Emotet attackiert WLAN Netze!

Schützen Sie Ihre Umgebung mit einem Trusted Wireless Environment

Jonas Spieckermann
Senior Sales Engineer

Jonas.Spieckermann@watchguard.com

14.12.2017 Monero in Buenos Aires

Starbucks-WLAN kapert Rechner zum Schürfen nach Digitalwährung

Dragonblood

DRAGONBLOOD

Sicherheitslücken in WPA3

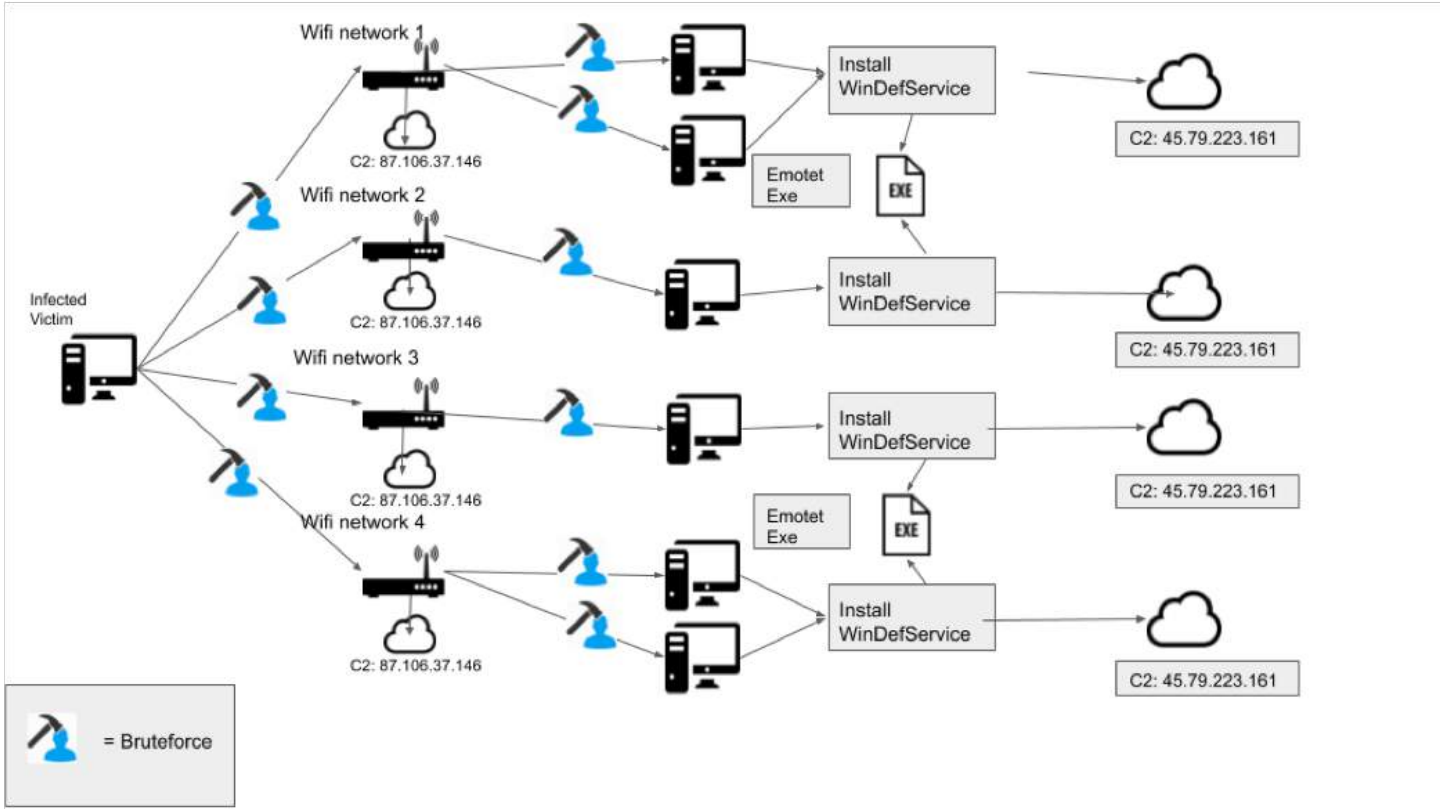
Eigentlich sollte WPA3 vor Angriffen wie Krack schützen, doch Forscher konnten gleich mehrere Schwachstellen im neuen WLAN-Verschlüsselungsprotokoll finden. Über diese konnten sie das Verschlüsselungspasswort erraten.

