

Compliance & Risiko

Wie sich autonome, geräteinterne Prävention auf regulatorische Verpflichtungen, Verstoßmeldungen, Datensouveränität, Cyberversicherungen und die Risikoberichterstattung auf Vorstandsebene auswirkt.

- [Sammelt Cyber Crucible Verschlüsselungsschlüssel?](#)
- [Müssen wir eine Sicherheitsverletzung trotzdem melden, wenn ein Angriff verhindert wurde?](#)
- [Wie unterstützt Cyber Crucible die HIPAA-Konformität im Gesundheitswesen?](#)
- [Wie unterstützt Cyber Crucible FERPA und den Datenschutz von Schülerdaten?](#)
- [Was bedeutet Datensouveränität für Cyber-Crucible-Implementierungen?](#)
- [Welches Compliance-Risiko entsteht durch die Hinterlegung von Verschlüsselungsschlüsseln \(Key Escrow\), und warum verzichtet Cyber Crucible darauf?](#)
- [Wie wirkt sich autonome Prävention auf Cyberversicherungen und die Berichterstattung an das Board aus?](#)

Sammelt Cyber Crucible Verschlüsselungsschlüssel?

Die kürzeste Antwort lautet: „Nein.“

Es gab eine Zeit, in der die Cyber Crucible Software die Ransomware-Verschlüsselung nicht vor der Verschlüsselung stoppte. Stattdessen wurden mögliche Verschlüsselungsschlüssel oder Einstellungen gesammelt und anschließend eine Vielzahl von Techniken eingesetzt, um nach einem Ransomware-Angriff das passende Entschlüsselungspaket (einschließlich der Schlüssel) zur Entschlüsselung zu ermitteln.

Aus der Sicht dessen, was wir gesammelt haben, könnte man dies mit einer Videokamera vergleichen, die Aufnahmen von allem macht, was möglicherweise ein Schlüssel zu einem Schließfach sein könnte. Anschließend würde ein Server die verschiedenen mathematischen Berechnungen durchführen, um den passenden Schlüssel und die passenden Einstellungen für die jeweilige Datei zu bestimmen. Informatiker würden dies als maschinelles Lernen bezeichnen.

Bevor wir uns von dem alten Softwaremodell „samme alles, was ein Schlüssel sein könnte“ verabschiedeten, organisierten wir bei Angriffen automatisch Tausende von Schlüsseln und Verschlüsselungseinstellungen pro Rechner.

Das kryptografische Analysemodul der Software hat sich mittlerweile zu einem zusätzlichen verhaltensbasierten Analysemodul weiterentwickelt, das als eine der Datenquellen dient, um festzustellen, ob Software versucht, unrechtmäßig auf Identitätsdaten oder „Daten-Daten“ zuzugreifen, um diese zu stehlen oder zu verschlüsseln.

Müssen wir eine Sicherheitsverletzung trotzdem melden, wenn ein Angriff verhindert wurde?

Kurze Antwort: In der Regel nein. Wenn ein Angriff gestoppt wird, bevor er ausgeführt werden kann, und keine Daten abgerufen, verändert oder exfiltriert wurden, liegt üblicherweise keine meldepflichtige Sicherheitsverletzung vor. Meldepflichten werden in der Regel durch unbefugten Zugriff auf geschützte Daten ausgelöst — nicht durch einen fehlgeschlagenen Versuch.

Ein reales Beispiel

Bei der Implementierung im Finanzdienstleistungssektor, bei der Cyber Crucible fast 10.000 bösartige Prozesse abgefangen hat, musste der CISO keinerlei behördliche Meldung vornehmen. Da die Angriffe vor der Ausführung gestoppt wurden und keine Daten betroffen waren, gab es keine erforderlichen Benachrichtigungen an Kunden, Anbieter oder staatliche Aufsichtsbehörden — und keine Schlagzeilen, wodurch das Vertrauen der Kunden erhalten blieb.

Ein wichtiger Vorbehalt

Meldepflichten variieren je nach Rechtsraum, Branche und Vertrag, und die konkreten Umstände eines Vorfalls sind entscheidend. Cyber Crucible ist keine Anwaltskanzlei, und dies stellt keine Rechtsberatung dar. Der verlässliche Grundsatz lautet, dass Prävention Ihr Meldungsrisiko im Vergleich zu nachträglicher Erkennung erheblich verringert — die endgültige Einschätzung für ein bestimmtes Ereignis sollten jedoch Ihr Rechtsbeistand und Ihr Compliance-Team vornehmen.

Wie unterstützt Cyber Crucible die HIPAA-Konformität im Gesundheitswesen?

Kurze Antwort: Die gesamte Analyse erfolgt lokal auf Kernel-Ebene, sodass geschützte Gesundheitsdaten für die Sicherheitsverarbeitung niemals den Endpunkt verlassen. Damit wird das HIPAA-Risiko vermieden, das durch Sicherheitstools entsteht, die sensible Dateien oder Schlüssel in Drittanbieter-Clouds hochladen, und Angriffe werden gestoppt, ohne klinische Systeme offline zu nehmen.

Das Problem mit anbietergehosteter Sicherheit

Viele anbietergehostete SOC- und MDR-Vereinbarungen erfordern das Hochladen sensibler Schlüssel, Dateien oder Telemetriedaten in Cloud-Datenbanken von Drittanbietern. Für eine dem Gesetz unterliegende Einrichtung (Covered Entity) entsteht dadurch ein reales Compliance-Risiko, und die Anzahl der Parteien, die geschützte Daten verarbeiten, wird erweitert.

Lokale Analyse, lokale Daten

Cyber Crucible führt die Analyse am Endpunkt durch. Sensible Assets verlassen niemals die sichere Grenze des Geräts – dies unterstützt sowohl die Datensouveränität als auch die damit verbundene regulatorische Position.

