Trusted Wireless Environment: Der Grundstein einer verantwortungsbewussten WLAN-Implementierung

Inhaltsverzeichnis

Eine **Trusted Wireless Environment** ist ein Konzept für den Aufbau eines WLAN, das schnell, leicht zu verwalten und vor allem sicher ist. Dieses Whitepaper befasst sich mit der Evolution der WLAN-Technologie und der damit einhergehenden Entwicklung der sechs bekannten Kategorien von WLAN-Bedrohungen: (1) Rogue-Access Point, (2) Rogue-Client, (3) benachbarter Access Point, (4) Ad-hoc-Netzwerk, (5) „Evil Twin"-Access Point und (6) fehlerhaft konfigurierter Access Point. Aus dem neuesten Miercom-Bericht geht deutlich hervor, welche Hersteller vor diesen sechs Bedrohungskategorien schützen, und welche Lösungen die neue **Trusted Wireless Environment** zur Verteidigung Ihrer Umgebung und zum Schutz Ihres Unternehmens rund um die Uhr unterstützen.

Evolution des WLAN

Mit dem Aufkommen internetfähiger Geräte sind auch die Sicherheitsrisiken in drahtlosen Umgebungen gestiegen. Im Jahr 2017 gab es 8,4 Milliarden verbundene Geräte. Diese Zahl soll laut dem Marktforschungsunternehmen Gartner bis 2020 auf 20,4 Milliarden ansteigen. Wenn drahtlose Geräte gehackt werden, können zahlreiche Probleme entstehen, darunter Denial-of-Service, unerlaubter Zugriff auf personenbezogene Daten und größere Infrastrukturausfälle – was Unternehmen einen großen Zeit- und Kostenaufwand verursacht. Hacker suchen sich bevorzugt das schwächste Glied der Sicherheitskette aus und können sich mithilfe leicht zugänglicher Werkzeuge und unzähliger Online-Anleitungsvideos ohne großen Aufwand in das WLAN einhacken. Selbst der unerfahrenste Hacker kann Ihren WLAN-Datenverkehr abfangen und wertvolle Daten von Smartphone, Tablet, Smartwatch oder Laptop stehlen. Schlimmer noch: Beim Eindringen in Ihr WLAN werden Ihre Unternehmensnetzwerke durch eingeschleuste Malware beschädigt und Anmeldedaten gestohlen. Dabei kann eine Summe von mehreren Millionen für Geldbußen und die Beseitigung von Schäden zusammenkommen.

Wusstest du schon...

1. **600.000 USD** = FCC-Geldstrafe gegen eine Hotelkette, deren drahtloses Sicherheitssystem die Auflagen nicht erfüllte[1]
2. **1 Mrd. USD** = geschätzte Kosten des WLAN-Verstoßes von TJ Maxx im Jahr 2005[2]

Die sechs bekannten Kategorien von WLAN-Bedrohungen

1. **Rogue-Access Points** sind mit dem autorisierten Netzwerk verbunden, in der Regel mit einer offenen SSID, sodass Angreifer die Perimetersicherheit umgehen können. Rogue-Access Points können ein physischer Access Point (AP) sein, oder auch ein Access Point, der in einer Software auf einem Computer erstellt und mit dem autorisierten Netzwerk verbunden wurde.

2. **Rogue-Clients** definiert man als Clients, die sich zuvor mit einem Rogue-Access Point oder einem anderen bösartigen Access Point im Bereich eines privaten Netzwerks verbunden haben. Dieser Client könnte von einer Vielzahl von Man-in-the-Middle (MitM)-Angriffen betroffen sein, so z. B. Ransomwürmern, Malware oder Backdoors zum Client.

3. **Benachbarte Access Points** sind unabhängige APs, die nicht von Netzwerkadministratoren kontrolliert werden. Sie bieten Zugriff über ein separates Netzwerk und können dazu verwendet werden, interne Sicherheits- oder Inhaltsfilterungsrichtlinien zu umgehen.

4. **Ad-hoc-Verbindungen** sind Peer-to-Peer-WLAN-Verbindungen zwischen Clients, die die Perimetersicherheit umgehen können und es Clients ermöglichen, Firewalls sowie Inhalts- und Sicherheitskontrollen zu umgehen.

5. **Evil Twin-Access Points** ahmen einen legitimen AP nach, indem sie seine SSID und seine eindeutige MAC-Adresse fälschen (Spoofing). Neben einem allgemein bekannten physischen Access Point greifen die Hacker auf Softwareprogramme zurück, die WLAN-Netzwerkadapter in Standard-Laptops und -Tablets oder bestimmte native mobile Geräte verwenden, um den physischen Fußabdruck zu minimieren und die Aufmerksamkeit weg von großen Antennen, Geräten oder Kabeln zu lenken.

6. **Fehlerhaft konfigurierte Access Points** sind mit Ihrem privaten Netzwerk mit einer Konfiguration verbunden, die nicht Ihren Sicherheitsrichtlinien entspricht und unsichere Verbindungen ermöglicht. Wenn beispielsweise Ihre WLAN-Sicherheitsrichtlinie in der Wi-Fi Cloud so konfiguriert ist, dass nur SSIDs auf Ihren autorisierten APs mit WPA2-Verschlüsselung gesendet werden dürfen, und ein Administrator versehentlich einen autorisierten AP zur Übertragung einer offenen, unverschlüsselten SSID falsch konfiguriert, gilt dieser AP als falsch konfiguriert.

