COHESITY

WHITEPAPER

Ihre Roadmap zur Verteidigung gegen Ransomware

INHALTSVERZEICHNIS

Datenresilienz vs. Cyber-Resilienz

Die meisten Unternehmen verfügen über eine Datenresilienzstrategie in Form von Business Continuity und Disaster Recovery (BC/DR). Allerdings führen die für die **Datenresilienz** entwickelten Technologien und Prozesse im Zeitalter von **Ransomware** nicht immer zu echter Cyber-Resilienz.

Um Cyber-Resilienz in einem Unternehmen zu erreichen, bedarf es Kommunikation, Zusammenarbeit, Sicherheitstools, Authentifizierungssysteme, Backup-Plattformen und eine Vielzahl anderer Systeme für die folgenden Punkte:

- Untersuchung, wie der Angriff erfolgte
- Kommunikation mit betroffenen Personen, Aufsichts- und Strafverfolgungsbehörden
- Eindämmung der Gefahr eines Wiederauftretens
- Wiederherstellung der Produktion

Bei destruktiven Cyberangriffen, auch als Wiper-Angriffe bekannt, ändert sich der herkömmliche Ablauf von Erkennung, Reaktion und Wiederherstellung in einen iterativen Ablauf. In diesem müssen die Reaktions- und Kommunikationsfähigkeiten wiederhergestellt werden, bevor die Ermittlung überhaupt beginnen kann. Deshalb ist die Sicherungs- und Wiederherstellungsplattform in diesen Fällen von entscheidender Bedeutung, da sie den mit der Vorfallsreaktion beauftragten Teammitgliedern (Incident Responder) als maßgebliche Quelle für forensische Daten dient.

Damit Unternehmen cyber-Resilienz erreichen und modernen Cyberangriffen widerstehen, müssen sie zwei Bereiche berücksichtigen, die für den Erfolg entscheidend sind:

1. Angreifer dürfen die Fähigkeit zur Wiederherstellung nicht ausschalten können
2. Die Reaktionsplanung darf nicht nur Vorkehrungen für die schnelle Wiederherstellung der Produktionssysteme, sondern muss auch welche für die Sicherheits-, Authentifizierungs- und Kommunikationsplattformen enthalten, die für eine effektive und effiziente Vorfallsreaktion erforderlich sind.

Da sich Wiederherstellung und Reaktion bei Ransomware- und Wiper-Angriffen abwechseln, ist eine enge Zusammenarbeit zwischen den SecOps- und IT-Teams erforderlich, um die Auswirkungen solcher Angriffe zu minimieren.

Erstellung eines Cyber-Resilienz-Programms

Bei herkömmlichen BC/DR-Szenarien wie Überschwemmungen, Bränden und Naturkatastrophen kann die Ursache des Ereignisses schnell ermittelt werden. Bei Ransomware-Attacken arbeiten Angreifer aktiv daran, jede Wiederherstellung zu verhindern, damit das Opfer letztendlich zahlen muss.

Diese Angreifer passen sich ständig an die Verteidigungsmaßnahmen an, sodass ein präskriptives Untersuchungs- und Reaktionsprogramm von unschätzbarem Wert ist, wenn es darum geht, die Art des Angriffs zu ermitteln und den richtigen Wiederherstellungsprozess zu verstehen. Im Rahmen der Untersuchung können Unternehmen außerdem die Schwachstellen erkennen, die den Angriff ermöglichten, und die Abwehrmaßnahmen verstärken, um zukünftige Vorfälle zu verhindern. Im Gegensatz dazu kann bei einer herkömmlichen Katastrophe die Reaktion fast sofort erfolgen.

Um für einen Cyberangriff gerüstet zu sein oder ihn zu überstehen, bedarf es mehr als nur eines Plans für den Technologieeinsatz. IT- und Sicherheitsteams müssen die Angreifer und die Arten von Attacken verstehen. Mit solchen Informationen können sie gezielte Abwehrmaßnahmen ergreifen, um Angriffe besser abwehren oder früher entdecken zu können. Frameworks wie MITRE ATT&CK ermöglichen es Unternehmen, Bedrohungen zu quantifizieren und Abhilfemaßnahmen standardisiert zu kommunizieren.

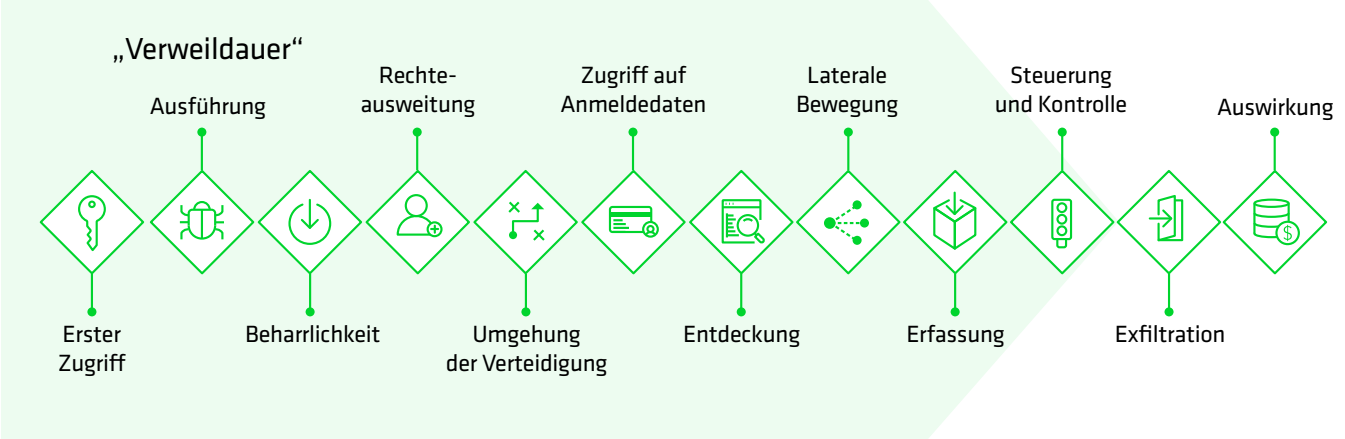
Das folgende Diagramm zeigt zum Beispiel, was Angreifer tun könnten, während sie sich in der Umgebung aufhalten, bevor die Ransomware aktiviert wird. In einigen Fällen könnten diese Aktionen für den Erfolg der Ransomware-Payload erforderlich sein, während sie in anderen Fällen dem Angreifer helfen könnten, im Netzwerk zu bleiben und zukünftige Angriffe durchzuführen. Die Verweildauer in den Systemen kann von Tagen bis hin zu Monaten reichen. Wenn die Sicherheitsteams wissen, wie Angreifer in ihrer Umgebung vorgehen, können sie proaktiv nach Indikatoren für einen Angriff suchen.

> Die Verweildauer bezieht sich auf die Zeit, in der Angreifer Zugriff auf ein kompromittiertes System haben, bevor die Attacke entdeckt wird. Eine längere Verweildauer bietet Angreifern mehr Möglichkeiten, Schaden anzurichten oder vertrauliche Informationen zu stehlen.

