GCM	Der Galois/Counter-Modus ist eine Betriebsart für kryptographische Blockchiffrierungen mit symmetrischen Schlüsseln, die aufgrund ihrer Leistung weit verbreitet ist.
HDD	Festplattenlaufwerk
HMG	Her Majesty's Government – umfasst die Regierungsbehörden des Vereinigten Königreichs
ISMS	Informationssicherheits-Managementsystem. Ist ein Regelwerk von Richtlinien und Verfahren, das alle rechtlichen, physischen und technischen Kontrollen umfasst, die an den Informationsrisikomanagement-Prozessen eines Unternehmens beteiligt sind.
ISO 27001	Ist eine Industriestandardspezifikation für ein Informationssicherheits-Managementsystem (ISMS).
ISO 27017	Code of Practice für Informationssicherheitsmaßnahmen auf der Grundlage von ISO/IEC 27002 für Cloud-Dienste
ISO 7816	Ist eine internationale Norm für elektronische Identifikationskarten mit Kontakten, insbesondere Chipkarten, die gemeinsam von der International Organization for Standardisation (ISO) und der International Electrotechnical Commission(IEC) verwaltet wird.
NAS	Ein Einzelspeichergerät für Dateien.
NIST	Das National Institute of Standards and Technology ist ein physikalisch-wissenschaftliches Labor und eine nicht regulierende Behörde des United States Department of Commerce (Handelsministeriums der Vereinigten Staaten).
PCI DSS	Der Payment Card Industry Data Security Standard (PCI DSS) ist ein Informationssicherheitsstandard für Unternehmen, die mit Markenkreditkarten der großen Kartensysteme arbeiten.
Privilegierte Konten	Ein privilegierrte Nutzer ist ein Nutzer, der administrativen Zugriff auf kritische Systeme hat
RSA	(Rivest-Shamir-Adleman) ist eines der ersten Kryptosysteme mit öffentlichem Schlüssel und wird häufig für die sichere Datenübertragung verwendet.
SAN	Ein lokales Netzwerk mit mehreren Geräten, die mit Datenträgerblöcken arbeiten
SSD	Solid State Drive (Festkörperspeicher)

28.Änderungshistorie.

Versionsnr.	Datum	Änderung durch	Kurzbeschreibung der Änderung(en)
0.1	30.10.2017	Mark Tilston	Interner Entwurf für Mapping und zur Aktualisierung des Inhalts

Versionsnr.	Datum	Änderung durch	Kurzbeschreibung der Änderung(en)
0.2	10.04.2019	Tim Hunt	Auf neues Format übertragen
1.0	01.05.2019	Ian Morton	Zum Thema erhoben
1.1	01.10.2019	Karen Tanner	Zusätzliche Sicherheitsmaßnahmen als Teil der Erhöhung der BT-Sicherheitsanforderungen hinzugefügt

29. Dokument Genehmigung

Rolle	Datum
Mark Tilston	06.11.2019

30. Compliance

Wir schätzen es sehr, dass die meisten BT-Mitarbeiter professionell und in Übereinstimmung mit unseren Werten handeln. Sollten Sie sich jedoch auf eine Weise verhalten, die mit diesem Standard nicht vereinbar ist, kann BT gemäß den lokalen Gesetzen und Vorschriften entsprechende Disziplinarmaßnahmen ergreifen.

Wenn Sie sich in einer Weise verhalten, die nicht mit diesem Standard übereinstimmt, können wir die Vereinbarungen, die wir mit Ihnen für Ihre Dienste getroffen haben, beenden.

31. Hilfreiche Links und Informationen

Für BT-Mitarbeiter:

Über diesen Link können Sie alle Richtlinien und Standards von BT nachlesen .

Wir überprüfen unsere Richtlinien und Standards mindestens einmal jährlich. Unser Überprüfungsprogramm finden Sie hier.

Um einen „Security Incident“ (Sicherheitsvorfall) zu melden, wenden Sie sich bitte an: Security Control Centre.

Wenn Sie mehr Informationen oder Hilfe zu diesem Standard oder einer anderen Sicherheitsrichtlinie benötigen, wenden Sie sich an: security.policy@bt.com

Für Drittanbieter:

Über diesen Link können Sie alle relevanten Standards und Sicherheitsvorgaben einsehen.

32. Eigentum und Vertraulichkeit

Dieses Dokument darf ohne schriftliche Zustimmung von BT nicht an andere Dritte weitergegeben werden. Dieser Standard und alle damit verbundenen Unterlagen bleiben Eigentum von BT und müssen auf Wunsch zurückgegeben werden.

Dieses Dokument ist als „intern“ klassifiziert, wenn es jedoch von einem Drittanbieter heruntergeladen wird, muss es als „vertraulich“ behandelt werden.