

# hogaAKTIV fragt nach

## Interview mit Stefan Dinnendahl, Geschäftsführer des Hotelverbands Deutschland (IHA)

**I**T-Sicherheit in der Hotellerie: Nur wer die Risiken kennt, kann sich schützen“: Im November 2012 fand die erfolgreiche Auftaktveranstaltung statt zur geplanten Reihe „IT-Sicherheit in der Hotellerie“. Sie wurde in Kooperation von Hotelverband Deutschland (IHA) e. V., TeleTrust – Bundesverband IT-Sicherheit e. V. und DEHOGA NRW, gefördert durch das Bundesministerium für Wirtschaft und Technologie (BMWi) im Rahmen der Task Force „IT-Sicherheit in der Wirtschaft“, durchgeführt.

chungssystemen – in der Hotellerie gibt es zahlreiche Berührungspunkte mit dem Thema IT-Sicherheit. Allerdings wird dabei der IT-Sicherheitsaspekt nicht selten unterschätzt oder nicht richtig erkannt.

 hoga AKTIV

**Nach dem Motto, nur wer die Risiken kennt, kann sich davor schützen?**

**Stefan Dinnendahl:** Richtig, deshalb haben wir auch in einem „Live Hacking“ zeigen lassen, wie Profiha-

cker vorhandene Sicherheitslücken oder menschliche Schwächen mit krimineller Energie geschickt ausnutzen können. Gerade bei Angriffen aus dem Netz bemerken viele Opfer den Angriff gar nicht oder erst viel zu spät, nämlich dann, wenn der Schaden bereits eingetreten ist. Im Gegensatz zu Einbruch oder Diebstahl hinterlassen Hacker keine sichtbaren Spuren, allerdings kann man anhand der Schäden die Spur bis zum Hotel zurückverfolgen und hat so noch einen zusätzlichen Imageschaden. Aber auch eine fahrlässig programmierte Hotelhomepage kann von Hackern leicht manipuliert werden und damit Schaden anrichten.

nen zusätzlichen Imageschaden. Aber auch eine fahrlässig programmierte Hotelhomepage kann von Hackern leicht manipuliert werden und damit Schaden anrichten.

 hoga AKTIV

**An welche Gefahren bzw. IT-Sicherheitsrisiken denken Sie dabei besonders?**

**Stefan Dinnendahl:** In der letzten Zeit haben oft die sogenannten Abmah-

nen für Schlagzeilen gesorgt. Opfer solcher Abmahnungen sind in der Regel Hotspot-Betreiber wegen illegalen Downloads bzw. Filesharings oder Webseiteninhaber bei Verstößen gegen Informationspflichten z. B. Impressumspflicht, Buttonlösung oder rechtswidrige AGB. Ein besonderes Risiko liegt aber im Umgang mit extrem vielen Zahlungs-/Kundendaten, die die Hotellerie zum Top-Ziel in der Kreditkarten-Kriminalität macht. Kreditkarten-Organisationen, Händlerbanken und Verbände sind über die Angriffe sehr besorgt und sehen intensiven Handlungsbedarf.

 hoga AKTIV

**Wie können sich Hotels vor solchen Risiken schützen?**

**Stefan Dinnendahl:** Grundsätzlich benötigt ein Hotel ein sicheres IT-Netzwerk bestehend aus zeitgemäßer, sicherer Technik (Soft- und Hardware) und einem angemessenen Sicherheitskonzept. Zusätzlich bedarf es geschulter Mitarbeiter, die verstehen,



Stefan Dinnendahl

 hoga AKTIV

**Herr Dinnendahl, warum hat der IHA diese Pilotveranstaltung zur IT-Sicherheit in der Hotellerie unterstützt?**

**Stefan Dinnendahl:** Der Grund ist einfach, die Anforderungen an die IT-Sicherheit in der Hotellerie sind in den letzten Jahren stetig gewachsen. Ob der Umgang mit personenbezogenen Daten, die Nutzung von WLAN oder die Sicherheit von Webseiten und Bu-





wie wichtig sorgsamer Umgang mit Daten ist. Und last but not least eine entsprechende Rechtsvorsorge durch Rechtsberatung, aber auch durch Versicherungskonzepte. Diese Punkte wurden anlässlich unserer Pilotveranstaltung aufgegriffen. Für 2013 plant der IHA gemeinsam mit TeleTrust bereits eine bundesweite Fortsetzung der Veranstaltungsreihe, die dank der Unterstützung des BMWi für teilnehmende Hotels wieder kostenfrei sein wird.

 hoga **AKTIV**

**Sie haben eben die Kreditkartensicherheit angesprochen, was müssen Hoteliers dort beachten?**

**Stefan Dinnendahl:** Zahlungs-/Kundendaten, die über die Kreditkartenabwicklung gespeichert werden, sind höchst wertvoll für Hacker und deren Auftraggeber. Internationale Kreditkartenorganisationen haben deshalb mit „Payment Card Industry Data Security Standards“ (kurz: PCI DSS) weltweit gültige Sicherheitsstandards geschaffen. Sie enthalten verbindliche Regeln für alle Unternehmen, die Kartendaten verarbeiten, um diese besser vor Missbrauch zu schützen. Die Einhaltung dieser Richtlinien hilft Hoteliers, Sicherheitslücken in ihren Netzwerken aufzudecken und sich so vor kriminellen Angriffen aus dem Internet zu schützen. Der Nachweis der eigenen PCI DSS Konformität kann bei Bekanntwerden von Kreditkartendiebstahl auch die Haftungsfrage eines Hotels erheblich beeinflussen.

 hoga **AKTIV**

**Wie hilft der Hotelverband Hotels bei Sicherheitsfragen bzw. Risiken?**

**Stefan Dinnendahl:** Ein Verband unterstützt am besten durch Informationen. So hat der IHA speziell zu Haf-



*Gerade bei Angriffen aus dem Netz bemerken viele Opfer den Angriff gar nicht oder erst viel zu spät, nämlich dann, wenn der Schaden bereits eingetreten ist.*

tungsfragen beim Internetzugang für Gäste in Hotels ein Merkblatt erstellt, um das Haftungsrisiko für Hotels zu minimieren. Das Lösungskonzept basiert auf vier Säulen: einer technisch sicheren Hotspot-Komplettlösung, Hinweisen zur Nutzung des Internetzuganges durch den Gast, einer Versicherungslösung für das verbleibende Haftungsrisiko und einer Rechtsberatung durch eine spezialisierte Anwaltskanzlei.

Des Weiteren arbeiten wir an einer Lösung, die kleinen und großen Hoteliers Rechtssicherheit in einem immer komplexeren und riskanteren Umfeld

bietet und die Anfang 2013 als „Hotelprotect“ auf den Markt kommt. Herausforderungen wie ein rechtskonformes Online-Marketing, gesetzliche Vorgaben wie die „Buttonlösung“ sowie Angriffe durch Abmahnungen werden mit der Unterstützung von Hotelprotect effektiv und kostengünstig bewältigt. Die IHA will dadurch erreichen, dass innovative Leistungen und klare Kostenstrukturen im Online-Direktvertrieb für Hotels kalkulierbar bleiben. ■

 [www.ihade.de](http://www.ihade.de)