Betrachten Sie jede Aktion im Diagramm als eine Angriffsphase. Es mag überraschen, dass 10 der 12 Phasen durchlaufen werden, bevor die Payload überhaupt aktiviert wird. Im Falle eines Ransomware-Angriffs werden die Systeme vollständig kompromittiert, bevor die Verschlüsselung oder Datenexfiltration beginnt. Wenn sie sich im Netzwerk festsetzen konnten, können Angreifer die Wiederherstellung vereiteln und neue Angriffe starten, um mehrere Zahlungen zu erpressen. Dies wird als Double-Bubble- oder Double-Tap-Ransomware bezeichnet und wird bei Angreifern immer beliebter, um sich eine beständige Einnahmequelle zu verschaffen.

Für Opfer kann bereits ein einziger Angriff verheerend sein, da er die Lieferung von Waren und Dienstleistungen verhindern kann. Wenn Unternehmen mehreren Angriffen ausgesetzt sind, erhöht sich die Wahrscheinlichkeit von Folgeschäden:

- Rufschädigung
- Rechtsstreitigkeiten mit Betroffenen und Partnern
- Bußgelder wegen unzureichenden Schutzes der Daten von betroffenen Personen



Erschwerend kommt hinzu, dass es umso wahrscheinlicher wird, dass Artefakte des Angriffs in Backups gespeichert werden, je länger ein Angreifer im Netzwerk verbleiben kann. Wenn diese Artefakte in die Wiederherstellung aufgenommen werden, ohne dass sie identifiziert und entfernt werden, kann der Angriff erneut beginnen. Solche Fälle treten häufig auf, wenn Unternehmen, die sich von Ransomware-Angriffen erholt haben, nicht für eine saubere Wiederherstellung von Daten sorgen.

Unternehmen sollten die DFIR-Prozesse (Digital Forensics & Incident Response) befolgen, um sicherzustellen, dass saubere Daten innerhalb der Security Operations Centers wiederhergestellt werden. In der Vergangenheit verließ man sich für DFIR auf Folgendes:

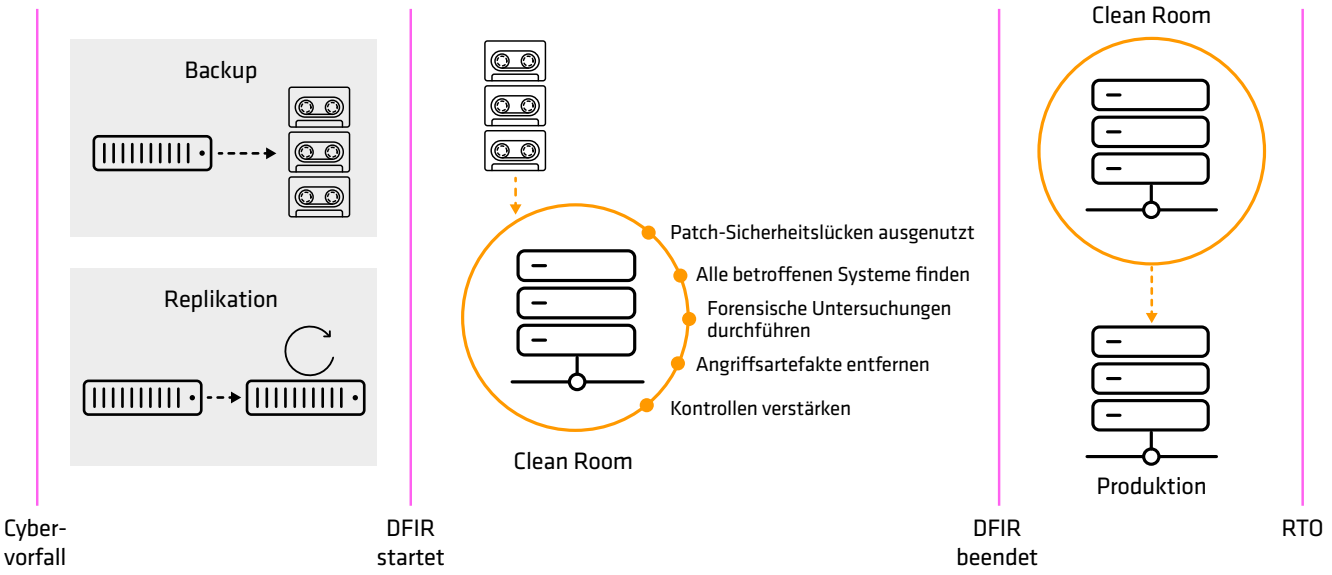
- Forensisches Imaging eines kompromittierten Hosts
- Nutzung von Untersuchungsprozessen und -tools zur Ermittlung des zeitlichen Ablaufs eines Vorfalls
- Auffinden und Analysieren der bei dem Angriff verwendeten binären Artefakte
- Aufdeckung der verwendeten Methoden zur Privilegienerweiterung und Persistenz
- Suche nach anderen kompromittierten Systemen, um das Ausmaß des Vorfalls zu ermitteln
- Scannen nach zu behebenden Schwachstellen, bevor eine Plattform wieder in Betrieb genommen wird
- Ermittlung, warum Kontrollen zur Prävention und Erkennung den Angriff nicht verhindern oder aufdecken konnten

In der Regel werden diese Aufgaben in einer Isolated Recovery Environment (IRE) oder einer Clean-Room-Umgebung durchgeführt.

Natürlich kann ein forensisches Imaging eines gelöschten oder verschlüsselten Systems keine aussagekräftigen Beweise liefern, sodass sich die Ermittler bei ihren Untersuchungen auf Backup-Repositorys verlassen. Anhand von Backup-Daten können sie Veränderungen im Laufe der Zeit erkennen und den Lebenszyklus des Angriffs verfolgen.

Cohesity bietet eine unveränderliche, forensisch fundierte Plattform für den Start des DFIR-Prozesses. Die Ermittler erhalten Zugriff auf historische Dateisystem-Snapshots, die über eine API schnell instanziiert und orchestriert werden können. Diese zeigen nicht nur den Kontext der betroffenen Systeme, sondern bieten auch Einblicke in das Dateisystem während des gesamten Zeitraums des Vorfalls. Es ist, als könnten Analysten durch die Zeit reisen. Sie können Dateisysteme über einen längeren Zeitraum hinweg vergleichen, um Methoden der Angreifer zu erkennen. Dazu zählen beispielsweise das Ändern von Konfigurationsdateien, um die Persistenz aufrechtzuerhalten, das Überschreiben legitimer Binärdateien und Bibliotheken mit schädlichen Kopien oder das Identifizieren anderer schädlicher Artefakte, die bei dem Angriff verwendet werden.

Recovery Time Objective (RTO) ist die maximal akzeptable Zeit für die Wiederherstellung eines Netzwerks oder einer Anwendung und die Rückgewinnung des Datenzugriffs nach einer ungeplanten Unterbrechung.



Durch die Einbeziehung der Backup-Infrastruktur in den DFIR-Prozess können die Untersuchungen abgeschlossen werden, bevor die Daten wieder in die Produktion gelangen. Hierbei gibt es folgende Herausforderung: Dies kann sich negativ auf das vom Unternehmen festgelegte Recovery Time Objective (RTO) auswirken. Schließlich wurden die meisten RTOs nicht für die Untersuchungen berechnet, die bei einem Cyberangriff erforderlich sind.

Durch die Verwendung der Backups zur Schaffung eines Clean Rooms wird die gesamte Ausfallzeit verkürzt. Außerdem wird damit gewährleistet, dass die wiederhergestellten Daten sauber sind, sodass der Prozess bei einer Neuinfektion nicht erneut durchlaufen werden muss. Dies hilft Unternehmen, ihre RTOs einzuhalten und längere Ausfallzeiten zu vermeiden.