1. http://www.networkcomputing.com/wireless/fcc-marriott-wifi-blocking-fine-opens-pandoras-box/2053001237
2. http://www.zdnet.com/article/tjxs-failure-to-secure-wi-fi-could-cost-1b/

Säulen einer Trusted Wireless Environment

Ihre WLAN-Systeme sind leider nicht mehr zeitgemäß. Ihre Mitarbeiter, Lieferanten und Gäste verlassen sich darauf, dass Sie für ihre Sicherheit sorgen. Und Sie sind dafür verantwortlich, dass Sie die WLAN-spezifischen Sicherheitsrisiken und deren Auswirkungen auf Ihr Unternehmen kennen. Als verantwortungsbewusstes Unternehmen entscheiden Sie, die Sicherheit Ihrer WLAN-Netzwerke zu erweitern, stellen aber fest, dass zahlreiche Anbieter wie Cisco Meraki, Aruba und Ruckus keine passenden Produkte anbieten.

Ihr Unternehmen benötigt Technologien und Lösungen, mit denen Sie eine umfassende Trusted Wireless Environment aufbauen können, die alle drei Kernanforderungen erfüllt – marktführende Leistung, skalierbares Management und nachgewiesene umfassende Sicherheit. Und Sie möchten außerdem vor allen sechs bekannten Kategorien von WLAN-Bedrohungen geschützt sein.

Eine Trusted Wireless Environment ist ein Konzept für den Aufbau eines WLAN, das schnell, leicht zu verwalten und vor allem sicher ist. Unternehmen stehen vor der Verantwortung, Trusted Wireless Environments zu schaffen und ihre Mitarbeiter und Kunden vor Hackern zu schützen, die die mangelnde oder gar nicht existente Sicherheit traditioneller WLAN-Netzwerke leicht ausnutzen können.

Unternehmen, die eine Trusted Wireless Environment anbieten, erfüllen diese drei Kernanforderungen:

1. **Marktführende Leistung:** Damit Ihre Umgebung mit der erforderlichen Geschwindigkeit, Vernetzung und Clientdichte unterstützt werden kann, sind Sie auf eine den Anforderungen entsprechende Leistung angewiesen. Dabei sollten Sie jedoch in keinem Fall Einbußen bei der Sicherheit hinnehmen.
2. **Skalierbares Management:** Aufgrund der einfachen Einrichtung und Verwaltung sollten Sie in der Lage sein, Ihr gesamtes WLAN – ob groß oder klein – über eine einzige Schnittstelle zu steuern und wichtige Prozesse zum Schutz Ihrer Umgebung und Ihrer Benutzer auszuführen.
3. **Nachgewiesene umfassende Sicherheit:** Zahlreiche Anbieter begnügen sich bei der Bereitstellung von WLAN-Sicherheit mit uneindeutigen Lösungen. Sie müssen die Gewissheit haben, dass Ihre Sicherheitslösung Ihr Unternehmen vor Angriffen auf das WLAN schützt und die folgenden Vorteile bietet:
   - Automatischer Schutz vor den sechs bekannten Kategorien von WLAN-Bedrohungen
   - Möglichkeit, dass legitime externe Access Points in derselben Umgebung betrieben werden können
   - Beschränkung der Möglichkeit, dass Benutzer eine Verbindung zu nicht zugelassenen WLAN-Access Points herstellen können

Miercom-Test und wichtige Erkenntnisse

Miercom – ein international anerkanntes Unternehmen, das Branchenberichte auf Grundlage praktischer Vergleichstests erstellt – hat kürzlich eine bahnbrechende, neuartige Reihe von Tests durchgeführt, um festzustellen, wie effektiv ein Access Point Echtzeitanwendungen wie Sprache, Video und Daten unterstützen und gleichzeitig die häufigsten WLAN-Sicherheitsbedrohungen erkennen und verhindern kann.

Für jede WLAN-Bedrohung wurde die Zeit erfasst, bis die Gefahren erkannt und abgewehrt waren. Dabei wurden WLAN-Geräte von WatchGuard, Aruba, Cisco Meraki und Ruckus verwendet.

Testdaten

Access Points, Firmware und Management-Plattformen, die in allen Tests verwendet wurden:

Anbieter	Access Point-Modell	Management-Plattform	Firmware
WatchGuard	AP420	Wi-Fi Cloud	8.5.0-658
Aruba	AP335	Aruba Central/Aruba Instant	8.3.0.0_64659
Cisco Meraki	MR53	Meraki Cloud Controller	MR 25.11
Ruckus	R710	Zone Director 1200	10.1.1.0

In jedem Testfall für eine WLAN-Bedrohung wurde IP-Multicast-Datenverkehr erzeugt, um die Access Points auszulasten. In einer realen Umgebung müssen APs in der Lage sein, sowohl die Clients zu bedienen als auch ausreichenden Sicherheitsschutz zu bieten, ohne die Qualität der Benutzererfahrung zu beeinträchtigen. Die Multicast-zu-Unicast-Konvertierung wurde in allen APs eingesetzt und diente insgesamt 18 Clients, davon 6 auf 2,4 GHz und 12 auf 5 GHz. Die Spektralanalyse wurde kontinuierlich durchgeführt: Keine anderen benachbarten APs verwendeten während der Prüfung Kanal 1 oder 149-153. Die Kanalauslastung lag während der Tests bei 60 % für 2,4 GHz und bei 40 % für 5 GHz.

