Whitepaper

Sicherheit im Einzelhandel: Kundendaten schützen und gleichzeitig Geld und Zeit sparen

Überblick

In den IT-Umgebungen des Einzelhandels vollzieht sich gerade ein beispielloser technologischer Wandel. Die Anforderungen in Geschäften und Läden steigen, und Kunden erwarten bei den Services vor allem Leistung und Sicherheit. Auch Einzelhandelsunternehmen haben mit gut organisierten Hackern zu kämpfen, die Sicherheitslücken in den Netzwerken und Point-of-Sale-Systemen (POS) ausnutzen. Viele Angriffe enden bedauerlicherweise mit dem Diebstahl von Kreditkarten- und Kundendaten.

In diesem Whitepaper werden die Herausforderungen für Netzwerke im Einzelhandel zusammengefasst. Darüber hinaus wird die Sicherheitslösung von Cisco® erläutert, die hier effektiven, aktuellen und zuverlässigen Schutz bietet: Cisco Cloud Web Security (CWS).

Bedrohungen in Einzelhandelsumgebungen nehmen zu

Es ist keine leichte Aufgabe, die ladeneigenen Netzwerke an die Leistungs- und Sicherheitsanforderungen anzupassen. Von der einfachen Kontrolle des Internetzugangs bis hin zu den komplexen Compliance-Anforderungen des Payment Card Industry Data Security Standard (PCI DSS) – Einzelhandelsunternehmen benötigen eine proaktive Kontrolle des Netzwerkverkehrs. Eine effektive Sicherheitslösung für das Netzwerk im Laden muss eine umfassende Kontrolle ermöglichen und gleichzeitig mit immer schnelleren Veränderungen Schritt halten. Noch wichtiger: Sie muss in der Lage sein, sich der zunehmenden Komplexität der Bedrohungslandschaft anzupassen.

Trotz der Bemühungen von Sicherheitsexperten und der gesamten Branche nimmt die Anzahl der Angriffe und Sicherheitsverletzungen, die in Medien Beachtung finden, weiterhin zu. Hiervon betroffen sind neben Fortune 10-Einzelhändlern auch globale Franchising-Restaurants (Abbildung 1). Das Ziel der Angreifer sind immer wieder die Zahlungssysteme dieser Unternehmen. Diese Sicherheitsverletzungen haben Firmenmarken und Kundenvertrauen geschädigt. Maßnahmen zur Schadensminderung oder Entschädigung belaufen sich teilweise auf mehrere hundert Millionen Dollar.

Abbildung 1. Die größten Datensicherheitsverletzungen in der Geschichte Amerikas (basierend auf Kosten der Angriffe)

Quellen: Bloomberg, Privacy Rights Clearinghouse, Breach Level Index

Wi-Fi-Zugänge für Kunden und interaktive mobile Einkaufsmöglichkeiten haben dazu geführt, dass Läden und Geschäfte ihren Kunden mittlerweile immer öfter auch Shopping-Apps und einen Netzwerkzugang zur Verfügung stellen. Diese Services haben zwar einen nachweislichen Kundennutzen, führen aber auch zu einer zunehmenden Komplexität des Netzwerks und erhöhen den Druck für bestehende IT-Ressourcen. Die Online-Services vergrößern die Angriffsfläche. Unternehmen sind vermehrt Angreifern ausgesetzt, die nach Sicherheitslücken im Netzwerk suchen und sie für ihre Zwecke ausnutzen. Einzelhändler müssen daher unbedingt sowohl in den Filialen als auch in der Zentrale in den Schutz von Kundendaten investieren.

Das Internet of Things (IoT) ist ein weiterer IT-Trend, mit dem Händler umgehen müssen. Das IoT ist ein Netzwerk der physischen Objekte, die mit dem Internet verbunden sind und mit dem internen Netzwerk und der externen Umgebung interagieren. Einzelhändler können beispielsweise relevante Produktinformationen in Echtzeit an mobile Geräte von interessierten Kunden weiterleiten. Diese Informationen sind auf kontextabhängige Kundeninformationen abgestimmt, die von Waren im Laden gesammelt werden.

