Wiederherstellung nach Ransomware-Angriffen: Eine umfassende Anleitung

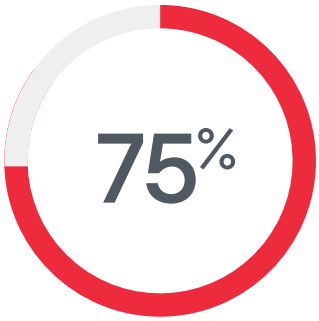
Inhalt

Einführung

Ransomware-Angriffe sind mittlerweile an der Tagesordnung und betreffen Unternehmen aller Größen und Branchen. Laut dem Veeam-Report „Trends bei Ransomware“ waren 75 % der Unternehmen im Jahr 2023 von mindestens einem Ransomware-Angriff betroffen, viele sogar von mehreren Angriffen.

Die finanziellen Kosten für die Lösegeldzahlung sind nicht die einzigen Kosten, die Unternehmen nach einem Angriff entstehen. Ransomware kann den Umsatz und den Betrieb eines Unternehmens lahmlegen. Daher müssen sich Unternehmen darauf vorbereiten, indem sie starke Cybersicherheitsmaßnahmen, eine umfassende Backup-Strategie und einen leistungsstarken Plan zur Reaktion auf Vorfälle implementieren. Diese Pläne müssen regelmäßig getestet werden, um sicherzustellen, dass die Backups vollständig und brauchbar sind und der Plan für die Reaktion auf Vorfälle schnell implementiert werden kann.

Dieses E-Book dient als Anleitung zur Wiederherstellung nach Ransomware-Angriffen, indem es Erkenntnisse aus praktischen Erfahrungen und Ratschlägen von Experten einbezieht.



der Unternehmen waren 2023 mindestens einmal einem Ransomware-Angriff ausgesetzt

Was ist die Wiederherstellung nach Ransomware-Angriffen?

Ransomware gehört heute zu den größten Bedrohungen für Unternehmen. Der Report 2024 State of Ransomware von Veeam zeigt, dass 96 % der Ransomware-Angriffe auf Backup-Repositorys ausgerichtet waren und 43 % der betroffenen Daten nicht wiederhergestellt werden konnten.

Die Wiederherstellung nach Ransomware-Angriffen ist eine Reihe von Maßnahmen, die Unternehmen ergreifen, um die Auswirkungen von Ransomware-Angriffen zu minimieren. Es ist immer ratsam, die Best Practices für den Schutz vor Ransomware zu befolgen. Als Präventivmaßnahme müssen Unternehmen unveränderliche Daten-Backups und Konfigurations-Snapshots implementieren, die es ihnen ermöglichen, ihre Systeme wiederherzustellen.

Die erfolgreiche Wiederherstellung nach Ransomware-Angriffen hängt zu einem großen Teil von der Effektivität der Backup- und Datensicherungsprozesse des Unternehmens und dem Plan für die Reaktion auf Vorfälle ab.

Ransomware-Angriffe verstehen

Bei Ransomware-Angriffen geht es nicht nur darum, Daten zu verschlüsseln und ein Lösegeld zu fordern. Bedrohungsakteure haben es oft auf Backup-Repositorys abgesehen, um eine schnelle Wiederherstellung zu verhindern, und in einigen Fällen löschen sie sogar Backups.

Ein wachsender Trend bei Ransomware-Angriffen ist die doppelte Erpressung, bei der Bedrohungsakteure Daten nicht nur verschlüsseln, sondern auch exfiltrieren. Wenn das Lösegeld nicht gezahlt wird, drohen sie damit, die gestohlenen Daten zu veröffentlichen. Diese Taktik erhöht den Druck auf Unternehmen, das Lösegeld zu zahlen, da die mögliche Preisgabe sensibler Unternehmens- und Kundendaten schwerwiegende Folgen haben kann.