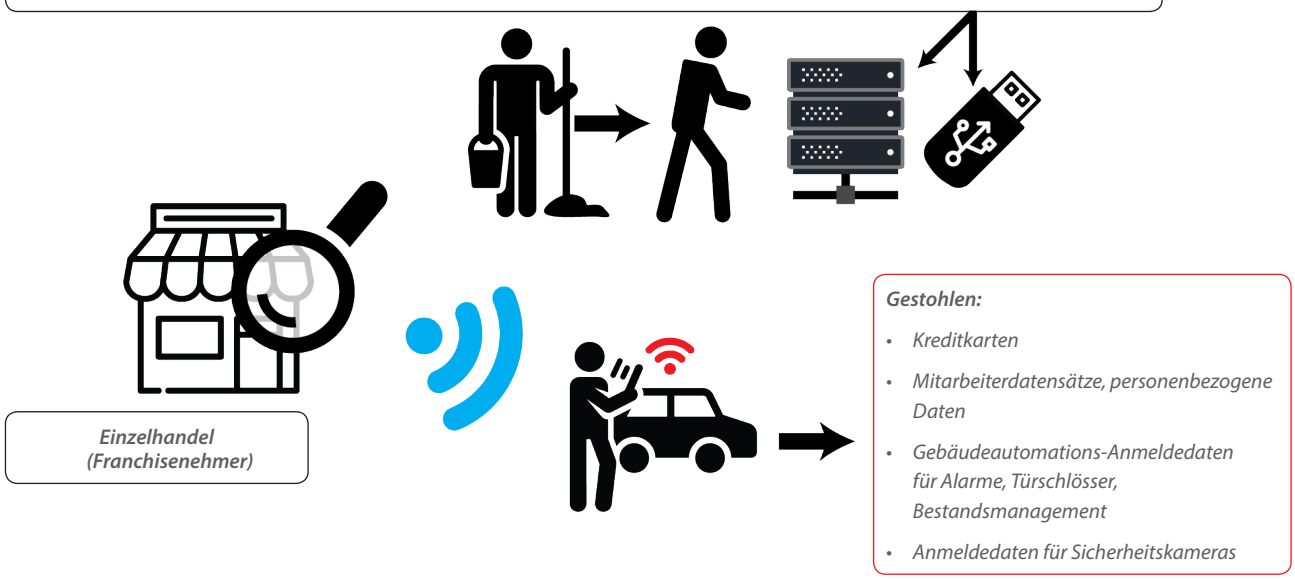
Client-Geräte, die für die kontinuierliche Generierung des Datenverkehrs bei allen WLAN-Bedrohungstests verwendet wurden:

- 18 – Acer-Laptops mit Qualcomm Atheros 1x1 Wave 2 WLAN-Fähigkeit und Windows 10-Betriebssystem

Rogue-AP – Testdaten

Rogue-APs sind eine gefährliche WLAN-Sicherheitsbedrohung, bei der ein AP von einer skrupellosen – häufig versteckte SSIDs sendenden – Person mit einem privaten Netzwerk verbunden wird, sodass Angreifer in Reichweite Zugriff auf interne Netzwerkressourcen erhalten können. Übliche Ziele sind z. B. Kreditkartendaten (CDE: Karteninhaberdatenumgebung) – sie stellen ein gravierendes PCI-Compliance-Risiko dar – und Bedienungselemente der Gebäudeautomation, z. B. für Alarme, Türschlösser und Videokameras.

Jeder, der Zugang zum „Kabelschrank" hat, kann einen winzigen Access Point einstecken und ihn im Kabelchaos verstecken. Ein solcher Rogue-AP sendet ein WLAN-Signal nach draußen an einen Angreifer, der dann in einem privaten Netzwerk wie einer Kreditkartendatenumgebung (CDE) auf Daten zugreifen könnte – ein klarer PCI-Verstoß. Nun befindet sich der Angreifer innerhalb des Netzwerks und könnte sich auch Zugang zu Systemen für Tür-/Beleuchtungs-/Alarm-/Bestandsmanagementsysteme verschaffen.



Clients, die bei Rogue-AP-Tests verwendet wurden:

- 1 – OnePlus2 QCA 1x1 Wave Android
- 1 – Samsung S2 Tab BCM 2x2 Wave 1 Android

AP, der als Rogue-AP verwendet wurde:

- Apple Airport Express*

** Bei zahlreichen WLAN-Sicherheitslösungen wird die MAC-Adressen-Korrelation verwendet, um Geräte im selben Netzwerk zu identifizieren. Der Apple AirPort AP, der in diesem Test als Rogue-AP verwendet wurde, weist eine Differenz von mehr als 5 Bit zwischen der drahtgebundenen und der drahtlosen Schnittstelle auf. Diese Abweichung kann u. U. dazu führen, dass ein Korrelationsalgorithmus fehlschlägt, was den AP in der drahtgebundenen Schnittstelle nicht nachweisbar und damit als Rogue-AP nicht erkennbar macht.*

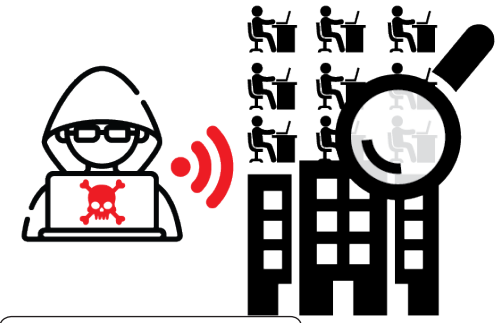
Testmethode:

