Cisco Lösung zum Schutz vor, während und nach Angriffen

Mit Cisco Cloud Web Security Premium kann ein globaler Öl- und Gaskonzern dauerhafte Infektionen durch Ransomware erkennen und beseitigen.

Herausforderungen

In der heutigen Zeit, in der Datendiebstahl oder Datenschädigung zu den primären Anreizen für Angriffe zählen, ist es schwieriger denn je, die Sicherheit von Inhalten zu gewährleisten. Im Cisco Annual Security Report 2014 wurde erläutert, dass 100 Prozent der analysierten Unternehmensnetzwerke Daten von Websites übertragen, die Malware hosten.[1] Beobachtungen dieser Aktivitäten ergaben weiterhin, dass infizierte Netzwerke wahrscheinlich über einen längeren Zeitraum hinweg befallen waren und die zentrale Infektion nicht erkannt wurde.[2]

Die folgenden Faktoren erschweren Sicherheitsteams die Vermeidung und Erkennung von Bedrohungen:

- Ohne geeignete Sicherheitsmaßnahmen reduzieren **Mobility- und Cloud-Lösungen** die Transparenz und steigern die Komplexität. Da immer mehr Unternehmen Trends wie Cloud Computing, Virtualisierung, Mobility, Remote-Mitarbeit und Bring-Your-Own-Device (BYOD) unterstützen, werden auch immer mehr mobile Daten außerhalb der Kontrolle von Unternehmen übertragen. Das Netzwerk wird durchlässiger und anfälliger für Angriffe. Und da immer mehr geschäftskritische Services in die Cloud verlagert und außerhalb des gesicherten Perimeters des Unternehmens verwendet werden, wird die Angriffsfläche weiter vergrößert.
- Dem *Cisco Annual Security Report 2014* zufolge werden **Angriffe immer komplexer**. So versuchen Angreifer aktiv herauszufinden, welche Sicherheitslösungen bereitgestellt werden und greifen auf weniger offensichtliche Methoden zurück – die Bedrohungen sind also sehr gut getarnt.[3] Diese Bedrohungen sind eine immense Herausforderung für Sicherheitslösungen und -experten. Unternehmen müssen sich darauf einstellen, dass Angreifer „vermehrt verschlüsselten Datenverkehr, Scrambling und Randomisierung nutzen werden, sodass Command-and-Control-Aktionen (C&C) kaum noch vom echten Datenverkehr zu unterscheiden sind“.[4]

KUNDENPROFIL

Branche: Öl und Gas

Mitarbeiter: ca. 15.000

Geschäftsbetrieb: global

Sicherheitspersonal: 12

Andere Sicherheitsmaßnahmen: Virenschutz, Firewall, Intrusion Detection System (IDS), Security Information and Event Management (SIEM)

HERAUSFORDERUNG

- Erkennen komplexer, vom Internetdatenverkehr ausgehender Bedrohungen, die die vorhandenen Sicherheitslösungen umgehen und sich im Unternehmensnetzwerk festsetzen
- Bereitstellen aussagekräftiger Daten, anhand derer Sicherheitsteams Bedrohungen priorisieren können
- Bestimmen einer Komplettlösung für die verteilte Umgebung, die in die vorhandene Sicherheitsinfrastruktur integriert werden kann und während des gesamten Angriffskontinuums Schutz bietet

LÖSUNG

- Cisco CWS Premium, welches alle Funktionen von Cisco CWS Essentials umfasst
- Cognitive Threat Analytics (CTA) und Advanced Malware Protection (AMP) zur Automatisierung der Suche im Web nach Bedrohungen mit extrem hohem Risiko und für transparente Einblicke in komplexe Angriffe, die im Unternehmensnetzwerk aktiv sind

ERGEBNISSE

- Dauerhafte und zuvor nicht erkannte Malware-Infektionen werden identifiziert und beseitigt.
- Bedrohungsschutz besteht während des gesamten Angriffskontinuums.
- Sicherheitsteams beim Kunden können sich auf die relevantesten Bedrohungen konzentrieren.

[1] Cisco 2014 Annual Security Report: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.
[2] Ibid.
[3] Ibid.
[4] Ibid.

