TANIUM

Der ultimative Leitfaden zur Abwehr von Ransomware

Verhindern von System-Lockdowns, Aufrechterhalten des operativen Betriebs und Reduzieren der Angriffswahrscheinlichkeit

TANIUM

Der ultimative Leitfaden zur Abwehr von Ransomware

Verhindern von System-Lockdowns, Aufrechterhalten des operativen Betriebs und Reduzieren der Angriffswahrscheinlichkeit

Inhalt

ZUSAMMENFASSUNG

Rechtzeitiges Handeln, bevor es zu spät ist

Ransomware ist zu einer der häufigsten und schwerwiegendsten Bedrohungen in der Cybersicherheitslandschaft geworden. Ransomware-Angriffe gehen mit höheren Kosten als andere Arten von Vorfällen einher, die Kosten und Frequenz dieser Angriffe steigen und jede Branche hat bekannte Vorfälle erlitten.

Alle Organisationen müssen sich jetzt als potenzielles Ziel für diese Bedrohung betrachten und eine effektive Verteidigung dagegen aufbauen, bevor es zu einem Vorfall kommt.

In diesem E-Book erfahren Sie, wie Sie genau das erreichen. Darin werden die folgenden Themen behandelt:

- Ein typischer Angriff durch eine Ransomware-Kampagne
- Die genauen Taktiken zur Verteidigung Ihres Unternehmen in jeder Phase einer Ransomware-Kampagne – vor, während, und nach dem Angriff
- Fünf Schritte, mit denen Sie so schnell wie möglich eine effektive Ransomware-Verteidigung aufbauen
- Die Rolle, welche die richtigen Tools bei einer effektiven Ransomware-Verteidigung spielen
- Weshalb veraltete Sicherheitstools in der Regel moderne Umgebungen nicht gegen Ransomware verteidigen können
- Wie Tanium die Fehler veralteter Tools korrigiert und welche Rolle diese Lösung beim Aufbau einer effektiven, effizienten – und schnellen – Verteidigung gegen Ransomware spielen kann
- Wie Tanium bei vielen Organisationen für effektive Sicherheit gesorgt hat
- Wie sich mit Tanium Ihre Ransomware-Verteidigung erweitern oder ausbauen lässt

Warum Sie Ransomware jetzt ernst nehmen sollten

Ransomware kommt Sie teurer zu stehen als andere Bedrohungen der Cybersicherheit.

Der jüngste Bericht des Ponemon Institute über die Kosten von Datenschutzverletzungen ergab, dass die durchschnittlichen Gesamtkosten eines Ransomware-Vorfalls um 250.000 USD höher waren als die durchschnittlichen Gesamtkosten einer Standardverletzung.[1]

4,27 Millionen USD

Durchschnittliche Gesamtkosten eines böswilligen Verstoßes.

4,52 Millionen USD

Durchschnittliche Gesamtkosten eines Ransomware-Verstoßes.

Ransomware ist mit immer höheren Kosten verbunden und die Angriffe treten häufiger auf.

Der jüngste Bericht des FBI zur Internetkriminalität ergab, dass Ransomware-Angriffe von 2018 bis 2019 häufiger wurden und größere Verluste verursachten.[2]

37 %

Jährliche Zunahme der gemeldeten Ransomware-Fälle

147 %

Jährlicher Anstieg der Verluste durch Ransomware-Angriffe

Darüber hinaus rechnet das Cybersecurity Magazine, dass sich die Rate der Ransomware-Angriffe in den letzten fünf Jahren mehr als verdreifacht und der geschätzte globale Schaden sich mehr als verdoppelt hat.[3]

Ransomware-Angriffsrate

40 Sekunden

Angriffsrate 2016

14 Sekunden

Angriffsrate 2019

11 Sekunden

Angriffsrate im Jahr 2021 (prognostiziert)

Weltweit geschätzter Schaden durch Ransomware-Angriffe

8 Milliarden USD

2018

11,5 Milliarden USD

2019

20 Milliarden USD

2021 (prognostiziert)

Ransomware wird in jeder Branche zu einem ernsthaften Problem.

In den letzten Jahren hatte jede Branche mit bekannten Verstößen durch Ransomware zu kämpfen.

Einige Beispiele:

- **Gesundheitswesen:** Im September 2020 schien eine Krankenhauskette mit 400 Standorten von dem größten Ransomware-Angriff im Gesundheitswesen in der US-Geschichte betroffen zu sein.[4]
- **Regierung:** Im Jahr 2019 erlitt die Stadt Baltimore einen Ransomware-Angriff, der mehr als 18 Millionen US-Dollar kostete und den Zugriff auf die Dienste der Stadtverwaltung unterbrach.[5]
- **Bildung:** Ransomware-Angriffe betrafen im Jahr 2020 mehr als 85 Hochschuleinrichtungen und störten den Betrieb von über 1.200 Schulen.[6]
- **Technologie:** Ein IT-Dienstleistungsunternehmen wurde 2020 von einem Maze-Ransomware-Angriff getroffen, dessen Gesamtauswirkungen sich voraussichtlich auf 50 bis 70 Millionen USD belaufen werden.[7]
- **Einzelhandel:** Im Dezember 2020 erlitt Kmart einen Ransomware-Angriff, der die Dienste mitten im Weihnachtsgeschäft störte.[8]

Niemand ist vor Ransomware sicher. Jede Organisation muss sich selbst als potenzielles Ziel sehen und effektive Abwehrmechanismen gegen dieses Angriffsmuster aufbauen, bevor sie zum nächsten großen Opfer wird. In diesem E-Book wird ein klarer, praktischer Weg zum Aufbau dieser Abwehrmaßnahmen beschrieben.

