

ICT-Security-Dienstleister findet mit „Wargooqing“ etliche Private Keys

Compass Security AG warnt: Unwissende PGP-Nutzer geben vertrauliche Daten im Internet preis

Rapperswil, 25. März 2009 – Zahlreiche User der Verschlüsselungsfunktion PGP führen das Verfahren ad absurdum. Dies hat der Schweizer ICT-Sicherheitsspezialist Compass Security AG herausgefunden. Gibt man bei Google die Textfolge filetype:asc intext:"BEGIN PGP PRIVATE KEY BLOCK" ein, so spuckt die Suchmaschine mehrere hundert PGP Private Keys aus. Diese haben Anwender aus Unwissenheit oder versehentlich in Kombination mit ihrem Schlüsselpaar ins Netz gestellt und ahnen nicht, dass sie damit Datendieben Tür und Tore öffnen.

Das Prinzip der PGP-Verschlüsselung funktioniert wie folgt: Der User besitzt einen Public und einen Private Key. Um sicher Daten austauschen zu können, wird zum Verschlüsseln der öffentliche Schlüssel des Empfängers benötigt, zum Entschlüsseln der private. Damit der Absender verschlüsseln kann, ist es sinnvoll, den Public Key ins Internet zu stellen. Der Private Key hingegen ist geheim und soll die Zugriffssicherheit gewährleisten. Wenn nun jemand „aus Versehen“ das komplette Paar auf seine Webseite legt, stellt dies eine gefährliche Sicherheitslücke dar, da so vertrauliche Daten entschlüsselt werden können. Um den Content zu dechiffrieren, wird zwar eine Passphrase benötigt, aber erfahrungsgemäß definieren die meisten User sehr einfache Passwörter. Compass hat zur Veranschaulichung das Tool „CodeSnapper“ entwickelt, mit dem eine Dictionary-Attacke durchgeführt werden kann.

„Es ist erstaunlich, wie viele Menschen ihren Private Key im Internet bekannt geben“, erklärt Marco Di Filippo, Regional Director Germany bei Compass. „Aufmerksam geworden bin ich darauf durch einen Zufall. Jemand hat mir eine signierte Nachricht gesendet. Als ich auf seiner Website den Public Key downloaden wollte, entdeckte ich, dass er dort das komplette Schlüsselpaar publiziert hat. So begann die Suche nach Personen, die den gleichen Fehler machen. Das Resultat: knapp 250 Treffer.“ Zu finden ist in dieser Übersicht auch der folgende Link: <https://www.hacking-lab.com/contact/brandyarcoiz.asc>. Hierbei handelt es sich um ein von Compass veröffentlichtes Schlüsselpaar für Demozwecke.

Wargooing: „Sag’ mir deinen Namen und ich sage dir dein Passwort“

Die PGP-Keys sind jedoch nicht die einzigen Sicherheitslücken, die sich über die gewaltigen Suchoptionen von Google ausnutzen lassen. Die Methodik nennt sich „Wargooing“ und wurde von Jonny Long geprägt. Das Ziel ist das Auffinden vertraulicher Daten im Internet. Nach diesem Mechanismus können Inhalte wie Zugangsdaten, SessionIDs etc. aufgespürt werden. So kursierte beispielsweise eine Liste mit 8.000 User-Namen und Passwörtern der Firma Comcast, einer der größten Internet Service Provider der USA, frei verfügbar im Netz.

Marco Di Filippo warnt: „Wir möchten für die Gefahren, die im Internet lauern, sensibilisieren. Google bietet eine breite Angriffsfläche für Hacker, die auf die Unachtsamkeit unwissender User spekulieren. Daher können wir nur dazu raten, sorgsam mit persönlichen Daten im Internet umzugehen und sich über mögliche Risiken zu informieren.“

Kurzporträt Compass Security AG:

Die 1999 gegründete Compass Security AG mit Sitz in Rapperswil (CH) hat sich als europäisches Dienstleistungsunternehmen auf Security-Assessments zur Vertraulichkeit, Verfügbarkeit und Integrität von Unternehmensdaten spezialisiert. Mittels Penetrationstests, Ethical Hackings und Reviews beurteilt Compass ICT-Lösungen hinsichtlich Sicherheitsrisiken präventiv, spürt vorhandene Schwachstellen auf und unterstützt bei deren Beseitigung. IT-Forensische Experten ermöglichen durch Erfassung, Prüfung und Auswertung digitaler Spuren die Rekonstruktion und beweisdienliche Dokumentation von Missbrauchsfällen im Zusammenhang mit digitalen Systemen. Praxisnahe Workshops und Schulungen zum Thema IT-Security sowie Live-Hacking-Vorträge zur Usersensibilisierung runden das Portfolio ab. Neutralität und Produktunabhängigkeit sind dabei wesentliche Bestandteile der Unternehmensphilosophie. Der Kundenstamm setzt sich aus nationalen und internationalen Kunden jeglicher Größenordnung und unterschiedlicher Branchen zusammen. Weitere Informationen unter: www.csnc.ch

Weitere Informationen:

Compass Security AG
Postfach 1628
Glärnischstrasse 7
CH-8640 Rapperswil

Tel.: +41 55 214 41 60
Fax: +41 55 214 41 61
www.csnc.ch

PR-Agentur:

Sprengel & Partner GmbH
Nisterstraße 3
D-56472 Nisterau

Ansprechpartner:

Ulrike Peter
Tel.: +49 (0)26 61-91 26 0-0
Fax: +49 (0)26 61-91 26 0-29
E-Mail: ulrike.peter@sup-pr.de
www.sup-pr.de