Whitepaper

Abdeckung des gesamten Angriffskontinuums: vor, während und nach einem Angriff

Die Zeit für ein neues Sicherheitsmodell ist gekommen

Die Bedrohungslandschaft hat sich in den letzten zehn Jahren drastisch verändert. An die Stelle einzelner Hacker, die mit einfachen Angriffen überschaubare Schäden verursachten, sind Gruppen von Cyberkriminellen getreten, die Unternehmen und der nationalen Infrastruktur mit komplexen, finanziell unterstützten Angriffsmethoden erhebliche Schäden zufügen können. Diese modernen Angriffe sind nicht nur schwer zu erkennen, sondern verbleiben für längere Zeit in den Netzwerken und sammeln Netzwerkressourcen, um an anderer Stelle Angriffe zu starten.

Herkömmliche Abwehrmechanismen, die ausschließlich auf Erkennung und Blockierung basieren, sind daher nicht mehr ausreichend. Die Zeit für ein neues Sicherheitsmodell, das das gesamte Angriffskontinuum abdeckt – und zwar vor, während und nach einem Angriff – ist gekommen.

Die Industrialisierung von Hackerangriffen

Die ersten PC-Viren tauchten vor 25 Jahren auf. Damals war nicht vorstellbar, dass diese nur die Spitze des Eisbergs bedeuteten und später zur Industrialisierung von Hackerangriffen ausarten würden.

Knapp zehn Jahre lang waren Computerviren die primäre Angriffsform und nach und nach wurden viele Blockierungs- und Schutzmechanismen entwickelt. Die Angreifer wurden, motiviert durch das Wissen über neu entdeckte und veröffentlichte Schwachstellen, immer einfallsreicher. Die Folge waren verschiedene Bedrohungszyklen, die einem „Cyber-Wettrüsten“ ähnelten. Etwa alle fünf Jahre bringen Angreifer neue Bedrohungen hervor – von Makroviren und Würmern über Spyware zu Rootkits – und die Verantwortlichen bemühen sich, schnell Lösungen zum Schutz der Netzwerke zu entwickeln.

Es ist wirklich kein Wunder, dass sich diese Zyklen mit großen Technologietrends in Verbindung bringen lassen, die neue Angriffsvektoren boten (siehe Abbildung 1). Früher zielten Viren überwiegend auf das Betriebssystem ab und verbreiteten sich dann über das sogenannte Turnschuhnetzwerk (Sneaker Net). Makroviren hingegen nutzten den Austausch von Dateien zwischen Benutzern zur Verbreitung. Computerwürmer, die sich von Rechner zu Rechner ausbreiteten, machten sich Unternehmensnetzwerke und die zunehmende Verwendung des Internets zunutze. Das Aufkommen von Spyware und Rootkits ging einher mit neuen Anwendungen, Geräten und Online-Communitys. Heutzutage haben wir es mit hochentwickelter Malware, gezielten Angriffen und Advanced Persistent Threats (APT) zu tun. Was die heutigen Bedrohungen von den damaligen unterscheidet, sind die zugrunde liegenden Motivationen und verwendeten Tools. Daher sind sie mittlerweile besonders schwierig zu erkennen, zu verstehen und aufzuhalten.

Abbildung 1. Die Industrialisierung von Hackerangriffen

Die Industrialisierung von Hackerangriffen schafft eine schnellere, effektivere und effizientere kriminelle Umgebung, die von den Angriffen auf unsere IT-Infrastruktur profitiert. Der organisierte Austausch von Exploits ist ein florierendes und lukratives Geschäft, wobei die Verlagerung von der Ausbeutung hin zu Diebstahl, Unterbrechungen und Zerstörungen durch den offenen Markt noch begünstigt wird. Und seit Cyberkriminelle erkannt haben, dass hier viel Geld zu verdienen ist, ist ihre Arbeit standardisierter, mechanisierter und prozessorientierter geworden. Angreifer kennen die herkömmlichen statischen Sicherheitstechnologien und ihre getrennten Bereitstellungen und nutzen deren Lücken und Schwachstellen aus. Hacker-Gruppen halten sich sogar über Softwareentwicklungsprozesse auf dem Laufenden, z. B. qualitätssichernde Untersuchungen von Sicherheitstechnologien vor deren Veröffentlichung, um sicherzustellen, dass sie den gängigen Schutzmechanismen weiter entgehen.