1. Modus „Apple AirPort Open/NAT" konfigurieren
2. Apple AirPort mit dem Netzwerk des DUTs verbinden
3. Automatische Prävention aktivieren
4. Timer starten, sobald Apple AirPort SSIDs von NetSpot oder inSSIDer erkannt werden
5. Clients mit Apple AirPort verbinden (1 Client mit 2,4 GHz und 1 Client mit 5 GHz)
6. Von den Clients, die mit dem Rogue-AP verbunden sind: kontinuierliches Ping-Signal an drahtgebundenen Host senden
7. Ungefähre Zeit bis zur Gefahrenerkennung und -abwehr durch WIPS aufzeichnen (maximal 10 Minuten zulässig)

Rogue-Client – Testdaten

Jeder Client, der zuvor mit einem Rogue-AP oder einem anderen bösartigen AP in Reichweite eines privaten WLAN-Netzwerks verbunden war, gilt als Rogue-Client. Dieser Client könnte von einer Vielzahl von Man-in-the-Middle (MitM)-Angriffen betroffen sein, so z. B. Ransomwürmern, Malware oder Backdoors zum Client.

In einem Client, der Opfer eines WLAN-Angriffs – z. B. eines Karma-Angriffs – wurde (im Büro oder in Reichweite eines schwachen WIPS), können jetzt Ransomware, Malware und Backdoors installiert sein, die nun versuchen werden, auch das restliche Büro anzugreifen. Das nennt man „Rogue-Client".



Büroangestellte in Gebäuden

Während des Mittagessens wurde auf dem Laptop des Mitarbeiters ein Ransomwurm von einem sich in der Nähe des Gebäudes befindlichen Karma-Angreifer geladen. Der Mitarbeiter hat sich gerade eingeloggt und die Ransomware beginnt, sich zu verbreiten ... Hilfe!!!!

Clients, die bei Rogue-Client-Tests verwendet wurden:

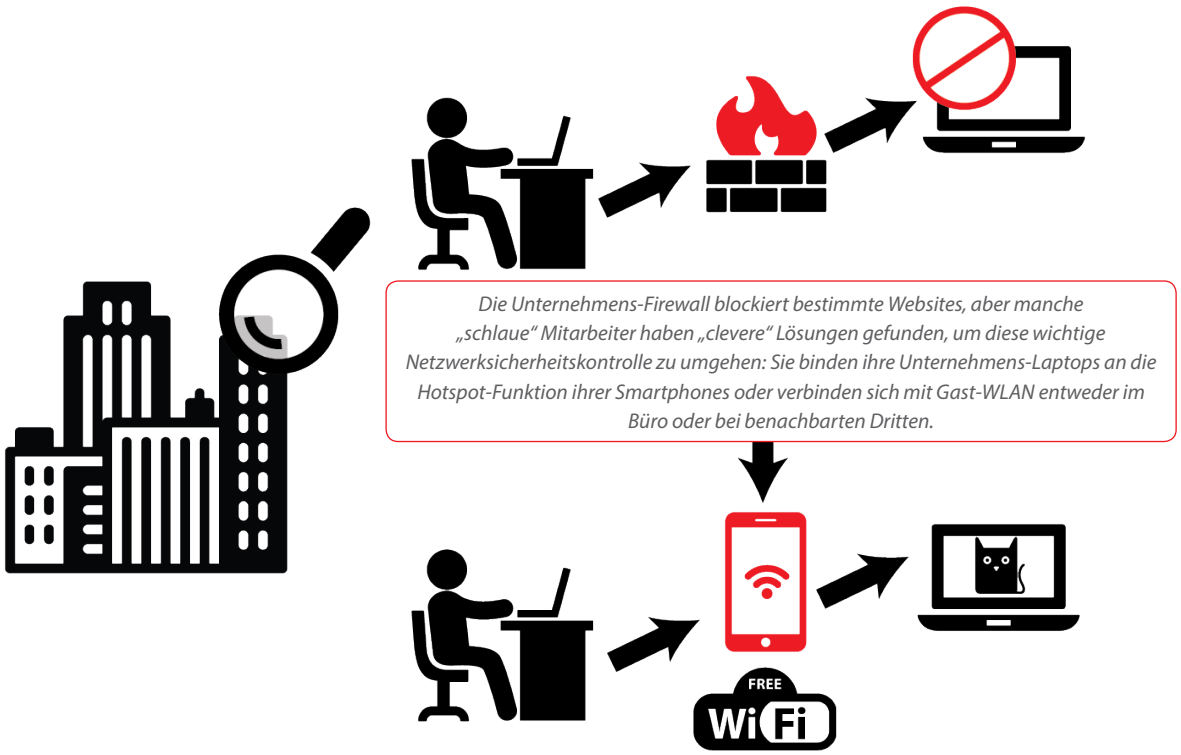
- 1 – Samsung S2 Tab BCM 2x2 Wave 1 Android

Testmethode:

1. Mit einem nicht kategorisierten Client starten
2. Rogue-AP aufrufen (z. B. Apple-Rogue und/oder AP, der durch die MAC-Nachbarschaft für DUT erkennbar ist, der den Apple AirPort nicht als „Rogue" erkennen kann)
3. Nicht kategorisierten Client mit Rogue-AP verbinden
4. Bestätigen, dass Rogue-AP vom DUT als „Rogue" erkannt wurde
5. Prüfen, ob der nicht kategorisierte Client nun als Rogue-Client erkannt wird
6. Rogue-Client vom Rogue-AP trennen
7. Automatische Prävention in DUT aktivieren
8. Client mit dem autorisierten AP verbinden und Ping-Signal kontinuierlich an drahtgebundenen Host senden
9. Timer starten, sobald sich der Rogue-Client mit dem autorisierten AP verbindet
10. Ungefähre Zeit bis zur Gefahrenerkennung und -abwehr durch WIPS aufzeichnen (maximal 10 Minuten zulässig)

