TANIUM

Das „Inside-out“-Unternehmen: Neudefinition von IT-SecOps für den heutigen Remote-First-Arbeitsplatz

Mit Veränderung kommt die Chance.

Das „Inside-out“-Unternehmen: Neudefinition von IT-SecOps für den heutigen Remote-First-Arbeitsplatz

Die Pandemie hat die IT von Unternehmen für immer verändert. Der schnelle Wechsel zu einem Homeoffice-Modell (Work from Home, WFH) zwang IT-Organisationen dazu, Remote-Mitarbeiter standardmäßig zu unterstützen. Prozesse für die Sicherheit und den Betrieb der IT, bei denen angenommen wurde, dass Mitarbeiter immer vor Ort sein würden, waren plötzlich überholt.

Jetzt passen sich die IT-Teams von Unternehmen an eine neue IT-Landschaft an, in der die Belegschaft größtenteils oder vollständig auf unbestimmte Zeit remote arbeiten kann. Immer mehr Anwendungen und gespeicherte Daten werden in die Cloud verlagert. Und Cyberkriminelle, die diese Veränderungen beobachten, konzentrieren ihre Aufmerksamkeit auf neue Ziele und neue Angriffsformen.

Vergleichen Sie die heutige IT-Landschaft mit der vor zehn Jahren und Sie können sehen, dass die traditionelle Unternehmens-IT auf den Kopf gestellt wurde. Mitarbeiter arbeiten von zu Hause aus oder an anderen entfernten Standorten. Anwendungen und Daten, die einst auf intern verwaltete Rechenzentren konzentriert waren, werden nun über mehrere öffentliche und private Clouds verteilt.

In diesem E-Book betrachten wir drei Herausforderungen im Zusammenhang mit der Verwaltung von Clients – IT-Endpunkten, einschließlich Server, Desktops, Laptops, Tablets und Smartphones – im „Inside-out“-Unternehmen. Diese Herausforderungen sind:

- Asset-Inventar, Bewertung von Schwachstellen und Patch-Management
- Help-Desk-Reaktion und Mitarbeiterproduktivität
- Client-Sicherheit

Wir zeigen, wie das „Inside-out“-Modell mit vielen der Tools und Prozesse bricht, auf die IT-Unternehmen seit Jahrzehnten setzen. Gleichzeitig birgt es jedoch Chancen für eine flexiblere, agilere und sicherere IT-Umgebung und verbessert gleichzeitig das Mitarbeitererlebnis.

Asset-Erfassung, Bewertung von Schwachstellen und Patch-Management

Bevor Sie die Endpunkte von Mitarbeitern verwalten können, müssen Sie wissen, wie viele es gibt und wo sie sich befinden. Sie müssen zur Verwaltung von Softwarebereitstellungen, Updates und Patches auch die Hardware- und Softwarekonfigurationen katalogisieren können.

In traditionellen Unternehmensumgebungen haben sich diese Informationen leicht erfassen lassen – zumindest theoretisch. Fast alle Endpunkte befanden sich im internen Netzwerk. Sie konnten Software ausführen, die das Netzwerk gescannt und entdeckt hat. Da die IT-Abteilung alle Endpunkte ausgewählt und bereitgestellt hat, war keine große Vielfalt an Endpunkten zu erwarten.

Einige Remote-Mitarbeiter und Vertriebsmitarbeiter sind möglicherweise häufig unterwegs und haben andere Arten von Geräten (wie MacBooks in einer Organisation, welche sonst die Nutzung von PCs angeordnet hat). Aber diese Mitarbeiter kehrten fast immer irgendwann ins Büro zurück. IT-Mitarbeiter konnten ihre Systeme visuell überprüfen. Überraschungen waren selten zu finden – oder das glaubten zumindest die IT-Organisationen.

