IDC
Analyze the Future

I D C T E C H N O L O G Y S P O T L I G H T

Das Netzwerk als Sicherheitssensor und Kontrollinstrument

Oktober 2015

Adaptiert von *Worldwide Enterprise Network Infrastructure Forecast*, 2015–2019, Autoren: Nolan Greene, Rohit Mehra, Rich Costello u. a., IDC #258012

Gesponsert von Cisco

Bei der Umsetzung von Geschäftszielen spielen Unternehmensnetzwerke heute eine wichtigere Rolle als je zuvor. Als Folge dieser Entwicklung fließen größere Mengen sensibler Daten über Kabel- und Wireless-Netzwerke. Diese Fülle an wertvollen Daten gerät zunehmend ins Visier von Hackern und Malware. Die vernetzten Informationen und die verteilte Struktur des Netzwerks, welche das Angriffsziel vieler Cyberkrimineller sind, bieten alle Voraussetzungen für ein proaktives Security-Tool. Mithilfe von Transparenz und der Segmentierung des Datenverkehrs kann ein modernes Unternehmensnetzwerk als Sicherheitssensor und Kontrollinstrument eingesetzt werden.

Einführung

Mit der Einführung einer Netzwerkinfrastruktur, die von IDC als „dritte Plattform“ bezeichnet wird, entsteht derzeit ein neues Technologie- und Anwendungskonzept für Cloud, Mobility und Social-Business. Das Netzwerk ist heute ein zentraler Faktor für die Innovationsfähigkeit eines Unternehmens. Einer der Gründe für diese Entwicklung ist der zeitlich uneingeschränkte Zugriff auf geschäftskritische Anwendungen, der mit Einführung der dritten Plattform möglich wurde und die Zusammenarbeit durch den Abbau zeitlicher und geografischer Hürden erleichtert. Die rasante Verbreitung neuer Geräte und Anwendungen in den Unternehmen hat dazu geführt, dass die im Netzwerk übertragenen Daten erheblich sensibler geworden sind. Dementsprechend sind auch die Anforderungen an die Netzwerksicherheit vom Core bis zum Edge gestiegen. Tatsächlich dürften rund 80 % der Unternehmen von mindestens einer erfolgreichen Sicherheitsverletzung betroffen sein. Der durchschnittliche Schaden durch Sicherheitsbedrohungen und Angriffe beläuft sich, selbst bei Nichtbeachtung der schwerwiegendsten Vorfälle, auf 1,3 Mio. USD.

Auf den Punkt gebracht: Unternehmensnetzwerke waren noch nie so komplex wie heute. Jede einzelne Netzwerkverbindung, sei es durch Knoten, Apps, Zertifikate, Geräte, Benutzer oder die Cloud, könnte eine Virusinfektion oder Sicherheitsverletzung des Netzwerks bedeuten. Wird ein solcher Vorfall nicht sofort entdeckt und bekämpft, besteht die Gefahr, dass sich ein Malware-Code oder ein ähnlicher Angriff rasch im gesamten Netzwerk ausbreitet. Die intelligente Anbindung der Netzwerkressourcen, die eine große Angriffsfläche für Hacker bildet, kann gleichzeitig als hocheffizientes Abwehrsystem gegen Bedrohungen eingesetzt werden. Intelligente Netzwerkfunktionen können dazu eingesetzt werden, um viele verschiedene Angriffstypen und Sicherheitsverletzungen proaktiv zu erkennen und zu beheben. Durch diese Fortschritte im Bereich der Netzwerkintelligenz lässt sich das Netzwerk als Sensor einsetzen, der schnelle Einblicke in Netzwerkbedrohungen ermöglicht. Ein Netzwerk, das seine normalen Prozesse genau kennt, identifiziert jede ungewöhnliche Aktivität in sehr kurzer Zeit. Im Zuge der Entwicklung des Netzwerks zu einem Instrument der netzwerkweiten Zugriffskontrolle und Abwehr von Angriffen gewinnt seine Rolle als Sicherheitsressource weiter an Gewicht.

