WLAN-Absicherung mit WatchGuards Wireless Intrusion Prevention System (WIPS)

Einführung

Der weltweite Siegeszug des WLAN bietet Cyberkriminellen attraktive Möglichkeiten, die Daten und Systeme ahnungsloser Nutzer auszuspionieren, zu stehlen und zu infizieren. Zum Zeitpunkt der Veröffentlichung dieses Dokuments finden sich allein auf YouTube über 300.000 Videos, die erklären, wie sich Geräte im WLAN hacken lassen. Die Werkzeuge dazu sind schnell beschafft und einfach zu bedienen. Wer als Unternehmen WLAN anbietet – sei es für Mitarbeiter oder für Kunden und Gäste – sollte daher solch böswilligen Absichten von Anfang an einen Riegel vorschieben. Die folgenden Ausführungen zeigen auf, wie sich das Problem mit WIPS (Wireless Intrusion Prevention System) von WatchGuard lösen lässt. WIPS ist für alle cloudfähigen Access Points von WatchGuard verfügbar, deren Verwaltung über die WatchGuard Wi-Fi Cloud erfolgt.

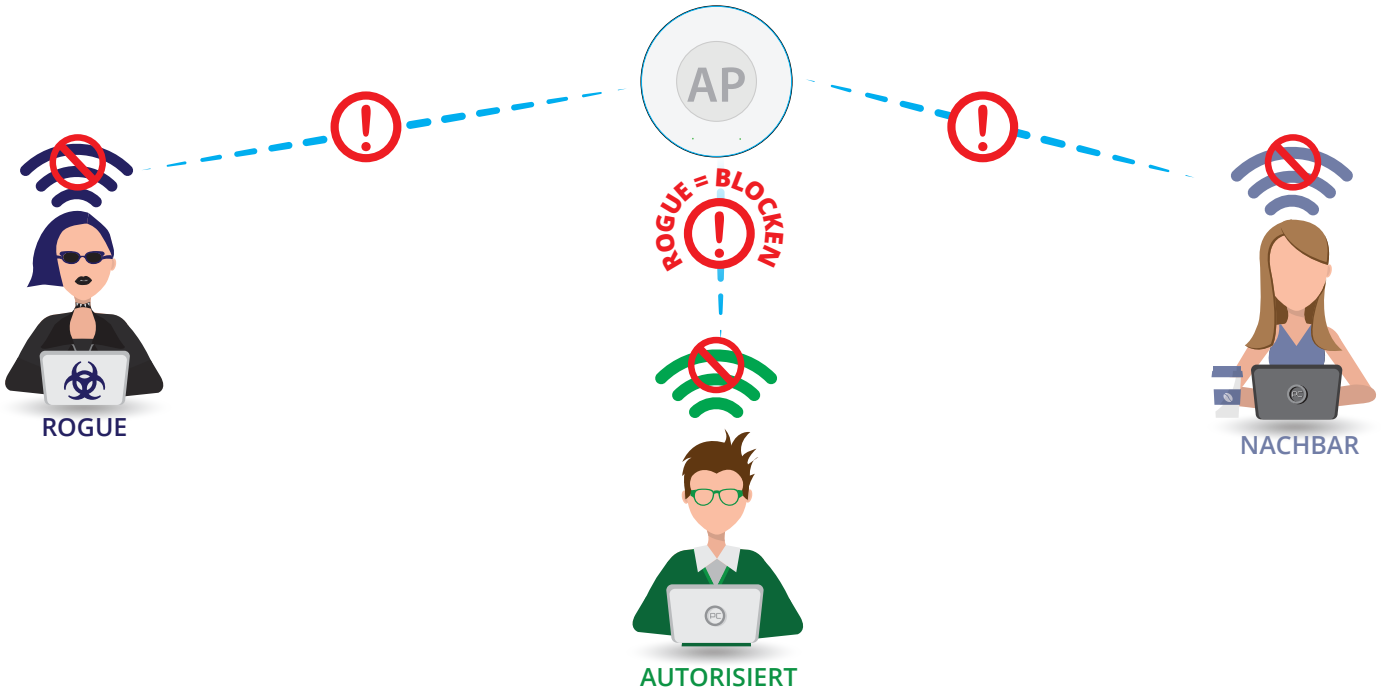
Derzeitige Lösungen weisen gravierende Mängel auf

