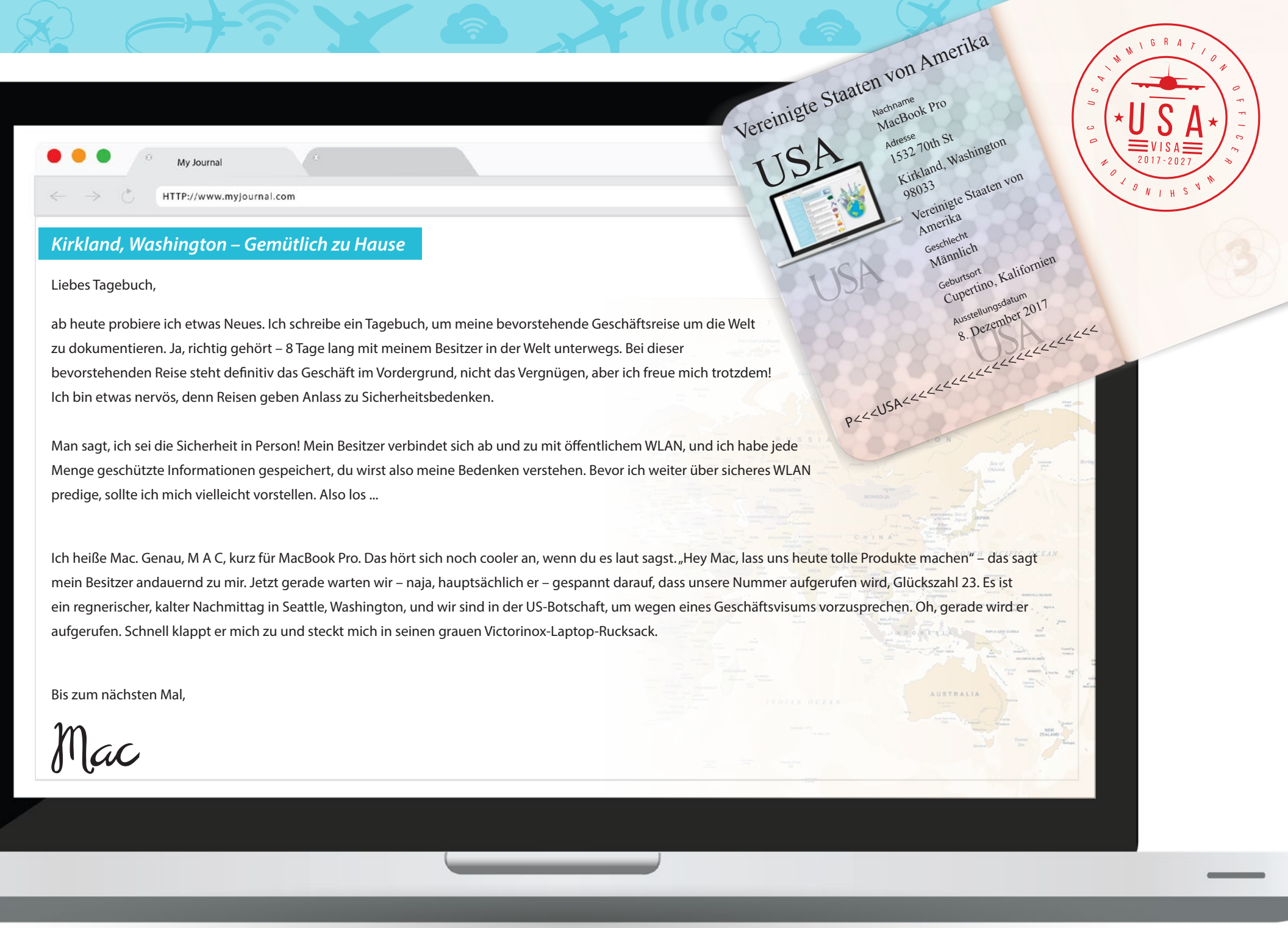
Eine praktische Anleitung zu sicherem WLAN

Beobachtungen Ihres Laptops

WatchGuard®

Inhaltsverzeichnis



Kirkland, Washington – Gemütlich zu Hause

Liebes Tagebuch,

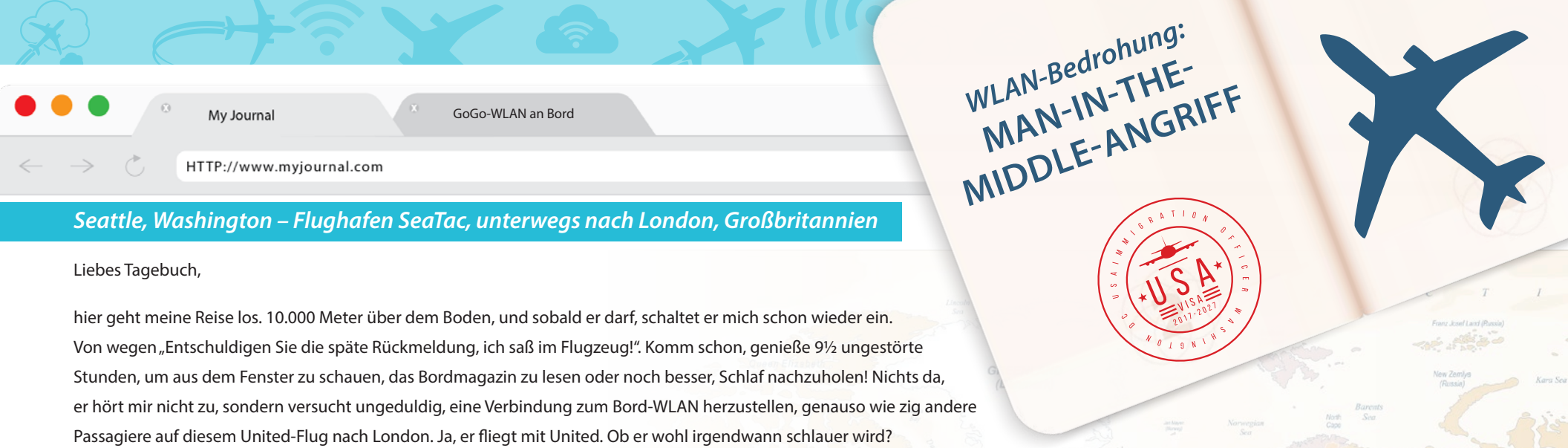
ab heute probiere ich etwas Neues. Ich schreibe ein Tagebuch, um meine bevorstehende Geschäftsreise um die Welt zu dokumentieren. Ja, richtig gehört – 8 Tage lang mit meinem Besitzer in der Welt unterwegs. Bei dieser bevorstehenden Reise steht definitiv das Geschäft im Vordergrund, nicht das Vergnügen, aber ich freue mich trotzdem! Ich bin etwas nervös, denn Reisen geben Anlass zu Sicherheitsbedenken.

