TANIUM

Es ist an der Zeit für ausgereifte Cyber-Hygiene

Sonderausgabe: Herstellung

Die größten und wichtigsten Produktionszentren Europas befinden sich im Wandel.

In den letzten Jahren wurde die Geschäftskontinuität durch fehlende Komponenten, steigende Energiepreise und geopolitische Verwerfungen erschüttert. Darüber hinaus ist die Branche jetzt auch das Hauptangriffsziel von Cyberkriminellen geworden – und hat in dieser Hinsicht zum ersten Mal den Finanzdienstleistungssektor überholt.

Hersteller, Produzenten und Verarbeitungsunternehmen sind einem breiten Spektrum von Cyberbedrohungen ausgesetzt: von einfachen E-Mail-Phishing-Angriffen bis hin zu gezielten Angriffen auf Fertigungsprozesse. Zwar sind diese Bedrohungen aufgrund vieler unvorhergesehener externer Ereignisse gewachsen, aber es lässt sich auch nicht bestreiten, dass viele Unternehmen aufgrund unzureichender Daten- und Asset-Management-Kontrollen intern anfälliger geworden sind.

Dies ist aufgrund der raschen Einführung von Cloud-Technologien der nächsten Generation und der Digitalisierung von Fertigungs-, Herstellungs- und Verarbeitungsanlagen durchaus verständlich. Das Zeitalter von IIoT, Prozessautomatisierung, Robotik und KI ist nunmehr vollständig angebrochen – mit revolutionären technologischen Veränderungen, die manchem Unternehmen aber auch erhebliche Probleme bereiten können. Wir können allerdings von zukunftsorientierten OEMs lernen, die eine Begabung dafür entwickelt haben, die Interaktionen von Unternehmensnetzwerken und Werkhallen – und umgekehrt –genau zu analysieren.

Gut funktionierende Governance-Ebenen dürfen nicht ignoriert werden, wenn es um Datenschutz und Cybersicherheit geht. Unternehmer, Aktionäre, Regulierungsbehörden und (in zunehmendem Maße) Endbenutzer verlangen mehr Transparenz bei der Datenhygiene. Haben Sie die Antworten parat? Sind diese Antworten im Fall eines Audits oder Vorfalls ausreichend?Lesen Sie weiter, um zu erfahren, wie Sie Ihre Asset-Visibilität mit angemessenen Prüfungen, Prozessen und Tools verbessern können.

Ihre Herausforderung: die Verwaltung von Millionen dynamischer, dezentral verteilter und vielfältiger Assets.

Aufgrund global verteilter Belegschaften und verborgener Assets - deren Anzahl exponentiell ansteigt - sind die Beibehaltung eines vollständigen und genauen Inventars aller IT-Assets sowie eine skalierte Visibilität in Echtzeit schwieriger als jemals zuvor. Schließlich müssen wir wissen, wie viele Türen und Fenster es gibt und wo sie sich befinden, damit wir diese Türen und Fenster verschlossen halten können.

Und dennoch konnte die Branche keine praktikable Lösung für das Problem mit der Visibilität liefern und bietet Hub-and-Spoke-Modelle als langsame und durchweichte Netzwerke an, die stattdessen die Visibilität in modernen und komplexen Umgebungen einschränken.

Es ist also kein Wunder, dass viele Unternehmen wesentliche Details über ihre Umgebung nicht genau melden können.

Zur Lösung dieses Problems heißt es also, zurück zu den Basics zu gehen.

Um die Cyber-Hygiene aufrechtzuerhalten und zu verbessern, müssen Sie zunächst wissen, welche IT-Assets Sie haben.

Nutzen Sie 50.000, 100.000 oder 500.000 Computer und Server in Ihrer Organisation?

- Wo befinden sich diese?
- Was sind sie?
- Was wird auf ihnen ausgeführt?
- Welche Dienstleistungen bieten sie an?
- Bei der Beantwortung dieser Fragen geht es um die Entwicklung der Asset-Visibilität – und um die Befolgung eines **Asset-Discovery und -Inventory-Prozesses**.