15. April 2019, 17:08 Uhr, Moritz Tremmel

(Bild: Lilawind/Pixabay)

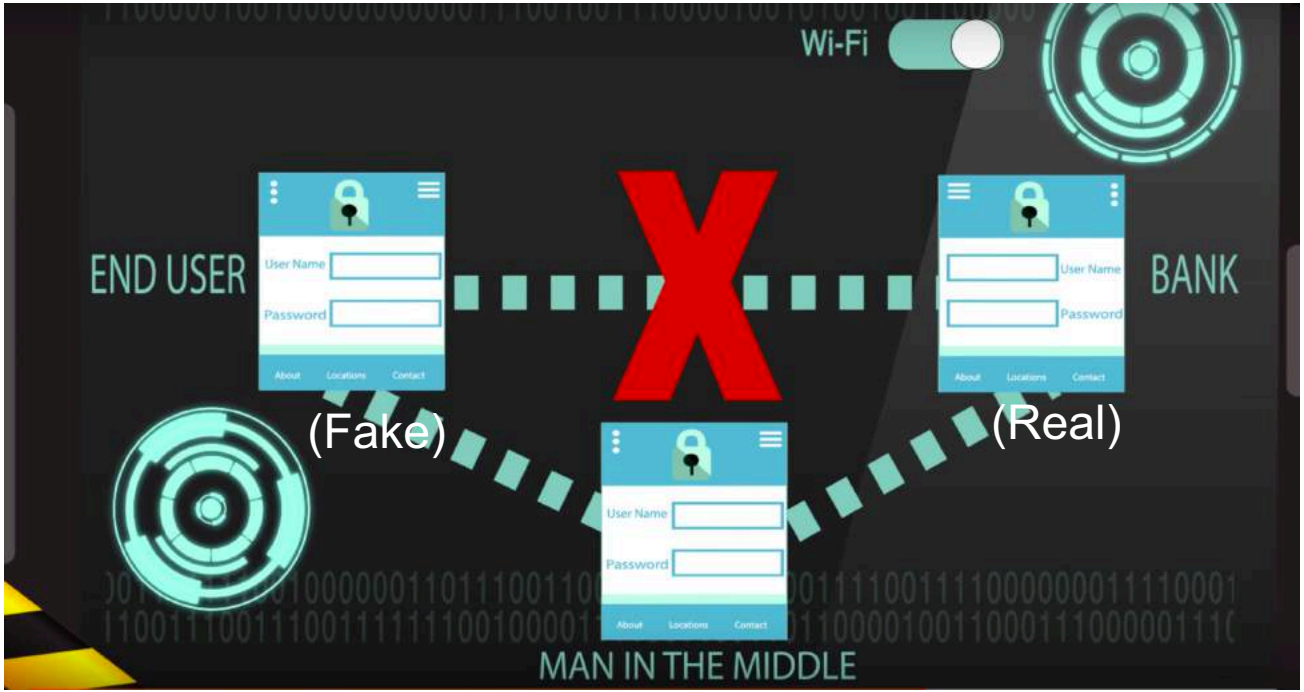
WPA3 und die Drachen: mit Dragonblood gegen Dragonfly.

Emotet verbreitet sich auch über das WLAN



Quelle: https://www.binarydefense.com/emotet-evolves-with-new-wi-fi-spreader/

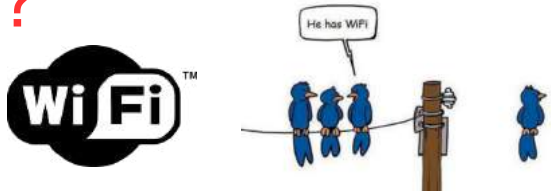
Ist WLAN sicher?

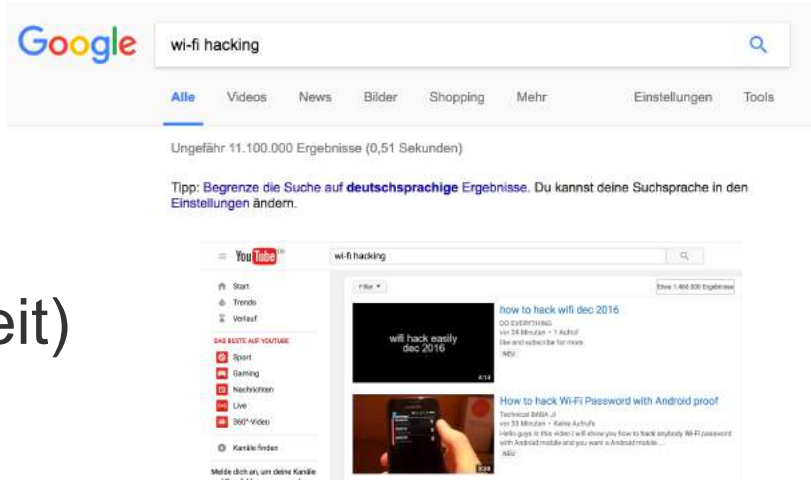


Jonas Spieckermann
Senior Sales Engineer
Jonas.Spieckermann@watchguard.com

Wie werde ich zum “WLAN Hacker“?

