Wi-Fi Cloud und Sicherheit

Einführung

Bei mittelständischen und dezentral aufgestellten Unternehmen sowie im öffentlichen Sektor ist es inzwischen gang und gäbe, die interne Datenverarbeitung in die Cloud auszulagern – entweder über die eigene IT-Abteilung oder Service Provider. Die Sicherheitsabteilungen sehen dies jedoch mit gewisser Skepsis. Denn damit werden immerhin die Datensicherheitskontrollen, die bislang intern gehandhabt wurden, in fremde Hände gegeben. Diese Bedenken gelten auch für WLAN-Angebote, die über die Cloud verwaltet werden. Deshalb hat WatchGuard umfangreiche Maßnahmen bei der Erstellung eines stabilen Sicherheitsprogramms in Bezug auf die Cloud ergriffen – ein weiteres, starkes Argument für die WLAN-Produkte und Sicherheitslösungen von WatchGuard. Das Sicherheitsprogramm der WatchGuard Wi-Fi Cloud basiert auf mehreren Säulen, die im Folgenden genauer beschrieben werden.

Lokale Datenebene, cloudbasierte Verwaltungsebene

In der Architektur der WatchGuard Wi-Fi Cloud befindet sich die drahtlose Datenebene (A) lokal im Netzwerk. Anders die Verwaltungsebene: Diese befindet sich in der Cloud (B). Der Funk-Datenverkehr über WatchGuard AP (Access Points) fließt nicht in die Wi-Fi Cloud, sondern wird entsprechend der Einstellungen netzwerkintern geroutet. Das vereinfacht auch die lokale Durchsetzung von Datensicherheitskontrollen, beispielsweise in Hinblick auf Content Filtering und forensisches Logging. Die Authentifizierungs- und Autorisierungsfunktionen der Datenebene greifen ebenfalls netzwerkintern. Die Verwaltungskonsole zur Konfiguration und Überwachung des drahtlosen Netzwerks wird von der Wi-Fi Cloud zur Verfügung gestellt. Diese Konsole übernimmt zudem die Sicherheitsüberwachung der WLAN-Umgebung im Unternehmen, um dortige unerwünschte Aktivitäten zu ermitteln und einzudämmen.

Die Steuerungsebene befindet sich lokal im Netzwerk zwischen den AP (C). Auf dieser Ebene werden Nachrichten zwischen den AP zwecks Übergabe, Lastausgleich, Funkoptimierung usw. ausgetauscht. Nach der anfänglichen Konfiguration ist hierfür kein konstanter Input von der Verwaltungsebene erforderlich.

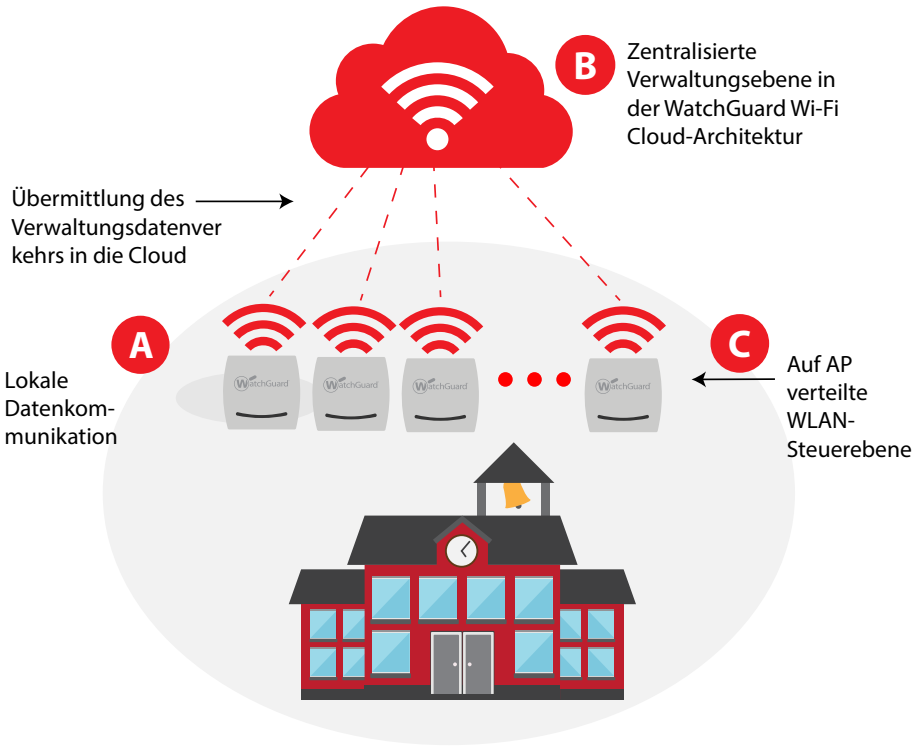
Datenerfassung per cloudbasierter Verwaltungsebene