Andere IoT-Geschäftsanwendungen verfolgen über RF-Tags eingehende Warenlieferungen in Echtzeit oder ermöglichen Supply Chain-Lieferanten Zugriff auf die internen Systeme, um die operativen Vorgänge zu beschleunigen. Die vielen verschiedenen Geräte im IoT erhöhen die Anzahl kritischer Technologien im Laden selbst. In vielen Fällen sind keine Sicherheitsvorkehrungen in diese Geräte integriert. Sie können höchstens nachträglich hinzugefügt werden.

Aufgrund der anspruchsvollen Gewinnspannen im Einzelhandel gehört es für Unternehmen zur harten Realität, einerseits die sich ständig verändernde Bedrohungslage bewältigen und andererseits Kunden innovative, personalisierte Einkaufserfahrungen ermöglichen zu müssen. Immer häufiger ist es erforderlich, POS-Systeme zu aktualisieren oder in Sicherheitstechnologien zu investieren, um das Risiko eines Datenverlusts einzudämmen. Der Einzelhandel steht angesichts der zunehmenden Bedrohungslage nicht still. Erst kürzlich haben sich Unternehmen zusammengeschlossen, um die Initiative Retail Cyber Intelligence Sharing Center (R-CISC) ins Leben zu rufen.

Die Schwachstelle im Einzelhandel

Dem Verizon Data Breach Investigations Report 2013 zufolge standen Einzelhandelsunternehmen und Restaurants im Jahr 2013 auf Platz zwei der am häufigsten angegriffenen Unternehmen. Kunden kaufen zwar weiterhin auch bei Einzelhändlern ein, die Opfer eines Angriffs wurden, jedoch legt ein von Retail News Insider im Jahr 2014 veröffentlichter Bericht nahe, dass sie vermehrt mit Bargeld statt mit Kreditkarte zahlen, was zu einem Rückgang der Ausgaben führt.

Laut einem Bericht von Interactions Consumer Experience Marketing aus dem Jahr 2014 sind Angreifer nicht besonders kreativ, wenn es um das Ziel Einzelhandel geht. „Im Vergleich zu anderen Branchen setzten Angreifer im Einzelhandel relativ wenige Methoden für den Datenabruf ein", so das Ergebnis der Gruppe. 97 Prozent der Angriffe auf Einzelhandelsunternehmen waren Manipulationen von Abrechnungssystemen.

Die Erkennung von Sicherheitsverletzungen ist für Einzelhandelsunternehmen eine große Herausforderung. In der Regel verbleibt Malware solange in der IT-Umgebung bis eine Drittpartei (in der Regel die Strafverfolgung oder Betrugserkennung) Anzeichen für ungewöhnliche Aktivitäten erkennt. Wie eine dreijährige Studie von Verizon Enterprise Solutions belegt, die 2014 in einem Artikel in Bloombergs Businessweek zitiert wurde, erkennen Unternehmen Sicherheitsverletzungen im Durchschnitt nur in 31 Prozent der Fälle mithilfe eigener Überwachungsprozesse. Bei Einzelhändlern sind es 5 Prozent.

Tabelle 1 zeigt vier Beispiele für die größten im Jahr 2014 gemeldeten Sicherheitsverletzungen. Zusätzlich wird angegeben, wie lange die Malware vor ihrer Entdeckung bereits in die IT-Umgebung integriert war.

Tabelle 1. Merkmale der größten Verletzungen der Netzwerksicherheit im Jahr 2014

Angriff	Dauer	Angriffsmethode	Problemstelle
Spirituosenhandlung (USA)	17 Monate	„Low-and-Slow"	Technologie
Handwerkskette (USA und Kanada)	8 bis 9 Monate	Manipulierte POS-Systeme	Prozesse
Baumarktkette (USA und Kanada)	6 Monate	Angepasste Malware – Umgehung von Erkennungsprozessen und Angriff auf Kassensysteme	Sicherheit keine Priorität; Produktfunktionen ungenutzt
Online-Einzelhandel	3 Monate	Datenbank-Hacking	Mitarbeiter und Technologie

Quellen: Sophos, Bank Information Security, Krebs on Security, Bloomberg News, Private WiFi.com und die Huffington Post

Funktionalitäten und funktionale IT-Anforderungen nehmen zu

Die IT-Netzwerkumgebungen von Einzelhändlern werden zunehmend komplexer. Auch ihre Verwaltung wird immer aufwändiger. Der Mangel an Spezialisten in der IT-Branche macht die Verwaltung dieser über die Netzwerke der Läden verbundenen Umgebungen noch schwieriger. Um fehlende IT-Kräfte besonders im Bereich der Internetsicherheit zu kompensieren, zentralisieren IT-Gruppen Verwaltung und Betrieb der IT-Umgebung.

