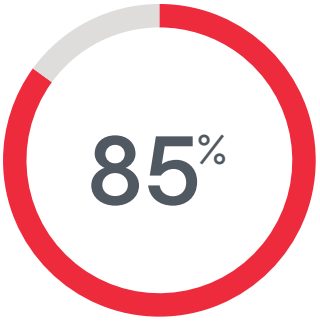
Eine Strategie für Datenwiederherstellung, die Schutz vor Cyberangriffen bietet

Inhalt

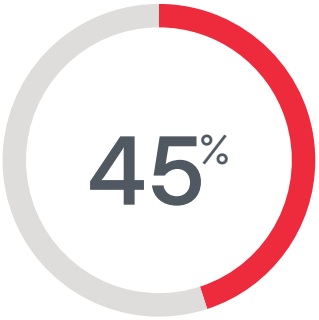
Einführung

Datensicherheit steht bei der Strategie eines jeden Unternehmens an erster Stelle, denn die Bedrohung durch Cyberangriffe, vor allem durch Ransomware, stellt eine eindeutige und allgegenwärtige Gefahr dar. Leider haben 85 % der Unternehmen im Jahr 2022 mindestens einen Ransomware-Angriff erlebt (Veeam Data Protection Trends Report 2023). Besonders besorgniserregend ist die Tatsache, dass moderne Ransomware Unternehmen nicht nur den Zugriff auf ihre Daten verwehrt, sondern die Daten auch ausschleust oder stiehlt, um sie zu verkaufen, für künftige Angriffe zu nutzen oder im Rahmen eines oder mehrerer Erpressungsversuche zu verwenden.

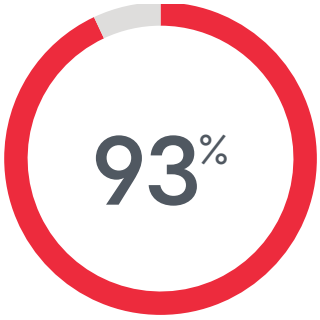
Den böswilligen Zugriff auf diese Daten zu verhindern, sollte das oberste Ziel eines jeden Cybersicherheitsprogramms sein. Allerdings sollte kein Unternehmen davon ausgehen, dass seine Schutzmaßnahmen immer ausreichen. Daher ist die Fähigkeit zur Datenwiederherstellung als letzte Verteidigungslinie genauso wichtig. Unternehmen, die Opfer von Ransomware wurden, haben durchschnittlich 15 % ihrer Produktionsdaten verloren (Veeam Ransomware Trends Report 2023). Dies zeigt, wie wichtig ein gut durchdachter und zuverlässiger Plan zur Datenwiederherstellung ist.



der Organisationen wurden von einem Ransomware-Angriff im Jahr 2023* betroffen



der Produktionsdaten waren von Cyberangriffen betroffen*.



der Ransomware-Angriffe gezielte Backups*

Quelle: 2023 Ransomware Trends Report von Veeam

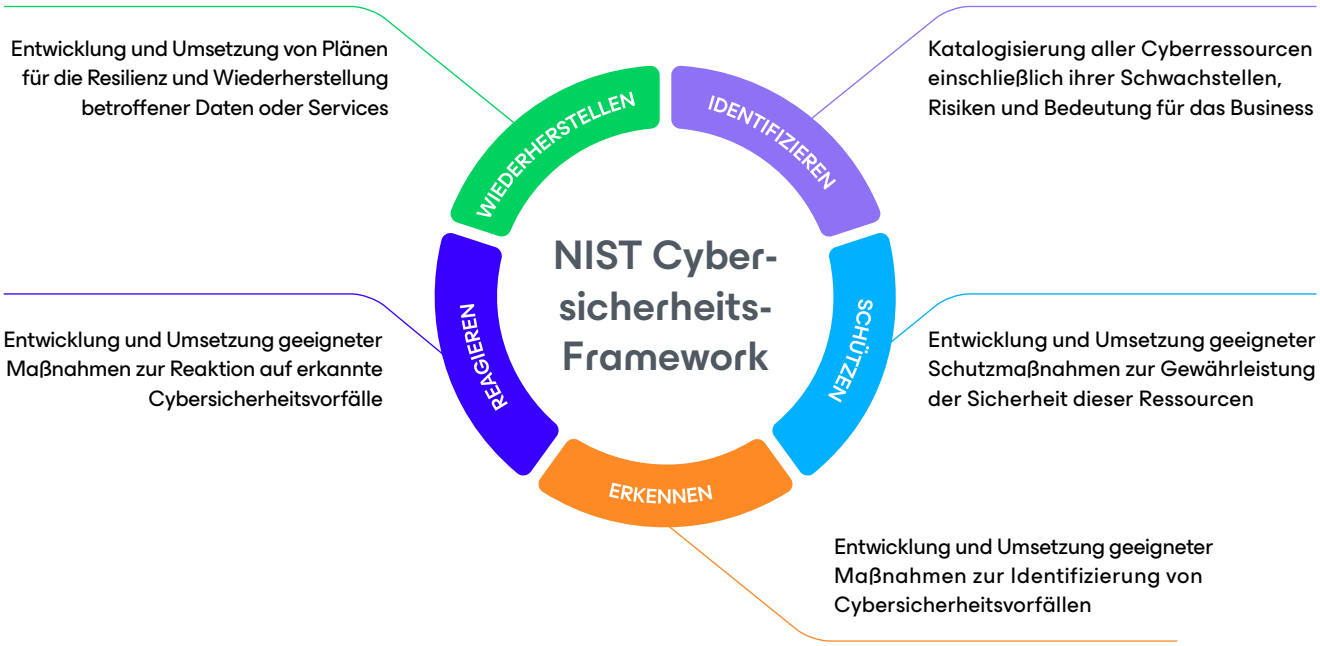
Eine Grundlage für zuverlässige Datenwiederherstellung