Benachbarter AP (fehlerhafter Client) – Testdaten

In Umgebungen wie Büros, Flughäfen, Gesundheitseinrichtungen, Einzelhandelsgeschäften und Restaurants befinden sich häufig zahlreiche unternehmenseigene WLAN-Client-Geräte, die sich nur mit unternehmenseigenen SSIDs verbinden dürfen, sodass Netzwerksicherheitskontrollen, Verschlüsselung und Transparenz des Datenverkehrs gewährleistet werden können. Öffentliche Gast-Clients werden dagegen nicht vom Unternehmen verwaltet. In diesen Umgebungen dürfen unternehmensverwaltete WLAN-Clients unter keinen Umständen eine Verbindung zu benachbarten SSIDs von Drittanbietern oder sonstigen Stellen herstellen dürfen. Eine solche Verbindung würde alle wichtigen Netzwerksicherheitskontrollen umgehen und die Transparenz des Datenverkehrs für Netzwerkadministratoren verhindern. So darf sich beispielsweise das Handkartenlesegerät eines Restaurants, das über WLAN betrieben wird, nur mit der unternehmensintern verwalteten SSID innerhalb des Restaurants verbinden – und nicht mit benachbarten öffentlichen Hotspots oder mobilen bzw. LTE-WLAN-Hotspots, die häufig nicht verschlüsselt und leichte Beute für Angreifer sind. Ein weiterer, häufig vorkommender Fall sind „schlaue" Mitarbeiter, die unternehmenseigene Smartphones, Laptops und Tablets mit nahegelegenen öffentlichen WLAN-Hotspots oder internen Gast-WLAN-SSIDs verbinden, um Web-Content-Filterungskontrollen zu umgehen.



Die Unternehmens-Firewall blockiert bestimmte Websites, aber manche „schlaue" Mitarbeiter haben „clevere" Lösungen gefunden, um diese wichtige Netzwerksicherheitskontrolle zu umgehen: Sie binden ihre Unternehmens-Laptops an die Hotspot-Funktion ihrer Smartphones oder verbinden sich mit Gast-WLAN entweder im Büro oder bei benachbarten Dritten.

Clients, die im Test für benachbarte APs verwendet wurden:

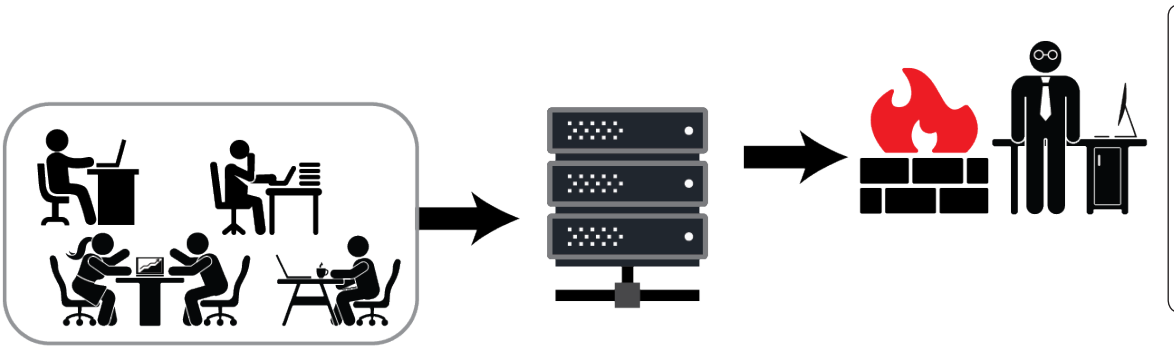
2 – Samsung S2 Tab BCM 2x2 Wave 1 Android

Testmethode

1. Autorisierte SSID hinzufügen
2. Überprüfen, ob der AP in der Benutzeroberfläche als autorisierter AP aufgeführt ist
3. Client mit dem autorisierten AP verbinden
4. Überprüfen, ob der Client in der Benutzeroberfläche als autorisierter Client aufgeführt ist
5. Benachbarten AP aufrufen (z. B. Mobile HotSpot)
6. Automatische Prävention in DUT aktivieren
7. Einen benachbarten Client mit benachbartem AP verbinden und Ping-Signal kontinuierlich an drahtgebundenen Host senden
8. Autorisierten Client mit benachbartem AP verbinden und Ping-Signal kontinuierlich an drahtgebundenen Host senden
9. Timer starten, sobald sich der autorisierte Client mit dem benachbarten AP verbindet
10. Ungefähre Zeit bis zur Gefahrenerkennung und -abwehr durch WIPS aufzeichnen (maximal 10 Minuten zulässig)

Ad-hoc-Netzwerk – Testdaten

In bestimmten Umgebungen kann es ein Sicherheitsrisiko darstellen, wenn sich WLAN-Clients direkt miteinander verbinden. Grund dafür ist, dass der in dieser Peer-to-Peer-Sitzung erzeugte Datenverkehr für Netzwerkadministratoren unsichtbar ist.



Netzwerkadministratoren möchten, dass der Datenverkehr der Mitarbeiter im Netzwerk stattfindet, denn auf diese Weise können sie alle Inhaltskontroll-, Datenprüfungs- und Zugriffskontrollrichtlinien gewährleisten.

