ANWENDERBERICHT

Schwermaschinenhändler wehrt sich mit Tanium gegen einen Ransomware-Angriff und gewinnt

Nach einem Angriff nutzte Ring Power, ein in Florida ansässiger Händler von Cat®-Geräten, Tanium, um die Zahlung von Lösegeld zu vermeiden und gleichzeitig den vollen Betrieb seines Rechenzentrums und seiner Endgeräte wiederherzustellen.

Branche
Schwermaschinenhändler

Hauptsitz
St. Augustine, Florida, USA

Verwaltete Endpunkte
2.300

Lösungen von Tanium

- Threat Hunting
- Asset-Discovery und -Inventory
- Sensitive Data Monitoring
- Risk & Compliance-Management
- Client Management

Herausforderung

Durch einen Ransomware-Angriff war Ring Power mit seinem Rechenzentrum vollständig abgeschnitten – und eine unbekannte Zahl der Endpunkte waren infiziert.

Lösung

Mit der Hilfe von Tanium erholte sich Ring Power vollständig vom Angriff – und ohne das Lösegeld zahlen zu müssen.

Ergebnis

Mit der Hilfe von Tanium musste Ring Power das Lösegeld nicht bezahlen – und auch gar nicht erst mit seinen Angreifern kommunizieren.

Wenn Ransomware zuschlägt, kann Tanium Organisationen bei einer schnellen und effizienten Wiederherstellung unterstützen.

Wie sich Ring Power mithilfe von Tanium von Ransomware erholte

Im September 2019 wurde Kevin Bush eines frühen Morgens durch einen Telefonanruf geweckt und darüber informiert, dass Ring Power Opfer eines Ransomware-Angriffs geworden ist. Anschließend stellte er fest, dass das gesamte Rechenzentrum des Unternehmens von der Außenwelt getrennt wurde. Darüber hinaus war eine unbekannte Zahl der 2.300 Endpunkte des Unternehmens gefährlich infiziert.

Mit der Hilfe von Tanium konnten Bush und sein zehnköpfiges IT-Team die IT-Infrastruktur von Ring Power in wenigen Wochen vollständig von Malware bereinigen und wiederherstellen. Und das ganz ohne das Lösegeld zahlen zu müssen – tatsächlich ohne jemals mit den Angreifern zu kommunizieren.

Irgendwann am Vorabend hatte einer der Manager von Ring Power unwissentlich eine Phishing-E-Mail angeklickt.

Herausforderung

Um 4:30 Uhr nachts wurde Kevin Bush, VP IT für den Schwermaschinenhändler Ring Power Corp., durch einen Telefonanruf geweckt wurde, den er niemals kriegen wollte.

Der nächtliche Anrufer, ein Vertreter des MSP von Ring Power, hatte schlechte Nachrichten. Irgendwann am Vorabend hatte einer der Manager von Ring Power unwissentlich eine Phishing-E-Mail angeklickt. In den darauffolgenden Stunden wurde die IT-Infrastruktur des Unternehmens von Ransomware angegriffen. Und nun, mit einer unbekannten Zahl infizierter Endpunkte, war das Rechenzentrum von Ring Power bei einem Ransomware-Angriff als „Geisel“ genommen worden.

Das alles ereignete sich erst am 11. Tag, an dem Bush für Ring Power arbeitete. „Ransomware ist wie eine schreckliche Krankheit“, sagt er heute dazu. „Man hat davon gehört, aber man hofft insgeheim, dass es einen nie treffen wird.“

Lösung

Mit der Hilfe von Tanium haben Bush und sein Team die IT-Infrastruktur innerhalb weniger Wochen wiederhergestellt. Und das gelang, während sich das Unternehmen nicht nur weigerte, das Lösegeld zu bezahlen, sondern die Angreifer dabei auch überhaupt nicht kontaktieren musste.

„Tanium machte die Erholung nach dem Angriff so viel einfacher", sagt Brian Hall, MIS Operations Manager von Ring Power und Mitglied des IT-Teams von Bush.

Das alles erreichten Bush und sein 10-köpfiges IT-Team in ca. drei Wochen. An diesem Morgen im September 2019 war die erste Maßnahme nach Erhalt des Telefonanrufs, ins Büro zu eilen und den Schaden zu beurteilen. Die vorzufindenden Umstände waren nicht gut. Das gesamte Rechenzentrum von Ring Power, einschließlich aller 150 Server, war vollständig von der Außenwelt getrennt.

