12 | 17 Sonderdruck für WatchGuard

IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

WatchGuard Access Point AP120 und Wi-Fi-Cloud

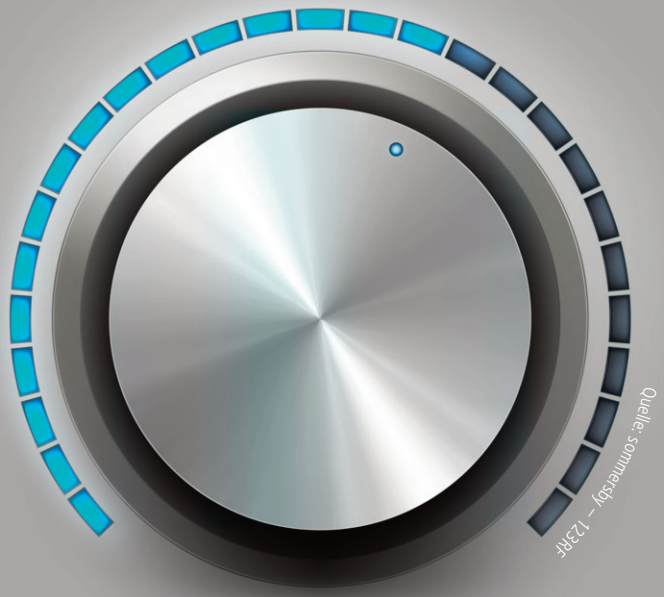
www.it-administrator.de

WatchGuard Access Point AP120 und Wi-Fi-Cloud

AP-Regler in der Wolke

von Frank-Michael Schlede und Thomas Bär

Kaum eine Firma – ganz gleich ob Mittelstand oder Enterprise – kommt heute noch ohne ein gut funktionierendes WLAN aus. Die Firma WatchGuard kombiniert ihre Access Points mit einer umfassenden Verwaltung via Cloud – wir haben uns die Lösung einmal genauer betrachtet. Dabei hat uns vor allem die Template-basierte Verwaltung der Access Points sehr gut gefallen.



Vom Standpunkt der Endanwender aus ist ein WLAN eine nahezu ideale Lösung: Sie können sich problemlos mit allen mobilen Geräten und nicht nur mit dem PC mit dem Internet verbinden, es müssen keine Kabel verlegt werden und spätestens seit immer mehr Access Points (AP) mit dem Standard 802.11ac ausgerüstet sind, klappt es meist auch mit der Geschwindigkeit. Wie in vielen Fällen sieht es für die Profis in der IT-Abteilung zumeist etwas anders aus. Sie müssen nicht nur sicherstellen, dass genügend WLAN-APs vorhanden sind, damit die Nutzer überall ins Netz kommen, sondern sich auch um die Konfiguration und Verwaltung der Netzwerkkomponenten kümmern.

Eine ganze Reihe von Herstellern solcher Hardware bietet deshalb grafische Oberflächen und Werkzeuge an, die Konfiguration und Überwachung von WLAN-Installationen einfacher machen sollen. Dabei kommen sowohl lokale Installationen der Verwaltungssoftware als auch Lösungen aus der Cloud zum Einsatz. Die Firma WatchGuard bietet Cloud-fähige Access Points im Zusammenspiel mit einem Abonnement der sogenannten WatchGuard Wi-Fi-Cloud an, die eine Verwaltung des WLANs aus der Cloud über ein Browser-Interface erlaubt.

Funk über MIMO, Strom über PoE

Für unseren Test haben wir uns mit dem Access Point AP120 das kleinste Modell aus der Angebotspalette von WatchGuard ausgesucht. Der Hersteller positioniert es als Gerät, das dann zum Einsatz kommen kann, wenn nur begrenzte Räumlichkeiten oder eine geringe Anzahl von Geräten zu verwalten sind. Also ein AP, der gerade für kleine und mittelständische Betriebe gut geeignet scheint. Es handelt sich hierbei um einen Access Point gemäß 2x2 MIMO 802.11ac für den Innenbereich. MIMO steht für "Multiple Input Multiple Output" und bezeichnet ein Übertragungsverfahren, bei dem mehrere Antennen zum Einsatz kommen. Das Gerät verfügt über zwei Funksysteme, die parallel genutzt werden können, und funkt auf den Bändern 2,4 und 5 GHz. Unterstützung finden dabei die Standards 802.11 a/b/g/n und ac.

