Wireless Intrusion Prevention Systems

Freund und Feind klar unterscheiden

Zur Absicherung von WLAN-Umgebungen setzen immer mehr Unternehmen auf ein Wireless Intrusion Prevention System (WIPS). Während die Erkennung potenzieller Gefahren meist kein Problem darstellt, zeigen sich hinsichtlich der automatisierten Ergreifung vorbeugender Maßnahmen zum Schutz des Unternehmensnetzwerks oft große Unterschiede zwischen den verschiedenen Lösungsansätzen.

Mit der fortschreitenden Etablierung von WLAN-Strukturen ergeben sich für Hacker ganz neue Angriffsmöglichkeiten, Daten mithilfe ahnungsloser Nutzer auszuspionieren beziehungsweise zu stehlen und Systeme zu infizieren. Aktuell 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. So ist die Gefahr, die von veralteten Protokollen wie WEP ausgeht, mittlerweile hinlänglich bekannt. Dennoch finden solche in der Praxis nach wie vor weite Verbreitung. Auch bei moderneren Verschlüsselungsmethoden wie WPA und WPA2 gibt es angreifbare Schwachstellen. Besonders wenn kurze, wenig komplexe Preshared Keys zum Einsatz kommen, kann ein Angreifer in kürzester Zeit mit frei erhältlichen Hilfsmitteln die Anmeldeinformationen ermitteln.

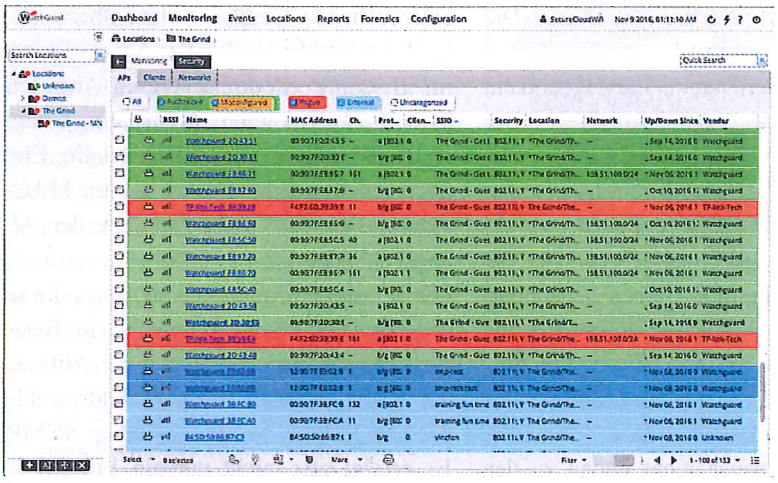
Wer demnach als Unternehmen einen Access Point (AP) mit nicht optimal konfigurierter Verschlüsselungstechnik einsetzt, öffnet auch einem darüber hinausgehenden Zugriff auf das physische Unternehmensnetzwerk Tür und Tor. Daran sind nicht zuletzt weitere Bedrohungsszenarien geknüpft wie beispielsweise das gezielte Einschleusen von Malware, das Mitschneiden und Abfangen von Kommunikation sowie böswilliger Datendiebstahl. Bei optimal segmentierten Netzwerken schaffen gängige UTM-Lösungen (Unified-Threat-Management) meist Abhilfe und beugen Übergriffen auf sensible Netzwerkbereiche vor – aber auch dort sind im Rahmen von WLAN-Infrastrukturen Grenzen gesetzt.

Rogue Hotspots als Quell vieler Übel

Hinsichtlich des WLAN-Schutzes kommt die Rede immer wieder auf die sicherheitskritischen „Rogue Hotspots", die es effektiv zu identifizieren und auszuschalten gilt. Denn diese können in vielerlei Hinsicht zur Bedrohung werden. Zum einen lassen sich darüber auf einfache Weise Man-in-the-Middle-Attacken steuern, bei denen Clients des WLANs unbemerkt auf manipulierte Seiten umgeleitet werden, die dazu dienen, vertrauliche Daten abzugreifen oder Malware beziehungsweise Ransomware zu streuen. In anderen Fällen ließe sich der feindliche Access Point dazu missbrauchen, über Wireless-DoS-Angriffe (Denial of Service) – also die Erzeugung eines hohen Datenvolumens – das WLAN zu blockieren oder zu stören.