Die größte Herausforderung in puncto Komplexität stellen Netzwerke dar, die ursprünglich verwendet wurden, um POS-Kassen mit Backend-Servern und dem unternehmensweiten WAN zu verbinden. Diese auf geringen Datenverkehr ausgerichteten Netzwerke bedienen nun auch viele andere Anwendungen, beispielsweise Marketing, Intranet- und Internetzugang für Mitarbeiter, IoT-Anwendungen, Alarm- und Videoüberwachungssysteme und Wi-Fi für Gäste.

Das Angebot an hochentwickelten Technologien für Einzelhändler steigt ständig. Sie bieten Kunden herausragenden Mehrwert und werden daher für den Einzelhandel unverzichtbar sein. Diese Lösungen benötigen jedoch gleichzeitig mehr Bandbreite und bedeuten einen erhöhten Datenverarbeitungsaufwand. Es ist schwierig, Bandbreitenanforderungen vorherzusagen, da sie standortabhängig sind. Das macht die Lage noch komplizierter. Die Anforderungen hängen nicht nur von der Ladengröße, sondern auch von den verwendeten Technologien ab.

Ursprünglich war das Sicherheitsmodell der meisten Netzwerke in Geschäften auf den Schutz des internen Netzwerkverkehrs ausgelegt. Nun werden jedoch auch Kommunikationen außerhalb des Heimnetzes unterstützt, beispielsweise Verbindungen zu Geschäftspartnern, Lieferanten und dem Internet.

Ausreichende Sicherheit kann nur gewährleistet werden, wenn Unternehmen neue präventive und detektive Kontrollfunktionen implementieren, die Geräte und Benutzer auf Netzwerkebene besser differenzieren, die Netzwerknutzung besser kontrollieren und akzeptable Nutzungsrichtlinien bereitstellen können. Angesichts der Art der Malware und Angriffe im Einzelhandel ist offensichtlich, dass sich alle in das Einzelhändlernetzwerk eingebundene Geräte in einer feindlichen Umgebung befinden.

Wie lässt sich die Bedrohungslage definieren? Eindringlinge nehmen in erster Linie den einfachsten Weg. Daher liegt der Fokus auf den POS-Kassen. Hardware, Betriebssysteme und Softwarekomponenten vieler führenden POS-Systeme sind leider Standardausfertigungen, die bereits durch simple Angriffe gefährdet sind. Die POS-Anbieter mögen die Systeme zwar regelmäßig patchen, die Betriebskosten für das Patchen von hunderttausenden Geräten sind jedoch erheblich. In der Regel sind auch manuelle Aktualisierungen erforderlich.

Die herkömmlichen Verbindungen von POS-Systemen in das öffentliche Internet sind ein großer Risikofaktor. Eine solche Installation lässt den Remote-Betrieb zu, bei dem sich die POS-Backend-Systeme in einer anderen Einrichtung befinden und Support remote bereitgestellt werden kann. Die für den Betrieb zuständigen Gruppen müssen zwischen optimierter Geräteverwaltung und geringerem Risiko von Netzwerkangriffen wählen. Dieser Kompromiss sollte nicht notwendig sein.

Konventionelle Security-Gateways erfordern die Installation eines zentralen Gateways in der Unternehmenszentrale. Die einzelnen Geschäfte oder Filialen leiten den gesamten Verkehr an den zentralen Aggregationspunkt weiter. Dort wird er geprüft, bevor er an das Internet weitergeleitet wird. Aufgrund des erhöhten Datenaufkommens (ein- und ausgehend) in den Geschäften benötigt dieser Ansatz eine große Bandbreite. Compliance ist ebenfalls ein wesentlicher zu berücksichtigender Faktor, da die IT des Einzelhandels weiterhin zum Zuständigkeitsbereich des PCI DSS gehört. Um Vorschriften einhalten und jährliche Prüfungen bestehen zu können, müssen Unternehmen Verbindungen durch proaktive Netzwerkkontrollen schützen und die laufende Sicherheit von Systemen gewährleisten, welche die Daten von Karteninhabern verarbeiten.