Die WIPS-Lösungen anderer Anbieter setzen aufgrund der möglichen Beeinträchtigung benachbarter, legitimer WLAN-Netzwerke meist nur auf Erkennung statt Prävention. Das liegt an der hohen Quote an Fehleinschätzungen (False Positives) auf Basis der zugrundeliegenden Technologie. Die Folge: Nicht selten ignorieren Administratoren die Warnmeldungen oder schalten entsprechende Benachrichtigungen komplett aus – und riskieren somit die Sicherheit des Unternehmensnetzwerks. Die Angebote der Mitbewerber erfordern meist einen hohen Administrationsaufwand und bieten kaum verlässliche Erkennung der sogenannten schadhaften „Rogue Access Points". Viele Unternehmen, die auf solche Systeme vertrauen, wägen sich daher in falscher Sicherheit: Tatsächlich sind ihre Netzwerke anfällig für alle von Rogue Access Points ausgehenden Gefahren.

Volle Kontrolle im WLAN

Mit WatchGuards WIPS gewinnen Unternehmen bei minimalem Verwaltungsaufwand WLAN-Sicherheit auf Enterprise-Niveau – alle gängigen Standards wie PCI, HIPAA oder Sarbanes Oxley werden dabei erfüllt. Das WIPS von WatchGuard greift auf die patentierte Marker Packet-Technologie zurück und bietet damit das branchenweit zuverlässigste WIPS mit der geringsten False-Positives-Quote. Damit behalten Sie die Kontrolle über Ihr WLAN.

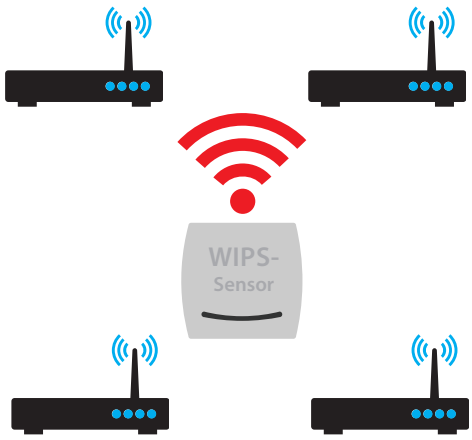
Wie lässt sich WatchGuards WIPS aktivieren und einrichten?



WatchGuard WIPS wird auf sämtlichen cloudfähigen Access Points (AP) von WatchGuard unterstützt, die über WatchGuard Wi-Fi Cloud mit aktiven Lizenzen verwaltet werden. Das WIPS lässt sich über zwei Wege einrichten:

1. Empfohlen: dedizierte WIPS-Sensoren

Diese Variante beinhaltet die Konfiguration der cloudfähigen AP als dedizierte WIPS-Sensoren. Als dedizierter WIPS-Sensor wird der AP parallel zu anderen AP installiert, die für den Client-Datenverkehr konfiguriert sind. Er selbst lässt für drahtlose Clients keine Verbindung zu. Als Faustregel gilt: Für vier AP sollte ein WIPS-Sensor eingesetzt werden. Dieses von WatchGuard empfohlene Einsatzszenario sorgt für ein Höchstmaß an Sicherheit im WLAN: Dedizierte WIPS-Sensoren schützen ununterbrochen die drahtlose Umgebung und verhindern, dass Angreifer sich Funktionslücken zunutze machen, die entstehen können, wenn ein WIPS-Sensor gleichzeitig als „normaler" AP agiert.



2. AP mit Doppelfunktion

Alle cloudfähigen AP können so konfiguriert werden, dass sie ihre Leistung prozentual auf die Abwicklung des WLAN-Client-Verkehrs sowie die Scans im Rahmen des WIPS aufteilen. In diesem Modus fungiert die Plattform als Access Point und gleichzeitig als WIPS-Sensor. Die WLAN-seitige „Packet Injection"-Funktion ist dann jedoch nicht verfügbar.

