04/2014

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

**Gewinnspiel**
Freikarten zur IT-Trends
(siehe Rückseite)

# Wenn einer eine Reise tut

## Risiken für Geschäftsreisende durch die Nutzung von Hotspots

*Das Hotspot-Netzwerk in Deutschland wächst stetig. Viele Mitarbeiter neigen dazu, auf Ihren Geschäftsreisen ein solches WLAN-Netzwerk zu nutzen, da diese oftmals schneller oder besser verfügbar als der firmeneigene UMTS-Zugang sind. So gehören in Bahnhöfen, Flughäfen und Cafés (kostenfreie) öffentliche Internetzugänge schon fast zum Standard. Doch hierbei bestehen auch Gefahren für die Unternehmensdaten und Informationen, auf die die UIMC schon deshalb hinweist, da der Einsatz von mobilen Geräten in Unternehmen durch Smartphones und Tablets immer größer wird, viele Nutzer aber sehr unbedarft mit den Geräten, Apps und Netzwerken umgehen.*

Der Zugang ist schnell eingerichtet: WLAN-Netzwerk auswählen, verbinden und ggf. noch ein Passwort eingeben und schon ist der Mitarbeiter mit seinem dienstlichen Smartphone, Laptop oder Tablet im Internet. Doch neben den gewohnten Risiken, die jede Internetverbindung birgt, wird diese durch eine Verbindung mit einem öffentlichen Hotspot erhöht. So nutzen Angreifer zum Teil die gängigen Namen wie „Deutsche Bahn“, „Starbucks“ oder „Free-Wifi“, um „ahnungslose“ User anzulocken und die Kommunikation auszuhorchen. So können ggf. Kreditkarten- oder andere vertrauliche Daten mitgelesen werden.

Eine weitere Gefahr besteht darin, dass sich das mobile Endgerät automatisch mit bekannten Netzwerken verbindet. Wenn der Name mit einem bereits genutzten Netzwerk identisch ist, wird i. d. R. automatisch eine Verbindung aufgebaut. Somit kann auch eine Verbindung mit einem gefakten (unsicheren) anstelle mit einem „seriösen“ (sicheren) Hotspot hergestellt werden, und etwaige Manipulationen und Unregelmäßigkeiten – beispielsweise beim Abrufen der E-Mails – werden noch schlechter bemerkt.

Im betrieblichen Alltag sollte also stets darauf geachtet werden, dass die Mitarbeiter – sofern die Nutzung eines öffentlichen Hotspots beispielsweise aufgrund vom schlechten Mobilfunkempfang geboten scheint – stets eine VPN-Verbindung aufbauen. Doch auch die Nutzung einer VPN-Verbindung schützt nicht vor Man-in-the-Middle-Attacken, Malware oder anderen Schadprogrammen. Da dies erfahrungsgemäß den Benutzern aber nicht bekannt ist, kann hierdurch sogar eine gefährliche „trügerische Sicherheit“ erzeugt werden. Diese Gefährdung erfordert aber primär gezielte Angriffe. Nichtsdestotrotz sollte geprüft werden, die VPN-Verbindungen beispielsweise mit IPSec zusätzlich abzusichern.

Des Weiteren weist die UIMC darauf hin, dass Unternehmen zum einen verbindliche Vorgaben für die Mitarbeiter machen und zum anderen die Smartphone-User entsprechend sensibilisieren sollten. Nur jene Mitarbeiter, die die Gefahren und Verhaltensregeln kennen, können sich auch entsprechend schützen. Erfahrungsgemäß kommen solche Vorfälle nicht durch mutwilliges Verhalten, sondern durch Unwissenheit zustande.

Dies gilt im Übrigen auch für Mitarbeiter, die keine dienstliche Hardware (wie z. B. Laptop oder Smartphone) erhalten haben, aber beispielsweise über eine Internetseite auf Ihre E-Mails zugreifen können (z. B. Outlook Web Access/OWA). Trotz verschlüsselter Internetverbindung wie SSL/TLS, https o. ä. bestehen die o. g. Gefahren des Mitlesens etc., wenn der Mitarbeiter sich (in diesem Fall mit seinem privaten Smartphone) in einem öffentlichen Hotspot bewegt.

Doch auch bei aller technischen Vorsicht, weist Dr. Jörn Voßbein, mehrfach bestellter Datenschutzbeauftragter und Sicherheitsbeauftragter, auch darauf hin, dass – losgelöst von den dargestellten technischen Risiken – oftmals Dritte (ob nun bewusst oder unbewusst) die Möglichkeit erhalten, einfach Kenntnis von Informationen zu erlangen. So achten die Benutzer erfahrungsgemäß nicht darauf, wer in der Umgebung mitlesen kann; so können der Tischnachbarn im Café, der nebenan Wartende am Flughafen oder der Sitznachbar im ICE die Inhalte des Displays einfach mit verfolgen.

Dies zeigt, dass vor dem Einsatz von neuen IT-Systemen stets eine Risiko-Analyse durchgeführt werden sollte, in der die möglichen Gefahren-Szenarien im Zusammenhang mit der Kritikalität der Informationen betrachtet werden. Das Ergebnis sollte eine Vorgehensweise sein, mit der die Risiken auf ein akzeptables Maß reduziert werden.