Die Methoden der Angreifer, via Rogue AP Zugriff zum WLAN und darüber hinaus zu erhalten, sind facettenreich und ausgeklügelt. So gibt es beispielsweise die sogenannten „Honeypots". Bei dieser Methode werden fremde APs im Unternehmensumfeld platziert und mit der Firmen-SSID versehen. Danach muss der Angreifer nur noch abwarten, bis sich ein Client fälschlicherweise verbindet und somit das Fundament für vielfältige Manipulationen und die Ausnutzung von Schwachstellen legt. So lässt sich zum Beispiel Malware ins Netzwerk einschleusen, die einen späteren Remote-Zugriff ermöglicht.

Oder aber die Cyberkriminellen tarnen ihre eigenen Systeme durch im Netzwerk bekannte MAC-Adressen, die zuvor ausspioniert wurden, und verschaffen sich auf diesem Weg Zugang zu unternehmensinternen Daten. Im schlimmsten Fall sind die Rogue APs von Anfang an direkt mit dem physischen Netzwerk eines Unternehmens gekoppelt und treiben von dort ihr böses Spiel. Ein Extremfall, der durchaus Realität werden kann: Es reicht ein unbeobachteter Moment, um beispielsweise hinter



Die Klassifizierung der unterschiedlichen im WLAN identifizierten Access Points sollte intuitiv erkennbar sein. Bild: Watchguard Technologies

der Rezeption im Eingangsbereich eines Unternehmens einen eigenen Access Point an die LAN-Buchse des Druckers anzuschließen. Im Handumdrehen existiert ein unautorisierter Zugang zum physischen Netzwerk. Umso mehr zählt eine Lösung, die solche „Eindringlinge" erkennt und ein entsprechendes Eingreifen auf Unternehmensseite ermöglicht.

Unterschiedliche Klassifikationsverfahren

An dieser Stelle kommen Wireless Intrusion Detection Systems (WIDS) und – in der Weiterentwicklung – Wireless Intrusion Prevention Systems ins Spiel. Der Erkennung der jeweiligen Access Points im WLAN liegen von Anbieter zu Anbieter unterschiedliche Methoden zugrunde, und die Unterscheidung erfolgt entsprechend mehr oder weniger zuverlässig nach „Rogue" APs (nicht autorisierte, im LAN ohne Wissen des Administrators installierte APs), „autorisierten" APs (verwaltete APs im LAN, die der Administrator kennt) und „externen" APs (unverwaltete APs im drahtlosen Umfeld, die nicht mit dem überwachten LAN verbunden sind).

Ein durchaus gängiges Vorgehen ist die signaturgestützte Klassifikation. Dabei erfolgt die Einordnung auf der Basis benutzerseitig konfigurierter Klassifikationssignaturen, für die Unmengen von AP-Eigenschaften herangezogen werden – beispielsweise SSID, Anbieter, Leistungspegel, Verschlüsselungseinstellungen und Kanal. Die physische Netzwerkverbindung zwischen AP und Netzwerk kann, muss aber kein Faktor für die Klassifizierung sein. Der Nachteil: Die Signaturverwaltung erfordert einen hohen Konfigurationsaufwand. Zudem sind Signaturen regelmäßig zu aktualisieren – beispielsweise, wenn sich die bekannte Konfiguration eines benachbarten, harmlosen WLANs geändert hat und dort eine andere SSID zu Einsatz kommt.