Die Datenwiederherstellung als Teil einer Datenverfügbarkeitsstrategie ist oft der letzte Baustein eines Cybersicherheitsplans und muss daher gut durchdacht und geplant sein. Konzepte wie eine 3-2-1-1-0-Datensicherungsstrategie und der Einsatz eines einzelnen Tools, mit dem Daten in der gesamten Infrastruktur gesichert und bei Bedarf nach einem Cybervorfall wiederhergestellt werden können, verschaffen Unternehmen die nötigen Voraussetzungen, um Daten in jeder Situation wiederherstellen zu können.

Veeam-Kunden können dieses Ziel mit der Veeam Data Platform erreichen und Daten sicher, orchestriert und gut dokumentiert wiederherstellen. Mithilfe der gesamten Suite, einschließlich Veeam Backup & Replication, Veeam ONE und Veeam Recovery Orchestrator, können Kunden Ziele im Bereich der Datensicherheit erreichen, die sich an allen Stufen des NIST Cybersecurity Framework orientieren und weit über Datensicherung und Wiederherstellung hinausgehen.

Ein gängiges Framework für die Planung der Cybersicherheit

Das NIST Cybersecurity Framework ist ein bewährtes Rahmenwerk, mit dem Unternehmen ihr Cybersicherheitsprogramm verbessern können. Das Framework ist in eine wiederholbare Reihe von Phasen und Funktionen gegliedert, die auf verschiedene IT- und Geschäftsprozesse angewendet werden können, und soll Unternehmen Orientierungshilfe beim Umgang mit Cybersicherheitsrisiken bieten.



Software zur Sicherstellung der Datenverfügbarkeit ist zwar eine Schlüsselkomponente der Wiederherstellungsphase des NIST Cybersecurity Framework, aber meistens wird diese nicht unbedingt in den anderen Phasen eines Cybersicherheitsprogramms eingesetzt. Veeam ist seit vielen Jahren bestrebt, seine Stellung als Datensicherungsplattform für Unternehmen zu nutzen, um seine Kunden optimal mit den Informationen auszustatten, die sie zum Schutz ihrer Daten benötigen.

IT-Organisationen, Sicherheitsteams und verantwortliche Entscheidungsträger erhalten in diesem Dokument auf dem NIST Cybersecurity Framework basierende Einblicke und Kenntnisse, um mithilfe der Veeam Data Platform eine weitere umfangreiche Informationsquelle und Fähigkeiten bereitzustellen, die bei der Identifizierung kritischer Daten, der Erkennung von Malware, dem Schutz von Daten, der schnellen Reaktion auf aktive Bedrohungen und der raschen Wiederherstellung von sauberen Daten helfen.

Identifizierung kritischer Daten

Wie bei jeder Katastrophe, die ein Unternehmen erleiden kann, ist die Planung das A und O. Die Cybersicherheit hat mit der traditionellen Notfallwiederherstellung ein zentrales Leitprinzip gemeinsam: **Man kann nicht schützen, wovon man nichts weiß**. Die Katalogisierung und Kategorisierung schützenswerter Assets mag im Vergleich zum aktiven Schutz vor und zur Reaktion auf eine Cybersicherheitsbedrohung unerheblich erscheinen. Aber zu wissen, welche Ressourcen gefährdet sind und welche Priorität sie haben, ist der erste Schritt. Mit den folgenden Funktionalitäten kann Veeam ein wichtiger Bestandteil einer mehrstufigen Strategie zur **Identifizierung** kritischer Daten sein.