Dediziertes Scannen	Scannen im Hintergrund
Ausschließliche Scan-Funktionalität – Dualband-Scan im Rundlaufverfahren (jeder Funkkanal wird alle fünf Sekunden für 100 Millisekunden gescannt)	Einsatz als AP mit Dualband-Scan im Hintergrund (Off-Traffic-Kanal wird alle zwei Minuten für 100 Millisekunden gescannt)
Schnelle Gefahrenerkennung auf allen Kanälen	Gefahrenerkennung für Off-Traffic-Kanäle kann dauern (trotzdem immer noch die beste Aufdeckungsquote für Rogue Access Points, da Einsatz der Marker Packets™ zeitlich abgestimmt ist)
Sowohl funk- als auch drahtgestützte Abwehr. Sperrung für sämtliche Bedrohungsarten.	Nur drahtgestützte Abwehr (Rogue-AP-Aktivität wird via LAN über das sogenannte Teergrube-Verfahren unterbunden)
Hauptanwendungsbereich: Hochsicherheitsumgebungen/ Compliance-sensible Branchen (Finanzwesen, Öffentliche Verwaltung, Gesundheitswesen, Technologie-Sektor, Bildungsbereich usw.)	Hauptanwendungsbereich: Einzelhandel (PCI Compliance)

So funktioniert WIPS von WatchGuard

LAN-seitiger Marker Packet-Einsatz

WIPS injiziert Marker Packets via Kabel des WIPS/AP in das LAN Diese Pakete werden von Access Points, die mit dem überwachten LAN verbunden sind, ins WLAN übertragen. Die anschließende Erkennung erfolgt über Funk von der drahtlosen Seite des WIPS/AP. Der AP kann in einem Subnetz oder – bei mehreren Subnetzen – auf dem Trunk-Port eines Managed Switchs platziert werden.

Diese Variante bietet die folgenden Vorteile:

- sie erfordert kein direktes Zusammenspiel mit den Netzwerk-Switches
- sie erfordert weder anfängliche noch fortlaufende Konfigurationen für den Betrieb
- die Technik ermittelt schnell die Anbindung der AP – unabhängig von der Größe des Netzwerks, da dies für jedes lokale Subnetz simultan erfolgt
- der Umfang des durch Packet Injection erzeugten Datenverkehrs ist durchaus vernachlässigbar (weniger als 0,1 Prozent der LAN-Port-Kapazität)
- bei dieser Variante sind Fehlalarme ausgeschlossen, da Rogue Access Points nie als externe AP gekennzeichnet werden und umgekehrt

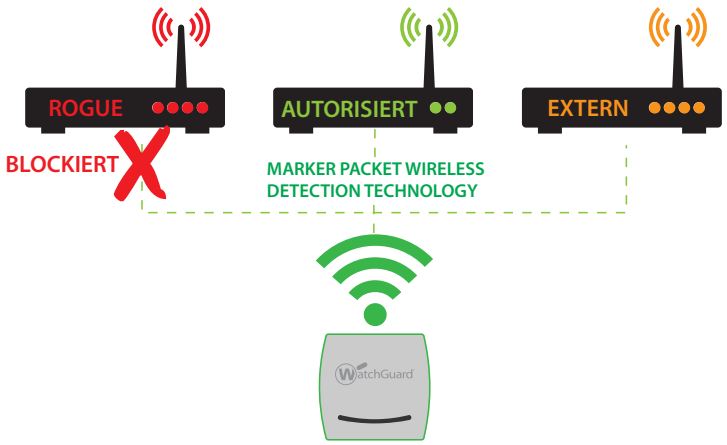
WLAN-seitiger Marker Packet-Einsatz

Wenn der WIPS/AP einen mit einem AP verknüpften Client erkennt, sendet er Pakete mit einer eindeutigen Kennung (Marker Packets) von der drahtlosen Seite des potenziellen Rogue AP in Richtung der IP-Adressen eines bekannten LAN-Hosts. Diese Pakete der Verbindung zum Client mit dem potenziellen Rogue-AP hinzugefügt. Wenn eines dieser Pakete am Ziel-Host eingeht, erfolgt die Bestätigung, dass der AP mit dem überwachten LAN verknüpft ist.