Für Geheimhaltung gibt es jetzt beträchtliche finanzielle Anreize und viele „Hacktivistengruppen“ werden dazu motiviert, Angriffe für wirtschaftliche oder politische Ziele zu starten, die kaum geahndet oder strafrechtlich verfolgt werden. Durch neue Methoden wie Port- und Protokoll-Hopping, verschlüsselte Tunnel, Dropper und kombinierte Bedrohungen und Techniken, die Social Engineering und Zero-Day-Angriffe nutzen, werden Hackerangriffe einfacher, schneller und günstiger. Die Gegenseite tut sich dabei zunehmend schwer, die Angriffe zu erkennen und abzuwehren. Was diese Angriffe noch schwerer fassbar macht, ist die Tatsache, dass sie sich auf ihrem Weg durch das Unternehmen ständig verändern und sich eine feste Ausgangsposition suchen, um wichtige Daten zu stehlen.

Die Any-to-Any-Herausforderung

Moderne erweiterte Netzwerke und ihre Komponenten entwickeln sich laufend weiter und bringen neue Angriffsvektoren mit sich. Hierzu zählen Mobilgeräte, webbasierte und mobile Anwendungen, Hypervisoren, Social Media, Webbrowser und integrierte Computer sowie die starke Verbreitung neuartiger Geräte und Services, die das Internet of Everything hervorbringt. Die Menschen bewegen sich innerhalb und außerhalb des Netzwerks, nutzen diverse Geräte und greifen auf beliebige Anwendungen in vielen verschiedenen Cloud-Umgebungen zu. Diese Allgegenwart ist es, was die Any-to-Any-Herausforderung ausmacht. Zwar hat diese Dynamik unsere Kommunikationstechniken verbessert, sie bietet aber auch mehr Angriffspunkte und Methoden für Hackerangriffe. Unglücklicherweise hat sich der Umgang von Unternehmen mit dem Thema Sicherheit nicht an diese Entwicklung angepasst.

Der Großteil der Unternehmen sichert erweiterte Netzwerke mithilfe unterschiedlicher Technologien ab, die nicht miteinander arbeiten oder es schlicht nicht können. Sie verlassen sich vielleicht auch zu sehr auf Service Provider, die sich um die Sicherheit in der Cloud kümmern, und auf Hosting-Unternehmen, die die Internet-Infrastruktur schützen sollen. In dieser neuen Situation haben Administratoren allzu wenig Einblick in oder Kontrolle über die Geräte und Anwendungen, die auf das Unternehmensnetzwerk zugreifen, und kaum Möglichkeiten, mit den neuen Bedrohungen Schritt zu halten.

Neue Sicherheitsdynamiken

Sicherheitsexperten, die mit komplexen Angriffen und der Any-to-Any-Infrastruktur konfrontiert sind, stellen sich selbst die drei folgenden wichtigen Fragen:

1. *Wie halten wir die Sicherheit und Compliance mit den neuen Geschäftsmodellen und Angriffsvektoren aufrecht, während sich unsere IT-Landschaft weiter verändert?* Unternehmen, die den Übergang zur Cloud, zur Virtualisierung oder zu Mobilgeräten vollziehen, weil diese Technologien Produktivität, Flexibilität und Effizienz bieten, müssen ihre Sicherheitsinfrastruktur entsprechend anpassen.
2. *Wie verbessern wir unsere Fähigkeit, uns in einer dynamischen Bedrohungslandschaft laufend vor neuen Angriffsvektoren und immer komplexeren Bedrohungen zu schützen?* Angreifern ist es egal, wen sie attackieren, sie greifen sich einfach das schwächste Glied in der Kette. Sie verwenden für ihre Angriffe häufig Tools, die speziell zur Umgehung der von ihrem Angriffsziel ausgewählten Sicherheitsinfrastruktur konzipiert sind. Sie achten penibel darauf, unbemerkt zu bleiben, und verwenden Technologien und Methoden, die zu beinahe unmerklichen Indications of Compromise führen.
3. *Wie gehen wir die ersten beiden Fragen an, und wie verringern wir gleichzeitig die Komplexität und Fragmentierung der Sicherheitslösungen?* Unternehmen können sich keine Sicherheitslücken leisten, die erfahrene Angreifer von heute gerne ausnutzen. Gleichzeitig bieten getrennte, nicht integrierte Sicherheitslösungen bei zunehmender Komplexität nicht den erforderlichen Schutz gegen moderne Bedrohungen.

> *„100 Prozent der Unternehmen sind mit Domänen verbunden, die als Malware-Seiten bekannt sind.“*
>
> –Cisco Annual Security Report 2014

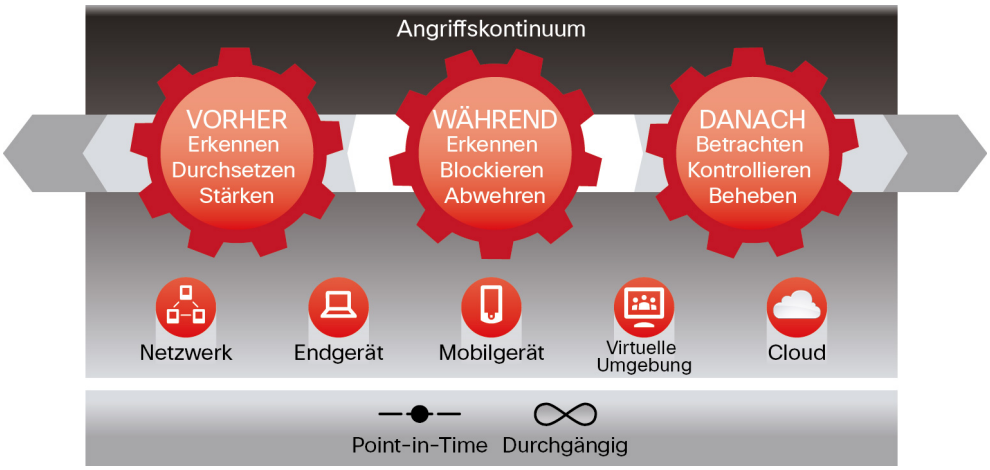
Diese Dynamik aus veränderten Geschäftsmodellen, einer dynamischen Bedrohungslandschaft und der Komplexität und Fragmentierung von Sicherheitslösungen ist verantwortlich für Sicherheitslücken, die Unterbrechung des Sicherheitslebenszyklus und die Verringerung der Transparenz sowie für neue Herausforderungen beim Sicherheitsmanagement. Um Unternehmen wirklich vor diesen Auswirkungen zu schützen, müssen wir unseren Sicherheitsansatz ändern. Die Zeit für ein neues bedrohungsorientiertes Sicherheitsmodell ist gekommen.

