Whitepaper

Web Security: Schützen Sie Ihre Daten in der Cloud

Überblick

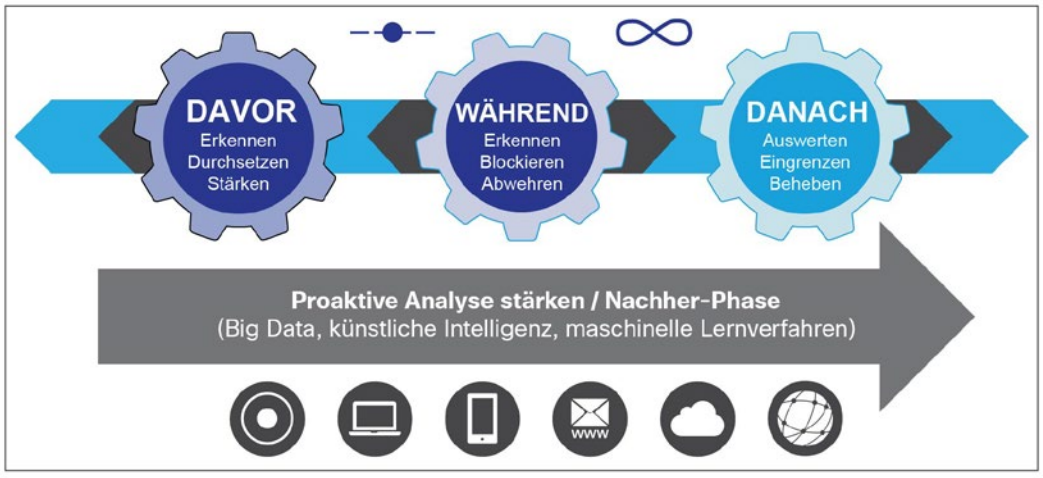
Sicherheitsteams können nicht überall sein, aber im aktuellen Umfeld ist es für Unternehmen unerlässlich, ihre Daten überall dort zu schützen, wo Bedrohungen lauern können. „Überall“ – dazu gehören Netzwerke, mobile Geräte, virtuelle Umgebungen und die Cloud oder das Rechenzentrum.

Die heutigen Gefahren und Bedrohungen sind so komplex, dass sie sämtliche Verteidigungsmaßnahmen überwinden können. Angreifer arbeiten aktiv daran, herauszufinden, welche Art von Sicherheitslösung implementiert ist, und steigen auf weniger sichtbare und schlechter erkennbare Verhaltensmuster um. **Dem Cisco Annual Security Report 2014** zufolge verfolgen die meisten Cyberkriminellen ein primäres Ziel – den Diebstahl besonders wertvoller Daten.[1]

Unterdessen sorgt das Aufkommen von auf mehrere Standorte verteilte Unternehmen und neuen Geschäftsmodellen wie Cloud Computing-, Mobility- und BYOD-Umgebungen für eine Erosion des konventionellen Sicherheitsperimeters und eine Erweiterung der Angriffsfläche. Sicherheitsteams haben Mühe, Schritt zu halten. Sie wissen nicht, welche Bedrohungen sie priorisieren sollen und können viele Gefahren schlicht und einfach nicht sehen.

Es ist offensichtlich, warum die aktuellen präventiven Punktlösungen modernen Unternehmen keinen ausreichenden Schutz bieten. Natürlich ist keine Nachweismethode wirklich perfekt, und es wird unweigerlich Bedrohungen geben, die so raffiniert und gut getarnt sind, dass sie alle Schutzfilter passieren können. Was also wird benötigt? Fortlaufende und retrospektive Sicherheitsmaßnahmen, die das gesamte Angriffskontinuum abdecken: vor, während und nach einem Angriff.

Abbildung 1. Das Angriffskontinuum



[1] Cisco Annual Security Report 2014: http://www.cisco.com/c/en/us/products/security/annual_security_report.html.

Cisco Cloud Web Security Essentials

Mit Cisco® Cloud Web Security meistern Unternehmen die Herausforderung, im erweiterten Netzwerk fortlaufende Sicherheit garantieren zu müssen. Diese Lösung bietet branchenführende Sicherheit und Kontrolle für Unternehmen mit mehreren Standorten und verfügt über die umfassendste Auswahl an Bereitstellungsoptionen. Die Cloud Web Security-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.