In der komplexen und dynamischen Bedrohungslandschaft zielt der moderne Ansatz der Content-Sicherheit eher auf die Entdeckung der Viren und Bedrohungen als auf ihre Beseitigung ab. Unternehmen müssen sich heutzutage auf die Prüfung von Inhalten, die Erkennung von abnormalem Verhalten und fortschrittliche Forensik konzentrieren, um Gefahren sichtbar zu machen, die sich bereits in den Netzwerken eingenistet haben. Dabei geht es um die Phase „nach“ einem Angriff.

Abbildung 1. Neues Sicherheitsmodell: durchgängige Sicherheit nach Angriffen

Mit Cisco® Cloud Web Security (CWS) meistern Unternehmen die Herausforderung, im erweiterten Netzwerk fortlaufende Sicherheit garantieren zu müssen. Die Cisco CWS-Plattform, eine Cloud-basierte Version von Cisco Web Security, erweitert die Websicherheit auf mobile Geräte und verteilte Umgebungen. Mithilfe von Threat Intelligence und fortschrittlichen Abwehrfunktionen bietet sie sogar für Roaming-Benutzer das ideale Maß an Schutz. Die Plattform beinhaltet sämtliche Funktionen von Cisco CWS Essentials und ergänzt sie noch durch zwei innovative Malware-Erkennungssysteme, die die Suche nach Bedrohungen mit hohen Sicherheitsrisiken im Internetverkehr automatisieren:

- **Cognitive Threat Analytics (CTA)** ist ein Analysesystem, welches das Netzwerkverhalten nahezu in Echtzeit analysiert und dank maschineller Lernverfahren und erweiterten Statistiken ungewöhnliche Aktivitäten im Netzwerk – so genannte Indicators of Compromise (IOCs) – aufspürt. CTA entdeckt Unregelmäßigkeiten und weist Sicherheitsanalysten auf potenzielle Probleme hin. So können die zuständigen Experten ihren Arbeitsaufwand reduzieren und Bedrohungen priorisieren.
- **Advanced Malware Protection (AMP)** setzt bei der Erkennung und Abwehr von Bedrohungen über das gesamte Angriffskontinuum hinweg auf eine Kombination aus Dateireputation, Datei-Sandboxing und retrospektiven Dateianalysen.

Mit dieser Lösungskombination kann CWS Premium neue Command-and-Control-Kanäle identifizieren, die in der Sicherheitsbranche bisher noch nicht erkannt wurden.

In dieser Fallstudie wird untersucht, wie ein globaler Öl- und Gaskonzern mit CWS Premium die folgenden Vorteile erzielte:

- Transparentere Einblicke in große und zunehmende Datenvolumen im Internet (mehr als 35 Millionen HTTP-/HTTPS-Anfragen pro Tag)
- Generierung aussagekräftiger Bedrohungsinformationen, um die Priorisierung zu vereinfachen
- Bereitstellung einer Komplettlösung, die sich in die vorhandene Sicherheitsinfrastruktur integrieren lässt und während des gesamten Angriffskontinuums Schutz bietet – vor, während und nach Angriffen

Lösung

Cisco empfahl ein Upgrade auf CWS Premium mit CTA und AMP. Das Unternehmen erhielt somit einen umfassenderen Einblick in sein Netzwerk, und das für die Abwehr von Bedrohungen zuständige Team konnte Gefahren einfacher priorisieren.

Die retrospektive Analysefunktion kann Dateien aufdecken, die beim Passieren des Perimeterschutzes zwar als „sauber“ angesehen wurden, in Wirklichkeit jedoch gut getarnte Malware sind. AMP benachrichtigt sofort den Sicherheitsadministrator und veranschaulicht deutlich, welche Benutzer im Netzwerk möglicherweise wann infiziert wurden.

CTA erkennt unterdessen auch besser getarnte Bedrohungen, die alle Schutzmechanismen passiert haben und im Unternehmensnetzwerk aktiv sind. Das innovative System zur Malware-Erkennung kann befallene Geräte mithilfe von Verhaltensanalysen und Erkennung von Unregelmäßigkeiten genau bestimmen. CTA verwendet für die unabhängige Identifizierung neuer Bedrohungen erweiterte statistische Modellierungs- und maschinelle Lernverfahren. Das Programm lernt aktiv dazu und passt sich mit der Zeit ohne Tuning- oder Konfigurationsaufwand an.