Wie sich Organisationen gegen Ransomware verteidigen können

Dieser Abschnitt beschreibt eine effektive Sicherheitsstrategie zur Bekämpfung von Ransomware und die Umsetzung dieser Strategie in der Praxis.

Darin wird Folgendes untersucht:

- Aussehen und Verlauf eines typischen Ransomware-Angriffs
- Taktiken für Organisationen, um Probleme mit Ransomware ohne Lösegeldzahlungen zu beheben
- Wie können Organisationen in fünf Schritten eine effektive Verteidigung gegen Ransomware aufbauen?

Ransomware im Detail: Ein Blick über die Lösegeldforderung hinaus

Oberflächlich betrachtet sieht ein Ransomware-Angriff recht einfach aus. Die Mitarbeiter einer Organisation versuchen, sich an ihrer Workstation anzumelden. Die Systeme sind gesperrt. Eine Anmeldung ist nicht möglich. Stattdessen wird eine Nachricht angezeigt.

Die Nachricht stammt von einem Angreifer und weist die Organisation an, ein Lösegeld für die Wiederherstellung des Systems und der gespeicherten Daten zu bezahlen. Die Organisation bezahlt entweder das Lösegeld oder vertreibt den Angreifer, und der Angriff ist vorbei. Diese Beschreibung trifft größtenteils zu, ist aber unvollständig.

Wenn der Angreifer erst ein Lösegeld verlangt, ist es normalerweise schon zu spät. Der Angreifer hat bereits Tage, Wochen oder sogar Monate damit verbracht, sich auf diesen Moment vorzubereiten.

Der Angreifer musste vor dem Angriff nicht unerhebliche Schritte ausführen. Der Angreifer kann die Attacke auch verlängern, nachdem er bezahlt oder die Systeme von seinem Zugriff bereinigt wurden. Ein umfassenderes Bild eines Ransomware-Angriffs wird rechts dargestellt.

Wenn der Angreifer erst ein Lösegeld verlangt, ist es normalerweise schon zu spät. Der Angreifer hat bereits Tage, Wochen oder sogar Monate damit verbracht, sich auf diesen Moment vorzubereiten. Und an diesem Punkt muss sich die Organisation der bitteren Wahrheit stellen. Die Organisation:

- Hatte nicht die Fähigkeit, sich gegen das Fortschreiten des Angriffs zu verteidigen.
- Kann höchstwahrscheinlich den Angreifer nicht zuverlässig vertreiben.
- Muss bezahlen und hofft, dass der Angreifer nicht wieder zuschlägt.

So können Sie dieses Szenario verhindern.

Verteidigung gegen Ransomware: Es gibt keine Wunderwaffe

Keine einzelne Taktik ermöglicht alleine die effektive Verteidigung gegen Ransomware. Jede wirksame Verteidigung muss so komplex und facettenreich wie der Angriff selbst sein. Unternehmen müssen bei jedem Schritt in der Kampagne des Angreifers eine breite Palette an Abwehrmaßnahmen einsetzen.

Kurz gesagt, bei der Verteidigung gegen Ransomware gibt es viel zu tun. Viele Organisationen können zumindest einen Teil dieser Taktiken nicht durchführen. Einige sind damit sogar komplett überfordert.

Der Prozess muss aber von allen Organisationen angestoßen werden.

Profil eines Ransomware-Angriffs

Vor dem Angriff

Der Angreifer sammelt die notwendigen Informationen, übernimmt die entsprechende Kontrolle und Einflusskraft, um die Organisation in eine schwierige Lage zu bringen.

Der Angreifer geht nach diesen Schritten vor:

- Scannen des Netzwerks der Organisation auf Schwachstellen.
- Starten von Standardangriffen wie Phishing oder Ausnutzen bekannter Schwachstellen wie nicht gepatchter Assets.
- Laterale Bewegung durch die anfälligen Systeme der Organisation.
- Versuch, in der Umgebung festen Fuß zu fassen.
- Sammeln von Informationen über die kritischen Systeme der Organisation.
- Herausfiltern so vieler sensibler Daten wie möglich.
- Entwickeln der Fähigkeit, die Kontrolle über die Systeme der Organisation zu übernehmen.

Während des Angriffs

Der Angreifer schafft so viele Probleme für die Organisation wie möglich und sendet eine Lösegeldforderung.

Der Angreifer geht nach diesen Schritten vor:

- Sperren jedes kritischen Systems unter der Kontrolle des Angreifers.
- Drohen damit, die vom Angreifer gestohlenen sensiblen Daten zu löschen oder zu verkaufen.