Cyber-Resilienz von der Planung bis zur Ausführung

Vorbereitung

Gründen Sie ein funktionsübergreifendes Ransomware-Resilienzteam mit allen Stakeholdern.

Vorfälle mit Ransomware unterscheiden sich von anderen Cyberangriffen. Sie wirken sich auf das gesamte Unternehmen und dessen Fähigkeit aus, Produkte und Dienstleistungen für Kunden zu liefern. Jede Sekunde, die eine Reaktion und Wiederherstellung dauert, ist ein Primärverlust. Mitarbeiter sind nicht in der Lage, zu kommunizieren und ihre Arbeit zu erledigen. Die Presse wird schnell Berichte über den Vorfall veröffentlichen wollen und Kunden werden frustriert sein. Es ist von entscheidender Bedeutung, dass jeder in einem Unternehmen seine Rolle während eines Cyberangriffs kennt.

Dazu muss Folgendes festgelegt sein:

- Wie die Kommunikation ablaufen wird, wenn die wichtigsten Kommunikationswege wie E-Mail ausfallen
- Wer die Führung für jede Funktion und Phase der Reaktion übernimmt
- Welches Verfahren zu befolgen ist, wenn ein Teammitglied nicht verfügbar ist, und wer der zweite Ansprechpartner ist

Auch Mitarbeiter, die nicht direkt an der Reaktion und Wiederherstellung beteiligt sind, sollten wissen, was von ihnen erwartet wird. Warum? Weil in Ermangelung zuverlässiger Informationen Gerüchte und Mutmaßungen die Reaktion behindern und die Wiederherstellung ausbremsen können.

Führen Sie mit allen Stakeholdern eine realistische Tabletop-Ransomware-Simulation durch.

Eine der besten Möglichkeiten, das Unternehmen zu einen, ist eine realistische Tabletop-Ransomware-Simulation, die sich auf die Besonderheiten des Unternehmens konzentriert. Sie erhalten dadurch einen Einblick in Bedrohungen und Herausforderungen bei der Reaktion auf Ransomware, mit denen Sie bei einem echten Ransomware-Angriff wahrscheinlich konfrontiert werden.

Berücksichtigen Sie bei der Berechnung des Ransomware-Risikos alle Auswirkungen. Dazu zählen:

- Primäre Auswirkungen:
  - Die Unfähigkeit des Unternehmens, Produkte und Dienstleistungen zu liefern
- Sekundäre Auswirkungen:
  - Betriebskosten für die Untersuchung von und die Reaktion auf Vorfälle, einschließlich Professional Services und etwaiger Zahlungen an den Ransomware-Angreifer
  - Image-Schaden des Unternehmens
  - Bußgelder im Zusammenhang mit dem Ransomware-Vorfall oder Zahlungen an sanktionierte Staaten oder Organisationen
  - Verlust von intellektuellem Kapital
  - Rechtsstreitigkeiten mit Partnern oder Kunden im Zusammenhang mit Datenschutzverletzungen

Integrieren Sie das Ransomware-Risiko in das Risikomanagement Ihres Unternehmens.

Obwohl die Auswirkungen von Ransomware offensichtlich sind, betrachten viele Unternehmen diese nicht als ein bedeutendes Betriebsrisiko. Die Integration des Ransomware-Risikos in das unternehmensweite Risikomanagement trägt dazu bei, ein angemessenes Maß an Governance zu etablieren, um ausreichend Rückhalt für die Cybersicherheitsrichtlinien zu erhalten. Außerdem hilft es, ein adäquates Maß an Risikomanagement aufrechtzuerhalten.

Erstellen Sie eine unternehmensweite Ransomware-Richtlinie. Sie sollte folgende Kriterien erfüllen:

- **Legen Sie klare Kriterien fest, nach denen ein Vorfall als Ransomware-Angriff eingestuft wird.** Die Workflows für die Reaktion auf Ransomware und die anschließende Wiederherstellung unterscheiden sich von denen, die sich mit herkömmlicher Malware und Datenexfiltration befassen. Die Kriterien, anhand derer SOC-Analysten Vorfälle melden können, sollten festgelegt werden, damit sie die entsprechenden Untersuchungs-, Eindämmungs- und Beseitigungsmaßnahmen ergreifen können. Ohne diese

Klarheit kann sich ein Ransomware-Angriff innerhalb eines Unternehmens ausbreiten, während das SOC noch die Genehmigung zur Durchführung dieser Schritte einholen muss.

- **Legen Sie Ihre Cyber-Backup-Strategie fest.** Die Backup-Strategie für Cyber-Resilienz-Szenarien kann sich von der Datenresilienz-Strategie für herkömmliche Disaster Recovery und Business Continuity unterscheiden. Sie wird durch die Struktur und den Reifegrad der Reaktions- und Wiederherstellungsfähigkeit bestimmt.
  - Nur Backup-Daten: Hochfahren von Servern, die für die Untersuchung des Vorfalls und den Wiederaufbau der Infrastruktur aus Bare Metal benötigt werden, und anschließende Wiederherstellung von Daten. In dieser Richtlinie sollte festgelegt werden, wie die für die Wiederherstellung verwendeten Golden Master Images gepflegt werden, einschließlich der Überprüfung auf Schwachstellen und Fehlkonfigurationen.
  - Backup-Infrastruktur: Recovery der gesamten Infrastruktur und anschließende Bereinigung, indem verschiedene Teile an unterschiedlichen Punkten wiederhergestellt werden die von der Vorfallsreaktion abhängen.
- **Definieren Sie Kategorien für betriebliche Resilienz.** Diese Kategorien basieren auf Ihrer bereits erstellten Business-Impact-Analyse zur Datenresilienz und schließen die Möglichkeit ein, Cohesity-Reaktionstools innerhalb eines Clean Rooms sowie Ihre Backup-Strategien für die Cyber-Resilienz zu nutzen.
  - **Dazu gehört auch die Fähigkeit, die Kommunikations- und Sicherheitsinfrastruktur wiederherzustellen, die für die Vorfallsreaktion und Wiederherstellung erforderlich ist.** Bedenken Sie folgende Punkte:
    - Physische Zugangskontrolle
    - Domain Name Services
    - Sprachkommunikation
    - E-Mails
    - Kollaborationsplattformen für eine koordinierte Reaktion
    - Case Management
    - Forensische und Vorfallsreaktionstools
    - Schwachstellen-Scans und -Management
    - Identitäts- und Zugriffsmanagement
- **Legen Sie fest, unter welchen Bedingungen das Unternehmen eine Zahlung in Betracht ziehen würde.**
  - Wie würde das Unternehmen die nötigen Mittel für die Zahlung aufbringen?
  - Schließt die Versicherungspolice des Unternehmens Zahlungen an Cyberkriminelle ein?
  - Behandelt die Versicherung Ransomware-Angreifer, die zu einer feindlich gesinnten Gruppe gehören, als Kombattanten?
  - Übernimmt die Versicherung Zahlungen an sanktionierte Staaten oder Organisationen?
  - Welchen Ansatz verfolgt das Unternehmen bei Verhandlungen mit Angreifern, die Ransomware einsetzen?
  - Was sind die rufbezogenen, regulatorischen und strafrechtlichen Implikationen, z. B. wenn die Gruppe, die die Zahlung erhält, sanktioniert ist?
  - Wie würde Ihr Unternehmen Kryptowährung für die Zahlung erhalten? Berücksichtigen Sie die Zeit für die Bestätigung der KYC-Zeitpläne.
- **Stellen Sie sicher, dass die Ransomware-Richtlinie regelmäßig aktualisiert wird.** So können Sie der sich ständig ändernden Ransomware besser gerecht werden.