Die Cloud-Verwaltungsebene erfasst und speichert MAC- und IP-Adressen von Geräten im Netzwerk, die von den internen AP ermittelt werden. Darüber hinaus werden Metadaten zu Geräten erfasst, darunter Infos zur Layer 2-Drahtlosaktivität (Tests, Verknüpfungen), Betriebssystem, Hostname, Anwendungsnutzung, Standorte in Bezug auf die Distanz zu AP sowie 802.1x-Anmeldekennungen, die zur Verbindungsherstellung mit dem WLAN per Funk übertragen werden.

Wichtig hierbei: Kennwörter für die 802.1x-Authentifizierung werden nicht in der Wi-Fi Cloud erfasst oder gespeichert. Denn diese werden von lokalen RADIUS-Servern geprüft. 802.1x-Benutzerkennwörter sind für die AP ebenso nicht sichtbar, da sie ausschließlich zwischen Client- und Authentifizierungsserver ausgetauscht werden.

Bei WLAN-Gastnetzen erfasst die Cloud-Verwaltungsebene darüber hinaus die Kennung von Gastbenutzern während der WLAN-Authentifizierung. Dies erleichtert Sicherheitsprüfungen für die Gastbesucher. Unternehmen können bei Bedarf auch ein Gäste-WLAN mit anonymem Zugriff einrichten.

Architektur der WatchGuard Wi-Fi Cloud



AP-zu-Cloud-Kommunikation

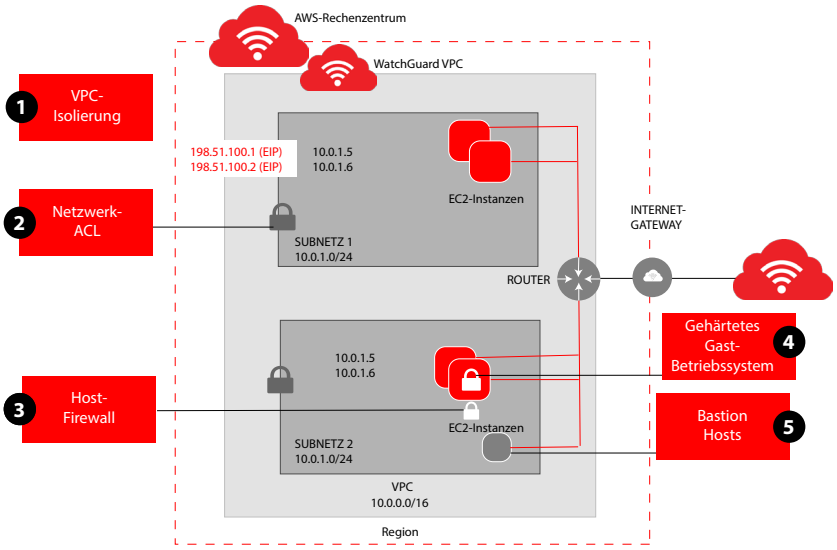
Für den umfassenden Schutz bei der AP-zu-Cloud-Kommunikation greifen drei Sicherheitsmaßnahmen.

1. **Gegenseitige Authentifizierung**: Erfolgt jedes Mal, wenn ein AP eine Verbindung zur Wi-Fi Cloud herstellt. Hierbei handelt es sich immer um eine von innen nach außen gerichtete Anfrage: Der AP und die Cloud authentifizieren sich gegenseitig. Dadurch wird die Identität beider Parteien geprüft.
2. **Nachrichtenbezogene Authentifizierung**: Hierbei wird ein HMAC SHA-1-Authentifizierungscode für jede Nachricht verwendet, die von einem AP an die Wi-Fi Cloud gesendet wird. Die Authentizität der Kommunikation wird im Zuge dessen anhand der Bestätigung, dass die Nachricht von der richtigen Einheit stammt und bei der Übertragung nicht verändert wird, sichergestellt.
3. **AES-Verschlüsselung**: Wird durchgängig in der AP-zu-Cloud-Kommunikation verwendet. Dadurch wird sichergestellt, dass die Nachrichten vertraulich bleiben und nicht abgefangen werden können.

