Netzwerke der nächsten Generation: Sicherheit für heute und morgen

Wenn Netzwerke vor modernen Bedrohungen geschützt werden sollen, die für veraltete Anforderungen entwickelt wurden, entstehen für das Unternehmen Sicherheitslücken.

Computing-Umgebungen in Unternehmen entwickeln sich als Reaktion auf die Annäherung von IT an den Verbraucher, auf Mobilität und Cloud Computing rasch weiter. Durch diese Trends ergeben sich für das Unternehmen neue strategische Möglichkeiten — und neue Risiken und Sicherheitslücken. Die IT-Abteilungen müssen einen Weg finden, die Vermögenswerte des Unternehmens zu schützen und gleichzeitig dem Unternehmen zu ermöglichen, Nutzen aus diesen neuen Trends zu ziehen. Dies kann komplizierter als nötig sein, wenn die IT-Abteilung ein Netzwerk unterstützt, das „Good-enough" (gerade gut genug) ist. Dieses Whitepaper befasst sich mit den Auswirkungen der Absicherung eines „Good-enough"-Netzwerks mit geringen Investitionen im Vergleich zu einem Netzwerk der nächsten Generation, das eine sicherere IT-Umgebung unterstützt.

Das Netzwerksicherheitsmodell von gestern

Vor nicht allzu langer Zeit war das Absichern der IT-Umgebung einfacher als heute. Bei grundlegenden Informationen wie z. B. dem Standort der Benutzer, den ausgeführten Anwendungen und den verwendeten Gerätetypen handelte es sich um bekannte Variablen. Zudem waren diese Informationen verhältnismäßig statisch, sodass die Sicherheitsrichtlinien vergleichsweise einfach skaliert werden konnten. Die Anwendungen wurden auf dedizierten Servern im Datencenter ausgeführt. IT-Abteilungen kontrollierten den Zugriff auf diese Anwendungen und richteten Grenzen zur Durchsetzung der Sicherheitsrichtlinien ein. Die Anwendungen und Endgeräte waren gesichert, und der Netzwerkzugriff wurde beschränkt. Das Netzwerk diente dazu, in einer Client-/Serverarchitektur Benutzer mit IT-Ressourcen zu verbinden. Zudem wies das Netzwerk, zumindest größtenteils, vorhersagbare Datenverkehrsmuster auf.

Die sich rasch entwickelnden Computing-Trends wirken sich in zweierlei Hinsicht auf die Netzwerksicherheit aus. Zunächst verändern sie die Netzwerkarchitektur. Die Netzwerk-Edge musste weiterentwickelt werden, da unterschiedliche Mobilgeräte von verschiedenen Standorten aus auf das Unternehmensnetzwerk zugreifen. Auch die Anwendungen selbst sind in Bewegung geraten — sie werden virtualisiert und möglicherweise zwischen Servern oder sogar Datencentern verschoben. Gleichzeitig erweitern die Benutzer das Unternehmensnetzwerk, indem sie in der Cloud kollaborative Anwendungen wie z. B. Dropbox oder Google Docs verwenden. Die IT-Abteilung weiß weder, welche Geräte eine Verbindung mit dem Netzwerk herstellen, noch von wo aus dies erfolgt. Es handelt sich nicht mehr nur um von der IT bereitgestellte Anwendungen. Die Daten sind nicht sicher im Datencenter gespeichert. Sie durchqueren auf Smartphones und Tablet-PCs das ganze Land und befinden sich in der Cloud und somit außerhalb des IT-Bereichs.

Ein zweiter Trend, der die Netzwerksicherheit beeinflusst, sind die zunehmend komplexen und ausgeklügelten Bedrohungen. Die Netzwerke von gestern wurden von breit angelegten Angriffen heimgesucht. So sendeten die Hacker

SONDERVERÖFFENTLICHUNG VON
CSO Custom Solutions Group

UNTERSTÜTZT VON
CISCO

Anfängliche Kosteneinsparungen werden rasch aufgefressen, da „Good-enough“-Netzwerke nicht über integrierte Sicherheit verfügen. Daher muss die IT-Abteilung Risiken mit mehreren Einzellösungen begegnen.

UNTERSTÜTZT VON

CISCO

beispielsweise zwei Millionen Spam-E-Mails, die ein bekanntes Risiko oder eine Sicherheitslücke ausnutzten. Dabei wurde darauf gehofft, dass ein bestimmter Anteil der Empfänger die E-Mail öffnen und auf den Angriff hereinfallen würden.