Selbst in dieser kontrollierten Umgebung kam die Asset-Erfassung leider oft zu kurz. Herkömmliche Tools zur Asset-Erfassung übersehen häufig bis zu 10–20 % der Endpunkte. Diese nicht entdeckten Endpunkte blieben dann von Software-Updates und Patch-Routinen ausgeschlossen. Sie wurden anfälliger für Angriffe und gefährdeten mit größerer Wahrscheinlichkeit die Leistung und das Erlebnis der Mitarbeiter.

In der heutigen Welt des Homeoffice ist alles möglich, wenn es um den Standort, die Konfiguration und den Status von Endpunkten geht. Mitarbeiter verwenden Laptops und Desktops, die von der IT bereitgestellt werden, aber wahrscheinlich zudem auch andere tragbare Geräte, einschließlich ihrer persönlichen Laptops, Tablets und Smartphones. Diese Geräte werden in Heimnetzwerken und öffentlichen WLAN-Hotspots wie in Cafés genutzt. Diese Geräte befinden sich nicht im lokalen Netzwerk des Unternehmens. Meistens sind sie auch nicht mit einem virtuellen privaten Netzwerk (VPN) verbunden.

Wenn eine IT-Organisation diese Geräte katalogisieren, bilanzieren und angemessen verwalten möchte, muss sie sich auf Technologie verlassen, die über normale Internetverbindungen funktioniert und kein VPN erfordert.

Die Genauigkeit der Tools zur Asset-Erfassung muss verbessert werden, damit sich alle Geräte erkennen und nachverfolgen lassen, und nicht nur 80 % davon. Und da das „Inside-out“-Unternehmen bleiben wird, müssen die nötigen Tools vorhanden sein, damit Remote-Endpunkte kontinuierlich erkannt und verwaltet werden können – und nicht nur im Rahmen eines tiefgreifenden Sonderprojekts.

Help-Desk-Support und Mitarbeiterproduktivität

Der Help-Desk ist eine weitere IT-Funktion, die vom „Inside-out“-Unternehmen nachhaltig verändert wurde.

Wenn ein Mitarbeiter zuvor ein Problem hatte, konnte er den Help Desk oder den Service Desk anrufen oder eine E-Mail senden. Um das Problem zu lösen, konnte ein Help-Desk-Mitarbeiter mit dem betroffenen Mitarbeiter sprechen, Fragen stellen und Ratschläge geben.

Bei schwierigen Problemen konnte der Agent die Remote-Zugriffssoftware verwenden, um eine Verbindung zum Endpunkt des Mitarbeiters herzustellen. Bei besonders schwierigen Problemen konnte der Help-Desk-Mitarbeiter den Flur hinuntergehen, das Büro oder den Arbeitsplatz des Kollegen aufsuchen und direkt bei der Problembehandlung mitwirken.

Die meisten dieser Ansätze lassen sich jetzt so nicht mehr durchführen. Hier sind die Gründe dafür:

- Remote-Zugriffssoftware erfordert in der Regel eine Verbindung über ein lokales Netzwerk oder ein VPN: Keines davon ist für die heutigen Remote-Mitarbeiter verfügbar.
- Help-Desk-Mitarbeiter können nicht zu den Schreibtischen der Kollegen gehen, da diese aus der Ferne arbeiten.
- Die Kommunikation per Telefon ist weiterhin möglich, aber die telefonische Fehlerbehebung gestaltet sich schwierig. Der Help-Desk-Mitarbeiter kann nicht erkennen, wie das System konfiguriert ist, oder sehen, welche Prozesse darauf derzeit ausgeführt werden.

Für dieses Problem gibt es zwei Lösungen.