Zusammenfassend kann man also sagen, dass Netzwerke in Läden und Geschäften ursprünglich mit dem alleinigen Ziel eingerichtet wurden, die POS-Systeme mit dem unternehmensweiten WAN zu verbinden. Die Lösungen wurden in der Regel innerhalb des Sicherheitsperimeters des Unternehmens bereitgestellt. Die aktuellen Sicherheitsverletzungen der POS-Systeme legen nahe, dass diese Netzwerkarchitektur für Läden und Geschäfte nicht mehr geeignet ist.

Gängige Lücken in IT-Umgebungen

Da der Druck auf Einzelhändler steigt, Sicherheitsprobleme möglichst zügig zu lösen, greifen sie häufig auf Punktlösungen zurück. Ein umfassendes Sicherheitsmodell muss jedoch mehr bieten als eine Punktlösung. Es muss alle Sicherheitskontrollen implementieren, die die heutigen und zukünftigen Anforderungen erfüllen können.

Der Unterschied zwischen einer Punktlösung und einer umfassenden Sicherheitslösung kann bei der direkten Internetanbindung in den Geschäften veranschaulicht werden. Bei der direkten Internetverbindung wird das Ladennetzwerk durch eine neue Firewall geschützt. Für die Firewall sind zwei Modelle möglich.

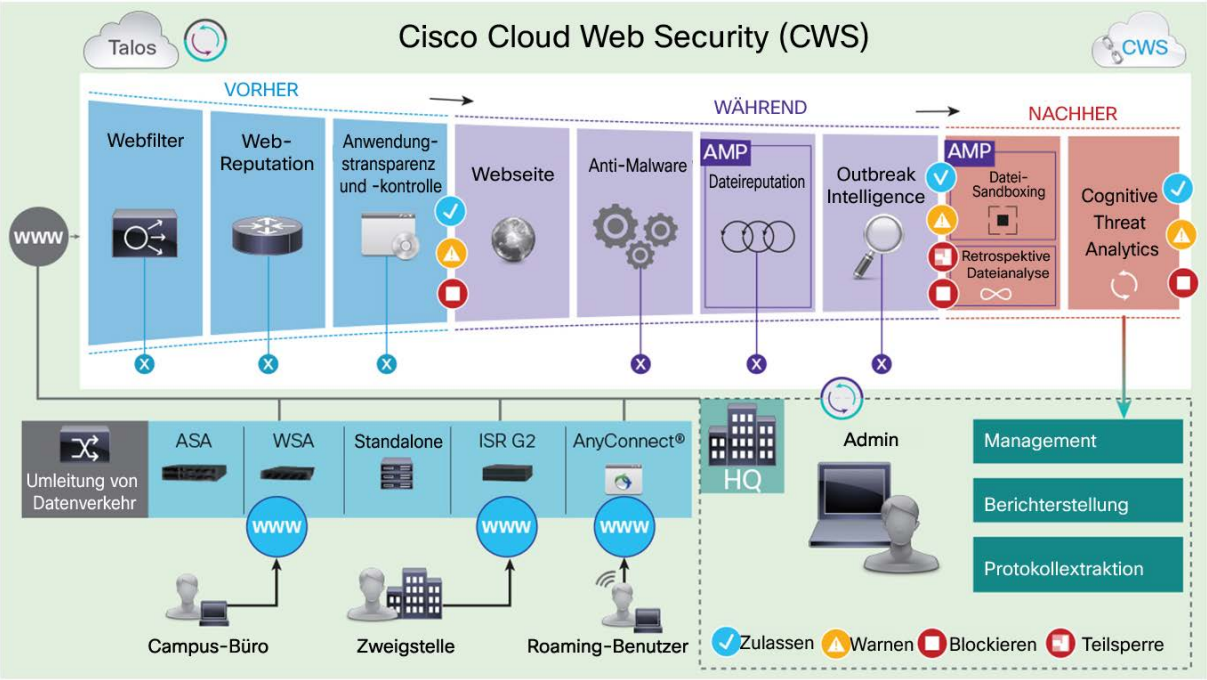
1. Im WAN-Router werden Regeln festgelegt, die die Übertragung des Internetdatenverkehrs an die neue Firewall betreffen.
2. Die mit dem Ladennetzwerk verbundenen Geräte verwenden die Firewall als Standard-Gateway, sodass das Netzwerk nicht mehr kontrolliert oder überwacht wird. Wird der Datenverkehr nicht korrekt an den Prüfpunkt weitergeleitet, kann bei einer Wi-Fi-Verbindung nicht sichergestellt werden, dass keine Unternehmensdaten in das Internet gelangen. Darüber hinaus gibt es keine Garantie, dass die Richtlinien für akzeptable Nutzung durchgängig befolgt werden.