Nach dem Angriff

Der Angreifer kann zusätzliche Angriffe starten. In vielen Fällen erhöht die Bezahlung einer Lösegeldforderung die Wahrscheinlichkeit, dass ein Angreifer erneut zuschlägt.

Der Angreifer geht nach diesen Schritten vor:

- Offenhalten einer versteckten Hintertür in die Umgebung.
- Ausnutzen anderer Netzwerkschwachstellen, die beim vorherigen Angriff entdeckt wurden.
- Herausfiltern weiterer Daten.
- Letztendlich Sperren der Systeme, Drohen, die Daten erneut zu löschen oder zu verkaufen, und Stellen einer weiteren Lösegeldforderung.

Effektiver Schutz vor Ransomware-Angriffen

Vor dem Angriff

Die Organisation muss die Barriere für den Zugang zum Netzwerk erhöhen und die Wahrscheinlichkeit eines opportunistischen Angriffs verringern.

Die Organisation sollte:

- Für kontinuierliche Visibilität der Endpunkte, einschließlich Anwendungen und deren Aktivitäten sorgen.
- Bekannte Schwachstellen auf Assets durch ständiges Patchen, Aktualisieren und Konfigurieren entfernen.
- Proaktiv nach IOC (Indicators of Compromise = Kompromittierungsindikatoren) als Beweis für laufende Angriffe suchen, bevor sie sich ausweiten.

Während des Angriffs

Die Organisation muss die Attacke beheben und den Angreifer schnell ausschließen.

Die Organisation sollte:

- Den Angriff untersuchen, um seine Ursache, seine laterale Ausbreitung und alles, was die Angreifer berührt haben, zu identifizieren.
- Die verbleibenden Schwachstellen in der Umgebung schließen, um die weitere Ausbreitung des Angriffs einzudämmen.
- Den Angriff beheben, die Angreifer entfernen und die Kontrolle über die Systeme ohne erheblichen Datenverlust zurückerlangen.

Nach dem Angriff

Die Organisation muss die Umgebung schützen und sicherstellen, dass der Angreifer wirklich weg ist und das Netzwerk nicht erneut gefährden kann.

Die Organisation sollte:

- Die Instanzen jeder Schwachstelle auffinden, die der Angreifer ausgenutzt hat, und für die Assets schließen.
- Alle verbleibenden Hintertüren schließen, die die Angreifer möglicherweise noch haben, und sie effektiv aussperren.
- Kontinuierlich den allgemeinen Zustand und die Sicherheit der Endpunktumgebung verbessern, um neue Angriffe zu verhindern.

Vorgehensweise: Fünf Schritte zum Aufbau einer effektiven Verteidigung vor Ransomware

Wenn Sie diese Schritte befolgen, können Sie:

- Die Lücken in Ihrer aktuellen Ransomware-Verteidigung identifizieren.
- Die kritischsten Lücken beheben, die Sie möglicherweise aufdecken.
- Eine starke Ransomware-Verteidigung aufbauen, auch wenn Sie von Grund auf damit anfangen.

Schritt eins: Bewerten Sie Ihre aktuelle Ransomware-Verteidigung.

Stellen Sie sich zunächst ein paar Fragen, um Ihre derzeitige Verteidigung gegen jede Phase eines Ransomware-Angriffs zu beurteilen:

- Haben wir einen genauen Katalog aller Assets in unserer Umgebung?
- Können wir diese Assets überwachen und darauf nach spezifischen IOCs suchen?
- Werden diese Assets jederzeit gepatcht, aktualisiert und konfiguriert?
- Wie schnell können wir ein kompromittiertes Asset oder eine andere Bedrohung erkennen?
- Können wir jedes Asset und jedes Datenelement bestimmen, das ein Angreifer berührt hat?
- Wie schnell könnten wir einen Vorfall eindämmen und beheben?
- Können wir einen Angreifer in dem Vertrauen aussperren, dass er wirklich weg ist?
- Wie schnell könnten wir unsere Umgebung vor ähnlichen Angriffen schützen?

Fragen Sie sich schließlich:

Könnten wir einen Ransomware-Angriff erkennen und beheben, bevor er unsere kritischsten Operationen beeinträchtigt – oder müssten wir das Lösegeld bezahlen?

Schritt zwei: Schaffen Sie umfassende Visibilität für Ihre Assets.

In Bezug auf die Priorität müssen Sie zuerst alle Sichtbarkeitslücken füllen, die Sie identifizieren. Visibilität ist die Grundlage und dient als Multiplikator für alle anderen Aktivitäten.

Sie müssen Visibilität für die Assets in Ihrer Umgebung entwickeln – unabhängig davon, ob sie verwaltet werden oder nicht und ob sie vor Ort, in Remote-Netzwerken oder in das bzw. aus dem Netzwerk verschoben werden.

Für jedes dieser Assets ist die Visibilität aus folgenden Gründen wichtig:

- Identifizieren der Hardware sowie der darauf ausgeführten Software.
- Überprüfen des aktuellen Status Ihrer Patches, Softwareversionen, Konfigurationseinstellungen, Administratorenrechte und bekannten Schwachstellen.
- Legen Sie eine Ausgangssituation für das normale Verhalten dieser Assets und ihrer Benutzer fest, überwachen Sie das aktuelle Verhalten kontinuierlich anhand dieser Ausgangssituation und lösen Sie bei abnormalem Verhalten Warnungen aus.
- Definieren Sie das messbare Risiko jedes Assets und ordnen Sie die potenzielle Entwicklung und die Auswirkungen zu, wenn ein erfolgreicher Ransomware-Angriff stattfinden sollte.

