BARCLAYS

Kontrollpflichten externer Lieferanten

Physische Sicherheit

Version 10.0, Oktober 2020

Bezeichnung der Kontrolle	Beschreibung der Kontrolle	Über die Bedeutung
1. Sicherheitsrisikobewertungen	Der Lieferant sorgt für die Durchführung von Sicherheitsrisikobewertungen, um physische Sicherheitsmaßnahmen und -prozesse zu überprüfen. Diese Bewertungen sind von einer hinreichend erfahrenen oder qualifizierten Person durchzuführen, wobei es die Relevanz und Effektivität physischer Sicherheitskontrollen zu berücksichtigen gilt, um sowohl das aktuelle Gefährdungsprofil des Gebäudes als auch eventuell drohende Probleme zu mindern, die sich auf den Standort auswirken könnten. Die Häufigkeit der Risikobewertungsmaßnahme muss Zweck und Kritikalität des Standorts entsprechen. Es wird erwartet, dass die für den Betrieb von Barclays-Prozessen kritischen Standorte (einschließlich Datenzentren) mindestens einmal jährlich bewertet werden. Die Ergebnisse der Sicherheitsrisikobewertung müssen dokumentiert, Maßnahmenpläne müssen erstellt und die festgestellten Probleme/Risiken müssen einem Verantwortlichen zugewiesen und bis zu ihrer Behebung überwacht werden. Barclays ist innerhalb von 10 Werktagen nach ihrer Feststellung über alle signifikanten Ergebnisse zu informieren.	Sicherheitsrisikobewertungen sind eine wesentliche Voraussetzung, um eine genaue Bewertung der physischen Sicherheitsumgebung, Kontrollen und Prozesse des Lieferanten sowie ihrer aktuellen Wirksamkeit zu gewährleisten. Dadurch werden neue oder vorhandene Schwachpunkte und Sicherheitslücken erkannt und die Gefahr von Verlusten oder Schäden an Ressourcen von Barclays sowie einer damit verbundenen Rufschädigung bzw. Konventionalstrafe oder Zensur vermindert.
2. Zugriffssteuerung	In allen Geschäftsräumen, in denen Aktivitäten in Verbindung mit Barclays-Verträgen vorgenommen werden, ist eine elektronische, mechanische oder digitale Zugriffssteuerung einzurichten und zu verwalten. Alle Sicherheitssysteme müssen gemäß den gesetzlichen und aufsichtsrechtlichen	Eine effektive Zugriffssteuerung ist Teil der mehrstufigen Kontrollverfahren, die nötig sind, um Geschäftsräume vor unbefugtem Zugang zu schützen und die Sicherheit der Ressourcen zu gewährleisten. Sind keine effektiven Maßnahmen zur Zugriffssteuerung vorhanden, besteht das Risiko, dass unbefugte

	Bestimmungen installiert, betrieben und gewartet werden. Der Zugriff auf das System muss auf autorisierte Mitarbeiter beschränkt und der Zugang zu Schlüsseln und Kombinationen muss streng organisiert und kontrolliert werden. 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 werden nach Eingang der entsprechenden Genehmigung ausgefertigt. Jeder Zugang zu Bereichen mit Zugangsbeschränkung muss in angemessenen Abständen rezertifiziert werden. Ist der Zugang zu einem Geschäftsraum oder einem Bereich mit Zugangsbeschränkung nicht mehr erforderlich, müssen die Zugangsdaten innerhalb von 24 Stunden nach entsprechender Benachrichtigung deaktiviert werden.	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.
3. Einbruchserkennungssysteme und Überwachungskameras	Einbruchserkennungssysteme (Intruder Detection Systems, IDS) und Überwachungskameras sind zu installieren, 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 geltenden Branchenstandards installiert, betrieben und gewartet 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.