Nun hat sich das Angriffsmodell umgekehrt. Hacker zielen nicht mehr auf eine große Zahl von Personen ab. Auch nutzen sie keine bekannten Sicherheitslücken mehr aus. Stattdessen führen sie komplexere und gezieltere Angriffe durch. Hacker können beispielsweise die sozialen Netzwerke nutzen, um Informationen über die Zielperson zu erhalten, und anschließend das Vertrauen der Benutzer in eine Anwendung oder einen anderen Benutzer ausnutzen, um Malware zu installieren oder Daten zu stehlen. Diese sehr gezielten Angriffe sind wahrscheinlicher als breit angelegte Angriffe, da die Hacker noch lange nachdem der Schaden angerichtet wurde unentdeckt bleiben.

Sichern des „Good-enough“-Netzwerks

Leider werden die Sicherheitsbemühungen der IT-Abteilungen von einer weiteren Entwicklung verkompliziert. Einige Analysten und Anbieter verleiten die IT-Abteilungen dazu, das Netzwerk als Gebrauchsgut zu betrachten. Es wird also behauptet, dass ein beliebiges Netzwerk ausreiche, und dass die IT-Abteilungen lediglich ein günstig zu beschaffendes Netzwerk implementieren müssten, das „gut genug“ ist. Anfängliche Kosteneinsparungen werden jedoch rasch aufgefressen, da solche Netzwerke nicht über integrierte Sicherheit verfügen. Daher muss die IT-Abteilung Risiken mit mehreren Einzellösungen entgegentreten — und somit mehr Zeit und Anstrengung in das Bereitstellen, Konfigurieren und Verwalten der Lösungen investieren. Die IT-Sicherheit kann mit den Sicherheitsrisiken nicht Schritt halten, geschweige denn, diese vorhersagen. Da Einzellösungen nicht integriert sind, kann die Durchsetzung konsistenter Sicherheitsrichtlinien in der gesamten IT-Umgebung erschwert werden. Was die Verteidigung angeht, so kann die IT-Abteilung Netzwerkangriffe besser abwehren, wenn sie über mehr Kontext verfügt. Wenn die Informationen verschiedener Systeme erst zugeordnet werden müssen, um diesen so wichtigen Kontext zu erhalten, so ist dies kontraproduktiv.

Ein „Good-enough“-Netzwerk mit den vielen Einzellösungen ist ein instabiles Netzwerk mit einem höheren Ausfallrisiko. Sicherheitslücken oder der Absturz eines der vielen Systeme können zu Ausfallzeiten führen. Wenn das Netzwerk ausfällt, zieht es alles andere mit runter, einschließlich des Umsatzes.

Moderner Ansatz für die Netzwerksicherheit

Ein „Good-enough“-Netzwerk und dessen Folgen für die Sicherheit ist jedoch nicht die einzige Option die Ihnen offen steht. Die Innovationen bei der Netzwerksicherheit haben mit den sich schnell entwickelnden Computertrends Schritt gehalten. Ein Netzwerk der nächsten Generation berücksichtigt die Technologien von Morgen und verfügt über eine Architektur mit integrierten Sicherheitsfunktionen für einen proaktiven Schutz gegen gezielte und komplexe Bedrohungen. Es ist dieser Schutz, der es der IT-Abteilung erlaubt, mit Zuversicht strategische Unternehmensentscheidungen zu Gelegenheiten wie Mobilität und Cloud Computing zu treffen.

Ein Netzwerk der nächsten Generation bietet eine allgegenwärtige Sichtbarkeit und Steuerung mit vollständiger Kontextsensitivität. Dies sorgt im gesamten Netzwerk für Sicherheit — vom Hauptsitz bis in die Niederlassungen, für interne Mitarbeiter ebenso wie für Mitarbeiter, die mit kabelgebundenen, drahtlosen und VPN-Geräten arbeiten. Mithilfe einer Netzwerkrichtlinienarchitektur können Sicherheitsregeln erstellt, verteilt und überwacht werden, die auf einer Kontextsprache beruhen, z. B. „wer“, „was“, „wo“, „wann“ und „wie“. Bei der Durchsetzung können Maßnahmen wie z. B. das Sperren des Daten- oder Gerätezugriffs oder das Einführen einer Datenverschlüsselung ergriffen werden. Wenn beispielsweise ein Mitarbeiter von einem Smartphone eine Verbindung zum Unternehmensnetzwerk herstellt, ermittelt das Netzwerk das Gerät und den Benutzer sowie die ihm erteilten Berechtigungen. Das Richtlinienmodul richtet nicht nur Richtlinien für den Benutzer und das Gerät ein, sondern verteilt diese an alle Punkte des Netzwerks. Zudem werden beim Auftauchen eines neuen Geräts im Netzwerk umgehend die entsprechenden Informationen aktualisiert.