Wir bekamen das recht schmucklose Gerät nur mit einem PoE-Netzteil (Power over Ethernet) und einem Netzwerkkabel geliefert. Genauso spartanisch geht es am Plastikgehäuse selber weiter: Hier findet der Nutzer neben dem GBit-Ethernet-Anschluss, der das Gerät via PoE mit dem nötigen Strom versorgen kann, nur noch einen Anschluss für ein separat zu erwerbendes 12-V-Netzteil, falls eine Stromversorgung mittels PoE nicht funktioniert. Auf der Rückseite ist der AP zusätzlich mit

WatchGuard AP120 und Wi-Fi-Cloud

Produkt
Access Point samt Lösung zur Cloud-basierten Konfiguration und Verwaltung.

Hersteller
WatchGuard
www.watchguard.com/de/

Preis
WatchGuard AP120 und ein Jahr Basic Wi-Fi: 386 Euro inklusive AP mit Fireware-Wireless-Controller und Standard-Support.

WatchGuard AP120 und ein Jahr Secure Wi-Fi: 499 Euro inklusive AP mit Wi-Fi-Cloud-Lizenz, Standard-Support und WIPS.

WatchGuard AP120 und ein Jahr Total Wi-Fi: 576 Euro inklusive AP mit Wi-Fi-Cloud-Lizenz, Standard-Support, WIPS, Engage Captive Portals, Analyze Location Analytics und der Go Mobile Web App.

Systemvoraussetzungen
Internet-Zugang und gängiger Browser, empfohlen sind Mozilla Firefox und Google Chrome. Ethernet mit PoE-Unterstützung oder entsprechendes externes Netzteil.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