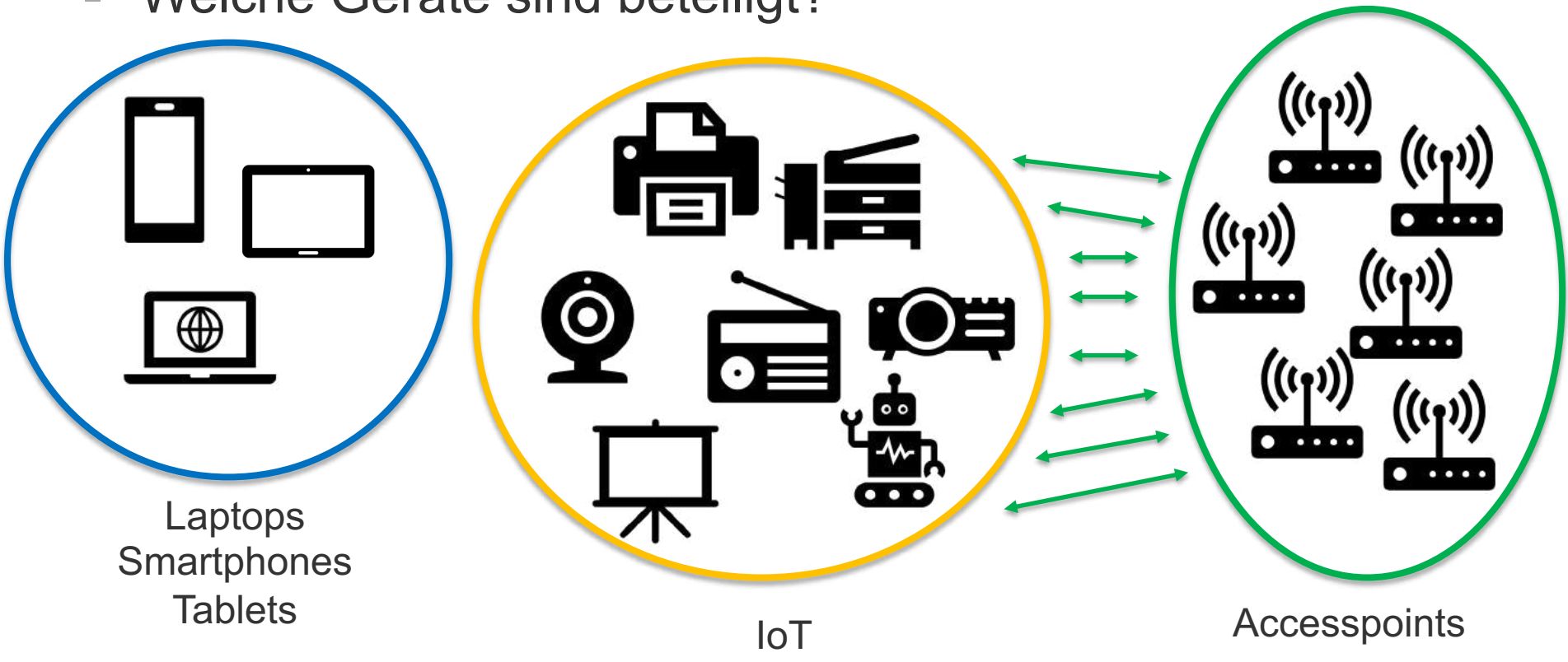
- Grundlegende Wi-Fi Kentnisse
- Online Tutorials
- Video Anleitungen
  - Über 1.000.000 Anleitungen bei Youtube zu „Wi-Fi Hacking“
- geringe Investition (Geld und Zeit)
  - Frei verfügbare Software
  - Standard Wi-Fi Hardware