Man sagt, ich sei die Sicherheit in Person! Mein Besitzer verbindet sich ab und zu mit öffentlichem WLAN, und ich habe jede Menge geschützte Informationen gespeichert, du wirst also meine Bedenken verstehen. Bevor ich weiter über sicheres WLAN predige, sollte ich mich vielleicht vorstellen. Also los ...

Ich heiße Mac. Genau, M A C, kurz für MacBook Pro. Das hört sich noch cooler an, wenn du es laut sagst. „Hey Mac, lass uns heute tolle Produkte machen" – das sagt mein Besitzer andauernd zu mir. Jetzt gerade warten wir – naja, hauptsächlich er – gespannt darauf, dass unsere Nummer aufgerufen wird, Glückszahl 23. Es ist ein regnerischer, kalter Nachmittag in Seattle, Washington, und wir sind in der US-Botschaft, um wegen eines Geschäftsvisums vorzusprechen. Oh, gerade wird er aufgerufen. Schnell klappt er mich zu und steckt mich in seinen grauen Victorinox-Laptop-Rucksack.

Bis zum nächsten Mal,

Mac



Seattle, Washington – Flughafen SeaTac, unterwegs nach London, Großbritannien

Liebes Tagebuch,

hier geht meine Reise los. 10.000 Meter über dem Boden, und sobald er darf, schaltet er mich schon wieder ein. Von wegen „Entschuldigen Sie die späte Rückmeldung, ich saß im Flugzeug!". Komm schon, genieße 9½ ungestörte Stunden, um aus dem Fenster zu schauen, das Bordmagazin zu lesen oder noch besser, Schlaf nachzuholen! Nichts da, er hört mir nicht zu, sondern versucht ungeduldig, eine Verbindung zum Bord-WLAN herzustellen, genauso wie zig andere Passagiere auf diesem United-Flug nach London. Ja, er fliegt mit United. Ob er wohl irgendwann schlauer wird?

Wusstest du, dass ein WLAN-Angriff in einem offenen Netzwerk weniger als 2 Sekunden dauern kann? Das ist erschreckend! Hallo? Jemand da? Du musst wissen, wie du WLAN-Hotspots sicher nutzt, und wenn du schon verbunden bleiben musst, könnest du wenigstens eine VPN-Verbindung verwenden? Oder besser noch, fahr mich herunter, lehn dich zurück, entspann dich und genieß den Flug.

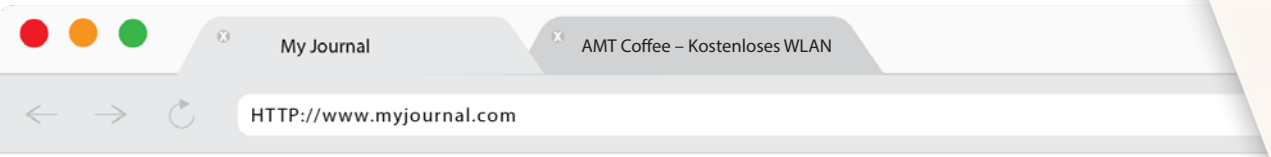
Wusstest du, dass sich das Haupt-WLAN, das Passagiere auf diesem Flug nutzen sollen, in keinster Weise von dem öffentlichen WLAN in einem Café, Einkaufszentrum oder Hotel unterscheidet? Ich habe immer gedacht, dass es deutlich sicherer wäre, wenn man all die Sicherheitsmaßnahmen bedenkt, die wir bei Flugreisen über uns ergehen lassen müssen. Nein, das Netzwerk ist offen.

Für Hacker ist es ganz einfach, mit einem Man-in-the-Middle-Angriff (MitM) deine Daten abzuhören, während sie von Punkt A (beispielsweise deinem Laptop) zu Punkt B (einer Website) übertragen werden, und zu sehen, welche Websites du aufrufst, von dir gesendete und empfangene E-Mails zu lesen und Kennwörter abzufangen, mit denen du dich bei Facebook anmeldest.

GUTER JUNGE! Er meldet sich beim WatchGuard Firebox-SSL-VPN an. Das habe ich ihm beigebracht!

Bis zum nächsten Mal,

Mac



WLAN-Bedrohung:
EVIL-TWIN-ACCESS-POINT

London, Großbritannien – Evil-Twin-Access-Point

Liebes Tagebuch,
es ist 7 Uhr früh und ich weiß ja nicht, wie es dir geht, aber ich habe letzte Nacht wie ein Baby geschlafen, ganz ohne Melatonin. Ich bin voll aufgeladen und bereit, richtig aufzudrehen und eine Runde mit dem roten Doppeldeckerbus zu fahren. Darauf habe ich mein ganzes Leben lang gewartet. Das ist ein Symbol Großbritanniens. Die Londoner Busse sind nicht immer rot gewesen. Vor 1907 waren auf den verschiedenen Strecken Busse unterschiedlicher Farben unterwegs. Hättest du's gewusst?

Während wir warten, dass sich mein Besitzer in aller Ruhe fertig macht – komm schon Mann, die Socken sind in Ordnung –, erzähle ich dir noch einige weitere interessante Dinge, diesmal aber zur WLAN-Sicherheit.

Wusstest du, dass 94% der Reisenden WLAN als wichtigste Annehmlichkeit nennen? Mein Reisebegleiter gehört wahrscheinlich auch zu den 75%, die sagen, dass eine Woche ohne WLAN schlimmer sei als eine Woche ohne Kaffee. Wie haben die Leute früher nur ohne WLAN leben können? WLAN wurde zum ersten Mal 1997 vom IEEE mit dem Standard 802.11 ratifiziert und entsprechende Produkte wurden bis 1999 veröffentlicht. Der 802.11-Standard führte zur Schaffung von Milliarden WLAN-fähiger Geräte.