Abdeckung des gesamten Angriffskontinuums: vor, während und nach einem Angriff

Die meisten Security-Tools von heute sorgen vor allem für Transparenz im Netzwerk und blockieren Malware beim Eintritt in das Netzwerk. Sie scannen Dateien zu dem Zeitpunkt, an dem sie erstmals in das Netzwerk eintreten, auf ihre Schädlichkeit. Allerdings treten moderne Bedrohungen nicht zu einem bestimmten Zeitpunkt auf, sondern immer wieder und bedürfen deshalb einer kontinuierlichen Beobachtung. Die Widersacher wenden jetzt Taktiken wie Port-Hopping, Datenkapselung, Zero-Day-Angriffe, Umgehung der C&C-Erkennung (Command and Control), Standby-Techniken, laterale Bewegungen, verschlüsselten Datenverkehr, kombinierte Bedrohungen und die Sandbox-Umgehung, um einer anfänglichen Erkennung zu entgehen. Wenn die Datei nach dem Eintritt in die Umgebung nicht entdeckt wird oder sich weiterentwickelt und Schäden anrichtet, funktionieren Point-in-Time-Erkennungstechnologien nicht mehr und können die Folgeaktivitäten des Angreifers nicht identifizieren.

Sicherheitsmethoden dürfen sich nicht nur auf die Erkennung allein konzentrieren, sondern müssen auch die Auswirkungen abschwächen können, sobald ein Angreifer sich Zutritt verschaffen konnte. Unternehmen müssen ihr Sicherheitsmodell ganzheitlich betrachten und sich über das erweiterte Netzwerk und das gesamte Angriffskontinuum einen Überblick und Kontrolle verschaffen, und zwar bevor ein Angriff eintritt, während ein Angriff im Gange ist und sogar nachdem die Beschädigung von Systemen einsetzt oder Informationen gestohlen werden (siehe Abbildung 2).

Abbildung 2. Das neue Sicherheitsmodell



- **Vorher:** Verantwortliche müssen einen umfassenden Überblick darüber haben, was im erweiterten Netzwerk vor sich geht, um Richtlinien und Kontrollmechanismen zu dessen Verteidigung implementieren zu können.
- **Während:** Das Hauptaugenmerk liegt auf der kontinuierlichen Erkennung und Blockierung von Malware.
- **Danach:** Verantwortliche benötigen Retrospective Security, um die Auswirkungen eines Angriffs einzugrenzen. Dazu müssen sie den Eintrittspunkt sowie den Umfang des Schadens ermitteln, die Bedrohung kontrollieren, das Risiko einer erneuten Infektion eliminieren und Unterbrechungen beheben.

Vor einem Angriff

Kontextbewusste Angreifer erfordern kontextbewusste Sicherheit. Unternehmen müssen sich gegen Angreifer wehren, die häufig besser mit der Infrastruktur vertraut sind, als die Verantwortlichen, die sie zu schützen versuchen. Um Angriffe vor ihrem Auftreten abzuwehren, benötigen Unternehmen einen vollständigen Überblick über ihre Umgebung, also u. a. über physische und virtuelle Hosts, Betriebssysteme, Anwendungen, Services, Protokolle, Benutzer, Inhalte und das Netzwerkverhalten, um damit die Oberhand über die Angreifer zu gewinnen. Die Verantwortlichen müssen die Risiken für ihre Infrastruktur verstehen, die auf deren Zielwert, der Legitimität eines Angriffs und dem Verlauf basieren. Wenn sie nicht verstehen, was sie zu schützen versuchen, können sie dafür auch keine Sicherheitstechnologien konfigurieren. Transparenz muss im gesamten Netzwerk gewährleistet sein, d. h. für Endgeräte, E-Mail- und Web-Gateways, für virtuelle Umgebungen und Mobilgeräte sowie das Rechenzentrum. Und auf Basis dieser Transparenz müssen umsetzbare Warnmeldungen erzeugt werden, damit die Verantwortlichen fundiertere Entscheidungen treffen können.