1. Unternehmen sollten Client-Management-Lösungen finden, mit deren Hilfe sich Help-Desk-Mitarbeiter mit Remote-Endpunkten verbinden und diese überprüfen können, ohne eine VPN-Verbindung zu benötigen. Diese Lösungen müssen sich sicher über Standard-Internetverbindungen verbinden können, sodass ein Help-Desk-Mitarbeiter auch ohne VPN Endpunkte sicher in Echtzeit untersuchen und Probleme beheben kann.
2. Unternehmen sollten Self-Service-Optionen für die Remote-Fehlerbehebung und das Patching in Betracht ziehen. Angenommen, der Help-Desk arbeitet mit einem Remote-Mitarbeiter zusammen und stellt fest, dass durch ein Upgrade einer Anwendung das Leistungsproblem am Endpunkt des Mitarbeiters gelöst werden kann. Wenn es ein sicheres Self-Service-Portal für Anwendungs-Upgrades gibt, kann der Help-Desk-Mitarbeiter den betroffenen Kollegen einfach zu diesem Portal weiterleiten. Der Mitarbeiter kann die Aktualisierung durchführen, wann es für ihn am bequemsten ist, und der Help-Desk kann zur Ticketwarteschlange zurückkehren und einen anderen Mitarbeiter unterstützen, der Hilfe benötigt.

Von einem Self-Service-Modell profitieren alle Beteiligten. Die Mitarbeiter erhalten eine schnelle Lösung für ihre Probleme und der Help-Desk benötigt weniger Zeit für Upgrade- und Patching-Mechaniken. Die Mitarbeiter sind es gewohnt, Updates auf ihren persönlichen Mobilgeräten zu installieren. Dieses Modell greift diese Vorgehensweise einfach auf und wendet sie auch auf die Computer des Unternehmens an.

Wenn Remote-Mitarbeiter Probleme schneller lösen können, verbessert sich ihre Produktivität und auch das Nutzererlebnis bei der Arbeit gewinnt an Qualität.

Client-Sicherheit

Der dritte kritische Punkt ist die Client-Sicherheit. Im „Inside-out"-Unternehmen sind die Endpunkte der Mitarbeiter nicht sichtbar und in Bezug auf ihre Software-Patches wahrscheinlich veraltet. Schlimmer noch: Cyberkriminelle wissen, dass Mitarbeiter im Homeoffice anfälliger sind als vor Ort hinter einer Firewall des Unternehmens. Sie erstellen Phishing-Nachrichten und andere Arten von Angriffen, die speziell auf isolierte Mitarbeiter abzielen.

Fast drei Viertel der Unternehmen in den USA und Großbritannien mussten im vergangenen Jahr eine Art von Datenschutzverletzung aufgrund eines Phishing-Angriffs hinnehmen, so das E-Mail-Sicherheitsunternehmen Egress.[1]

[1] https://www.itproportal.com/news/phishing-attacks-hit-a-huge-number-of-businesses-last-year/

Neben dem Erkennen, Aktualisieren und Patching von Remote-Endpunkten benötigen IT-Organisationen eine Möglichkeit, um:

- Remote-Endpunkte auf Sicherheitsschwachstellen und Bedrohungen zu scannen
- Alle Patches oder Konfigurationsänderungen anzuwenden, die erforderlich sind, um Schwachstellen zu beheben und Compliance-Anforderungen zu erfüllen
- Endpunkte zu konfigurieren, damit häufig von Angreifern zur Verbreitung von Malware verwendete Ports und Pfade geschlossen werden können
- Schnell jeden Angriff auf einen Endpunkt zu stoppen, sobald der Angriff erkannt wurde

Auch hier benötigen IT-Abteilungen Visibilität und Kontrolle über Endpunkte, ohne dass VPN-Verbindungen die Grundvoraussetzung sind. Wenn ein Endpunkt angegriffen wird, können Sie nicht erwarten, dass sich ein Mitarbeiter dann über VPN mit der Zentrale verbindet. IT-Teams müssen so auf den Endpunkt zugreifen können, wie er ist – und ohne Start einer neuen Netzwerkverbindung, die möglicherweise die Verbreitung von Malware beschleunigen könnte.

Die Client-Sicherheitssoftware sollte ohne VPN-Verbindung in der Lage sein:

- Endpunkte zu scannen und zu analysieren
- Angriffe zu erkennen
- Warnungen über Angriffe und Patch-Anforderungen auszugeben
- Analysten des Security Operation Centers (SOC) Echtzeit-Visibilität in Endpunktaktivität zu ermöglichen
- Angriffe durch sofortige Isolation von Endpunkten einzudämmen

ANWENDERBERICHT

Eindämmung eines Ransomware-Angriffs bei Ring Power

Die Vorteile des dezentralen Client-Managements in Echtzeit zeichneten sich vor Kurzem für Ring Power Corp., einen Schwermaschinenhändler mit Sitz in Saint Augustine, Florida, deutlich ab.