Das bewegliche Sicherheitsziel

In vielen Unternehmen sorgen BYOD-Initiativen und der Siegeszug der Mobilitätslösungen für eine Vielzahl neuer Geräte im Netzwerk. BYOD-Geräte machen den Schutz des Netzwerks zu einer komplexen Aufgabe und können das Gesamtvolumen der sensiblen Daten noch weiter vergrößern. Zudem bedeuten mehr angebundene Geräte auch mehr Endpunkte, deren Sicherheit gewährleistet werden muss. Der Wunsch von Mitarbeitern, ihre Mobilgeräte auch für geschäftskritische Aufgaben zu nutzen, hat zu einem unüberschaubaren Angebot an mobilen Cloud-Anwendungen geführt. Diese Anwendungen und ihre Daten können standortintern oder -extern, in Public- oder Private-Clouds gehostet werden und erhöhen somit die Komplexität der Datenverkehrsströme. Sie werden dann über das Unternehmensnetzwerk an verschiedene Standorte übertragen, etwa von der Unternehmenszentrale an eine Zweigstelle oder an das Mobilgerät eines externen Mitarbeiters. Die Anwendungen mit ihren großen Mengen potenziell sensibler Daten bieten nicht nur zusätzliche Angriffsflächen, sie können auch als Einfallschneisen ins Netzwerk das Risiko von Sicherheitsverletzungen erhöhen.

Auch die Ausbreitung des Internet of Things (IoT) sorgt für eine Zunahme der Netzwerkkomplexität. Das IoT ist das Netzwerk aller Netzwerke von eindeutig identifizierbaren Endpunkten (oder „Dingen"), die ohne menschlichen Eingriff per IP-Anbindung lokal oder global kommunizieren. IDC erwartet, das bis 2020 rund 30 Milliarden IoT-Geräte im Einsatz sein werden. Diese Endpunkte oder Sensoren vergrößern die Angriffsfläche im Netzwerk. In diesem frühen Entwicklungsstadium des IoT ist die Konfiguration der Sicherheitsschnittstellen noch nicht besonders intuitiv. Auch bei der Integration in die Sicherheitsinfrastruktur treten oft Schwierigkeiten auf. Die Ungewissheit bezüglich der Sicherheit des IoT ruft bei vielen Bedenken hervor. Der Nutzen des IoT liegt zum großen Teil in den Daten, die von IoT-Geräten bzw. Sensoren erfasst werden. Das Volumen, die Breite und die Tiefe dieser Daten sind beispiellos. IoT-Geräte, die bereits heute in zahlreichen Produktionsumgebungen eingesetzt werden, sammeln enorme Mengen an strukturierten und unstrukturierten Daten. Der Großteil dieser Daten benötigt ein hohes Maß an Sicherheit und Datenschutz. Um das volle Potenzial des IoT auszuschöpfen, ist eine umfassende Integration der Netzwerksicherheit notwendig.

Durch die ständige Weiterentwicklung der Mobility-Funktionen in Unternehmen, die Einführung produktivitätssteigernder in der Public-Cloud gehosteter Geschäftsanwendungen und der rasanten Entwicklung des IoT haben IT-Entscheidungsträger längst die Notwendigkeit erkannt, die Strategien für die Netzwerksicherheit auf den Prüfstand zu nehmen. Laut einer kürzlich veröffentlichten IDC-Studie befürchten 52 % der Sicherheitsexperten, dass ihre Mitarbeiter die Wichtigkeit von Sicherheitsrichtlinien unterschätzen. Fast genauso viele (45 %) sind wegen der zunehmenden Komplexität der Angriffe besorgt. Ein signifikanter Teil der Befragten (38 %) hält das zur Verfügung stehende Budget für unzureichend, um angemessen auf neue Herausforderungen reagieren zu können.