Sie müssen einen umfassenden, genauen und aktuellen Asset-Bestand entwickeln. Ihr Bestand sollte gegenüber Veränderungen in Ihrer Umgebung widerstandsfähig sein. Und Sie müssen alle Assets – oder Asset-Gruppen – in Ihrem Bestand schnell nach bestimmten Schwachstellen oder IOCs abfragen können.

Schritt drei: Verbessern Sie Ihren Ansatz für die Cyber-Hygiene.

Als Nächstes sollten Sie sich auf eine verbesserte Cyber-Hygiene konzentrieren. Die meisten Ransomware-Angriffe nutzen bekannte Schwachstellen in der Umgebung aus.

Sie müssen jederzeit eine gute Cyber-Hygiene aufrechterhalten und eine hohe Barriere zum Schutz vor Eindringlingen aufbauen. Daher müssen Sie bekannte Schwachstellen in Ihren Assets aus der Ferne, in großem Maßstab und innerhalb eines geschlossenen Systems schließen können, in dem Kontrollen korrekt durchgeführt werden.

Für eine dauerhaft gute Cyber-Hygiene Ihrer Anlagen sollten Sie:

- Eine hohe Patch-Compliance aufrechterhalten und schnell neue Patches auf Assets anwenden.
- Software und Betriebssysteme mit den aktuellsten Versionen auf dem neuesten Stand halten.
- Richtlinien, Zugriffsrechte und Konfigurationen für Assets durchsetzen.
- Sich an Ihre gesetzlichen Anforderungen halten.

Sie sollten jede dieser Compliance-Kontrollen nahezu perfekt erfüllen. Ein Angreifer muss nur eine Schwachstelle auf einem Asset finden und ausnutzen, um in Ihr Netzwerk einzudringen und eine Ransomware-Kampagne einzuleiten. Sie können Compliance-Raten von 70 %, 80 % oder sogar 90 % nicht mehr als „gut genug“ akzeptieren.

Schritt vier: Bauen Sie Ihre Fähigkeiten zur Reaktion auf Zwischenfälle aus.

Erweitern Sie als Nächstes Ihre Visibilität und Kontrollmechanismen über die Prävention hinaus. Diese Mechanismen müssen Attacken schnell stoppen und Angreifer aufhalten können.

Um effektiv auf die schnelle Verbreitung der meisten Ransomware-Angriffe zu reagieren, sollten Sie eine breite Palette von Visibilitäts- und Kontrollfunktionen in nahezu Echtzeit in Ihrer gesamten Umgebung ausführen können.

Zur Reaktion auf Ransomware-Vorfälle sollten Sie:

- Ihre Reaktionspläne testen können, damit Sie wissen, wie Sie während eines Vorfalls handeln werden.
- Angriffe erkennen, bevor sie zuschlagen – das gilt auch für unbekannte, unvorhersehbare Attacken.
- Echtzeit- und Langzeitdaten zur Definition von Angriffsketten kombinieren.
- Genau wissen, was der Angreifer berührt, aufgerufen und gefährdet hat.
- Vorfälle beheben, bevor der Angreifer Systeme sperrt und Daten herausfiltert.
- Feststellen, ob der Angreifer noch eine Hintertür in Ihre Asset-Umgebung offen hat.
- Aus Vorfällen lernen und proaktiv Abwehrmaßnahmen gegen ähnliche Muster aufbauen.

Sie können die oben genannten Aktionen nur dann schnell und skaliert ausführen, wenn sie auf einer einzigen Plattform zusammengefasst werden. Während eines Vorfalls haben Sie keine Zeit, um mit mehreren Tools, Teams und Datensätzen zu jonglieren. Sie benötigen optimierte, kollaborative Prozesse, die auf der Grundlage einer Single Source of Truth und einem gemeinsamen Toolset arbeiten.

Schritt fünf: Bewerten Sie Ihre Tools neu.

Werfen Sie abschließend einen genauen Blick auf Ihre Endpunkt-Tools. Sie bilden die Grundlage für jede der Fähigkeiten in diesem E-Book. Sollten bei einer dieser Fähigkeiten Lücken bestehen, haben Sie wahrscheinlich:

- Kein Tool zur Bereitstellung dieser Fähigkeit eingesetzt.

ODER

- Sie haben das falsche Tool für Ihre Umgebung bereitgestellt.

Sehen Sie sich die von Ihnen eingesetzten Tools an, die Visibilität, Cyber-Hygiene und die Reaktion auf Zwischenfälle ermöglichen sollen. Erstellen Sie eine Liste aller Tools, die Ihnen bei Ihrer täglichen Arbeit keinen Nutzen bringen.