Die finanziellen Auswirkungen eines Ransomware-Angriffs gehen über die Lösegeldzahlung hinaus und beeinträchtigen den Betrieb, den Umsatz und die Kunden. Laut dem Veeam-Report „Trends bei Ransomware“ 2024 entfallen nur 32 % der Kosten auf die Lösegeldzahlung, die restlichen 68 % auf andere finanzielle Auswirkungen auf Unternehmen.

32% der Kosten ist in der Regel die Lösegeldzahlung

68% ergeben sich aus anderen finanziellen Auswirkungen auf Unternehmen

Best Practices für die Wiederherstellung nach Ransomware-Angriffen

Es gibt viele gute Dokumentationen von Behörden und Regierungsorganisationen zum Thema Cybersicherheit. Sie alle bieten gute Unterstützung bei der Dokumentation und dem Monitoring.

Manchmal informieren lokale oder nationale Behörden Unternehmen darüber, dass sie die Verbreitung ihrer exfiltrierten Daten im Dark Web beobachten.

Es gibt verschiedene Dokumente mit Empfehlungen für verschiedene Branchen. Anstatt also nur diese Dokumentation oder Blueprints zu lesen, erfahren Sie in den folgenden Abschnitten mehr über praktische Erfahrungen und Ratschläge.

Es wird jedem dringend empfohlen, sich diese hilfreichen Unterstützungen und Dokumentationen von Organisationen anzusehen wie:

- **Australisches Zentrum für Cybersicherheit**
- **Kanadisches Zentrum für Cybersicherheit**
- **Bundesamt für Sicherheit in der Informationstechnik, Bundesrepublik Deutschland**
- **Nationales Zentrum für Cybersicherheit der Niederlande**
- **Nationales Zentrum für Cybersicherheit von Neuseeland**
- **Behörde für Internet und Sicherheit von Korea**
- **Nationale Cyber-Direktion Israels**
- **Nationales Zentrum für Störfallbereitschaft und Cybersicherheitsstrategie Japans**
- **Cybersicherheitsbehörde von Singapur**

Ransomware-Angriffe

Fangen wir mit den Grundlagen an: Was passiert bei einem Ransomware-Angriff? Es gibt mehrere Anzeichen dafür, dass ein Unternehmen angegriffen wird. Durch den Verlust des Zugriffs auf Systeme und Dateien merken die Mitarbeiter des Unternehmens, dass etwas nicht in Ordnung ist. In einigen Fällen können Bedrohungsakteure Bildschirme sperren, wie bei CryptoLocker, das eine Meldung auf Windows-Computern anzeigt. Dies geschieht jedoch nicht immer. Bei einer Datenexfiltration bemerkt das Unternehmen möglicherweise nicht, dass die Daten gestohlen werden. Alles läuft wie gewohnt weiter, bis eine Lösegeldforderung auftaucht. Manchmal ist die Lösegeldforderung nur eine der verschlüsselten Dateien, oder sie kommt in einer E-Mail.

Sofortige Reaktion

Bei einem Ransomware-Angriff ist die sofortige Reaktion entscheidend. Es ist wichtig, dass Sie ruhig bleiben und die Situation bewerten, bevor Sie etwas unternehmen. Eine zu schnelle Trennung der Systeme kann laufende Verschlüsselungsprozesse stören, was die Wiederherstellung noch schwieriger macht.

Bleiben Sie ruhig, geraten Sie nicht in Panik und suchen Sie nach Fachwissen. Arbeiten Sie dazu mit internen Experten zusammen oder wenden Sie sich an einen externen Experten. Sprechen Sie immer mit Ihrer Rechtsabteilung, insbesondere über die Lösegeldforderung und darüber, ob Sie eine Cyberversicherung abgeschlossen haben. Informieren Sie das Cyberversicherungsunternehmen über den Angriff.