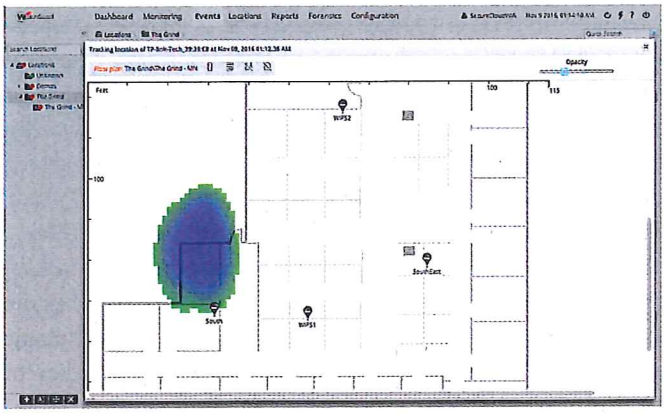
Ferner kann es durchaus vorkommen, dass WLAN-Konfigurationen neu erkannter APs möglicherweise nicht genau zu den definierten Signaturen passen. In diesem Fall ist ein manueller Eingriff erforderlich, um diese APs zu klassifizieren. Zudem lassen sich bei diesem Ansatz echte Bedrohungen häufig nicht erkennen. So würde beispielsweise eine Klassifikationssignatur wie „if ‚SSID = freewifi AND signal strength = Low'" zur Klassifikation eines bekannten benachbarten APs von einem Rogue AP mit geringer Übertragungsleistung und SSID-Konfiguration „freewifi" ausgehebelt.

Prüfungen anhand von MAC-Adressen

Ein weiteres Verfahren stellt die MAC-Tabellenprüfung dar: Es vergleicht MAC-Adressen von Geräten im WLAN mit den MAC-Adressen, die an den Ports von Managed Switches im LAN registriert sind. Wenn eine zwischen WLAN und LAN übereinstimmende MAC-Adresse auftaucht, erfolgt die Annahme, dass das entsprechende Gerät mit dem überwachten LAN verbunden ist. Bei Access Points im Bridging Mode ist dieser Abgleich jedoch erst möglich, wenn ein Client eine Verbindung zum AP herstellt: Erst dann registriert der Switch dessen MAC-Adresse an dem Port, 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 (Content-Addressable Memory) für jeden Switch über SNMP. Es erfolgt also nicht nur ein Eingriff in die Infrastruktur, sondern zur Abfrage der MAC-Tabellen der Switches ist zudem die Verwaltung der Switch-Kennungen im WIPS erforderlich. Aus diesem Grund sind MAC-Tabellenüberprüfungen für alle Managed Switches im Netzwerk eine ressourcenintensive und zeitaufwendige Aufgabe – besonders in großen Netzwerken mit Hunderten Switches. Die Erkennung mithilfe dieser Technik erfordert nicht zuletzt Glück: Denn sobald der Client inaktiv wird, verschwindet sein MAC-Eintrag aus der Tabelle. Bei einer entsprechenden Abfrage ist dieser Ansatz nur von Erfolg gekrönt, wenn der Client tatsächlich gerade mit dem Rogue AP verbunden ist.

Alternativ dazu setzen einige WIPSs auf passive MAC-Korrelation. Dabei hört der WIPS-Sensor seine kabelgebundene Schnittstelle passiv nach im Subnetz aktiven MAC-Adressen ab. Die ermittelten MAC-Adressen lassen sich für die MAC-Adressen-Korrelation auf LAN- und WLAN-Seite nutzen. Doch selbst bei diesem Ansatz kann das Problem auftreten, dass das System für nicht mit dem überwachten Netzwerk verbundene APs (beispielsweise benachbarte APs) fälschlicherweise eine Verbindung mit dem eigenen Netzwerk unterstellt. Dies passiert, wenn Clients zwischen den beteiligten APs wechseln.



Über Triangulation mithilfe der spezifischen WIPS-Sensoren und APs lässt sich der Standort des einzelnen identifizierten APs beziehungsweise Clients bestimmen. Bild: Watchguard Technologies

Auch die rein kabelseitige Verfolgung ist nicht zielführend. Bei dieser Technik versucht ein WIPS-Sensor, nachdem er einen AP im Netz ermittelt hat, LAN-seitig aktiv eine Verbindung zum AP herzustellen. Der WIPS-Sensor schickt dann entweder ein Ping-Signal über das drahtgebundene Netzwerk zum potenziellen Rogue AP oder er 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. Die aktive Verbindungsherstellung zum AP unterliegt jedoch 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-Sensor

auf die AP-Leitung fokussiert und kann die Scan-Funktion nicht ausführen. Erkennt das System viele potenzielle Rogue APs, dann lässt sich diese Methode daher nur unregelmäßig anwenden. Die Folge ist eine große Verzögerung bei der Ermittlung der AP-Verbindungen.

