+ + PRESSEMITTEILUNG + +

CeBIT: Massive Sicherheitslücke in Hotel-WLANs – Steganos stellt neues Schutzprogramm vor

Berlin, 04. März 2013 – Zur CeBIT werden wieder Besucher aus der ganzen Welt in Hannovers Hotels erwartet – und dort arglos die öffentlichen Hotspots nutzen. Das ist riskant, wie das Berliner Sicherheitsunternehmen Steganos zeigt. Für das Hacken eines öffentlichen WLANs braucht man nämlich nur zwei Dinge: Ein Smartphone und eine spezielle Netzwerkanalyse-App. Dem Berliner Sicherheitsunternehmen Steganos ist es mit dieser schlichten Ausstattung gelungen, sich Zugang zu sensiblen Daten in Hotel-Netzwerken zu verschaffen. Unverschlüsselte Daten von Gästen, die über den Hotel-Router ins Internet gehen, können so problemlos mitgelesen werden. Um das Mitschneiden dieser Daten im WLAN zu verhindern, hat Steganos das Programm Steganos Online Shield 365 entwickelt. Dieses ist ab dem 5. März 2013 unter www.steganos.com verfügbar.

Schauplatz der WLAN-Hacks waren mehrere Hotels namhafter Ketten in Berlin Mitte. Während sich ein Steganos-Mitarbeiter mit seinem Notebook in das öffentliche WLAN des Hotels einloggte, startete ein anderer Mitarbeiter von seinem Smartphone aus die Netzwerkanalyse-App dSploit. Der Mitarbeiter am Smartphone konnte nicht nur das Mail-Passwort problemlos mitlesen, sondern ganze Facebook-Sitzungen live übernehmen. So konnten gefälschte Nachrichten auf Facebook gepostet werden, private E-Mails mitgelesen, Instant-Messaging-Nachrichten abgefangen werden und vieles mehr.

Ursache ist eine eklatante Sicherheitslücke vieler öffentlicher WLANs. Die Daten, die zwischen dem Notebook und dem Router ausgetauscht werden, also alle Daten, die beim Surfen anfallen, werden im Regelfall unverschlüsselt übertragen. Sicher ist der Nutzer nur dann, wenn die angesurfte Webseite eine HTTPS-Verbindung anbietet.

Denn nur dann können die Daten TLS-verschlüsselt (TLS = Transport Layer Security – früher SSL – ist ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet) übertragen werden. Manche Router verfügen über eingebaute Schutzmechanismen gegen Tools wie dSploit – man weiß jedoch nie, ob in einem öffentlichen WLAN ein solcher Router zum Einsatz kommt.

„Es ist unfassbar, wie leicht sich öffentliche WLANs immer noch hacken lassen. Dabei sind diese Sicherheitslücken in der Branche längst bekannt. Und man benötigt kaum technisches Verständnis oder Hackerkenntnisse“, erklärt Gabriel Yoran, Geschäftsführer von Steganos. „Mit den abgefangenen Passwörtern hätten wir die Online-Identität des Mitarbeiters übernehmen können. Das Aussperren vom eigenen Facebook-Account oder der Versand von Spam über den Computer des Mitarbeiters wären dann noch harmlose Szenarien gewesen. Durch die Verwendung des Autorisierungsverfahrens Facebook Connect, das auf vielen Websites zum Einsatz kommt, könnte man sich so die Identität seines Opfers aneignen – selbst wenn man ‚nur’ den Facebook-Zugang mitgeschnitten hat.“

Steganos Online Shield 365 schützt jede Verbindung ins Internet

Einen wirksamen Schutz gegen Hackerangriffe bekommen Nutzer mit dem neuen Programm Steganos Online Shield 365. Technisch handelt es sich hier um eine VPN-Lösung (VPN = Virtual Private Network) mit integrierter TLS-Verschlüsselung. Ist das Programm auf dem Rechner aktiviert, verschlüsselt und anonymisiert es automatisch die Verbindung ins Internet. Egal, ob der Nutzer zu Hause, im Büro oder in einem öffentlichen WLAN surft: Die verschlüsselte Verbindung ist sicher und von außen nicht angreifbar.

Die Verbindung ins Internet wird dabei vom Computer des Nutzers über speziell gesicherte Steganos-Server, die in speziell gesicherten Rechenzentren stehen, aufgebaut. Steganos unterliegt als Berliner Unternehmen dem deutschen Datenschutzrecht und hat seit 1997 Erfahrung bei der Entwicklung von Verschlüsselungssoftware.

Der Nutzer surft mit Steganos Online Shield 365 aber nicht nur sicher, sondern auch anonym. Denn beim Aufbau der Verbindung tauscht das Programm automatisch die echte IP-Adresse gegen eine zufällige aus. Somit ist die wahre Identität des Nutzers, die durch die IP-Adresse verraten wird, beim Surfen ebenfalls geschützt.

Steganos Online Shield 365 ist sowohl als kostenfreie Version (maximales Traffic-Volumen: 500 MB pro Monat) als auch als kommerzielle Version (1-Jahresversion, unbegrenztes Traffic-Volumen) verfügbar.

Key Features:

- Schützt jede Verbindung ins Internet mit einer sicheren TLS-Verschlüsselung
- Schützt vor Passwort-Diebstahl und Identitäts-Diebstahl
- Bietet speziell gesicherte Server in Deutschland, Großbritannien, Frankreich, den USA und der Schweiz
- Schützt die wahre IP-Adresse, so dass die Anonymität beim Surfen 100%ig gewahrt bleibt
- Schnelle Server für optimale Datenübertragung bei höchster Sicherheit

Eine Seriennummer zum Testen sende ich Ihnen auf Anfrage gerne zu.

Bildmaterial und die Pressemeldung zum Download finden Sie hier:
www.steganos.com/de/unternehmen/presse-center

Preise:

• Bis 500 MB Datenverkehr/Monat: Kostenlos

• Unbegrenzter Datenverkehr: 59,95 Euro/Jahr

Systemvoraussetzung:

Windows XP, Vista, 7 und 8 (jeweils 32-/64-bit), Internet-Verbindung, 1 GB RAM, 50 MB Festplattenplatz

Verfügbarkeit:

Steganos Online Shield 365 steht ab dem 05.03.2013 unter folgender URL zum Download bereit: https://www.steganos.com/de/produkte/ sicher-surfen/online-shield

Über Steganos Software GmbH

Steganos ist seit über 15 Jahren die Referenz beim Schutz vor Hackern durch Verschlüsselung. Das 1997 in Deutschland gegründete Unternehmen stellt bekannte Sicherheits-Produkte wie Steganos Privacy Suite, Steganos Safe und Steganos Passwort-Manager her. Mehr Infos erhalten Sie unter www.steganos.com.

Pressekontakt:

Laubstein Media

Anja Eichelsdörfer (ehem. Laubstein)

Untere Parkstraße 42

85540 Haar

Tel. +49 - 89 - 41 85 84 85

Fax +49 - 89 - 41 85 84 86

Mobil +49 - 151 - 41 20 22 32

Mail steganos@laubstein-media.de

Web www.laubstein-media.de