

# Sicherheitsprogramm & Betrieb

Wie Cyber Crucible sein Sicherheitsprogramm betreibt — Change Management, Patch- und Schwachstellenmanagement, Disaster Recovery und Business Continuity, Incident- und Breach-Response sowie Endpunktkontrolle — beschrieben für Prüfer des Anbiiterrisikos. Legt klar dar, was dokumentiert ist und was unter NDA bereitgestellt wird, und erhebt keinen Anspruch auf Zertifizierungen.

- [Verfügt Cyber Crucible über einen Change-Management-Prozess?](#)
- [Verfügt Cyber Crucible über ein Patch-Management-Programm?](#)
- [Verfügt Cyber Crucible über einen Notfallwiederherstellungs- und Geschäftscontinuitätsplan?](#)
- [Verfügt Cyber Crucible über einen Prozess zur Reaktion auf Vorfälle und zur Benachrichtigung bei Datenschutzverletzungen?](#)
- [Wie sichert und kontrolliert Cyber Crucible Endpunkte?](#)
- [Welche Sicherheitsrichtlinien pflegt Cyber Crucible, und wie kann ich diese anfordern?](#)

# Verfügt Cyber Crucible über einen Change-Management-Prozess?

**Kurze Antwort:** Ja. Produktionsänderungen folgen einem dokumentierten Change-Management-Prozess mit Überprüfung, Tests und Freigabe. Da das Produkt auf Kernel-Ebene arbeitet, wird Änderungsdisziplin als Sicherheitskontrolle behandelt und nicht lediglich als technische Praxis.

## Was der Prozess abdeckt

Änderungen an Anwendungscode, Kernel-Treibern, Serverkonfigurationen und unterstützender Infrastruktur durchlaufen definierte Lebenszyklusphasen: Sicherheitsanforderungen werden bereits im Design festgelegt; der Quellcode wird versionskontrolliert verwaltet, und Geheimnisse werden niemals im Klartext eingebettet; automatisierte Tests validieren Änderungen vor der Freigabe; und Produktionsänderungen erhalten eine formelle Überprüfung und Genehmigung. Die Aufgabentrennung wird eingehalten, sodass der Urheber einer Änderung nicht deren alleiniger Genehmiger ist. Server-Baselines folgen genehmigten Konfigurationsrichtlinien, und nicht benötigte Dienste werden nach Möglichkeit deaktiviert.

## Notfalländerungen und Treiberänderungen

Notfalländerungen nutzen einen beschleunigten Pfad, der dennoch eine Autorisierung, gezielte Tests und eine Überprüfung nach der Umsetzung erfordert. Windows-Kernel-Treiber durchlaufen eine interne Qualitätssicherung und werden vor der Veröffentlichung zur Zertifizierung im Rahmen des Windows Hardware Compatibility Program (WHCP) von Microsoft eingereicht – eine unabhängige, externe Prüfung der am höchsten privilegierten Komponente.

## Abgleich mit Rahmenwerken und die ehrliche Grenze

Der Prozess orientiert sich an NIST SP 800-53 (CM-Familie) und ISO/IEC 27001:2022 A.8.32. Cyber Crucible beansprucht keine Zertifizierung. Das detaillierte Change-Management-Verfahren sowie unterstützende Nachweise werden Prüfern unter NDA zur Verfügung gestellt.

# Verfügt Cyber Crucible über ein Patch-Management-Programm?

**Kurze Antwort:** Ja. Ein risikobasiertes Patch- und Schwachstellen-Management-Programm hält Software, Kernel-Treiber, Server und Endpunkte auf dem neuesten Stand, und Feststellungen werden bis zur Behebung nachverfolgt.

## Funktionsweise

Kontinuierliche automatisierte Sicherheitstests laufen innerhalb der Entwicklungspipeline, risikobasierte manuelle Penetrationstests werden mit einer jährlichen Mindestfrequenz durchgeführt, und ereignisgesteuerte Tests laufen bei jeder wesentlichen Änderung, wobei sowohl interne als auch externe Netzwerke abgedeckt werden. Sicherheitspatches und Hotfixes werden gemäß Herstellerempfehlung eingespielt, und die verantwortlichen Gruppen (Owner Groups) sind dafür zuständig, bei den jeweils relevanten Patches auf dem Laufenden zu bleiben. Wechseldatenträger und tragbare Medien unterliegen demselben Schutz und derselben Prüfung wie fest installierte Medien.