Katalogisierung kritischer Systeme und Daten

Voraussetzung für die Erstellung eines zuverlässigen Wiederherstellungsplans ist die enge Zusammenarbeit von IT und Sicherheit mit dem Unternehmen: Alle im Unternehmen vorhandenen Workloads und Daten müssen identifiziert, katalogisiert und priorisiert werden. Ein guter Ausgangspunkt dafür sind die in Veeam ONE verfügbaren Berichte und der Katalog der von Veeam Backup & Replication gesicherten Systeme. Alle kritischen Daten sollten gesichert werden und Veeam kann aufzeigen, ob es virtuelle Maschinen oder Daten gibt, die nicht geschützt werden.

In ähnlicher Weise kann mit den vom Sicherheitsteam verwendeten Netzwerk- und Sicherheitstools eine Liste der Systeme in der Umgebung erstellt werden. Durch den Vergleich dieser verschiedenen Systeme wird oft deutlich, wo Daten in den einzelnen Tools nicht ordnungsgemäß geschützt sind. So wird sichergestellt, dass die Schutz- und Wiederherstellungspläne so vollständig wie möglich sind.

Identifizierung und Priorisierung von Daten durch Tagging und Klassifizierung

Mithilfe der Funktionen für Tagging und Datenklassifizierung in Veeam Backup & Replication können Kunden mit einem bestehenden Katalog von Workloads — ihren Backups — beginnen und Tags zur Identifizierung von System-Metadaten wie Standort, Eigentümer und Wiederherstellungspriorität anwenden. Dabei werden manchmal fehlende Daten, die auf eine Datenschutzlücke hinweisen, sowie wichtige Metadaten ermittelt, die für eine ordnungsgemäße Planung der Datenwiederherstellung erforderlich sind.

Sobald die Metadaten angewendet wurden, kann die assistentengestützte Wiederherstellungsplanung in Veeam Recovery Orchestrator genutzt werden, wodurch der Zeitaufwand für die Erstellung des Plans reduziert wird. Dieser Plan kann dann gemeinsam mit dem Unternehmen überprüft werden, um sicherzustellen, dass er den Anforderungen des Unternehmens entspricht und alle wichtigen Aspekte berücksichtigt.

Hervorheben von Lücken und Änderungen durch automatisierte Wiederherstellungstests

Die zuverlässigste Methode, um festzustellen, ob ein Backup oder ein Plan im Notfall einsatzbereit ist, besteht darin, beide zu testen. Die Funktionen für automatisierte Tests von Veeam Recovery Orchestrator stellen einen großen Vorteil dar, wenn es darum geht, die vollständige Wiederherstellbarkeit der gesamten oder eines Teils der Infrastruktur sicherzustellen. Neben dem offensichtlichen Vorteil der Arbeitsersparnis bei der Testdurchführung können durch eine Automatisierung des Testwiederherstellungsprozesses auch häufigere Tests durchgeführt werden. So werden Schwachstellen schneller aufgedeckt.

Eine der Schwachstellen, die durch häufige Tests aufgedeckt werden können, besteht darin, dass Systeme nicht gesichert werden oder in den Plänen nicht berücksichtigt wurden. Durch die regelmäßige Überprüfung dieser Testergebnisse und die rasche Behebung etwaiger Lücken wird das Wissen darüber erweitert, welche Assets geschützt werden müssen.

Schutz der Backup-Infrastruktur und der Daten

Die Backup-Infrastruktur nimmt in jeder IT-Umgebung einen besonderen Platz ein. Sie bildet nicht nur das letzte Sicherheitsnetz der Datensicherheit, sondern enthält auch mehrere Kopien aller Daten — je kritischer, desto mehr Kopien — einschließlich der Daten, die in der Produktion gelöscht worden sein könnten. Das macht sie zu einem attraktiven Ziel für Kriminelle, die Daten stehlen und das Sicherheitsnetz beseitigen wollen, um den Erfolg ihrer Lösegeld- und Erpressungsaktionen zu steigern. Daher ist es besonders wichtig, die Backup-Infrastruktur selbst zu **schützen**.

Eine Backup-Infrastruktur, die niemandem vertraut

Der erste Schritt zum Schutz von Backups besteht darin, unbefugten Zugriff auf das Backup-Management-System selbst zu verhindern. Die Prinzipien von Zero Trust — explizite Verifizierung, Annahme eines Verstoßes und Zugriff mit minimalen Rechten — sollten angewandt werden, um ein Eindringen in die Backup-Infrastruktur so schwierig wie möglich zu gestalten.

