COHESITY

WHITEPAPER

Aufbau einer gezielten Reaktionsstrategie für destruktive Cyberangriffe

Sichere und schnelle Wiederherstellung nach Ransomware-Angriffen und anderen Cyberbedrohungen mit Cohesity

INHALTSVERZEICHNIS

Einleitung

Destruktive Cyberangriffe mit Ransomware und Wiper-Attacken erfordern einen anderen Ansatz für den IT-Betrieb als herkömmliche Business-Continuity- und Disaster-Recovery-Szenarien. Cyber-Sicherheitsteams stehen vor mehreren Herausforderungen, wenn sie sicherstellen wollen, dass angemessene Untersuchungen und Beseitigungen von Bedrohungen durchgeführt werden. Es reicht nicht aus, die Lieferung von Produkten und Dienstleistungen so schnell wie möglich wieder aufzunehmen. Unternehmen müssen zusätzlich für eine sichere Wiederherstellung sorgen, um weitere Ausfallzeiten infolge einer erneuten Infektion oder eines erneuten Angriffs zu verhindern.

Dieses Whitepaper dokumentiert die Best Practices für die Handhabung destruktiver Cyberangriffe und zeigt auf, wie Cohesity Ihrem Unternehmen helfen kann, diese operativen Ergebnisse zu erzielen.

Situationsanalyse: Warum Ihr Unternehmen in ruhigen und schwierigen Zeiten unterschiedlich agiert

„Ruhe“ beschreibt den betrieblichen Alltag Ihres Unternehmens. Warnungen von Sicherheitstools landen in der Regel in Ihrem Security Operations Center (SOC) oder bei Ihren Managed Security Service Providern (MSSP). Diese Warnungen werden nach Priorität geordnet und falsch-positive Meldungen werden herausgefiltert, während weitere Beweise gesammelt werden, um Hinweise auf ein Eindringen in die Infrastruktur Ihres Unternehmens zu identifizieren. Wenn die SOC-Analysten sicher sind, dass das Unternehmen angegriffen wird, melden sie einen Vorfall und setzen ihre Untersuchung fort. In diesem Moment beginnen für das Unternehmen sehr schwierige Zeiten.

Wenn die Analysten während der Untersuchung feststellen, dass die Vertraulichkeit, Integrität oder Verfügbarkeit der Systeme und Daten des Unternehmens beeinträchtigt wurden, melden sie einen Sicherheitsvorfall und setzen die Vorfallsreaktion fort.

Die Zeit, die Angreifer unentdeckt im Unternehmen verbringen konnte, wird als Verweildauer bezeichnet. Angreifer können durch Warnmeldungen der Sicherheitstools entdeckt werden. Doch allzu oft werden Unternehmen erst dann auf einen Angriff aufmerksam, wenn die Systeme nicht mehr zugänglich sind. Die Verweildauer kann erheblich variieren: von vier bis fünf Tagen bei Angriffen mit RaaS (Ransomware as a Service) bis hin zu Hunderten von Tagen bei Ransomware-Angriffen, die von Menschen durchgeführt werden, oder sogar Jahren im Falle von staatlichen Akteuren.

Beispiele für die Gefährdung der Vertraulichkeit, Integrität oder Verfügbarkeit:

- **Vertraulichkeit**: Die Daten des Unternehmens sind an Unbefugte weitergegeben worden. Dazu gehört auch die Exfiltration von Daten zu kriminellen Zwecken durch Ransomware-Banden oder zur Spionage durch staatliche Akteure vor dem Start eines Wiper-Angriffs.
- **Integrität**: Während der verschiedenen Phasen eines destruktiven Cyberangriffs ändern Angreifer Konfigurationsdateien, Registrys, Identitätsmanagementsysteme und möglicherweise sogar die Firmware, um die Persistenz im Unternehmen zu festigen. All diese Veränderungen beeinträchtigen die Integrität der Systeme.
- **Verfügbarkeit**: Ein destruktiver Cyberangriff zielt darauf, die IT-Infrastruktur eines Unternehmens, die für die Bereitstellung von Produkten und Dienstleistungen benötigt wird, unzugänglich zu machen. Zu diesem Zweck werden z. B. bei Ransomware-Angriffen Daten bzw. Systeme verschlüsselt und bei Wiper-Angriffen gelöscht.

Man muss verstehen, dass nicht alle Vorfälle zu Sicherheitsverletzungen eskalieren. Ein SOC erkennt Vorfälle im Frühstadium und reagiert kontinuierlich darauf, um sie zu neutralisieren. Einige Sicherheitsverletzungen werden im Unternehmen mithilfe von standardmäßigen Reaktionsplänen bewältigt, bevor sie sich ausbreiten können.

Bestimmte Vorfälle, insbesondere Ransomware- und Wiper-Angriffe, können jedoch weitreichende Auswirkungen haben. Sie können Systeme ausschalten, die für die Lieferung von Produkten und Dienstleistungen benötigt werden, sowie interne IT-Systeme, die zur Bewältigung von Vorfällen wichtig sind. Das können Systeme für den physischen Zugang zu Einrichtungen, für die Kommunikation mit Aufsichtsbehörden, betroffenen Parteien und Personen oder für die Koordination mit Versicherern, Strafverfolgungsbehörden und der Presse sein. In solchen Fällen kann das Unternehmen eine Cyber-**Krise** ausrufen und einen anderen Workflow übernehmen, um den Vorfall zu bewältigen.

Sobald die Sicherheits- und IT-Teams den Vorfall, die Sicherheitsverletzung oder die Krise bewältigt, die Recovery der Systeme wieder in einen vertrauenswürdigen Zustand zurückversetzt und die Gefahr eines erneuten Angriffs gemindert haben, kann das Unternehmen zum „Betrieb in ruhigen Zeiten“ zurückkehren.

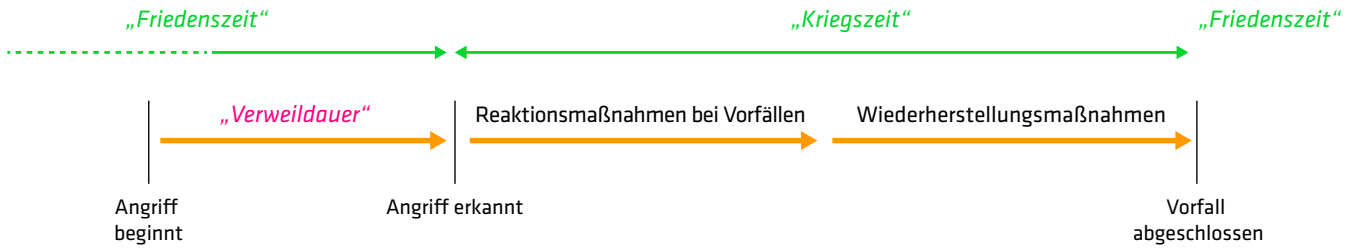


Abbildung 1: Ruhige und schwierige Phasen bei einem destruktiven Cyberangriff

Warum destruktive Cyberangriffe anders sind als Business Continuity

Vor dem Aufkommen destruktiver Cyberangriffe konnte man die Ursachen für IT-Ausfälle an einer Hand abzählen: Überschwemmungen, Brände, Hardware- oder Softwarefehler, Fehlkonfigurationen oder Stromausfälle. Diese Vorfälle erforderten nur minimale Untersuchungen und die Standardreaktion bestand lediglich in der Wiederherstellung des letzten Backup-Snapshots.

Ransomware ist jedoch viel komplexer. Im Gegensatz zu herkömmlichen Viren oder Würmern handelt es sich dabei nicht um einzelne Binärdateien, die gescannt werden können. Die Angriffe verlaufen in einer Kette von 14 Phasen und verwenden Hunderte von Methoden, um die Ziele jeder Phase zu erreichen. Sie entwickeln sich ständig weiter und die Konfigurationen von Sicherheitskontrollen werden schnell unwirksam.

Die derzeitige weltweite geopolitische Lage hat das Risiko von Wiper-Angriffen durch staatliche Akteure noch erhöht. Diese Cyberkriminellen verfügen über unvergleichliche operative Fähigkeiten, finanzielle Mittel und eine hohe Motivation, sodass Unternehmen ihre Cyber-Resilienz über das Maß hinaus ausbauen müssen, das für kriminelle Ransomware-Banden erforderlich ist.

