

**ICT-Security-Dienstleister warnt vor Gefahren in Facebook, Xing & Co.**

**Compass Security AG weist auf Sicherheitslücken in Social Networks hin**

**Rapperswil, 06. Mai 2009** – Es ist gemeinhin bekannt, dass sich unvorsichtige User in Online Communities wie Xing, StudiVz und Facebook durch unüberlegte Angaben, Bilder etc. für die breite Öffentlichkeit transparent machen. Neben dem freiwilligen Verlust der Privatsphäre durch die Offenheit vieler User lauern jedoch zusätzliche Bedrohungen. Dass Social Networks auch technologisch zahlreiche Sicherheitsrisiken bergen, ist den wenigsten bewusst. So hat die Compass Security AG bereits etliche Schwachstellen identifiziert, die es ermöglichen, User-Accounts zu manipulieren und kompromittieren, Nachrichten mitzulesen und vieles mehr.

Ulrike Peter, Senior Vice President der Sprengel & Partner GmbH, hat erlebt, wie schnell man einer derartigen Attacke zum Opfer fallen kann: „Ich telefonierte mit Marco Di Filippo von Compass Security und er schickte mir dabei eine E-Mail mit dem Link <https://www.xing.com/bestoffers/>, in der er ein Angebot bei Xing suggerierte. Es öffnete sich nach dem Anklicken die übliche XING-Anmeldemaske und ich habe mich wie gewohnt in meinen Account eingeloggt. Nachdem ich dies getan hatte, las er mir mein Passwort vor. Ich war völlig perplex.“ Dieses Beispiel diente Demozwecken, verdeutlicht aber die Brisanz sowie die möglichen Folgen. Der Angreifer, der durch eine derartige „Man in the Middle-Attacke“ an ein Passwort oder weitere Daten gelangt, könnte sich so z.B. auch Zugriff zu weiteren Accounts des jeweiligen Users verschaffen. Denn die meisten Menschen neigen dazu, immer das gleiche Kennwort zu verwenden. Gleichzeitig könnten die Angreifer eine Vielzahl solcher Links im Web 2.0 oder bei Google streuen und unbedarfte User würden sie bedenkenlos nutzen.

Der Wegbereiter sind typische Schwachstellen in Social Networks, die sich mit denen anderer Web-Applikationen decken. Die in vorherigem Fall angewandte Angriffsmethode nennt sich Redirecting-Attacke und lässt sich auf alle möglichen Plattformen übertragen, für die eine Authentifikation notwendig ist. Weitere WepApp-Schwachstellen (siehe [http://www.owasp.org/index.php/Top\\_10\\_2007](http://www.owasp.org/index.php/Top_10_2007)) erlauben die Ausführung diverser Skripts, um User-Sitzungen zu „stehlen“, Websites zu verunstalten, Malware zu installieren etc.

Marco Di Filippo, Regional Director Germany bei Compass, erklärt: „Ursache sind die zum Teil fehlerhaften und unsicheren technologischen Umsetzungen dieser Internetdienste bzw. Web-Applikationen. Programmierer konzentrieren sich bei der Entwicklung häufig primär auf die Funktionalität, anstatt auf die Security. Neben den seit Jahren bekannten Schwachstellen werden zunehmend neue Verwundbarkeiten entdeckt, die es Angreifern beispielsweise erlauben, auf nicht freigegebene Informationen zuzugreifen.“ Vor wenigen Wochen wurde z.B. die Internetseite von Wolfgang Schäuble und des FC Schalke gehackt. Auf letzterer wurde eine Meldung platziert, die besagte, dass Kevin Kurani von seinen vertraglichen Pflichten entbunden wurde und vom Verein mit sofortiger Wirkung freigestellt worden sei. Wie sich herausstellte, war hierfür eine Sicherheitslücke im Content-Management-System Typo3 (SQL-Injection-Lücke) verantwortlich.

Diese Art Schwachstellen machen sich Angreifer zu Nutze. Als ICT-Sicherheits-Dienstleister entdeckt Compass regelmäßig neue Angriffsszenarien und macht durch Live-Demos sowie Web Application Security-Tests auf die Gefahren aufmerksam, um so zu deren Beseitigung beizutragen.

**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](http://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](http://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](mailto:ulrike.peter@sup-pr.de)  
[www.sup-pr.de](http://www.sup-pr.de)