Zur Schadensbegrenzung haben Bush und sein Team schnell gehandelt. Sie haben alle Server heruntergefahren. Sie schützten ihre Backup-Systeme, indem sie sie offline nahmen. Und sie kontaktierten die 26 Standorte des Unternehmens telefonisch und forderten die Mitarbeitenden auf, die Computer auf Infektionen zu testen. Wenn Word oder Excel geöffnet werden konnte, war der Rechner sauber. Aber wenn sie stattdessen das „Ryuk"-Symbol auf dem Bildschirm sehen würden – das ist der Name eines Ransomware-Typs – dann wäre der Rechner infiziert. In diesen Fällen wurden die Mitarbeiter angewiesen, ihren Computer auszuschalten, ihn zu verpacken und an die Zentrale von Ring Power zu senden, wo der Rechner von der Schadsoftware bereinigt werden sollte.

Nach Abschluss dieser Aufgabe stand die Wiederherstellung der Systeme auf der Tagesordnung. Der Neustart dieser 150 Server, die erneute Bereitstellung von rund 200 Anwendungen und die Wiederinbetriebnahme von etwa 2.300 Endgeräten war eine große Aufgabe. Da es so viel zu tun gab, haben Bush und sein Team zwei lange Monate anstrengende 80-Stunden-Wochen gearbeitet.

Der nächste Schritt von Bush war die Installation von Tanium auf allen bereinigten Endpunkten. Ring Power hatte vor kurzem einen Vertrag für Tanium as a Service (TaaS) unterzeichnet, aber so kurzfristig, dass die Installationen noch nicht gestartet waren. Das IT-Team hat Tanium-Tools auf viele tragbare USB-Laufwerke geladen und sie mit Anweisungen an die Niederlassungen gesendet.

Bush dazu: „Wir verteilen Tanium wie Butter."

> Tanium bringt für unser gesamtes Team Visibilität auf einen Bildschirm. Wenn man diese Art von Visibilität nicht hat, kann man nachts nicht schlafen.
>
> **Kevin Bush**
> VP of IT, Ring Power Corp.

„Tanium hat uns wirklich dabei geholfen, uns von diesem Angriff zu erholen"

Kevin Bush, VP IT bei Ring Power, einem Schwermaschinenhändler mit Sitz in St. Augustine, Florida.

> Ich finde Tanium gerade wirklich klasse. Das System wird nach Ihren Wünschen konfiguriert und läuft dann einfach. Tanium muss wirklich nur einmal eingerichtet werden, mehr nicht.

Brian Hall
MIS-Betriebsführer bei Ring Power Corp.

Ergebnis

Nachdem alle Nutzer von Ring Power Tanium auf ihren Computern hatten, konnten sie ihre Anwendungen selbst neu bereitstellen. Das bedeutete, dass Bush und sein Team die Arbeit nicht manuell erledigen mussten – eine große Zeitersparnis angesichts der großen Anzahl an Standorten, Nutzern und Systemen von Ring Power.

Es bedeutete auch, dass Ring Power keinerlei durch die Ransomware gestellten Lösegeldforderungen bezahlen musste. Tatsächlich hat das Unternehmen nie mit den Angreifern kommuniziert. Stattdessen gab Bush die E-Mail-Adresse der Angreifer einfach an das FBI weiter. Später sagte der Agent, der diesem Fall zugewiesen war, dass Ring Power bereits besser als 90 % der Unternehmen aufgestellt sei, mit denen er zu tun hat. Da der Agent durchschnittlich vier neuen Fällen pro Tag zugewiesen wird, ist diese Einschätzung maßgeblich.

Mit Tanium hat Ring Power auch die Visibilität von Endpunkten in seinem Netzwerk erheblich verbessert. Ring Power hatte den Einsatz des SCCM-Systemmanagement-Tools von Microsoft in Betracht gezogen, empfand es aber im Vergleich zu Tanium als viel komplizierter und komplexer.

„Tanium ist extrem einfach zu verwalten", so Hall. „Außerdem verfügt es über eine Vielzahl von Modulen und Fähigkeiten, die SCCM nicht hat. Das hat uns die Entscheidung leicht gemacht."

Durch die Nutzung von Tanium konnte Ring Power auch Patches und Updates automatisieren. Zuvor musste das MIS-Team mit großem Zeitaufwand Software manuell installieren. Jetzt, da Tanium diese Arbeit erledigt, spart das Unternehmen schätzungsweise eineinhalb Stunden pro Tag.

Sie benötigen weitere Informationen? Besuchen Sie uns auf **www.tanium.com**