

Welches Compliance-Risiko entsteht durch die Hinterlegung von Verschlüsselungsschlüsseln (Key Escrow), und warum verzichtet Cyber Crucible darauf?

Kurze Antwort: Die zentrale Speicherung von Verschlüsselungsschlüsseln schafft einen Single Point of Failure, ein hochwertiges Angriffsziel und eine Angriffsfläche für erzwungene Offenlegung. Der Präventionsansatz von Cyber Crucible ist nicht darauf angewiesen, Schlüssel zu erfassen oder zu hinterlegen, sodass es keinen zentralen Schlüsselspeicher gibt, der abgesichert, per Vorladung angefordert oder kompromittiert werden könnte.

“ Die direkte produktbezogene Antwort finden Sie im bestehenden Artikel **„Sammelt Cyber Crucible Verschlüsselungsschlüssel?“** Diese Seite behandelt die Compliance- und Datensouveränitätsüberlegungen hinter dieser Antwort.

Warum dies bewusst so gestaltet ist

Cyber Crucible hat ursprünglich eine Technologie zur Schlüsselerfassung zur Ransomware-Abwehr entwickelt und patentiert. Bis 2021 hatten sich Ransomware-Varianten jedoch so weiterentwickelt, dass sie diese aushebeln konnten – durch den Einsatz benutzerdefinierter Verschlüsselungsbibliotheken, einzigartiger Implementierungen pro Ausführung und Streaming-Chiffren, die gegen Schlüsselerfassung immun sind. Wir haben diese Kryptoanalyse 2021 öffentlich auf der BSides Pittsburgh vorgestellt.

Das Risiko, das wir bewusst nicht eingegangen sind

Abgesehen davon, dass sie nicht mehr funktioniert, erfordert die Schlüsselerfassung eine zentrale Speicherung von Verschlüsselungsschlüsseln. Dies führt zu einem Single Point of Failure, einem hochwertigen Angriffsziel und der Möglichkeit einer erzwungenen Offenlegung ohne Wissen des Kunden.

Die Verhinderung des Angriffs, bevor die Verschlüsselung beginnt, macht Schlüssel vollständig überflüssig – was sowohl eine stärkere Verteidigung als auch eine geringere Compliance-Angriffsfläche bedeutet.

Revision #1

Created 2026-07-24 04:38:17 UTC by Dennis Underwood

Updated 2026-07-24 04:38:17 UTC by Dennis Underwood