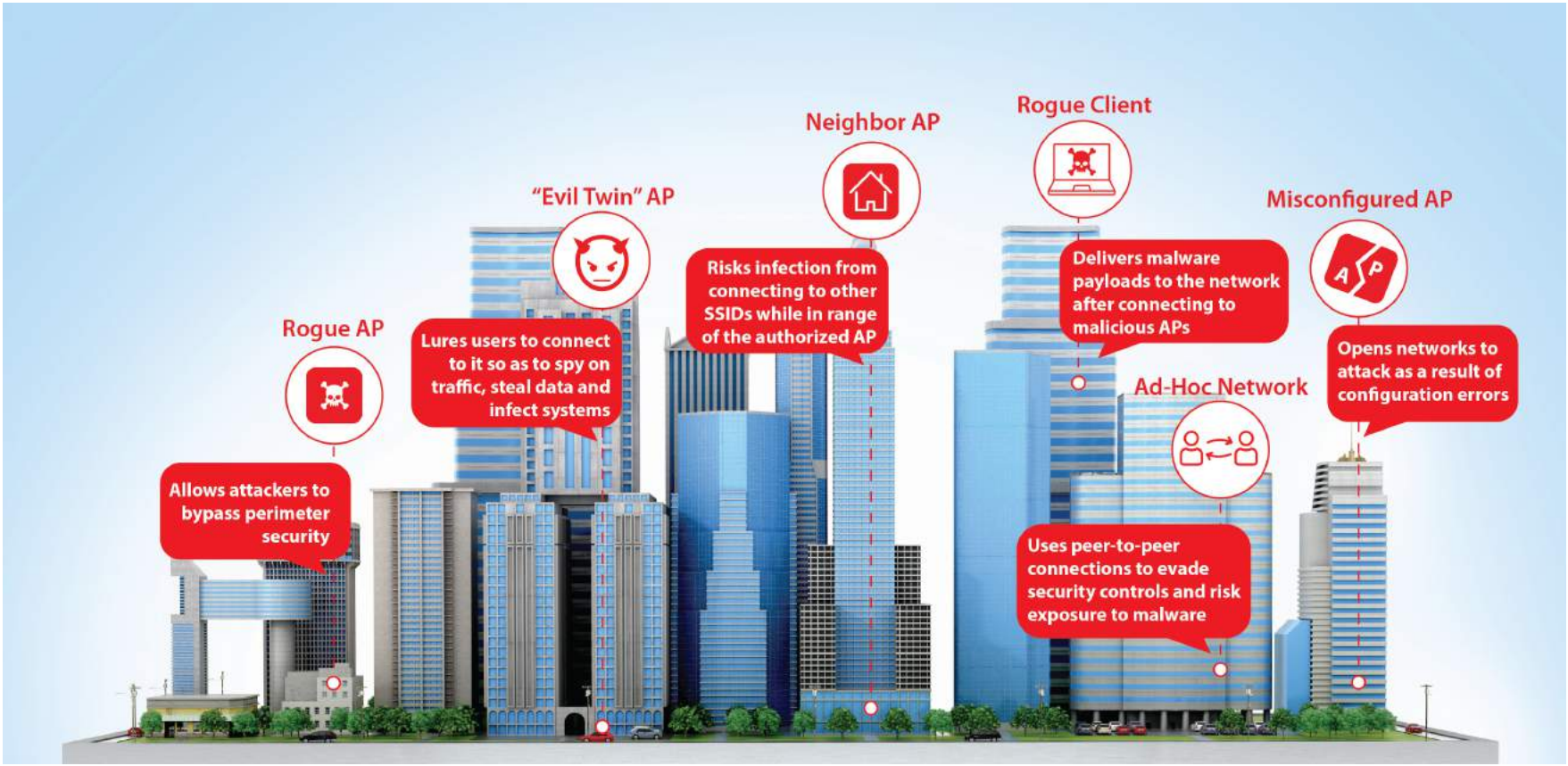


Grundlagen WLAN

- Welche Geräte sind beteiligt?



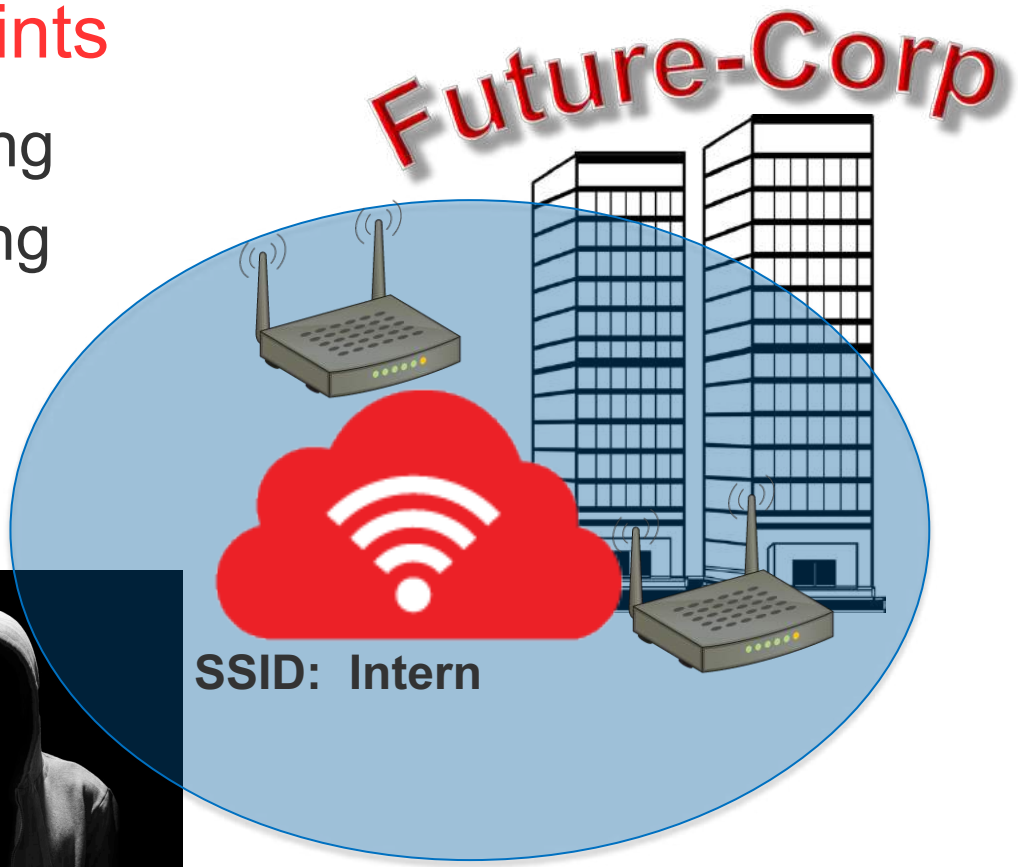
6 bekannte Gefahren für Wi-Fi im Firmenumfeld




