Datenschutz und Persönlichkeitsrechte im Web 2.0 –
Schutz vor falschen Freunden

Michael Hange, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Cyber-Kriminelle nehmen zunehmend auch soziale Netzwerke ins Visier. Mit gestohlenen Daten können sie dort Betrugsdelikte begehen und haben eine regelrechte Schattenwirtschaft für elektronische Identitäten geschaffen. Nutzer sind daher verstärkt aufgefordert, ihre Daten zu schützen – zum eigenen Nutzen und im Interesse der Internet-Community.

Heute ist das World Wide Web für viele Menschen ein Raum, in dem ganz selbstverständlich persönliche Kontakte geknüpft und Freundschaften gepflegt werden. Soziale Netzwerke bilden dafür eine beliebte Plattform, auf der die Nutzer oft sehr private Informationen veröffentlichen. Vor allem junge Menschen nutzen diese Angebote in großer Zahl: Die größten sozialen Netzwerke haben mehrere hundert Millionen Mitglieder, Tendenz weiterhin steigend.

Doch wie im „echten Leben" sollten Nutzer auch im Web 2.0 ein gesundes Misstrauen an den Tag legen. Die bedenkenlose Preisgabe von Daten macht es Cyberkriminellen einfach, in sozialen Netzwerken potenzielle Opfer auszuspionieren und gezielt anzugreifen. Durch Phishing mithilfe gefälschter E-Mails verschaffen sich die Täter beispielsweise Zugang zu einem Nutzerprofil und können danach unter falschem Namen andere Nutzer täuschen. So nutzen sie das gegenseitige Vertrauen, das in den sozialen Netzwerken herrscht, für betrügerische Zwecke aus.

Soziale Netzwerke sind attraktiv für Online-Kriminelle

Da die Profile in sozialen Netzwerken oft detaillierte Angaben zu persönlichen Interessen enthalten, sind sie auch für den gezielten Versand von Werbung attraktiv. Gefährdungspotential geht zudem von den Kontaktlisten der Nutzer von sozialen Netzwerken aus, die oft hunderte Adressen umfassen, an die Kriminelle Schadsoftware verschicken können – so verbreitete sich zum Beispiel der Wurm „Koobface" 2009 dramatisch in Facebook und MySpace. Vor diesem Hintergrund hat sich der Handel mit gestohlenen Identitäten und persönlichen Informationen inzwischen zu einem Millionengeschäft für IT-Kriminelle entwickelt, die die Daten auf Online-Plattformen handeln. So wurde der „Identitätsdiebstahl" zu einer der am schnellsten wachsenden Bedrohungen im Internet, wie der Lagebericht zur IT-Sicherheit 2009 des Bundesamts für Sicherheit in der Informationstechnik zeigt.

Michael Hange
Diplom-Mathematiker, ist seit 1977 in der Bundesverwaltung auf dem Gebiet der IT-Sicherheit tätig. Von 1994 bis Anfang 2009 war er Vizepräsident des BSI, bis Oktober 2009 ständiger Vertreter des IT-Direktors im BMI. Seit dem 16. Oktober 2009 ist Michael Hange Präsident des Bundesamtes für Sicherheit in der Informationstechnik.

Der Bedarf an unabhängiger Aufklärung ist groß

Wir verstehen es vor diesem Hintergrund als wichtigen Auftrag, dem Thema Web 2.0 künftig eine bedeutende Rolle bei der Aufklärung und Sensibilisierung der IT-Nutzer einzuräumen. Denn in der Öffentlichkeit stellen wir einen zunehmenden Bedarf an Informationen über Gefährdungen und Schutzmöglichkeiten von kompetenter und unabhängiger Stelle fest. Bereits heute leistet das BSI beispielsweise durch die Beratung von Behörden, Bürgern und Unternehmen und mit Dienstleistungen wie dem Bürger-CERT und der Webseite www.bsi-fuer-buerger.de einen Beitrag. Mit dem geplanten

Ausbau des BSI als zentrale Cyber-Sicherheitsbehörde wird unser Engagement im Bereich Aufklärung und Sensibilisierung in Zukunft noch zunehmen – auch in Kooperation mit Partnern und Initiativen. Ziel ist es, die IT-Sicherheit kontinuierlich zu erhöhen und so den Schutz sensibler Daten – ob privater oder geschäftlicher Natur – zu gewährleisten.

Neben dem sensiblen Umgang mit den eigenen Daten bedarf es dabei auch ganz handfester technischer Schutzmaßnahmen. Die Bedrohungsszenarien der Informationstechnik haben sich in den letzten Jahren erheblich verändert und entwickeln sich zunehmend aggressiver mit technisch ausgefeilter Finesse und krimineller Energie. IT-Sicherheit ist in dieser Hinsicht Grundvoraussetzung für Datensicherheit.

Für den Bürger heißt das: Grundlegenden Schutz bietet eine aktuelle Schutzsoftware mit Virenscanner und Firewall. Aber auch hier ist mittlerweile Vorsicht geboten: Kriminelle bieten online gefälschte Virenscanner, so genannte Scareware an, die nicht nur wirkungslos sind, sondern einen Computer ganz im Gegenteil sogar mit Schadsoftware infizieren können. Neben einem aktuellen Antivirenschutz bleibt es auch in sozialen Netzwerken unverzichtbar, ein sicheres Passwort zu wählen – Geburtstagsdaten haben dort nichts zu suchen. Zum Schutz vor Schadsoftware sollten Internetnutzer darüber hinaus niemals auf Links klicken, die in E-Mails von unbekannten Absendern angeboten werden. Bei dubiosen E-Mails von Freunden, in denen man zum Beispiel um Geld gebeten wird, sollte man nachfragen – vielleicht verbirgt sich dahinter eine falsche Identität.

Schutz des Einzelnen bedeutet auch Schutz der Gemeinschaft

Diese individuellen Sicherheitsmaßnahmen schützen nicht nur den einzelnen Nutzer – von ihnen profitieren alle Bürger im Internet. Denn jeder schlecht geschützte Computer ist ein potenzielles Einfallstor für die Täter, die aus gekaperten PCs riesige „Botnetze“ mit zum Teil mehreren tausend PCs bilden. Deren große Rechenkapazität dient dann zum massenhaften Versand von Spam-Mails oder für Angriffe auf Webseiten („Distributed Denial-of-Service-Attacken“). Hier kann jeder IT-Nutzer durch Aufmerksamkeit und grundlegende Sicherheitsvorkehrungen dazu beitragen, den Tätern ihr Geschäft so schwer wie möglich zu machen. Dann bleibt das Internet auch in Zukunft ein gerne besuchter Raum für geschäftliche und private Aktivitäten.