Das ist die Grundlage für die Schaffung und Aufrechterhaltung von Cyber-Hygiene. Und wir haben dieses E-Book geschrieben, um Ihnen zu helfen, die nötige Visibilität zu erreichen

In diesem E-Book beschäftigen wir uns mit Folgendem:

- Warum Asset-Visibilität zum Aufrechterhalten der Cyber-Hygiene unerlässlich ist
- Wie Sie in modernen Netzwerken für Asset-Visibilität sorgen
- Welche Tools Sie benötigen, um diese Ergebnisse zu erzielen

Die Verwaltung ist nicht möglich, falls Ihnen die Assets nicht bekannt sind.

Um Ihre Endpunkte zu verwalten, benötigen Sie Wissen und Informationen auf drei Ebenen:

1. Welche Assets haben Sie und wo befinden sich diese?
2. Welche Software wird darauf ausgeführt und ist sie lizenziert?
3. Sie benötigen mehr als nur einen Hostnamen oder eine IP-Adresse.

> **“Da die Technologieumgebungen immer komplexer werden, müssen die Hersteller Wege finden, um die Kosten für deren Betrieb und Schutz zu senken. Die Verschlankung des Technologiebestands bedeutet oft eine Modernisierung. Viele Unternehmen suchen daher nach integrierten Plattformansätzen, um veraltete Technologien und das Dickicht an Einzellösungen, die zu ihrer Verwaltung verwendet werden, zu ersetzen.”**
>
> **Tom Molden**
>
> CIO Global Executive Engagement, Tanium

Warum die Cyber-Hygiene von Asset-Visibilität abhängt

Alle Unternehmen, unabhängig von ihrer Größe, benötigen diese Informationen, die sich in der modernen IT zudem auch ständig ändern. Netzwerk-Assets kommen und gehen, insbesondere bei in vielen Unternehmen mittlerweile gängigen und zunehmend verbreiteten BYOD-Richtlinien („Bring Your Own Device“). Einige Assets tauchen dabei nur gelegentlich im Netzwerk auf. Da immer mehr Unternehmen die Mitarbeiter dazu ermutigen, von zu Hause aus zu arbeiten (WFH = „Work from Home“), steigt die Komplexität.

Und da die Netzwerke immer komplexer werden und sich schneller verändern, wird es immer schwieriger, die Visibilität beizubehalten – und die Konsequenzen, wenn der genaue Überblick über die Assets und deren Aktionen fehlt, werden immer größer.

> **“Mit der sich schnell entwickelnden Konvergenz von IT und OT suchen Unternehmen nach Möglichkeiten, eine durchgängige Sichtbarkeit, Verwaltung und einen Schutz von Technologie-Assets im gesamten Fertigungsbereich zu erreichen. In den meisten Unternehmen sind die Unternehmens-IT und die Fertigungstechnik seit Jahren unabhängig voneinander im Einsatz - der kombinierte Lösungsraum ist nicht ausgereift und es fehlt an ganzheitlichen Lösungen.”**

Tom Molden

CIO Global Executive Engagement, Tanium

Die Kosten von Unkenntnis

Um es mit den Worten des ehemaligen Eagle Don Henley zu formulieren: „Wenn Sie mit geschlossenen Augen fahren, werden Sie bestimmt mit etwas zusammenstoßen." Wenn Sie nicht wissen, welche Assets sich in Ihrem Netzwerk befinden, entspricht das für Ihre IT einer Fahrt mit geschlossenen Augen.

Eines der ersten Dinge, auf die Sie wahrscheinlich „stoßen" werden, sind Sicherheitslücken. Wenn Sie ein Asset nicht verwalten können, können Sie es nicht schützen. Und die Verwaltung ist nicht möglich, wenn Ihnen die Assets erst gar nicht bekannt sind. Sie wissen dann einfach nicht, ob die Software richtig gepatcht ist. Es kann also Angriffsvektoren geben, die Ihnen gar nicht bewusst sind.