Untersuchung und Eindämmung traditioneller Malware und Ransomware

Herkömmliche Malware, z. B. Viren und Würmer, können durch Systemscans nach schädlichen Binärdateien aufgespürt werden. Nach der Erkennung können Sicherheitsteams die schädlichen Binärdateien einfach unter Quarantäne stellen oder löschen. Im Gegensatz dazu führen Ransomware- oder Wiper-Angriffe zu einer Kette von Ereignissen, die es Angreifern ermöglichen, innerhalb weniger Tage nach einer neu bekannt gegebenen Sicherheitslücke Zugang zu erlangen. Diese Angriffe können Ihre IT-Infrastruktur für ein Live-off-the-Land-Vorgehen ausnutzen, autorisierte Konten für sich nutzen, Konfigurationen ändern, um Privilegien zu erweitern oder die Persistenz aufrechtzuerhalten, sensible Daten für die Exfiltration stagen und natives Skripting und Makros verwenden, die in Ihre Betriebssysteme und Anwendungen integriert sind. Dabei umgehen die Angreifer Kontrollen und beeinträchtigen so die Möglichkeiten zur Erkennung, Reaktion und Wiederherstellung. Im Gegensatz zu herkömmlicher Malware gibt es keine einzelnen Binärdateien, die gescannt und entfernt werden können.

Um eine sichere Wiederherstellung nach einem Ransomware- oder Wiper-Angriff durchführen zu können, muss untersucht werden, wie es zu dem Vorfall kam. Unternehmen müssen die gefundenen Bedrohungen und Schwachstellen beseitigen, um eine erneute Infektion und weitere Ausfallzeiten zu verhindern. Dies ist der Kern aller Best Practices für die Vorfallsreaktion im Bereich der Cybersicherheit.

Unternehmen müssen in drei kritischen Bereichen Abhilfe schaffen, um sicherzustellen, dass sie in Zukunft ähnlichen Angriffen widerstehen und erneute Infektionen der wiederhergestellten Systeme nach dem aktuellen Angriff verhindern können:

1. **Angriffsfläche**: Die häufigsten Zugangsvektoren für Ransomware sind Schwachstellen in der Internet-Infrastruktur, wiederverwendete legitime Zugangsdaten und Social-Engineering-Taktiken wie Phishing-E-Mails. Sie müssen herausfinden, wie der „Patient Zero", der ursprüngliche Zugangspunkt oder das erste identifizierte Opfer, kompromittiert wurde, und dann die Bedrohung in den wiederhergestellten Systemen beseitigen. Dies kann das Patchen anfälliger Systeme, die Platzierung anfälliger Systeme hinter einem Schutz wie einer Web Application Firewall (WAF) und die Entfernung der Phishing-E-Mail, die den ersten Zugriff ermöglichte, aus dem entsprechenden Posteingang beinhalten.
2. **Umgehungstechniken oder Lücken in den Sicherheitskontrollen**: Die frühzeitige Verhinderung oder Erkennung von Sicherheitsvorfällen, noch bevor sie sich auf die Vertraulichkeit, Integrität oder Verfügbarkeit auswirken, verursacht zwar Betriebskosten, hilft aber, Umsatzeinbußen, Rufschädigungen sowie potenziell kostspielige Bußgelder und Rechtsstreitigkeiten mit Geschäftspartnern oder betroffenen Personen zu vermeiden.

Ransomware-Banden integrieren Umgehungsmethoden für gängige Sicherheitskontrollen in ihre RaaS-Plattformen, darunter Endpoint Detection & Response (EDR) und Extended Detection & Response (XDR). Außerdem haben sie den Vorteil, dass sie bereits handeln können, bevor die Cyber Threat Intelligence Feeds mit ihren Angriffsmethoden aktualisiert und verbreitet werden können.

Bevor Sie die Produktion wieder aufnehmen, müssen Sie verstehen, warum die vorhandenen Sicherheitskontrollen den Angriff nicht stoppen oder erkennen konnten, bevor er die IT-Dienste unterbrochen hat. Anschließend können Sie sicherstellen, dass die Sicherheitstools wieder in einen vertrauenswürdigen Zustand versetzt und ihre Regeln aktualisiert werden, um zukünftige Angriffe zu verhindern oder frühzeitig zu erkennen.

3. **Persistenzmechanismen**: Bei einem typischen Ransomware- oder Wiper-Angriff hinterlassen Angreifer oft Dutzende von Artefakten. Diese könnten einen Ausgangspunkt für weitere Angriffe schaffen, wenn Systeme wiederhergestellt werden, ohne dass die Hinterlassenschaften vollständig verstanden und entfernt wurden. Unternehmen verbringen häufig Tage mit der Recovery ihrer Systeme und übersehen dabei Persistenzmechanismen, woraufhin sie innerhalb von Minuten erneut infiziert werden. Da destruktive Cyberangriffe in mehreren Phasen erfolgen, ist in der Regel eine Kombination aus Bedrohungssuche und forensischer Analyse erforderlich, um eine zeitliche Abfolge des Angriffs und eine umfassende Liste von zu entfernenden Artefakten zu erstellen.

Das IoC-Missverständnis (Indicators of Compromise)

Das IoC-Konzept ist der Schlüssel zu taktischer Cyber Threat Intelligence. Bevor wir uns mit den Maßnahmen zur Bewältigung destruktiver Cyberangriffe in schwierigen Zeiten befassen, müssen wir IoCs definieren.

IoCs liefern Hinweise darauf, dass ein System ***möglicherweise*** kompromittiert wurde. Sie dienen zwar als Ausgangspunkt für die Suche nach dem Verhalten des Gegners, weisen aber häufig lediglich den Weg zum Ziel. Für eine sichere Wiederherstellung müssen sich Unternehmen ein Bild von dem Angriff machen und ihn analysieren, um die im vorherigen Abschnitt behandelten Abhilfemaßnahmen ergreifen zu können. So ist beispielsweise eine geänderte Konfigurationsdatei, die beim Neustart einen bestimmten Code erneut ausführt, ein IoC, ebenso wie eine schädliche DLL mit demselben Namen wie eine legitime DLL, die in einem Verzeichnis abgelegt wurde. Auch die Manipulation der PATH-Variable, um diese schädliche DLL vor der legitimen DLL auszuführen, ist eine IoC. Diese IoCs geben uns zwar Hinweise, aber kein vollständiges Bild des Angriffs.

Die Suche nach IoCs ist für die Reaktion auf Cybersicherheitsvorfälle von entscheidender Bedeutung, doch müssen Unternehmen sie dann auch im richtigen Kontext anwenden. Wenn Sie sich allein auf IoCs verlassen, kann es passieren, dass Sie unangemessene Maßnahmen ergreifen. Außerdem kann eine vorzeitige Wiederherstellung von Backups ohne genauere Untersuchung zu einer Neuinfektion führen oder andere Verfügbarkeitsprobleme verursachen.

Werden Dateien ohne genauere Untersuchung einfach unter Quarantäne gestellt oder frühere Dateiversionen aus einem Backup-Snapshot mit dem IoC für die Recovery verwendet, wird die eigentliche Ursache nicht beseitigt. Sie wissen dann immer noch nicht, wie die Angreifer in das System eingedrungen sind, um diese Änderungen vorzunehmen, sodass sie Ihre Systeme immer wieder angreifen können. Außerdem könnte die Rückkehr zu älteren, inkompatiblen Konfigurationen zu Verfügbarkeitsproblemen führen, insbesondere wenn die Binärdateien seit Beginn des Angriffs auf neuere Versionen gepatcht wurden.

Ebenso ist das Nichtvorhandensein von IoCs in einem Backup-Snapshot keine Garantie dafür, dass er frei von Malware ist. Da IoCs lediglich als Wegweiser zu schädlichen Aktivitäten dienen, bleibt das Ziel auch nach deren Entfernung intakt. Wenn automatisch auf ältere Snapshots zurückgegriffen wird, könnte der zugrunde liegende Angriff beim Incident Response Team unbemerkt bleiben.