CTA erkannte und meldete Belege für Malware-Aktivität im Netzwerk des Kunden. Die Malware bestand aus einer Zusammenstellung von Modulen, die von einer Malware-Instanz gesteuert wurden. In diesem Fall war der Payload die Ransomware Cryptolocker, eine Malware-Art, die Dateien auf den Computern der Opfer verschlüsselt und ihr Gerät so lange sperrt, bis ein „Lösegeld“ bezahlt wird.[5]

Wie in Abbildung 2 dargestellt, betrieb der Angreifer zur Durchführung des Angriffs eine Command-and-Control-Infrastruktur. Diese Kampagne bestand aus vier grundlegenden Schritten:

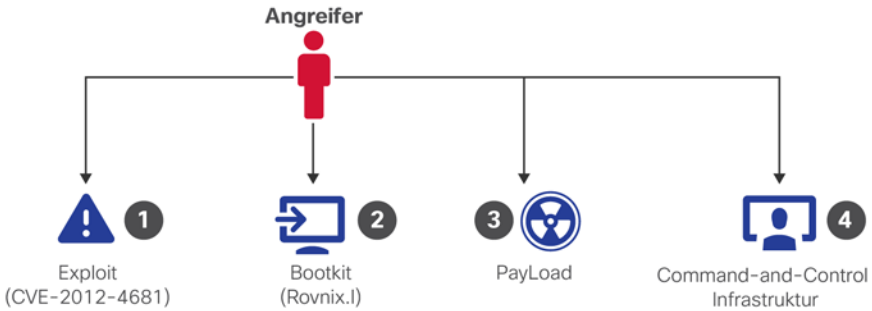
Schritt 1. Mit einem Exploit (CVE-2012-4681) konnte der Angreifer eine Sicherheitslücke in der Java Runtime Environment-(JRE-)Komponente von Oracle Java SE 7 Update 6 ausnutzen und Code unter Umgehung des Sicherheitsmanagers remote ausführen.

Schritt 2. Dann wurde das Bootkit (Rovnix.I) installiert, um den Verbleib im System sicherzustellen.

Schritt 3. Anschließend wurde der Payload für die volle Betriebsfähigkeit der Malware geliefert. (In diesem Fall war der Payload die Ransomware Cryptolocker.)

Schritt 4. Mit der Einrichtung von Command-and-Control-Kanälen wurde die Aktivität sichergestellt.