Wie sieht es mit den finanziellen Auswirkungen aus? Haben Sie allgemein ein Gefühl dafür, wofür Sie Ihr Geld ausgeben? Zum Beispiel für Softwarelizenzen von gängigen Produktivitätsprogrammen wie Microsoft Office. Wenn Sie eine Lizenz für 10.000 Kopien haben, verwenden Sie 20.000 oder nur 5.000 davon? Nutzen Sie die Lizenz, für die Sie bezahlen, effizient? Oder sind Sie nicht compliant und Ihnen drohen unter Umständen teure rechtliche Schritte?

Darüber hinaus geht es bei Compliance nicht nur um Softwarelizenzen. Es ist ein weiterer Betriebsbereich, der sehr stark von dem Wissen abhängt, welche Assets sich in Ihrem Netzwerk befinden.

Nehmen wir das Gesundheitswesen als Anwendungsfall.

Gesundheitsorganisationen müssen die Einhaltung der DSGVO- und PCI-Bestimmungen nachweisen, die geschützte Gesundheits- und Kreditkartendaten abdecken. Wissen Sie, wo diese Daten gespeichert werden? Ist das nicht der Fall, lässt sich die Compliance nicht nachweisen. Wenn die Compliance nicht nachgewiesen werden kann, bringt das zwei erhebliche Nachteile: regulatorische Sanktionen und kein effektives Erbringen Ihrer Dienstleistungen.

Die Beispiele dafür sind schier endlos. Wenn Sie nicht wissen, welche Assets sich in Ihrem Netzwerk befinden und welche Aktionen sie ausführen, können Sie sie nicht schützen, Sie können sie nicht verwalten und Sie können in Ihrer gesamten Umgebung keine effektive Cyber-Hygiene erreichen.

Und – leider – haben viele Unternehmen derzeit Schwierigkeiten, grundlegende Fragen zu den Assets in ihrer Umgebung zu beantworten. Hier sind die Gründe dafür.

Warum Unternehmen Schwierigkeiten haben, Asset-Visibilität zu schaffen

Es gibt zwei Hauptgründe, weshalb Unternehmen Schwierigkeiten dabei haben, grundlegende Fragen zu ihren Assets zur Aufrechterhaltung der Cyber-Hygiene zu beantworten.

Erstens bewegt sich die Endpunkterkennung als Zielsetzung ständig weiter.

Nicht jeder Endpunkt in einem Netzwerk ist ein Desktop-Computer, Laptop oder Server. Dazu gesellen sich Drucker, Telefone, Tablets und eine wachsende Anzahl von IoT-Geräten (Internet of Things). Mobile Device Management (MDM) ist ein wachsendes Anwendungsfeld.

Aber warum sollten Sie sich Sorgen darum machen müssen, dass ein IoT-Endgerät das Unternehmensnetzwerk beeinträchtigt? Hier sind die Gründe dafür: Eine Mitarbeiterin von einem unserer Kunden arbeitete von zu Hause aus. Das Sicherheitsteam des Unternehmens erhielt Warnmeldungen, dass jemand versuchte, in ihren Laptop einzubrechen. Die Quelle war ein Kühlschrank mit Malware, die das Heimnetzwerk scannte und in das Gerät eindringen wollte, das sich vorübergehend im Unternehmensnetzwerk befand. Dasselbe kann bei einem intelligenten Lichtschalter, Thermostat, einer Sicherheitskamera – oder was auch immer passieren.

Dies gilt auch für Maschinen im Fertigungsbereich, von denen viele mit Sensoren ausgestattet sind, die über drahtlose Netzwerke und das Internet mit Fertigungsanwendungen kommunizieren. Dieses Feld mit der Bezeichnung „operative Technologie“ macht im Wesentlichen aus jeder Maschine in einer Fabrikhalle ein Netzwerkgerät. Jeder Gerätetyp kann Betriebs- und/oder Sicherheitsrisiken bergen, und die Anzahl dieser Typen wird in den kommenden Jahren nur noch weiter zunehmen.