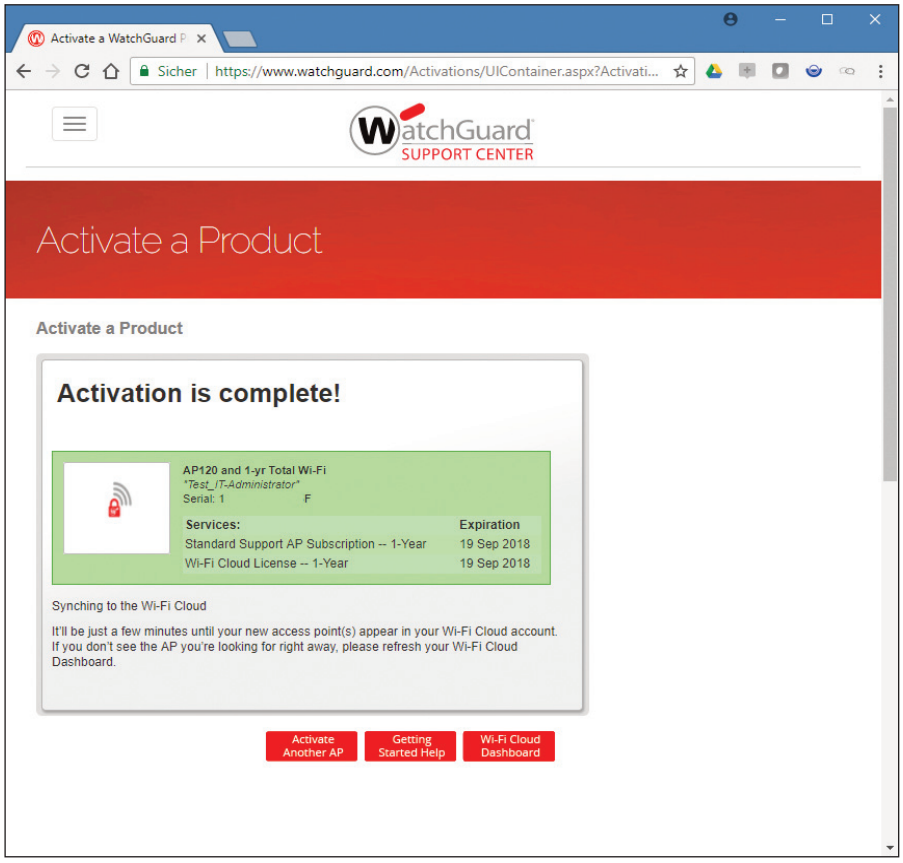


Bild 1: Ohne Anmeldung in der Cloud funktioniert es nicht: Hat der Administrator die Lizenznummer richtig entziffert und bekommt der Access Point vom lokalen DHCP-Server eine gültige IP-Adresse, taucht das Gerät bald im Konto des Nutzers auf.

den benötigten Bohrungen und Vorrichtungen für eine Wandmontage ausgestattet. Vier LEDs auf der Oberseite signalisieren zudem, ob er eingeschaltet ist, eine Netzwerkverbindung besitzt und das 2,4- beziehungsweise 5,0 GHz-Band aktiv ist.

Wir haben das Gerät mit dem PoE-Netzteil problemlos betreiben können und es über einen Switch mit unserem Testnetzwerk und dem darin konfigurierten Router verbunden. Der AP120 benötigt für die Erstinstallation einen DHCP-Server im Netzwerk und ist standardmäßig so konfiguriert, dass er sich dann davon automatisch eine Netzwerkadresse holt. Der Administrator kann den Access Point später natürlich auch so konfigurieren, dass er feste IP-Adresse verwendet oder selbst als DHCP-Server im lokalen WLAN fungiert.

Die Cloud spricht nur englisch

Für die Inbetriebnahme des Access Points mittels der WiFi-Cloud muss der Nutzer zunächst auf der WatchGuard-Webseite ein Konto anlegen, das neben den notwendigen Informationen wie Name und Passwort leider weitere Informationen wie den Geschäftsbereich der eigenen Firma zwingend voraussetzt – Daten, die wohl eher dem Marketing als der Verwaltung des Gerätes dienen. Der Nutzer findet dann im Menü unter "My WatchGuard" die Möglichkeit, seinen Access Point mittels der Wifi-Cloud zu verwalten.

Auch wenn er sich auf der deutschen Webseite des Herstellers angemeldet hat, erfolgt ab nun jede weitere Kommunikation in englischer Sprache. Darauf angesprochen betonte der Hersteller, dass Administratoren in der Regel keine Probleme mit Oberflächen und Hilfetexten in englischer Sprache hätten. Das mag für Administratoren in großen Unternehmen mit dedizierter IT-Abteilung und -Mannschaft durchaus zutreffen. Aber gerade das hier getestete Modell ist nach unserer Einschätzung sehr gut für den Einsatz in kleinen und mittelständischen Betrieben geeignet – einfache Installation, schnelle Einrichtung sowie standardmäßig hohe Sicherheit sprechen für sich. Aber ob sich diese Zielgruppe wirklich mit der komplett englischen Nutzerführung anfreunden kann, bezweifeln wir doch etwas.

Taucht der Eintrag "Manage Wi-Fi-Cloud" nicht auf, so kann das daran liegen, dass das benötigte Cloud-Abonnement nicht zusammen mit dem Gerät erworben wurde. Uns stand mit "Total Wi-Fi" das umfangreichste einjährige Abonnement zur Verfügung, das neben der grundsätzlichen Wi-Fi-Cloud-Lizenz den Standard-Support und Sicherheitsfeatures wie WIPS (Wireless Intrusion Prevention System) sowie die Go Mobile Web App beinhaltet.

Nach der Kontoerstellung gilt es, das Gerät mittels der Seriennummer zu aktivieren. Diese findet sich auf einem Aufkleber an der Unterseite und ist in einer Drei-Punkt-Schrift aufgedruckt, die selbst bei Einsatz einer Lesebrille nur unter Zuhilfenahme einer Lupe fehlerfrei auszulesen ist. WatchGuard ist leider nicht der einzige Hersteller, der diese Unart pflegt. Bleibt die Frage, warum der ausreichende Platz auf der Unterseite nicht für eine größere und damit kundenfreundlichere Schriftgröße genutzt werden kann.