## Priorisierung und Bereitstellung

Feststellungen werden nach Schweregrad und Ausnutzbarkeit priorisiert, wobei aktiv ausgenutzte Schwachstellen über einen beschleunigten, außerplanmäßigen Weg bearbeitet werden. Patches durchlaufen den Change-Management-Prozess – sie werden vor der Überführung in die Produktivumgebung validiert –, und Kernel-Treiber-Updates werden vor der Veröffentlichung erneut über Microsoft WHCP validiert.

## Ausrichtung an Rahmenwerken und die ehrliche Grenze

Das Programm orientiert sich an NIST SP 800-40, NIST SP 800-53 (SI-2, RA-5), CIS Control 7 und ISO/IEC 27001:2022 A.8.8. Es wird keine Zertifizierung beansprucht. Konkrete Zielfristen für die Behebung sowie entsprechende Nachweise werden Prüfern unter NDA zur Verfügung gestellt.

# 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.

# Verfügt Cyber Crucible über einen Prozess zur Reaktion auf Vorfälle und zur Benachrichtigung bei Datenschutzverletzungen?

**Kurze Antwort:** Ja. Ein dokumentierter Prozess zur Reaktion auf Datenschutzverletzungen definiert die Rollen und Schritte für die Reaktion auf einen vermuteten Diebstahl, eine Verletzung oder eine Offenlegung geschützter Daten, einschließlich der Benachrichtigung von Kunden. Für regulierte Kunden kann vertraglich eine verbindliche Benachrichtigungsfrist festgelegt werden.

## Der Reaktionsprozess

Ein vermuteter Vorfall wird unverzüglich über interne Kanäle gemeldet, die von der Funktion Informationssicherheit überwacht werden. Nach der Identifizierung wird der Zugriff auf die betroffene Ressource entzogen, und es wird ein Incident-Response-Team einberufen, das vom Executive Management geleitet wird. Forensische Ermittler und Experten, die im Rahmen der Cyber- und Technologieversicherung von Cyber Crucible bereitgestellt werden, ermitteln, wie es zu dem Vorfall kam, welche Daten betroffen waren, welche Parteien betroffen sind und welche Grundursache vorliegt. Gemeinsam mit den Bereichen Recht, Kommunikation und Personalwesen wird ein Kommunikationsplan entwickelt, um Mitarbeiter, die Öffentlichkeit und betroffene Parteien angemessen zu benachrichtigen – einschließlich der Kundenbenachrichtigung über einen einvernehmlich vereinbarten Kanal – gefolgt von einer Nachbetrachtung des Vorfalls (Post-Incident Review).

## Support-Reaktion und Benachrichtigung

Kundenrelevante Vorfälle werden anhand der veröffentlichten SLA-Schweregrad-Stufen (SEV1 bis SEV4) verfolgt, und für regulierte Kunden kann eine vertraglich festgelegte Benachrichtigungsfrist für Datenschutzverletzungen oder Vorfälle vereinbart werden.

# Ausrichtung an Rahmenwerken und die ehrliche Grenze

Der Prozess orientiert sich an NIST SP 800-61 und ISO/IEC 27001:2022 A.5.24–A.5.26. Es wird keine Zertifizierung beansprucht. Das vollständige Verfahren zur Reaktion auf Vorfälle und zur Benachrichtigung bei Datenschutzverletzungen wird Prüfern im Rahmen einer NDA zur Verfügung gestellt.

# Wie sichert und kontrolliert Cyber Crucible Endpunkte?

**Kurze Antwort:** Auf zwei Arten. Das Produkt selbst ist eine autonome Endpunktschutzlösung, die auf Kernel-Ebene arbeitet, und Cyber Crucible kontrolliert seine eigenen Unternehmens- und Entwicklungsendpunkte im Rahmen eines formalen Programms. Beides basiert darauf, dass der privilegierteste Code intern entwickelt wird.

## Produkt-Endpunktschutz

Das Produkt bietet autonomen Schutz vor Ransomware, speicherbasierten (dateilosen) Angriffen und Prozessinjektion, durchgesetzt auf Kernel-Ebene. Es ist bewusst von Betriebssystembibliotheken entkoppelt, sodass das Produkt auch dann weiterläuft, durchsetzt und meldet, wenn Angreifer diese Bibliotheken im Arbeitsspeicher kompromittieren oder kapern. Da Erkennung und Reaktion lokal ausgeführt werden, bleibt der Schutz auch bei einem Ausfall des Management-Backends oder in einer bewusst air-gapped Bereitstellung bestehen.

