WHITEPAPER

# Klassifizierung – der entscheidende Schwachpunkt zahlreicher WIPS

## Inhaltsverzeichnis

### Inhalt



## 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. Daher überrascht es nicht, dass dem Thema Angriffsabwehr im WLAN hohe Beachtung zukommt, wenn es darum geht, ob und zu welchem Zeitpunkt eine WLAN-Lösung umgesetzt werden soll. WLAN-Anbieter weltweit begegnen der Bedrohung mit der Einführung von Wireless Intrusion Detection Systemen (WIDS) und Wireless Intrusion Prevention Systemen (WIPS). Angesichts der Vielzahl verfügbarer Produkte wird die Auswahl der wirksamsten Lösungen selbst für die technisch versiertesten Käufer zum Problem. In diesem Dokument sind die wichtigsten Komponenten einer effektiven WIPS-Lösung beschrieben. Es bietet Entscheidern einen Überblick über die für eine Kaufentscheidung relevanten Aspekte.

## Wireless Intrusion Prevention System – Funktionsweise und Vorteile

Internetkriminelle schleusen unbefugte Rogue-Geräte ins Unternehmensumfeld ein, um Unternehmensdaten abzufangen und zu stehlen. Ein Wireless Intrusion Prevention System oder WIPS fungiert im Prinzip als grundlegendes „Sicherheitsnetz" für drahtlose Netzwerke, in denen sensible Daten übertragen oder gespeichert werden. WIPS ermöglichen es Netzwerkadministratoren, ihre WLAN-Umgebung vor unbefugten Geräten, Denial-of-Service-Angriffen, Rogue AP und vielem mehr zu schützen.

Mit anderen Worten: Eine umfassende WIPS-Lösung muss Geräte und Access Points (AP) wirksam und zuverlässig erkennen, klassifizieren und vor Bedrohungen schützen können.

- Erkennung – Die Fähigkeit zur Erkennung sämtlicher Geräte und Access Points in einer WLAN-Umgebung (einschließlich Smartphones, Tablets, Laptops etc. sowie alle verbundenen Geräte wie multifunktionale Drucker).
- Klassifizierung – Die Fähigkeit zur schnellen und präzisen Klassifizierung einzelner Access Points und Geräte entsprechend der Kategorien „autorisiert", „extern" oder „potenziell gefährlich" (Rogue).
- Prävention – Die Fähigkeit sämtliche Rogue-Geräte oder Access Points innerhalb einer WLAN-Umgebung umgehend unter Quarantäne zu stellen und böswillige Machenschaften dadurch bereits im Vorfeld zu verhindern.

**TIPP**

Die granulare Erkennung macht den Unterschied: Sie ermöglicht im Gegensatz zu einer generischen Erkennung eine präzise Klassifizierung – prüfen Sie daher die Klassifizierungsgenauigkeit Ihres WIPS!

Im Rahmen der Weiterentwicklung von Sicherheitskonzepten für WLAN-Umgebungen sind die Erkennung und der Schutz von Geräten und AP mittlerweile zur Norm geworden. Gegenwärtig ist es der Klassifizierungsaspekt, der Probleme bereitet. Die Fähigkeit zur Unterscheidung zwischen wirklich schadhaften Geräten oder AP und harmlosen externen Plattformen ist für eine wirksame Schadensbegrenzung entscheidend. Die fehlerhafte Rogue-Klassifizierung externer Geräte und AP sowie deren nachfolgende Isolierung kann eine ganze Reihe negativer Auswirkungen haben – von Reputationsverlust bis hin zu rechtlichen Folgen.

## Die Folgen einer fehlerhaften Klassifizierung

Eine gute WIPS-Lösung erkennt und gibt Aufschluss über sämtliche Access Points und Geräte in Ihrer WLAN-Umgebung. Auch Geräte und AP, die nicht unmittelbar mit Ihrem Netzwerk verbunden sind, werden innerhalb der WLAN-Umgebung angezeigt. Für Unternehmen ist es daher äußerst wichtig, Geräte nicht nur zu erkennen, sondern feststellen zu können, ob diese wirklich mit ihrem WLAN verbunden sind oder sich lediglich innerhalb der WLAN-Reichweite befinden, bevor entsprechende Abwehrmaßnahmen getroffen werden.

In innerstädtischen Bereichen können beispielsweise Dutzende von Unternehmen mit eigenen WLAN-Umgebungen in einem einzigen Häuserblock ansässig sein. Infolgedessen ist es unerlässlich, dass jedes Unternehmen in der Lage ist, die Sicherheit des eigenen WLAN zu gewährleisten und Konflikte mit WLAN-Nutzern und -Services benachbarter Firmen zu vermeiden. Eine Störung benachbarter WLAN-Umgebungen ist nicht nur unerwünscht, sondern auch illegal.

