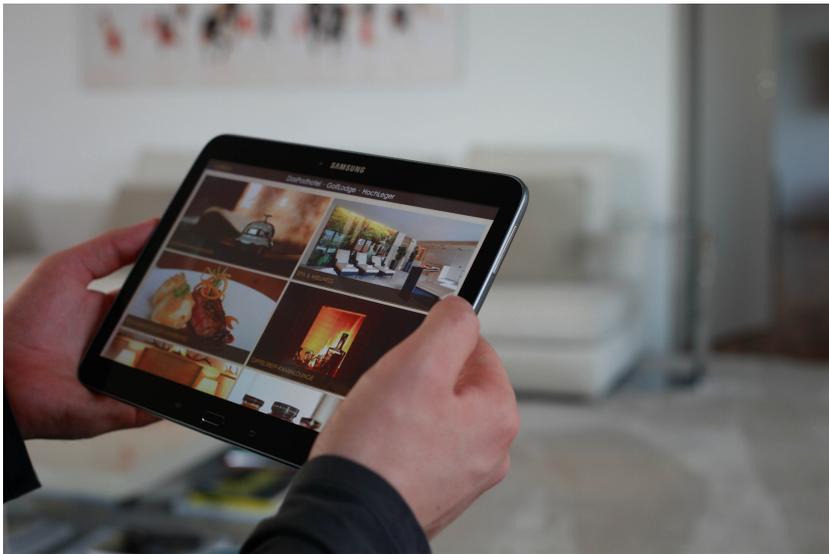


## Pressemitteilung

### Hacker im Hotelzimmer: Tipps für Hotels zum Schutz der IT Infrastruktur und wichtiger Gastdaten

*Russische Hacker entwenden Login-Informationen von Milliarden Internetnutzern weltweit und in China wird die Gebäudesteuerung eines Hotels von einem Gast kontrolliert. Was können Hotels tun um Schadsoftware und möglichen Angriffen vorzubeugen? Die Firma SuitePad gibt ein paar einfache Tipps.*



(Berlin, 11. August 2014) Im chinesischen Shenzhen wurde kürzlich medienwirksam die Gebäudesteuerung eines 5-Sterne Hotels von einem spanischen Hacker gekapert. Jesus Molina gelang es, Licht- und Gardinensteuerung in Zimmern anderer Gäste zu kontrollieren. Vorfälle wie dieser werfen mit der zunehmenden Digitalisierung in vielen Bereichen der Hotellerie immer wieder Fragen der IT-Sicherheit auf. Besonders kritisch ist das Thema für Privathotels, die sich oft kein ausreichend geschultes Personal für IT-Sicherheit leisten können. Dass dies jedoch nicht nur ein Problem für kleine Hotels ist, zeigt der aktuelle Fall aus Shenzhen, wo es eine international renommierte Hotelkette traf. Auch wenn es absolute Sicherheit in der IT nicht geben mag, gibt es doch ein paar Tipps und Tricks, die Hotelbetriebe sicherer vor Angriffen machen können.

#### **Trennung von Gebäudesteuerung und Gast-WLAN**

In manch kleinerem Betrieb greifen Mitarbeiter und Gäste durch dasselbe WLAN Netzwerk auf das Internet zu. Somit wird es für Eindringlinge deutlich einfacher, sich Zugriff auf hoteleigene Systeme zu verschaffen. Am Beispiel des Hotels in Shenzhen zeigt sich dies besonders deutlich, denn auch hier wurde die Gebäudesteuerung über das Gast-WLAN Netzwerk angesprochen. So konnte der Hacker den Netzwerkverkehr auslesen und Rückschlüsse auf die Funktionsweise der Gebäudesteuerung ziehen. Mit Hotelsystemen vernetzte Geräte sollten daher unbedingt vom Gästenetzwerk getrennt bleiben.