Integrierte netzwerkweite Richtlinien ermöglichen natürlich die sichere Umsetzung von Richtlinien für den Ansatz „Verwenden Sie Ihr eigenes Gerät“[1], mit Netzwerken der nächsten Generation können jedoch zudem Sicherheitsbedenken im Zusammenhang mit Cloud Computing gelöst werden. Auf Knopfdruck können Unternehmen den Webverkehr in weit verteilten Netzwerken intelligent umleiten, um detaillierte Sicherheits- und Kontrollrichtlinien umzusetzen.

[1] „Verwenden Sie Ihr eigenes Gerät“ bezieht sich auf einen neuen Trend, bei dem die Mitarbeiter mit privaten Geräten wie z. B. Smartphones oder Tablets auf Unternehmensressourcen zugreifen.

Wenn ein Netzwerk mit geringen Investitionsausgaben implementiert wird, laufen die IT-Abteilungen Gefahr, neue Technologien oder geschäftliche Vorhaben ablehnen zu müssen, da das Netzwerk diese nicht unterstützen kann.

UNTERSTÜTZT VON

CISCO

Das „Good-enough"-Netzwerk im Vergleich zum Netzwerk der nächsten Generation

Das Netzwerk der nächsten Generation bietet weitaus mehr als nur eine integrierte Sicherheit. Ein Netzwerk der nächsten Generation wird strategisch entwickelt, um optimal auf die aktuellen Anforderungen ausgelegt zu sein. Die Architektur ermöglicht jedoch zudem die Integration zukünftiger umwälzender Technologien und den Investitionsschutz. Mit anderen Worten: Ein Netzwerk der nächsten Generation ist ein dynamisches Netzwerk, das Mobilität, Cloud Computing und die sich verändernden Bedrohungsszenarien unterstützt. Zudem verwandelt es das Netzwerk in einen Dienstbereitstellungsmechanismus, der es CSOs erlaubt, zukünftige strategische Unternehmensanstrengungen zu unterstützen.

Beim Berechnen der Gesamtbetriebskosten für das Netzwerk sollten CSOs darauf achten, dass sie betriebswirtschaftlichen Mehrwert nicht unterschätzen, der sich aus strategischen Gelegenheiten ergeben kann. Wenn sie Netzwerke mit geringen Investitionskosten implementieren, laufen IT-Abteilungen Gefahr, neue Technologien oder geschäftliche Vorhaben ablehnen zu müssen, da das Netzwerk diese nicht unterstützen kann. Das bedeutet: Keine „Verwenden Sie Ihr eigenes Gerät"-Richtlinien, keine Ausdehnung der Virtualisierungsanstrengungen für unternehmenswichtige Geschäftsanwendungen, keine Cloud-Dienste und keine Rich Media. Alle Kosteneinsparungen-, Wettbewerbs- und Produktivitätsvorteile und Flexibilitätssteigerungen gehen verloren, weil am Netzwerk ein paar Euro gespart wurden. Die Vorteile wiegen jedoch die Gesamtkosten eines Unternehmensnetzwerks der nächsten Generation mehr als auf.

Betrachten wir nun genauer, was ein kostengünstiges oder „Good-enough"-Netzwerk von einem geschäftsfördernden Netzwerk der nächsten Generation unterscheidet:

- **Zweck des Netzwerks:** Ein „Good-enough"-Netzwerk hat nur einen Zweck: einen Benutzer mit den IT-Ressourcen zu verbinden. Dies mag im Jahr 2005 angemessen gewesen sein, als die Benutzer an Desktopcomputern mit Ethernetanschlüssen saßen. Bei einem Unternehmensnetzwerk der nächsten Generation handelt es sich um ein vereinheitlichtes Netzwerk, das aus kabelgebundenen, drahtlosen und Remote-Clients besteht. Es umfasst viele Geräte, Zugriffsmöglichkeiten und die Energieüberwachung. Es kann für verschiedene Zwecke verwendet werden, darunter die Verbindung zwischen Computern, die für neue Sensornetzwerke oder Datencentersicherungsanwendungen erforderlich sind.
- **Sicherheit:** Bei einem „Good-enough"-Netzwerk ist die Sicherheit kein integraler Bestandteil. Mit anderen Worten: Die Sicherheit wird durch getrennte Produkte gewährleistet, die bei der Integration Probleme verursachen können. Ein Netzwerk der nächsten Generation verfügt über integrierte Sicherheitsfunktionen vom Büro bis in die Cloud. Durch die Integration entstehen ein geringerer Verwaltungsaufwand und weniger Sicherheitslücken.
- **Anwendungsintelligenz:** Ein „Good-enough"-Netzwerk erkennt weder Anwendungen noch Endgeräte. Es geht davon aus, dass Daten einfach nur Daten sind. Ein Netzwerk der nächsten Generation hingegen erkennt Anwendungen und Endgeräte. Es passt sich der bereitzustellenden Anwendung und dem Endgerät an, auf dem sie ausgeführt wird.
- **Dienstqualität:** Heutige „Good-enough"-Netzwerke wurden auf QoS-Standards aufgebaut, die für Videodatenverkehr und virtualisierte Desktops möglicherweise nicht ausreichen. Ein Netzwerk der nächsten Generation umfasst medienerkennende Steuerungen für die Unterstützung der Sprach- und Videointegration.
- **Standards:** Ein „Good-enough"-Netzwerk beruht auf Standards, die nicht auf die Zukunft ausgerichtet sind. Ein Netzwerk der nächsten Generation unterstützt nicht nur aktuelle Standards, sondern treibt Innovationen voran, die zu den Standards der Zukunft führen.
- **Garantie:** „Good-enough"-Netzwerke weisen eine begrenzte Art von Wartungssupport und Garantiebestimmung auf. Die Anbieter von Netzwerken der nächsten Generation bieten eine Garantie sowie intelligente Dienste mit integrierter Verwaltung an.
- **Übernahmekosten:** Die bei den Investitionsausgaben gesparten Kosten können durch die geringeren betrieblichen Gesamtaufwendungen aufgewogen werden, wenn es andernfalls zu Integrationskosten, häufigeren Ausfällen oder ernsthaften Sicherheitslücken kommt. Die Anbieter von „Good-enough"-Netzwerken spielen diese Kosten herunter, während die Anbieter von Netzwerken der nächsten Generation einen Systemansatz bewerben, mit dem nicht nur die Netzwerkkosten im Zusammenhang mit den Gesamtbetriebskosten verringert, sondern zudem IT-Serviceverbesserungen und neue Geschäftsgelegenheiten gefördert werden, was zu einer höheren Rendite führt.

Das Sichern veralteter Netzwerke für die Technologien von heute ist ein aussichtsloser Kampf. Um die Risiken und komplexen Bedrohungen durch eine verbraucherorientierte IT, Mobilität und Cloud Computing vorherzusehen, benötigt die IT unbedingt ein Netzwerk der nächsten Generation.

UNTERSTÜTZT VON

CISCO

Borderless Network Architecture

Cisco hat mit der Borderless Network-Architektur ein Framework für Netzwerke der nächsten Generation vorgestellt. Hiermit wird definiert, wie die langfristige Vision von Cisco für das Bereitstellen einer neuen Reihe von Netzwerkdiensten ausgelegt ist, mit denen die Anforderungen von Unternehmen und Endbenutzern erfüllt werden. Diese Dienste versetzen das Unternehmen in die Lage, den neuen und sich entwickelnden Anforderungen von Benutzern und der IT-Abteilung besser gerecht werden. Intelligente Netzwerkdienste sind für das Senken der Gesamtbetriebskosten ebenso von grundlegender Bedeutung, wie für das Verbessern der Möglichkeiten der IT, neue Geschäftsfunktionen bereitzustellen.

Cisco hat sich dem Ziel verschrieben, Systeme zu entwerfen, damit die IT-Abteilung weniger Zeit mit der grundlegenden Netzwerkintegration verbringen muss, da ihr eine Reihe von Netzwerkdiensten zur Verfügung stehen, dank derer das Netzwerk die Anforderungen des Unternehmens und der Benutzer besser erfüllen kann.