Cisco Cloud Web Security bietet intuitive Tools zur Erstellung, Durchsetzung und Überwachung von Richtlinien für den ein- und ausgehenden Internetdatenverkehr. So haben Unternehmen umfassende Kontrolle über den Zugriff von Endbenutzern auf Internetinhalte. Kurzum: Cloud Web Security ist ein Sicherheitsperimeter in der Cloud. Das Programm sorgt für detaillierte und kontextbezogene Kontrolle und Durchsetzung von Richtlinien. Weitere Vorteile:

- Dynamische Blockierung von Bedrohungen in Echtzeit
- Schutz von Netzwerk und Benutzern vor unerwünschten Webinhalten
- Optimierung der Netzwerkressourcen durch Reduzierung von Bandbreitenüberlastung
- Umfassende Berichterstellung und Überwachung von Online-Aktivitäten
- Schutz des Unternehmens vor Datenlecks

Cloud Web Security kann mit Cisco Firewalls, Zweigstellen-Routern und Client-basierter Software integriert werden und bietet Benutzern an allen Arbeitsplätzen umfassenden Schutz. Der Datenverkehr – ob vom Hauptsitz, von den Zweigstellen oder von mobilen oder Remote-Benutzern – wird stets durch ein globales Netzwerk von Rechenzentren geleitet. Cloud Web Security beseitigt Backhaul, beschleunigt die Websicherheit und vergrößert den Wert bestehender Cisco Investitionen.

Mit der kürzlichen Übernahme der Security-Unternehmen Sourcefire und Cognitive Security kann Cisco nun eine verbesserte Version von Cloud Web Security bereitstellen, die ausgefeilte Malware-Bedrohungen besonders in der Phase nach dem Angriff verhindert und die Echtzeiterkennung von Sicherheitsrisiken während des Angriffs optimiert. Diese Lösung wird über ein optionales Premium-Abonnement angeboten wie unten beschrieben.

Cloud Web Security Premium

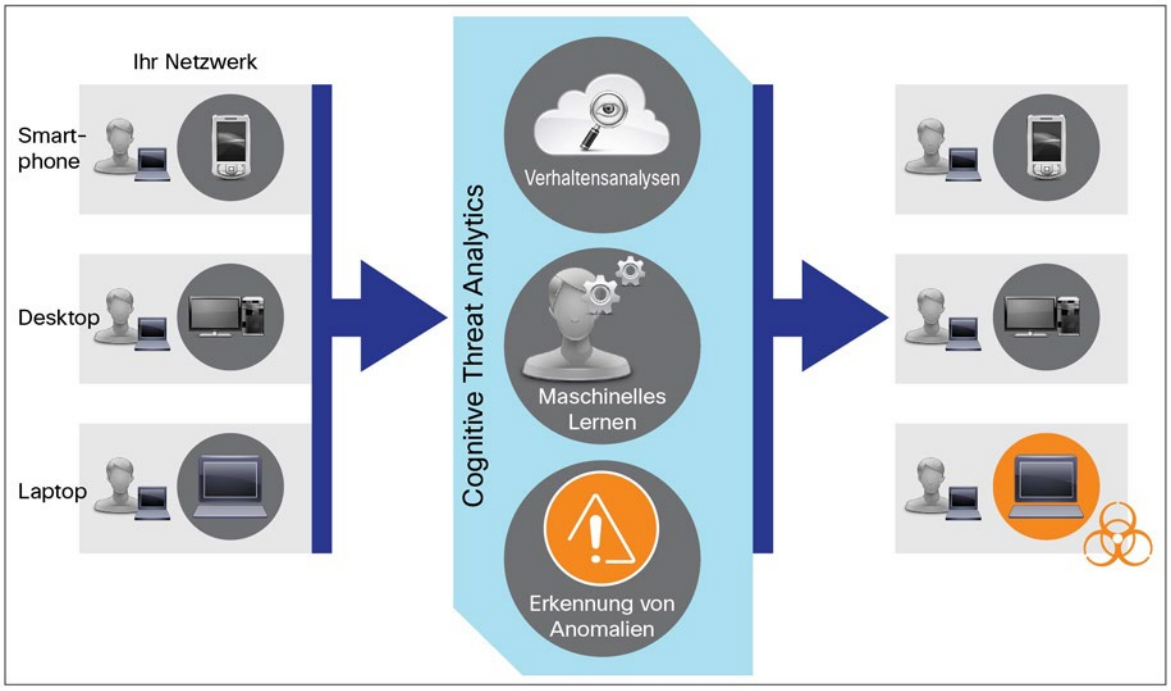
das Cloud Web Security Premium-Paket umfasst sämtliche Funktionen des Essentials-Pakets und ergänzt sie durch zwei innovative Systeme zur Erkennung von Malware: Cognitive Threat Analytics (CTA) und Advanced Malware Protection (AMP). Diese Systeme automatisieren die Suche nach Bedrohungen mit hohen Sicherheitsrisiken im Internetdatenverkehr von Unternehmen. Mit zusätzlichem Punktschutz, Retrospective Security und Funktionen zur fortlaufenden Analyse unterstützt Cloud Web Security Premium Unternehmen bei der Erkennung und Behandlung der wichtigsten Bedrohungen. Bedrohungen, die bereits in den Netzwerken aktiv sind, können noch schneller entdeckt werden.