Im Allgemeinen schafft das Flickwerk der Punktprodukte eine Situation, in der das eigentliche Risiko für Unternehmen nicht ohne Weiteres kontrolliert, erkannt oder verwaltet werden kann.

Bedrohungen im Einzelhandel sorgen schon seit Jahren für Schlagzeilen. Denken wir beispielsweise an den großen Angriff im Jahr 2006, bei dem bis zu eine Million Kreditkartendaten gestohlen wurden. Hacker nutzten die schwache Kontrolle in den Läden aus, um Zugriff auf Kreditkarten und andere Kundendaten zu erlangen. Sobald sie eine Sicherheitslücke finden, bewegen sie sich lateral durch die Unternehmensnetzwerke und gefährden auch private Daten.

Da Hacker Angriffstaktiken austauschen und ihre Angriffe automatisieren können, suchen sie sich das schwächste Glied in der Kette als Angriffspunkt für große Unternehmen aus. Das sind häufig die Einzelhandelsgeschäfte mit den unterdurchschnittlichen Kontrollen.

Abbildung 2. Funktionsweise von Cisco Cloud Web Security

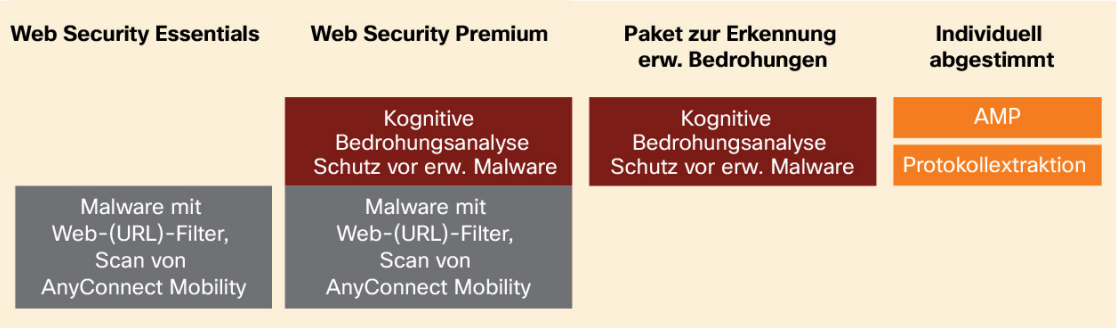


Flexibler Schutz und Kontrolle

Cisco hat ein Portfolio an Produkten und Funktionen für die Sicherheits- und Netzwerkanforderungen von IT-Umgebungen im Einzelhandel entwickelt. Diese Lösungen reichen von drahtlosen Zugangspunkten, über Routing und Switching bis hin zu Cloud-basierten erweiterten Sicherheitsservices.

Abbildung 3 gibt einen Überblick über die Kaufoptionen für Cisco CWS.

Abbildung 3. Kaufoptionen für Cisco CWS



Die marktführenden Produkte Cisco Web Security Appliance (WSA) und Cisco Cloud Web Security (CWS) bieten flexible Bereitstellungsmodelle und gewährleisten die Sicherheit Ihrer Inhalte sowohl am Standort als auch in der Cloud. Mit Cisco WSA für den Netzwerkschutz der Zentrale und Cisco CWS für Zweigstellen erfüllen Sie alle IT-Sicherheitsanforderungen. Gleichzeitig entfällt die Notwendigkeit, zur Verbesserung des Schutzes neue Hardware für alle Zweigstellen erwerben zu müssen. Durch die direkte Integration mit den ladeneigenen Technologien, wie z. B. den Cisco Adaptive Security Appliance-Firewalls (ASA),

den Cisco Integrated Services Routers (ISRs) und den Cisco AnyConnect®-Clients, ist es mit Cisco CWS möglich, die vorhandenen Investitionen und operativen Supportprozesse mit verbesserten Schutzfunktionen und effizienterer Betriebsunterstützung zu ergänzen.