Eindeutiges Unterscheidungsmerkmal: Automatische AP-Klassifizierung

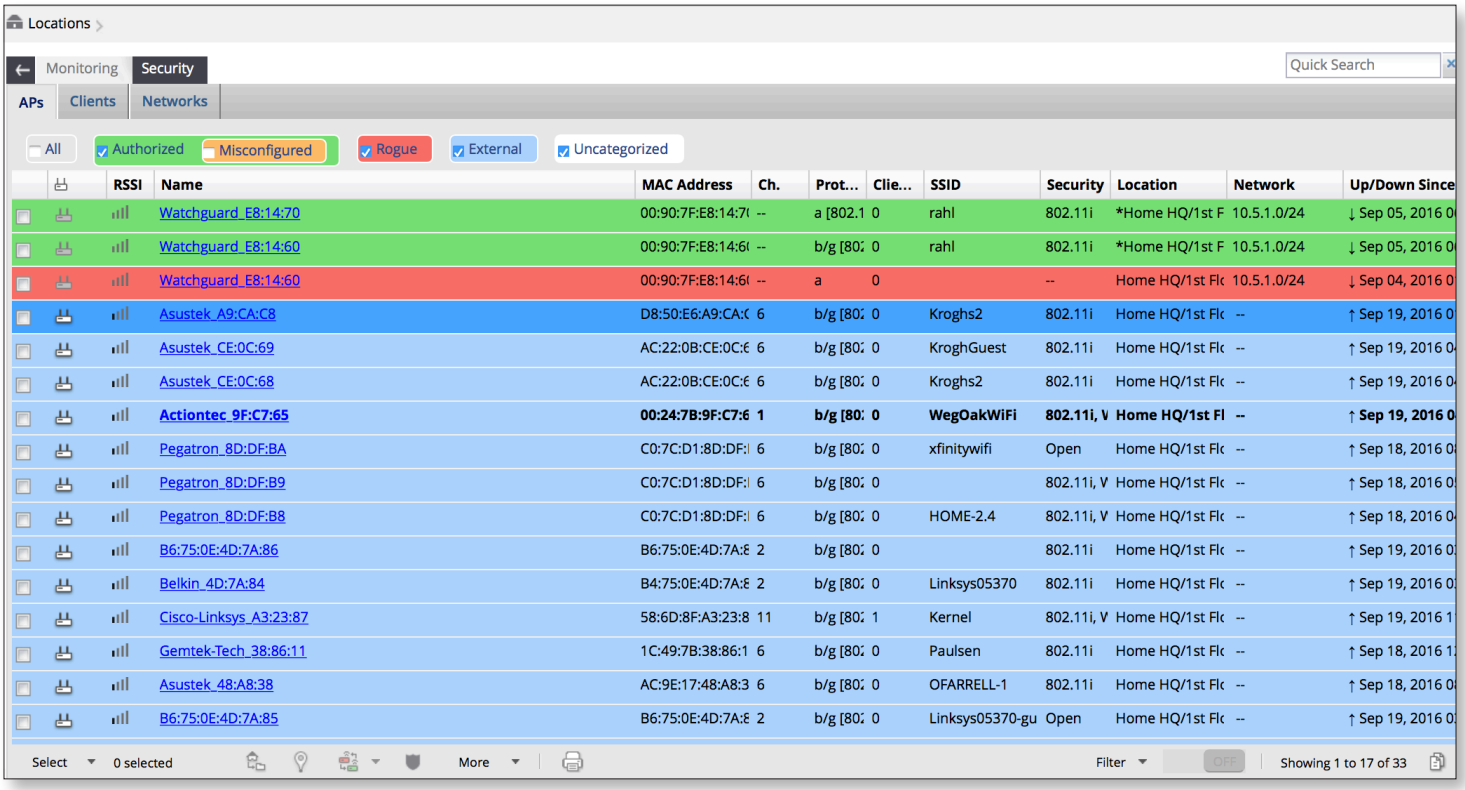
Am natürlichsten und elegantesten lassen sich AP klassifizieren, indem man ihre Netzwerkverbindung ermittelt. Diese Art der automatischen Klassifizierung ist unabhängig von unzuverlässigen oder nicht-verwaltbaren Klassifikationssignaturen basierend auf SSID, Anbieter, Leistungspegel, Verschlüsselungseinstellung oder Leitung. Es sind lediglich eine zuverlässige Netzwerkverbindung und Zugriff auf die gewünschten VLAN erforderlich.

Eine präzise, zuverlässige automatische AP-Klassifizierung ist der Schlüssel zu einem effektiven Wireless Intrusion Prevention System. WIPS von WatchGuard ist die einzige Technologie, die eine auf AP-Netzwerkverbindung basierende Autoklassifizierung integriert. Ermöglicht wird dies durch die einzigartige Marker Packet-Technologie, die die Netzwerkverbindung aller AP-Arten zuverlässig erkennt. Im Rahmen von WIPS-Lösungen ist die Marker Packet-Technologie ein klares Alleinstellungsmerkmal.