Zweitens haben ältere Tools Schwierigkeiten, in dieser neuen Umgebung Visibilität zu schaffen.

Tools zur Asset-Erkennung, die vor 10 Jahren entwickelt wurden, griffen vielen Aspekten voraus, mit denen moderne IT-Umgebungen heute täglich arbeiten. Zwei Beispiele: Container und Hybrid Clouds.

Diese Tools können die Geschwindigkeit der Veränderungen, die wir jetzt sehen, nicht bewältigen. Dennoch halten viele Unternehmen an vertrauten Tools fest, auch wenn viele davon nicht einfach zu bedienen sind.

Vielleicht sind sie sogar stolz darauf, mit schwer zu bedienenden Tools zurechtzukommen. Sie haben möglicherweise benutzerdefinierte Skripte verfasst, damit sie effektiver arbeiten können. Nicht nur das: Ein ganzes Partner-Ökosystem hat sich darum entwickelt, IT-Abteilungen genau bei diesen Aufgaben zu unterstützen.

Die unbeabsichtigten – und bedauerlichen – Folgen davon sind IT-Richtlinien und -Prozesse, die nicht deshalb entwickelt wurden, weil sie die beste Möglichkeit zur Problemlösung bieten, sondern weil sie den Fähigkeiten der verwendeten Tools entsprechen. Das ist praktisch die IT-Version der Weisheit „wenn man einen Hammer hat, muss alles ein Nagel sein“. Die Richtlinien sind: „ Wir müssen Dinge festnageln.“ Festgefahrene Tools werden Teil des IT-Ökosystems. Aber die besten IT-Richtlinien sollten nicht vom Tool abhängen. In den 90er- oder den Nullerjahren entwickelte Tools können diese Flexibilität nicht bieten.

Das Ergebnis dieser beiden Probleme

Wenn Unternehmen versuchen, mithilfe älterer Tools Asset-Visibilität in modernen Umgebungen zu schaffen, wird ihr Asset-Discovery- und -Inventory-Prozess:

- **Komplex:** Sie müssen immer mehr Tools hinzufügen, nur um ihre Assets zu identifizieren, und jedes dieser Tools muss in die anderen integriert werden.
- **Teuer:** Sie zahlen für teure Software – und die Support-Teams bzw. -Infrastruktur, die niemand verwendet, ist wahrscheinlich veraltet und verbraucht Ressourcen.
- **Veraltet:** Sie produzieren unvollständige Daten, die oft Tage, Wochen oder sogar Monate zu spät vorliegen und nicht den aktuellen Zustand des Netzwerks widerspiegeln.

Zusammenfassung: Organisationen brauchen eine neue Möglichkeit, um Asset-Visibilität in modernen Netzwerken aufzubauen.

Überdenken Sie Ihre alten Tools zur Asset-Visibilität

Zunächst müssen Sie entscheiden, ob Ihre alten Tools für die Asset-Visibilität Ihnen noch zu Diensten stehen.

Wenn Sie Schwierigkeiten haben, Visibilität in Ihrem gesamten Bestand zu schaffen, müssen Sie möglicherweise die Nutzung eines oder mehrere Ihrer bisherigen Tools einstellen und diese durch moderne Optionen ersetzen.

Welche Funktionen sind für ein modernes Toolset für die Asset-Verwaltung wichtig?