Wi-Fi Cloud-Umgebung im AWS-Rechenzentrum

Die WatchGuard Wi-Fi Cloud wird als VPC (Virtual Private Cloud) im Rechenzentrum von AWS (Amazon Web Services) bereitgestellt. In der VPC-Architektur ist die Wi-Fi Cloud-Umgebung logisch von Umgebungen anderer Einheiten isoliert, die ebenfalls im AWS-Rechenzentrum gehostet werden. Für die physische und umgebungsbezogene Absicherung der VPC sorgt AWS (1). Innerhalb der WatchGuard VPC befinden sich mehrere Subnetze, die WatchGuard-Anwendungsserver hosten. Für jedes Subnetz gibt es eine Netzwerk-ACL (Access Control List), die nur bestimmte Protokolle innerhalb und außerhalb des Subnetzes zulässt (2). Die virtuellen Maschinen der Anwendungsserver, die in Form von EC2-Instanzen (Elastic Compute Cloud) bereitgestellt werden, sind mit diesen Subnetzen verbunden. Jede von WatchGuard bereitstellte EC2-Instanz hat eine Host-basierte Firewall, die so konfiguriert ist, dass nur Protokolle zugelassen werden, die für die entsprechenden Anwendungen innerhalb und außerhalb des Servers erforderlich sind (3).

WatchGuard VPC im Amazon-Rechenzentrum



Die WatchGuard-Anwendungen, die auf diesen EC2-VM ausgeführt werden, sind wiederum Port-gebunden. So wird sichergestellt, dass keine unbefugten Services und Ports darauf zugreifen können (4). Die Wi-Fi Cloud wird in AWS-Rechenzentren an weltweit verteilten Standorten bereitgestellt, wie beispielsweise innerhalb der EU.

Schwachstellenscans

WatchGuard führt auf den Cloud-gehosteten Anwendungen regelmäßig drei unterschiedliche Schwachstellenscans durch.

1. **Port-Scans**: Wenn Recheninstanzen in verschiedenen Bereichen des Rechenzentrums gestartet werden, muss unbedingt sichergestellt werden, dass offene Ports entsprechend beschränkt werden und allein der Zugriff auf die Anwendungsfunktionalität zugelassen ist. Dadurch wird die Angriffsoberfläche drastisch verkleinert. WatchGuard führt für die Cloud-Umgebung regelmäßig Port-Scans durch.
2. **WAS-Scans (Web Application Security)**: WAS-Scans konzentrieren sich auf Schwachstellen auf der Webanwendungsebene. Da der Zugriff auf die Cloud-Anwendung per HTTPS (Port 443) und somit über das allgemeine Internet erfolgt, sollen WAS-Scans sicherstellen, dass sich unbefugten Benutzer beim Versuch, auf die Anwendung zuzugreifen, keine Schwachstellen bieten. Außerdem soll vermieden werden, dass ein autorisierter (authentifizierter) Benutzer einschlägige Sicherheitskontrollen umgeht, beispielsweise hinsichtlich Injection-Angriff, Privilegstufen, Multi-Tenancy usw. Um die WAS-Scans bei WatchGuard kümmern sich die WhiteHat Security-Services – automatisiert und rund um die Uhr. Zweimal pro Jahr führen WhiteHat Security-Experten zusätzlich manuelle Tiefenscans durch.
3. **Softwarekomponenten-Scans**: Bei diesen Scans werden Softwaremodule innerhalb der Anwendung auf fehlende Sicherheitspatches, veraltete Versionen und Fehlkonfigurationen überprüft. Die Softwarekomponenten in sämtlichen Cloud-Anwendungen werden von WatchGuard mindestens einmal pro Quartal mithilfe des Nessus Enterprise-Tools gescannt.

Datenverschlüsselung

WatchGuard verschlüsselt Daten bei der Übertragung mit AES. Dies umfasst die Management-GUI-Kommunikation (HTTPS) zwischen dem WatchGuard AP und der Wi-Fi Cloud sowie alle Interaktionen zwischen verschiedenen WatchGuard-Servern und Anwendungen in der Cloud (HTTPS). Die AES-Verschlüsselung wird auch auf gespeicherte Daten angewendet. Datenbanksicherungen von WatchGuard-Anwendungen in der Cloud werden in AWS S3 und Glacier gespeichert, ebenfalls mit AES-Verschlüsselung. Die Live-Datenbank der Wi-Fi Cloud-Verwaltung, die als Hauptanwendung die drahtlose Verwaltungskonsole bereitstellt, befindet sich in AWS EBS (Elastic Block Storage) und ist ebenfalls AES-verschlüsselt.