Die Erkennung von IoCs hängt auch von der Erfassung, Analyse und Verbreitung von Informationen über Cyber Threat Intelligence ab, die oft nicht mit den sich entwickelnden Methoden der Gegner mithalten können. Das heißt, es vergeht eine gewisse Zeit, bis die veränderten Angriffsmethoden von unseren Sicherheitstools erkannt werden. Dies erklärt, warum einige der weltweit größten Unternehmen trotz umfangreicher Cybersicherheitsbudgets und -Teams mit den neuesten und besten Cybersicherheitstools immer noch von Ransomware betroffen sind. Die Angreifer ändern ihr Verhalten, bevor die aktuellen Cybersecurity-Tools diese Änderung erfassen, sodass sie unbemerkt in die Systeme von Unternehmen eindringen können. Sobald sie einen Zugang gefunden haben, können sie die Sicherheitskontrollen der Endgeräte ausschalten. Wenn die Anbieter von Sicherheitstools die neuen Verhaltensweisen von Angreifern bemerken und die entsprechende Threat Intelligence in ihre Tools einspeisen, ist es bereits zu spät. Die Tools wurden bereits umgangen und reagieren nicht.

Angesichts dieser Herausforderungen sollten Sie eine regelmäßige proaktive Bedrohungssuche mit einer Lösung wie **Cohesity DataHawk** in Erwägung ziehen. Die Lösung arbeitet unabhängig von herkömmlichen Sicherheitskontrollen und kann nicht umgangen werden. Mit DataHawk können Sie Angriffe aufspüren, die möglicherweise durchs Netz geschlüpft sind, als sie noch nicht in den Quellen für Cyber Threat Intelligence aufgeführt waren.

Gezieltes Vorgehen: Untersuchung, Bedrohungseindämmung und sichere Wiederherstellung

Der beste Ansatz ist der Aufbau von Resilienz und Bereitschaft, indem Sie die richtigen technologischen Lösungen einsetzen. So können Sie die mit der Vorfallsreaktion beauftragten Teammitglieder (Incident Responders) stärken, klare Prozesse definieren und ein operatives Modell erstellen, damit jeder genau weiß, was er zu tun hat. Nutzen Sie nach Möglichkeit Automatisierung und Orchestrierung. Darüber hinaus sollte das Personal entsprechend geschult werden und an realistischen Übungen teilnehmen, um im Ernstfall gezielt reagieren zu können.

Cyber-Resilienz kann man nicht einfach kaufen. Es ist eine Eigenschaft, die dann zum Vorschein kommt, wenn ein vorbereitetes Unternehmen richtig auf einen Cybervorfall reagiert. Um Cyber-Resilienz zu erreichen, müssen Sie mit einem Anbieter zusammenarbeiten, der die Herausforderungen nach einem destruktiven Cyberangriff realistisch einschätzt und die richtige Technologie sowie die notwendige Unterstützung für den Aufbau einer robusten Strategie zur Vorfallsreaktion bietet.

Die Reaktion auf Cybersicherheitsvorfälle ist komplex. Sie kann nur von Erfolg gekrönt sein, wenn man diese Komplexität anerkennt und nicht ignoriert. Wer die Augen davor verschließt, wird zum denkbar ungünstigsten Zeitpunkt, nämlich während eines Vorfalls, einen Rückschlag erleiden.

Digitale Forensik im Bereich Cybersicherheit und Best Practices für die Vorfallsreaktion

Es gibt vier weit verbreitete Frameworks für die digitale Forensik und Vorfallsreaktion:

1. NIST SP800-61 Computer Security Incident Handling Guide
2. SANS Institute Six-Step Incident Response Process
3. RE&CT („React“) Framework
4. MITRE D3FEND („Data-Driven Defense“)

In diesem Whitepaper konzentrieren wir uns auf das Modell des SANS Institute. Unabhängig davon stimmen alle Frameworks weitgehend in den Schritten überein, die zur Vorbereitung und Reaktion auf einen Cyberangriff unternommen werden müssen:

Abbildung 2: Digitale Forensik im Bereich Cybersicherheit und Best Practices für die Vorfallsreaktion

Umsetzung operativer Best Practices mit Cohesity

Für Angriffssituationen umfassen alle Best-Practice-Frameworks für die Reaktion auf Cybersicherheitsvorfälle die Phasen der Begrenzung, Untersuchung, Eindämmung und Wiederherstellung. Unternehmen, die die ersten drei Phasen abkürzen und sich sofort auf die Wiederherstellung konzentrieren, lassen die Schwachstellen, die den Angriff ermöglichten, unberührt.

Die Lücken in der Verteidigung, die den Angriff nicht erkannt oder verhindert haben, bleiben offen, und oft werden die Persistenzmechanismen und andere Angriffsartefakte mit wiederhergestellt. Dies führt häufig zu einer Neuinfektion oder einem erneuten Angriff und damit zu längeren Ausfallzeiten. Es ist nicht ungewöhnlich, dass Unternehmen, die sich direkt nach Ransomware-Angriffen auf die Wiederherstellung konzentrieren, dies mehr als ein Dutzend Mal tun müssen.

Identifizierung

Die Identifizierung findet in zwei Phasen statt:

1. **Anfängliches Bewusstsein, dass ein potenzieller Vorfall im Gange ist**: Dabei kann es sich um eine Meldung eines Benutzers oder einer Drittpartei handeln, die zur Bestätigung ihres Wahrheitsgehalts und Umfangs geprüft werden muss, oder um eine Warnung einer technischen Kontrolle.
2. **Verständnis dessen, wie es zu dem Angriff kam**: Dies gewährleistet die angemessene Beseitigung der Bedrohung und der ausgenutzten Schwachstellen sowie die Verstärkung der Kontrollen, sodass die Systeme in einem sicheren und resilienten Zustand wiederhergestellt werden können.

Sehen wir uns die einzelnen Phasen genauer an:

Anfängliches Bewusstsein

Das anfängliche Bewusstsein entsteht technisch gesehen in einer ruhigen Phase, da die schwierige Zeit erst beginnt, wenn das Unternehmen einen laufenden Angriff feststellt. Daher ist es wichtig, die Mechanismen zur Erkennung von Angriffen wie Ransomware zu erörtern, um zu verstehen, wie sich dies auf den Workflow während der Vorfallsreaktion auswirken kann.

RaaS-Plattformen haben die Umgehung gängiger Sicherheitstools wie EDR und XDR zum Standard gemacht, sodass diese für Angriffe blind sind. Im MITRE ATT&CK Framework, der am weitesten verbreiteten Taxonomie zur Beschreibung der Durchführung von Cyberangriffen, weist die Taktik „Defense Evasion“ fast doppelt so viele Techniken auf wie die danach folgende der insgesamt 14 Taktiken. Diese von Ransomware-Angreifern verwendeten Mechanismen können die Anomalieerkennung von **Cohesity DataProtect** und die Bedrohungssuche von DataHawk nicht umgehen.

Alarme, wie die **KI-basierte Anomalieerkennung** von DataProtect, sind aufgrund weniger falsch-positiver Hinweise sehr **vertrauenswürdig** und sehr **genau**, wodurch der SOC-Analyst umfangreiche Informationen zur Untersuchung des Alarms erhält. Dies beschleunigt den Triage- und Untersuchungsprozess und verkürzt die nötige Zeit, um die Systeme sicher wieder in Betrieb zu nehmen.

Wenn sich bei der Triage herausstellt, dass zur Vorfallsreaktion nötige Systeme beeinträchtigt wurden oder dass die Verschlüsselung oder Löschung von Systemen im gesamten Unternehmen einen bestimmten vordefinierten Schwellenwert überschreitet, kann das Unternehmen eine **Cyberkrise** ausrufen. Ein vordefinierter Workflow für Cyberkrisen ermöglicht es Unternehmen, verschiedene Eskalationsstufen und vordefinierte Befugnisse für Incident Responder festzulegen, um bestimmte Maßnahmen durchzuführen, die über das normale Vorgehen bei Cybervorfällen hinausgehen.

Es kann sich herausstellen, dass die für die Vorfallsreaktion benötigten Systeme beeinträchtigt, nicht verfügbar oder nicht vertrauenswürdig sind. Dies könnte zu folgenden Problemen führen:

- Es kann sein, dass keine Kontaktlisten für Stakeholder verfügbar sind, wie z. B. leitende Angestellte, Aufsichtsbehörden, Cyberversicherungen, beauftragte Incident-Response-Unternehmen, Lieferkettenpartner und die Presse.