Stellen Sie sich dann für jedes Tool eine letzte Frage:

„Wenn diese Tools unter normalen Umständen keinen Nutzen bringen, ist das dann inmitten eines Ransomware-Angriffs der Fall?“

Jedes Tool, für das Sie diese Frage mit „Nein“ beantworten, sollte ersetzt werden.

Wie Unternehmen Ransomware mit den richtigen Tools stoppen können

In diesem Abschnitt werden die Tools ausführlich besprochen. Sie erfahren, wie Sie Sicherheitstools zum Schutz gegen Ransomware auswählen.

Darin wird Folgendes untersucht:

- Weshalb Organisationen sich nicht mit Legacy-Tools verteidigen können.
- Wie Tanium die grundlegenden Probleme mit Legacy-Tools korrigiert.
- Wie mehrere Organisationen mithilfe von Tanium ihre Sicherheit verbessert haben.

Neues Problem, alte Lösung: Weshalb veraltete Tools im Kampf gegen Ransomware scheitern

Ransomware bewegt sich schnell weiter. Wenn Sie Opfer eines Angriffs werden, haben Sie keine Zeit für die Entwicklung neuer Sicherheitstools. Die Verteidigung gegen einen Angriff funktioniert nur mit den bereits vorhandenen Tools.

Wenn Sie die richtigen Tools haben, können Sie die Attacke stoppen und den Angreifer aussperren. Wenn Sie auf die falschen Tools setzen, spüren Sie die Auswirkungen eines Angriffs.

Leider sind die älteren Sicherheitssysteme, welche die meisten Organisationen nutzen, häufig die falschen Tools bei der Verteidigung gegen Ransomware.

Das Problem ist ganz einfach. Legacy-Tools wurden für den Schutz von veralteten Betriebsumgebungen entwickelt. Diese Legacy-Umgebungen waren:

- **Klein.** Unternehmen stellten eine relativ geringe Anzahl an Assets bereit. Sie arbeiteten immer noch größtenteils manuell ohne viele Geräte oder Anwendungen.
- **Einfach.** Assets wurden von der IT bereitgestellt und vor Ort genutzt. Die IT wusste jederzeit, welche Assets sich in der Umgebung befanden und was diese machten.
- **Statisch.** Die Asset-Umgebungen der Organisation änderten sich nicht allzu oft. Alle neuen Geräte, Anwendungen oder Updates wurden langsam und unter Aufsicht bereitgestellt.

Gleichzeitig waren Legacy-Umgebungen relativ vorhersehbaren, unkomplizierten Bedrohungen ausgesetzt und die Verteidigung dagegen war einfacher.

Aber die Zeiten haben sich geändert. Organisationen betreiben heute moderne IT-Umgebungen.

Diese digitalen Infrastrukturen sind:

- **Groß.** Die Organisationen stellen jetzt eine große Menge an Assets bereit. Die Mitarbeiter führen nun den Großteil ihrer Arbeit auf Geräten und Anwendungen aus.
- **Komplex.** Assets werden häufig von Nutzern bereitgestellt und außerhalb des Netzwerks eingesetzt. Die IT weiß nicht, welche Assets sich in ihrer Umgebung befinden oder was diese tun.
- **Chaotisch.** Die Asset-Umgebungen ändern sich schnell. Neue Geräte, Anwendungen und Updates werden schnell und ohne Wissen der IT bereitgestellt.

Darüber hinaus sind moderne Unternehmen mit unvorhersehbaren und ausgefeilten Bedrohungen wie Ransomware konfrontiert, deren Behebung umfangreiche Fähigkeiten erfordert. Wenn Unternehmen versuchen, ihre modernen Umgebungen mit veralteten Tools vor Bedrohungen wie Ransomware zu schützen, scheitern diese Tools normalerweise.

Sie liefern veraltete Daten, die blinde Flecken lassen und Angreifern Platz zum Verstecken geben. Sie können keine einfachen Aktionen wie Patches und Updates für ihre Assets durchführen.

Sie können Angreifer bei Vorfällen nicht schnell, effizient oder sicher vertreiben. Und sie zwingen die Organisationen dazu, eine große Anzahl isolierter punktueller Lösungen einzusetzen, deren Betrieb teuer und komplex ist und deren Zusammenarbeit sich schwierig gestaltet.

Einfach gesagt scheitern ältere Tools, da sie für ältere Umgebungen entwickelt wurden. Zum Schutz moderner Umgebungen müssen Unternehmen auf moderne Tools setzen. Tools wie Tanium.

Eine moderne Sicherheitslösung für Ransomware

Tanium wurde für den Schutz moderner Umgebungen entwickelt.

Tanium verfolgt im Vergleich zu den aktuellen Strategien der meisten Organisationen einen anderen Ansatz. Die Tanium Platform geht auf die Herausforderungen ein, denen sich Organisationen beim Einsatz älterer Tools für die Sicherheit und Verwaltung ihrer Umgebungen gegenübersehen.

Tanium nutzt eine leichte, verteilte Architektur. Diese Architektur bedeutet, dass Tanium die Kernaktivitäten der Ransomware-Verteidigung in zentralisierten und Remote-Umgebungen durchführen kann – unabhängig davon, wie viele Assets diese enthalten – ohne dass dadurch eine erhebliche Netzwerkbelastung entsteht.