Durch die Verwendung von Multifaktorauthentifizierung und ein separates, dediziertes Identitäts- und Zugriffsmanagementsystem (IAM) für die Datensicherung zur Kontrolle der Benutzerrichtlinien wird sichergestellt, dass die Benutzer ordnungsgemäß verifiziert werden und nicht so leicht zu manipulieren sind. Durch die Einführung eines Zugriffs mit minimalen Rechten, z. B. durch getrennte Verwaltungs- und Betriebskonten, werden unbeabsichtigte Fehler vermieden und die Ausweitung von Rechten wird minimiert. Außerdem sollte die gesamte Konfiguration unter der Annahme erfolgen, dass der Rest der Infrastruktur bereits kompromittiert wurde. Dazu werden die Backup-Komponenten in einem separaten Netzwerk isoliert und der Zugriff auf die Veeam Backup & Replication-Konsole selbst über ein VPN oder eine Remote-Verbindung eingeschränkt.

Diese Ansätze sollten auf jeder Ebene der Sicherungsinfrastruktur berücksichtigt werden, können aber auf jeder Ebene etwas anders aussehen. Betriebssysteme, Dateifreigaben, Out-of-Band-Verwaltung und alle anderen Anwendungen, die zu deren Verwaltung eingesetzt werden, sollten ähnlichen Grundsätzen folgen.

Analysieren der Compliance Ihrer Backup-Infrastruktur

Um Kunden bei der ordnungsgemäßen Anwendung der Zero Trust-Prinzipien zu unterstützen, verfügt die Veeam Backup & Replication-Konsole über ein integriertes Dienstprogramm namens Security & Compliance Analyzer (früher Best Practices Analyzer genannt), das die Veeam-Infrastruktur analysiert und Berichte zu Konfigurationselementen erstellt, die nicht gemäß den Empfehlungen von Veeam implementiert wurden. Diese Analyse sollte regelmäßig durchgeführt werden und alle Mängel sollten entweder korrigiert oder ignoriert werden. Bei ignorierten Elementen wird protokolliert, wann und von wem sie ignoriert wurden. Nach Abschluss der Fehlerbehebung sollte die Analyse noch einmal ausgeführt werden, wobei die Ergebnisse dokumentiert werden.

Sicherstellung der Verfügbarkeit von Backups

Das Löschen von Backups, sodass die Daten nicht wiederhergestellt werden können, ist inzwischen ein gängiges Merkmal von Ransomware. Daher ist es wichtig sicherzustellen, dass Backups nicht geändert oder gelöscht werden können.

Unveränderlichkeit ist ein sehr altes Konzept in der Informatik, das in letzter Zeit zu einem wichtigen Merkmal von Backups geworden ist, insbesondere von solchen, die unverändert oder fehlerfrei bleiben müssen, um die Aufbewahrungsanforderungen zu erfüllen. Unter Verwendung von abgesicherten Repositories, Objektspeicher, Deduplizierungs-Appliances von Drittanbietern oder Band können Veeam-Backups in einem Zustand gespeichert werden, in dem nicht einmal Administratoren die Daten ändern oder löschen können. Wie bei jedem Sicherheitssystem gibt es oft Umgehungslösungen. Daher ist es wichtig, den gesamten Stack — bis hin zum Rechenzentrum — zu berücksichtigen, um sicherzustellen, dass diese Umgehungslösungen beseitigt oder streng kontrolliert werden.

Es gibt einen alten Witz in der Cybersicherheit: Das sicherste System ist das, das ausgeschaltet, vom Netz getrennt und in einem Raum untergebracht ist, zu dem niemand Zugang hat. Auch wenn der Witz völlig zutreffend ist, ist er doch lustig, weil ein solches System keine Existenzberechtigung hat. Wenn es um die Sicherheit von Backups geht, kann ein solches System allerdings sinnvoll sein. Solange ein offline gespeichertes Backup bei Bedarf zugänglich ist, ist die Wahrscheinlichkeit einer Manipulation hier am geringsten. Veeam bietet mehrere Optionen für diesen Air-Gap-Ansatz zur Speicherung von Backups. Diese reichen von Online-Systemen, die eine andere Authentifizierung erfordern, bis hin zum idealen Offline-Speicher: Band.

Man sollte sich aber niemals nur auf eine einzige Sicherheitsebene verlassen. Daher kann Veeam Backup & Replication für die Löschung von Backups eine Autorisierung nach dem „4-Augen-Prinzip“ aktivieren. Ähnlich wie bei dem alten Zwei-Schlüssel-Prinzip beim Atomwaffeneinsatz muss das Löschen eines Backups bei dieser Konfiguration von zwei Administratoren autorisiert werden, damit Backups nicht versehentlich oder böswillig gelöscht werden.

Zero-Trust-Sicherheitsmodell

Mit dem Konzept des „Zero Trust“ soll das inhärente Vertrauen vermieden werden, das traditionell innerhalb der Umgebungssicherheit besteht, um so zu verhindern, dass sich Bedrohungen in einer Umgebung ungestört bewegen können. Nach dem Motto „Niemals vertrauen, immer prüfen“ wird ein Sicherheitsmodell ohne Perimeter geschaffen, bei dem nicht angenommen wird, dass Cyberbedrohungen von der Firewall aufgehalten werden. Bei diesem Modell sollte jedes System jede neue Interaktion überprüfen und nicht davon ausgehen, dass sie sicher ist.