- Die Workflows für die Vorfallsreaktion sind möglicherweise nicht verfügbar.
- Verträge für Ihre Cyberversicherung und beauftragte Incident Responder sind möglicherweise nicht verfügbar.
- Managementserver und Konfigurationen für physische Zugangskontrollsysteme oder Umweltkontrollen für Gebäude können ausfallen.
- Kommunikationssysteme, z. B. E-Mail oder Voice-over-IP, die für die Kontaktaufnahme mit Stakeholdern erforderlich sind, können ausgefallen sein oder sich in einem nicht vertrauenswürdigen Zustand befinden.
- Router- und Switch-Konfigurationen oder -Firmware können nicht vertrauenswürdig sein, sodass jede Verbindung zum Internet für Software-as-a-Service-Anwendungen oder Kommunikation abgehört oder gestört werden kann.
- Sicherheitstools können umgangen oder unbrauchbar gemacht worden sein.

Es ist verständlich, dass die meisten Unternehmen der Wiederherstellung der kritischsten Anwendungen den Vorrang geben, d. h. den Anwendungen, die für die Wiederaufnahme der Produkt- und Dienstleistungsbereitstellung unerlässlich sind, auch bekannt als Minimum Viable Company (MVC). Unternehmen, die von einer destruktiven Cyberattacke betroffen sind, erkennen jedoch, dass eine Untergruppe von Konten, Anwendungen und Infrastrukturen ebenfalls benötigt wird, um den Vorfall effektiv zu bewältigen. Diese Systeme gewährleisten, dass kritische Produktionssysteme nicht nur wiederhergestellt, sondern in einen **sicheren Zustand** versetzt werden können, während gleichzeitig die gesetzlichen Verpflichtungen des Unternehmens erfüllt werden.

Cohesity definiert diese Untergruppe wesentlicher Infrastrukturen und Ressourcen für die Verwaltung von Reaktions- und Wiederherstellungsmaßnahmen als Minimum Viable Response Capability (MVRC). Angenommen, eine Komponente der MVRC ist nicht mehr vertrauenswürdig oder nicht mehr verfügbar. In diesem Fall benötigen Unternehmen eine schnelle Methode, um diese Ressourcen verfügbar zu machen und ein zuverlässiges Toolset wiederherzustellen, damit sie die Reaktionsmaßnahmen ergreifen können. Die **Cohesity Clean Room-Lösung** ermöglicht es Unternehmen, ihr MVRC schnell wieder in einen vertrauenswürdigen Zustand zu versetzen und die zur Bewältigung des Vorfalls erforderlichen Ressourcen innerhalb von Minuten bereitzustellen.

Verständnis dessen, wie es zu dem Angriff kam

Sobald die erste Triage abgeschlossen ist und die Gewissheit besteht, dass ein zerstörerischer Cyberangriff im Gange ist, meldet der Analyst einen Vorfall und setzt eine gründlichere Untersuchung fort. Normalerweise ist die Bereitstellung von Verschlüsselungsprogrammen auf Servern und Endgeräten die letzte Aktion von Ransomware-Banden, da dies die auffälligste Phase des Angriffs ist, sowohl für die Erkennungskontrollen als auch, was die Sichtbarkeit für Endbenutzer angeht.

Wenn sich Unternehmen bei Untersuchungen und Abhilfemaßnahmen nur auf verschlüsselte Systeme konzentriert, ist es unwahrscheinlich, dass sie die eigentliche Ursache des Angriffs aufdecken können. Die Untersuchung muss über diese Systeme hinausgehen. Unverschlüsselte Systeme sind oft von größerem Interesse für Ermittler, da sie möglicherweise Persistenzmechanismen enthalten, die Angreifer nutzen können, um nach einem Wiederherstellungsversuch zurückzukehren.

Bevor wir uns diese tiefgreifendere Ebene der Identifizierung genauer ansehen, ist es wichtig zu verstehen, wie ein anderer Aspekt aller Best-Practice-Prozesse zur Vorfallsreaktion unsere Fähigkeit zur Durchführung dieser Aufgabe beeinträchtigen kann: die Begrenzung.

Begrenzung

Die Begrenzung ist eine Voraussetzung für alle Incident Response Frameworks, da sie die Ausbreitung des Angriffs verhindert und jegliche Befehls- und Kontrolltätigkeit oder Datenexfiltration unterbricht. Allerdings stellt die Begrenzung auch einige Herausforderungen für die SecOps-Teams dar:

- **Remote Imaging funktioniert nicht bei Isolation**. Die meisten Unternehmen sind von der physischen Erfassung von Festplatteninhalten zum forensischen Remote Imaging übergegangen. Die Isolation eines infizierten Hosts oder seines Netzwerks kann jedoch dazu führen, dass das Unternehmen diese Aufgabe plötzlich nicht mehr ausführen kann. **DataProtect** bietet eine Bedienoberfläche und eine API, die es den Verantwortlichen für einen Vorfall ermöglicht, forensische Untersuchungen auf Dateiebene durchzuführen. Diese können nicht nur für den letzten Snapshot, sondern für eine ganze Serie von Snapshots im Zeitverlauf bis zur Aufbewahrungsfrist des Unternehmens vorgenommen werden. So können digitale Forensiker praktisch durch die Zeit reisen, um nach Binärdateien und anderen Artefakten zu suchen, die der Angreifer bereits bereinigt hat, und um schädliche Deltas in Konfigurationen und anderen Dateien schnell zu identifizieren. Im Gegensatz zu Endpoint-Security-Lösungen und SIEMs, die in der Regel nur Protokolle aus einem kurzen Zeitraum aufbewahren, ermöglicht es Cohesity Incident Respondern, Ereignisse und Protokollinhalte über den gesamten Zeitraum zu untersuchen, für den Backups

für das betreffende System aufbewahrt werden. Dies alles geschieht über eine unveränderliche Plattform und gewährleistet eine starke Beweiskette. Das Beste daran ist, dass diese Funktionen auch ohne Netzwerkverbindung zur Verfügung stehen. Sie sind immun gegen Abhörangriffe und Unterbrechungen, da DataProtect eine Offline-Kopie des Dateisystems für diese Aufgabe verwendet.

- **Endpunktlösungen werden isoliert und Query/Response-Vorgänge dadurch unmöglich.** Obwohl die Architektur verschiedener Endpunktlösungen wie EDR und XDR unterschiedlich ist, verfügen fast alle über einen zentralen Managementserver, der Telemetriedaten von Endpunkt-Clients empfängt. Wenn die Verbindung zwischen dem Managementserver und den Endpunkten unterbrochen wird, stehen den Analysten nur die Informationen zur Verfügung, die zuvor an den Managementserver gesendet wurden. Query/Response-Vorgänge sind nicht mehr möglich, um die Vorgänge an den Endpunkten in Echtzeit zu analysieren.
- Zur Begrenzung gehört auch die Einrichtung isolierter Umgebungen, in denen Reaktions- und Wiederherstellungsmethoden zur Vorfallsreaktion angewendet werden können. Die Cohesity Clean Room-Lösung ermöglicht eine flexible Erstellung solcher Umgebungen. Sie hilft Unternehmen, sich an Best Practices zur Vorfallsreaktion zu orientieren und ein geeignetes Modell der geteilten Verantwortung zwischen Sicherheit und IT-Betrieb einzuführen. Dieser Ansatz unterstützt Unternehmen, längere Ausfallzeiten zu vermeiden und eine Neuinfektion nach der Wiederherstellung zu verhindern.
- Die Cohesity Clean Room-Lösung:
- Ermöglicht die schnelle Wiederherstellung der MVRC oder der betroffenen oder umgangenen Infrastruktur, was für die Untersuchung und Behebung des Vorfalls unerlässlich ist.
- Erstellt eine isolierte Untersuchungsumgebung, die es SecOps-Teams ermöglicht, die nativen Sicherheitsfunktionen der Cohesity Data Cloud-Plattform zusammen mit ihren anderen Sicherheitstools zu nutzen, um den End-to-End-Angriff zu verstehen und die entsprechenden Behebungsmaßnahmen zu planen, um zukünftige Angriffe zu verhindern.
- Schafft eine isolierte Eindämmungsumgebung, in der die Untersuchungsergebnisse des Security Operations-Teams in Behebungsmaßnahmen einfließen, z. B. die schnelle Recovery von Systemen auf der Grundlage bekannter funktionsfähiger Installations-Images und -konfigurationen, die Wiederherstellung von Systemen und das Patchen ihrer Schwachstellen, die Verstärkung von Kontrollen, damit sie nicht umgangen werden können, und die erfolgreiche Verhinderung oder Erkennung künftiger ähnlicher Angriffe. Schließlich können die Systeme auf ihre Funktionalität und Leistung getestet werden, bevor sie wieder in die Produktionssysteme integriert werden.