In einigen Fällen enthielt ein Teil der verschlüsselten Dateien die Cyber-Versicherungspolice. Es ist wichtig, Backups zu haben, und zwar eine entsprechende Richtlinie an mehreren Orten und mit mehreren Backups. Dies ist der richtige Zeitpunkt, um die zuvor eingerichteten Kommunikationskanäle mit allen Stakeholdern im Unternehmen zu aktivieren.

Eindämmung

Mobilisieren Sie das Reaktionsteam, einschließlich der Forensik, und konzentrieren Sie sich auf die Eindämmung. Die erste Empfehlung lautet, alle Artefakte zu sammeln, einschließlich Lösegeldforderungen, Muster verschlüsselter Dateien und jeglicher Malware oder ausführbarer Dateien, die an der Verschlüsselung oder Datenübertragung beteiligt waren. Diese Daten sollten dann von dem Team analysiert werden. Das Hauptaugenmerk sollte auf der Eindämmung und dem Bewahren der Ruhe liegen.

Zu den wichtigsten Schritte für die anfängliche Eindämmung gehören:

- Identifizierung der betroffenen Systeme und Daten
- Ändern von Administrator-Passwörtern
- Isolieren der Endpunkte
- Kenntnis der RTOs und RPOs
- Interne Kommunikation
- Überprüfung der Versicherungspolice

Mehrere Zonen und eine gut verteilte Architektur machen es einfacher, betroffene Systeme zu isolieren.

Bewertung

Der nächste Schritt ist die Bewertung der betroffenen Systeme und Dateien. Bestimmen Sie die Art der Verschlüsselung und die verwendeten Dateierweiterungen. In einigen Fällen werden die Dateien nicht wirklich verschlüsselt, sondern lediglich umbenannt, sodass sie nicht mehr zugänglich sind.

Die Bedrohungsakteure verfügen über unterschiedliche Fachkenntnisse, von professionellen Organisationen und erfahrenen Einzelkämpfern bis hin zu neuen und unbedarften Akteuren. Konzentrieren Sie sich auf die Auswertung Ihrer Backups und stellen Sie sicher, dass diese sauber und frei von Malware sind. Bewerten Sie die für die Wiederherstellung benötigte Zeit. Fachkundige Unterstützung, z. B. von Coveware by Veeam, kann die Prognose der Wiederherstellung auf der Grundlage einer vollständigen Bewertung aller zuvor genannten Artefakte erleichtern.

Verhandlung mit Bedrohungsakteuren

Mit Bedrohungsakteuren in Kontakt zu treten, bedeutet nicht unbedingt, das Lösegeld zu bezahlen. Dies kann eine Gelegenheit sein, wertvolle Informationen darüber zu erhalten, wie der Angriff erfolgte. Einige Bedrohungsakteure können detaillierte Informationen über die von ihnen ausgenutzten Schwachstellen bereitstellen. Gehen Sie jedoch davon aus, dass jede Kommunikation öffentlich gemacht werden könnte, bleiben Sie also professionell.

Selbst wenn beide Parteien zustimmen, gibt es keine Garantie dafür, dass die Entschlüsselungsschlüssel zur Verfügung gestellt werden oder dass die exfiltrierten Daten gelöscht werden. Die Erfahrung lehrt, dass viele Gruppen von Bedrohungsakteuren auf ihren Ruf bedacht sind und möglicherweise fair verhandeln, um diesen zu wahren. Einige Gruppen stellen jedoch möglicherweise keine geeigneten Entschlüsselungstools oder -schlüssel zur Verfügung, sodass die Entschlüsselung selbst dann schwierig ist, wenn der Bedrohungsakteur das Tool und die Schlüssel zur Verfügung gestellt hat. Denken Sie daran, dass dies ein langwieriger Prozess sein könnte, den Sie während der Verhandlungen für Ihre Wiederherstellungsbemühungen nutzen können.