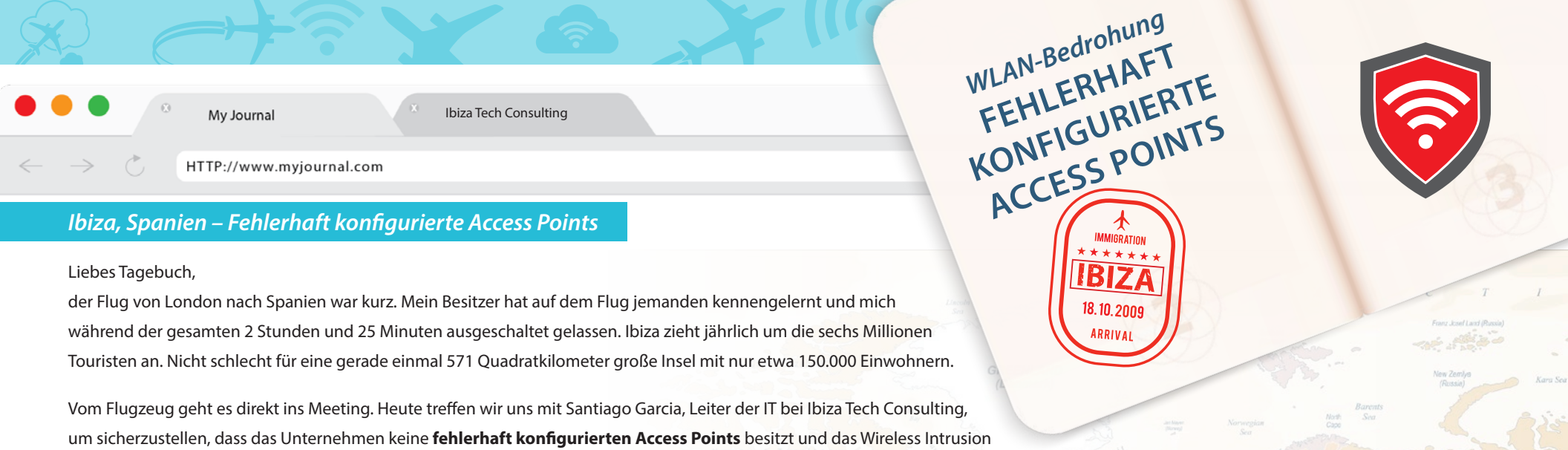
Ups, ich bin etwas abgeschweift und habe nicht gemerkt, dass wir gerade unser Ziel erreicht haben. Mein Besitzer verbindet sich natürlich sofort mit einem WLAN in einem der besten Cafés Londons, dem AMT Coffee. Bedenkt man unsere Vorabrecherchen, ist der Ort erstaunlich angesagt. Er nippt an seinem Espresso und macht das Gleiche wie immer – E-Mails lesen, CNN lesen, und dann sehe ich, wie der Typ neben uns www.bankofamer eingibt... und verliere gleich die Fassung! Online-Banking in einem offenen Netzwerk? In einem beliebigen Café? Ist er verrückt?! Das ist ein klares No-Go. Da sind doch überall Datendiebe. Und ein deutliches Warnzeichen, das mir direkt aufgefallen ist, weil ich ein WLAN-Ninja bin: er hat sich mit einem fremden Access Point verbunden. Oh Mann!

Bei der Herstellung einer Verbindung mit einem Evil-Twin-Access-Point, der den WLAN-Namen und die eindeutige Hardware-Adresse des echten Access Point imitiert, sind Anwender wie er dem Risiko ausgesetzt, private Dokumente mit teils hochvertraulichen Inhalten wie Bankdaten an Cyberkriminelle zu verlieren, die Daten im Netz abfangen, um sie für ihre eigenen, unlauteren Zwecke zu verwenden.

Bevor dieser Typ noch mehr Schaden anrichten kann, kommt zum Glück seine Essensverabredung und rettet die Lage. Morgen geht es nach Spanien.

Bis zum nächsten Mal,

Mac



Ibiza, Spanien – Fehlerhaft konfigurierte Access Points

Liebes Tagebuch,
der Flug von London nach Spanien war kurz. Mein Besitzer hat auf dem Flug jemanden kennengelernt und mich während der gesamten 2 Stunden und 25 Minuten ausgeschaltet gelassen. Ibiza zieht jährlich um die sechs Millionen Touristen an. Nicht schlecht für eine gerade einmal 571 Quadratkilometer große Insel mit nur etwa 150.000 Einwohnern.

Vom Flugzeug geht es direkt ins Meeting. Heute treffen wir uns mit Santiago Garcia, Leiter der IT bei Ibiza Tech Consulting, um sicherzustellen, dass das Unternehmen keine **fehlerhaft konfigurierten Access Points** besitzt und das Wireless Intrusion Prevention System (WIPS) in der Wi-Fi Cloud aktiviert ist. Die Bereitstellung von Access Points ohne Beachtung der gängigen Empfehlungen zur WLAN-Sicherheit kann unbeabsichtigte Fehlkonfigurationen zur Folge haben, die häufig in Sicherheitsrisiken münden.

Der häufigste Fehler besteht darin, die werkseitig festgelegten Standardkonfigurationen von Access Points beizubehalten, etwa Benutzernamen, Kennwörter oder SSID (Service Set Identifier). Laut Gartner werden die meisten WLAN-Sicherheitsbedrohungen durch schlecht konfigurierte Access Points verursacht. NICHT MIT UNS!

Wir melden uns schnell bei der WatchGuard Wi-Fi Cloud an und gehen jeden Access Point durch. Das sehen wir gerne! Jeder AP erfüllt die richtigen Sicherheitsrichtlinien.