Durch den Einsatz dieser modernen Architektur kann Tanium große, komplexe und chaotische Asset-Umgebungen effektiv gegen Bedrohungen wie Ransomware schützen.

Die Verteidigung gegen Ransomware mit Tanium bietet Organisationen zahlreiche Vorteile:

Schaffen umfassender Visibilität für ihre Assets.

Tanium findet „versteckte“ Assets, die Legacy-Tools übersehen, mit einzigartigen Methoden. Wenn Organisationen Tanium erstmals einführen, finden Sie in der Regel 10 % bis 20 % mehr Assets, als ihnen bekannt waren. Tanium schafft für jedes dieser Assets Visibilität in die Anwendungen, Benutzer, Zugriffsrechte, Konfigurationen und bekannten Schwachstellen sowie das messbare Risiko jedes Assets.

Dann behält Tanium diese Visibilität bei. Tanium kann die Asset-Umgebung kontinuierlich in Echtzeit scannen und Organisationen zu jedem beliebigen Zeitpunkt alles mitteilen, was auf ihren Endpunkten geschieht.

Schaffen und Aufrechterhalten nahezu perfekter Cyber-Hygiene.

Tanium nutzt verteiltes Edge-Computing, um groß angelegte Patches, Updates, Konfigurationen und andere grundlegende Maßnahmen in Minuten, Stunden oder Tagen umzusetzen – anstatt in Wochen oder Monaten. Tanium validiert die Anwendung dieser Maßnahmen und kann wieder zu einem vorherigen Stand zurückkehren, um mögliche Fehlanwendungen zu korrigieren.

Tanium kann innerhalb von 24 Stunden nach der Installation eine Patch-Visibilität von 99 % erzielen. Davon ausgehend kann Tanium schnell neue Maßnahmen auf Assets anwenden und so eine nahezu perfekte Hygiene gewährleisten.

Reaktion auf Zwischenfälle innerhalb einer einzigen, einheitlichen Plattform.

Tanium ist eine einheitliche Plattform mit den meisten Kernfunktionen zum Erkennen, Untersuchen und Beheben von Ransomware-Bedrohungen in einem Tool. Diese Fähigkeiten ergänzen sich, arbeiten mit denselben Daten als Grundlage, fördern eine kollaborative Reaktion auf Bedrohungen – und eliminieren gleichzeitig die Kosten sowie Komplexität der Bereitstellung mehrerer individueller Produkte.

Die Organisationen können mehrere Tanium-Funktionen kombinieren, um komplexe Angriffsketten zu erkennen und zu untersuchen, Vorfälle nahezu in Echtzeit zu beheben und Angreifer sicher zu stoppen sowie die Abwehr gegen ähnliche Attacken zu stärken.

Wie Tanium mit Ransomware in jeder Phase des Angriffs umgeht

Wie in der rechten Spalte dargestellt, bietet Tanium eine komplexe, mehrstufige Verteidigung gegen Ransomware mit einer Vielzahl von defensiven Fähigkeiten, um jeder Phase der Kampagne des Angriffs von einer einzigen, einheitlichen Plattform aus entgegenzuwirken.

Tanium bekämpft Ransomware in jeder Angriffsphase. Damit können Unternehmen Tanium auf eine von zwei Arten zur Verteidigung gegen Ransomware nutzen:

- Sie können Tanium als zentralen Knotenpunkt einsetzen, um Ransomware zu bekämpfen.

ODER

- Sie können mit Tanium die Lücken in ihrem aktuellen Sicherheitssystem schließen.

Tanium ist eine flexible, erweiterbare Plattform mit offenen API-Integrationen. Tanium lässt sich sofort mit vielen anderen Sicherheitsanbietern und Orchestrierungsplattformen einsetzen. Die Organisationen können die Daten von Tanium verwenden, um Endpunktmetriken als Teil einer breiteren Sicherheitsstrategie und eines größeren Ökosystems zum Schutz vor Ramsomware-Angriffen zu aggregieren, zu zentralisieren und zu analysieren.

Wie Tanium Ihre Organisation vor Ransomware schützt

Vor dem Angriff

Tanium sorgt in den dynamischsten, vielfältigsten und verteiltesten Asset-Umgebungen für nahezu perfekte Cyber-Hygiene.

Einsatzmöglichkeiten von Tanium für Organisationen:

- Erstellen eines umfassenden Echtzeit-Inventars an Endpunkten, einschließlich Software, Nutzer und Schwachstellen.
- Patchen, Aktualisieren, Konfigurieren oder Anwenden von Kontrollmaßnahmen auf Hunderttausenden von Endpunkten in Stunden oder Tagen.
- Kontinuierliches Scannen oder Spot-Suchen in Echtzeit nach spezifischen IOCs über Endpunkte hinweg.

Während des Angriffs

Tanium kann Angriffe nahezu in Echtzeit untersuchen und schnell Maßnahmen ergreifen, um den Angreifer zu stoppen.