In Verbindung mit den Schwierigkeiten, angemessene Mittel und Unterstützung für die Netzwerksicherheit bereitzustellen, können diese wachsenden Herausforderungen dafür sorgen, dass die Erkennung und die Bekämpfung von Sicherheitsverletzungen durch die IT zu spät erfolgen und präventive Maßnahmen gegen ähnliche Verstöße in der Zukunft nur schleppend umgesetzt werden. Den Erkenntnissen von IDC zufolge vergeht mehr als ein Jahr, bis sich Aktualisierungen der Sicherheitsinfrastruktur der dritten Plattform, wie Endgerätehärtung oder Benutzerverwaltung, innerhalb eines Unternehmens allgemein durchgesetzt haben. Im Zeitalter der dritten Plattform hat die Implementierung einer flexiblen, intelligenten und skalierbaren Sicherheitsarchitektur, die plattformbasiert und vollständig in die Netzwerkinfrastruktur integriert ist, an Bedeutung gewonnen. Dieses Bereitstellungsmodell für Netzwerksicherheit nutzt die inhärente verteilte Netzwerkintelligenz, um das Netzwerk von einer anfälligen Angriffsfläche in ein wirksames Abwehrsystem gegen Sicherheitsverletzungen zu verwandeln. Angreifer sind anpassungsfähig. Zur Gewährleistung der Netzwerksicherheit gilt es, alle Vorteile auszuschöpfen, um ebenso flexibel reagieren zu können.

Das Netzwerk als Sicherheitsressource

Aufgrund der zunehmenden Standardisierung des Netzwerkmanagements profitieren Unternehmen heute von einer beispiellosen Transparenz ihrer Netzwerke, die vom Rechenzentrum bis hin zum Edge reicht, selbst bei geografisch weit verstreuten Standorten. Diese Transparenz schließt Geräte, Benutzer und Anwendungen ein. Durch ihre wachsenden Fähigkeiten, all diese Daten zu erfassen und zu analysieren, sind Netzwerke besser als je zuvor für die Erkennung ungewöhnlicher und verdächtiger Aktivitäten gerüstet. Eine missbräuchliche Nutzung des Netzwerks wie Malware, anormale Datenverkehrsströme, unberechtigte Anwendungsnutzung und andere Verstöße gegen Benutzerrichtlinien sowie unberechtigte Geräte und Wireless-Access-Points (APs) werden leichter identifiziert, unter Quarantäne gestellt und mithilfe intelligenter Netzwerkfunktionen beseitigt.

Um eine effiziente Nutzung des Netzwerks zu Sicherheitszwecken zu ermöglichen, muss jeder Punkt im Netzwerk als Sensor und Kontrollinstrument verstanden werden – also jedes Endgerät und jede Anwendung in allen Rechenzentren, Zweigstellen oder Campusumgebungen. Dabei geht es nicht um einen Ersatz herkömmlicher Security-Tools wie Firewalls und Advanced Malware Protection, sondern vielmehr um deren Ergänzung. Im folgenden Abschnitt wird dargestellt, wie die End-to-End-Lösungen von Cisco für dieses Ziel eingesetzt werden können.

Der Ansatz von Cisco

Das Portfolio der Netzwerksicherheitslösungen von Cisco basiert auf dem Konzept einer integrierten und flächendeckenden Sicherheit im Netzwerk. Mithilfe von NetFlow, das die Sensorfunktion des Netzwerks ermöglicht, seiner Integration mit der Identity Services Engine (ISE) für ein präzises Richtlinienmanagement, sowie TrustSec zur Durchsetzung der Netzwerksegmentierung, lässt sich eine nahtlose Netzwerksicherheit von der Infrastruktur bis hin zum Endbenutzer verwirklichen. Die in diesem Abschnitt beschriebenen Tools ermöglichen eine vollständige Implementierung dieses Konzepts.

NetFlow und Lancope

Im Mittelpunkt des Cisco Ansatzes „Netzwerk als Sensor“ steht NetFlow, ein Tool, das kontinuierlich Datensätze der gesamten Kommunikation anlegt, die über Router und Switches sowie einige weitere Wireless-Produkte von Cisco übertragen wird. Jede Kommunikationssitzung auf einem NetFlow-fähigen Gerät bietet umfassende Transparenz und tief reichende Einblicke in sechs Bereiche, die oft von entscheidender Bedeutung sind: Netzwerk-Scans, Botnet-Erkennung, Denial-of-Service, Fragmentierungsangriffe, Änderung der Host-Reputation und Verbreitung von Würmern.