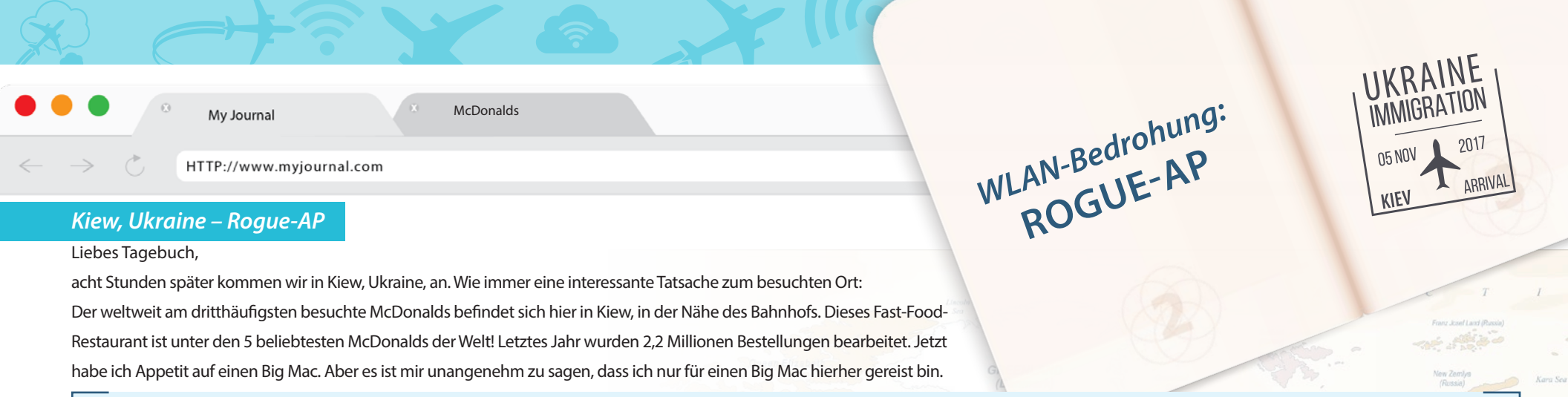
Im Allgemeinen sieht die WLAN-Einrichtung gut aus, es fehlt jedoch **ein wichtiger Aspekt der Wi-Fi Cloud – das WIPS** ist noch nicht konfiguriert. Du fragst dich, was es mit dem WIPS auf sich hat? Der Begriff WIPS stammt aus der WLAN-Branche und bezieht sich auf die Verhinderung von Bedrohungen über das WLAN. Die Erkennungs- und Präventionsmethoden unterschieden sich je nach WLAN-Anbieter, aber WatchGuard WIPS nutzt die fortschrittliche patentierte Marker Packet™-Technologie zu folgenden Zwecken:

- Automatisches, präzises Identifizieren von WLAN-Geräten in deinem Netzwerk
- Erkennen und Blockieren von Rogue-APs
- Erkennen benachbarter APs außerhalb deines Netzwerks
- Erkennen fehlerhaft konfigurierter APs

Wäre das WIPS aktiviert worden, hätten wir uns diese Reise gespart, da das WIPS fehlerhaft konfigurierte APs erkennt. Aber ich weiß, hier geht es um Beziehungsaufbau! ***Auf geht's, WLAN!***

Bis zum nächsten Mal,

Mac



Kiew, Ukraine – Rogue-AP

Liebes Tagebuch,

acht Stunden später kommen wir in Kiew, Ukraine, an. Wie immer eine interessante Tatsache zum besuchten Ort:

Der weltweit am dritthäufigsten besuchte McDonalds befindet sich hier in Kiew, in der Nähe des Bahnhofs. Dieses Fast-Food-Restaurant ist unter den 5 beliebtesten McDonalds der Welt! Letztes Jahr wurden 2,2 Millionen Bestellungen bearbeitet. Jetzt habe ich Appetit auf einen Big Mac. Aber es ist mir unangenehm zu sagen, dass ich nur für einen Big Mac hierher gereist bin.

Es mag unmöglich erscheinen, aber in einem Unternehmen ohne die WIPS-Sicherheit von WatchGuard kann ein Internetkrimineller ungehindert einen fremden Access Point mit deinem Netzwerk verbinden und ahnungslose Benutzer animieren, einen Rogue-AP anstelle des beabsichtigten AP zu verwenden. Das passiert häufiger, als du denkst. Ein Hacker kann mit einem Rogue-AP im Rucksack in dein Gebäude marschieren, ihn unter einem Schreibtisch verstecken und mit deinem Netzwerk verbinden, sodass sich einige oder sogar alle Mitarbeiter mit dem falschen WLAN verbinden und sensible Daten abgefangen werden.

Und es muss nicht immer ein Hacker sein, der Rogue-APs installiert. In vielen Fällen tut dies einer deiner Mitarbeiter, der einen AP an seinem Schreibtisch verbindet, um ein besseres WLAN-Signal zu erhalten. Auch wenn er keine bösen Absichten verfolgt, damit öffnet er dein Netzwerk für ernste Sicherheitsrisiken über das WLAN.

Was würde also verhindern, dass jemand wie du einem Rogue-AP in deinem Büro zum Opfer fällt? Als Unternehmensinhaber hast du nur eine Möglichkeit – WIPS. Ganz genau, das Wireless Intrusion Prevention System. Ich habe im vorherigen Eintrag darüber geschrieben, daher könnte dir die Abkürzung bekannt vorkommen. WLANs zählen im Rahmen der Unternehmenssicherheit zu den Schwachstellen, die am häufigsten übersehen werden. WatchGuard WIPS ist die einzige Lösung auf dem Markt, die alle APs in der Umgebung scannt und als autorisierte, externe oder Rogue-APs klassifiziert.

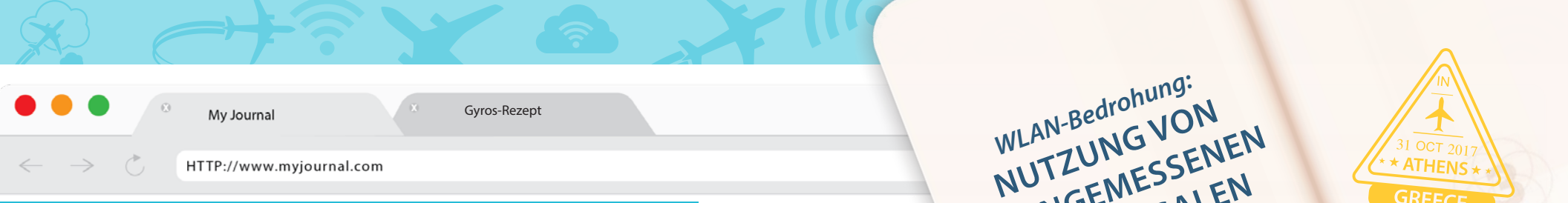
- **Autorisiert** – Bekannter AP, der mit deinem Netzwerk verbunden ist
- **Extern** – Benachbarter AP, der nicht mit deinem Netzwerk verbunden ist
- **Rogue** – Unbekannter AP, der mit deinem Netzwerk verbunden ist

WatchGuard WIPS unterscheidet schnell und zuverlässig zwischen benachbarten, externen und Rogue-APs. Und wenn ein Rogue-AP in deinem Netzwerk erkannt wird, werden alle eingehenden Verbindungen zum Rogue-AP augenblicklich blockiert. Voilà!