Während eines Angriffs

Bösartige Angriffe treten nicht zu einem bestimmten Zeitpunkt auf, sondern laufen kontinuierlich und erfordern daher fortlaufende Sicherheitsüberprüfungen. Herkömmliche Sicherheitstechnologien können nur Angriffe erkennen, die zu einem bestimmten Zeitpunkt auftreten und auf einem einzelnen Datenpunkt des Angriffs basieren. Dieser Ansatz ist gegen moderne Angriffe machtlos. Was hier nötig ist, ist eine Sicherheitsinfrastruktur, die alle Informationen mit einbezieht. Gemeint ist eine Infrastruktur, die Daten aus dem erweiterten Netzwerk aggregieren und mit historischen Merkmalen und weltweiten Informationen zu Angriffen korrelieren kann. Sie muss Kontext liefern und bloße Hintergrundgeräusche von aktiven Angriffen, Datendiebstahl und Ausspähung unterscheiden können. Auf diese Weise entwickelt sich das Sicherheitssystem von einer Aufgabe, die zu einem bestimmten Zeitpunkt durchgeführt wird, zur kontinuierlichen Analyse und Entscheidungsfindung. Sollte also eine Datei eingedrungen sein, die auf den ersten Blick harmlos war, sich aber später als schadhaft entpuppt, können Unternehmen Maßnahmen dagegen ergreifen. Dank diesen Echtzeitinformationen können Sicherheitsexperten intelligente Automatisierungsservices einsetzen, mit denen Sicherheitsrichtlinien ohne manuelle Eingriffe durchgesetzt werden.

Nach einem Angriff

Um das gesamte Angriffskontinuum abzudecken, brauchen Unternehmen Retrospective Security. Retrospective Security stellt eine Big Data-Herausforderung dar und eine Funktion, die nur wenige Systeme leisten können. Sicherheitsteams können mit einer Infrastruktur, die laufend Daten für den Erwerb von Sicherheitsinformationen erfasst und analysiert, durch Automatisierung Indications of Compromise identifizieren und Malware erkennen, die so ausgereift ist, dass sie ihr Verhalten ändert, um einer Erkennung zu entgehen. Abschließend wird das Problem behoben. Gefährdungen, die andernfalls über Wochen oder Monate unerkannt geblieben wären, können so identifiziert, gründlich betrachtet, kontrolliert und behoben werden.

Durch dieses bedrohungsorientierte Sicherheitsmodell sind Unternehmen in der Lage, das gesamte Angriffskontinuum über alle Angriffsvektoren hinweg abzudecken und jederzeit in Echtzeit zu reagieren.

Umsetzung des neuen Sicherheitsmodells

Cisco ist davon überzeugt, dass sich moderne Sicherheitstechnologien auf drei strategische Anforderungen konzentrieren müssen, damit das neue Sicherheitsmodell funktioniert: Sie müssen transparent, bedrohungsorientiert und plattformbasiert sein.

Transparent: Sicherheitsadministratoren müssen genau sehen können, was aktuell geschieht. Hierzu ist ein gewisser Umfang und auch Tiefe erforderlich (siehe Abbildung 3). Der Umfang macht die Fähigkeit aus, Daten von allen potenziellen Angriffsvektoren in der gesamten Netzwerkstruktur, aus E-Mails und Web-Gateways, Mobilgeräten, virtuellen Umgebungen und in der Cloud zu überblicken und zu erfassen, um Informationen über Umgebungen und Bedrohungen zu erlangen. Die Tiefe bietet die Fähigkeit, diese Informationen zu korrelieren, Informationen zum besseren Verständnis des Kontexts einzusetzen, fundiertere Entscheidungen zu treffen und Maßnahmen entweder manuell oder automatisch zu treffen.

