AMP Everywhere – Übersichtskarte

Problem:	Unternehmen stehen heute unter ständigem Beschuss. Täglich brechen Cyber-Angriffe auf sie herein, und ebenso häufig kommen Sicherheitsverletzungen vor – die spektakulärsten davon gelangen sogar in die Schlagzeilen. Die Drahtzieher dieser Angriffe sind global aufgestellt und äußerst innovativ. Für ihre Kampagnen führen sie immer raffiniertere Malware ins Feld, die über unterschiedlichste Angriffsformen und -vektoren in Unternehmen aller Größenordnungen eingeschleust wird. Firewalls und IPS hatten dem bislang nur Point-in-Time-Erkennungstools entgegenzusetzen. Doch diese dynamischen Angriffe können selbst die besten von ihnen mühelos umgehen. Darin, wofür diese Tools entwickelt wurden – die Kontrolle des Datenverkehrs und der Dateien beim Eintritt in das Netzwerk –, sind sie zwar effektiv, doch sie ermöglichen nur minimalen Einblick in die Aktivitäten von Bedrohungen. Doch vor etwas, das man nicht sieht, kann man sich nicht schützen. Und so tappen die Teams aus der IT-Sicherheit schließlich im Dunkeln, was den Umfang einer potenziellen Kompromittierung betrifft, und können Malware-Infektionen somit nicht schnell genug eingrenzen, bevor erheblicher Schaden entsteht. Point-in-Time-Erkennung allein ist niemals zu 100 % effektiv. Schon bei einer einzigen Bedrohung kann die Erkennung versagen und das Netzwerk kompromittiert werden. Unternehmen benötigen eine Lösung, die den gesamten Lebenszyklus des Problems der fortschrittlichen Malware über das gesamte Angriffskontinuum hinweg effizient angehen kann und Sicherheitsverletzungen erkennen, darauf reagieren und beseitigen kann, ohne dabei das Budget zu überlasten oder die Betriebsabläufe zu beeinträchtigen.
Zentrale Botschaft	Malware wird zunehmend komplexer, zielgerichtete Angriffe nehmen weiter zu, und Cyberkriminelle starten ihre Angriffe über verschiedene Angriffsvektoren. Der Cisco Annual Security Report 2015 charakterisiert die Cyberkriminellen von heute wie folgt: • Sie ändern dynamisch ihre Taktiken und Tools, verschwinden aus einem Netzwerk, bevor sie erkannt werden können oder schalten blitzschnell auf eine andere Methode um. • Sie tarnen Malware als Tools, denen Benutzer vertrauen oder die sie als unbedenklich betrachten, um von deren Systemen aus unbemerkt weitere Infektionen einzuleiten. • Sie nisten sich bei ihrem Zielunternehmen ein, teilweise über Wochen oder Monate hinweg, bis sie genügend Ausgangspositionen in der Infrastruktur und den Benutzerdatenbanken eingerichtet haben. Erst dann starten sie ihre eigentlichen Aktivitäten. Das Sicherheitskonzept eines Unternehmens muss so umfassend sein wie die Angriffe, die gegen es gestartet werden. Es muss in der Lage sein, schwer zu erfassende Malware auszumerzen, bekannte Angriffe und schadhaftes Verhalten zu erkennen und verschiedene Schwachstellen für Angriffe auf das Unternehmen, von Mobilgeräten und Endpunkten bis hin zu Netzwerkkontrollpunkten, sichtbar zu machen. Um im Kampf gegen fortschrittliche Malware effektiv zu sein, muss der Schutz überall bestehen – kontinuierlich und rückwirkend. Cisco® Advanced Malware Protection-Lösung (AMP) geht über die Point-in-Time-Erkennung hinaus, um *überall* Schutz zu bieten und *kontinuierlich* Dateien und Dateiaktivitäten zu überwachen und bereits die ersten Anzeichen böswilligen Verhaltens zu erkennen. Die Lösung bietet das Maß an Transparenz und Kontrolle, das Sie benötigen, um komplexe Bedrohungen zu stoppen, die auf anderen Sicherheitsebenen übersehen wurden. Sie erhalten umfassenden Schutz für Ihr Unternehmen über das gesamte Angriffskontinuum hinweg – vor, während und nach dem Angriff. Die Lösung bietet fortlaufende und Zero-Day-Erkennung, moderne Analysen, Threat-Intelligence zu Malware, und kann über mehrere Angriffsvektoren bereitgestellt werden, um proaktiv vor modernsten Angriffen zu schützen und schnell auf sie zu reagieren.
Lösung	Die Advanced Malware Protection-Lösung (AMP) von Cisco ist eine intelligente, integrierte Analyse- und Schutzlösung zur Abwehr fortschrittlicher Malware. Sie ist als Abonnement erhältlich, wird über eine benutzerfreundliche, browserbasierte Management-Konsole verwaltet und kann für eine Vielzahl von Angriffsvektoren und Kontrollpunkten bereitgestellt werden: • als netzwerkbasierte, in Cisco ASA Firewall- und Cisco FirePOWER Network Security-Appliances integriere Lösung, die ein breites Spektrum an Netzwerkdurchsatz und Verarbeitungsleistung abdeckt • als Endpunktlösung für PCs, Macs, Mobilgeräte und virtuelle Umgebungen • als virtuelle Private-Cloud-Appliance vor Ort, die für Umgebungen mit hohen Datenschutzanforderungen konzipiert wurde • als integrierte Funktion in Cisco Cloud Web Security- oder Cisco Web Security- und E-Mail Security-Appliances • als Standalone-Threat-Intelligence- und dynamische Malwareanalyse-Lösung über das AMP Threat Grid, bereitgestellt als Appliance oder Cloud-basiertes Abonnement und entwickelt mit Technologie, die Cisco im Juni 2014 von ThreatGRID übernommen hat