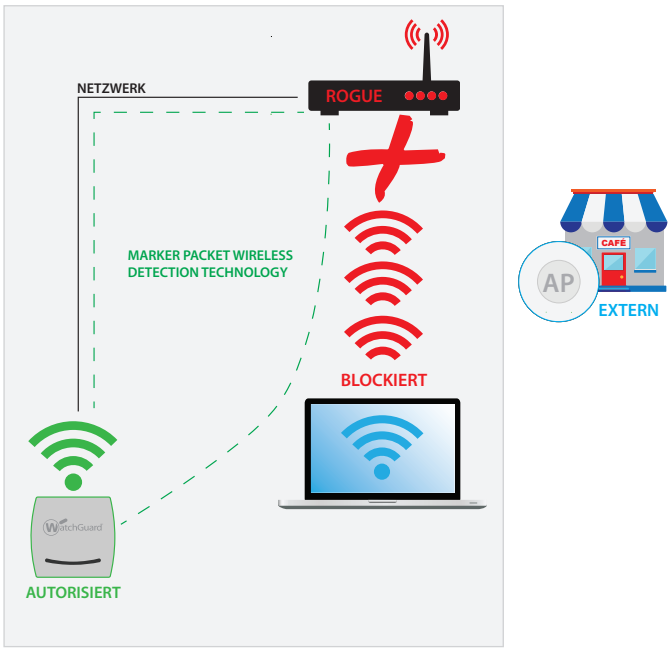
Bei der automatischen AP-Klassifizierung werden sichtbare AP in drei Kategorien unterteilt:

- **Autorisiert**: Verwaltete AP im LAN, die der Administrator kennt
- **Extern**: Unverwaltete AP im drahtlosen Umfeld, die nicht mit dem überwachten LAN verbunden sind
- **Rogue**: Nicht-autorisierte, im LAN ohne Wissen des Administrators installierte AP



Vorteile von WatchGuard WIPS:

- Echte **Prävention** statt nur **Erkennung**
- Marker Packet-Technologie
- Präzise Klassifikation von Geräten im LAN, mit minimaler Fehleinschätzungsquote (False Positives)
- Erkennung, Klassifikation und Abwehr von NAT-, verschlüsselten und Soft-AP
- Erkennung und Unterbindung von nicht-autorisiertem Client-Verhalten
- Automatische Prävention ohne Beeinträchtigung benachbarter Geräte oder Netzwerke
- Abwehr vielfältiger Gefahren über zahlreiche Leitungen von einem einzelnen Sensor aus
- Abwehr unterschiedlichster 802.11-DoS-Angriffsarten
- Durchsetzung von WLAN-Policies nach VLAN, SSID und Standort
- Multi-VLAN-Support (bis zu 100 VLAN von einem einzelnen Sensor aus)
- Keine Abhängigkeit von CAM-Tabellenprüfungen oder SNMP
- Mobilgerät-Überwachungsliste
- Offline-Sensormodus (Rund-um-die-Uhr-Schutz)
- Remote Packet Capture (R-PCAP) von beliebigem Sensor
- Präzise Standortverfolgung von einzelnem Sensor
- Verwaltung Tausender Sensoren über eine einzelne Konsole
- Diverse automatisierte Sicherheits- und Compliance-Berichte
- Einfache Bedienung und Bereitstellung, geringste Gesamtbetriebskosten
- Übererfüllung der Anforderungen gemäß DoD 8100.2 WIDS
- Konstante Durchsetzung von „Kein Wi-Fi"-Vorgaben für verdrahtete VLAN im Netzwerk

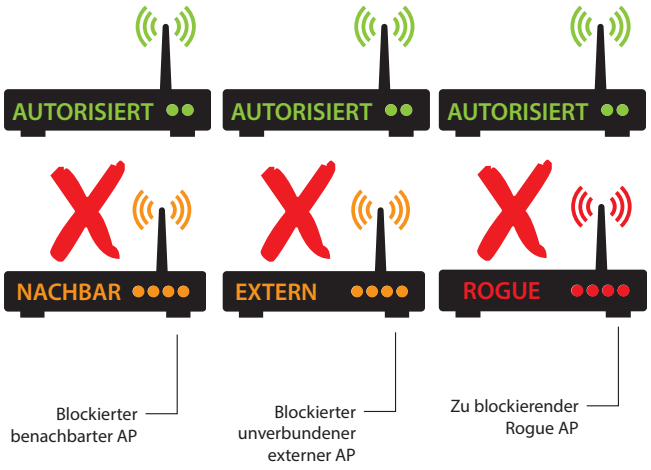


Fünf Fallstricke anderer WIPS-Lösungen

Jedes WIPS ist anders aufgebaut. Zur Verdeutlichung sind nachfolgend fünf Stolpersteine aufgeführt, die in den meisten WIPS-Lösungen anderer Anbieter zu finden sind:

1. Erkennung von Rogue AP

Als Rogue AP kann jeder unautorisierte AP definiert werden, der mit einem autorisierten Netzwerk verbunden ist. Rogue AP stellen eine ernsthafte Bedrohung für Netzwerke dar, da sie den unbefugten drahtlosen Zugang zum privaten Netzwerk erlauben. Rogue AP können versehentlich oder aber mit böser Absicht von Mitarbeitern ins Netzwerk eingeschleust werden. Viele WIPS-Lösungen im Markt verwenden für die Erkennung von Rogue AP im LAN eine unzulängliche Methode: Dabei wird jeder ermittelte AP, der nicht in der Liste der autorisierten AP aufgeführt ist, als Rogue AP deklariert.



Ein solcher Ansatz hat folgende Nachteile:

- **Fehlalarme**: Sicherheitswarnungen werden auch dann erzeugt, wenn ein unautorisierter AP erkannt wird, der jedoch nicht mit dem überwachten LAN verbunden ist und daher kein Sicherheitsrisiko darstellt.
- **Manueller Eingriff**: Der Systemadministrator muss identifizierte, nicht-autorisierte AP manuell überprüfen, um zu entscheiden, bei welchen es sich tatsächlich um Rogue AP handelt und welche externe (also benachbarte) AP sind.
- **Keine sofortige automatische Abwehr**: Da benachbarte AP weder versehentlich oder absichtlich beeinträchtigt werden sollten, ist eine sofortige und automatische Sperrung von Rogue AP bei diesem Ansatz nicht möglich.

2. Signaturgestützte WIPS

Viele andere WIPS versuchen, AP anhand von benutzerseitig konfigurierten Klassifikationssignaturen zu kategorisieren. Zur Definition von Klassifikationssignaturen werden Unmengen von AP-Eigenschaften herangezogen – beispielsweise SSID, Anbieter, Leistungspegel, Verschlüsselungseinstellungen und Kanal. Die Netzwerkverbindung zwischen AP und Netzwerk kann, muss aber kein Faktor für die Klassifizierung sein. Dieser Ansatz hat mehrere Nachteile:

- **Signaturverwaltung:** Für die Definition von Klassifikationssignaturen ist ein erheblicher Konfigurationsaufwand erforderlich. Die Signaturen müssen regelmäßig aktualisiert werden. Beispiel: Was passiert, wenn die bekannte Konfiguration eines benachbarten, harmlosen WLAN geändert und eine andere SSID verwendet wird?
- **Fortlaufende manuelle Eingriffe**: WLAN-Konfigurationen neu erkannter AP passen möglicherweise nicht genau zu den definierten Signaturen; in diesem Fall ist ein manueller Eingriff erforderlich, um die neu erkannten AP zu klassifizieren.
- **Unerkannte Gefahren**: Bei diesem Ansatz werden echte Bedrohungen häufig nicht erkannt. So wird beispielsweise eine Klassifikationssignatur wie „if "SSID = freewifi AND signal strength = Low"“ zur Klassifikation eines bekannten benachbarten AP von einem Rogue AP mit geringer Übertragungsleistung und SSID-Konfiguration „freewifi“ ausgehebelt.

3. MAC-Tabellenprüfungen

Bei dieser Technik werden MAC-Adressen von Geräten im WLAN mit den MAC-Adressen verglichen, die an den Ports von Managed Switches im LAN registriert sind. Wenn eine zwischen WLAN und LAN übereinstimmende MAC-Adresse erkannt wird, wird davon ausgegangen, dass das Gerät mit dieser MAC-Adresse mit dem überwachten LAN verbunden ist.