Schwachstellen WLAN Infrastruktur

Angriff auf Accesspoints

- Analyse der Umgebung
- Störung der Umgebung
- Pakete mitschneiden
  - WPA Handshake
- PSK cracken
  - Offline
- Zugriff auf das Wi-Fi Netz



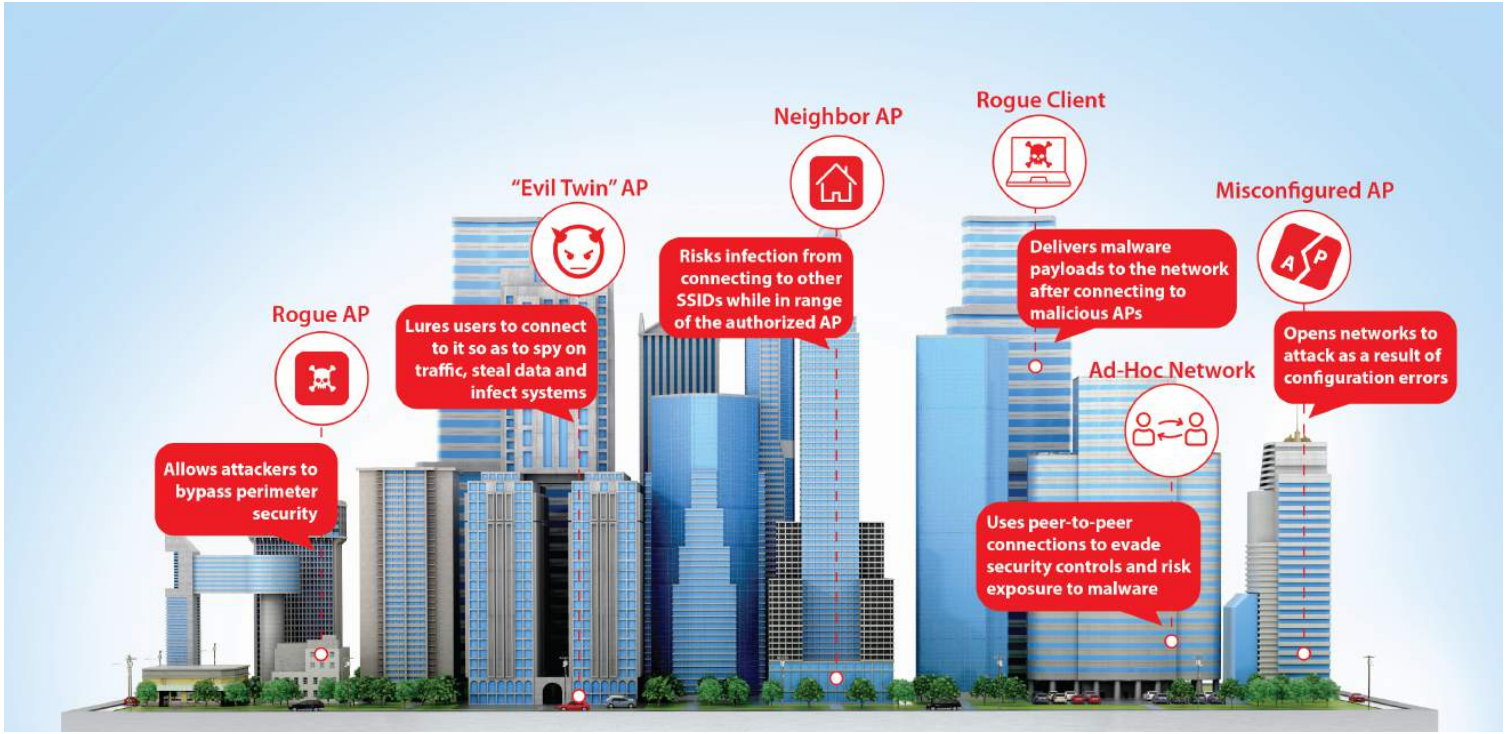
Rogue AP

- Ein nicht verwalteter oder unbekannter Accesspoint, der eine LAN-Verbindung hat