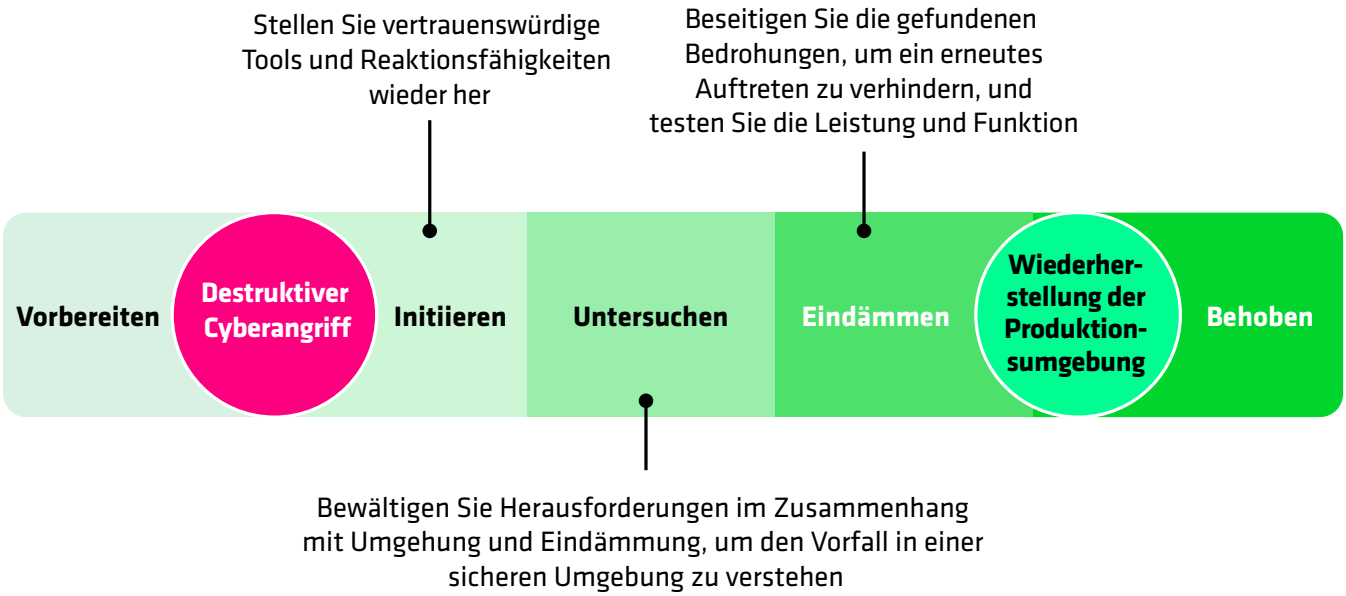


Abbildung 3: Die vier Phasen der Cohesity Clean Room-Lösung zum Beheben von Cyberangriffen

Identifizierung überdacht: Der Cohesity Clean Room

Dank digitaler Forensik und Best Practices zur Vorfallsreaktion haben Unternehmen die infizierten Netzwerke und Hosts nun unter Kontrolle. In dieser Phase wird die betroffene Infrastruktur, die zur Untersuchung und Behebung des Vorfalls benötigt wird, wieder in einen vertrauenswürdigen Zustand versetzt: Sie können sich auf Ihre Internetverbindung verlassen und Ihre cloudbasierten IT-, Geschäfts- und Sicherheitsdienste nutzen. Außerdem wird Ihre Kommunikationsfähigkeit mit den Stakeholdern wiederhergestellt. Vor allem aber haben die Sicherheits- und IT-Teams alle Unterlagen und Ressourcen, die zur Unterstützung der Vorfallsreaktion und der Wiederherstellung benötigt werden, sofort zur Hand.

Wir werden nun erörtern, wie Cohesity diese tiefergehende Untersuchungsphase unterstützt, während die zu untersuchenden Assets durch die Begrenzung isoliert wurden.

Aufdeckung der bei dem Angriff ausgenutzten Schwachstellen

Ransomware-Banden und Staaten, die sich auf Wiper-Angriffe vorbereiten, verschaffen sich den ersten Zugang meist über Schwachstellen in internetbasierten Assets. Es kommt sogar vor, dass sich Angreifer über Schwachstellen einen ersten Zugang verschaffen und Persistenzmechanismen installieren. Diese ermöglichen es ihnen, zu verbleiben und sie dann zu patchen, um zu verhindern, dass andere Angreifer Zugang zu diesen Systemen erhalten.

Wie können Unternehmen feststellen, welche Schwachstellen zum Zeitpunkt eines Angriffs bestanden? Dies wird noch schwieriger, wenn Angreifer das System gelöscht haben oder wenn Begrenzungsmaßnahmen den Zugang zum System für eine Schwachstellensuche verhindern.

Cohesity CyberScan bietet eine Lösung, mit der Unternehmen Backup-Snapshots mit ihrer Tenable Vulnerability Management-Lizenz auf Schwachstellen überprüfen können. Auf diese Weise können SecOps-Teams während eines Angriffs Schwachstellen identifizieren, selbst wenn ein System aufgrund von Begrenzungsmaßnahmen nicht erreichbar ist, gelöscht wurde oder vom Angreifer nachträglich gepatcht wurde.

Forensische Untersuchung des Dateisystems

File System Forensics, d. h. forensische Untersuchungen von Dateisystemen, sind eine Kerndisziplin der Vorfallsreaktion. Viele Unternehmen verwenden Tools für die Remote-Erfassung von forensischem Imaging. Sobald jedoch Maßnahmen zur Begrenzung ergriffen wurden, sind die Systeme, die ein forensisches Imaging erfordern, oft nicht mehr zugänglich.

DataProtect bietet Analysten nicht nur Zugriff auf einen einzelnen Dateisystem-Snapshot, sondern auch auf eine ganze Serie von Snapshots im Zeitverlauf. Auf diese Weise können forensische Prüfer die Zeitachse eines Vorfalls und den gesamten Aufbewahrungszeitraum der Backups nachvollziehen. Eine Serie von Volumina im Zeitverlauf kann schnell erstellt und verglichen werden, um schädliche Deltas zu identifizieren. Zudem können Dateiobjekte für Reverse Engineering, Detonation in Sandboxes oder

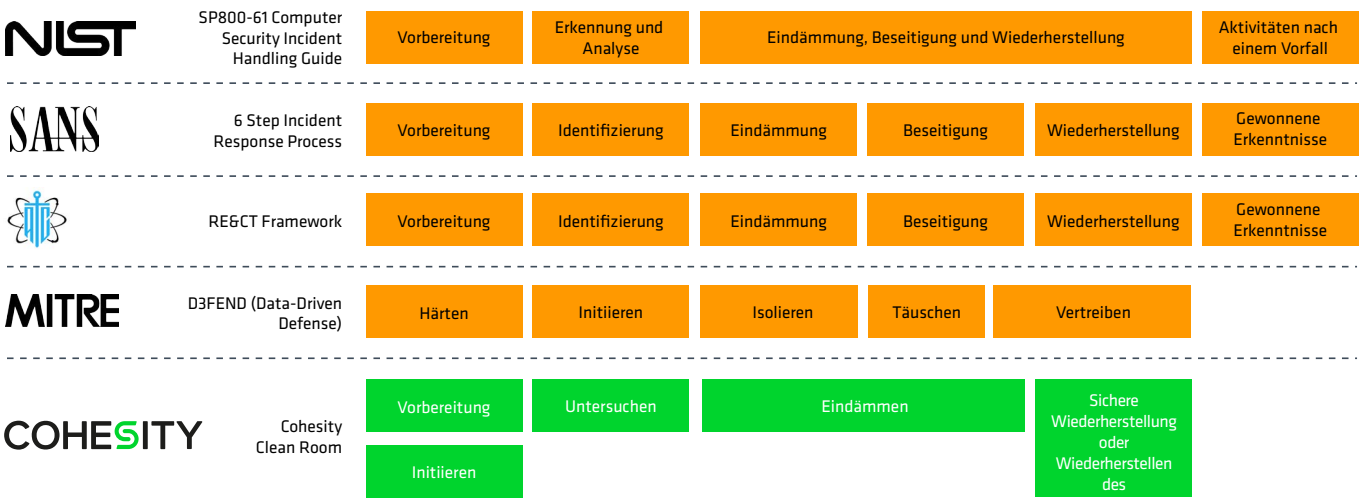


Abbildung 4: Anpassung des Cohesity Clean Rooms an die Best Practices zur Vorfallsreaktion

Analysen extrahiert werden, indem sie an cloudbasierte Dienste gesendet werden.