Cisco verlagert den Schutz von Internetverbindungen nach unten auf die Ladenebene. Dafür ist keine zusätzliche Hardware erforderlich. Der Datenverkehr muss nur dann zurück transportiert werden, wenn die Richtlinie es so vorgibt. Der risikoarme Datenverkehr geht direkt in das Internet. Der restliche Datenverkehr wird an den zentralen Standort geleitet und dort geprüft.

Als Schutz vor bekannten und neuen Bedrohungen verwendet Cisco CWS eine Vielzahl von Techniken zur Suche nach Angriffen, darunter traditionelle Malware-Signaturen sowie Filter nach Datei- und Site-Reputation und Outbreak-Filter. Zudem kann Cisco CWS mit Cisco Collective Security Intelligence (CSI) integriert werden, der branchenführenden intelligenten Funktion zur Erkennung und Abwehr von Bedrohungen, zu der auch die Talos-Sicherheitsintelligenz und -Forschungsgruppe gehört. Dank Cisco CSI und Talos können Kunden von den anderen zehntausend Kunden profitieren, die Cisco Technologie verwenden.

Cisco CWS liefert detaillierte Berichte, unter anderem mit traditionellen Informationssicherheitsdaten und fundierten Analysen der Bandbreitennutzung und -auslastung. In Umgebungen mit eingeschränkter Bandbreite ist Transparenz ein wichtiges Tool für Effizienz. Eine weitere Berichtsfunktion liefert Daten zum Browsing-Verhalten der Gäste im Wi-Fi. Produktvergleiche und Preisprüfungen bei Online-Einzelhändlern werden sichtbar gemacht und verhindert. Auch das Aufrufen anstößiger Inhalte wird nicht zugelassen. Die Berichtsfunktionen von Cisco CWS sind daher nicht nur für die IT-Sicherheitsteams, sondern auch für das gesamte Einzelhandelsunternehmen wertvoll.

Fast noch wichtiger: Als Cloud-Lösung ermöglicht Cisco CWS (Abbildung 2) eine einfache Skalierung und Optimierung der Bandbreite von Unternehmen. Das bedeutet direkte, quantifizierbare Kosteneinsparungen und deutliche Verbesserungen bei der Effektivität von ladenbezogenen Threat Management-Funktionen. Die Einsparungen werden durch Auslagerung der gesamten Datenverkehrsverwaltung und -kontrolle von der lokalen Hardware auf Cloud-basierte Systeme erzielt. Mit dem SaaS-Modell (Software-as-a-Service) zur Bereitstellung von richtlinienbasierten Datenverkehrsentscheidungen reduziert Cisco CWS die Belastung der Netzwerk-Hardware im Laden erheblich.

Vorteile von Cisco CWS für Einzelhandelsunternehmen

Beispiele zeigen, wie Cisco CWS Einzelhandelsunternehmen vor den heutigen Bedrohungen schützen kann: Ein IT-Sicherheitsmanager wurde beauftragt, eine Kette mit 1.500 Läden zu schützen. In den einzelnen Läden wird Technologie implementiert, die den Kunden Internetzugang und eine Reihe von zusätzlichen Services ermöglicht. Der Sicherheitsmanager ist sich bewusst, dass seit Kurzem eine neue Flut komplexer Malware-Angriffe ladeneigene Systeme (auch POS-Geräte) gefährdet. Er möchte diese Angriffe rasch erkennen und effektiv beseitigen. Eine weitere Herausforderung ist die eingeschränkte Bandbreite in vielen Läden. Zudem muss die Lösung die Netzwerkverbindungen zu den jeweiligen Läden optimieren.