Mit dem Dashboard alle Einstellungen im Griff

Nach dem Überwinden dieser kleinen Hürde dauerte es nur kurze Zeit, bis das Dashboard mit dem sogenannten Launchpad in unserem Konto auftauchte und zur Verwaltung bereitstand. Hier bieten sich dem Nutzer die zwei Kategorien "Services" und "Apps". WatchGuard empfiehlt für den Start, die als "Go" bezeichnete App einzusetzen. Sie bietet eine einfache Oberfläche, die dem Nutzer mit wenigen Fragen dabei hilft, ein oder mehrere WLAN-Netz(e) einzurichten.

Insgesamt ist es möglich, bis zu acht WLAN-Netzwerke mittels Go zu konfigurieren – nur vier davon können jedoch gleichzeitig aktiv sein, denn das Gerät besitzt intern vier Antennen. Der Nutzer kann bei dieser Schnelleinrichtung auch festlegen, ob es sich bei dem Netzwerk um ein privates oder ein Gastnetzwerk handelt. So gelang dann sehr schnell die Einrichtung des WLANs und diverse

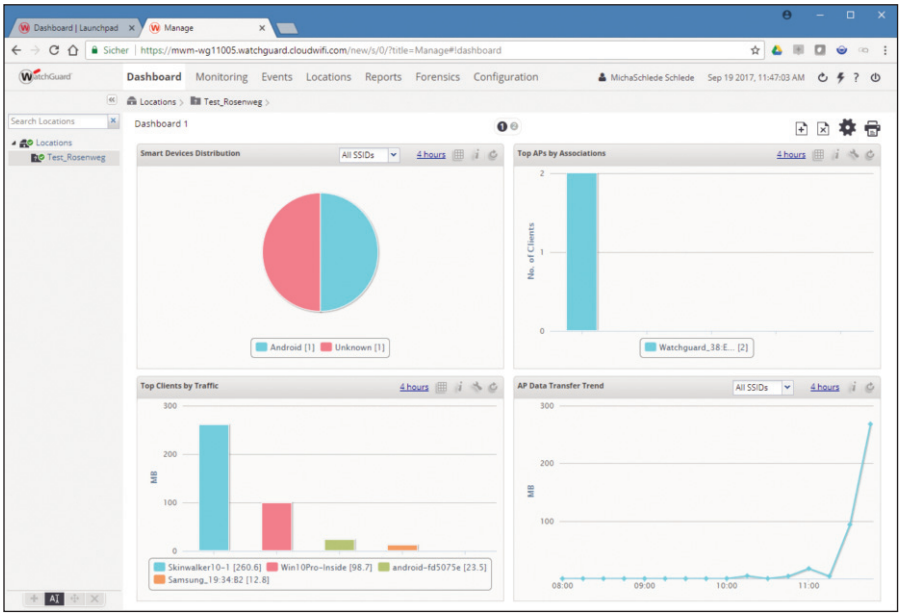


Bild 2: Mittels des Dashboards, das individuell konfigurierbar ist, kann sich der Admin schnell einen Überblick über das WLAN und die aktiven Clients verschaffen.

Clients vom Android-Smartphone über ein Tablet und ein Windows-10-Notebook bis hin zum Kindle konnten sich problemlos mit dem WLAN verbinden.

Der nächste Schritt führte uns dann zur eigentlichen Konfiguration: Unter dem Eintrag "WatchGuard Manage" findet der Nutzer alle Möglichkeiten, um seinen Access Point zu konfigurieren. Unter dem Reiter "Monitoring" tauchen anschließend die verwalteten Geräte in der übersichtlichen Oberfläche auf. Auf der linken Seite des Dashboards findet der Nutzer den sogenannten "Location Tree". An dieser Stelle können die Anwender dann ihre Access Points in einer hierarchischen Struktur geordnet darstellen. Nach dem Start wurde unser erstes Gerät automatisch in den Standardordner mit dem Namen "Unknown" eingereiht. Diesen Namen kann ein Administrator händisch in die entsprechende Bezeichnung ändern.