Die drei Prinzipien des Zero-Trust-Sicherheitsmodells sind folgende:

1. explizite Verifizierung
2. Zugriff mit minimalen Rechten
3. Annahme eines Verstoßes

Verschlüsseln Ihrer eigenen Backups

Um Daten nach der Ausschleusung vor Missbrauch zu schützen, können Backups von Veeam verschlüsselt werden, damit niemand außerhalb der Veeam-Infrastruktur auf sie zugreifen kann. So lässt sich zwar nicht verhindern, dass die Daten über Ransomware entwendet oder gesperrt werden, aber es ist sehr unwahrscheinlich, dass die Daten für Erpressungen missbraucht werden können. Diese Verschlüsselung kann intern in Veeam verwaltet oder mit einem Schlüsselverwaltungssystem (KMS) eines Drittanbieters verknüpft werden, um die Verwaltung dieser Schlüssel auszulagern und zu zentralisieren.

Erkennen von Cyberbedrohungen

Sobald die gesamte System- und Datenlandschaft identifiziert wurde, muss das Unternehmen Pläne und Systeme für die schnelle Erkennung von Eindringversuchen in diese Assets einrichten. Durch eine schnelle Erkennung werden die Verweildauer und die Auswirkungen der Bedrohung erheblich reduziert, was sich in der Regel in Geldverlusten widerspiegelt. Auch hierbei kann die Software von Veeam eine Schlüsselkomponente in einer mehrstufigen Strategie zur **Erkennung** von Cyberbedrohungen sein.

Sensibilisierung für abweichende Verhaltensweisen

Eine der wichtigsten Strategien bei Malware ist es, eine Entdeckung zu vermeiden, während die Rechte ausgeweitet werden und sich die Malware in der Umgebung seitwärts bewegt, um so viele Systeme wie möglich zu infizieren. Dazu nimmt sie möglicherweise jeweils nur geringfügige Änderungen vor, um unbemerkt zu bleiben. Außerdem sind die Ersteller von Malware mittlerweile geschickter darin, unsere Bemühungen zur Wiederherstellung der Daten, die sie zur Erpressung nutzen möchten, zu unterlaufen, und sind dazu übergegangen, Backups zu löschen, die Aufbewahrungszeiten für Backups zu verkürzen oder Backup-Jobs zu deaktivieren. Veeam kann diese Arten von abweichendem Verhalten durch verschiedene Alarme und Berichte in Veeam ONE erkennen und darauf hinweisen.

Scannen auf Malware während der Backup-Erstellung

Mithilfe integrierter Malware-Erkennung kann Veeam Backup & Replication Blöcke beim Durchlaufen der Veeam Proxy-Knoten auf Anzeichen für eine neue Verschlüsselung analysieren — ein wichtiger Indikator für aktive Malware. Der Index des Backups wird nach bösartigen Dateinamen und Signaturen durchsucht und entsprechende Backups werden als verdächtig gekennzeichnet.

Erkennen von Malware in Backups

Das SureBackup-Feature von Veeam Backup & Replication wurde ursprünglich entwickelt, um die Wiederherstellung und Validierung von Backups zu automatisieren und zu gewährleisten, dass sie wiederherstellbar sind. Da Software zur Endpoint Sicherung nicht immer perfekt ist und Malware nach wie vor in die Backups gelangen kann, verfügt SureBackup über eine Reihe zuverlässiger Funktionalitäten, mit denen Backups auf Malware überprüft werden können.

Im Rahmen eines Wiederherstellbarkeitstests kann SureBackup mithilfe von Tools zum Scannen von Malware die wiederhergestellte virtuelle Maschine scannen. Auf diese Weise können Unternehmen nach dem Prinzip „Trust but Verify“ ein zweites Tool zur Erkennung von Malware einsetzen. Ein weiterer Vorteil ist, dass die Produktions-Workloads durch den SureBackup-Scan nicht beeinträchtigt werden, sodass ein umfassenderer Scan möglich ist. SureBackup kann auch einzelne Festplatten auf einen Testrechner mounten, der dann die Dateien auf Malware scannen kann. Dies ermöglicht einen noch schnelleren und ressourceneffizienteren Malware-Scan, wenn eine vollständige Wiederherstellung nicht erforderlich ist.

Wenn bei diesen Scans etwas gefunden wird, wird der betreffende Wiederherstellungspunkt als verdächtig eingestuft.