Kontinuität ist klinisch entscheidend

Eine Eindämmung, die das Isolieren eines Geräts oder einen erzwungenen Neustart erfordert, ist inakzeptabel, wenn die Patientenversorgung davon abhängt. Die selektive Aussetzung ausschließlich des bösartigen Prozesses bedeutet, dass der Angriff in weniger als 200 Millisekunden neutralisiert wird, während medizinische Abläufe, vernetzte Geräte und klinische Systeme weiterlaufen.

Wie unterstützt Cyber Crucible FERPA und den Datenschutz von Schülerdaten?

Kurze Antwort: FortressAI prüft den Datenzugriff direkt auf dem Gerät, sodass Schülerakten und Familiendaten nicht versehentlich in ein öffentliches KI-Tool gelangen können. Cyber Crucible stoppt Ransomware autonom, ohne dass ein rund um die Uhr besetztes Security Operations Center erforderlich ist – etwas, das sich die meisten Schulbezirke und Bildungseinrichtungen nicht leisten können.

Die beiden Probleme im Bildungsbereich

Schulen und Universitäten sind bevorzugte Ziele für Ransomware-Angriffe, verfügen jedoch selten über das Budget für eine durchgehende SOC-Besetzung. Gleichzeitig hat sich die Nutzung von KI im Unterricht deutlich schneller entwickelt als die entsprechende Governance dafür.

Beide Probleme lösen

- **Ransomware ohne SOC:** Autonomer Schutz auf Kernel-Ebene stoppt Angriffe in weniger als 200 Millisekunden – ohne dass Analysten eingestellt oder ein 24/7-Überwachungsvertrag finanziert werden müssen.
- **KI-Nutzung im Einklang mit FERPA:** FortressAI bewertet jede Eingabeaufforderung direkt auf dem Gerät, sodass geschützte Bildungsdaten und persönliche Familiendaten nicht in einem öffentlichen KI-System landen – auch nicht als Trainingsdaten.

Diese Kombination schützt Schüler und Mitarbeiter, ohne den IT-Aufwand nennenswert zu erhöhen.

Was bedeutet Datensouveränität für Cyber-Crucible-Implementierungen?

Kurze Antwort: Ihre Daten bleiben dort, wo Sie sie platzieren. Analyse und Durchsetzung erfolgen auf dem Endpunkt, und Cyber Crucible kann vollständig On-Premises bereitgestellt werden — in physisch gesicherten Serverracks statt in einer Public Cloud, ohne Plattformen von Drittanbietern, ohne externen Zugriff und ohne Datenweitergabe.

Warum zentralisierte Sicherheitsdaten ein Risiko darstellen

Sicherheitsarchitekturen, die sensible Materialien zentralisieren – Verschlüsselungsschlüssel, Sitzungstoken, Identitätsdaten – schaffen einen einzelnen Ausfallpunkt (Single Point of Failure) und ein hochwertiges Ziel sowohl für kriminelle als auch staatlich unterstützte Angreifer.

Es besteht ein zweites Risiko, dem weniger Aufmerksamkeit geschenkt wird: Eine Regierung könnte sich durch eine geheime Vorladung oder einen National-Security-Letter Zugang zu zentral gespeicherten Daten verschaffen, ohne Wissen oder Zustimmung des Kunden. Dies stellt eine erhebliche Gefährdung der Datensouveränität ohne jegliche Transparenz dar.

Die On-Premises-Option

Für Organisationen, die absolute Kontrolle benötigen, bietet Cyber Crucible eine vollständige On-Premises-Installation an, einschließlich Air-Gapped-Bereitstellung und einer Multi-Tenant-Architektur, die sich eignet, um mehrere Abteilungen oder Behörden von einer einzigen sicheren Instanz aus zu verwalten.

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.

Wie wirkt sich autonome Prävention auf Cyberversicherungen und die Berichterstattung an das Board aus?

Kurze Antwort: Prävention verändert, worüber Sie berichten. Anstatt Vorfälle, Ausfallzeiten und Behebungskosten zu dokumentieren, berichten Sie über Angriffe, die ohne Betriebsunterbrechung, ohne Offenlegungspflicht und ohne Lösegeldzahlung gestoppt wurden.

Was das Board wirklich interessiert

Bei dem in dieser Wissensdatenbank durchgängig referenzierten Einsatz im Finanzdienstleistungsbereich konnte der CISO vier Ergebnisse berichten:

- **Keine Betriebsunterbrechung** — Angriffe wurden im Arbeitsspeicher gestoppt; Betrieb und legitime Transaktionen liefen weiter.
- **Keine behördliche Offenlegung** — es wurde nichts zugegriffen, sodass keine Benachrichtigung erforderlich war.
- **Kein PR-Schaden** — keine Schlagzeilen, das Kundenvertrauen blieb erhalten.
- **Starker ROI** — ein Bruchteil der Kosten des Legacy-Stacks erledigte die Arbeit, die der Legacy-Stack versäumt hatte.

Zu Lösegeldzahlungen

Rund 90 % der Ransomware-Opfer zahlten 2023 das Lösegeld. Kunden von Cyber Crucible zahlten nichts, da die Angriffe die Verschlüsselungsphase nicht erreichten.

Für Versicherer

Underwriter fragen zunehmend danach, welche Kontrollen einen Vorfall verhindern, statt danach, welche Tools einen Vorfall erkennen. Eine autonome, kernelbasierte Kontrolle, die ohne

menschliche Reaktionszeit arbeitet, ist eine substanzielle Antwort — die konkreten Deckungsbedingungen werden jedoch stets von Ihrem Versicherer festgelegt.