Einer der Erfolgsgaranten von Cisco Borderless Networks ist das Cisco SecureX Framework — ein Sicherheitssystem, das vom Endpunkt bis zur Cloud reicht und an allen „Hops" im Netzwerk Richtlinien und Kontrollelemente bereitstellt. Zudem ermöglicht es eine zentralisierte Verwaltung und verfügt über integrierte Tools für die Vorplanung, Konfiguration, netzwerkweite Richtlinienverteilung und Fehlerbehebung.

Das Framework Cisco SecureX

Cisco SecureX vereint die Leistung des Cisco-Netzwerk mit der kontextsensitiven Sicherheit, um moderne Unternehmen zu schützen, unabhängig davon wann, wo oder wie die Mitarbeiter das Netzwerk verwenden. Das Framework Cisco SecureX baut auf drei grundlegenden Prinzipien auf:

- **Kontextsensitive Richtlinie:** Hierfür wird eine vereinfachte beschreibende Geschäftssprache verwendet, mit der die Sicherheitsrichtlinien anhand von fünf Parametern definiert werden: der Identität der Person, der verwendeten Anwendung, dem Zugriffsgerät, dem Standort und der Uhrzeit. Diese Sicherheitsrichtlinien ermöglichen eine effektivere Sicherheit. Zudem erfüllen Sie die Konformitätszielsetzungen mit größerer Betriebseffizienz und Kontrolle.
- **Kontextbezogene Sicherheitsdurchsetzung:** Hierfür wird die Netzwerk- und globale Intelligenz verwendet, um Durchsetzungsentscheidungen für das gesamte Netzwerk zu treffen und überall im Unternehmen eine konsistente, durchgängige Sicherheit bereitzustellen. Flexible Bereitstellungsoptionen wie z. B. integrierte Sicherheits-Services, eigenständige Anwendungen oder cloudbasierte Sicherheits-Services bringen den Schutz näher zum Benutzer, sodass dieser erhöht und die Netzwerkauslastung verringert wird.
- **Netzwerk und globale Intelligenz** geben tiefgreifende Einblicke in die Netzwerkaktivitäten und die globale Bedrohungslandschaft was einen schnellen, genauen Schutz und eine Durchsetzung der Richtlinien ermöglicht:
  - > Die lokale Intelligenz der Cisco-Netzwerkinfrastruktur setzt die Zugriffs- und Datenintegritätsrichtlinien mithilfe des Kontexts durch, z. B. Identität, Gerät, Sicherheitsstatus, Standort und Verhalten.
  - > Die globale Intelligenz des globalen Sicherheitsrahmens von Cisco (Cisco Security Intelligence Operations, SIO) bietet den vollständigen, aktuellen Kontext und den Umgang mit Bedrohungen, sodass ein zielgerichteter Echtzeitschutz möglich ist.

Cisco SecureX ermöglicht es Unternehmen, Mobilitäts- und Cloud-Lösungen umzusetzen und gleichzeitig die wichtigsten Vermögenswerte des Unternehmens zu schützen. Es bietet im gesamten Unternehmen eine detaillierte Sichtbarkeit und Kontrolle bis hin zur Benutzer- und Geräteebene. Dadurch erhalten IT-Sicherheitsabteilungen einen schnelleren und genaueren Schutz vor Bedrohungen mit einer stets verfügbaren End-to-End-Sicherheit und integrierter globaler Intelligenz. Die IT-Abteilung profitiert dank verbesserter Betriebseffizienz, vereinfachter Richtlinien, integrierter Sicherheitsoptionen und einer automatischen Sicherheitsdurchsetzung.

Zusammenfassung

Das Sichern veralteter Netzwerke für die Technologien von heute ist ein aussichtsloser Kampf. Um die Risiken und komplexen Bedrohungen durch eine verbraucherorientierte IT, Mobilität und Cloud Computing vorherzusehen, benötigt die IT unbedingt ein Netzwerk der nächsten Generation. Ein Netzwerk der nächsten Generation, mit einer durchgängigen und integrierten Architektur, erleichtert die Unterstützung des Unternehmens und bietet gleichzeitig den erforderlichen Sicherheitsstatus für unternehmenswichtige moderne IT-Systeme. **Weitere Informationen erhalten Sie unter www.cisco.com/go/security.**