Bei der herkömmlichen digitalen Forensik erfassen die Spezialisten für Vorfälle in der Regel ein einzelnes Image des Systems nach dem Angriff, stellen eine Hypothese darüber auf, wie das System in diesen Endzustand gelangt ist, und arbeiten sich dann zurück, um Beweise zu sammeln, die diese Theorie stützen oder entkräften. Mit DataProtect hingegen können die Incident Responder jetzt Dateisystemänderungen über einen viel größeren Zeitraum des Vorfalls hinweg sehen, was auch dann noch funktioniert, wenn die Begrenzungsmaßnahmen den infizierten Host isoliert haben.

Threat Hunting

Die Suche nach IoCs ist eine weitere Aufgabe, die die Incident Responder normalerweise übernehmen müssen. Die Bedrohungssuche in schwierigen Zeiten lässt sich normalerweise in zwei Kategorien unterteilen:

Scannen nach IOCs, die von einer dritten Partei geliefert wurden: Bei diesen Dritten kann es sich um einen Cyber Threat Intelligence-Anbieter, eine Regierungsbehörde oder eine vergleichbare Organisation handeln. Kunden von Cohesity, die DataHawk nutzen, können die Vorteile des häufig aktualisierten Feeds von über 117.000 IoCs nutzen, die von Ransomware-Banden und staatlichen Akteuren eingesetzt werden. Die Threat Scanning-Funktion von DataHawk unterstützt auch kommerzielle CrowdStrike Threat Intelligence Feeds, die das Unternehmen lizenziert hat, und kann alle IoCs im YARA-Format von anderen Drittanbietern nutzen.

Scans zur Suche nach IoC, die Ihr Unternehmen entdeckt hat: Wenn Ihre Mitarbeiter bei einer Untersuchung auf Artefakte stoßen, müssen sie in der gesamten Infrastruktur des Unternehmens nach eben diesen IoCs suchen. Im Anschluss an die Suche kann bestimmt werden, ob weitere Systeme in die Reaktion auf den Vorfall einbezogen werden sollten.

Dies geschieht normalerweise durch die Erstellung von YARA-Regeln, die das gefundene Artefakt so beschreiben, dass eine Erkennung möglich ist, aber unnötige Fehlalarme vermieden werden. Mit Cohesity können Sie forensische Analysen durchführen (wie im vorherigen Abschnitt beschrieben), Dateisystemartefakte extrahieren und diese in Sandboxes wie Cuckoo ihre schädliche Wirkung entfalten lassen. Über ein Plugin werden dann automatisch YARA-Regeln für alle IoCs generiert, die mit dieser Datei in Verbindung stehen. Die Threat Hunting-Funktion von DataHawk ist unabhängig von Endpoint Clients. Sie funktioniert auch dann noch, wenn das Unternehmen Systeme zur Begrenzung isoliert hat. Die Funktion ist nicht anfällig gegenüber den üblichen Umgehungsmethoden, die es Endpunkt-Sicherheitslösungen unmöglich machen, ein effektives Threat Hunting durchzuführen.

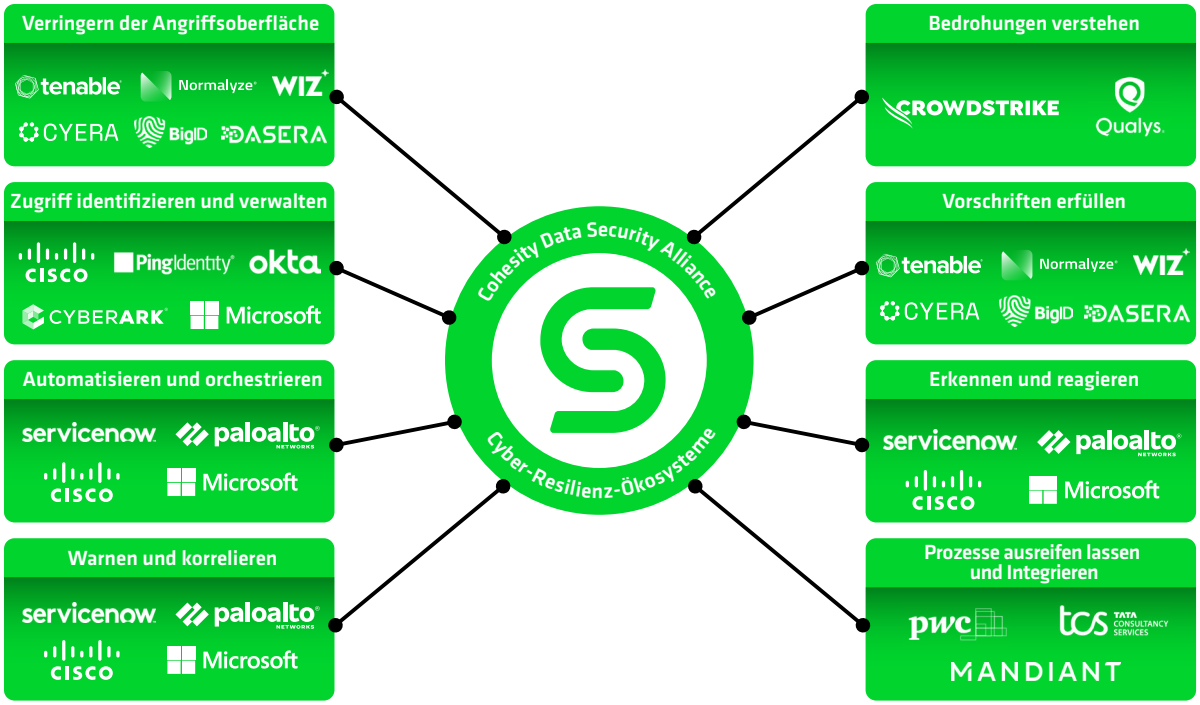


Abbildung 5: Cohesity Data Security Alliance – ein Ökosystem für Cyber-Resilienz

Funktionen wie Cohesity Global Search ermöglichen es den Incident Respondern, in der gesamten gesicherten Infrastruktur schnell nach Dateien zu suchen, was bei der Suche nach einem bestimmten Artefakt oder einer bestimmten Datei helfen kann.

Einhaltung behördlicher Vorschriften

Viele kürzlich aktualisierte Compliance-Vorschriften wie HIPAA, DORA und NIS 2 schreiben nicht nur solide Prozesse zur Vorfallsreaktion vor, sondern verpflichten Unternehmen auch dazu, Aufsichtsbehörden und betroffene Personen im Falle einer Verletzung der Cybersicherheit zu informieren. Zur Identifizierungsphase gehört das Verständnis der Art der Sicherheitsverletzung, ihrer Auswirkungen und die Sicherstellung einer rechtzeitigen Benachrichtigung.

Wenn der Vorfall die Kommunikation beeinträchtigt, hilft Cohesity als Teil der MVRC, diese Fähigkeit wiederherzustellen. Die Digital Jump Bag™ enthält mit den Kommunikationsvorlagen die Grundlage eines Clean Rooms. Darüber hinaus kann DataHawk Backups scannen, um sensible und regulierte Daten zu identifizieren, was Unternehmen hilft, die gesetzlichen Anforderungen zu erfüllen. Nach einem destruktiven Cyberangriff ist dies besonders wertvoll, wenn wichtige Datenspeicher verschlüsselt oder gelöscht wurden.