Du willst doch nicht zu den Unternehmen gehören, die Mitarbeiter, Gäste und Kunden einladen, Opfer von WLAN-Hacking zu werden? Implementiere WIPS und aktiviere die automatische Prävention. Glaub mir, WLAN-Angreifer werden innerhalb von Sekunden wissen, dass deine Umgebung geschützt ist, und sich weniger gut gesicherten Hotspots zuwenden. Deine Mitarbeiter, Kunden und Gäste werden stets geschützt sein, wenn dein WLAN durch WatchGuard gesichert ist.

Bis zum nächsten Mal,

Mac



WLAN-Bedrohung:
NUTZUNG VON UNANGEMESSENEN UND ILLEGALEN INHALTEN

Athen, Griechenland – Unangemessene und illegale Nutzung

Liebes Tagebuch,

Opa! Seit meinem letzten Besuch der Inseln vor ungefähr 15 Jahren freue ich mich darauf, Griechenland noch einmal zu besuchen. Diesmal bin ich in der historischen Stadt Athen, die etwas anders ist als Mikonos und Santorini – schließlich ist es eine Geschäftsreise.

Griechenland ist eines meiner liebsten Reiseländer – 250 Tage Sonnenschein, tolle Strände, leckeres Gyros, Oliven und Ouzo. ***Opa! Opa!***

Spaß beiseite: Heute helfen wir einer örtlichen Schule (Kinder im Alter zwischen 6 und 12 Jahren), indem wir die Lehrkräfte darüber informieren, wie wichtig es ist, die Nutzung unangemessener und illegaler Inhalte zu unterbinden. Wir möchten ihnen zeigen, wie einfach sie mit der sicheren WLAN-Lösung von WatchGuard jugendgefährdende Inhalte im Internet herausfiltern können, um eine möglichst sichere Lernumgebung für ihre Schüler sicherzustellen.

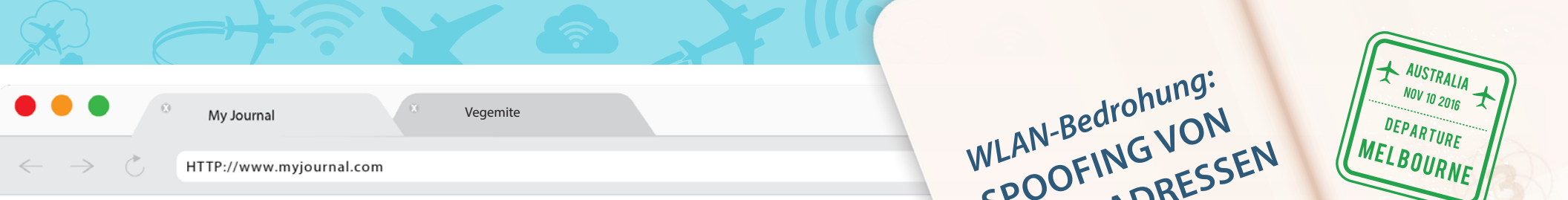
Beängstigende Statistik: Laut Nielsen haben **45% der Kinder zwischen 10 und 12 Jahren Smartphones** und **68% der Eltern sind besorgt angesichts der mangelnden Kontrolle über die Inhalte,** die ihre Kinder online sehen. Mobilgeräte verändern die Art und Weise, in der Kinder heutzutage lernen. Zugriff auf Highspeed-WLAN ist erforderlich, um umfangreiche webbasierte Bildungsressourcen bereitstellen zu können. In vielen Schulen wird die WLAN-Sicherheit erst nachträglich bedacht und nur sehr wenige denken an URL-Inhaltsfilterung nach jugendgefährdenden Inhalten und anderen unangemessenen Websites.

WatchGuard ist bekannt für hohe Sicherheit und wir bringen diesen Fokus auch in unsere WLAN-Produkte. Unsere sichere WLAN-Lösung blockiert nicht nur unangemessene und illegale Inhalte, sie schützt auch Schüler, Lehrkörper und Mitarbeiter vor Datendiebstahl, Kennwortdiebstahl, durch Malware kompromittierten Websites und vielen anderen schädlichen Angriffen.

Heute Abend kann ich mich entspannt zurücklehnen und ein paar leckere Oliven mit Ouzo genießen, für die ich hier hergekommen bin – denn ich weiß, dass die Kinder vor unsicherem WLAN in der Schule geschützt sind.

Bis zum nächsten Mal,

Mac



WLAN-Bedrohung: SPOOFING VON AP-MAC-ADRESSEN

Melbourne, Australien – Spoofing von AP-MAC-Adressen

Liebes Tagebuch,
wusstest du, dass jedes Jahr 22,7 Millionen Gläser Vegemite in Australien hergestellt werden? Das sind 235 Gläser pro Minute! Hast du schon einmal Vegemite probiert? YOLO!

Ein Vegemite-Sandwich ist für ein australisches Kind das, was ein Sandwich mit Erdnussbutter und Marmelade für ein amerikanisches Kind ist – nur der Geschmack ist vollkommen anders! Dr. Cyril P. Callister erfand den ersten Vegemite-Brotaufstrich im Jahr 1922. Er nahm Bierhefe und mischte den Hefeextrakt mit Zutaten wie Sellerie, Zwiebel, Salz und ein paar geheimen Zutaten, um die Paste zu kreieren. Und heute ist Fisherman's Bend in Port Melbourne der einzige Ort auf der Welt, an dem Vegemite hergestellt wird. Ich sagte doch, dass es nicht das typische Erdnussbutter-Marmeladen-Sandwich ist.

Wahrscheinlich hast du schon erraten, wo wir sind – genau, in Melbourne, Australien. Wir nehmen uns die Internetkriminellen Land für Land vor! Heute sind wir in einem örtlichen Krankenhaus (dessen Name aus datenschutzrechtlichen Gründen anonym bleibt). Drahtlose Netzwerke von Krankenhäusern sind supereinfache Ziele für Cyberangriffe – sie sind voller elektronischer Patientenakten. Eine Goldmine! Immer mehr Organisationen im Gesundheitswesen schaffen neue Geräte an, um mit der Erweiterung des IoT Schritt halten zu können. Dabei müssen sie die damit verbundenen, nur allzu realen Cybersicherheitsrisiken im Auge behalten und erforderliche Vorsichtsmaßnahmen ergreifen. Das meint nicht zwangsläufig die Aktualisierung der Geräte mit neuer Software, sondern zielt auch auf die WLAN-Infrastruktur des Krankenhauses ab.