Proaktive Herangehensweise

- **Verstehen Sie die Ransomware-Angreifer und ihre Tools, Methoden und Verfahren** (Tools, Techniques & Procedures, TTPs).
  - Beschaffen Sie sich Informationen aus staatlichen, kommerziellen oder Open-Source-Quellen über Ransomware-Banden, Kampagnen und Methoden.
  - Priorisieren Sie das Sammeln von Informationen und die Analyse von Ransomware-Angreifern und solchen, die Wiper-Angriffe durchführen und in Ihrem vertikalen Markt oder Ihrer Region tätig sind.
  - Gleichen Sie die von den Angreifern verwendeten Methoden mit dem MITRE ATT&CK Framework ab.
  - Planen Sie regelmäßige Phishing-Tests, bei denen die neuesten Methoden der Ransomware-Banden berücksichtigt werden.

  - Stellen Sie sicher, dass Schwachstellen, die von Ransomware-Angreifern ausgenutzt werden, in Ihrem Vulnerability-Management-Programm vorrangig gepatcht werden.
  - Verstehen Sie, wie Ransomware-Betreiber die Beziehungen zwischen Dritten und Managed Service Providern ausnutzen, um ähnliche Unternehmen wie das Ihre anzugreifen. Berücksichtigen Sie dies bei Ihren Risikobewertungen und Kontrollen für Drittparteien.
- **Dokumentieren und pflegen Sie Kontaktdaten.** Beziehen Sie alle Mitglieder und Ersatzleute Ihres Reaktionsteams, die wichtigsten Mitarbeiter und die Stakeholder ein, idealerweise über einen Kommunikationskanal, der nicht von Ransomware betroffen ist.
- **Erstellen Sie Reporting-Kanäle.** Beziehen Sie Dritte wie Kunden, ähnliche Unternehmen und Lieferkettenpartner in die Meldung von Ransomware-Vorfällen ein.
- **Schaffen Sie einen Meldekanal für interne Benutzer, um Ransomware-ähnliches Verhalten zu melden.** Erfassen Sie Folgendes:
  - Name und Funktion der meldenden Person
  - Wann der Angriff stattfand
  - Wann er bemerkt wurde
  - Warum er für Ransomware gehalten wurde
  - Was die Person in diesem Moment getan hat
  - Wo sich die Person physisch befand und mit welchen Netzwerken sie verbunden war
  - Welches Konto die Person verwendete
  - Welche Systeme die Person verwendete (Betriebssystem, Hostname, IP-Adresse)
  - Bei welchem Konto die Person angemeldet war
  - Wen die Person kontaktiert und was sie ihm mitgeteilt hat
  - Worauf die Person in ihrer Funktion normalerweise zugreift
- **Schaffen Sie einen Reporting-Kanal für Strafverfolgungs- und Cybersicherheitsbehörden, um Ransomware- oder Wiper-Vorfälle zu melden, die Ihr Unternehmen betreffen.**
- **Stellen Sie ein Cyber Crisis Response Team zusammen.** Schließen Sie folgende Mitglieder ein:
  - Führungskräfte
  - IT (inkl. Wiederherstellung und Schwachstellenmanagement)
  - Operational Technology (falls relevant)
  - SecOps (u. a. Incident Response Manager, digitale Forensik und, falls das Unternehmen darüber verfügt, Malware Reverse Engineering, Hunt Team und Threat Intelligence)
  - Anwälte
  - Public Relations
  - Personalabteilung
- **Beauftragen Sie gegebenenfalls ein Unternehmen für die Reaktion auf Vorfälle.**
  - Holen Sie eine Vorabgenehmigung für die Beauftragung des Incident-Response-Unternehmens ein.
  - Wenn Sie sich bei der Vorfallsreaktion auf eine Versicherung verlassen, müssen Sie Folgendes wissen: Diese könnte Beweise für Verstöße gegen die bei Abschluss der Police abgegebenen Erklärungen suchen und sich nicht nur mit dem eigentlichen Ransomware-Vorfall befassen.
- **Entwerfen Sie Holding Statements und Vorlagen für die Meldung von Verstößen.** Wenn Sie den größten Teil eines Statements bereits verfasst haben, können Sie schneller reagieren und Spekulationen vermeiden, auch wenn Sie später Einzelheiten hinzufügen müssen.
  - Ernennen Sie einen Sprecher und einen Stellvertreter für das Unternehmen, die sowohl im Umgang mit den Medien als auch in der Kommunikation von Sicherheitsverletzungen geschult sind.
  - Bereiten Sie einen Kommunikationskanal für Briefings und Interviews mit der Presse vor (einen, der nicht durch einen Vorfall beeinträchtigt ist).
- **Bauen Sie bereits im Vorfeld Beziehungen zu den Strafverfolgungsbehörden sowie den nationalen Computer Emergency Response Teams auf.**
- **Lassen Sie alle Vereinbarungen mit den Strafverfolgungsbehörden von einem Anwalt überprüfen.**
- **Lassen Sie die vorgeschlagenen Reaktionspläne und Statements sowie die mögliche zivil-, aufsichts- und strafrechtliche Haftung von einem Anwalt prüfen.**

Angriffsfläche verringern

- **Priorisieren Sie das Patchen von Systemen mit Schwachstellen, die häufig von Ransomware-Banden ausgenutzt werden.** Identifizieren Sie Schwachstellen von betriebskritischen Assets und patchen Sie sie.
- **Verstärken Sie Ihre Systeme.** Priorisieren Sie die kritischen Systeme und Angriffsvektoren, die Ransomware-Banden verwenden und die durch Ihre Threat Intelligence entdeckt wurden. Konfigurieren Sie Geräte ordnungsgemäß mit Ports und Protokollen und deaktivieren Sie Geräte, die nicht für Geschäftszwecke verwendet werden. Ransomware-Angreifer verwenden legitime Tools für Living-off-the-Land-Angriffe, sodass ein eingeschränkter Zugriff auf diese Tools die Wahrscheinlichkeit eines Angriffs verringert.
- **Befolgen Sie Best Practices für das Remote Desktop Protocol und andere Remote-Desktop-Services.** Remote-Zugriffsdienste sind ein primärer Einstiegsvektor für Angreifer, die Ransomware einsetzen. Erzwingen Sie Kontosperren nach einer bestimmten Anzahl von Anmeldeversuchen, Multifaktor-Authentifizierung und die Protokollierung aller Remote-Desktop-Anmeldeversuche. Vergewissern Sie sich, dass ein triftiger geschäftlicher Grund für Remote-Desktop-Dienste den Remote-Zugriff rechtfertigt. Überprüfen Sie Ihr Netzwerk auf unbefugte Nutzung von Remote-Desktop-Services.
- **Deaktivieren oder blockieren Sie Dateifreigabeprotokolle.** Dazu gehören das ausgehende SMB-Protokoll (Server Message Block) und das Entfernen oder Deaktivieren veralteter Versionen von Dateifreigabeprotokollen. Kriminelle verwenden Dateifreigabeprotokolle, um Malware innerhalb von Unternehmen zu verbreiten.
- **Stellen Sie sicher, dass die Anmeldeinformationen und Zugriffsrechte auf allen Systemen nach dem Least-Privilege-Prinzip verwaltet werden, und begrenzen Sie die Anzahl der privilegierten Konten.**
- **Verhindern Sie, dass privilegierte Konten für alltägliche Aktivitäten verwendet werden.**
- **Implementieren Sie eine Netzwerksegmentierung.** Die Netzwerksegmentierung ist nach wie vor eine der effektivsten Methoden, um die Verbreitung von Ransomware einzuschränken und die Wahrscheinlichkeit der Entdeckung von lateralen Bewegungen zu erhöhen.
- **Verwenden Sie Basiskonfigurationen und Änderungskontrolle bei der Implementierung.** Durch Basiskonfigurationen und aufgespürte Änderungen können Backup-Images während der Untersuchungen mit dem funktionierenden Zustand verglichen werden.
- **Identifizieren Sie schlecht gesicherte Datenspeicher innerhalb Ihres Unternehmens.** Die Datenklassifizierung von Cohesity DataHawk scannt alle Backups, um sensible Daten zu identifizieren, ohne die Produktionssysteme zu beeinträchtigen. Dank dieses umfassenden Überblicks über die Speicherorte sensibler Daten können Unternehmen ihre Risiken besser einschätzen.