Sicherheitsteams können nun kontinuierliche Websicherheit gewährleisten, sodass die Systeme während des gesamten Angriffskontinuums geschützt sind. Im Folgenden werden die beiden Systeme zur Malware-Erkennung näher erläutert.

Cognitive Threat Analytics

Das von Cognitive Security entwickelte System Cognitive Threat Analytics (CTA) analysiert das Netzwerkverhalten nahezu in Echtzeit. Mithilfe von maschinellen Lernverfahren und erweiterten Statistiken werden ungewöhnliche Aktivitäten im Netzwerk, die Symptome einer Infektion, aufgespürt. Die Lösung ist nicht auf Regelsets angewiesen, das heißt, die Technologie kann auch ohne Eingriff durch Benutzer eingestellt und angepasst werden. Gleich nach seiner Aktivierung nimmt CTA die Suche nach Bedrohungen auf. Daten werden in der Cloud korreliert, um eine schnellere, flexiblere und gründlichere Erkennung von Anomalien zu ermöglichen.

Abbildung 2. Übersicht zu CTA



CTA lernt selbständig. Es passt sich mit der Zeit an und identifiziert neue, von der Sicherheitsbranche noch nicht erkannte Command-and-Control-Kanäle. Es bewertet das Verhalten von Entitäten (beispielsweise Benutzern) im Internet und berechnet mithilfe von Verhaltensmodellierung das erwartete Verhalten dieser Entitäten. CTA modelliert das Netzwerkverhalten über einen langen Zeitraum und kann so scheinbar ungleichartige Aktivitäten in Bezug setzen. Die korrelierten Daten werden mit dem Verhalten einzelner Benutzer im spezifischen Kundennetzwerk verglichen. So können Bedrohungen schneller entdeckt werden.

Die Art der Bedrohung ist dabei unerheblich. CTA kennzeichnet alle signifikanten oder anhaltenden Abweichungen vom erwarteten Verhalten. Die von CTA ausgeführten Aktionen sind mit denen eines Sicherheitsteams vergleichbar, das versucht, Ladendiebe ausfindig zu machen, noch bevor sie die Möglichkeit haben, einen Diebstahl zu begehen: Welches Verhalten macht diese Person im Vergleich zu anderen Einkäufern auffällig? Trägt sie eine große Tasche bei sich anstelle eines Einkaufswagens oder -korbs? Versucht sie, den Laden durch die Hintertür zu verlassen und nicht durch die Vordertür? Auch wenn sich das auffällige Verhalten im Nachhinein als legitim erweist, ist eine Überprüfung immer sinnvoll.

CTA entdeckt Unregelmäßigkeiten und weist Sicherheitsanalysten auf potenzielle Probleme hin. So können die zuständigen Experten ihren Arbeitsaufwand reduzieren und Bedrohungen priorisieren. Das Programm ergänzt die vorhandenen Sicherheitslösungen von Cisco und ermöglicht eine präzisere und umfassendere Erkennung unbekannter oder ungewöhnlicher Verhaltensweisen im Netzwerk. Die Sicherheitsfunktionen von Cisco werden auf die Phase erweitert, die „nach“ einem Angriff stattfindet. Noch wichtiger: Mit CTA passen sich die Sicherheitsfunktionen an die sich ständig verändernden Sicherheitsbedrohungen an.

