Anhang 5 – Sicherheitsanforderungen für externes Hosting

Die vorliegenden Anforderungen gelten für das Hosting aller **„vertraulichen" (IC)** oder **„streng vertraulichen" (ISC)** Anwendungen und Daten von BT an einem Ort, der nicht BT gehört oder von BT verwaltet wird. Dazu gehören unter anderem, jedoch nicht ausschließlich Cloud-Dienste, bei denen a) die Daten bei der Übertragung sicher und davor geschützt sind, abgefangen zu werden, in der Regel durch den Einsatz eines verschlüsselten Protokolls, und b) die BT-Daten stationär innerhalb des Cloud-Dienstes verschlüsselt sind.

Die folgenden Bestimmungen gelten für vertrauliche Anwendungen und Daten, die außerhalb von BT gehostet werden:

- Das Rechenzentrum muss im Besitz einer gültigen ISO 27001-Zertifizierung (oder von Zertifizierungen, die gleichwertige Kontrollen belegen) für Sicherheitsmanagement sein oder die Sicherheitsanforderungen der ISO 27001-Zertifizierung oder Sicherheitsrichtlinien erfüllen, die sich an ISO 27001 orientieren und/oder innerhalb eines mit BT vereinbarten Zeitrahmens auf die ISO 27001 hinarbeiten;
- Daten müssen bei der Übertragung stark verschlüsselt werden, um die BT-Daten zwischen dem Ausgangspunkt bei BT und dem Grenzpunkt des Rechenzentrums (in der Regel der Lastverteiler und die Verschlüsselungsvorrichtung hinter der Firewall des Grenzpunkts des Rechenzentrums) zu schützen;
- Techniker des Rechenzentrums mit physischem Zugang zu den Servern dürfen keinen logischen Zugang zur Produktionsumgebung haben, und Administratoren mit logischem Zugang zu den Systemen dürfen keinen physischen Zugang zum Rechenzentrum haben.
- Die Gesamtheit des logischen Zugangs ist von einem Kontosicherheitssystem zu kontrollieren, um zu gewährleisten, dass die Verwaltung von Kennwörtern kontrolliert wird und dass ein geeigneter Autorisierungsprozess implementiert ist, um die Identität des Anfragenden zu gewährleisten, z. B. CyberArk.
- Für privilegierten Zugriff (unter anderem DBA) hat die Verwaltung von Kennwörtern zeitgebunden zu sein und nach Möglichkeit zusätzliche Beschränkungen für die Quell-IP-Adresse vorzusehen.
- Privilegierter Zugriff wie z. B. DBA, ASG usw. auf Systeme, die BT-Informationen verarbeiten, muss die Anforderungen in Anhang 1 erfüllen – Informationsklassifikation.
- Für Fernzugriff ist ein sicheres virtuelles privates Netzwerk in Verbindung mit rollenbasierter Zwei-Faktor-Authentifizierung zu verwenden; zusätzlich darf der Fernzugriff von Dritten mit privilegiertem Zugriff auf Systeme mit BT-Daten, die übertragen werden oder sich im Ruhezustand befinden, nur aus demselben Land wie dem des Rechenzentrums erfolgen oder aus einem Land oder Gebiet, das ein ausreichendes Maß an Schutz für die BT-Daten gewährleistet.
- Implementieren Sie den gesamten Lebenszyklus umspannende Chiffrierschlüssel-Verwaltungsprozesse, die bewährter Branchenpraxis angemessen sind.
- Für physischen Zugang zu Bereichen oder Anlagen, in bzw. auf denen BT-Informationen gespeichert oder verarbeitet werden, muss ein überprüfbarer Prozess vorhanden sein, z. B. Änderungsanfrage, um zu gewährleisten, dass der Zugang nur für die erforderliche Mindestdauer gewährt wird, d. h. kein Dauerzugang.
- Externe Sicherungsdatenspeicher müssen gemäß den Anforderungen von Anhang 1 verschlüsselt sein;

- Es müssen Kontrollen vorhanden sein, um nicht autorisierten Zugriff zu entschärfen, zu erkennen und zu verhindern. Kontrollen müssen ein Protokoll unter Verwendung des Grundsatzes „Wer-Was-Wo-Wann" generieren.
- Wer der Benutzer war, z. B. Benutzerkonto-ID;
- Worauf zugegriffen wurde, z. B. Daten;
- Von wo zugegriffen wurde, z. B. IP-Adresse; und
- Wann, z. B. Zeitstempel.
- Jeder physische und logische Zugriff muss protokolliert werden, wobei die Protokolldateien für (mindestens) ein Jahr aufzubewahren sind;
- Für den Fall eines Sicherheitsereignisses, bei dem BT-Daten gefährdet, gestohlen oder geändert werden, muss ein Prozess vorhanden sein, um zu gewährleisten, dass BT innerhalb einer zumutbaren Frist mit einem ausreichenden Maß an Einzelheiten benachrichtigt wird.

Im Fall von ISC-Informationen gilt zusätzlich Folgendes:

- Das Rechenzentrum muss eine Sicherheitsüberprüfung vor Ort bestehen.
- Anwendungsserver, Datenbanken usw. sollten sich auf dedizierter, nicht von mehreren Mietern genutzter Infrastruktur befinden und in einem speziellen Rack innerhalb eines Sicherheitskäfigs untergebracht sein. Kann diese Anforderung nicht erfüllt werden, muss durch eine BT-Risikobewertung der Nachweis erbracht werden, dass eine ausreichende Trennung der BT-Daten von den Daten anderer Kunden in derselben Umgebung gegeben ist, um zu gewährleisten, dass DBAs keinen Anmeldezugriff auf Kundeninstanzen haben und keine Kundendaten in zusammengesetzter Form sehen. Datenbanktabellen und -zeilen, dürfen nicht die Ansicht einer einzelnen Kundeninstanz widerspiegeln.
- Es müssen Prozesse vorhanden sein, um zu gewährleisten, dass ISC-Daten am Ende ihres Lebenszyklus in der Cloud sicher gelöscht werden. Alle Speichervorrichtungen, die ISC-Daten enthalten, müssen wie in Anhang 1 erläutert bereinigt/gelöscht werden.