Zugriffssteuerung

Zur Bereitstellung, Wartung und Lösung von Supportproblemen benötigen WatchGuard-Mitarbeiter Zugriff auf die Cloud-Anwendungen. Die von WatchGuard implementierten Steuerungsmechanismen beschränken jedoch den Zugriff auf Kundenkonten auf ein Mindestmaß. Darüber hinausgehende intervenierende Aktionen müssen zuerst vom Kunden genehmigt werden und sind zeitlich begrenzt. Bevor Mitarbeiter mit solchen Sonderrechten ausgestattet werden, wird ihr Hintergrund genau durchleuchtet. Der Zugriff auf einen EC2-Server zu Wartungszwecken erfolgt über Bastion Hosts. Für die Anmeldung an den Bastion Hosts ist SSH erforderlich – zudem ist dies nur spezifischen IP-Adressen gestattet. Bastion Hosts verwenden starke Zugriffssteuerungs- und Prüffunktionen, um unbefugte Wartungszugriffe zu verhindern (5).

Compliance-Zertifizierungen

WatchGuard verfügt über mehrere sicherheitsrelevante Compliance-Zertifizierungen. Dies beinhaltet auch die externe Prüfung und Validierung der Sicherheitskontrollen der WatchGuard Wi-Fi Cloud im Hinblick auf Vertraulichkeit, Integrität und Verfügbarkeit.

WatchGuard ist zertifiziert gemäß ISO 27001:2013 für das Information Security Management System (ISMS). Die ISO-Zertifizierung von WatchGuard deckt sämtliche Bereiche ab.

Derzeit durchläuft WatchGuard für die Wi-Fi Cloud die Prüfung zur SSAE 16 SOC 2-Zertifizierung. Die AWS-Rechenzentren, in denen WatchGuard-Anwendungen gehostet werden, sind selbstverständlich bereits gemäß SSAE 16 SOC 2 zertifiziert. Eine bloße SSAE-Zertifizierung der Rechenzentren reicht jedoch nicht aus, um die lückenlose Sicherheit für die Kunden in der Cloud zu gewährleisten. Der Grund: Diverse Cloud-Funktionen werden von Anwendungsprovidern wie WatchGuard übernommen, die nicht der SSAE-Zertifizierung des Rechenzentrums unterliegen. Der SSAE-Kontrollrahmen von WatchGuard deckt diese Aspekte ab.

Fazit

Durch den Wechsel von der herkömmlichen Controller-basierten hin zur modernen cloudbasierten Verwaltung ergeben sich unzählige Vorteile – angefangen bei massiv gesenkten Gesamtbetriebskosten bis hin zu höherer Skalierbarkeit. Mit der WatchGuard Wi-Fi Cloud kommen Unternehmen in den Genuss sämtlicher Funktionen einer cloudbasierten Verwaltungslösung – ohne Abstriche in puncto Sicherheit.

Über WatchGuard

WatchGuard Technologies gehört zu den führenden Anbietern im Bereich Netzwerksicherheit. Mehr als 75.000 Unternehmen weltweit vertrauen auf die ausgeklügelten Schutzmechanismen auf Enterprise-Niveau, wobei dank der einfachen Handhabung insbesondere kleine bis mittlere sowie dezentral aufgestellte Unternehmen vom Einsatz profitieren. Neben der Zentrale in Seattle im US-Bundesstaat Washington verfügt WatchGuard über Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter WatchGuard.com.

Wenn Sie mehr über WatchGuard, unsere Werbeaktionen und Updates erfahren möchten, folgen Sie uns auf Twitter @WatchGuard, auf Facebook oder LinkedIn. Lesen Sie auch unseren InfoSec-Blog Secplicity. Darin wird einfach und nachvollziehbar beschrieben, wie Sie den neuesten Bedrohungen am besten begegnen. Hier geht's zum Blog: www.secplicity.org.

Deutschland, Österreich, Schweiz: +49 700 92229333 INTERNATIONALER VERTRIEB: +1.206.613.0895 www.watchguard.de

Teilenr. WGCE66942_092616