Wiederherstellung

Wenn es um die Wiederherstellung geht, ist es ideal, saubere Backups zu haben. Es ist jedoch auch wichtig, die für die Wiederherstellung benötigte Zeit zu bewerten. Überlegen Sie, wie viel Zeit Sie für den Betrieb haben, wie viele Daten Sie sich leisten können, zu verlieren, und andere Faktoren. Je nach Situation müssen einige Systeme neu aufgebaut werden, und manchmal müssen sogar die Daten selbst neu aufgebaut werden. Dieser Prozess kann einige Tage bis mehrere Wochen dauern.

Ein wichtiger Ratschlag ist, die Priorisierung der Daten zu dokumentieren, ähnlich wie bei Playbooks für die Wiederherstellung und Reaktion auf Vorfälle. Priorisieren Sie, was zuerst wiederhergestellt werden muss. In einigen Fällen kann es sein, dass während der Verhandlungen die Entscheidung getroffen wird, nur die digitalen Vermögenswerte mit der höchsten Priorität wiederherzustellen, während andere Daten verloren gehen können. Es ist wichtig, dass Sie wissen, was höchste Priorität hat und was zuerst wiederhergestellt werden muss. Bestimmen Sie, was kritisch genug ist, um für Entschlüsselungsschlüssel zu bezahlen, da die Wiederherstellung dieser kritischen Teile zuerst die Wiederherstellung des Rests später ermöglicht. Bei diesem Schritt gibt es viele Dinge zu beachten.

Daten aus Veeam-Backups wiederherstellen

Mit der Veeam Data Platform haben Sie bei der Wiederherstellung die Wahl zwischen der Wiederherstellung auf ursprünglichen Servern oder in isolierten Reinräumen. Diese zweite Option bietet die Möglichkeit, in einer isolierten Umgebung die Wiederherstellung zu bereinigen, zu überprüfen und zu testen.

Die Veeam Data Platform bietet eine Vielzahl von Wiederherstellungsoptionen, um die Datenresilienz und Wiederherstellung in verschiedenen Umgebungen zu gewährleisten. Hier finden Sie einige Optionen:

VM-Wiederherstellung:
Dies ermöglicht das Wiederherstellen ganzer virtueller Maschinen in verschiedenen Datensicherungsumgebungen wie VMware vSphere, Hyper-V, Azure und Amazon EC2.

Festplattenwiederherstellung:
Wiederherstellen und Exportieren von Festplatten aus Backups.

Objektwiederherstellung:
Dazu gehört die Wiederherstellung von VM-Dateien, Gastbetriebssystemdateien und -ordnern sowie Anwendungsobjekten.

Wiederherstellung auf Dateiebene:
Ermöglicht die granulare Wiederherstellung einzelner Dateien und Ordner aus Backups.

Plattformübergreifende Wiederherstellung:
Unterstützt die Wiederherstellung über mehrere Plattformen hinweg, darunter VMware, Hyper-V, AWS, Azure und Google Cloud.

Quick Rollback:
Ermöglicht die schnelle Wiederherstellung, indem nur die seit dem letzten Backup geänderten Blöcke wiederhergestellt werden.

Cloud-Plattformen:
Bietet umfassende Wiederherstellungsoptionen für die wichtigsten Public Clouds, mit speziellen Schritten für die Wiederherstellung von Amazon EC2-Instanzen und Microsoft Azure-VMs.

Orchestrierung in jedem Umfang und Veeam-Support:
Umfangreiche Wiederherstellungen können orchestriert werden für Premium-Benutzer der Veeam Data Platform.

Entscheidung zur Zahlung des Lösegelds

Die Entscheidung, ob Lösegeld gezahlt wird, sollte basierend auf einer umfassenden Bewertung möglicher Auswirkungen getroffen werden, darunter:

- Auswirkungen auf Leben und Sicherheit
- Beeinträchtigung des Geschäftsbetriebs
- Finanzielle Auswirkungen
- Auswirkungen auf den Umsatz
- Auswirkungen auf Enduser oder Kunden
- Auswirkungen auf den Ruf
- Dauer der Wiederherstellung

In Branchen wie dem Gesundheitswesen kann die Entscheidung eine Frage von Leben oder Sicherheit sein. Auch das Regierungssystem und das öffentliche Schulsystem sind wegen der Auswirkungen auf Enduser ein häufiges Ziel.