Diese Mitarbeiter wollten Dateien einfacher und schneller versenden, indem sie ihre Laptops drahtlos miteinander verbinden. Aber dieser Datenverkehr ist für Netzwerkadministratoren völlig unsichtbar und kann ein ernsthaftes Sicherheitsrisiko darstellen.

Geräte, die im Test für Ad-hoc-Netzwerke verwendet wurden:

1 – MacBook Air BCM 2x2 Wave 1 MacOS (als Ad-hoc-AP)

1 – Acer Laptop mit Qualcomm Atheros 1x1 Wave 2 und Windows 10-Betriebssystem (als Client)

Testmethode:

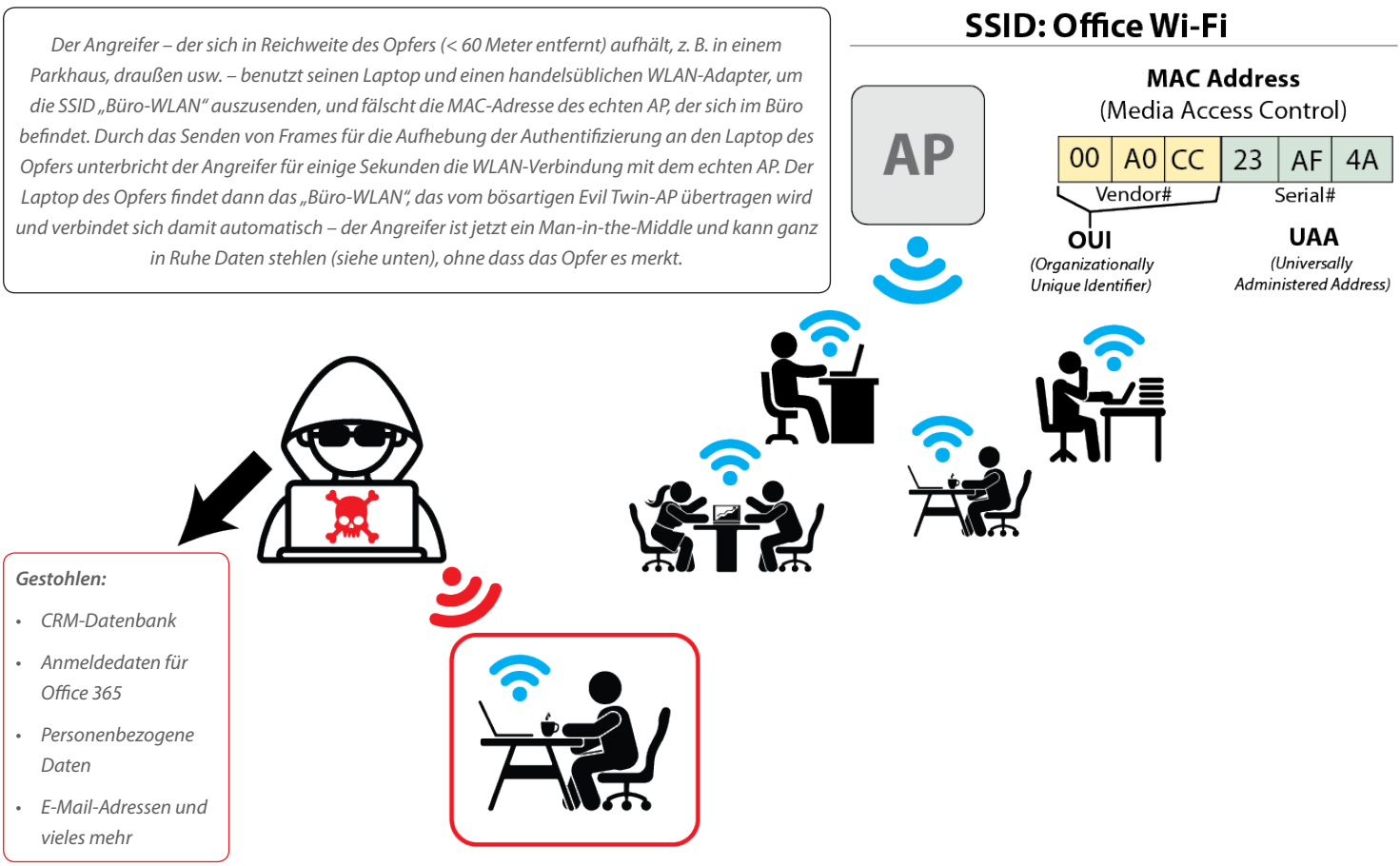
1. Ad-hoc-AP erstellen
2. Automatische Prävention aktivieren
3. Autorisierten Client mit Ad-hoc-AP verknüpfen und Ping-Signal kontinuierlich an drahtgebundenen Host senden
4. Timer starten, sobald Ad-hoc-SSID von NetSpot oder inSSIDer erkannt wird
5. Ungefähre Zeit bis zur Gefahrenerkennung und -abwehr durch WIPS aufzeichnen (maximal 10 Minuten zulässig)