## **Verschiedene Kennwörter nutzen und diese regelmäßig ändern**

Viele Internetnutzer benutzen privat immer wieder das gleiche Kennwort. Leider verwenden viele Anwender dieselben Passwörter auch noch in ihrem Arbeitsumfeld. Das ermöglicht Eindringlingen, die einmal das Passwort geknackt haben, Zugang zu allen Logins im privaten und im geschäftlichen Bereich. Daher sollte für kritische Systeme immer ein separates, langes Passwort verwendet werden. Regelmäßige Passwort-Änderungen werden ebenfalls empfohlen, insbesondere wenn sich mehrere Nutzer einen Account teilen. Ein Tipp: wenn sich mehrere Mitarbeiter einen sicheren Zugang und Passwort teilen müssen, sollte kein leicht zu erratendes Passwort genutzt werden (z.B. „Hotelname2014“), sondern eher die Anfangsbuchstaben eines leicht zu merkenden Satzes: „Wir haben 210 Zimmer im Haus“ = „Wh2ZiH“.

## **Der größte Schutz entsteht durch geschulte Mitarbeiter**

Die beste IT-Sicherheitsinfrastruktur nützt jedoch nichts, wenn Mitarbeiter unvorsichtig sind. Es ist problematisch, wie freimütig viele Angestellte USB-Sticks von Gästen am Rezeptionscomputer einlesen um Dokumente auszudrucken. Dabei kann sehr einfach schädliche Software auf dem System installiert werden. Dies ist insbesondere dann ein Problem, wenn Gastdaten auf den Computern gespeichert sind. Durch intelligente Client-Server- oder Cloud-Lösungen relativiert sich dieses Problem, doch oft befinden sich auf diesen Rechnern immer noch relevante Kundenkarteien.

Moderne IT-Systeme sind aus dem Alltag der Hotellerie nicht mehr wegzudenken. Der Nutzen, der damit für Hotels einhergeht, ist einfach zu groß. Selbiges gilt auch für den Gast, der auf einen gewissen Komfort nicht mehr verzichten möchte. Lösungen wie SuitePad, das sind Tablet PCs, die die Gästemappe ersetzen, lassen den Gast zum Beispiel Hotelservices buchen, internationale Zeitungen lesen oder Informationen zur Umgebung abrufen. Da Gäste nun in immer mehr Hotels Zugriff auf derartige Produkte bekommen, werden sie darauf langfristig kaum noch verzichten wollen. Umso wichtiger ist es, dass Hotels und Anbieter solcher Lösungen gleichermaßen grundlegende Sicherheitsvorkehrungen einhalten.

Absolute Sicherheit kann es weder für Hotels noch für andere Unternehmen geben. Mit geschulten Mitarbeitern und grundlegenden Sicherheitsmaßnahmen können jedoch viele Gefahren ausgeschlossen werden. Das führt dazu, dass sich Hotel und Gast wieder auf die großen Vorteile moderner Technologien konzentrieren können. Denn letztlich sind es diese innovativen Produkte die den Gast während seines Aufenthalts begeistern und dafür sorgen, dass er wiederkommt.

## *Über SuitePad*

*Die SuitePad GmbH mit Sitz in Berlin wurde 2012 von Moritz von Petersdorff-Campen und Tilmann Volk gegründet. Die SuitePad GmbH entwickelt tabletbasierte Kommunikationslösungen für die Hotellerie. Gäste können über SuitePads Hotelservices und externe Angebote direkt per Knopfdruck buchen. Gleichzeitig kann der Gast über das SuitePad Entertainmentangebote wie Nachrichten, Musik und Videos abrufen. SuitePad ist damit Vorreiter in der Hotel- und Gastkommunikation und bringt Entertainmentlösungen im Hotelzimmer auf ein neues Niveau.*

*Pressekontakt für Rückfragen:*

*SuitePad GmbH*

*Moritz von Petersdorff-Campen*

*Christinenstraße 5*

*10119 Berlin*

*Tel.: +49 (0) 30 692039752*

*info@suitepad.de*

*www.suitepad.de*

*Stichwörter: SuitePad, IT-Sicherheit, Security, Cloud, Tablet PC, Innovation, Hotels, Tourismus, Hotelzimmer, Gästeinformation, Zimmermappe, Service, Hotelgast, Concierge, Mehrwert, Nutzen, mehr Umsatz, Berlin*