Bei Access Points im Bridging-Mode ist der Abgleich erst möglich, wenn ein Client eine Verbindung zum AP erstellt. Nachdem der Client die Verbindung hergestellt hat, wird dessen MAC-Adresse an dem Switch-Port registriert, an dem der AP angeschlossen ist. Die Sammlung von MAC-Adressen, die an den Ports von Managed Switches im Netzwerk registriert sind, erfolgt durch Abfrage der CAM-Tabellen für jeden Switch über SNMP.

Dieses Vorgehen bringt mehrere Nachteile mit sich:

- Hierbei wird in die Switching-Infrastruktur eingegriffen. Es erfordert die Verwaltung von Switch-Kennungen im WIPS, damit MAC-Tabellen der Switches abgefragt werden können. Außerdem gibt es Probleme hinsichtlich der Interoperabilität von Switches verschiedener Anbieter.
- MAC-Tabellenüberprüfungen aller Managed Switches im Netzwerk sind eine ressourcenintensive und zeitaufwendige Aufgabe, insbesondere in großen Netzwerken mit Hunderten Switches. Darum kann die Erkennung von Netzwerkverbindungen in großen Netzwerken mit diesem Ansatz nur unregelmäßig erfolgen.
- Die Erkennung erfordert nicht zuletzt Glück. Wenn der Client inaktiv wird, verschwindet sein MAC-Eintrag aus der MAC-Tabelle. Bei einer MAC-Tabellenabfrage (die meist in regelmäßigen Abständen erfolgen) ist dieser Ansatz nur von Erfolg gekrönt, wenn der Client tatsächlich gerade mit dem Rogue AP verbunden ist.

4. Passive MAC-Korrelation

Mit dieser Methode sollen die Nachteile der vorangehend dargestellten MAC-Tabellenprüfung überwunden werden. Bei dieser Technik hört der WIPS AP seine drahtseitige Schnittstelle passiv nach im Subnetz aktiven MAC-Adressen ab. Die dabei ermittelten MAC-Adressen werden für die MAC-Adressen-Korrelation auf LAN- und WLAN-Seite genutzt. Doch selbst bei diesem Ansatz kann das Problem auftreten, dass für nicht mit dem überwachten Netzwerk verbundene AP (beispielsweise benachbarte AP) fälschlicherweise eine Verbindung mit diesem Netzwerk angenommen wird. Das passiert, wenn Clients zwischen diesen AP wechseln.

5. Drahtseitige Verfolgung

Bei dieser Technik versucht ein WIPS AP, nachdem er einen AP im Netz ermittelt hat, LAN-seitig aktiv eine Verbindung zum AP herzustellen. Der WIPS AP schickt dann entweder ein Ping-Signal über das drahtgebundene Netzwerk zum potenziellen Rogue AP oder sendet ein Paket an einen bekannten Host auf der drahtgebundenen Seite des Netzwerks, um zu ermitteln, ob der AP mit dem Unternehmens-LAN verbunden ist. Diese aktive Verbindungsherstellung zum AP unterliegt gewissen Beschränkungen; so dauert es eine gewisse Zeit, bis eine solche AP-Verbindung via Layer 2 und 3 steht (bis zu fünf Sekunden). In diesem Zeitraum ist der WIPS AP auf die AP-Leitung fokussiert und kann die Scan-Funktion nicht ausführen. Wenn der WIPS AP viele potenzielle Rogue AP erkennt, kann diese Methode daher nur unregelmäßig angewendet werden. Die Folge ist eine große Verzögerung bei der Ermittlung der AP-Verbindung. Mehr noch: Dieses Verfahren ist nicht in der Lage, Rogue AP mit besonderen Einstellungen zu erkennen, beispielsweise eine autorisierte Client-MAC-Adressliste an der drahtlosen Schnittstelle, wodurch eine aktive Zuordnung des potenziellen Rogue AP durch den WIPS AP nicht möglich ist.

Premium-WIPS und UTM im Paket

Mit jedem innovativen Produkt von WatchGuard soll für kleine und mittlere Unternehmen Sicherheit auf Enterprise-Niveau geschaffen werden. Mit der WatchGuard Wi-Fi Cloud können IT-Profis ihren Anwendern ein leistungsstarkes WLAN bieten – ohne Abstriche bei der Sicherheit. Das Fundament ist die unschlagbare Kombination aus weltweit führender WIPS-Technologie mit branchenführenden UTM-Services.

Weitere Informationen zur Produktreihe der WLAN-Sicherheits-Lösungen von WatchGuard finden Sie unter www.watchguard.com/wifi.

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. WGCE66941_092617