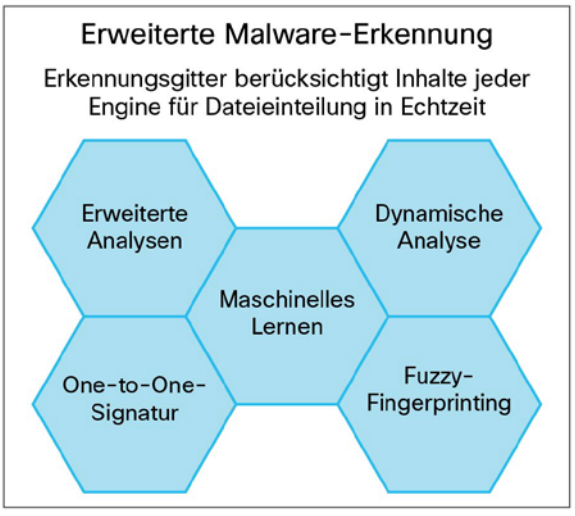
Advanced Malware Protection

Das zweite in Cloud Web Security Premium integrierte Erkennungssystem ist Advanced Malware Protection (AMP) von Sourcefire. AMP ist nicht auf Malware-Signaturen angewiesen, die oftmals erst nach Wochen oder Monaten für die einzelnen neuen Malware-Muster erstellt werden können. Stattdessen setzt es bei der Erkennung und Abwehr von Bedrohungen über das gesamte Angriffskontinuum eine Kombination aus Dateireputation, Datei-Sandboxing und retrospektiven Dateianalysen.

Dateireputation

Unter Dateireputation versteht man die Möglichkeit, in Datenbanken zu prüfen, ob eine Datei „sauber“, bekannte Malware oder unbekannt ist. AMP erfasst einen „Fingerabdruck“ der einzelnen vom Cloud Web Security-Service geprüften Dateien und fragt das gemeinsame Cloud-basierte Intelligence-Netzwerk von Cisco und Sourcefire nach einem Urteil oder Ergebnis bezüglich der Dateireputation. Auf Basis dieser Ergebnisse kann AMP schädliche Dateien automatisch blockieren und vom Administrator definierte Richtlinien anwenden. Abbildung 3 zeigt die verschiedenen Engines zur Echtzeiterkennung fortschrittlicher Malware und Ermittlung von Dateireputationen.

Abbildung 3. Advanced Malware Protection



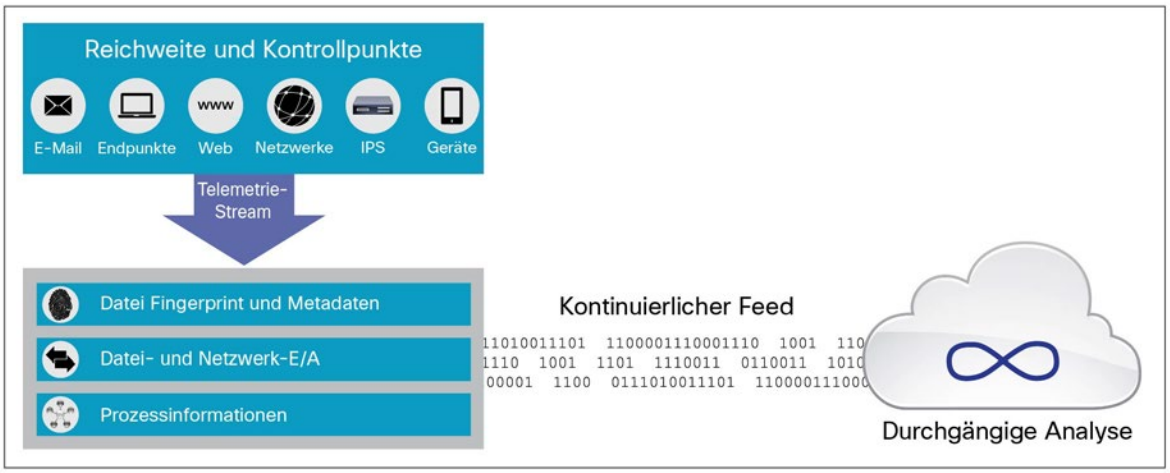
Datei-Sandboxing

Das Sandboxing von Dateien ist eine wichtige Funktion von AMP und Cloud Web Security Premium. Beim Sandboxing analysiert AMP die unbekannten Dateien, die das Netzwerk passieren. In der äußerst sicheren Sandbox-Umgebung sammelt AMP präzise Informationen über das Verhalten von Dateien und kombiniert sie mit detaillierten benutzerseitigen und maschinellen Analysen, um die Bedrohungsstufe der Datei festzulegen. Diese Informationen werden anschließend in das Cloud-basierte Intelligence-Netzwerk von Cisco und Sourcefire eingelesen, wo sie die AMP-Cloud-Datensets dynamisch aktualisieren. Mit der aktiven Berichterstellung können Sicherheitsteams informative, einfach zu lesende Berichte zu den analysierten Dateien anzeigen.