Evil Twin-APs – Testdaten

Evil Twin-APs sind äußerst gefährlich, da die Opfer derartiger Angriffe in der Regel nicht ahnen, dass alle über das WLAN gesendeten Daten von einem Angreifer abgefangen werden und der Datenverkehr für alle Netzwerksicherheitskontrollen unsichtbar ist. Der Angreifer geht dabei keine großen Risiken ein, da in der Regel keine auf den Täter hinweisenden Spuren hinterlassen werden. Ein Evil Twin ist ein AP, bei dem der Angreifer denselben SSID-Namen wie ein legitimer AP in Reichweite kopiert und sendet, häufig die MAC-Adresse des legitimen APs fälscht (Spoofing) und damit eine „bösartige" Kopie des echten AP erzeugt. Die WLAN-Clients der Angriffsopfer verbinden sich automatisch mit bösartigen Evil Twin-APs, da keine offensichtlichen Unterschiede zwischen dem echten AP und dem bösartigen AP bestehen. Sobald die Verbindung mit einem Evil Twin-AP hergestellt ist, wird der erzeugte Datenverkehr durch einen „Man-in-the-Middle" geleitet, sodass der Angreifer sensible Informationen abfangen und Pakete in den Datenstrom einbringen kann, um die Kommunikation zu verändern.

Diese Büroangestellten arbeiten unermüdlich an ihren WLAN-fähigen Laptops. Die Geräte sind alle mit dem Access Point (AP) verbunden, der mit der SSID „Büro-WLAN" verknüpft ist.

Der Angreifer – der sich in Reichweite des Opfers (< 60 Meter entfernt) aufhält, z. B. in einem Parkhaus, draußen usw. – benutzt seinen Laptop und einen handelsüblichen WLAN-Adapter, um die SSID „Büro-WLAN" auszusenden, und fälscht die MAC-Adresse des echten AP, der sich im Büro befindet. Durch das Senden von Frames für die Aufhebung der Authentifizierung an den Laptop des Opfers unterbricht der Angreifer für einige Sekunden die WLAN-Verbindung mit dem echten AP. Der Laptop des Opfers findet dann das „Büro-WLAN", das vom bösartigen Evil Twin-AP übertragen wird und verbindet sich damit automatisch – der Angreifer ist jetzt ein Man-in-the-Middle und kann ganz in Ruhe Daten stehlen (siehe unten), ohne dass das Opfer es merkt.



Geräte, die im Test für Evil Twin-APs verwendet wurden:

1 – Samsung S2 Tab BCM 2x2 Wave 1 Android (Client)

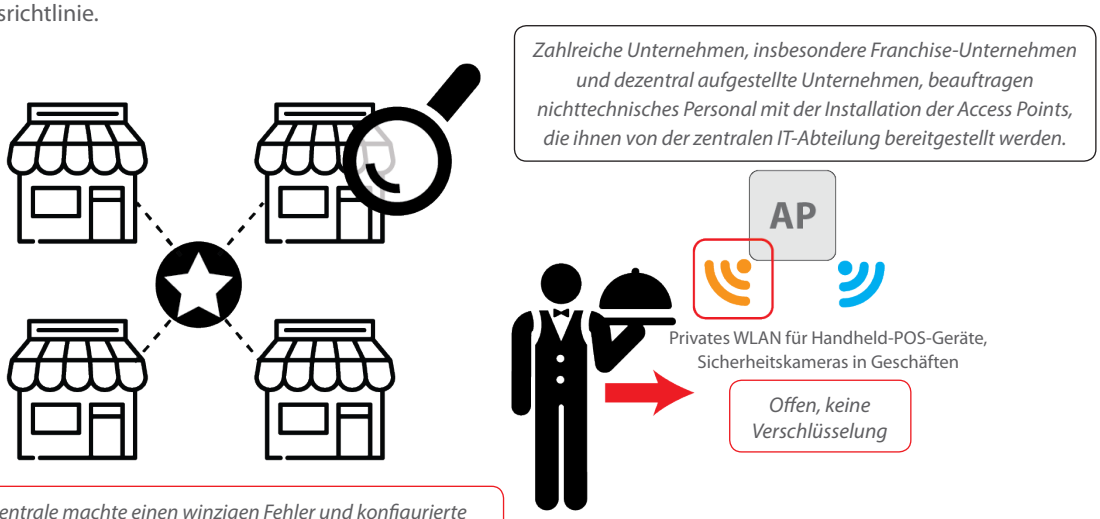
1– Wi-Fi Pineapple Tetra von Hak5 (Evil Twin-AP für das Spoofing von SSID und MAC)

Testmethode:

1. SSID zum Evil Twin-AP hinzufügen
2. Sicherstellen, dass die SSID nur im 5-GHz-Band aktiviert ist
3. Überprüfen, dass die nicht bösartige Instanz des Evil Twin-AP in der Benutzeroberfläche als „autorisiert" erkannt wird
4. Automatische Prävention in DUT aktivieren
5. Wi-Fi Pineapple AP Spoofer im 2,4 GHz-Band aktivieren (nur SSID)
6. Timer starten, sobald Evil Twin-AP von NetSpot oder inSSIDer erkannt wird
7. Einen Client der nicht bösartigen Instanz des Evil Twin-AP zuordnen, der gefälscht werden soll, und Ping-Signal kontinuierlich an drahtgebundenen Host senden
8. Einen Client dem gefälschten Evil Twin-AP zuordnen, und Ping-Signal kontinuierlich an drahtgebundenen Host senden
9. Ungefähre Zeit bis zur Gefahrenerkennung und -abwehr durch WIPS aufzeichnen (maximal 10 Minuten zulässig)

Fehlerhaft konfigurierter AP – Testdaten

In stark frequentierten Netzwerken, in denen neue APs bereitgestellt werden, ist es nicht unüblich, dass Netzwerkadministratoren versehentlich Konfigurationsfehler begehen, wie z. B. das Öffnen einer privaten SSID ohne Verschlüsselung, wodurch sensible Informationen von Angreifern abgefangen werden könnten.
Bei einem fehlerhaft konfigurierten AP entspricht die Konfiguration – beispielsweise eine Konfiguration mit Verschlüsselungsanforderungen – nicht der Netzwerksicherheitsrichtlinie.



