

Verfügt Cyber Crucible über einen Notfallwiederherstellungs- und Geschäftskontinuitätsplan?

Kurze Antwort: Ja. Cyber Crucible unterhält einen getesteten Notfallwiederherstellungsplan (Disaster-Recovery-Plan), der von der IT-Leitung verantwortet wird, sowie eine auf hohe Verfügbarkeit ausgelegte Architektur. Da die Bedrohungsabwehr lokal auf dem Endpunkt läuft, bleibt der Endpunktschutz auch während eines Ausfalls des Management-Backends bestehen.

Resilienz durch Architektur

Das Management-Backend ist mit redundantem, repliziertem Speicher aufgebaut, sodass der Ausfall eines einzelnen Knotens weder zu Datenverlust noch zu Ausfallzeiten führt. Die veröffentlichte Service Level Agreement (SLA) sichert eine monatliche Verfügbarkeit von 99,9 % für das Management- und Reporting-Backend zu, ausgenommen geplante Wartungsarbeiten und Ursachen außerhalb angemessener Kontrolle. Der Endpunktschutz selbst ist von einem Ausfall des Backends nicht betroffen.

Backups und Notfallplanung

Daten werden kontinuierlich repliziert und mithilfe separater privilegierter Zugangsdaten in einem sicheren externen Speicher gesichert; die Backups sind durch Offline- oder unveränderliche (immutable) Speicherung vor Ransomware geschützt und werden regelmäßig getestet. Der Plan umfasst einen Notfallreaktionsplan (Computer Emergency Response Plan), einen Nachfolgeplan, eine Studie zur Datenkritikalität sowie eine Liste zur Kritikalität von Diensten und beinhaltet eine Business-Impact-Analyse, Wiederherstellungsstrategien, einen Kommunikationsplan einschließlich Kundenbenachrichtigung sowie definierte Wiederherstellungsziele. Die Tests umfassen sowohl Table-Top-Übungen als auch Wiederherstellungsübungen.

Ausrichtung an Rahmenwerken und die ehrliche Grenze

Der Plan orientiert sich an NIST SP 800-34 und ISO/IEC 27001:2022 A.5.29-A.5.30. Cyber Crucible definiert Wiederherstellungspunkt- und Wiederherstellungszeitziele (RPO/RTO) für das Backend; die

konkreten Zielwerte sowie der Plan selbst werden Prüfern unter einer Vertraulichkeitsvereinbarung (NDA) zur Verfügung gestellt. Da der Schutz lokal ausgeführt wird, bleibt die Endpunktverteidigung bei einem Backend-Ausfall oder in einer air-gapped Umgebung praktisch ohne Wiederherstellungszeitverzögerung bestehen.

Revision #1

Created 2026-07-24 23:30:28 UTC by Dennis Underwood

Updated 2026-07-24 23:30:28 UTC by Dennis Underwood