Einsatzmöglichkeiten von Tanium für Organisationen:

- Definieren der Angriffsquelle, Zuordnen der gesamten Angriffskette und Identifizieren der Assets, die der Angriff gefährdet hat.
- Identifizieren, auf welche anderen Assets sich der Angriff ausbreiten könnte, und Vorbereitung der Assets in Echtzeit auf das Muster.
- Aufnahme von Verhandlungen in dem Wissen, dass der Angreifer gestoppt werden kann, bevor der Betrieb beeinträchtigt wird.

Nach dem Angriff

Tanium kann aus dem Angriff lernen und die Verteidigung der Umgebung gegen einen zweiten Schlag oder ähnliche Angriffsmuster stärken.

Einsatzmöglichkeiten von Tanium für Organisationen:

- Durchführen von Spot-Suchen, um verbleibende Instanzen der im Angriff ausgenutzten Schwachstellen zu finden und zu schließen.
- Scannen der Umgebung auf verbleibende Spuren der Angreifer und deren zuverlässiges Entfernen.
- Aufrechterhaltung der grundlegenden Cyber-Hygiene auf hohem Niveau, um die Wahrscheinlichkeit eines weiteren Vorfalls zu verringern.

Echte Kunden, echte Ergebnisse: Wie Organisationen Tanium nutzen

Diese Lösung ist mehr als Theorie. Viele Organisationen schützen mithilfe von Tanium bereits heute ihre Asset-Umgebungen vor einer Vielzahl von Cyberbedrohungen, einschließlich Ransomware. Hier finden Sie einige Beispiele.

Global tätige Anwaltskanzlei

„Wir reagierten langsamer auf Ereignisse als nötig. Mit Tanium wurde das Team viel schneller."

HERAUSFORDERUNG:

Erfüllung der Sicherheitsanforderungen des stark regulierten Kunden zur Reaktion auf Zwischenfälle, Verteilung von Patches usw.

VOR TANIUM:

Die Incident Response Teams mussten sich direkt mit kompromittierten Endpunkten verbinden, was Dienstreisen oder den Versand des Endpunkts erforderte sowie bis zum Erledigen der Aufgabe Stunden oder Tage dauerte.

NACH TANIUM:

Die Endpunktvisibilität beschleunigte sich von Wochen auf Minuten, und die Triage- und Behebungsaktivitäten erfolgen für die Endpunkte nun aus der Ferne, was die Reaktion auf Zwischenfälle beschleunigt.

Global tätige Einzelhandelsgruppe

„Wir können uns auf Tanium als zentrale Anlaufstelle für Visibilität und Kontrolle verlassen, auf die Verwaltung und Sicherung unseres Unternehmens und auf die erhöhte Effizienz unserer Investments."

HERAUSFORDERUNG:

Mangelnde Visibilität und manuelle Behebung von Vorfällen in einer verteilten globalen Organisation mit 25.000 Mitarbeitern.

VOR TANIUM:

Ineffizienter Schutz der Endpunkte, der bis zu einer Woche bis zur Lösung kritischer Probleme benötigte und kompromittierte Geräte tagelang gefährdete.

NACH TANIUM:

Aktivitäten zum Schutz der Endpunkte, die bis dahin fast eine Woche in Anspruch nahmen, dauern jetzt weniger als einen Tag – in einigen Fällen unter vier Stunden.

Führendes Technologieunternehmen

„Wir können jetzt automatisieren, was wir wissen, um mehr Zeit mit der Suche nach dem zu verbringen, was wir nicht wissen. Letztlich wird auch das automatisiert."

HERAUSFORDERUNG:

Die Teams konnten Bedrohungen versiert identifizieren, hatten jedoch keine umfassende Visibilität in ihrer Umgebung und standen vor Herausforderungen, die gefundenen Bedrohungen gründlich zu untersuchen.

VOR TANIUM:

Die Incident Response Teams verwendeten iterative Tools zur Bedrohungssuche und -untersuchung, die zum Erfassen von Bedrohungen zu viel Zeit benötigten, was die Reaktion weiter verzögerte.

NACH TANIUM:

Teams untersuchen und reagieren jetzt remote in Echtzeit auf Bedrohungen, wodurch die mittlere Wiederherstellungszeit drastisch reduziert und die Fähigkeit, Schwachstellen zu schließen, beschleunigt wird.

Verteidigung gegen Ransomware mit Tanium: Grundlegende Lösungen

Während die für die Sicherheit verantwortlichen Personen in diesen Organisationen eine breite Palette von Taniums Fähigkeiten nutzten, um die Verteidigung gegen Ransomware und andere moderne Bedrohungen zu stärken, betrachteten sie die unten beschriebenen Lösungen als die effektivsten.

Asset-Discovery und -Inventory

Erkennen, welche Endpunkte und Anwendungen sich in der Umgebung befinden, auch wenn sich die Umgebung schnell verändert.

Risk- & Compliance-Management

Sie können das Risiko und die Auswirkungen von Exploits in Echtzeit bewerten, einschließlich lateraler Bewegungen.

Threat Hunting

Beantworten Sie die folgende Frage zuversichtlich: „Ist alles in Ordnung?“ Sie wissen, dass Sie innerhalb von Sekunden über jeden Endpunkt an jedem Ort berichten können. So lassen sich Vorfälle stoppen, bevor sie zu großen Schäden führen.