Die Lösung geht über eine einfache Entdeckungsstrategie hinaus und gewährleistet Schutz über das gesamte Angriffskontinuum hinweg – vor, während und nach einem Angriff.

Vor einem Angriff nutzt AMP branchenführende, globale Threat-Intelligence, um den Netzwerkschutz gegen bekannte und unbekannte Angriffe zu stärken. Cisco Collective Security Intelligence und die Premiuminhalte von AMP Threat Grid bieten umfangreiche, kontextbezogene Threat-Intelligence, um aktuelle Bedrohungen abzuwehren.

Während eines Angriffs nutzt AMP diese Informationen in Kombination mit bekannten Dateisignaturen und der dynamischen Malwareanalysetechnologie von AMP Threat Grid, um gegen die Richtlinien verstoßende Dateitypen und schädliche Dateien, die in das Netzwerk eindringen wollen, zu identifizieren und zu blockieren.

Was die Cisco AMP jedoch einzigartig macht, sind die Aktivitäten nach einem Angriff. Sie analysiert kontinuierlich alle Dateien und sämtlichen Datenverkehr auf schadhaftes Verhalten auch über die Anfangsinspektion hinaus. Wenn jetzt eine Datei nach dem Angriff schadhaftes Verhalten zeigt, erkennt AMP diese und bietet Sicherheitsteams die erforderliche Transparenz und Kontrolle, damit diese schnell reagieren und die Bedrohung entfernen können. Möglich wird dies durch Retrospective Security: die Möglichkeit, die Aktivität jeder Datei im System aufzuzeichnen und dann rückwirkend nachzuvollziehen, wo der Ursprung einer möglichen Bedrohung liegt und welches Verhalten sie gezeigt hat, und die Möglichkeit, integrierte Reaktionsfähigkeiten anzubieten, um die Bedrohung zu beseitigen.

Kontinuierliche Erkennung von Sicherheitsverletzungen

- *Mehr Transparenz*: Die Cisco AMP-Lösung geht über die Point-in-Time-Erkennung hinaus, um Dateien und Datenverkehr kontinuierlich zu erfassen und zu analysieren. Diese Funktionen ermöglichen Retrospective Security – die Möglichkeit, Prozesse, Dateiaktivitäten und Kommunikationswege zeitlich zurückzuverfolgen, um für Unternehmen das vollständige Ausmaß einer Infektion sowie deren Ursache zu ermitteln und sie zu beseitigen.