Fehlkonfiguration bestehender Accesspoints

- Schwache und veraltete Verschlüsselung
- VLAN Konfiguration
  - Gast-Netz ist “plötzlich“ im internen LAN
- PSK statt 802.1x
- Station Isolation
  - Nicht durchgehend konfiguriert
  - Teils wirkt diese Option nur pro Accesspoint

Live Demo



Schwachstellen und Angriffe bei Wi-Fi Clients

Grundlage: Wi-Fi Clients

Ist hier „Future-Corp Private“ ?

Ist hier „Free Hotspot“ ?

Ist hier „Home Network“ ?

Ist hier „Hotel ABC“ ?

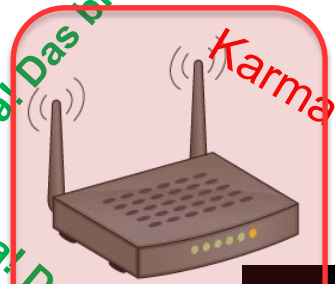
SSID Spoofing

Man-in-the-Middle

Karma Attack

Ja! Das bin ich!

Ja! Das bin ich!



Grundlage: Man-in-the-Middle

Online Banking
Social Media
Webmail
File Sharing
Video Streaming
Corporate Access
Collaboration

Hacking Gadgets

Mit speziellen Hacking-Gadgets sind Angriffe auf Rechner, Smartphones und Netzwerke leicht wie nie. c't hat 15 der frei verkäuflichen Geräte im Labor von der Leine gelassen.

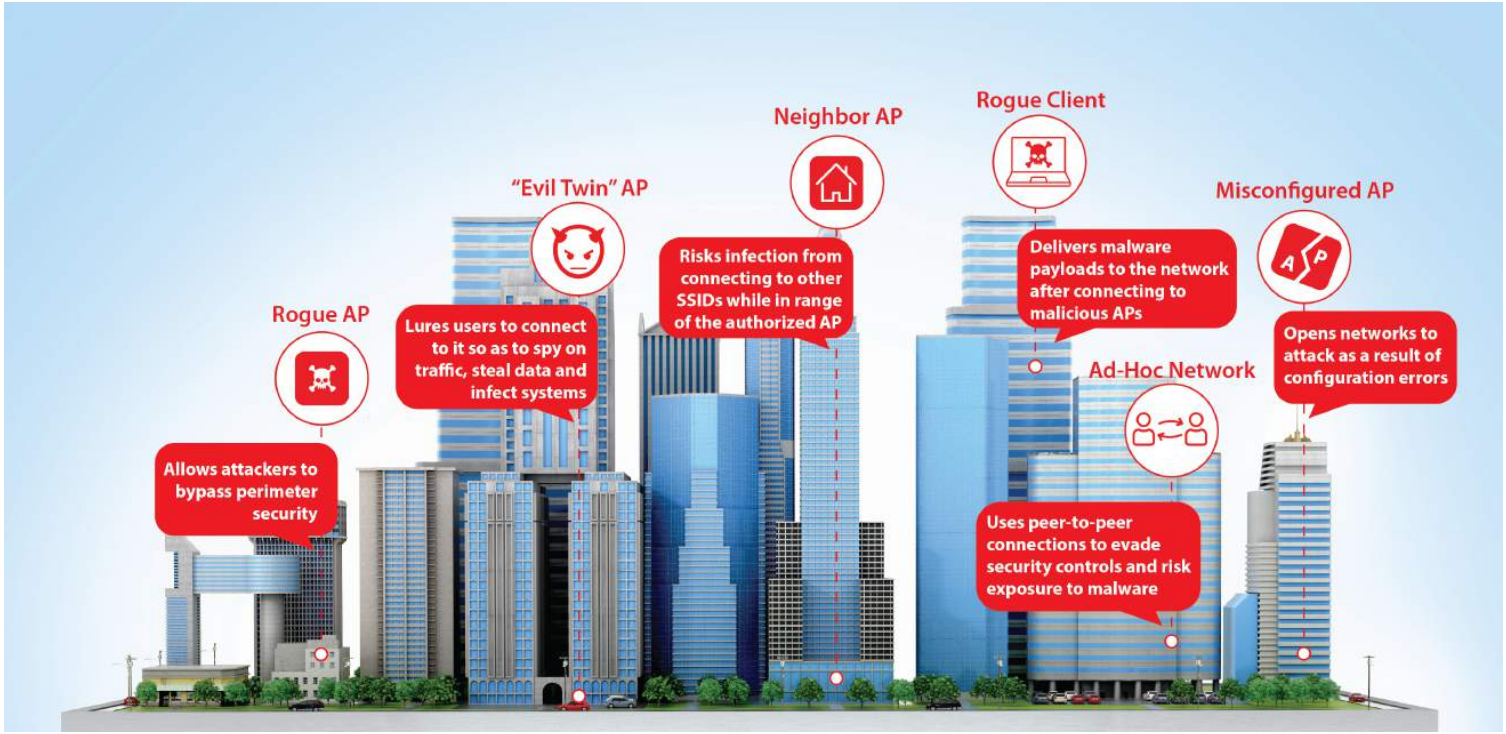
Für eine Handvoll Dollar bieten Online-Shops spezielle Geräte an, die sich für perfide Angriffe auf Rechner, Smartphones und Netzwerke eignen. Diese Hacking-Gadgets nutzen die Schwächen von USB, WLAN, Bluetooth und NFC aus, um Backdoors einzurichten, Daten abzugreifen oder gar Hardware dauerhaft zu zerstören. Penetration Tester nutzen diese Gadgets, um Sicherheitslücken in der Infrastruktur ihrer Auftraggeber aufzuspüren – in den falschen Händen werden diese Geräte jedoch zu gefährlichen Cyber-Waffen. c't hat 15 völlig unterschiedliche Geräte im Labor von der Leine gelassen und die von ihnen ausgehende Gefahr bewertet.