Zahlen Sie das Lösegeld erst, wenn Sie sich vergewissert haben, dass alles eingedämmt und gesichert ist. Schöpfen Sie zunächst alle Wiederherstellungsoptionen des Backups aus. Benachrichtigen Sie die Strafverfolgungsbehörden und halten Sie die Branchenvorschriften ein.

Fachkundige Reaktion auf Vorfälle

Während eines Ransomware-Ereignisses ist eine fachkundige Reaktion auf Vorfälle entscheidend, um die Bedrohung einzudämmen, Störungen zu minimieren und wichtige Entscheidungen zu treffen. Unternehmen für digitale Forensik und Reaktion auf Vorfälle (Digital Forensics and Incident Response, DFIR) identifizieren Angriffsvektoren, bewerten den Umfang der Kompromittierung und stellen Systeme wieder her, während sie forensische Beweise sichern. Ransomware-Verhandlungsführer verhandeln mit den Bedrohungsakteuren, analysieren die Forderungen und beraten über Zahlungsstrategien, um die finanziellen und rufschädigenden Auswirkungen zu verringern.

Experten wie Coveware by Veeam führen zunächst eine schnelle Folgenabschätzung durch, um das Ausmaß eines Angriffs abzuschätzen, die betroffenen Systeme zu identifizieren und die Folgen zu prognostizieren — der Schlüssel zur Gestaltung der Reaktionsstrategie und zur Risikominderung. Es folgt eine forensische Analyse, bei der Angriffsmethoden, ausgeführte Aktionen und verdächtige Aktivitäten identifiziert werden. Die Zuordnung von Bedrohungsakteuren anhand von Taktiken, Techniken und Verfahren (TTPs) unterstützt Sie dabei, Eskalationsrisiken vorherzusagen, die Datenexfiltration zu bewerten und die Einhaltung von Sanktionen und behördlichen Beschränkungen zu gewährleisten, um rechtliche und finanzielle Risiken zu verringern.

Die Verschlüsselungsüberprüfung durch Recon stellt die Integrität der Ransomware fest und bewertet mögliche Wiederherstellungsoptionen wie die Verfügbarkeit von Entschlüsselungsprogrammen oder ausnutzbare Schwachstellen, bevor Verhandlungen aufgenommen werden. Der Einsatz von Reverse Engineers von Weltrang verbessert die Wiederherstellungsbemühungen noch weiter, indem sie die Integrität der Verschlüsselung bewerten und, wenn möglich, die Entschlüsselung unterstützen, sodass Unternehmen den Betrieb zuverlässig wiederherstellen können.

Die Verhandlung dient strategischen Zwecken, die über die Lösegelddiskussion hinausgehen. Sie liefert Informationen über exfiltrierte Daten, Entschlüsselungsfunktionalitäten und die Absichten Ihrer Gegner. Auch ohne Bezahlung können Sie dabei Zeit für die Wiederherstellung des Systems, forensische Analyse und Compliance-Reporting gewinnen. Erfahrene Verhandlungsführer nutzen frühere Auseinandersetzungen mit Bedrohungsgruppen, um die Glaubwürdigkeit von Forderungen einzuschätzen, auf Zugeständnisse zu drängen und festzustellen, ob ein Bedrohungsakteur wahrscheinlich ein funktionierendes Entschlüsselungsprogramm bereitstellen oder die Datenunterdrückung akzeptieren wird.