Backups schützen

- **Stellen Sie sicher, dass Backup-Systeme über ein ausreichendes Air Gap verfügen.** Das soll verhindern, dass sie von Angreifern gelöscht oder beschädigt werden. Cohesity FortKnox verbessert die Cyber-Resilienz mit einer unveränderlichen Kopie der Daten in einem von Cohesity gemanagten Cloud-Tresor mittels virtuellem Air Gap.
- **Stellen Sie sicher, dass Backup-Systeme unveränderliche Datenspeicher verwenden, die verhindern, dass die Systeme von Angreifern beschädigt oder gelöscht werden.** Die Cohesity Data Cloud basiert beispielsweise auf einer unveränderlichen Speicherplattform mit einer Data-Lock-Funktion, die verhindert, dass selbst Personen mit erweiterten Rechten Backups löschen können.
- **Verwenden Sie Multifaktor-Authentifizierung für Backup-Administratorkonten.** Implementieren Sie mehrere Optionen für den Fall, dass Ihr primärer Identitäts- und Zugriffsverwaltungsserver von Ransomware befallen wird. Cohesity unterstützt sowohl den SSO- als auch den TOTP-Multifaktor-Ansatz.
- **Verwenden Sie rollenbasierte Zugriffskontrollen (RBAC), um geringstmögliche Berechtigungen zuzuweisen.** Die Benutzer Ihres Backup-Systems sollten nur die Mindestberechtigungen erhalten, die für die Durchführung der mit ihrer Funktion verbundenen Aufgaben erforderlich sind. Cohesity verfügt über eine granulare RBAC, um geringste Berechtigungen zu unterstützen.
- **Stellen Sie sicher, dass Backup-Systeme eine Aufgabentrennung haben, um zu verhindern, dass ein kompromittiertes Administratorkonto schädliche Änderungen vornimmt.** Die Quorum-Funktion von Cohesity ermöglicht es Unternehmen, mehrere Autorisierungsebenen für Aufgaben im Zusammenhang mit der Datensicherung und -wiederherstellung zu definieren.
- **Übernehmen Sie eine 3-2-1-Backup-Strategie.** Erstellen Sie drei Kopien Ihrer Daten auf zwei verschiedenen Arten von Datenträgern, wobei mindestens eine Kopie abseits des Standorts aufbewahrt werden sollte.
- **Testen Sie Ihre Backups regelmäßig.** Backup-Tests sollten in regelmäßigen Abständen und automatisch durchgeführt werden. Melden Sie die Ergebnisse der Tests, damit bei Bedarf Korrekturmaßnahmen ergriffen werden können. Cohesity DataProtect unterstützt automatisierte Tests.

- **Erfassen und melden Sie Metriken zu abgeschlossenen, gescheiterten und getesteten Backups kritischer Systeme.**
- **Stellen Sie eine angemessene Speicherkapazität der Backup-Infrastruktur für das Wachstum sicher.**
- **Stellen Sie sicher, dass das Backup-System die Cybersicherheitsfunktionen unterstützt, die für die Reaktion auf Ransomware-Vorfälle erforderlich sind.** Während eines Vorfalls kann das Sicherheitsteam kein forensisches Image des betroffenen Systems erstellen, da es verschlüsselt wurde. Es muss sich also auf das Backup-System verlassen, um den Vorfall untersuchen zu können. Cohesity hat seine Datenmanagementplattform mit Reaktionsfähigkeiten wie Datenklassifizierung, Threat Intelligence Feeds und Threat Hunting versehen. Außerdem bietet Cohesity über die Data Security Alliance vorintegrierte Lösungen von führenden Sicherheitsanbietern wie Splunk, Cisco, Palo Alto, Tenable, Qualys, Crowdstrike und ServiceNow.
- **Erstellen und pflegen Sie Golden Masters für kritische Systeme, um den Wiederaufbau nach einem Vorfall zu beschleunigen.** Verwahren Sie Image-Vorlagen, die ein vorkonfiguriertes Betriebssystem und die zugehörige Anwendungssoftware enthalten, die schnell eingesetzt werden können, um ein System im Clean Room wiederherzustellen.

Ransomware-Schutz stärken

- **Identifizieren Sie Lücken in Ihren vorhandenen Kontrollmaßnahmen zur Prävention und Erkennung gegen die von Ransomware-Banden verwendeten ATT&CK-Methoden.** Machen Sie dies regelmäßig, um Ihre Chancen auf Prävention oder Erkennung zu maximieren, wenn die Angreifer ihr Verhalten anpassen.
  - Typische Indicators of Compromise (IOCs), die in den Phasen der Prävention, Erkennung und Reaktion verwendet werden können, sind:
    - Anomale Dateitransaktionen (Verschlüsselungen und abweichende Löschungen von Datenspeichern)
    - Verdächtige Startzeit von Diensten und Anwendungen
    - Vorhandensein unbekannter und unerwarteter Dienste und Anwendungen
    - Vorhandensein von nicht autorisierter Remotezugriffs- bzw. VPN-Software
    - Verminderte Systemleistung (erhöhte CPU/RAM-Auslastung)
    - Verschlechterte Leistung/deaktivierte Funktion der Host Security Tools, deaktivierte Security Agents
    - Unbekannte/unerwartete Verbindungen zwischen Domainnamen und IP-Adressen
    - Unstimmigkeiten im Protokoll
    - Hashes von bekanntermaßen schädlichen Dateien
    - Verdächtige Änderungen von Konfigurationsdateien
    - Anomaler eingehender und ausgehender Traffic oder ungewöhnliche Quellen bzw. Ziele
    - Verdächtige Prozesse und Texte in Memory Dumps
    - Verdächtige Konten bei angemeldeten Benutzern (Verlauf und aktuell)
    - Verdächtige Netzwerkfreigaben und übernommene Netzwerkfreigaben
    - Verdächtige Benutzerkonten
    - Verdächtige installierte Zertifikate
    - Verdächtige Einträge in ARP- und DNS-Caches
    - Anomalien bei Datum und Uhrzeit in Systemen, Protokolldateien oder auf NTP-Servern
    - Verdächtige Einträge oder Leases in DHCP-Protokollen
    - Anomale User-Agent-Strings
    - Nicht standardisierte Application Beacons und Aktualisierungen
    - Binärdateien innerhalb einer vollständigen Paketerfassung
- **Testen Sie Inhalte zur Prävention und Erkennung.** Testen Sie alle erstellten Regeln gegen Ransomware-IOCs.
- **Implementieren Sie die Erkennung von Anomalien im Dateisystem des Endpunkts, die auf Ransomware- und Wiper-Angriffe hinweisen, z. B. Verschlüsselung oder Löschung von Dateien.** Cohesity verwendet Machine Learning, um diese Muster zu erkennen.
- **Implementieren Sie E-Mail-Gateway-Filter, um E-Mails mit bekannten Indikatoren für Malware zu blockieren.**

