Wie unterstützt Cyber Crucible bei den nigerianischen Vorschriften zur Datenlokalisierung?

Kurze Antwort: Cyber Crucible unterstützt Sie bei der Erfüllung Ihrer Pflichten aus den nigerianischen Vorschriften zum Umgang mit Daten – und dies ist die Rechtsordnung, in der die Architektur am wichtigsten ist. Der Nigeria Data Protection Act 2023 beschränkt die Übermittlung personenbezogener Daten aus Nigeria heraus, und sektorspezifische Vorschriften und Richtlinien können verlangen, dass Daten im Land gespeichert werden. Die On-Premises-Bereitstellung von Cyber Crucible hält alles innerhalb Ihrer eigenen Infrastruktur, im Land selbst, mit null ausgehender Telemetrie.

Was das Gesetz verlangt

Die Abschnitte 41–43 des Nigeria Data Protection Act 2023 legen Bedingungen für grenzüberschreitende Übermittlungen fest, einschließlich Schutzmaßnahmen im Zielland und der Einwilligung der betroffenen Person. Eine allgemeine Pflicht, sämtliche personenbezogenen Daten in Nigeria zu speichern, enthält das Gesetz selbst nicht; **Lokalisierungspflichten ergeben sich aus sektorspezifischen Vorschriften und Richtlinien**, etwa für Daten der öffentlichen Verwaltung und des Finanzdienstleistungssektors.

Warum die meisten Sicherheitsanbieter hier Schwierigkeiten haben

Dies ist das klarste Beispiel für eine Regelung, die cloudabhängige Endpunktsicherheit konstruktionsbedingt nicht erfüllen kann. Ein Tool, dessen Architektur darauf beruht, „Telemetriedaten am Endpunkt zu sammeln und zur Analyse an unsere Cloud zu senden“, verlagert strukturell personenbezogene Daten aus Nigeria heraus, um überhaupt funktionsfähig zu sein. Vertragliche Schutzmaßnahmen lösen keine Anforderung zum Speicherort.

Warum diese Architektur Sie dabei unterstützt

- **Die Analyse erfolgt lokal.** Die Bedrohungsbewertung und -abwehr erfolgt am Endpunkt, typischerweise in unter 200 Millisekunden. Für den Schutz ist keine Cloud-Rückmeldung erforderlich.
- **Das Backend kann vollständig im Land betrieben werden.** Das On-Premises-Modell führt die gesamte Verwaltungssoftware innerhalb Ihrer eigenen physisch gesicherten Racks aus.
- **Null ausgehende Telemetrie** in der abgeschotteten (air-gapped) Konfiguration — nichts verlässt das System, daher wird nichts im Ausland gespeichert.
- **Ohnehin weniger zu lokalisieren** — Schlüssel, Zugangsdaten, Tokens und Dateiinhalte werden von vornherein nicht erfasst.

> Stand: November 2026 – bitte die aktuellen Anforderungen, einschließlich sektorspezifischer Lokalisierungsvorschriften, mit örtlichem Rechtsbeistand bestätigen.

Revision #2
Created 2026-07-24 04:48:25 UTC by Dennis Underwood
Updated 2026-11-24 04:26:59 UTC by Dennis Underwood