Die Tools oder Plattformen, die Sie für Asset-Discovery und -Inventory verwenden, sollten über folgende Eigenschaften verfügen:

- Genauigkeit
- Geschwindigkeit
- Skalierung
- Benutzerfreundlichkeit

Sie sollten die erforderliche Asset-Visibilität entwickeln für:

1. **Einblicke in die Endpunkte, derer Sie sich nicht bewusst sind, um das Risiko zu reduzieren.**Nicht sichtbare Endpunkte lassen sich nicht verwalten. Die vielfältige, dynamische und dezentral verteilte Infrastruktur von heute schafft eine komplexe Umgebung, in der sich Endpunkte leicht verstecken können und sich ständig ändern, wodurch die Sicherheitsrisiken steigen. Sie sollten für Folgendes sorgen:
   - Entdeckung aller Endpunkte in Ihrer Umgebung innerhalb von Minuten – nicht Tagen oder Wochen – einschließlich schwer zu findender Endpunkte in entfernten Subnetzen.
   - Nachverfolgung eines Echtzeit-Bestands, in dem kontinuierlich neue Assets entdeckt und kategorisiert werden und es Ihnen möglich ist, diese zu verwalten.
2. **Wertsteigerung Ihrer CMDB mit genauen Echtzeitdaten.**Die meisten älteren Tools können nur eine einzige Frage für eine einzelne Asset-Klasse beantworten, was Unternehmen zum Einsatz Dutzender komplexer, individueller Produkte zwingt.Die IT-Teams versuchen dann, die von diesen Punktlösungen bereitgestellten Daten in ihre CMDB zu integrieren, zu zentralisieren und zu normalisieren. Die Folge davon sind ungenaue und unzureichende Asset-Daten. Eine bessere Vorgehensweise wäre:
   - Die Verbindung mit Ihrer CMDB unter der Gewissheit, dass Endpunkt- und Nutzungsdaten aktuell und zutreffend sind.
   - Der regelmäßige Export Ihrer Asset-Daten nach einem Zeitplan in die CMDB, basierend auf den Anforderungen für eine konsistente Berichterstattung, bessere Zusammenarbeit und fundierte Entscheidungsfindung.
   - Schaffung einer Single Source of Truth, die von Sicherheits-, Betriebs-, Risiko-, Beschaffungs-, Finanz- und Führungsteams verwendet wird.
3. **Vermeiden Sie unnötige Hard- und Softwarekosten.** Unternehmen können heute nur schwer erkennen, welche Software auf den Rechnern installiert ist und wie stark sie verwendet wird. Sie können ihre Software weder für Audits noch für Wiederverwendungszwecke genau bewerten. Das führt zu hohen Softwareausgaben – sowohl bei den Audit-Gebühren als auch bei den wiederkehrenden Lizenzkosten. Sie sollten für Folgendes sorgen:
   - Eine vollständige Liste der Software nach Produkt oder Anbieter in Ihrer Umgebung muss jederzeit verfügbar sein.
   - Nicht autorisierte oder nicht ausgelastete Software muss auffindbar sein, um Lizenzen zurückzufordern oder neu zu verteilen.
   - Sofort einsatzbereites Reporting muss verwendet werden, um Nutzungsstatistiken auf einen Blick zu verstehen.

Halten Sie mit dem vierstufigen Zyklus der Asset-Visibilität die Cyber-Hygiene aufrecht

Als Nächstes sollten Sie erkennen, dass die Schaffung von Asset-Visibilität und Cyber-Hygiene kein einmaliges Projekt ist. Ihre Umgebung verändert sich ständig und erfordert für ein klares Bild und grundlegende Sicherheit im jetzigen Zustand einen kontinuierlichen Prozess.

Viele unserer Kunden nutzen den folgenden Prozess, um für eine effektive Visibilität und Cyber-Hygiene ihrer Assets zu sorgen:

SCHRITT 1

Sorgen Sie für Visibilität, indem Sie die gesamte Umgebung zunächst einmal umfassend scannen.

SCHRITT 2

Finden Sie Probleme, indem Sie unbekannte, nicht verwaltete und anfällige Assets in der Umgebung aufdecken.

SCHRITT 3

Schützen Sie Ihre Geräte und andere Endpunkte, indem Sie Schwachstellen schließen und unbekannte und nicht verwaltete Endpunkte so gut wie möglich kontrollieren.