- **Implementieren Sie einen Mechanismus zum Entfernen von E-Mails mit Ransomware-Inhalten aus den Postfächern von Benutzern.**
- **Implementieren Sie die Richtlinie und Verifizierung von Domain-Based Message Authentication Reporting and Conformance (DMARC).** Dadurch ist die Wahrscheinlichkeit, dass Sie gefälschte oder veränderte E-Mails von gültigen Domains erhalten, geringer.
- **Deaktivieren Sie Makros in Microsoft Office-Dateien, die per E-Mail übertragen werden, es sei denn, es gibt eine spezielle geschäftliche Anforderung.**
- **Verwenden Sie Anwendungen, die das Whitelisting von betriebskritischen Assets ermöglichen, um sicherzustellen, dass nur autorisierte Software ausgeführt werden kann.** Nutzen Sie auf Windows-Plattformen die Microsoft Software Restriction Policy oder AppLocker. Setzen Sie Listen mit zulässigen Verzeichnissen ein, anstatt zu versuchen, alle möglichen Anwendungen aufzulisten. Eine Voreinstellung, die die Ausführung vieler Ransomware-Angriffsvektoren einschränkt, erlaubt die Ausführung von Anwendungen aus PROGRAMFILES, PROGRAMFILES(X86) und SYSTEM32, obwohl dies Living-of-the-Land-Angriffe nicht verhindern kann. Alle anderen Speicherorte sollten verboten werden, es sei denn, es wird eine Ausnahme für eine bestimmte Anwendung gewährt.
- **Verstehen Sie die Praktiken zu Risikomanagement und Cyberhygiene in der Lieferkette, von Drittparteien und Managed Service Providern (MSPs).** Viele Ransomware-Angriffe werden durch Dritte erleichtert.
  - Verstehen Sie die Rolle des Unternehmens und der Partner beim Management und der Kontrolle von Cyberrisiken. Stellen Sie sicher, dass die Rollen und Verantwortlichkeiten klar definiert und gemessen werden und dass Mechanismen für Korrekturmaßnahmen in die vertraglichen Vereinbarungen aufgenommen werden.
- **Verwenden Sie für so viele Dienste wie möglich eine Multifaktor-Authentifizierung, insbesondere für den Remotezugriff und privilegierte Konten.**
- **Implementieren Sie eine logische oder physische Netzwerksegmentierung, um Geschäftsbereiche oder Kategorien von IT-Ressourcen sowie beliebige OT-Umgebungen (Operational Technology) zu trennen.** Dadurch wird die Verbreitung von Ransomware bei einem Angriff eingeschränkt.
- **Verringern Sie die Möglichkeit, dass PowerShell für Living-off-the-Land-Angriffe missbraucht werden kann.**
  - Beschränken Sie die Verwendung von PowerShell von Fall zu Fall auf bestimmte Benutzer.
  - Aktualisieren Sie PowerShell auf Version 5.0 oder höher und deinstallieren Sie alle früheren PowerShell-Versionen.
  - Stellen Sie sicher, dass die Modul-, Skriptblock- und Transkriptionsprotokollierung aktiviert ist.
  - Stellen Sie sicher, dass das Windows Event Log „PowerShell“ und das Protokoll „PowerShell Operational“ auf Systemen mit aktivierter PowerShell einen Aufbewahrungszeitraum von mindestens 180 Tagen haben.
- **Analysieren Sie den Netzwerk-Traffic-Verlauf auf anomale Ost-West- und Nord-Süd-Muster.** Verwenden Sie Metadaten zum Netzwerk-Traffic (NetFlow/sFlow) oder, falls verfügbar, eine vollständige Paketaufzeichnung oder ein Network Intrusion Detection/Prevention System.
- **Sichern Sie die Domain-Controller.**
  - **Stellen Sie sicher, dass außer den Datenmanagement- und Sicherheitsagenten keine weitere Software auf den Domain-Controllern installiert ist.** Der Zugriff auf Domain-Controller sollte auf die Administratoren beschränkt werden. Alle Benutzer in dieser Gruppe sollten für ihre täglichen Aktivitäten ein separates, eingeschränktes Konto verwenden.
  - **Konfigurieren Sie die Host-Firewall auf den Domain-Controllern, um den Zugriff auf das Internet zu verhindern.**
  - **Aktivieren Sie Kerberos für die Authentifizierung und schalten Sie die NTLM-Überprüfung ein, damit möglichst nur NTLM v2-Antworten über das Netzwerk gesendet werden.**
  - **Überprüfen Sie LSASS.EXE, um zu verstehen, welche Anwendungen betroffen wären, wenn der Schutz durch Local Security Authentication aktiviert wäre.** Dadurch wird verhindert, dass Code-Injektion Anmeldeinformationen erlangt und diese Schutzmaßnahmen aktiviert, wenn die Auswirkungen akzeptabel sind.
  - **Stellen Sie sicher, dass eine SMB-Signierung zwischen den Hosts und den Domain-Controllern erforderlich ist.** So werden Wiederholungsangriffe auf das Netzwerk verhindert.

Ransomware-Erkennung stärken

- **Suchen Sie anhand von Verlaufsdaten proaktiv nach Bedrohungen, um Kompromittierungen zu finden.** Nutzen Sie neue Threat Intelligence und IOCs im Zusammenhang mit Ransomware-Banden, für die es keine Regeln zur Prävention oder Erkennung gibt. Cohesity enthält einen integrierten Threat Intelligence Feed mit 110.000 IOCs, die von Ransomware-Banden verwendet werden, und bietet die Möglichkeit, nach diesen in den Backups zu suchen. Durch die passive Suche nach Backups anstatt nach aktiven Systemen können Angreifer diese Aktivität nicht erkennen. Sie fällt also nicht unter die Methoden zur Verteidigungsumgehung, die Angreifer gegen Endpunktlösungen einsetzen. Außerdem sind die Aufbewahrungsfristen für Backups in der Regel länger als die von Sicherheitslösungen, sodass eine längerfristige Erkennung möglich ist.
- **Implementieren Sie einen Mechanismus für ungewöhnliche Änderungen der CPU- und Festplattenauslastung.** Diese Metriken werden in der Regel von IT-Operations-Plattformen erfasst, können aber auch als zusätzliche Signale an das SecOps-Team weitergeleitet werden, um die Erkennung zu verbessern.
- **Identifizieren Sie ungewöhnliche Netzwerkprotokolle.** Dazu gehören I2P oder TOR, die bekanntermaßen von Ransomware-Banden verwendet werden.
- **Identifizieren Sie Netzwerkverbindungen mit bekannten Ports oder Zielen, die in Ransomware und Wiper Command & Control genutzt werden.**

Vorfallsreaktion

- **Identifizieren und gruppieren Sie ähnliche Alarme, die sich auf die betroffenen Assets beziehen.**
- **Erstellen Sie eine erste Schadenseinschätzung (Explosionsradius) für den Vorfall, einschließlich:**
  - Geschätzte Anzahl der verschlüsselten/gelöschten Endpunkte
  - Von verschlüsselten/gelöschten Systemen betroffene Wertschöpfungsketten
  - Regulatorische Verpflichtungen bzgl. der betroffenen Daten (Anzahl der Datensätze, Art der Daten)
  - Jegliche Hinweise auf Exfiltrationen

Cohesity durchsucht automatisch das Backup der betroffenen Systeme, um die potenziellen regulatorischen Auswirkungen von Ransomware-Vorfällen zu identifizieren. Für Systeme, die gerade gesichert werden, kann eine On-Demand-Klassifizierung durchgeführt werden, sowohl vor einem Vorfall als auch als Reaktion darauf.