Die heutige WLAN-Schwachstelle ist das Spoofing von AP-MAC-Adressen. Das ist eine Technik, mit der böswillige Benutzer/Hacker die MAC-Adresse ihres eigenen Access Point, den sie in der Hosentasche dabei haben (du würdest dich wundern, wie klein diese Geräte heutzutage sind, batteriebetrieben und so groß wie ein Kartenspiel), entsprechend der MAC-Adresse eines der legitimen Access Points ändern. Im Wesentlichen ist das Spoofing von AP-MAC-Adressen mit der Änderung der Identität eines Access Point und dem Diebstahl wichtiger Informationen verbunden.

Wie verhinderst du, dass das deinem Unternehmen passiert? Gut, dass du fragst. Das Schlüsselwort ist WIPS – das ist die Antwort auf all deine Bedenken hinsichtlich der WLAN-Sicherheit. Die WIPS-Policy unserer Wi-Fi Cloud besitzt eine Einstellung zur Verhinderung des Spoofing von AP-MAC-Adressen. Du weißt nicht mehr, was es mit dem WIPS auf sich hat? Lies meinen Eintrag zu Ibiza, Spanien, als kleine Erinnerung. Sichere Wi-Fi Cloud-Lösungen von WatchGuard schaffen eine sichere, geschützte Umgebung für die Mitarbeiter dieses Krankenhauses und öffentliche WLAN-Umgebungen, eliminieren den Verwaltungsaufwand und ermöglichen beträchtliche Kostensenkungen.

Du kannst in puncto WLAN-Sicherheit keine Spekulationen gebrauchen? Dann brauchst du WIPS!

Bis zum nächsten Mal,

Mac

Sapporo, Japan – Key Reinstallation Attack „KRACK“

Liebes Tagebuch,

Sapporo ist wahrscheinlich vor allem für sein Bier bekannt. Die Hauptstadt von Hokkaido, Japans nördlichster Insel, wird von vielen internationalen Touristen (wie uns) aber auch wegen der weltberühmten Ramensuppe besucht. Ramen und Sapporo – was für eine tolle Essenskombination! Beim bloßen Gedanken daran werde ich hungrig.

Japan ist unser letzter Halt auf dieser Reise um die Welt. Wir treffen uns mit Ichiro-san von Origami IT Pros, um uns der neusten Schwachstelle zuzuwenden, die am 16. Oktober 2017 bekannt gegeben wurde – **Key Reinstallation Attack „KRACK“.** Sicherheitsforscher verkündeten mehrere Schwachstellen im WPA/WPA2-Verschlüsselungsprotokoll, die unzählige WLAN-fähige Geräte weltweit betreffen. Durch KRACK können Daten, die über mit WPA/WPA2 verschlüsselte Drahtlosnetzwerke gestreamt werden, wie Kennwörter und personenbezogene Daten, ohne das Wissen des Benutzers abgefangen, entschlüsselt und geändert werden. Diese Sicherheitslücke bedeutet, dass bei gefährdeten Clients und Access Points über WPA und WPA2 verschlüsselter WLAN-Datenverkehr potenziell gefährdet ist, bis gewisse Abhilfemaßnahmen ergriffen wurden.

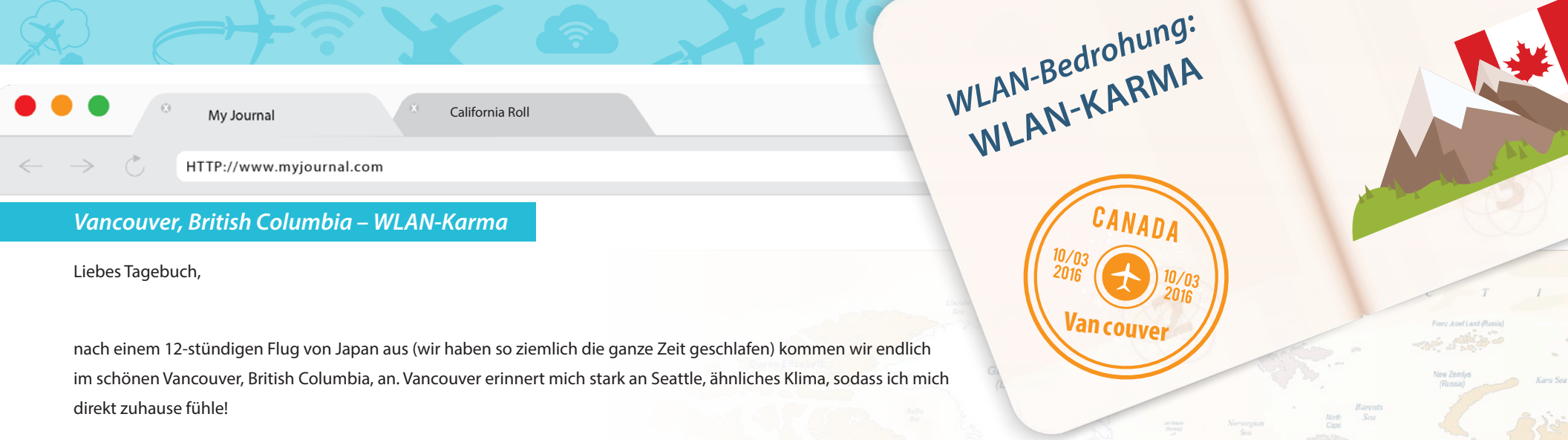
Zum heutigen Zeitpunkt gibt es 10 bekannte Schwachstellen in Verbindung mit KRACK. Wir bei WatchGuard haben Patches für unsere betroffenen Produkte bereitgestellt. Bei nicht von WatchGuard stammenden Geräten, wie etwa deinen Smartphones und Tablets, solltest du auf der Website des Herstellers und in den Sicherheitshinweisen nachlesen, ob sie betroffen und Updates verfügbar sind. Zwar werden die meisten Unternehmen Patches bereitstellen, jedoch ist es wahrscheinlich, dass nicht gepatchte Geräte mit deinem Netzwerk interagieren und dich gefährden.

WatchGuard wäre nicht WatchGuard, wenn es nicht zusätzliche Methoden bieten würde, um nicht gepatchte Client-Geräte vor KRACK zu schützen. Was must du also tun?

Aktualisiere die Firmware deines Access Point (AP), falls du das noch nicht getan hast. WatchGuard hat Patches für alle unterstützten APs (und Firebox-Tabletop-Appliances) mit integrierten WLAN-APs bereitgestellt. Aktiviere die Funktion zur Abwehr von Key Reinstallation Attacks in Verbindung mit WPA/WPA2 in Clients. Der AP kann bei Aktivierung dieser Einstellung nicht gepatchte Clients kompensieren. Diese Art der Abwehr wird nur so lange empfohlen, bis alle Clients gepatcht sind. Aktiviere alternativ die Einstellung zur Verhinderung des Spoofing von AP-MAC-Adressen in der WIPS-Policy der Wi-Fi Cloud.