Clients, die im Test für fehlerhaft konfigurierte APs verwendet wurden:

1 – Samsung S2 Tab BCM 2x2 Wave 1 Android

Testmethode:

1. Eine SSID mit offener Sicherheit unter Verwendung desselben SSID-Namens wie eine autorisierte SSID mit WPA2/PSK-Sicherheit hinzufügen
2. Automatische Prävention aktivieren
3. Einen Client dem richtig konfigurierten AP (WIPS-Test/WPA2PSK) zuordnen, und Ping-Signal kontinuierlich an drahtgebundenen Host senden
4. Einen Client dem fehlerhaft konfigurierten AP (WIPS-Test/offen) zuordnen, und Ping-Signal kontinuierlich an drahtgebundenen Host senden
5. Timer starten, sobald sich der Client mit dem fehlerhaft konfigurierten AP verbindet
6. Ungefähre Zeit bis zur Gefahrenerkennung und -abwehr durch WIPS aufzeichnen (maximal 10 Minuten zulässig)

Gleichzeitige Bedrohungen – Testdaten

Überfüllte Orte wie Konferenzzentren, Bahnhöfe, Flughäfen und Konzerte sind der perfekte Ort für Hacker – dort können sie ein WLAN aus allen Richtungen angreifen. Derart betriebsame Umgebungen sind gut für Angreifer geeignet – sie wissen, dass die Menschen dort normalerweise unter Zeitdruck stehen und von ihrer Umgebung abgelenkt werden.

Geräte, die im Test für gleichzeitige Bedrohungen verwendet wurden:

- 1 – OnePlus2 QCA 1x1 Wave Android
- 6 – Samsung S2 Tab BCM 2x2 Wave 1 Android
- 1 – MacBook Air BCM 2x2 Wave 1 MacOS (als Ad-hoc-AP)
- 1 – Acer Laptop mit Qualcomm Atheros 1x1 Wave 2 und Windows 10-Betriebssystem (als Client)
- Wi-Fi Pineapple Tetra von Hak5 (Evil Twin-AP für das Spoofing von SSID und MAC)
- Apple Airport Express (als Rogue AP)

Testmethode:

1. Automatische Prävention deaktivieren
2. Alle sechs Bedrohungen gleichzeitig aktivieren
3. Alle Clients zuordnen und kontinuierliche Pings an Host starten
4. Automatische Prävention aktivieren
5. Ungefähre Zeit bis zur Gefahrenerkennung und -abwehr durch WIPS aufzeichnen (maximal 10 Minuten zulässig)

Testergebnisse

	WatchGuard AP420		Aruba IAP335		Cisco Meraki MR53		Ruckus R710	
Test	**Erkennung**	**Prävention**	**Erkennung**	**Prävention**	**Erkennung**	**Prävention**	**Erkennung**	**Prävention**
Rogue-AP	P	P	F	–	F	MP	F	–
Rogue Client	P	P	F	–	F	MP	–	MP
Benachbarter AP	P	P	P	P	F	–	F	–
Ad-hoc-Netzwerk	P	P	F	–	F	–	P	–
„Evil Twin"-AP	P	P	P	F	P	MP	P	F
Fehlerhaft konfigurierter AP	P	P	P	–	–	–	–	–
Gleichzeitige Bedrohungen	P	P	F	F	F	F	F	F

Den vollständigen Miercom-Bericht finden Sie hier: **www.watchguard.com/wifi-security-report**

P = Pass (Bestanden)
F = Fail (Nicht bestanden)
MP = Marginal Pass (Knapp bestanden)
N/A = Funktion nicht unterstützt

Wichtige Erkenntnisse für WatchGuard

- Einziger Anbieter, der die sechs bekannten Kategorien von WLAN-Bedrohungen ohne Leistungseinbußen automatisch erkennt und bekämpft
- Einziger Anbieter, der automatische Erkennung und Prävention von Rogue APs und Rogue Clients unterstützt
- Einziger Anbieter, der automatische Erkennung und Verhinderung von Endpunkten bei der Kommunikation über eine Ad-hoc-WLAN-Verbindung unterstützt
- Einziger Anbieter, der automatische Verhinderung von Verbindungen zu „Evil Twins" und gefährlichen Verbindungen zu fehlerhaft konfigurierten APs wie privaten SSIDs ohne Verschlüsselung unterstützt

Weitere Informationen de.trustedwirelessenvironment.com

Über WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Netzwerksicherheit, sicheres WLAN, Multifaktor-Authentifizierung und Network Intelligence. Beinahe 10.000 Vertriebspartner und Dienstanbieter im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Dienste des Unternehmens, um mehr als 80.000 Kunden zu schützen. Die Philosophie von WatchGuard ist es, Sicherheit auf Enterprise-Niveau für Unternehmen jeder Größenordnung und Art zu realisieren. Das macht WatchGuard insbesondere für kleine und mittlere sowie dezentral aufgestellte Unternehmen zum idealen Anbieter. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter **WatchGuard.de**.

Deutschland, Österreich, Schweiz: +49 700 92229333 INTERNATIONALER VERTRIEB +1 206 613 0895 www.watchguard.de