Regelmäßiges Testen des Wiederherstellungsplans, um Gefährdungen zu erkennen

Auch hier kann ein regelmäßiges Testen der Wiederherstellungspläne für die Cybersicherheit nützlich sein, da dadurch die durch Malware verursachten Beschädigungen aufgezeigt werden. Fehler bei einem umfassenden Test des Wiederherstellungsplans, einschließlich einer Anwendungsüberprüfung, könnten auf Bereiche der Infrastruktur hinweisen, in denen eine Schlüsseldatei verschlüsselt oder eine Konfigurationsdatei auf unzulässige Weise geändert wurde. Dies könnte besonders nützlich sein, um Malware zu erkennen, die während einer Startsequenz ausgeführt wird.

Zentrale Protokollberichterstattung und Korrelation

Das Senden von Protokolldateien an einen externen Syslog-Dienst sorgt sowohl für ein sekundäres Repository von Protokollen als auch für eine Zentralisierung, die eine systemübergreifende Ereigniskorrelation ermöglicht. Für die meisten Sicherheitsteams ist das die wichtigste Funktion eines Security Incident and Events Manager (SIEM)-Systems. Durch die Einrichtung des SIEM-Systems als Syslog-Ziel können von Veeam entdeckte Hinweise auf eine Kompromittierung direkt in dem System erfasst werden, das vom Sicherheitsteam verwendet wird. Dadurch wird die Reaktionszeit verkürzt und die Sicherheitsanalysten erhalten einen zuverlässigeren Überblick über ein Ereignis.

Verweildauer

Die Verweildauer (wie lange sich die Malware in der Umgebung befindet, bevor sie entdeckt wird) ist die Zeit, in der sich die Malware in der Umgebung hält, ohne den primären Angriff auszuführen. In dieser Zeit kann sie weitere Konten kompromittieren, ihre Rechte ausweiten, sich tiefer in das Betriebssystem einbetten, sich seitlich auf andere Systeme ausbreiten und Informationen sammeln, die sie für aktuelle oder zukünftige Angriffe nutzen kann.

Externe Integrationen für Datensicherung

Die Incident API umfasst eine Reihe von Anwendungsprogrammierschnittstellen (APIs), anhand derer Cybersicherheits-Tools die Backup-Infrastruktur über eine entdeckte Infektion informieren und Backups als verdächtig oder infiziert kennzeichnen können. Veeam Backup & Recovery kann so konfiguriert werden, dass Administratoren auf Basis dieser Informationen gewarnt werden. So können sie Ereignisse schnell prüfen, verifizieren und darauf reagieren, wie z. B. mit der Erstellung eines sofortigen Backups, der Ausführung einer SureBackup-Aktion zur Überprüfung auf eine Infektion und Wiederherstellung sauberer Dateien sowie der Erstellung einer unveränderlichen Kopie eines Backups für Analysezwecke. Dieser offene Integrationspunkt zwischen den wichtigsten Sicherheitstools und der Datensicherungsplattform verbessert die Kommunikation erheblich, was die Verweildauer von Malware verringern kann und eine sauberere und schnellere Wiederherstellung ermöglicht.

Reaktion auf Cyberbedrohungen

Da ein 100%-iger Schutz nicht immer möglich ist, muss man sich auch darauf konzentrieren, Malware zu stoppen und so schnell wie möglich zu entfernen. Wie bei der Planung der Wiederherstellung nach einer Naturkatastrophe ist eines der wichtigsten Ziele, an dem sich alle Entscheidungen orientieren sollten, die RTO (Recovery Time Objectives, Wiederherstellungszeit). Bei einem Cybersicherheitsvorfall besteht ein ähnliches Ziel darin, die Malware zu stoppen und aus der Umgebung zu entfernen, damit die Systeme wieder in Betrieb genommen werden können. Wenn es gelingt, die Verweildauer der Malware zu verkürzen und Daten zu exfiltrieren, verringert sich der Bereinigungsaufwand und die Wiederherstellungszeit nimmt ab, weshalb es wichtig ist, eine schnelle **Reaktion** zu gewährleisten.

Verwendung von Backups für die Cyberforensik

Wie bereits erwähnt, ist SureBackup eine Funktion, die nicht nur die Wiederherstellbarkeit von Backups testet, sondern auch Malware erkennen kann. Eines der Ziele in der Reaktionsphase ist es, die Verweildauer zu ermitteln. Die Verwendung von Malware-Kennzeichnungen in der Veeam Backup & Replication-Konsole, die anzeigen, ob Malware in einem Wiederherstellungspunkt erkannt oder in diesem Zeitraum von einem Drittanbieter-Tool über die Incident API gefunden wurde, erleichtert die Suche nach dem ersten Infektionspunkt.

Secure Restore ist eine weitere Funktion von Veeam Backup & Replication, mit der Festplatten vor einer vollständigen Wiederherstellung gemountet und auf Malware gescannt werden können. Wird dieser Prozess wiederholt, bis ein nicht infizierter Punkt entdeckt wird, kann der Zeitpunkt des ersten Auftretens der Malware auf einem bestimmten System leichter ermittelt und eine erneute Infektion durch Wiederherstellung inaktiver Malware vermieden werden.