Integration von SecOps-Tools

Cyber-Resilienz ist ein Teamsport. Keine Lösung eines einzelnen Anbieters kann einen Vorfall in seiner Gesamtheit untersuchen und beheben. Deswegen hat Cohesity die Data Security Alliance ins Leben gerufen. Dieses kollaborative Ökosystem ermöglicht es, die Leistungsfähigkeit von Daten im Laufe der Zeit durch Integrationen für Governance, Untersuchung und Wiederherstellung in umfassenderen Sicherheitstools und -diensten zu nutzen.

Automatisierung und Orchestrierung

Cohesity unterstützt die API-Integration, die es einer SOAR-Plattform (Security Orchestration and Automated Response) ermöglicht, diese Untersuchungen zu steuern und die Effizienz der Analysten weiter zu steigern.

Beseitigung und Wiederherstellung

Wir haben die Phasen der Beseitigung und Wiederherstellung zu einer Eindämmungsphase zusammengefasst. Nach Ansicht von Cohesity sollte kein Unternehmen versuchen, sich von einem destruktiven Cyberangriff zu erholen, ohne die entsprechenden Maßnahmen zu ergreifen. Nur durch sie kann sichergestellt werden, dass die Angreifer die Systeme des Unternehmens nicht erneut infizieren oder dass ein künftiger Angriff derselben Art vereitelt wird.

Die Cohesity Clean Room-Lösung unterstützt die schnelle Recovery von Laufwerken, sodass ein komplettes Dateisystem wiederhergestellt werden kann, bevor Abhilfemaßnahmen zur Beseitigung von Bedrohungen angewendet werden. Dies gewährleistet eine sichere Systemwiederherstellung und erleichtert gleichzeitig den schnellen Neuaufbau von Systemen aus vertrauenswürdigen Software-Images und nachweislich funktionierenden Konfigurationen. Jeder Ansatz hat seine Vor- und Nachteile:

Wiederherstellen und bereinigen	
Vorteile	**Nachteile**
Die Verwaltung ist vor einem Vorfall einfacher.	Untersuchungen müssen gründlicher durchgeführt werden.
	Die Behebungszeit ist in der Regel länger als bei neu aufgebauten Systemen.
Neuaufbau	
Vorteile	**Nachteile**
Es besteht die Möglichkeit, Daten wiederherzustellen, Systeme neu aufzubauen und Vorfälle parallel zu untersuchen, um die Systeme so schnell wie möglich wieder in einen sicheren Zustand zu versetzen.	Die Untersuchung muss in der Regel nicht so gründlich sein, da sich die Systeme in einem vertrauenswürdigen Zustand befinden.
Die Behebungsmaßnahmen sind kürzer und beschränken sich in der Regel auf die Überprüfung der Sicherheit von Konfigurationen, die Verstärkung von Kontrollen und das Patchen anfälliger Systeme.	Die Erstellung von Skripten für die Neuinstallation erfordert Fachkenntnisse.
	Installationsmedien, Lizenzschlüssel, Konfigurationsdateien und Skripte müssen in der Digital Jump Bag aufbewahrt werden.

Einige Cohesity-Kunden entscheiden sich dafür, sowohl Backups auf Laufwerkebene als auch Rebuilds zu unterstützen. Dies gibt ihnen die Möglichkeit, für jeden kompromittierten Host die am besten geeignete Methode zur sicheren Wiederherstellung zu wählen, je nachdem, wie hoch der Aufwand für die Systembereinigung ist und wie groß das Vertrauen ist, dass die Bereinigung keine Angriffsartefakte hinterlässt.

Kunden verwenden ihre Entwicklungsumgebung oft als Cohesity Clean Room Mitigation Environment. Dieser Ansatz ermöglicht es, die Produktionsserver parallel zu den Eindämmungsmaßnahmen im isolierten Clean Room zu reduzieren. Die Eindämmungsumgebung ist so konfiguriert, dass sie die Struktur der Produktionsumgebung mithilfe der in der Digital Jump Bag gespeicherten Konfigurationen nachahmt.

Die Systeme können getestet werden, sobald die in der Untersuchungsphase entdeckten Bedrohungen durch die Bereinigung oder Wiederherstellung eines vertrauenswürdigen Zustands entschärft sind. Dies kann in Form von Funktions- bzw. Leistungstests geschehen, um sicherzustellen, dass die Behebung von Mängeln, das Patchen und die Verstärkung von Kontrollen die Leistungsfähigkeit des Systems nicht beeinträchtigt haben.

Schließlich wird zu zwei Zwecken ein Snapshot dieser Systeme erstellt:

1. Wenn ein Angriffsartefakt übersehen wird, müssen Sie nicht wieder von vorne anfangen. Der nach der Behebung erstellte Snapshot dient als neue Ausgangsbasis für die Untersuchung sowie weitere Beseitigung und wird an die Untersuchungsphase weitergeleitet.
2. Da die Eindämmungsumgebung wie die Produktionsumgebung konfiguriert wurde, kann dieser Snapshot einfach in das Produktionsnetzwerk verschoben werden.

Gewonnene Erkenntnisse

Jedes Unternehmen, das seine Cyber-Resilienz ausbauen möchte, sollte eine kontinuierliche Verbesserung anstreben. Es gilt zu verstehen, was funktioniert hat, was nicht, und was verbessert werden kann. Dies ist entscheidend, um sicherzustellen, dass Unternehmen keine weiteren Ausfallzeiten erleiden und zukünftige Vorfälle effektiver und effizienter bewältigen können. Wie das Sprichwort sagt: „Kein Plan überlebt den Feindkontakt." Die Simulation realer Angriffe ist wichtig, um die technische Wiederherstellung zu testen, Prozessverbesserungen zu beschleunigen, Möglichkeiten zur Automatisierung zu identifizieren und die automatische Reaktion Ihrer Analysten und Incident Responder zu trainieren.

Einer der größten Vorteile der Cohesity Clean Room-Lösung besteht darin, einen kompletten Vorfall zu simulieren, ohne die Produktionssysteme zu beeinträchtigen. DataProtect ermöglicht das Klonen von Produktionssystemen, die dann von einem internen Red Team oder einem externen Anbieter für Penetrationstests angegriffen werden können, um einen End-to-End-Ransomware- oder Wiper-Angriff zu simulieren. Der gesamte Response- und Recovery-Workflow kann bis unmittelbar nach der Erstellung des Baseline-Snapshots der sanierten Systeme durchgeführt werden. Dies bietet Unternehmen ein realistisches Szenario und stellt sicher, dass die richtigen Mitarbeiter, Fähigkeiten, Prozesse und unterstützenden Technologien vorhanden sind, um die Auswirkungen eines destruktiven Cyberangriffs zu minimieren, wenn das Unvermeidliche eintritt.