Einfache Verwaltung durch Templates

Der Hersteller weist in diesem Zusammenhang explizit darauf hin, dass die Locations hier die SSID-Profile und Geräteschablonen (Device Templates), die die Sicherheit der AP-Geräte definieren, von der "Eltern-Location" erben. Deshalb ist es wichtig, dass der Administrator bei der Konfiguration der SSID-Profile die richtige Top-Level-Location wählt – das neue Profil erbt dann alle Einstellungen. Dieses Anlegen neuer SSID-Profile kann der Anwender unter dem Reiter "Configuration / Device Configuration" vornehmen. Hier stehen ihm neben den üblichen Einstellungen wie SSID-Name und natürlich der Name des Profils auch die Sicherheitseinstellungen und eine ganze Reihe weiterer Einstellmöglichkeiten zur Verfügung.

Hat der Nutzer ein SSID-Profil neu angelegt, muss er es einer Geräteschablone, eben dem Device Template zuweisen. Diese Einstellungen findet er ebenfalls im Bereich "Device Configuration". In dieser Geräteschablone finden sich dann unter anderem Werte wie der Modus, in dem das Gerät arbeiten soll (als Access Point oder als Sensor für das Sicherheitsfeature WIPS), die Einstellungen für das Frequenzband und die einzusetzenden Kanäle sowie für das Geräte-Passwort. Auch hier gilt wieder das "Vererbungsprinzip": Sogenannte Child-Locations erben automatisch diese Einstellungen.

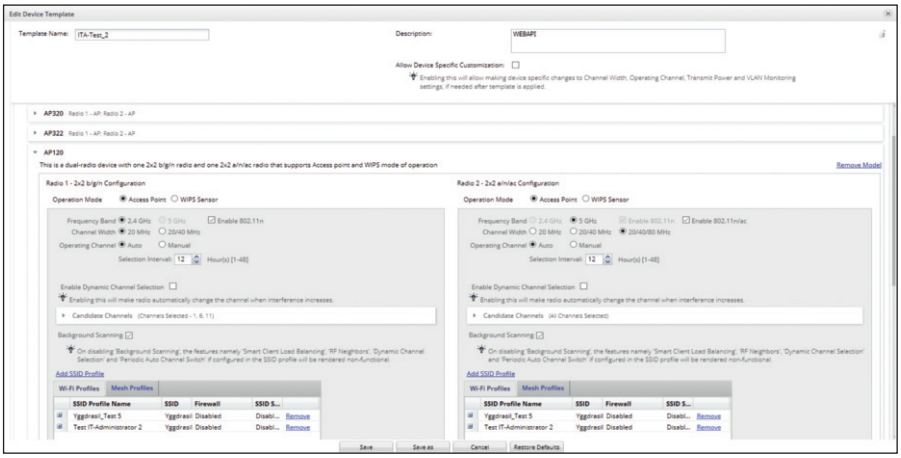
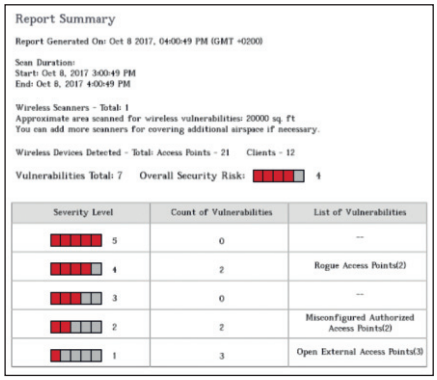


Bild 3: Wer seine WLAN-Netze nicht nur mit den Standardeinstellungen von WatchGuard Go anlegen will, kann seinen Access Points im Dashboard individuell konfigurierte Schablonen zuteilen.