- *Kontinuierliche Analyse*: Wird eine überwachte Datei nachträglich als schädlich erkannt, so löst das Cisco AMP-System auch dann noch eine retrospektive Warnmeldung aus, wenn die Datei den Endpunkt oder das Netzwerk bereits vor mehreren Stunden oder Tagen durchlaufen hat, damit Sie immer noch reagieren und den Schaden mindern können.

- *Erkennen und Blockieren von Exploit-Versuchen*: Bei Inline-Bereitstellung kann die AMP-Lösung clientseitige Exploit-Versuche erkennen und blockieren. Sie bietet außerdem Schutz gegen Exploits von Sicherheitslücken in Adobe Acrobat, Java, Flash und anderen Client-Anwendungen, die häufig Ziel von Angriffen sind.

Reagieren und Beheben

- *Erkennung bekannter und unbekannter Bedrohungen*: Das System blockiert schädliche Dateien auf dem Zielsystem und analysiert lokal Dateien mit unbekannter Einstufung. Die Dateien, die an AMP Threat Grid übermittelt werden, werden anhand von Verhaltensindikatoren und Milliarden von Malwareartefakten ausgewertet.

- *Schnelle Reaktion*: Die Trajectory-Ansichten von AMP erleichtern die Identifizierung der Ereigniskette, die zur Verbreitung von Malware geführt hat, um das Problem schnell einzudämmen. Dabei können bestimmte Anwendungen, Dateien, Malware oder Ursachen ins Visier genommen werden. So lässt sich die Angriffskette schnell und einfach unterbrechen.

- *Automatisierte Eindämmung*: AMP verfolgt Aktivitäten über Web, E-Mail, Endpunkte und Netzwerk-Appliances, erkennt automatisch Dateien und Anwendungen und führt mithilfe von Datei- und Anwendungskontrollrichtlinien eine breit angelegte Filterung von Dateien durch.

Stärkere Sicherheitsverfahren

- *Aufwertung Ihrer früheren Investitionen* in Sicherheit: AMP Threat Grid ist mit vorhandenen Sicherheitstechnologien integriert, um die Übertragung von Stichproben für Analysen und Berichte zu automatisieren.