Abbildung 3. Umfang und Tiefe

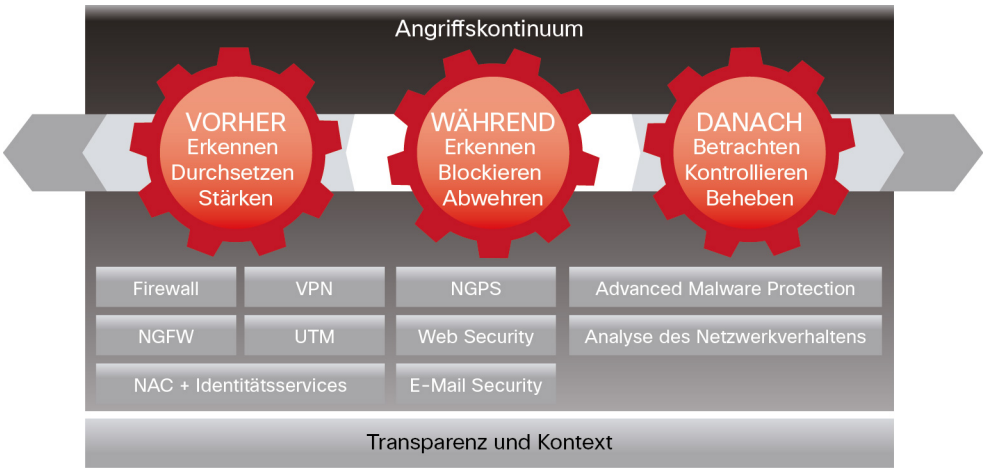
Bedrohungsorientiert: Netzwerke von heute dehnen sich dorthin aus, wo sich Mitarbeiter aufhalten, wo Daten vorhanden sind und von wo aus auf Daten zugegriffen werden kann. Trotz aller Bemühungen ist es für Verantwortliche kein Leichtes, mit den sich ständig weiterentwickelnden Angriffsvektoren Schritt zu halten, und das nutzen Angreifer aus. Richtlinien und Kontrollmechanismen werden benötigt, um Angriffen möglichst wenig Chancen einzuräumen. Trotzdem sind einige Bedrohungen unaufhaltsam. Technologien müssen sich daher auch mit der Erkennung, dem Verstehen und der Abwehr von Bedrohungen befassen. Eine Fokussierung auf die Bedrohung bedeutet, wie ein Angreifer zu denken, für Transparenz und Kontext zu sorgen, um Veränderungen in der Umgebung zu verstehen und anzupassen und dann Sicherheitsmechanismen gegen Bedrohungen zu entwickeln. Angesichts der modernen Malware und Zero-Day-Angriffe ist dies ein fortlaufender Prozess, bei dem kontinuierliche Analysen und Sicherheitsinformationen in Echtzeit aus der Cloud bereitgestellt und zur Verbesserung der Effizienz von allen Produkten gemeinsam genutzt werden.

Plattformbasiert: Sicherheit beschränkt sich nicht mehr auf das Netzwerk allein. Sie verlangt ein integriertes System an flexiblen und offenen Plattformen, die Netzwerke, Geräte und die Cloud abdecken. Diese Plattformen müssen erweiterbar und skalierbar sein sowie zentral verwaltet werden können, damit einheitliche Richtlinien und konsistente Kontrollen angewendet werden können. Kurz gesagt: So komplex wie Malware heute ist, so leistungsfähig muss die Absicherung dagegen sein. Hier vollzieht sich ein Wandel von der Anwendung einzelner Security-Appliances hin zur Integration einer echten Plattform mit skalierbaren Services und Anwendungen, die sich einfach bereitstellen lassen. Dieser plattformbasierte Ansatz verstärkt nicht nur die Effektivität der Sicherheitsmechanismen, indem er isolierte Umgebungen und die von ihnen verursachten Sicherheitslücken eliminiert, er beschleunigt auch die Erkennungszeit und optimiert die Durchsetzung.

Abdeckung des gesamten Angriffskontinuums

Um die Sicherheitsherausforderungen zu bewältigen und einen besseren Schutz zu erreichen, brauchen Unternehmen Lösungen, die das gesamte Angriffskontinuum abdecken. Das heißt, sie müssen hohe Transparenz bieten, auf Bedrohungen fokussiert und plattformbasiert sein. Cisco bietet ein umfassendes Portfolio an bedrohungsorientierten Cyber Security-Lösungen, die das gesamte Angriffskontinuum abdecken.