## Integrität der Lieferkette und unabhängige Validierung

Die Erkennungsalgorithmen, Kernel-Heuristiken, Sensoren und Treiber werden intern entwickelt und gepflegt; es sind keine unüberprüften Drittanbieterbibliotheken oder versteckten Telemetrie-Hooks in der Software eingebettet. Da die Komponente mit den höchsten Privilegien firmeneigen ist, wird eine ganze Klasse von Risiken durch Drittanbieter-Lieferketten beseitigt und nicht nur verwaltet. Alle Windows-Kernel-Treiber werden im Rahmen des Windows Hardware Compatibility Program (WHCP) von Microsoft validiert und signiert.

## Kontrollen für Unternehmensendpunkte

Verwaltete Endpunkte folgen genehmigten sicheren Konfigurationsbaselines, führen Endpunktschutz und Scans aus und wenden dieselben Kontrollen auf Wechsel- und tragbare Medien wie auf feste Medien an, wobei die unbefugte Nutzung von Medien eingeschränkt ist. Die Softwareinstallation unterliegt einer Richtlinie, Daten im Ruhezustand auf Endpunkten werden verschlüsselt, und Endpunkte werden im Rahmen des Patch-Management-Programms aktuell

gehalten.

# Ausrichtung an Rahmenwerken und die ehrliche Grenze

Die Endpunktkontrollen richten sich an den CIS Critical Security Controls (v8) und NIST SP 800-53 (SI-3, CM-2, MP-7) aus. Es wird keine Zertifizierung beansprucht. Detaillierte Konfigurationsstandards und Nachweise werden Prüfern unter NDA zur Verfügung gestellt.

# Welche Sicherheitsrichtlinien pflegt Cyber Crucible, und wie kann ich diese anfordern?

**Kurzantwort:** Cyber Crucible pflegt einen vollständigen Satz an Informationssicherheitsrichtlinien – der die zulässige Nutzung, Zugriff und Authentifizierung, Verschlüsselung, Änderungsmanagement, Notfallwiederherstellung, Vorfall- und Datenschutzverletzungsreaktion, Datenaufbewahrung und -vernichtung und mehr abdeckt. Richtlinien und unterstützende Nachweise stehen Prüfern unter NDA zur Verfügung.

## Repräsentative Richtlinienbereiche

Der Richtlinienatz umfasst zulässige Nutzung und Ethik; Zugriff, Authentifizierung und Fernzugriff; Verschlüsselung und Schlüsselschutz; sichere Entwicklung und Änderungsmanagement; Server- und Endpunktsicherheit; Notfallwiederherstellung und Geschäftskontinuität; Vorfall- und Datenschutzverletzungsreaktion; sowie Datenaufbewahrung, -vernichtung und E-Mail-Aufbewahrung. Programmzusammenfassungen für Compliance, Audit sowie KI-/SDLC-Governance werden zusammen mit den Richtlinien gepflegt.

## Was öffentlich ist und was unter NDA steht

Öffentliche Wissensdatenbank-Seiten beschreiben das Vorhandensein, die Grundsätze und die Ausrichtung an Rahmenwerken für jedes Programm, sodass ein Prüfer die Sicherheitslage auf einer übergeordneten Ebene verstehen kann. Die spezifischen Richtlinien dokumente, Konfigurationsstandards, genauen Kennzahlen (wie Aufbewahrungspläne und Wiederherstellungsziele) sowie Audit-Nachweise sind vertraulich und werden im Rahmen einer gegenseitigen NDA zusammen mit dem vorbereiteten Vendor-Due-Diligence-Paket bereitgestellt.

## Wie man sie anfordert

Prüfer können den Satz an Sicherheitsrichtlinien, das vorbereitete Vendor-Paket und unterstützende Nachweise unter **dpo@cybercrucible.com** anfordern. Die standardmäßige gegenseitige NDA von Cyber Crucible ist verfügbar, falls noch keine besteht. Es wird keine

Zertifizierung für ein bestimmtes Rahmenwerk beansprucht; die Dokumentation erläutert, wie die Architektur und die Kontrollen die jeweiligen Verpflichtungen unterstützen.