	• *Leistungsstarke Korrelation*: AMP zeigt die Risiken auf, die mit einem laufenden Angriff verbunden sind. Sie erstellt automatisierte und priorisierte Listen potenziell kompromittierter Geräte mit kombinierten Daten zu Sicherheitsereignissen aus mehreren Quellen. • *Kontextbasierte Malwareanalyse*: Die AMP-Lösung stellt fest, wie Malware agiert, einschließlich des zugehörigen HTTP- und DNS-Verkehr und TCP/IP-Strömen, betroffener Prozessen und Registry-Aktivitäten, was Sicherheitsteams in die Lage versetzt, Bedrohungen in ihren Netzwerken besser zu erkennen, und durch Malware verursachte Sicherheitsverletzungen möglichst gering zu halten. Diese Funktionen in ihrer Gesamtheit liefern eine umfassende Darstellung des Geschehens im erweiterten Netzwerk und für Sie die Informationen, die Sie benötigen, um wichtige Sicherheitsfragen zu beantworten – unter anderem: • Woher kam die Malware? • Welche Systeme waren betroffen? • Was tut die Bedrohung? • Und wie kann sie gestoppt werden? Mit diesen umsetzbaren Informationen können Sie fundiertere Entscheidungen zu Sicherheitsrichtlinien treffen, die Zeit zur Erkennung, Eindämmung und Beseitigung der Malware im Netzwerk deutlich verkürzen und ähnliche Angriffe in Zukunft verhindern. Das Ergebnis ist ein effektiverer, effizienterer und tiefer greifender Schutz für Ihr Unternehmen. **Lösungsüberblick in 100 Wörtern** Die Cisco Advanced Malware Protection-Lösung (AMP) schützt das erweiterte Netzwerk vor, während und nach einem Angriff. Die Lösung bietet kontinuierliche Erkennung und retrospektive Warnmeldungen, proaktive Threat-Intelligence, erweiterte Analysen und Funktionen der Enterprise-Klasse, um auf die modernsten Angriffe von heute schnell zu reagieren und sie schnell zu beseitigen. Vor einem Angriff nutzt AMP kontextbezogene Threat-Intelligence zur Verbesserung der Abwehrmechanismen des Netzwerks. Während eines Angriffs kombiniert AMP diese Informationen mit bekannten Dateisignaturen und dynamischer Malwareanalyse, um Malware, die in das Netzwerk eindringen will, zu identifizieren und zu blockieren. Nach einem Angriff stellt AMP einen gespeicherten Verlauf aller Dateiaktivitäten zur Verfügung, der Sicherheitsteams unübertroffene Transparenz und Kontrolle in ihren Umgebungen bietet. **Lösungsüberblick in 50 Wörtern** Die Cisco Advanced Malware Protection-Lösung (AMP) schützt das erweiterte Netzwerk vor, während und nach einem Angriff. Die Lösung bietet kontinuierliche Erkennung und retrospektive Warnmeldungen, Bedrohungsinformationen, erweiterte Analysen und Unternehmensfunktionen, die über mehrere Angriffsvektoren bereitgestellt werden können, um proaktiv vor modernsten Angriffen zu schützen und schnell auf diese zu reagieren. **Lösungsüberblick in 25 Wörtern** Die Advanced Malware Protection-Lösung (AMP) von Cisco bietet kontinuierliche Erkennung, retrospektive Warnmeldungen, Threat-Intelligence, erweiterte Analysen und Funktionen der Enterprise-Klasse, um proaktiv vor modernsten Angriffen zu schützen und schnell auf sie zu reagieren.
Themen und Grundideen zu Messaging	**<u>Allgemeine AMP-Themen</u>** AMP bietet Erkennung von, Reaktion auf und Beseitigung von Bedrohungen • AMP geht über Point-in-Time-Erkennung hinaus, um kontinuierliche Überwachung, verhaltensbasierte Erkennung und Reaktionsfähigkeiten bereitzustellen. • AMP ermöglicht Unternehmen, die Reaktion auf Bedrohungen über Retrospective Security zu verbessern. • Cisco verbessert die Bedrohungserkennung mithilfe der aktuellen Malware-Threat-Intelligence von AMP Threat Grid, um die bestehende Sicherheitsinfrastruktur zu stärken. • AMP wurde entwickelt, um Angriffe zu verhindern und Bedrohungen durch ein Eindringen schnell zu beheben, und bietet damit Schutz über das gesamte Angriffskontinuum hinweg.

Kernelemente der Botschaft und Funktionsüberblick

Durchgängige Erkennung und Retrospective Security

AMP geht über herkömmliche Point-in-Time-Erkennungsfunktionen hinaus, um retrospektive Warnmeldungen und dynamische Malwareanalysen bereitzustellen und bekannte und unbekannte Malware daran zu hindern, die implementierten Schutzfunktionen zu überwinden. Auch nachdem Dateien einen Sicherheitskontrollpunkt durchlaufen haben, überwacht AMP kontinuierlich alle Dateiaktivitäten und sämtlichen Datenverkehr auf Endpunkten, Mobilgeräten und im Netzwerk (unabhängig von der Einstufung der Dateien), analysiert und zeichnet jede ihrer Bewegungen auf. Wenn eine Datei mit einer unbekannten oder zuvor mit „gutartigen" Einstufung beginnt, schädliches Verhalten zu zeigen, alarmiert AMP sofort Sicherheitsteams durch eine retrospektiven Warnmeldung und Indications of Compromise und informiert, was genau geschehen ist. Sie können den gesamten Verlauf einer Bedrohung sehen – woher die Malware kam, wo sie sich befunden hat, welche Systeme betroffen waren und was die Bedrohung gerade tut. Diese retrospektive Funktion – die Aktivität jeder Datei auf Ihrem System aufzuzeichnen und dann zeitlich zurückzuverfolgen, um den Ursprung und das Verhalten einer potenziellen Bedrohung festzustellen – gewährleistet Sicherheitsteams die erforderliche Transparenz, um Bedrohungen schnell erkennen zu können, und bietet die benötigten Kontrollfunktionen, um sie zu stoppen. Sie können die Zeit bis zur Erkennung, Eindämmung und Beseitigung von Malware (auch von Zero-Day-Angriffen) deutlich verkürzen und in Zukunft ähnliche Angriffe verhindern.

