Kontrollpflichten externer Lieferanten

Physische Sicherheit (technische Kontrollen)

Version 12.0, Oktober 2022

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
1. Zugangskontrolle (TC 5.1)	In allen Geschäftsräumen, in denen Aktivitäten in Verbindung mit Barclays-Verträgen vorgenommen werden, muss eine elektronische, mechanische oder digitale Zugriffssteuerung eingerichtet und verwaltet werden. Alle Sicherheitssysteme müssen gemäß den gesetzlichen und aufsichtsrechtlichen Bestimmungen installiert, betrieben und gewartet werden. Der logische und administrative Zugriff auf elektronische Zutrittskontrollsysteme muss auf autorisiertes Personal beschränkt werden, und der Zugriff auf physische Schlüssel und Kombinationen muss streng verwaltet und kontrolliert werden. Es muss ein Audit-Trail mit Inhabern von Anmeldeinformationen/Schlüssel/Kombinationen geführt werden, der die Erteilung, Änderung und Aufhebung von Zugriffsberechtigungen umfasst. Alle Zugangsdaten müssen effektiv verwaltet werden, um das Risiko eines unbefugten Zugriff zu verringern. Zugangsdaten müssen in Übereinstimmung mit den Zugriffssteuerungsverfahren des Lieferanten verwaltet werden. Zugangsdaten können nur nach Eingang der entsprechenden Genehmigung ausgefertigt werden. Jeder Zugang zu Bereichen mit Zugangsbeschränkung muss in angemessenen Abständen erneut zertifiziert werden. Wenn der Zugang zu einem Gelände oder einem eingeschränkten Bereich nicht mehr erforderlich ist, muss die für die Verwaltung der Zugangsdaten zuständige Funktion die Zugangsdaten innerhalb von 24 Stunden nach Erhalt der Benachrichtigung der jeweiligen Geschäftseinheit oder Funktion über die Änderung der Anforderungen für den betreffenden Mitarbeiter (z. B. Wechsel der Rolle oder der	Die Aufrechterhaltung eines effektiven Zutrittskontrollsystems und der Prozesse und Verfahren für das Zugriffsmanagement ist eine wichtige Komponente innerhalb der mehrschichtigen Kombination von Kontrollen, die erforderlich sind, um das Gelände vor unbefugtem Zugriff zu schützen und die Sicherheit von Ressourcen zu gewährleisten. Sind keine effektiven Maßnahmen zur Zugriffssteuerung vorhanden, besteht das Risiko, dass unbefugte Personen in die Standorte oder in Bereiche mit Zugangsbeschränkungen an den Standorten des Lieferanten gelangen. Dies kann das Risiko für Verluste von oder Schäden an Ressourcen von Barclays erhöhen, woraus sich wiederum finanzielle Einbußen und damit verbundenen Rufschädigungen bzw. Konventionalstrafen oder Zensur ergeben.

	Verantwortlichkeiten oder Kündigung des Beschäftigungsverhältnisses) deaktivieren. Wenn Arbeiten außerhalb des Unternehmens erforderlich sind, bei denen der Lieferant oder seine Unterauftragnehmer auf vertrauliche Informationen von Barclays in physischer oder virtueller Form zugreifen, diese speichern oder verarbeiten (einschließlich personenbezogener oder sensibler Daten, die dem Lieferanten nach Wissensbedarf zur Verfügung gestellt werden), muss der Lieferant die Modalitäten mit Barclays abstimmen, bevor er den Zugriff auf diese Daten gestattet.	
2. Einbruchserkennungssysteme und Überwachungskameras (TC 5.2)	Einbruchserkennungssysteme (Intruder Detection Systems, IDS) und Überwachungskameras müssen installiert werden, um unbefugte Zugänge oder kriminelle Aktivitäten zu verhindern, festzustellen, zu überwachen und zu erkennen. Die Ausrüstung muss im Verhältnis zu den vorherrschenden physischen Sicherheitsbedrohungen installiert werden, die im Rahmen der Sicherheitsrisikobewertung am jeweiligen Standort festgestellt wurden. Alle Kamerasysteme und IDS müssen gemäß den aktuellen Industriestandards (z. B. International Organization for Standardization (ISO), System and Organization Control (SOC), den geltenden gesetzlichen und behördlichen Anforderungen sowie den aktuellen Herstellerspezifikationen) installiert, betrieben und gewartet werden. Es müssen Verfahren vorhanden sein, um sicherzustellen, dass die Alarme von IDS- und Überwachungskameras effektiv überwacht und verwaltet werden. Der Zugriff auf das System muss auf autorisierte Mitarbeiter beschränkt werden.	IDS und Kamerasysteme sind Teil der mehrstufigen Kontrollverfahren, die nötig sind, um Geschäftsräume vor unbefugtem Zugang zu schützen und die Sicherheit der Ressourcen zu gewährleisten. Werden diese System nicht ordnungsgemäß installiert, betrieben und gewartet, besteht das Risiko, dass Unbefugte Zutritt zu Standorten und Gebäuden erlangen, in denen sich Ressourcen und Daten von Barclays befinden, und dieser unbefugte Zutritt nicht zeitnah erkannt wird.
3. Rechenzentren, Hallen und Kommunikationsinstallationen (TC 5,3)	Alle eigenständigen Rechenzentren, Cloud-Anbieter, Datenzentren und Kommunikationseinrichtungen (einschließlich Serverräume und eigenständige Kommunikationsschränke) müssen wirksam	Damit sollen die in Datenzentren, Rechenzentren und an ähnlichen kritischen Standorten aufbewahrten Ressourcen bzw. Daten von Barclays vor dem Risiko von Verlusten, Schäden oder Diebstahl

	gesichert werden, um unbefugten Zugriff und Diebstahl oder Beschädigung von Barclays-Ressourcen oder -Daten zu verhindern. Alle Datenzentren müssen über mehrstufige technische, physische und personengeführte Kontrolleinrichtungen sowie standortspezifische Verfahren verfügen, um das Gelände, das Gebäude und die Integrität der Rechenzentren und aller anderen kritischen Bereiche wirksam zu schützen. Zu diesen Kontrolleinrichtungen zählen unter anderem Überwachungskameras, Einbruchserkennungssysteme, Zugangskontrollen und Sicherheitsbeauftragte. Wenn sich Installationen an gemeinsam genutzten Standorten befinden, muss eine wirksame Sicherheit um ihre diskrete Trennung herum eingerichtet werden.	infolge des unbefugten Zugangs zu Bereichen mit Zugangsbeschränkungen geschützt werden.

Dieser Standard muss in Verbindung mit dem folgenden Standard gelesen werden, in dem die als innerhalb des Geltungsbereichs liegenden identifizierten Managementkontrollen angewendet werden müssen:

Kontrollpflicht für Drittanbieter (TPSPCO), Managementkontrollanforderungen – Informationen, Cyber- und physische Sicherheit, Technologie, Wiederherstellungsplanung, Datenschutz, Datenmanagement, PCI DSS und EUDA.