Darunter befindet sich etwa ein mobiler WLAN-Accesspoint namens WiFi Pineapple, der mit zwei Funkmodulen und diversen professionellen Angriffstools ausgestattet ist. Er spannt sein Netz auf und versucht alles, damit WLAN-Clients in Funkreichweite darin hängen bleiben. Der WiFi Deauther für gerade einmal 25 US-Dollar zeigt benachbarte Funknetze auf seinem OLED-Display an und legt sie auf Knopfdruck lahm.

WiFi Pineapple Nano

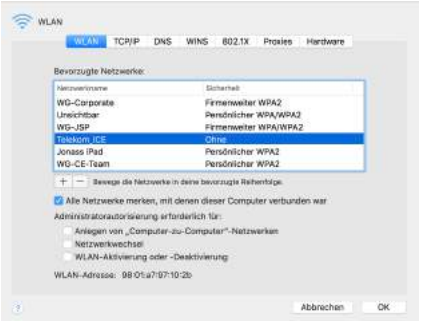
https://www.heise.de/security/meldung/Gefahr-durch-frei-verkaeufliche-Hacking-Gadgets-3806266.html

Live Demo



Allgemeine Maßnahmen

- Accesspoints
  - Aktuelle Verschlüsselung nutzen
  - Langer und komplexer PSK
  - Radius Authentication (WPA Enterprise)
  - Client Isolation
  - WLAN Netze segmentieren
- Clients
  - Client VPN in offenen Wi-Fi Netzen
  - Nicht jedes WiFi-Netz speichern
  - Automatische Verbindung?



Build a Trusted Wireless Environment Today!

The First Test Report on Wi-Fi Security

The Miercom Wi-Fi Security Report compares product efficacy against the six known Wi-Fi threat categories, and illustrates the hidden security deficits with many Wi-Fi solutions.