Aus diesem Grund muss eine WIPS-Lösung sämtliche Geräte und Access Points in einer WLAN-Umgebung erkennen und darüber hinaus Rogue-Geräte/AP von benachbarten (oder externen) AP unterscheiden können. Ohne eine zuverlässige WIPS-Klassifizierung ist kein wirksamer Schutz möglich. Dies wird durch eine alarmierend große Anzahl von Unternehmen belegt, die ihre WIPS bewusst auf WIDS-Lösungen herabstufen.

Sie nutzen somit lediglich den Erkennungsaspekt des Systems. Entsprechenden Maßnahmen zur Abwehr muss immer eine manuelle Klassifizierung der einzelnen Geräte und AP vorausgehen. Auch wenn unbefugte AP und Geräte letztlich manuell aus einem Netzwerk entfernt werden können, ist keine umgehende Bedrohungsabwehr möglich. Ein solcher Vorgang kann Stunden, Tage oder gar Wochen in Anspruch nehmen.

## Die Vorteile von WIPS nutzen – präzise AP- und Geräteklassifizierung

Die grundlegende Kenntnis der kaum kommunizierten Schwachstellen gängiger WIPS versetzt Entscheidungsträger aller Branchen in die Lage, bei anstehenden Kaufentscheidungen für WLAN-Lösungen die richtigen Fragen zu stellen. Vergewissern Sie sich zu Beginn, dass die angebotene Lösung WIPS beinhaltet, und informieren Sie sich dann im Detail über die Klassifizierungsmethoden des Systems. Fast alle WIPS-Lösungen unterscheiden sich im Hinblick auf die Geräte- und AP-Erkennung oder Reaktionszeiten nur geringfügig, aber nur die wenigsten ermöglichen eine ordnungsgemäße Klassifizierung. Ohne eine solche Klassifizierung ist jedoch kein unmittelbarer WIPS-Schutz gegeben. Für Unternehmen, egal ob mit oder ohne IT-Abteilung, wird die Ergreifung von Gegenmaßnahmen im Verdachtsmoment auf diese Weise zu einem zeitraubenden manuellen Prozess.

## WatchGuard Wi-Fi Cloud – zuverlässige Klassifizierung im WIPS

WatchGuard verfügt über ein umfassendes Sortiment an WLAN-Sicherheitslösungen. Hierzu zählt auch die WatchGuard Wi-Fi Cloud – eine sichere, skalierbare WLAN-Managementplattform mit umfangreichen Funktionen und einer Produktfamilie leistungsstarker, cloudfähiger Access Points.

WatchGuard WIPS ermöglicht Ihnen dank patentierter Verfahren für Wireless Intrusion Detection und Prevention nicht nur umfassenden Überblick zu jeder Zeit, sondern garantiert auch vollständige Kontrolle über sämtliche WLAN-Aktivitäten. WatchGuard WIPS nutzt die patentierte Marker-Packet-Technologie, um drahtlose Geräte innerhalb der WLAN-Umgebung schnell und automatisch als autorisierte, Rogue- oder externe Geräte zu klassifizieren.

Fehlalarme werden dadurch vermieden und Sicherheitsadministratoren müssen weniger Zeit für die Definition komplexer Regeln zur Identifizierung drahtloser Rogue-Geräte und für die manuelle Überprüfung von Geräten aufwenden.

Damit unterscheidet sich die Lösung hinsichtlich der Klassifikationsmöglichkeiten von den meisten anderen WLAN-Lösungen im Markt. Diese sind deutlich fehleranfälliger, da sie sich auf zeitaufwendige, mehrdeutige CAM-Referenztabellen, MAC-Korrelationen, Signaturen und passive, drahtgebundene Netzwerkanalysen stützen. Dank der fortschrittlichen Bedrohungserkennung ist das WIPS von WatchGuard das einzige im Markt, das unbefugte Access Points und Clients sicher und automatisch blockiert, ohne benachbarte WLAN-Umgebungen zu stören. Weitere Informationen zur Produktreihe der sicheren WLAN-Lösungen von WatchGuard finden Sie unter **www.watchguard.com/wifi**.

**TIPP**

Sprechen Sie bei der Evaluierung einer WLAN-Lösung mit Kunden des Anbieters. Erkundigen Sie sich, ob sie einen automatisierten Schutz nutzen und fragen Sie nach der Genauigkeit der Geräte- und AP-Klassifizierung!

## 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. WGCE66938_092616