Neuerungen zum Start am 7. April

- Bei AMP für Endpunkte können Benutzer ihre eigenen Indicators of Compromise (IoCs) von Endpunkten übermitteln, um zielgerichtete Angriffe abzufangen. Mit diesen Endpunkt-IoCs können Sicherheitsteams genauere Analysen zu weniger bekannten intelligenten Bedrohungen durchführen, die spezifisch für ihre Umgebung sind. Zielgerichtete Angriffe nehmen kontinuierlich zu, und Hacker erstellen Malware, die zielgerichtet bestimmte Anwendungen bestimmter Unternehmen angreifen. Endpunkt-IoCs sind eine großartige neue Möglichkeit, sich davor zu schützen.

- Bei AMP für Endpunkte zeigt unsere Low Prevalence-Funktion Dateien, die innerhalb des Unternehmens ausgeführt wurden, sortiert von der niedrigsten zur höchsten Anzahl an Instanzen. Im Allgemeinen sind Dateien, die von vielen Benutzern ausgeführt werden, legitime Anwendungen, während solche, die nur von einem oder zwei Benutzern ausgeführt wurden, möglicherweise schädlich sind. Über Low Prevalence können Sie diese unerkannten Bedrohungen, die nur von einigen wenigen Benutzern bemerkt wurden, beseitigen. Sie können dann das Trajectory-Tool von AMP nutzen, um den gesamten Verlauf der Datei einzusehen, und die Dateianalyse (unterstützt durch AMP Threat Grid) verwenden, um Dateien mit niedriger Verbreitung daraufhin zu analysieren, ob es sich bei diesen tatsächlich um ernsthafte Bedrohungen handelt.

Threat-Intelligence und erweiterte Analysen

Cisco AMP stützt sich auf das branchenweit umfangreichste Repository aus Echtzeit-Threat-Intelligence und -Analysen, das Cisco Collective Intelligence u. a. unter Einsatz der Forschungsergebnisse der Talos Security Intelligence and Research Group bereitstellt. AMP korreliert kontinuierlich und retrospektiv Dateien, Verhalten, Telemetriedaten und Aktivitäten mit dieser robusten, kontextbasierten Wissensdatenbank, um Malware und Indications of Compromise zu erkennen. Sicherheitsteams profitieren von der automatisierten Analyse durch AMP. Sie sparen Zeit bei der Suche nach schädlichen Aktivitäten und haben jederzeit Zugriff auf Threat-Intelligence, mit deren Hilfe sie fortschrittliche Angriffe, die ihr Unternehmen bedrohen, schnell verstehen, priorisieren und blockieren und ihre Umgebungen wiederherstellen können.

Neuerungen zum Start am 7. April

- Die neue Integration von AMP Threat Grid in die AMP-Lösungen bietet extrem genaue Feeds mit Bedrohungsinhalten, mit denen Unternehmen kontextbezogene Threat-Intelligence speziell für ihre Umgebung generieren können. Die Feeds werden in Standardformaten bereitgestellt, um sich nahtlos in bestehende Sicherheitstechnologien zu integrieren und die Chancen für Unternehmen, zukünftige Angriffe zu erkennen und zu verhindern, drastisch zu verbessern.

- AMP Threat Grid analysiert zudem Millionen von Stichproben pro Monat im Hinblick auf mehr als 350 Verhaltensmerkmale, was zu Milliarden von Artefakten führt. Diese Analyse liefert außerdem eine leicht verständliche Bewertung der Bedrohung, mit der Sicherheitsteams Bedrohungen priorisieren und fundiertere Sicherheitsentscheidungen treffen können. Diese umfassende Skalierbarkeit und Abdeckung globaler Bedrohungen ermöglicht Sicherheitsteams, potenzielle Bedrohungen in ihren Netzwerken besser zu erkennen und von Malware verursachte Sicherheitsverletzungen zu minimieren.