Eine effektive Reaktion nach Ransomware-Angriffen hängt von einer schnellen Bewertung, forensischer Analyse und strategischer Verhandlung ab. Durch die Nutzung früherer Fallerfahrungen, forensischer Hilfsmittel und Erkenntnisse über den Gegner unterstützen die Experten Unternehmen dabei, fundierte Entscheidungen zu treffen und gleichzeitig das Risiko zu minimieren. Coveware by Veeam bietet das Know-how, um die Krise zu bewältigen, den Betrieb wiederherzustellen und die Wiederherstellung zuverlässig zu unterstützen.

Abschließende Gedanken

Nach einem Ransomware-Angriff ist es wichtig, die daraus gezogenen Lehren zu dokumentieren. Dieser Prozess ermöglicht eine kontinuierliche Verbesserung der Prozesse, die Aktualisierung der Pläne und die Verfeinerung der Verfahren. Die Weitergabe dieser Erkenntnisse ist ebenso wichtig. Die interne und externe Verbreitung von Informationen durch Whitepapers, Blogs, Webinare und die Zusammenarbeit mit Cybersicherheitsorganisationen kommt allen zugute.

Die Cybersicherheitslandschaft bietet eine breite Palette von Tools und Software für mehrere Schutzschichten. Die Verwendung von Sicherheitstools, die Implementierung von Multifaktorauthentifizierung (MFA) und die Einhaltung des Prinzips der geringsten Rechte sind wesentliche Strategien zur Verhinderung von Angriffen. Selbst wenn ein Unternehmen kompromittiert wurde, können diese Maßnahmen die seitliche Bewegung innerhalb von Netzwerken und Systemen verhindern. Bei der seitlichen Bewegung geht es darum, den optimalen Pfad oder Standort für die Ausführung eines Angriffs zu finden, insbesondere im Hinblick auf Verschlüsselungs-, Befehls- und Steuerungs- sowie Datenexfiltrationstechniken.

Die Unterstützung durch professionelle Experten für die Reaktion auf Vorfälle macht einen Unterschied aus. Wenn die Finanzen und der Ruf der Organisation auf dem Spiel stehen, holen Sie sich die Unterstützung der Experten.

Schließlich müssen Unternehmen ihre Pläne und Verfahren für die Reaktion auf Vorfälle sowie die Wiederherstellung von Backups testen, da dies entscheidend ist, um auf künftige Angriffe vorbereitet zu sein und die Resilienz zu gewährleisten.

Weitere Informationen: veeam.com

Über Veeam Software

Veeam®, der Weltmarktführer im Bereich Datenresilienz, ist der Ansicht, dass jedes Unternehmen nach einer Unterbrechung des Geschäftsbetriebs in der Lage sein sollte, den Betrieb mit Gewissheit und der Kontrolle über alle seine Daten wieder aufzunehmen, wann und wo immer diese benötigt werden. Veeam nennt dies maximale Ausfallsicherheit, und wir arbeiten kontinuierlich daran, innovative Lösungen zu entwickeln, mit denen unsere Kunden diese Zielvorgabe erreichen. Die Lösungen von Veeam sind speziell darauf ausgerichtet, die Datenresilienz durch Daten-Backup, Datenwiederherstellung, Datenportabilität, Datensicherheit und Datenintelligenz zu erhöhen. Mit Veeam können Verantwortliche im IT- und Sicherheitsbereich darauf vertrauen, dass ihre Anwendungen und Daten in allen Umgebungen in der Cloud, ob virtuell, physisch, SaaS oder Kubernetes, sicher und jederzeit verfügbar sind. Veeam hat seinen Hauptsitz in Seattle und ist mit Niederlassungen in mehr als 30 Ländern vertreten. Weltweit hat Veeam mehr als 550.000 Kunden, darunter 68 % der Global 2000-Unternehmen, die auf Veeam vertrauen, um einen zuverlässigen Geschäftsbetrieb zu gewährleisten. Maximale Ausfallsicherheit beginnt mit Veeam. Erfahren Sie mehr unter www.veeam.com/de oder folgen Sie Veeam auf LinkedIn @veeam-software und X @veeam.