Abbildung 2. Die vier grundlegenden Schritte des Angriffs

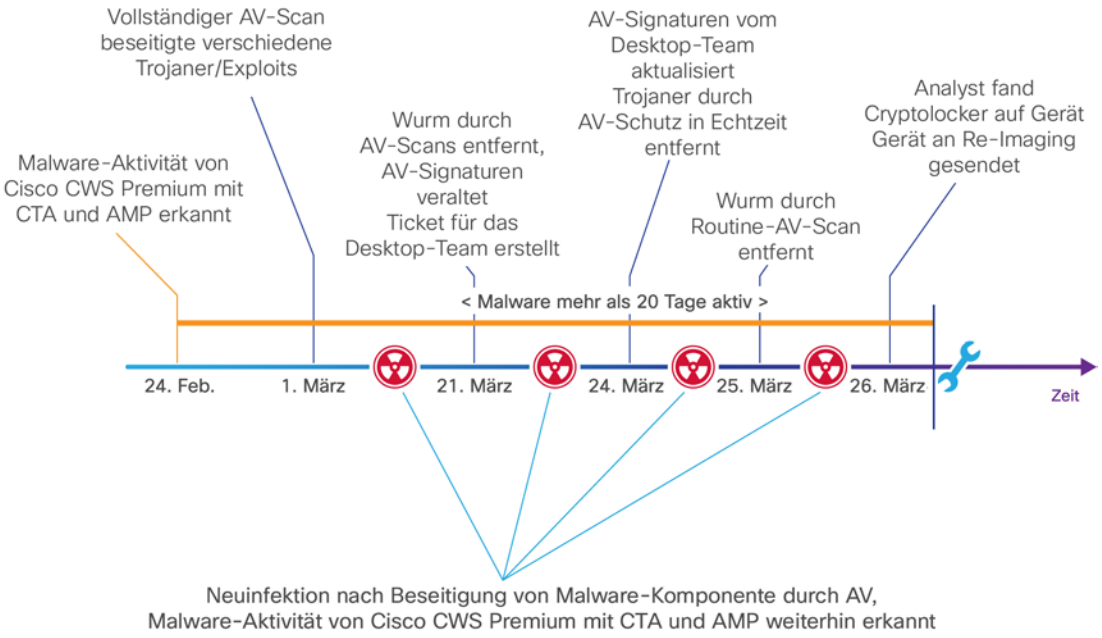


[5] Malvertising, Online-Werbung zur Verbreitung von Malware, spielte eine Schlüsselrolle bei der Verbreitung von Cryptolocker, das inzwischen neutralisiert wurde. Malvertising und Ransomware sind jedoch immer noch weit verbreitete Bedrohungen und werden von Angreifern verwendet, um zielgerichtete Kampagnen über das Internet zu starten. Weitere Informationen finden Sie im Cisco Midyear Security Report 2014: http://www.cisco.com/web/offer/grs/190720/SecurityReport_Cisco_v4.pd.

Das Sicherheitsteam beim Kunden versuchte, die Bedrohung mithilfe von Anti-Viren-Tools zu beseitigen. Da es sich jedoch um eine Rootkit-Infektion handelte, war die Malware tief im System verankert. Die Anti-Virus-Lösung konnte nur einen Teil der Malware-Komponenten beseitigen. Bis zur vollständigen Beseitigung der Infektion meldete CTA weiterhin dauerhafte schädliche Aktivitäten an das Sicherheitsteam.

Abbildung 3 zeigt die vollständige Zeitleiste ab Erkennung der Malware-Aktivität bis zur Beseitigung des Problems.

Abbildung 3. Zeitleiste zur Malware-Aktivität: Erkennung bis Beseitigung



Die Situation des Kunden zeigt den Nutzen von CWS Premium in der Phase „nach“ einem Angriff. Sie belegt darüber hinaus die Schwierigkeit, komplexe Angriffe mit Anti-Virus-Produkten zu beseitigen. Das CTA-System erbrachte Nachweise zur fortlaufenden Aktivität von Command-and-Control-Kanälen. Zusätzlich identifizierte es einige Domains, die an der Ausschleusung von Daten beteiligt waren. Solche Infektionen sind langfristige, in der Infrastruktur des Kunden verankerte Sicherheitsverletzungen.

Ergebnisse

Sicherheitsteams müssen heute täglich große Mengen an Vorfällen verwalten und haben keine Zeit, buchstäblich die Nadel im Heuhaufen zu suchen. Daher benötigen sie Unterstützung bei der Fokussierung auf besonders komplexe Angriffe. Das CTA-System kann solche Angriffe erkennen und kategorisieren.

Im Falle der Infizierung des Kundennetzes mit der Ransomware Cryptolocker erkannte CWS Premium Malware-Aktivität und konnte anhand der vorhandenen Sicherheitsinformationen einige der Command-and-Control-Kanäle blockieren, auf die das infizierte Geräte zuzugreifen versuchte. Der Angreifer verwendete dann jedoch eine zusätzliche IP-Adresse mit unbekannter Reputation. Dieser neue Kanal war während der Infektion funktionsfähig. Dieses Beispiel zeigt die Stärken (automatisches Blockieren) und Schwächen (neue Kanäle werden nicht blockiert) der Erkennung auf Signatur- und Reputationsbasis. Es belegt außerdem die Notwendigkeit eines fortlaufenden Schutzes auch nach einem Angriff.

Die folgenden Tabellen zeigen eine Analyse der vom CTA-System in CWS Premium identifizierten Command-and-Control-Kanäle sowie Beispiele für Web-Abfragen und Statistiken:

Tabelle 1. Angriffsinfrastruktur

Reihenfolge	Remote-Server	IP-Zieladresse	Zielland	Anzahl der Anfragen	Aktivitätsstatus
1	C&C-Server 1	109.XXX.XXX.XXX	Niederlande	17 (Versuche)	Durch Webreputation BLOCKIERT
2	**C&C-Server 2**	**94.XXX.XXX.XXX**	**Luxemburg**	**75**	**AKTIVER KANAL**
3	C&C-Server 3	fistristy.com	Luxemburg	175 (Versuche)	Durch Webreputation BLOCKIERT
4	C&C-Server 4	ffeed5.com	Russland	7 (Versuche)	Durch Webreputation BLOCKIERT

Tabelle 2. Durch CTA identifizierte Bedrohungen, die nachfolgend vom Gerät gelöscht wurden