Retrospektive Datenanalyse

Der wichtigste Aspekt von AMP ist möglicherweise die Funktion der retrospektiven Datenanalyse. Sie ermöglicht es Unternehmen, den Angriffszeitpunkt rückwirkend exakt zu ermitteln und anschließend den Schaden zu beurteilen. Mit der retrospektiven Datenanalyse können Dateien, die das Security-Gateway passiert haben, kontinuierlich analysiert werden. Dafür werden Echtzeitaktualisierungen aus dem Cloud-basierten Intelligence-Netzwerk von Cisco und Sourcefire verwendet.

Abbildung 4. Retrospektiver Analyseprozess von AMP

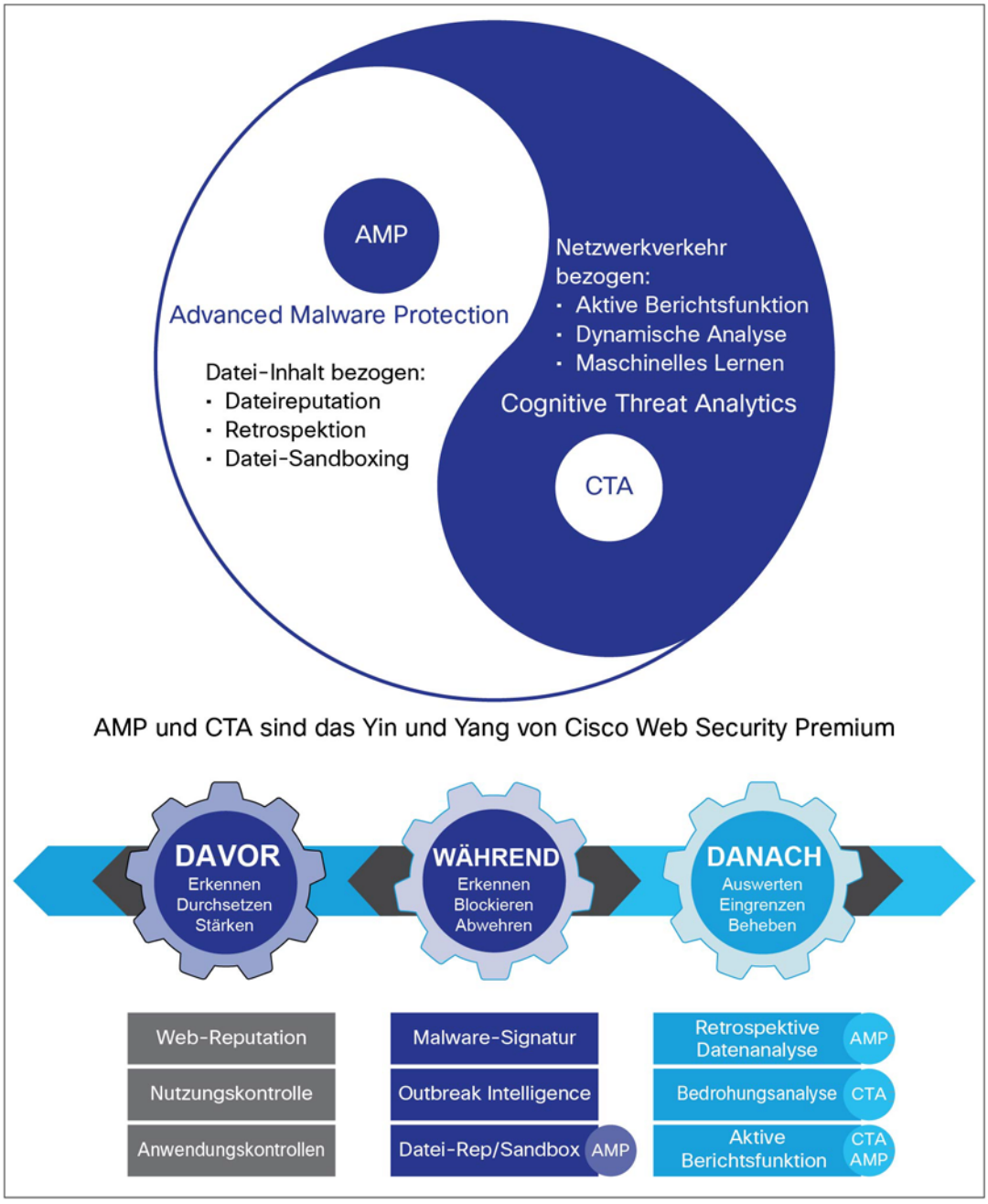


Die retrospektive Analyse kann Dateien aufdecken, die den Perimeterschutz als „sauber“ passieren konnten, eigentlich aber gut getarnte, komplexe Malware sind. AMP benachrichtigt in einem solchen Fall sofort den Sicherheitsadministrator und veranschaulicht deutlich, welche Benutzer im Netzwerk möglicherweise wann infiziert wurden. Sicherheitsteams können auf den Angriff schnell reagieren, noch bevor er sich ausbreiten kann.

Zusammenfassung

Cloud Web Security mit CTA und AMP verfolgt die Strategie, Unternehmen bei der Beseitigung bekannter und neuer Sicherheitsprobleme zu unterstützen. Mit Cisco CWS Premium sowie CTA und AMP können wir Unternehmen dabei helfen, Bedrohungen zu erkennen, zu verstehen und zu beseitigen. Die über die Cloud bereitgestellten fortlaufenden Analysefunktionen und intelligenten Sicherheitsmaßnahmen verbessern die Effizienz der vorhandenen Sicherheitslösungen. Durch die Kombination dieser drei Lösungen können Unternehmen neue, von der Sicherheitsbranche noch nicht erkannte Command-and-Control-Kanäle identifizieren und gleichzeitig Sicherheitsprobleme während des gesamten Angriffskontinuums beseitigen.

Abbildung 5. Cloud Web Security mit AMP und CTA: Sicherheit im gesamten Angriffskontinuum