4. Sicherheitspersonal	Sicherheitspersonal muss im Verhältnis zu den vorherrschenden physischen Sicherheitsbedrohungen am jeweiligen Standort engagiert werden. Alle Sicherheitsmitarbeiter (ob beim Lieferanten, einem Vermieter oder einem externen Anbieter beschäftigt) müssen entsprechend den örtlichen Gesetzen über einen akkreditierten, lizenzierten Dienstleister engagiert bzw. beauftragt werden. Die Mitarbeiter müssen eine Sicherheitsschulung absolvieren, die auf ihre Funktion und ihre Verantwortlichkeiten zugeschnitten ist. Alle durchgeführten Schulungen sind zu dokumentieren und für alle Sicherheitsmitarbeiter muss ein Schulungsprotokoll geführt werden.	Das Sicherheitspersonal ist Teil der mehrstufigen Kontrollverfahren, die nötig sind, um Geschäftsräume vor unbefugtem Zugang zu schützen und die Sicherheit der Ressourcen zu gewährleisten. Wird entsprechend den vorherrschenden Sicherheitsbedrohungen kein Sicherheitspersonal engagiert und ordnungsgemäß geschult, besteht das Risiko, dass Unbefugte Zutritt zu Standorten erlangen, an denen sich Ressourcen und Daten von Barclays befinden, oder dass dies nicht zeitnah erkannt wird. 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.
5. Management von Sicherheitszwischenfällen und Reaktionsstufen	Der Lieferant hält ein Verfahrenskonzept für das Management von Sicherheitszwischenfällen bereit und führt gegebenenfalls Untersuchungen durch. Sofern Ressourcen von Barclays betroffen sind, muss der Zwischenfall Barclays innerhalb von 48 Stunden gemeldet sowie formelle Berichte und Einzelheiten der Untersuchung schnellstmöglich, jedoch nicht später als 10 Werktage nach dem Zwischenfall, an Barclays übermittelt werden. Dazu zählen, soweit zutreffend und im Einklang mit den örtlichen Gesetzen und Vorschriften, Zugriffssteuerungsdaten und Aufzeichnungen von Überwachungskameras.	Andernfalls kann Barclays nicht darauf vertrauen, dass der Lieferant über ordnungsgemäß dokumentierte, geprüfte Verfahren für das Management von Sicherheitszwischenfällen verfügt. Dies kann dazu führen, dass nach einem Zwischenfall unangemessene Maßnahmen getroffen werden, was die Gefahr von Verlusten oder Schäden an Ressourcen bzw. Daten von Barclays sowie einer damit verbundenen Rufschädigung bzw. Konventionalstrafe/Zensur erhöht.
6. Transport	Die Lieferanten stellen sicher, dass sämtliche Ressourcen und Daten von Barclays sicher transportiert und angemessene Kontrollen durchgeführt werden, die im Verhältnis zum Wert der zu befördernden Ressourcen und Daten (in Hinblick auf sowohl finanzielle Verluste als auch Rufschädigungen) sowie zur Bedrohungsumgebung stehen, in die sie transportiert werden.	Damit sollen die zwischen Lieferanten und/oder Standorten von Barclays übermittelten Ressourcen bzw. Daten von Barclays geschützt werden, um die Gefahr von Verlusten, Diebstahl oder Schäden sowie einer damit verbundenen Rufschädigung bzw. Konventionalstrafe/Zensur zu mindern.

7. Daten- und Rechenzentren	Alle eigenständigen, zusammengelegten und externen Datenzentren, Cloud-Anbieter und Rechenzentren werden wirksam gesichert, um unbefugten Zugang und Diebstahl von oder Schäden an den Ressourcen bzw. Daten von Barclays 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 wirksam zu schützen. Zu diesen Kontrolleinrichtungen zählen unter anderem Überwachungskameras, Einbruchserkennungssysteme und Zugangskontrollen.	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 infolge des unbefugten Zugangs zu Bereichen mit Zugangsbeschränkungen geschützt werden.