Mit Veeam Recovery Orchestrator kann dieser Secure Restore-Prozess für die gesamte Umgebung in einem orchestrierten „Clean Room"-Ansatz ausgeführt werden. Dies ermöglicht nicht nur eine schnellere Überprüfung auf saubere Wiederherstellungspunkte, sondern liefert auch schnell wertvolle Informationen für die digitale Forensik eines Cybersicherheitsvorfalls.

Ausschleusung

Wenn Malware auf Daten zugegriffen und diese modifiziert hat, dann hat sie diese vermutlich zuerst gestohlen. Ausgeschleuste Daten sind Daten, die aus der Umgebung des Opfers zurück an die Cyberkriminellen gesendet werden. Nach einer Sicherheitsverletzung könnten diese Informationen von Cyberkriminellen veröffentlicht oder verkauft werden, was dazu führen könnte, dass Firmengeheimnisse preisgegeben, der Ruf geschädigt und personenbezogene Daten gestohlen werden, die zu künftigen Betrugsfällen oder Cyberangriffen führen könnten.

Verbesserte Suche nach Bedrohungen mit YARA

YARA ist ein Tool, das Experten für Bedrohungen der Cybersicherheit bereits kennen: ein regelbasierter Ansatz zur Identifizierung und Klassifizierung von Malware. Als Teil eines SureBackup- oder SecureRestore-Vorgangs kann eine YARA-Regel festgelegt und ausgeführt werden — sowohl für die anfängliche Klassifizierung der Malware als auch für die anschließende Suche nach ihr in den Backups.

Vorfallsverfolgung mit ServiceNow

Durch die direkte Integration in ServiceNow kann Veeam automatisch neue Fälle erstellen und bestehende Fälle im Laufe der Entwicklung der Situation aktualisieren, sodass die verschiedenen Teams effizienter kommunizieren können und eine automatisierte Dokumentation des Vorfalls erstellt wird.

Besonders schnelle Wiederherstellung sicherer Daten

Je nach Art des Cybervorfalls ist die Wiederherstellung sauberer Daten entscheidend für die Wiederherstellung der Dienste, insbesondere bei Ransomware. Bei einer langen Verweildauer können viele Wiederherstellungspunkte Malware enthalten, sodass möglicherweise weit zurückgegangen werden muss, um einen sauberen Wiederherstellungspunkt zu finden. Wie bei der klassischen Disaster Recovery ist es wichtig, sich an den Zielen zur Minimierung von Datenverlusten zu orientieren — dem Recovery Point Objective (RPO). Da es in der Reaktionsphase wichtig ist, den Beginn der Infektion festzustellen, laufen viele dieser Bemühungen parallel zu den Bemühungen um die **Wiederherstellung** der Daten.

Ein Backup ist nur nützlich, wenn es wiederherstellbar (und frei von Malware) ist

Die Kennzeichnung verdächtiger oder infizierter Wiederherstellungspunkte in der Erkennungs- und Reaktionsphase durch Funktionen wie SureBackup und die Incident API macht es sehr einfach, direkt in der Veeam Backup & Replication-Konsole festzustellen, ob Malware in den einzelnen Wiederherstellungspunkten entdeckt wurde. Dies ist ein guter Ausgangspunkt, garantiert aber nicht, dass frühere Wiederherstellungspunkte komplett malwarefrei sind.

Um die Wahrscheinlichkeit zu verringern, dass infizierte Daten wiederhergestellt werden, und um doppelten Aufwand zu vermeiden, sollten die Aktivitäten zur Wiederherstellung Hand in Hand mit der Cyberforensik gehen, die in der Reaktionsphase stattfindet. Eine enge Zusammenarbeit zwischen IT, Sicherheit und Unternehmen ist wichtig, um die richtigen Daten wiederherzustellen und die erneute Einführung von Malware zu verhindern.

Bei Verwendung aktueller Malware-Erkennungstools im Zusammenhang mit SureBackup und Secure Restore kann in früheren Wiederherstellungspunkten bisher unentdeckte Malware gefunden werden. Daher ist es wichtig, sich nicht nur auf Malware-Kennzeichnungen aus früheren Scans zu verlassen. Wenn die sauberen Wiederherstellungspunkte weiter zurückliegen als die definierten RPOs, können einzelne wichtige Daten auf Dateiebene wiederhergestellt werden, wobei die Malware im vollständigen Backup vermieden wird.