Bedrohungsname	Gelöscht
Wurm Cridex	19. März
Wurm Cridex.E	19. März
Trojaner Tesch.B	19. März
Java Exploit/CVE-2012-4681	19. März
Trojaner-Downloader Win32/Upatre	19. März
Wurm Cridex	21. März
Trojaner Win32/Viknok.C	24. März
Wurm Cridex	24. März
Crypto Defense	26. März

Kommunikation mit C&C-Server 1 (109.XXX.XXX.XXX)

Kommunikationseigenschaften:

- Gesamtanzahl der versuchten Server-Anfragen war 17; alle Anfragen waren C&C-Kommunikation und wurden durch Reputation blockiert.
- Die Anfragen wurden von CTA als Versuche erkannt, URL-Zeichenfolgen als Kommunikationskanal (Communication Channel, C&C) zu verwenden. Die URL (siehe Abbildung unten „Beispiel für HTTP-Anfrage“) stellt eine verschlüsselte Nachricht dar. Eine ähnliche Struktur der URL-Zeichenfolge (IP-Adresse/m/IbQ.*) wurde von mehreren in diesem Angriff verwendeten URLs gemeinsam verwendet. Die Tatsache, dass die Kommunikation durch das Reputationssystem blockiert wurde, ist ein weiterer kontextueller Beleg.
- Der Angreifer richtete außerdem einen zweiten C&C-Kanal auf einem Server ein, der noch nicht Teil der Reputations-Feeds war. So wurde die fortlaufende Funktionsfähigkeit der Malware sichergestellt. Die URL selbst ist eine verschlüsselte Nachricht.

Beispiel für HTTP-Anfrage (anonymisiert und gekürzt)

http://109.XXX.XX.XXX/m/IbQXXXVjjpcE6+54HXXXdmmGcNZxtMZdvqyB5EkJAUmL/1sOXXXvq5zzXtIu9SzgnJhjWlxdE7FiqDEYFm5A+TPlXXXQpGhxGu0r3WLZoX1KHnCShKJDAufwiISy69wApgn4e79NFw/108XXX.g+fq4XXXOTYke6uhGHDOEeqje76v7z7i+wgqXXXFBuMz5k08yocxOH63bwQ9JMfwy8uNRM…

Kommunikation mit C&C-Server 2 (94.XXX.XXX.XXX)

Kommunikationseigenschaften:

- Gesamtanzahl der Server-Anfragen war 75; alle C&C-Anfragen.
- Zwei C&C-Anfragen wurden von CTA als **HTTP-Datenverkehr an IP-Adresse erkannt (keine Domain festlegt)**. Diese Verhaltenskategorie erkennt anormale Anfragen in Form von Kommunikation ohne Einhaltung der Reihenfolge an eine reine IP-Adresse. Diese Aktivität kann durch Malware als Prüfung der Aktivität durchgeführt werden, um zu bestätigen, dass die Malware weiterhin aktiv ist oder um Daten auszuschleusen und weitere Anweisungen aus der schadhaften Infrastruktur (C&C) zu erhalten. Diese Art von Datenverkehr wird durch normales Internet-Browsing nicht erzeugt.
- Alle 75 C&C-Anfragen wurden von Technologien auf Signatur- oder Reputations-Basis nicht erkannt.

Beispiel für HTTP-Anfrage (anonymisiert und gekürzt)

http://94.XXX.XXX.XXX/m/IbQXXXVjj7iA+O54XXXodmmGcNZxtMZdvqyB5EkJAUmLb3pvGIRvqizzXtIu9SzgnJhjWlxdE7FiqDEYFm5A+TPlXXXQpGhxGu0r3WLZoX1KHnCShKJDAufwiISy69wApgn4e79NFw/108XXXog+fq4XXXaE0qfJf1FwalZJKnDc7U0H30+XkiXXXIApkslTo5yvM0TkHrZncwIvumxLCQ+fq4XXXOT…

Kommunikation mit C&C-Server 3 (fistristy.com)

Kommunikationseigenschaften:

- Gesamtanzahl der Anfragen an die Domain fistristy.com war 175; alle C&C-Kommunikation.
- Signaturbasierte und reputationsbasierte Technologien blockierten alle Anfragen.