Bis zum nächsten Mal,

Mac



Vancouver, British Columbia – WLAN-Karma

Liebes Tagebuch,

nach einem 12-stündigen Flug von Japan aus (wir haben so ziemlich die ganze Zeit geschlafen) kommen wir endlich im schönen Vancouver, British Columbia, an. Vancouver erinnert mich stark an Seattle, ähnliches Klima, sodass ich mich direkt zuhause fühle!

Hier kommt etwas Interessantes zu Vancouver – ich sagte doch, dass ich immer eine interessante Tatsache parat habe. Die California Roll wurde (auch wenn der Name etwas anderes suggeriert) von Chefkoch Hidekazu Tojo in Vancouver erfunden. Hier kannst du auch sein Restaurant Tojo besuchen – es soll hervorragend sein!

Jetzt wieder zum Geschäft. Während wir über den Flughafen laufen, verbindet sich mein WLAN automatisch mit dem kostenlosen Flughafen-WLAN, ohne dass mein Besitzer dies bemerkt hätte. Ups! Ich muss früher schon einmal eine Verbindung hergestellt haben und wiedererkannt worden sein. Ich deaktiviere mein WLAN sofort, um nicht Opfer eines WLAN-Karma-Angriffs zu werden. Denn wer weiß schon, welchen unbekannten Gefahren ich mich aussetze, wenn sich mein WLAN automatisch mit Netzwerknamen aus der Vergangenheit verbindet. Bei dieser Art des Angriffs werden meine praktischen WLAN-Funktionen genutzt, die WLAN-Namen und Kennwörter speichern, damit sich mein Besitzer diese nicht merken muss. Ich sende stets Testanfragen an drahtlose Netzeaus meiner Vergangenheit, um zu sehen, ob eines in der Nähe ist. Jemand, der ein Karma-Angriffstool ausführt, kann meine intelligenten Funktionen nutzen, ausspionieren nach welchem WLAN ich suche, und es mir anbieten, sodass ich mich mit dessen bösartigem Access Point verbinde und die Daten meines armen Besitzers im Handumdrehen gestohlen werden.

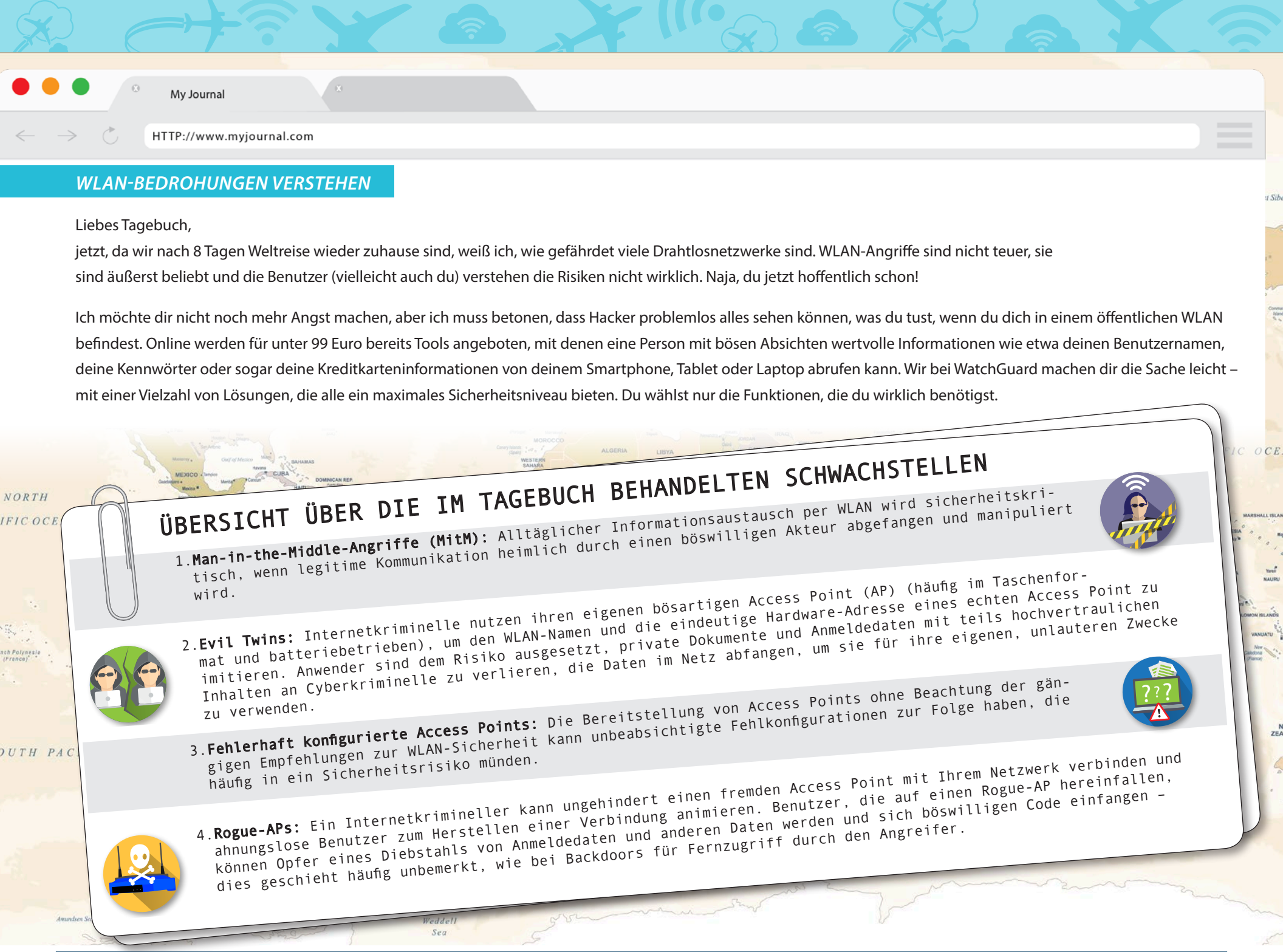
Siehst du hier irgendein Muster?