Wiederherstellung der Cybersicherheit: Backups und Replikation im Vergleich

Die Replikation kann Teil eines Wiederherstellungsplans für die Cybersicherheit sein. Dazu sollte man jedoch wissen, welche Ziele mit der Replikation im Vergleich zu Backups verfolgt werden. Bei der Replikation liegt der Fokus darauf, Daten so schnell wie möglich zu verschieben und zum letzten sauberen Replikat zurückzukehren. Backups werden nicht fortlaufend erstellt, sodass bei der Sicherstellung von Sauberkeit und Wiederherstellbarkeit methodischer vorgegangen werden muss. Die Wiederherstellung der Cybersicherheit muss auf der Verweildauer und der Zuverlässigkeit des Wiederherstellungspunkts basieren, weshalb Backups häufiger zum Einsatz kommen.

Schnellstmögliche Wiederherstellung nicht infizierter Daten

Automatisierung ist zwar das A und O für eine schnelle Wiederherstellung selbst der einfachsten Umgebung, aber auch die Art der Wiederherstellung kann einen Unterschied machen. Mithilfe von Speicher-Array-Snapshots und Instant Recovery können wiederhergestellte Backups nahezu sofort genutzt werden.

Veeam Recovery Orchestrator wurde entwickelt, um den gesamten Wiederherstellungsprozess zu definieren und auf Knopfdruck auszuführen. Durch die Kombination des Wiederherstellungsplans mit Infektionskennzeichnungen, Secure Restore, Storage-Array-Snapshots, Instant Recovery und Anwendungsüberprüfung verfügt Veeam über eine sehr leistungsfähige Kombination von Funktionen, um Daten schnell und effizient wiederherzustellen und gleichzeitig sicherzustellen, dass die Daten so gut wie möglich frei von Malware sind.

Visualisieren von E/A-Anomalien

Ein Diagramm ist manchmal die beste Möglichkeit, Trends zu zeigen. Auf der Benutzeroberfläche von Veeam Backup & Replication werden bei der Wiederherstellung eines Replikations-Jobs Diagramme angezeigt, die Aufschluss über den Zeitpunkt des Beginns der Massenverschlüsselung geben, sodass schneller ein Zeitpunkt vor der Verschlüsselung gefunden werden kann.

Zusammenfassung

Die Erstellung eines Cybersicherheitsprogramms ist heutzutage keine leichte Aufgabe. Angesichts der hohen Anzahl von Bedrohungen und des potenziell enormen Gewinns, den Kriminelle aus einer Datenschutzverletzung ziehen können, müssen Unternehmen alle ihnen zur Verfügung stehenden Mittel nutzen, um Sicherheitsebenen zu schaffen und so ihre Effektivität auf jeder Stufe des NIST Cybersecurity Framework zu maximieren. Veeam kann in allen Phasen des NIST Cybersecurity Framework einen Mehrwert bieten und so das gesamte Cybersicherheitsprogramm des Unternehmens verbessern:

- Das Erstellen und regelmäßige Testen von Wiederherstellungsplänen kann wertvolle Daten liefern, mit denen sich in der **Identifizierungsphase** sicherstellen lässt, dass kritische Daten identifiziert und geschützt werden können.
- Durch die Implementierung dokumentierter Best Practices und nativer Sicherheitsfunktionalitäten wird sichergestellt, dass die Backups und die Backup-Infrastruktur in der **Schutzphase** berücksichtigt werden.
- Da Backups alle Daten in der gesamten Infrastruktur betreffen, können sie eine wichtige zweite Überprüfung auf Malware darstellen, die beim Monitoring von Endpunkten in der **Erkennungsphase** möglicherweise übersehen wurde.
- Ein schneller Zugriff auf verschiedene Zeitpunkte und virtuelle „Clean Room"-Umgebungen können für die Informationserfassung in der **Reaktionsphase** sehr wichtig sein.
- Sicherungen, die nachweislich wiederherstellbar und frei von Schadsoftware sind, stehen bei Bedarf zur Verfügung und können so schnell wie möglich in einen sauberen und brauchbaren Zustand wiederhergestellt werden, um die **Wiederherstellungsphase** zu unterstützen.

Es ist an der Zeit, dass IT-Teams nicht mehr nur wiederherstellbare Daten aufbewahren, sondern sich aktiv am Cybersicherheitsplan beteiligen. Dank der Informationen in diesem Dokument sollten IT-Teams nun in der Lage sein, ein produktives Gespräch mit Sicherheitsteams zu führen, um in das allgemeine Cybersicherheitsprogramm eine Veeam-basierte Datensicherungsplattform zu integrieren.

Weitere Informationen zu den Features, die in diesem Dokument erwähnt wurden, finden Sie in den Benutzerleitfäden, die im Veeam Help Center verfügbar sind. Viele dieser Features werden mit dem Veeam Data Platform 23H2 Update eingeführt.

Veeam Data Platform 23H2 Update
Kostenlose 30-Tage-Premium-Testversion