Der Sicherheitsmanager installiert Cisco ISR-Edge-Router in den Läden. Diese Geräte unterstützen Cisco Intelligent WAN-Funktionen (IWAN), mit denen die Bandbreite der einzelnen Läden geschützt und gleichzeitig optimiert wird. IWAN vereinfacht die Verwaltung der Bandbreite durch kostengünstigere Internetverbindungen im Gegensatz zu teureren privaten Netzwerkanbindungen. Das Produkt bietet darüber hinaus einen unkomplizierten Migrationspfad, sodass das Unternehmen in seinem eigenen Tempo von den privaten Netzwerkanbindungen migrieren kann. Um sicherzugehen, dass die mobilen Geräte mit dem richtigen Netzwerk in den einzelnen Läden verbunden sind, schützt die Cisco Identity Services Engine (ISE) die Ladensysteme und legt fest, welche Benutzer und Geräte auf welche Teile der Netzwerke zugreifen dürfen.

Für den Schutz des Internetdatenverkehrs verwendet das Unternehmen Cisco CWS Premium für direkten Internetzugang, das über die Cisco ISR-Edge-Router ohne zusätzliche Hardware bereitgestellt werden kann. Cisco CWS Premium schützt alle Benutzer mithilfe der erweiterten Abwehrfunktionen von Cisco Advanced Malware Protection (AMP) und Cognitive Threat Analytics (CTA). CTA ist ein Analysesystem, das das Netzwerkverhalten nahezu in Echtzeit analysiert und mithilfe von maschinellen Lernverfahren und erweiterten Statistiken ungewöhnliche Aktivitäten im Netzwerk und mögliche Angriffe identifizieren kann. Mit einer Kombination aus Dateireputation, Datei-Sandboxing und retrospektiver Dateianalyse kann AMP Bedrohungen erkennen und beseitigen, die bereits im Netzwerk vorhanden sind.

Mit diesen Sicherheitslösungen von Cisco kann die Ladenkette mit 1.500 Filialen nun Bandbreitennutzung, Benutzerzugriff, Gefahrenabwehr und die Sicherheit von Inhalten verwalten. Dies ist nur eine mögliche Kombination der Cisco Security-Produkte. In diesem Fall kann der IT-Sicherheitsmanager die Netzwerk- und Sicherheitsziele für das verteilte Einzelhandelsnetzwerk erfüllen.

Vorteile von Cisco CWS

Unternehmen können mithilfe der integrierten Lösung von Cisco zum Schutz ihrer Netzwerke eine gemeinsame Richtlinie durchsetzen, erweiterte Angriffe erkennen und die Nutzung von Bandbreite im WAN optimieren. Das mit den Cisco ISR-Edge-Routern integrierte Cisco CWS Premium ermöglicht auch die Verfolgung von Botnets. Dadurch wird sichergestellt, dass POS-Geräte nicht gefährdet werden und Daten sicher an die Zentralen übertragen werden können. Durch Bündeln von Lösungen können Unternehmen weitere Kosten sparen.

Da alle Funktionen für die Zusammenarbeit entwickelt wurden, müssen sich Unternehmen nicht mit der Integration der einzelnen Elemente der Lösung befassen. IT-Mitarbeiter können nach Schätzungen von Cisco aufgrund des geringeren Aufwands für Konfiguration und Implementierung bis zu 40 Prozent an Zeit sparen. Unternehmen profitieren darüber hinaus weltweit von einem durchgängig hohen Sicherheitsniveau im Netzwerk. Anstatt sich um die Abwehr von Angriffen kümmern zu müssen, können sie sich auf das Kerngeschäft konzentrieren.

Zusammenfassung

Mit Cloud-fähigen Tools wie Cisco CWS können Einzelhandelsgeschäfte betriebliche Belastungen durch Überwachung, Verwaltung und Wartung der Netzwerke deutlich reduzieren. CWS lässt sich problemlos zusammen mit Cisco ASA und Cisco ISR nutzen und senkt den Bedarf an einer lokalen Durchsetzung von Sicherheitsrichtlinien. Zudem reduziert es die Bandbreitenanforderungen in den einzelnen Läden. Cisco CWS, laut Gartner das branchenführende Produkt im Sicherheitsmarkt, ergänzt ladeneigene Netzwerke auf intelligente Weise mit effektiven Sicherheitsfunktionen, ohne die operative Komplexität zu erhöhen.

Weitere Informationen

Weitere Informationen finden Sie unter http://cisco.com/go/cws.

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 C11-733817-00 02/15