Beispiel für HTTP-Anfrage

hXXp://fistristy.com/aa/

Kommunikation mit C&C-Server 4 (ffeed5.com)

Kommunikationseigenschaften:

- Gesamtanzahl der Anfragen an ffeed5.com war sieben; alle von CWS Premium blockierte C&C-Kommunikation.
- CTA erkannte sechs Anfragen als Anfragen der Kategorie **Unregelmäßiger HTTP-Datenverkehr**. Zu dieser Verhaltenskategorie gehört Malware-Verhalten, das im Allgemeinen nicht zur Baseline passt, die von der fortlaufenden CTA-Analyse festgelegt wurde. Der Begriff „Baseline“ bezieht sich auf den Status der vom CTA-System erstellten Statistikmodelle, das die Trends und Eigenschaften des analysierten Datenverkehrs im Web „lernt“. CTA passt die Baseline automatisch an das sich ändernde Netzwerk an (zum Beispiel Nacht und Tag), um die besten Erkennungsergebnisse zu gewährleisten.
- CTA modelliert das Netzwerkverhalten langfristig und kann so scheinbar ungleichartige Aktivitäten in Bezug setzen. Anschließend werden die Daten im Kundennetzwerk mit dem Verhalten von Benutzern verglichen, um gut getarnte und dauerhafte Bedrohungen aufzuspüren.

Beispiel für HTTP-Anfrage

hXXp://ffeed5.com/cmd?version=1.5&aid=555&id=24c6b407-5010-4d8d-a266-ffdac7d6f901&os=6.1.7601_1.0_64

Zusammenfassung

Das Sicherheitsteam des Kunden suchte nach einer einfacheren Möglichkeit zur Überwachung von Aktivitäten und zur Priorisierung von sicherheitsrelevanten Ereignissen in einem Netzwerk mit mehr als 15.000 Benutzern, die im Durchschnitt über 35 Millionen Web-Transaktionen pro Tag generieren. Der Kunde benötigte darüber hinaus eine Lösung, die Bedrohungen nicht nur blockieren, sondern auch potenzielle Gefahren identifizieren kann, die andere Schutzmechanismen zwangsläufig unerkannt passieren. Die vom Kunden gewünschte Technologie sollte die Sicherheitsmitarbeiter so lange über dauerhafte verdächtige Aktivitäten informieren, bis die Bedrohung vollständig beseitigt werden konnte.

Mit der Implementierung von CTA als Teil von Cisco CWS Premium verfügt der Kunde nun über ein Analysesystem, das nahezu in Echtzeit das Netzwerkverhalten analysieren und mithilfe von maschinellen Lernverfahren und fortschrittlichen Statistiken IOCs im Netzwerk erkennen kann. Im Beispiel der Infektion mit der Ransomware Cryptolocker warnte CTA so lange vor schädlichen Aktivitäten, bis das Sicherheitsteam die Infektion vollständig beseitigt hatte. Dank der Einblicke, die CTA in das Verhalten von Malware bietet, können sich Sicherheitsteams beim Kunden voll und ganz auf die gefährlichsten Bedrohungen konzentrieren – und das vor, während und nach einem Angriff.

Weitere Informationen

Cisco verfolgt die Strategie, Unternehmen bei der Beseitigung bekannter und neuer Sicherheitsprobleme zu unterstützen. Dementsprechend kann Cisco CWS Premium, in dessen Lieferumfang CTA und AMP enthalten sind, Unternehmen dabei helfen, Bedrohungen zu erkennen, zu verstehen und zu beseitigen. Hierfür werden fortlaufende Analysen und intelligente Sicherheitsmaßnahmen in Echtzeit verwendet. Diese werden über die Cloud bereitgestellt und in allen Sicherheitslösungen gemeinsam verwendet, um so gleichzeitig die Effizienz zu verbessern. Durch die Kombination dieser drei Lösungen kann CWS Premium neue, von der Sicherheitsbranche noch nicht erkannte Command-and-Control-Kanäle identifizieren und gleichzeitig Sicherheitsprobleme während des gesamten Angriffskontinuums beseitigen.

Weitere Informationen zu CWS Premium finden Sie unter http://www.cisco.com/go/cws.

Weitere Informationen zu CTA finden Sie unter http://www.cisco.com/go/cognitive.

Weitere Informationen zu AMP finden Sie unter http://www.cisco.com/go/amp.

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 C36-733153-00 10/14