Als ein Manager auf eine Phishing-E-Mail klickte, wurde das Unternehmen von einem Ransomware-Angriff getroffen. Dieser legte alle 150 Server im Rechenzentrum des Unternehmens und die 2.300 Endpunkte lahm, welche die Mitarbeiter zur täglichen Arbeit nutzten.

Glücklicherweise hatte das Unternehmen soeben Tanium-Lösungen für das Client-Management gekauft, einschließlich Module für die Erfassung und Bestandsaufnahme von Assets, Risiko- und Compliance-Management, Sensitive Data Monitoring und das Threat Hunting.

Mit der Hilfe von Tanium konnten Kevin Bush, VP of IT, und sein zehnköpfiges 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 überhaupt mit den Angreifern zu kommunizieren.

Anstatt eine Zahlung auszuhandeln, wurden die Systeme heruntergefahren, die Backups, isoliert, damit sie nicht durch Malware beschädigt wurden, alle Endpunktgeräte von den 26 Standorten des Unternehmens eingesammelt und von Malware bereinigt. Dabei wurde auch Tanium auf jedem Endpunkt installiert. Der Betrieb wurde mit bereinigten und jetzt geschützten Endpunkten wieder aufgenommen.

„Tanium bringt für unser gesamtes Team Visibilität auf einen Bildschirm“, so Bush. „Wenn man diese Art von Visibilität nicht hat, kann man nachts nicht schlafen.“

Laden Sie hier den vollständigen
Ring Power Anwenderbericht herunter.

Fazit

Das „Inside-out"-Unternehmen hat den Alltag für Mitarbeiter und die IT-Organisationen, die sie unterstützen, für immer verändert. Diese Transformation bringt Herausforderungen, aber auch Chancen mit sich. Insbesondere bietet es IT-Organisationen die Möglichkeit:

- Umfassende Tools zur Asset-Bestandsaufnahme zu implementieren, damit IT-Organisationen die 10–20 % der Endpunkte finden, verwalten und sichern können, die von herkömmlichen Tools übersehen werden.
- Genauere und zeitnahe Informationen über den Status von Endpunkten zu erhalten, damit sie schneller und effektiver gepatcht und aktualisiert werden können.
- Die Help-Desk-Effizienz zu verbessern, indem sich Mitarbeiter in Echtzeit mit Endpunkten an jedem Standort verbinden und Kollegen ihre eigenen Probleme schnell und einfach durch Self-Service-Vorgänge lösen können.
- Remote-Mitarbeitern eine bessere Endpunktsicherheit zu bieten, damit sie den neuesten Formen von Cyberangriffen standhalten können und damit infizierte Endpunkte keine großen Bereiche des Unternehmensnetzwerks gefährden.
- Die Sicherheitsbereitschaft zu verbessern, damit Angriffe schnell und effizient eingedämmt und abgeschwächt werden können (wie es Ring Power bei einem Angriff mit Ransomware möglich war).

Die IT-Landschaft von Unternehmen hat sich für immer verändert. Aber mit den richtigen Tools und der passenden Strategie für das Client-Management kann diese Änderung als Katalysator für großartige Neuerungen dienen: umfassendere und effizientere IT-Operations, ein verbessertes Nutzererlebnis der Mitarbeiter und robustere IT-Sicherheit für die Mitarbeiter überall, sodass die Mitarbeiterproduktivität an jedem Standort und auf jedem Gerät besser als je zuvor ausfällt.

Erfahren Sie, wie die Tanium Lösung Client Management Ihrem Unternehmen dabei helfen kann, diese Herausforderungen im heutigen „Inside-out"-Unternehmen zu meistern.