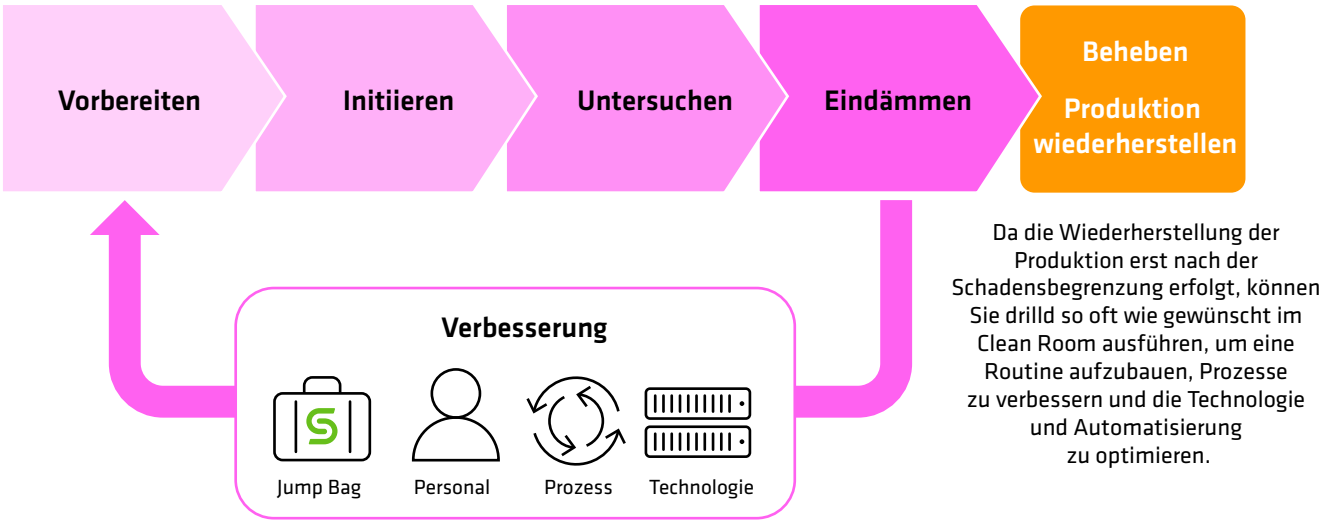
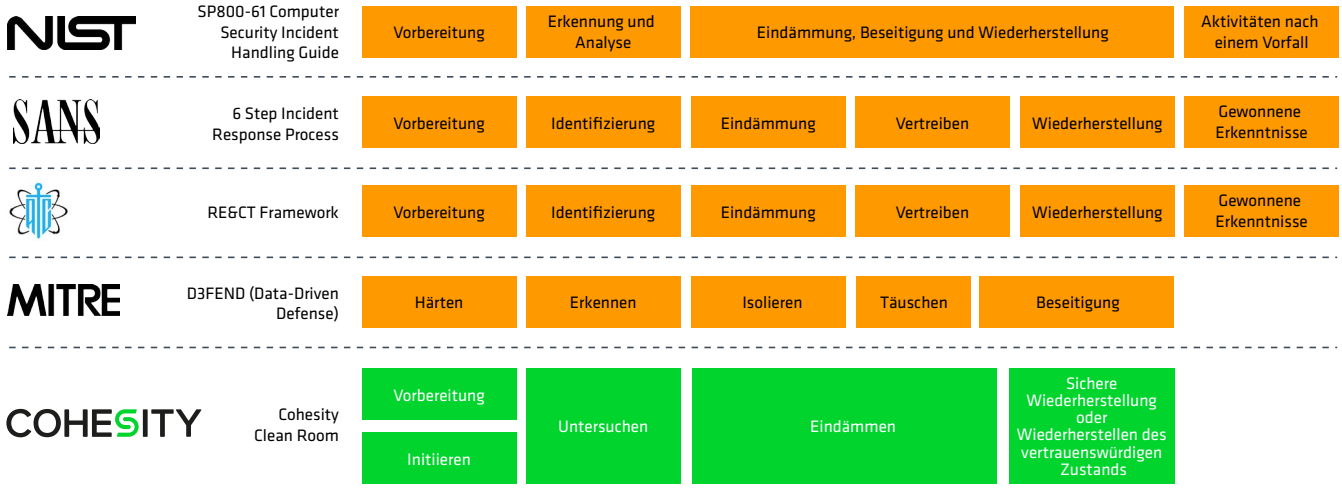


Abbildung 6: Die Cohesity Clean Room-Lösung ermöglicht eine kontinuierliche Verbesserung durch realistische Übungen für den Ernstfall

Zusammenfassung

Cohesity kann bei der Wiederherstellung einen enormen Mehrwert bieten und die Phasen der digitalen Forensik und der Vorfallsreaktion sowohl effektiv als auch effizient gestalten. Unser einzigartiger Cyber-Resilienz-Ansatz verkürzt die Zeit, die für eine sichere Wiederherstellung benötigt wird, und gibt Unternehmen die Gewissheit, dass ein ähnlicher Angriff keine weiteren Ausfallzeiten verursachen wird.



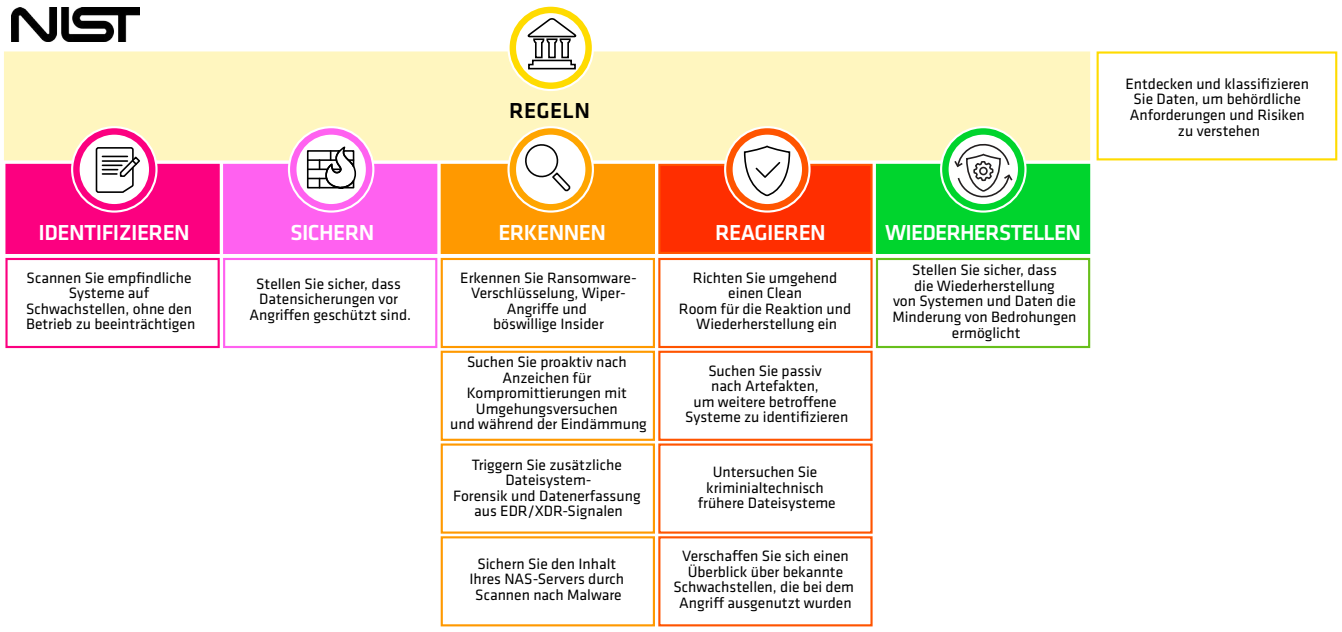


Abbildung 7: Reaktion auf Cybervorfälle und NIST Cybersecurity Framework Best Practices mit Cohesity

Über Cohesity

Cohesity ist führend im Bereich KI-gestützte Datensicherheit. Mehr als 13.600 Unternehmenskunden, darunter über 85 der Fortune 100 und fast 70 % der Global 500, vertrauen auf Cohesity, um ihre Resilienz zu stärken und gleichzeitig Gen-AI-Einblicke in ihre riesigen Datenbestände zu bekommen. Die Lösungen des Unternehmens, die aus dem Zusammenschluss von Cohesity und dem Datenschutzgeschäft von Veritas hervorgegangen sind, sichern und schützen Daten On-Premises, in der Cloud und am Edge. Cohesity wird von NVIDIA, IBM, HPE, Cisco, AWS, Google Cloud und anderen unterstützt. Der Hauptsitz des Unternehmens befindet sich in Santa Clara, Kalifornien, mit Niederlassungen auf der ganzen Welt. Folgen Sie Cohesity auf **LinkedIn**, **X** und **Facebook**, um weitere Informationen zu erhalten.

Empfohlene Lektüre

Die folgenden Whitepapers, Leitfäden und Blogs können ebenfalls hilfreich für Sie sein.

- Verbesserung der Cyber-Resilienz mit einer Digital Jump Bag™
- Aufbau von Cyber-Resilienz in einer Zeit destruktiver Cyberangriffe
- Introducing the Cohesity clean room design
- A field guide for AI-powered data security: How to deliver breakthrough business outcomes
- An executive's guide to modern data security and management
- Moderne Topologien für Datensicherheit und -management: Ein Leitfaden für IT-Führungskräfte

Erfahren Sie mehr bei Cohesity

COHESITY

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

2000058-002-DE 4-2025