Uns hat sehr gut gefallen, wie übersichtlich und einfach es hier für einen Administrator ist, die von ihm gewünschten beziehungsweise in seinem Unternehmen vorgegebenen Einstellungen für die WLAN-APs detailliert festzulegen und dann in die entsprechenden Schablonen zu überführen. Diese lassen sich dann beispielsweise direkt über die Cloud-Verbindung auf ein neues Gerät beziehungsweise einen neuen Standort ausrollen. Dort muss ein Mitarbeiter das Gerät nur an den richtigen Standort bringen und mit einem Ethernet-Kabel verbinden. Den Rest kann der Administrator via Browser von einem beliebigen Standort aus erledigen.

WIPS und weitere gelungene Sicherheitsfunktionen

Die WatchGuard-APs bieten im Zusammenhang mit Wi-Fi Cloud ein umfangreiches Set an Sicherheits-Features, die allerdings je nach Abonnement, das der Nutzer ausgewählt hat, unterschiedlich ausfallen. Die WIPS-Technik ist jedoch sowohl beim "Secure Wi-Fi"- als auch beim "Total Wi-Fi"-Paket mit dabei. Laut Aussagen des Anbieters handelt es sich beim Wireless Intrusion Prevention System um eine Weiterentwicklung der Wireless Intrusion Detection Systeme (WIDS). Die Technik bietet Netzwerk-



Report Summary

Report Generated On: Oct 8 2017, 04:00:49 PM (GMT +0200)

Scan Duration:
Start: Oct 8, 2017 3:00:49 PM
End: Oct 8, 2017 4:00:49 PM

Wireless Scanners - Total: 1
Approximate area scanned for wireless vulnerabilities: 20000 sq. ft
You can add more scanners for covering additional airspace if necessary.

Wireless Devices Detected - Total: Access Points - 21 Clients - 12

Vulnerabilities Total: 7 Overall Security Risk: 4

Severity Level	Count of Vulnerabilities	List of Vulnerabilities
5	0	--
4	2	Rogue Access Points(2)
3	0	--
2	2	Misconfigured Authorized Access Points(2)
1	3	Open External Access Points(3)

Bild 4: Mit Hilfe der Wi-Fi-Cloud lassen sich Reporte wie hier der Bericht zum "Wireless Vulnerability Assessment" in PDF-Form erstellen.

administratoren die Möglichkeit, ihre WLAN-Umgebung unter anderem vor unbefugten Geräten, Denial-of-Service-Angriffen und sogenannten Rogue Access Points zu schützen.

Eine solche WIPS-Lösung, wie sie mit dem von uns getesteten AP durch die Wi-Fi-Cloud-Umgebung zur Verfügung stand, hat die Fähigkeit, die Zugangspunkte und angeschlossenen Geräte wie Smartphones und Tablets in der WLAN-Umgebung als autorisiert, extern oder nicht autorisiert zu erkennen und klassifizieren. Das funktioniert grundsätzlich automatisch, der Administrator hat aber jederzeit die Möglichkeit, hier beispielsweise ein Gerät, das fälscherweise als "Rogue" markiert wurde, auch wieder als "autorisiert" freizugeben. Die automatische Klassifizierung der gefundenen Access Points erfolgt dabei in den drei Kategorien:

- Autorisiert: Verwaltete APs im LAN, die dem Administrator bekannt sind.
- Extern: Nicht verwaltete APs im Umfeld des eigenen drahtlosen Netzwerks, die aber nicht mit dem überwachten LAN verbunden sind.
- Rogue: Nicht autorisierte APs im LAN, die ohne Wissen und Zustimmung des Administrators installiert wurden.

WIPS wird auf sämtlichen Cloud-fähigen Access Points des Anbieters unterstützt. Diese müssen dazu aber über die WatchGuard Wi-Fi Cloud mit aktiven Lizenzen verwaltet werden. Administratoren richten die Technik auf zwei Wegen ein: So können sie ein solchen Cloud-fähigen AP als dedizierten WIPS-Sensor einrichten, was sich in der bereits beschriebenen Geräteschablone konfigurieren lässt. Ein solcher dedizierter WIPS-Sensor muss dann parallel zu anderen APs installiert werden, die dann für den Client-Datenverkehr zuständig sind. Der WIPS-Sensor-AP selbst lässt keine Client-Verbindungen zu.