- **Suchen Sie nach Staging-Umgebungen, die für die Datenexfiltration genutzt werden.** Identifizieren Sie Systeme in Ihrem Netzwerk, die einen unerwartet großen Anstieg der Datenmenge aufweisen, oder Arten von Daten, die Sie auf diesem Host nicht erwarten würden. Cohesity durchsucht automatisch das Backup der betroffenen Systeme, um die potenziellen regulatorischen Auswirkungen von Ransomware-Vorfällen zu identifizieren.
- **Isolieren Sie infizierte Hosts in kabelgebundenen und kabellosen Netzwerken.**
- **Wenn die Ransomware-Variante bekannt ist und sich von selbst verbreitet, blockieren Sie bekannte Kommunikations- und Infektionskanäle (Host- oder Netzwerk-Firewalls, E-Mail-Gateways, Netzwerkzugangskontrolle).**
- **Aktivieren Sie den Clean Room.** Wenn Sicherheitstools sowie Systeme für die Kommunikation, Zusammenarbeit oder Zugriffskontrolle beeinträchtigt wurden, sollten Sie schnell bekannte, funktionierende Instanzen bereitstellen damit die Reaktion beginnen kann.
- **Stellen Sie das letzte Backup der betroffenen Systeme in einem Clean Room wieder her.** Dies dient als forensisches Image, mit dem Sie Ihre Untersuchung beginnen können. Der Zustand des Systems zu anderen Zeitpunkten kann dabei helfen, historische Trends zu ermitteln und Änderungen im Dateisystem im Laufe der Zeit zu erkennen.
- **Stellen Sie im Clean Room vertrauenswürdige Tools für Ermittlungen, Reaktionen und Forensik erneut in den Systemen bereit.** Angreifer nehmen Endpunkt-Tools ins Visier, um die Erkennung umgehen zu können. Dadurch wird das Vertrauen in die korrekte Funktion der Endpunkt-Tools verringert. Mit der Neuinstallation von Endpunkt-Tools wird die ordnungsgemäße Funktionalität sichergestellt und das Vertrauen in die korrekte Berichterstattung der Tools gestärkt.

- **Ist die Ransomware-Variante nicht bekannt, ermitteln Sie sie wie folgt:**
  - Sammeln Sie Nachrichten mit Geldforderungen (grafische Popups, Text- oder Html-Dateien, die sich nach der Verschlüsselung automatisch öffnen können; Bilddateien wie Hintergrundbilder auf infizierten Systemen, die Kontakt-E-Mails enthalten; Sounddateien mit Geldforderungen)
  - Analysieren Sie die Nachrichten mit Geldforderungen, um die Ransomware-Bande und die Variante zu identifizieren (Name der Ransomware, verwendete Sprache, Syntax, Struktur, Phrasen, Artwork, Kontakt-E-Mail-Adresse, Benutzernamen, Art der Lösegeldforderung [d. h. Kryptowährung, Geschenkkarten], Zahlungsadresse im Falle von Kryptowährung; Support-Chat-Adresse oder Support-URL)
  - Analysieren Sie die verschlüsselten Dateien und andere erstellte Artefakte (Umbenennungsschema und -erweiterung verschlüsselter Dateien; angegriffene Dateitypen; angegriffene Dateispeicherorte; Verantwortung für Dateien und Gruppe betroffener Dateien; Änderungen an Datei-Metadaten z. B. Massenänderungen der Erstellungs-/Änderungszeiten von Dateien; Visualisierung von Entropie und Byte-Plot; für verschlüsselte Dateien verwendete Symbole; Datei-Flags; Datei mit Manifest verschlüsselter Dateien oder Schlüsselmaterial; andere Datendateien)
  - Untersuchen Sie den Infektionsvektor bei Bedarf genauer
  - Extrahieren Sie verdächtige Binärdateien aus instanziierten Dateisystemen, um Reverse Engineering durchzuführen, wenn es sich nicht um eine bekannte Variante handelt
  - Überprüfen Sie die gesammelten Artefakte, um Ransomware-Banden und -Varianten mithilfe von Websites wie diesen zu identifizieren:
    - Ransomware Census (https://goo.gl/b9R8DE)
    - CryptoSheriff (https://www.nomoreransom.org/crypto-sheriff.php)
    - ID Ransomware)
- **Suchen Sie nach Beweisen für Persistenz.** Historische Snapshots, die von Cohesity erstellt wurden, können instanziiert werden. So können Analysten Dateisysteme untersuchen und nach Anzeichen für Persistenz suchen. Dazu zählen beispielsweise:
  - Outside-in-Persistenzmechanismen, die einen authentifizierten Zugang zu externen Systemen über betrügerische Konten, Backdoors in Perimetersystemen sowie die Ausnutzung von Schwachstellen in Perimetersystemen umfassen können
  - Inside-out-Persistenz, die Malware auf den internen Systemen oder eine Reihe von Living-of-the-Land-Modifikationen umfassen kann (einschließlich des Einsatzes kommerzieller Penetrationstest-Frameworks wie Cobalt Strike, der Verwendung von PsTools, insbesondere PsExec, zur Remote-Installation und -Steuerung von Malware und zur Sammlung von Informationen sowie der Verwendung von PowerShell-Skripten)
- **Erfassen Sie ein Image des Speicherinhalts, um verdächtige Prozesse oder Text-Artefakte zu erkennen.**
- **Identifizieren Sie geänderte Registry Keys.**
- **Identifizieren Sie kürzlich erstellte komprimierte Dateien.**
- **Überprüfen Sie geplante Prozesse und Aufträge.**
- **Überprüfen Sie aktive bzw. laufende Netzwerkdienste mit denen, die in Betrieb sein sollten.**
- **Führen Sie das Data Loss Playbook aus, wenn Sie auf Beweise für ein Staging oder eine Exfiltration stoßen.** Cohesity DataHawk kann ermitteln, welche Daten sich zum Zeitpunkt des Angriffs auf diesen Systemen befanden, sodass Incident Responder die Compliance-Verpflichtungen ermitteln und die betroffenen Personen und Aufsichtsbehörden benachrichtigen können.
- **Identifizieren Sie Schwachstellen in Systemen, die bei dem Angriff ausgenutzt wurden.** Cohesity CyberScan ermöglicht es Incident Respondern, den Tenable Nessus Vulnerability Scanner in der Nähe des Punkts, wo der Angriff erfolgte, auf dem Snapshot laufen zu lassen. So können Sie ein Manifest mit Patches erstellen, die angewendet werden müssen, bevor das System wieder in Betrieb genommen wird. Dieses Manifest enthält auch alle Schwachstellen, die die Angreifer seit dem letzten geplanten Schwachstellen-Scan ausgenutzt haben könnten.
- **Identifizieren Sie Assets, die für das Staging verwendet wurden, indem Sie per Scan nach geistigem Eigentum, Finanzdaten oder personenbezogenen Daten auf nicht autorisierten Assets suchen.** Sensible Daten können in Staging-Umgebungen mithilfe der Datenklassifizierung von Cohesity DataHawk identifiziert werden.