Die erfassten Daten können für künftige Verwendungen gespeichert werden und machen NetFlow so zu einem wichtigen Tool für die Identifizierung von Sicherheitsverletzungen. Detaillierte Forensik und vollständige Kommunikationsprotokolle liefern präzise Informationen zu verdächtigen Aktivitäten im Netzwerk, was eine beschleunigte Erkennung und zielgenaue Bekämpfung ermöglicht. Die Kombination aus NetFlow und Lancope StealthWatch verbessert die Netzwerktransparenz und unterstützt Echtzeit-Benachrichtigungen bei erkannten Sicherheitsbedrohungen. Die Integration von Lancope StealthWatch mit der Cisco ISE ermöglicht die Korrelation von Gerätekontextinformationen (wer, was, wo, wann und wie) sowie Datenverkehr und ermöglicht es, infizierte Geräte schnell vom übrigen Netzwerk zu isolieren.

Identity Services Engine

Die Cisco Identity Services Engine ist eine Plattform zur Verwaltung von Sicherheitsrichtlinien und erleichtert die Bereitstellung einer konsistenten Zugriffskontrolle für Kabel- und Wireless-Netzwerke sowie VPN-Verbindungen. Der sichere Benutzerzugriff über die ISE beginnt mit der Benutzerauthentifizierung und Geräteklassifizierung, welche die ISE durch kontextbezogene Informationen für bessere Entscheidungsprozesse unterstützt. Auf diese Weise wird gewährleistet, dass jederzeit ein optimales Maß an Zugriffskontrolle Anwendung findet. Auf der Grundlage präziser kontextbezogener Informationen zu Rolle, Ort und Uhrzeit kann die ISE den Netzwerkzugriff gegebenenfalls einschränken und somit umfassende Sicherheit im Hinblick auf die Tiefe und Breite des Netzwerkzugriffs garantieren. Entsprechend den Richtlinienkriterien kann die ISE für bestimmte Benutzer und Geräte eine Auswahl an definierten Zugriffen erlauben. Einheitliche Richtlinien für das gesamte Netzwerk erhöhen die Betriebseffizienz, da die aufwendige Verwaltung und Durchsetzung separater und individueller Richtlinien entfällt und die Transparenzfunktionen für die Richtliniendurchsetzung integriert sind.

Software-definierte Segmentierung mit TrustSec

Cisco TrustSec ist eine in Cisco Switches und Router sowie Wireless- und Security-Komponenten integrierte Technologie, welche Unternehmen die Software-definierte Netzwerksegmentierung ermöglicht. TrustSec setzt eine rollenbasierte, in der Cisco ISE konfigurierte Zugriffskontrolle durch und erlaubt einen sicheren Zugriff auf sensible Netzwerkressourcen, wobei Identität und Rolle berücksichtigt werden. TrustSec vereinfacht Konfiguration und Verwaltung von Richtlinien, die festlegen, wer mit wem (oder was) im Netzwerk kommunizieren darf, wer Zugriff auf Ressourcen hat und wie Systeme mit anderen Systemen kommunizieren. Die Zugriffskontrolle mit TrustSec beginnt im Rechenzentrum und reicht bis zum Zugriffs-Edge und zu den Remote-VPNs.

Vorteile durch die Nutzung des Netzwerks als Security-Tool

In einer Zeit, in der alle Kapital- und Betriebskosten auf den Prüfstand gestellt werden, ist es für Unternehmen von entscheidender Bedeutung, Investitionsentscheidungen rechtfertigen zu können und Möglichkeiten einer zusätzlichen Wertschöpfung aus dem Netzwerk zu nutzen. Im Rahmen einer Verwendung des Netzwerks als Sicherheitssensor und Kontrollinstrument können wir uns mit bereits vorhandenen, eigenen Ressourcen vor Sicherheitsverletzungen schützen, die Geschäftsprozesse stören und Ertragseinbußen bewirken können. Eine umfassende Netzwerksicherheitsinfrastruktur wie die von Cisco angebotene Lösung nutzt wertvolle Metadaten, um schnellere Einblicke in den Netzwerkverkehr zu erlauben. Die Kombination aus TrustSec und der ISE lässt eine präzise richtlinienbasierte Zugriffskontrolle mit Software-definierter Segmentierung zu, die Bedrohungen eindämmen und deren Ausbreitung im Netzwerk verhindern kann. Da NetFlow, ISE und TrustSec im gesamten Netzwerk zum Schutz der Ressourcen aktiviert werden können, ist dieses Sicherheitskonzept zudem nahtlos skalierbar.