Abbildung 4. Abdeckung des vollständigen Angriffskontinuums



Diese spezifischen plattformbasierten Lösungen bieten die branchenweit umfangreichsten Durchsetzungs- und Behebungsoptionen an Angriffsvektoren, an denen sich Bedrohungen bemerkbar machen. Sie arbeiten zusammen, um Schutz über das gesamte Angriffskontinuum hinweg bereitzustellen und lassen sich in ergänzende Lösungen integrieren, um ein umfassendes Sicherheitssystem zu bieten.

- Vor einem Angriff stehen Sicherheitsexperten beispielsweise Firewalls, Firewalls der nächsten Generation, Netzwerkzugriffskontrolle und Identitätsservices zur Verfügung, die sie zur Erkennung von Bedrohungen und zu Durchsetzung und Stärkung von Richtlinien benötigen.
- Während eines Angriffs sorgen Intrusion Prevention-Systeme und E-Mail- bzw. Web-Security-Lösungen dafür, dass Angriffe, die das Netzwerk passiert haben und im Gange sind, erkannt, blockiert und Maßnahmen dagegen ergriffen werden.
- Nach einem Angriff können Unternehmen Lösungen von Cisco zum Schutz vor hochentwickelter Malware nutzen und eine Analyse des Netzwerkverhaltens durchführen, um einen Angriff schnell und effektiv zu betrachten, zu kontrollieren und zu beheben und so die Schäden gering halten.

Diese Lösungen sind auch für sehr große weltweite Unternehmen skalierbar und stehen ihnen jederzeit und in jeder Form zur Verfügung: als physische und virtuelle Appliance, oder als Cloud-basierte Services. Sie werden zudem integriert, um eine konstante Transparenz und Kontrolle des gesamten erweiterten Netzwerks und aller Angriffsvektoren zu ermöglichen.

Zusammenfassung

Die Industrialisierung von Hackerangriffen und die Any-to-Any-Herausforderung bringen eine grundlegende Veränderung der Art und Weise, wie wir unsere Systeme schützen müssen, mit sich und veranlassen uns, über neue Ansätze bei der Cyber Security nachzudenken. Sicherheitsstrategien, die sich auf die Perimeter-basierten Abwehrmechanismen und präventive Techniken konzentrieren, bieten Angreifern ein leichtes Spiel, sobald diese erst einmal in das Netzwerk eingedrungen sind.

Veränderte Geschäftsmodelle, eine dynamische Bedrohungslandschaft sowie Komplexität und Fragmentierung der Sicherheit haben Sicherheitslücken verursacht, den Sicherheitslebenszyklus unterbrochen, die Transparenz verringert und neue Herausforderungen beim Sicherheitsmanagement mit sich gebracht. Die Zeit für ein neues bedrohungsorientiertes Sicherheitsmodell ist gekommen, das Unternehmen die notwendige Transparenz und Kontrolle bietet, die sie im erweiterten Netzwerk und für das gesamte Angriffskontinuum benötigen.

Cisco ist der einzige Anbieter, der einen bedrohungsorientierten Sicherheitsansatz bieten kann, der Komplexität reduziert und hervorragende Transparenz, fortwährende Kontrolle und einen erweiterten Schutz vor Bedrohungen im gesamten Angriffskontinuum bereitstellt. Mit diesem neuen Sicherheitsmodell können Unternehmen intelligenter und schneller agieren als jemals zuvor – und zwar vor, während und nach einem Angriff.

Hauptgeschäftsstelle Nord- und Südamerika
Cisco Systems, Inc.
San Jose, CA

Hauptgeschäftsstelle Asien-Pazifik-Raum
Cisco Systems (USA) Pte. Ltd.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV Amsterdam,
Niederlande

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen mit Telefon- und Faxnummern finden Sie auf der Cisco Website unter **www.cisco.com/go/offices**.

Gedruckt in den USA C11-731741-01 06/14