Unternehmen könnten diese Lösungen rasch beschleunigen, indem sie die einfache, leichte Architektur und das cloudbasierte Angebot von Tanium nutzen: Tanium Cloud.

Mit Tanium Cloud führen Unternehmen neue Sicherheitsfunktionen in Stunden oder Tagen ein – nicht Wochen oder Monaten – und schließen für höhere Sicherheit schnell die Lücken in ihrer bestehenden Verteidigung oder schaffen eine neue durchgängige Strategie gegen Ransomware aus einer einzigen Lösung heraus.

Stärken Sie ab heute Ihre Verteidigung gegen Ransomware

Bisher haben wir eine umfassende Strategie zur Bekämpfung von Ransomware beschrieben:

- **Wählen Sie zunächst einen proaktiven Ansatz.** Die Häufigkeit und die Auswirkungen von Ransomware nehmen zu. Ransomware-Angriffe legen große Organisationen in jeder Branche lahm. Ihre Verteidigungsmechanismen müssen stehen, bevor Sie zum Angriffsziel werden.
- **Als Zweites müssen Sie die richtigen Fähigkeiten entwickeln.** Angriffe mit Ransomware sind komplex und verlaufen in mehreren Stufen. Es gibt keine Wunderwaffe. Im Kampf gegen Ransomware müssen Sie Echtzeit-Visibilität, makellose Cyber-Hygiene und Möglichkeiten zur Reaktion auf Zwischenfälle entwickeln.
- **Schließlich sollten Sie moderne Sicherheitstools einsetzen.** Legacy-Tools können moderne Umgebungen nicht vor schnell agierenden, komplexen Bedrohungen wie Ransomware schützen. Sie müssen Tools bereitstellen, die auf die Geschwindigkeit und Skalierbarkeit Ihrer modernen Asset-Umgebung abgestimmt sind.

Jetzt ist es an der Zeit, zu handeln.

Überprüfen Sie Ihre Fähigkeiten zur Verteidigung gegen Ransomware. Starten Sie Ihre Pläne für die Entwicklung von Fähigkeiten zur Bekämpfung dieser Bedrohung. Kontaktieren Sie uns und finden Sie heraus, ob Tanium die richtige Plattform ist, um Ihr Netzwerk und Ihre Endpunkte vor Ransomware-Angriffen zu schützen.

Vereinbaren Sie eine kostenlose Beratung und Demo von Tanium.

Jetzt anfragen →

Lassen Sie von Tanium die Cyber-Hygiene Ihrer aktuellen Umgebung bewerten.

Cyber-Hygiene-Assessment erhalten →

Starten Sie Tanium mit unserem cloudbasierten Angebot, Tanium Cloud.

Jetzt ausprobieren →

Tanium ist die Plattform, der Unternehmen vertrauen, wenn sie Visibilität und Kontrolle für alle Endpunkte in lokalen, Cloud- und hybriden Umgebungen erzielen möchten. Unser Ansatz bietet eine Lösung für die wachsenden Herausforderungen der heutigen IT. Durch die Bereitstellung präziser, vollständiger und aktueller Endpunktdaten erhalten Teams für IT-Betrieb, -Sicherheit und -Risiko die Möglichkeit, ihre Netzwerke schnell zu verwalten, zu sichern und zu schützen. Tanium verfolgt die Mission, Organisationen dabei zu helfen, jeden Endpunkt zu erfassen und zu kontrollieren. Das ist die Power of Certainty.

Besuchen Sie uns unter **www.tanium.com** und folgen Sie uns auf **LinkedIn** und **Twitter**.

TANIUM

Referenzen

1. Zorabedian, J. (2020). „What's new in the 2020 cost of a data breach report" [Online]. Zugriff im Internet unter https://securityintelligence.com/posts/whats-new-2020-cost-of-a-data-breach-report/
2. Office of Foreign Assets Control (OFAC) des US-Finanzministeriums (2020). „Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" [Online]. Zugriff im Internet unter https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf
3. Morgan, S. (2019). „Global ransomware damage costs predicted to reach $20 billion (USD) by 2021" [Online]. Zugriff im Internet unter https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
4. Collier, K. (2020). „Major hospital system hit with cyberattack, potentially largest in U.S. history" [Online]. Zugriff im Internet unter https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254
5. Torbet, G. (2019). „Baltimore ransomware attack will cost the city over $18 million" [Online]. Zugriff im Internet unter https://www.engadget.com/2019-06-06-baltimore-ransomware-18-million-damages.html
6. Srinivas, R. (2020). „Ransomware attacks in 2020! These are four most affected sectors" [Online]. Zugriff im Internet unter https://cisomag.eccouncil.org/ransomware-attacks-in-2020-these-are-4-most-affected-sectors/
7. Cimpanu, C. (2020). „Cognizant expects to lose between $50m and $70m following ransomware attack" [Online]. https://www.zdnet.com/article/cognizant-expects-to-lose-between-50m-and-70m-following-ransomware-attack/
8. Ballard, B. (2020). „Kmart is latest retailer to suffer major ransomware attack" [Online]. Zugriff im Internet unter https://www.techradar.com/news/kmart-is-the-latest-retailer-to-suffer-a-ransomware-attack