**Mehr Pressemitteilungen finden Sie hier: www.UIMC.de/communication**

## Schon gewusst?

Wenn Sie auf Ihrer Internetseite Tracking-Tools zur Analyse der Besucher-Aktivitäten einsetzen, müssen Sie hierüber innerhalb der Datenschutzerklärung informieren (LG Frankfurt am Main, Urteil vom 18.02.2014, Az 3-10 O 86-12). Diese Information muss wiederum von jeder (Einstiegs-) Seite erreicht werden können, so dass sich eine Verlinkung innerhalb der sog. „Meta-Navigation“ der Internetpräsenz anbietet. Als Beispiel für eine mögliche Umsetzung können Sie sich an unserer Internetseite orientieren:

**www.UIMC.de**

**Haben Sie Fragen?**
UIMC Dr. Voßbein GmbH & Co KG
Nützenberger Straße 119
42115 Wuppertal
Tel.: (02 02) 2 65 74 - 0
Fax: (02 02) 2 65 74 - 19
E-Mail: consultants@uimc.de
Internet: www.UIMC.de

Stets auf dem Laufenden sein?
www.UIMC.de/Communication

# UIMCommunic@tion

*Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert*

## Tipps für die Nutzung öffentlicher WLAN-/Wifi-Hotspots

Neben den gewohnten Risiken, die jede Internetverbindung birgt, erhöht die Verbindung mit einem Hotspot die Gefahr eines Angriffs. Mit folgenden Tipps können Sie das Surfen in einem Hotspot sicherer gestalten, wobei dies natürlich auch keine 100%ige Sicherheit verspricht:

1. Es ist stets zu empfehlen, eine eine VPN-Verbindung zu nutzen. Auch für den privaten Einsatz gibt es die passende Software mit ausreichenden Funktionen oftmals schon kostenlos.
2. VPN-Verbindungen lassen sich mit IPSec weiter verbessern bzw. weiter verschlüsseln. Dadurch kann die Identität von Sender und Empfänger überprüft werden.
3. Seien Sie trotz der vermeintlichen Sicherheit durch eine VPN-Verbindung weiterhin aufmerksam. Dies bedeutet (wie auch grundsätzlich), dass Sie externe Links stets genau prüfen.
4. Um sog. „Drive-by-Downloads“ bestmöglich zu verhindern, empfiehlt es sich, einen Script-Blocker zu nutzen, um bspw. (unsichere) aktive Inhalte (wie z. B. Java) zu blockieren bzw. einzeln freizugeben.
5. Achten Sie aktuelle Betriebssysteme und Software/Apps. Durch Updates/Patches werden Sicherheitslücken geschlossen.
6. Achten Sie, wer Ihnen beim Surfen in öffentlichen Bereichen über die Schulter guckt. Durch entsprechendes Hinsetzen, Drehen des Displays oder Nutzung von Sichtschutz-Folien können Sie ungewollte Einblicke verhindern.

Die o. g. Tipps sind sowohl für den dienstlichen als auch privaten Einsatz sinnvoll, so dass vertrauliche Informationen nicht ausgelesen werden.

Mehr Tipps finden Sie in der nächsten Ausgabe vom UIMCommunic@tion-Info-Brief oder erfahren Sie bei Ihrem Ansprechpartner!

**Auszug aus bisher erschienenen Hinweisen/Tipps:**
„Sichere Nutzung von E-Mails“ (09/2013)
„Sichere Nutzung von Smartphones“ (01/2013)
„Smartphone-Funktionen sicher nutzen“ (07/2013)

## Restplätze für ISO-Seminar

Für unser UIMCollege-Seminar „Auditierung und Zertifizierung gemäß ISO/IEC 27001“ haben wir noch Plätze frei.

Im Seminar werden Struktur und Inhalts der Norm vermittelt. Auch können Vorgehensweise der Auditierung und normgemäßen Zertifizierungsvorbereitung etc. diskutiert werden. Natürlich wird hierbei schon die Novelle (ISO/IEC 27001:2013) berücksichtigt. Es besteht Zeit, mit dem Refenten zu diskutieren!

**28.04.2014, Wuppertal**

## Gewinnspiel*

Unter allen UIMCommunication-Abonnenten, die eine Mail an communication@uimc.de mit dem Betreff „Freikarte“ bis zum 30.04.2014 gesendet haben, verlosen wir eine Freikarte im Wert von EUR 50,00.

Auf der diesjährigen IT-Trends „Sicherheit“ werden wir am **14.05.2014 in Bochum** über das Thema „Vertrauen ist gut, Kontrolle ist besser“ im Rahmen des Outsourcings informieren.

**IT-Trends Sicherheit**

## Bitte senden Sie mir neben den angekreuzten Themen weitere Informationen zu:

- ☐ Wenn einer eine Reise tut: Risiken für Geschäftsreisende durch die Nutzung von Hotspots
- ☐ Informationspflichten und weitere Datenschutzanforderungen auf Internetpräsenzen
- ☐ **Unser Tipp:** Bitte senden Sie mir zukünftig den UIMCommunic@tion-Info-Brief und regelmäßig weitere interessante Informationen per E-Mail zu! Mir ist bekannt, dass ich der künftigen Zusendung jederzeit formlos per E-Mail an communication@uimc.de widersprechen kann.

E-Mail: _____ Unterschrift: _____

per Fax an (0202) 265 74 - 19 oder formlos per Mail an communication@uimc.de

*) Teilnahmebedingungen: Die Teilnahme ist kostenlos und unabhängig von dem Erwerb von Waren oder Dienstleistungen. Ebenfalls werden die Gewinnchancen nicht durch etwaige Leistungen der Teilnehmer beeinflusst. Voraussetzung ist eine Abonnierung des UIMCommunic@tion-Info-Briefs zum Zeitpunkt des Einsendeschlusses.