SCHRITT 4

Etablieren Sie eine kontinuierliche Asset-Überwachung; wiederholen Sie diesen Zyklus, wenn neue Assets hinzukommen und sich der Status bekannter Assets ändert.

Denken Sie über die Cyber-Hygiene hinaus und legen Sie die Grundlage für Zero Trust

Schließlich sollte Cyber-Hygiene nur der erste Schritt zu einer höheren Sicherheit in Ihrer Organisation sein. Die richtige Fähigkeit zur Asset-Visibilität bildet auch die Grundlage für nahezu jede Zero-Trust-Strategie oder -Lösung, die Sie umsetzen möchten.

Wenn alle Geräte Netzwerkgeräte sind, gehen von allen diesen Geräten potenzielle Schwachstellen für die Sicherheit aus. Daher benötigen Sie Richtlinien und Verfahren, die Endpunkte in drei Kategorien unterteilen: verwaltet, nicht verwaltet und keine Verwaltung möglich.

Endpunkt-Discovery ist der erste entscheidende Schritt für den Trend hin zu Zero-Trust-Lösungen. CSO Online beschreibt Zero Trust als „ein Sicherheitskonzept, das auf der Überzeugung basiert, dass Unternehmen nicht automatisch allen Ressourcen innerhalb oder außerhalb der Schutzzone Ihres Netzwerks vertrauen sollten und stattdessen alle Zugriffe auf ihre Systeme genau überprüfen müssen, bevor sie diese gewähren."

Tools für Threat Response und die Behebung von Bedrohungen sind nur so gut wie die Breite der Endpunkte, auf denen sie ausgeführt werden. Und da der Endpunkt die Zone des Netzwerks erweitert, beginnt Cyber-Hygiene und -Sicherheit tatsächlich mit der Endpunkt-Discovery, und die Implementierung einer Zero-Trust-Praxis ist der nächste sinnvolle Schritt auf diesem Weg.

Neun Möglichkeiten, wie Tanium die Asset-Entdeckung und -Inventarisierung verbessert

1. Unbekannte Endpunkte auffinden
2. Endpunktdaten kontinuierlich erfassen
3. Verlorene Assets katalogisieren
4. Den Prozentsatz der verwalteten Endpunkte erhöhen
5. Die mittlere Verwaltungszeit senken
6. Die Softwarenutzung und die prozentuale Abdeckung verfolgen Endpunkte auffinden
7. Ressourcen neu zuweisen
8. Investitionen optimieren
9. Risiko und Ineffizienz mindern

Verbessern Sie die Asset-Visibilität und die Cyber-Hygiene – ab heute

Mit herkömmlichen Tools erfassen Sie veraltete, ungenaue und unvollständige Daten aus Ihren Assets und können die Cyber-Hygiene nur schwer aufrechterhalten.

Die Tanium Platform bietet eine skalierbare Single Pane-of-Glass für die Asset-Erkennung und -Verwaltung in der Fertigung. Erfahren Sie mehr und probieren Sie Tanium noch heute kostenlos aus.

Mehr über Tanium erfahren

Tanium testen →

Als branchenweit einziger Anbieter von konvergentem Endpunktmanagement (XEM) führt Tanium den Paradigmenwechsel bei herkömmlichen Ansätzen zur Verwaltung komplexer Sicherheits- und Technologieumgebungen an. Nur Tanium schützt jedes Team, jeden Endpunkt und jeden Arbeitsablauf vor Cyber-Threats, indem es IT, Compliance, Security und Risk in eine einzige Plattform integriert, die umfassende Visibilität über alle Geräte hinweg, einen einheitlichen Satz von Kontrollen und eine gemeinsame Taxonomie für einen einzigen gemeinsamen Zweck bietet: den Schutz kritischer Informationen und Infrastruktur.

Besuchen Sie uns auf www.tanium.de