Miercom

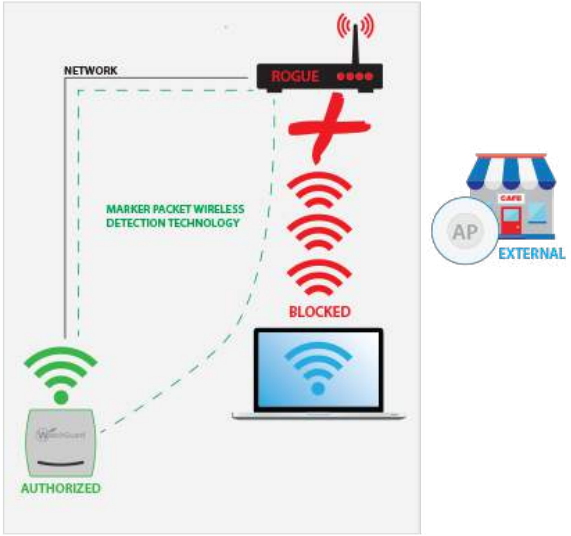
Contents

	WatchGuard AP420		Aruba IAP335		Cisco Meraki MR53		Ruckus R710	
Test	**Detect**	**Prevent**	**Detect**	**Prevent**	**Detect**	**Prevent**	**Detect**	**Prevent**
Rogue AP	P	P	F	N/A	F	MP	F	N/A
Rogue Client	P	P	F	N/A	F	MP	N/A	MP
Neighbor AP	P	P	P	P	F	N/A	F	N/A
Ad-Hoc Network	P	P	F	N/A	F	N/A	P	N/A
"Evil Twin" AP	P	P	P	F	P	MP	P	F
Misconfigured AP	P	P	P	N/A	N/A	N/A	N/A	N/A
Concurrent Threats	P	P	F	F	F	F	F	F

P – Pass
MP Marginal Pass; require manual prevention
F – Failure to detect or protect from the referenced test
N/A – Feature not supported

Wireless Intrusion Prevention System (WIPS)

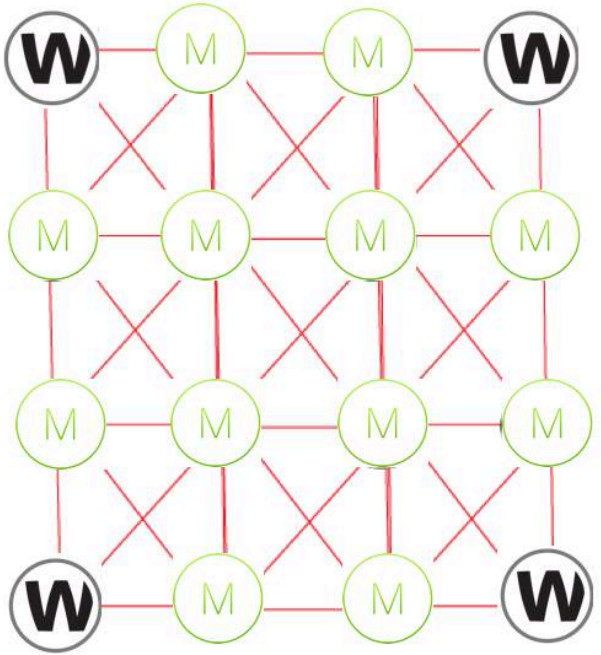
- Access Point überwacht die Wi-Fi Umgebung auf schädliche Aktivitäten
- WIPS Technologie blockiert die Gefahr automatisch
- “Sicherheits Schild” für Ihr Unternehmen und die Nutzer



Schutz bestehender Accesspoints

- WIPS kann ergänzend zu bestehenden Wi-Fi Lösungen (3rd Party) implementiert werden

- Schutz und Überwachung des vorhandenen Netzes ist möglich



Wi-Fi Cloud – 4 Produkte in 1 Lösung

Patented Wireless Security
Only hands-off automated WIPS with low false positives on the market

Management That Scales
Only platform to scale from 1 to unlimited APs, no infrastructure

Business Driven Analytics
Location tracking, footfall, dwell time, repeat visitors, and more at no extra cost and no 3rd party requirements

Powerful Engagement Tools
Captivating splash pages, campaigns to interact with visitors with social media, video, polls, and more

WatchGuard Wi-Fi Cloud

WatchGuard Wi-Fi Solution	Total Wi-Fi	Secure Wi-Fi	Basic Wi-Fi
Central management via hosted Wi-Fi Cloud	✓	✓	
Patented Wireless Intrusion Prevention System (WIPS) for stopping Wi-Fi attacks that steal passwords, credit cards, etc.	✓	✓	
Highly scalable management via templates and profiles	✓	✓	
Friendly Wi-Fi compliant URL filtering	✓	✓	WebBlocker required
Customizable dashboards	✓	✓	
Reporting engine with pre-built reports including PCI, HIPAA, DoD, wireless vulnerability assessment	✓	✓	
Floor map support with visualization of Wi-Fi and WIPS signal coverage	✓	✓	
Captive portals (splash pages) with pre-built templates	✓		
Splash page authentication: click-through, social, guest book, email, SMS, web form, poll, video	✓		
Landing pages and templates	✓		
Social Wi-Fi authentication (Facebook, Twitter, LinkedIn, Google+, Instagram, Foursquare)	✓		
Graphical and text templates for SMS + URL interception	✓		
Location-based analytics: footfall, dwell time, conversion, etc.	✓		
Social analytics: age, gender, birthday, language, etc.	✓		
Customizable analytics reporting	✓		
Floor map support for analytics	✓		
Central management via Firebox appliance			✓
Standard 24x7 Support	✓	✓	✓

Let’s Make Wi-Fi Security a Global Standard!

www.trustedwirelessenvironment.com