Herausforderungen und Chancen

Diese neue Sicht auf das Unternehmensnetzwerk als zentrales Element der Sicherheitsinfrastruktur bedeutet einen signifikanten Paradigmenwechsel gegenüber konventionellen Konzepten, bei dem der Schutz mithilfe externer Ressourcen bereitgestellt wurde. Wie bei jedem grundlegenden Wandel im Denken über IT-Technologien muss Entscheidungsträgern ein Verständnis für dieses Konzept durch entsprechende Informationsangebote vermittelt werden. Manche Unternehmen, die bereits in komplexe Sicherheitsinfrastrukturen investiert haben, werden zurückhaltend auf Konzepte reagieren, die ihre aktuellen Systeme infrage stellen (insbesondere dann, wenn diese zu funktionieren scheinen). IT-Abteilungen befinden sich oft auf einer Gratwanderung zwischen der Maximierung bestehender Investitionen und Maßnahmen zur Vorbereitung der vorhandenen Infrastruktur auf die Herausforderungen von morgen. Diese Situation ist dabei keine Ausnahme.

Wie bei den meisten Herausforderungen sind auch hier große Chancen im Spiel. Die Implementierung einer Netzwerkarchitektur mit eng integrierten Sicherheitskomponenten kann eine effizientere Investition darstellen, da die Redundanzen eines Stückwerks einzelner Implementierungen vermieden werden. Wer auf die Betriebseffizienz und den Return-on-Investment des Netzwerks verweisen kann, das als Sicherheitssensor und Kontrollinstrument neue Funktionen übernimmt, hat die vermutlich stärksten Argumente für diese vielversprechende Gelegenheit in der Hand.

Zusammenfassung

Im Zeitalter der dritten Plattform übernimmt das Unternehmensnetzwerk eine neue Rolle im täglichen Betrieb: bei der Interaktion mit Kunden und Mitarbeitern, der Differenzierung im Wettbewerb und der Innovation. Angesichts der enormen Mengen sensibler Daten, die über Unternehmensnetzwerke übertragen werden, versuchen viele Hacker und Cyberkriminelle Zugriff auf diese Daten zu erhalten. Als Folgen drohen erhebliche Schäden und Beeinträchtigungen im Alltag von Kunden und Mitarbeitern, womöglich auch negative Auswirkungen auf die Reputation des Unternehmens. Die gute Nachricht: Security-Tools können heute eng mit dem gesamten Netzwerk verwoben werden und verleihen ihm völlig neue Fähigkeiten zur Bekämpfung künftiger Angriffe. Eine Netzwerkinfrastruktur mit eng integrierten Sicherheitsfunktionen ist in diesem Zeitalter unverzichtbar. Die von Cisco angebotenen Lösungen sind die richtige Antwort auf diese Herausforderungen.

ÜBER DIESE PUBLIKATION

Diese Publikation wurde von IDC Custom Solutions veröffentlicht. Die Meinung, Analyse und die Forschungsergebnisse in diesem Dokument stammen aus einer detaillierteren Studie und Analyse, die unabhängig durchgeführt und von IDC veröffentlicht wurden, sofern keine anderen Quellen angegeben werden. IDC Custom Solutions stellt IDC-Inhalte in unterschiedlichen Formaten für die allgemeine Veröffentlichung durch verschiedene Unternehmen bereit. Aus einer Lizenz zur Veröffentlichung von IDC-Inhalten kann keine Billigung des Lizenznehmers und keine Stellungnahme zu diesem abgeleitet werden.

Weltweite Hauptgeschäftsstelle: 5 Speen Street Framingham, MA 01701, USA Tel.: +1-508-872-8200 Fax: +1-508.935.4015 www.idc.com