	• Laut Cisco Annual Security Report 2015 gibt es immer mehr Schwachstellen in Netzwerken von Unternehmen, und Sicherheitsteams wissen nicht, wie sie die anfälligsten Hosts identifizieren können oder um welche Schwachstellen sie sich zuerst kümmern sollen. Diese neue Schwachstellenfunktion von AMP für Endpoints liefert eine Liste anfälliger Software, eine Liste anfälliger Software auf jedem Host sowie der Hosts, die am ehesten angegriffen werden könnten. Unterstützt durch Threat-Intelligence und Sicherheitsanalysen ermittelt AMP anfällige Software, auf die Malware abzielt, und den möglichen Schaden, sodass Sie eine priorisierte Liste der Hosts erhalten, die mit Patches versehen werden müssen. **Ausgelegt für den Unternehmenseinsatz** Die Cisco AMP-Lösung ist ein abonnementbasierter Service, der sich über eine benutzerfreundliche Management-Konsole im Browser verwalten lässt. Dazu ist die Lösung auf verschiedenen Plattformen einsatzbereit und in der Lage, unterschiedlichste Leistungs- und Speicheranforderungen zu erfüllen, um den Bedürfnissen größerer Unternehmen zu entsprechen. Unternehmen können Ort und Art der Bereitstellung individuell auf ihre Sicherheitsanforderungen abstimmen. Folgende Bereitstellungsoptionen sind für die Lösung verfügbar: • netzwerkbasierte Lösung o integriert in eine dedizierte Cisco ASA-Firewall als Teil des Produkts Cisco ASA mit FirePOWER Services (AMP auf ASA mit FirePOWER Services) o integriert in eine dedizierte Cisco FirePOWER-Appliance für die Netzwerksicherheit, die ein breites Spektrum an Netzwerkdurchsatz und Verarbeitungsleistung abdeckt (AMP für Netzwerke) • als Endpunkt-Lösung für PCs, Macs, Mobilgeräte und virtuelle Umgebungen (AMP für Endpoints) • als virtuelle Private Cloud-Appliance vor Ort, die für Umgebungen mit hohen Datenschutzanforderungen konzipiert wurde (AMP Private Cloud Virtual Appliance) • als integrierte Funktion in Cisco Cloud Web Security- oder Cisco Web Security- und E-Mail Security-Appliances • als Standalone-Threat-Intelligence- und dynamische Malwareanalyse-Lösung über das AMP Threat Grid, bereitgestellt als Appliance oder Cloud-basiertes Abonnement • AMP für Endpunkte kann über das AnyConnect 4.1 Remote-Access-VPN auch auf Endpunkten gestartet und geladen werden. **Neuerungen zum Start am 7. April** Netzwerk • AMP auf ASA mit FirePOWER Services • AMP für dedizierte Netzwerk-Appliances • AMP Threat Grid Appliance Endpunkt • Mac Inhalt • Verbesserungen für ESA/WSA/CWS Management vor Ort • Private Cloud 2.0
Security-Services	Die zahlreichen Funktionen von AMP können als Service mit der Managed Threat Defence-Lösung (MTD) von Cisco genutzt werden. MTD ist eine vollständig verwaltete Sicherheitslösung, die zuverlässige Echtzeitanalysen verwendet, um Angriffe schneller zu erkennen, die Effizienz von Sicherheits- und Netzwerksachkenntnis zu optimieren und vor fortschrittlicher Malware über ausgedehnte Netzwerke von Unternehmen hinweg zu schützen. Der Incident Response Service von Cisco nutzt das AMP-Portfolio und die Threat-Intelligence von Cisco TALOS neben einem Team aus Experten zur Informationssicherheit, um Unternehmen dabei zu helfen, sich auf Vorfälle vorzubereiten, diese zu verwalten und schnell und effektiv auf sie zu reagieren und ihre Umgebung wiederherzustellen.