- **Extrahieren Sie verdächtige Binärdateien aus historischen instanziierten Dateisystemen.** Analysieren Sie diese, führen Sie ein Reverse Engineering durch oder laden Sie sie auf Dienste wie VirusTotal hoch. Die Instanziierung historischer Dateisysteme kann in Cohesity durch SOAR-Tools (Security Orchestration & Automated Response) wie ServiceNow Security Incident Response, Splunk Phantom und Palo Alto XSOAR orchestriert werden.
- **Extrahieren Sie verdächtige Binärdateien aus instanziierten Dateisystemen und lassen Sie sie in einer Sandbox zur Malware-Analyse frei, um ihre Auswirkungen zu erkennen.**
- **Überprüfen Sie ähnliche Systeme innerhalb des Unternehmens auf Infektionen.** Untersuchen Sie Hosts mit ähnlichen Benutzern und Gruppen. Wenn Systeme nicht verschlüsselt sind, vergleichen Sie die Instanzen dieser Hosts mit dem infizierten System, um die möglichen Auswirkungen zu ermitteln. Cohesity verfügt über Indexierungs- und Suchfunktionen, mit denen die Backup-Infrastruktur eines Unternehmens schnell abgefragt werden kann.
- **Überprüfen Sie lokale Konten, Identitäts- und Zugriffsmanagement-Tools sowie Directory Services auf neue Konten oder Änderungen von Berechtigungen/Zugriffsrechten.**
- **Identifizieren Sie andere Systeme, die versuchen, eine Verbindung zur Ransomware-Kommandosteuerung herzustellen.**
- **Verfolgen Sie die Untersuchungskette mithilfe von MITRE ATT&CK weiter, um den Patient Zero, also den anfänglichen Infektionsvektor und jeden infizierten Endpunkt zu finden.**
- **Geben Sie an, welche Präventions- oder Ermittlungskontrollen umgangen und welche Mechanismen dafür verwendet wurden.** Fügen Sie diese in Ihren Risikoeindämmungsplan ein, um die Kontrollen zu verstärken, bevor Sie die Produktion wieder aufnehmen.

Kommunikation

- **Kommunizieren Sie mit der Presse.** Geben Sie der Presse aktuelle Informationen, um kontraproduktive Spekulationen zu vermeiden.
- **Kommunizieren Sie mit betroffenen Personen.** Stellen Sie sicher, dass alle Meldungen den gesetzlichen und behördlichen Verpflichtungen entsprechen.
- **Kommunizieren Sie mit internen Stakeholdern.** Halten Sie Ihre Belegschaft über die Situation und Ihre Erwartungen an sie auf dem Laufenden, insbesondere da die Presse Plattformen wie LinkedIn nutzen könnte, um Mitarbeiter zu identifizieren und sie direkt zu kontaktieren.
- **Kommunizieren Sie mit den Aufsichtsbehörden, um die gesetzlichen Meldepflichten zu erfüllen.**
- **Informieren Sie Ihre Versicherung.**
- **Informieren Sie die Strafverfolgungsbehörden und das nationale bzw. brancheninterne CERT.**

Wiederherstellung nach dem Vorfall

Im besten Fall finden und entfernen Sie die Infektion und nehmen die Systeme mithilfe von Tools wie IMR (Instant Mass Restore, sofortige Massenwiederherstellung) wieder in Betrieb. In der Realität werden Sie wahrscheinlich eine Kombination aus Systemen haben, die wiederhergestellt werden können, und solchen, die von Grund auf neu aufgebaut werden müssen. Um Bare-Metal-Wiederherstellungen durchzuführen, benötigen Sie Zugang zu Gold Images kritischer Systeme, die sicher sind und mit den neuesten getesteten Patches versehen wurden. Diese Vorlagen können schnell genutzt werden, um Systeme neu aufzubauen, die nicht mehr wiederhergestellt werden können. Sie können auch mit den Tools aus der Cohesity Data Cloud gesichert werden, sodass sie bei einem Cyberangriff nicht beschädigt werden. Dann können Sie das Basisbetriebssystem und die Anwendungen sowie die zugehörigen Daten aus anderen Backups wiederherstellen. Dadurch wird das RTO optimiert, während gleichzeitig historische Backups der betroffenen Systeme für forensische Untersuchungen erstellt werden.

Während die Daten und Anwendungen wiederhergestellt werden, müssen Sie den Vorfall dokumentieren und verhindern, dass er sich wiederholt.

Unternehmen sollten:

- Das Wissen über den ursprünglichen Infektionsvektor, die ausgenutzten Schwachstellen und die Persistenzmechanismen nutzen und damit Ihre Wiederherstellungspläne aktualisieren, um sich vor zukünftigen Angriffen zu schützen und sicherzustellen, dass jede Komponente wieder in einen sicheren und stabilen Zustand gebracht werden kann
- Die verbleibenden Systeme schnell im Clean Room wiederherstellen und die oben genannten Schritte wiederholen, wobei alle Hinweise auf eine Gefährdung unter Quarantäne gestellt werden
- Gefundene Schwachstellen patchen
- Passwörter für alle betroffenen Systeme und Konten zurücksetzen
- Historische E-Mails mit Exploitation-Artefakten aus gelöschten E-Mail-Postfächern entfernen
- Die Überwachung vorher infizierter Systeme verstärken

Wichtigste Erkenntnisse und Follow-up-Maßnahmen

Stellen Sie sich nach einer Ransomware-Attacke die folgenden Fragen, um zu Erkenntnissen zu gelangen:

- Welche Produkte und Dienstleistungen waren betroffen?
- Was waren die Auswirkungen auf das Unternehmen?
- Welche Stakeholder waren betroffen?
- Wer waren die beteiligten Threat Actors?
- Was ist bei der Reaktion falsch gelaufen?
- Was ist bei der Reaktion richtig gelaufen?
- Wann haben wir den Angriff entdeckt?
  - Wie groß war die Zeitspanne zwischen ursprünglicher Infektion und Erkennung?
  - Warum wurde der Angriff nicht früher entdeckt?
  - Welche Kontrollen haben bei der Erkennung/Verhinderung versagt?
- Welche Kontrollen wurden umgangen und wie?
- Was muss bei den Geschäftsabläufen angepasst werden, um zukünftige Vorfälle zu verhindern?
- Wie kann dies in Zukunft vermieden werden?
- Konnten wir die Produktion innerhalb der erforderlichen RTO/RPO wiederherstellen?

Senden Sie neu entdeckte IOCs an alle autorisierten Partner und Anbieter.

- Aktualisieren Sie die Dokumentation und Playbooks.
- Senden Sie den Abschlussbericht über den Vorfall und die daraus gezogenen Lehren an die Stakeholder und Aufsichtsbehörden.

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 ist, 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.

Erfahren Sie mehr auf Cohesity.com.

COHESITY

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

2000048-002 EN 4-2025