Nach Berichten von Small Business Trends **haben 43 % aller Cyberangriffe kleine und mittlere Unternehmen zum Ziel**. Es gibt viele Gründe, aus denen jemand einen Karma-Angriff gegen dein Unternehmen ausführen könnte. Ein wichtiger Grund ist der, dass dein Unternehmen die begehrtesten **personenbezogenen Daten** (Personally Identifiable Information, PII) enthält.

Lösung? Hast du es wirklich noch nicht begriffen? **WatchGuard WIPS – gemacht, um Karma-Angreifer fernzuhalten**, wenn sie versuchen, die Kontrolle zu übernehmen. Jetzt gerade fühle ich mich wie ein gesicherter WLAN-Ninja-Krieger!

Bis zum nächsten Mal,

Mac



WLAN-BEDROHUNGEN VERSTEHEN

Liebes Tagebuch,
jetzt, da wir nach 8 Tagen Weltreise wieder zuhause sind, weiß ich, wie gefährdet viele Drahtlosnetzwerke sind. WLAN-Angriffe sind nicht teuer, sie sind äußerst beliebt und die Benutzer (vielleicht auch du) verstehen die Risiken nicht wirklich. Naja, du jetzt hoffentlich schon!

Ich möchte dir nicht noch mehr Angst machen, aber ich muss betonen, dass Hacker problemlos alles sehen können, was du tust, wenn du dich in einem öffentlichen WLAN befindest. Online werden für unter 99 Euro bereits Tools angeboten, mit denen eine Person mit bösen Absichten wertvolle Informationen wie etwa deinen Benutzernamen, deine Kennwörter oder sogar deine Kreditkarteninformationen von deinem Smartphone, Tablet oder Laptop abrufen kann. Wir bei WatchGuard machen dir die Sache leicht – mit einer Vielzahl von Lösungen, die alle ein maximales Sicherheitsniveau bieten. Du wählst nur die Funktionen, die du wirklich benötigst.

ÜBERSICHT ÜBER DIE IM TAGEBUCH BEHANDELTEN SCHWACHSTELLEN

1. **Man-in-the-Middle-Angriffe (MitM):** Alltäglicher Informationsaustausch per WLAN wird sicherheitskritisch, wenn legitime Kommunikation heimlich durch einen böswilligen Akteur abgefangen und manipuliert wird.

2. **Evil Twins:** Internetkriminelle nutzen ihren eigenen bösartigen Access Point (AP) (häufig im Taschenformat und batteriebetrieben), um den WLAN-Namen und die eindeutige Hardware-Adresse eines echten Access Point zu imitieren. Anwender sind dem Risiko ausgesetzt, private Dokumente und Anmeldedaten mit teils hochvertraulichen Inhalten an Cyberkriminelle zu verlieren, die Daten im Netz abfangen, um sie für ihre eigenen, unlauteren Zwecke zu verwenden.

3. **Fehlerhaft konfigurierte Access Points:** Die Bereitstellung von Access Points ohne Beachtung der gängigen Empfehlungen zur WLAN-Sicherheit kann unbeabsichtigte Fehlkonfigurationen zur Folge haben, die häufig in ein Sicherheitsrisiko münden.

4. **Rogue-APs:** Ein Internetkrimineller kann ungehindert einen fremden Access Point mit Ihrem Netzwerk verbinden und ahnungslose Benutzer zum Herstellen einer Verbindung animieren. Benutzer, die auf einen Rogue-AP hereinfallen, können Opfer eines Diebstahls von Anmeldedaten und anderen Daten werden und sich böswilligen Code einfangen – dies geschieht häufig unbemerkt, wie bei Backdoors für Fernzugriff durch den Angreifer.

ÜBERSICHT ÜBER DIE IM TAGEBUCH BEHANDELTEN SCHWACHSTELLEN

5. **Unangemessene und illegale Nutzung:** Wer einen WLAN-Gastzugang anbietet, lädt zu diversen illegalen bzw. gefährlichen Machenschaften ein. Nicht jugendfreie oder extremistische Inhalte können für andere Benutzer beleidigend sein. Illegale Downloads geschützter Medien bergen für Unternehmen das Risiko von Urheberrechtsprozessen.

6. **Spoofing von AP-MAC-Adressen:** Um die WLAN-Sicherheit zu kompromittieren, versuchen Internetkriminelle häufig, durch das Spoofing von MAC-Adressen ihre bösartigen Access Points als legitim oder bekannt zu tarnen.

7. **Karma-Angriff:** Dieser Angriff ist schon über zehn Jahre alt, aber immer noch aktuell. Bösartige Access Points antworten auf Testanfragen von Clients mit in der Vergangenheit genutzten WLAN-Namen, sodass sich das Opfer mit dem bösartigen AP verbindet und Daten, Anmeldedaten und andere sensible Informationen gestohlen werden können.

8. **WPA/WPA2-Verschlüsselungs-Cracking (KRACK):** Durch KRACK können Daten, die über mit WPA/WPA2 verschlüsselte Drahtlosnetzwerke gestreamt werden, wie Kennwörter und personenbezogene Daten, ohne das Wissen des Benutzers abgefangen, entschlüsselt und geändert werden. Diese Sicherheitslücke bedeutet, dass bei gefährdeten Clients und Access Points über WPA und WPA2 verschlüsselter WLAN-Datenverkehr potenziell gefährdet ist.

Ein wichtiger Rat, den wir dir mitgeben möchten: Lass das WLAN nicht zu deinem größten Sicherheitsrisiko werden. Wie ich mehrmals in diesem Tagebuch erwähnt habe, ist Hacking über das WLAN die größte Bedrohung für dein Sicherheitsnetzwerk, die zudem oft ignoriert wird – und deinen Mitarbeitern, Kunden und Anbietern kein sicheres WLAN zu bieten, schadet deinem Geschäft.

Bis zum nächsten Mal,

Mac

Hacking über das WLAN ist die größte Bedrohung für Ihr Sicherheitsnetzwerk, die zudem oft ignoriert wird – und Ihren Mitarbeitern, Kunden und Anbietern kein sicheres WLAN anzubieten, schadet Ihrem Betrieb. Weitere Informationen erhalten Sie unter: **www.watchguard.com/wifi**

Globale Hauptgeschäftsstelle USA
Tel: +1.800.734.9905
E-Mail: sales@watchguard.com

Hauptgeschäftsstelle Mitteleuropa
Tel: +49 (700) 9222 9333
E-Mail: germanysales@watchguard.com

Hauptgeschäftsstelle APAC-Ozeanien Singapur
Tel: +65.6536.7717
E-Mail: inquiry.sea@watchguard.com

Teilenr. WGCE67081_050418