Der Anbieter rät in den Unterlagen, dass für je vier Access Points ein solcher Sensor zum Einsatz kommen sollte. Die zweite Möglichkeit besteht darin, dass ein AP in Doppelfunktion arbeitet: Als Access Point für Clients und als WIPS-Sensor. Die Konfiguration sieht dann so aus, dass die Leistung der Geräte prozentual auf die Abwicklung des Client-Verkehrs im WLAN und die Scans im Rahmen der WIPS-Technik aufgeteilt wird. Unter "Configuration / Wips / Authorized WLAN Policy" kann der Administrator dann natürlich auch sogenannte Richtlinien-Schablonen für die Sicherheit anlegen, mit einer SSID verbinden und einer Location zuweisen.

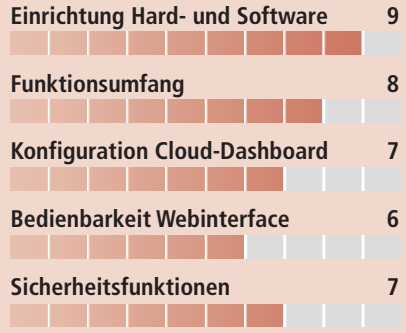
Fazit

Der WatchGuard Access Point AP120 konnte im Test überzeugen: Einrichtung, Anmeldung und Betrieb sind durch den vom Hersteller als "WatchGuard Wi-Fi Cloud" bezeichneten Ansatz so gehalten, dass selbst weniger erfahrene Administratoren kaum Probleme haben werden, ihr WLAN entsprechend ihren Wünschen zu konfigurieren und zu betreiben. Allerdings müssen sie dazu doch einigermaßen in der englischen Sprache bewandert sein, denn sowohl die insgesamt gut gestaltete Oberfläche als auch die umfangreichen Hilfetexte und Videos sind alle auf Englisch.

Wenn wir aber von dieser Einschränkung und der nur mit der Lupe zu lesenden Seriennummer absehen, dann ist dieses Gerät sicher eine Empfehlung wert – selten konnten wir ein Testgerät so leicht und schnell einrichten und in Betrieb nehmen. Auch die Funktionsvielfalt und die umfangreichen Sicherheitsfeatures konnten während unseres Testbetriebs überzeugen. Das Konzept der einfachen und übersichtlichen Verwaltung über die Cloud wird bei dieser Lösung konsequent durchgehalten und umgesetzt. Die WIPS-Technik hat uns in einer Laborinstallation des Anbieters ebenfalls überzeugen können – gerade die automatische Klassifizierung dürfte Admins in der Praxis viel Arbeit ersparen.

Natürlich bleiben die üblichen Vorbehalte gegen Lösungen aus der Cloud: Wenn die Firmenrichtlinien oder gesetzliche Vorgaben es nicht erlauben, Daten und/oder administrative Aufgaben in die Cloud auszulagern, dann kann dieser Ansatz sicher keine Alternative sein. Weiterhin müssen sich Firmen bei derartigen Ansätzen immer darüber Gedanken machen, wie zuverlässig der Cloud-Partner die Dienstleistung auch in den kommenden Jahren liefern wird. Allerdings zeigen unsere bisherigen Erfahrungen mit der Firma WatchGuard, dass der Kunde hier von einer entsprechenden Zuverlässigkeit und Langlebigkeit des Angebots ausgehen kann. *(ln)* IT

So urteilt IT-Administrator



Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik

Dieses Produkt eignet sich

optimal für kleinere und mittlere Betriebe, die ohne großen Aufwand ihr WLAN-Netz samt Gast-Netzwerke einfach und sicher über den Browser verwalten wollen.

bedingt für Administratoren größerer WLAN-Netze. Die Wi-Fi-Cloud ist eine sehr gute Management-Schnittstelle, die ortsunabhängig und ohne Installation eingesetzt werden kann. Was die eingesetzten APs betrifft, werden dann eher größere Geräte wie der AP320, AP322 oder AP420 zum Einsatz kommen.

nicht für Organisationen, die ein ausschließlich kabelgebundenes Netzwerk nutzen oder die aus Gründen der Compliance keine Administration über die Cloud erlauben.