8 Best Practices für Cyber-Resilienz

Ihr Wegweiser von der Planung zur Umsetzung noch vor dem nächsten Angriff

Überblick

Auch wenn Sie über einen Disaster Recovery-Plan verfügen, erfordert die Wiederherstellung nach destruktiven Cyberangriffen einen anderen Ansatz. Der Grund: Sie müssen in der Lage sein, schnell zu reagieren, den Vorfall effektiv zu untersuchen und Bedrohungen zu entschärfen, um eine sichere Wiederherstellung zu gewährleisten.

Begeben Sie sich mit diesen 8 Best Practices auf den Weg zu echter Cyber-Resilienz.

1. Vorbereitung

Ihre erste Aufgabe besteht darin, ein funktionsübergreifendes Team für die Resilienz gegen Ransomware mit allen Stakeholdern aufzubauen. Zwischenfälle mit Ransomware betreffen das gesamte Unternehmen. Daher ist es von entscheidender Bedeutung, dass jeder seine Rolle bei einem Cyberangriff kennt. Erwägen Sie die Durchführung einer realistischen Tabletop-Übung mit allen Stakeholdern, erstellen Sie eine unternehmensweite Richtlinie für Ransomware (und halten Sie diese auf dem neuesten Stand) und definieren Sie Ihre Strategien für Cyber-Backups und operative Resilienz.

2. Proaktive Herangehensweise

Verschaffen Sie sich einen Überblick über Ransomware-Betreiber und deren Tools, Techniken und Vorgehensweisen (Tools, Techniques, and Procedures, TTPs), indem Sie Informationen aus Ihrer Branche oder Region sammeln. Dokumentieren Sie die Kontaktdaten aller Mitglieder Ihres Reaktionsteams und halten Sie diese auf dem neuesten Stand, idealerweise über einen separaten Kommunikationskanal. Erstellen Sie einen Kanal, um ransomwareähnliches Verhalten zu melden. Stellen Sie ein Team für die Reaktion auf Cyberkrisen zusammen und beauftragen Sie gegebenenfalls ein Unternehmen, das auf die Bewältigung solcher Zwischenfälle spezialisiert ist.

3. Angriffsfläche verringern

Identifizieren und beheben Sie kritische Schwachstellen Ihrer Assets. Härten Sie Ihre Systeme und priorisieren Sie dabei die kritischen Systeme und Angriffsvektoren, die von Ransomware-Banden genutzt werden. Stellen Sie sicher, dass Anmeldedaten und Zugriffsrechte auf allen Systemen nach dem Prinzip der geringsten Rechte verwaltet werden. Implementieren Sie eine Netzwerksegmentierung, um die Ausbreitung von Ransomware zu begrenzen und die Wahrscheinlichkeit der Erkennung lateraler Bewegungen zu erhöhen. Identifizieren Sie unsichere Datenspeicher, die sensible Daten Ihres Unternehmens enthalten.

4. Backups schützen

Stellen Sie sicher, dass Backup-Systeme durch Air Gapping ausreichend geschützt sind, über eine Aufgabentrennung verfügen und unveränderliche Datenspeicher verwenden, die verhindern, dass sie von Angreifern beschädigt oder gelöscht werden können. Verwenden Sie Multifaktor-Authentifizierung (MFA) für Backup-Administratorkonten und rollenbasierte Zugriffssteuerung (RBAC). Erstellen und pflegen Sie Golden Masters für kritische Systeme, um den Neuaufbau zu beschleunigen. Stellen Sie sicher, dass Ihr Backup-System die erforderlichen Cybersicherheitsfunktionen unterstützt, um auf einen Ransomware-Zwischenfall reagieren zu können.

5. Ransomware-Schutz stärken

Identifizieren Sie Lücken in Ihren bestehenden präventiven und detektiven Kontrollen gegen die ATT&CK-Techniken, die von Ransomware-Banden eingesetzt werden. Implementieren Sie die Erkennung von Anomalien im Endpunkt-Dateisystem, die auf Ransomware- und Wiper-Angriffe hindeuten, wie beispielsweise die Verschlüsselung oder Löschung von Dateien. Implementieren Sie E-Mail-Gateway-Filter, um E-Mails mit bekannten schädlichen Indikatoren zu blockieren. Verwenden Sie Anwendungen, die das Whitelisting von betriebskritischen Assets ermöglichen, um sicherzustellen, dass nur autorisierte Software ausgeführt werden kann.

6. Ransomware-Erkennung stärken

Nutzen Sie historische Daten proaktiv, um Schwachstellen zu identifizieren. Implementieren Sie einen Mechanismus für ungewöhnliche Änderungen der CPU- und Festplattenauslastung. Identifizieren Sie ungewöhnliche Netzwerkprotokolle, einschließlich I2P oder TOR, die bekanntermaßen von Ransomware-Banden verwendet werden. Ermitteln Sie außerdem Netzwerkverbindungen anhand bekannter Ports oder Ziele, die in Ransomware und Wiper Command & Control verwendet werden.

7. Vorfallsreaktion

Identifizieren und gruppieren Sie ähnliche Alarme, die sich auf die betroffenen Assets beziehen. Erstellen Sie eine erste Verlustprognose (Ausbreitungsradius) für den Zwischenfall. Finden Sie Staging-Umgebungen, die für die Datenexfiltration verwendet werden, und isolieren Sie infizierte Hosts sowohl von kabelgebundenen als auch von kabellosen Netzwerken. Aktivieren Sie den Reinraum, stellen Sie das letzte Backup der betroffenen Systeme wieder her und installieren Sie vertrauenswürdige Erkennungs- und Reaktionstools erneut auf den Systemen im Reinraum. Suchen Sie nach Anzeichen für Persistenz und identifizieren Sie Schwachstellen in Systemen, die bei dem Angriff ausgenutzt wurden.

8. Kommunikation

Kommunizieren Sie mit internen Stakeholdern, mit der Presse, um schädliche Spekulationen zu verhindern, mit betroffenen Personen unter Einhaltung gesetzlicher und regulatorischer Verpflichtungen – und mit den Aufsichtsbehörden selbst. Informieren Sie Ihre Versicherung, die Strafverfolgungsbehörden und das nationale/branchenspezifische CERT.

Weitere Informationen zu den einzelnen Schritten finden Sie in unserem Whitepaper.

© 2025 Cohesity, Inc. Alle Rechte vorbehalten.

Cohesity, das Cohesity-Logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios und andere Cohesity-Marken sind Warenzeichen oder eingetragene Warenzeichen von Cohesity, Inc. in den USA und/oder international. Andere Unternehmens- oder Produktnamen können Warenzeichen der jeweiligen Unternehmen sein, mit denen sie verbunden sind. Dieses Material (a) soll Ihnen Informationen über Cohesity und unser Geschäft und unsere Produkte liefern, (b) wurde zum Zeitpunkt der Erstellung für wahrheitsgemäß und korrekt gehalten, unterliegt aber Änderungen ohne vorherige Ankündigung und (c) wird ohne Gewähr zur Verfügung gestellt. Cohesity lehnt alle ausdrücklichen oder impliziten Bedingungen, Zusagen und Gewährleistungen jeglicher Art ab.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

9100083-001-DE 4-2025