Hohe Quote an „False Positives"

Den bisher beschriebenen Verfahren ist eines gemeinsam: Selbst wenn sich alle im WLAN befindlichen APs erkennen lassen, ist die Quote der „False Positives" relativ hoch. Es kommt auch dann zu Sicherheitswarnungen, wenn ein unautorisierter AP erkannt wird, der jedoch nicht mit dem überwachten LAN verbunden ist und daher kein Risiko darstellt.

Ein modernerer Ansatz beruht auf dem Einsatz sogenannter „Marker"-Techniken. Dabei erfolgt die Klassifikation rein auf der Basis der Netzwerkverbindung des identifizierten APs. Marker-Pakete kommen in diesem Zusammenhang sowohl LAN- als auch WLAN-seitig zum Einsatz. Ihre Injektion ins LAN erfolgt über das Kabel des WIPS-Sensors, der entweder in einem Subnetz oder – bei mehreren Subnetzen – auf dem sogenannten Trunk-Port eines Managed Switches platziert ist. Diese Pakete übertragen dann APs, die mit dem überwachten LAN verbunden sind, ins WLAN. Die anschließende Erkennung erfolgt über Funk von der drahtlosen Seite des WIPS-Sensors.

Parallel dazu sendet der WIPS-Sensor, sobald er einen mit einem AP verknüpften Client im WLAN erkannt hat, Marker-Pakete mit einer eindeutigen Kennung von der drahtlosen Seite in Richtung der IP-Adresse eines bekannten LAN-Hosts. Diese Pakete werden 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. Die Klassifikation entsprechend der Kategorien „autorisiert", „Rogue" oder „extern" erfolgt automatisch.

Im Vergleich mit anderen Methoden ist diese Technik nicht nur zuverlässiger, sondern auch mit deutlich weniger manuellem Aufwand verbunden. Sie erfolgt unabhängig von Klassifikationssignaturen. Somit entfällt das direkte Zusammenspiel mit Netzwerk-Switches. Es sind lediglich eine zuverlässige Netzwerkverbindung und Zugriff auf die gewünschten VLANs erforderlich. Die Identifizierung erfolgt schnell und unabhängig von der Größe des Netzwerks, da jedes lokale Subnetz simultan gescannt wird. Der Umfang des durch „Packet Injection" erzeugten Datenverkehrs ist dabei durchaus vernachlässigbar (weniger als 0,1 Prozent der LAN-Port-Kapazität). Der entscheidende Vorteil dieses Verfahrens ist jedoch, dass Fehlalarme nahezu ausgeschlossen sind, da es Rogue APs nie als externe APs kennzeichnet und umgekehrt.

Erkennung ist Pflicht, Prävention die Kür

Die zuverlässige Klassifikation ist ein entscheidendes Kriterium, wenn es um die Ergreifung automatisierter Gegenmaßnahmen geht. Schließlich gilt es, unbedingt zu vermeiden, dass das WIPS Access Points, die eigentlich zu einem benachbarten WLAN gehören und fälschlicherweise als Rogue APs gekennzeichnet wurden, beispielsweise über Deauthentifizierungspakete oder eine Art DoS-Angriff stört beziehungsweise lahmlegt. In diesem Fall drohen sogar rechtliche Konsequenzen. Die Ergreifung sofortiger Abwehrmaßnahmen ist jedoch entscheidend, um Schaden vom eigenen Unternehmen abzuwenden. Bis ein erkannter Rogue Hotspot zuverlässig aus dem Netzwerk entfernt ist, sollte jegliche von ihm ausgehende Datenkommunikation effektiv gestört beziehungsweise unterbunden sein.

Idealerweise unterstützt ein WIPS in dabei auch die Ermittlung des Standorts des jeweiligen APs. Bei einer entsprechenden Menge an Sensoren lässt sich via Triangulation auf der Basis der Signalstärke des potenziell schädlichen Systems dessen Position metergenau bestimmen. In Kombination mit einer Gebäudegrafik ist die Suche schnell beendet.

Jonas Spieckermann/pf

Jonas Spieckermann ist Senior Sales Engineer bei Watchguard Technologies, www.watchguard.de.