Vorher: Erkennen. Durchsetzen. Stärken.

Cloud Web Security bietet Web-Reputation, Nutzungskontrollen, Anwendungskontrollen (auch für Mikroanwendungen), Malware-Signaturen und Outbreak Intelligence vor und während eines Angriffs.

Während: Erfassen. Blockieren. Abwehren.

Mit den Funktionen Dateireputation und Sandboxing sorgt AMP während des Angriffskontinuums für erhöhte Sicherheit. Schädliche Dateien werden automatisch blockiert und vom Administrator definierte Richtlinien auf Basis der bekannten Reputation einer Datei angewendet. Das Tool analysiert darüber hinaus unbekannte Dateien, die das Netzwerk durchlaufen, und aktualisiert die Bedrohungsinformationen entsprechend. Mit diesen Funktionen können Sicherheitsanalysten die zu untersuchenden Bedrohungen nach Prioritäten einteilen.

Nachher: Auswerten. Eingrenzen. Beheben.

CTA und AMP ermöglichen eine fortlaufende Analyse und Beseitigung von Bedrohungen in der kritischen Phase „nach“ dem Angriff. Mit den CTA-Echtzeitanalysen des Netzwerkverhaltens werden ungewöhnliche Verhalten entdeckt. Die retrospektive Dateianalyse von AMP spürt schädliche Dateien auf, die den Perimeterschutz bereits passiert haben. Mit den aktiven Berichtsfunktionen von AMP können Reputation und Verhalten der Dateien im Netzwerk transparent gemacht werden. Sicherheitsteams können das Ziel des Angriffs leichter erkennen und bewerten und für eine schnelle Lösung sorgen.

Die maschinellen Lernverfahren, die von CTA und AMP in der Nachher-Phase eingesetzt werden, optimieren und aktualisieren die Erkennungsfunktionen nahezu in Echtzeit, die Cloud Web Security Premium während eines Angriffs anwendet.

Weitere Informationen

Weitere Informationen zu Cisco Cloud Web Security Essentials und Cloud Web Security 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 C11-734836-00 06/15