Polizei und Neue Medien

Soziale Medien wie „Facebook“, „Twitter“ und „Skype“ beeinflussen die Polizeiarbeit und bieten neue Fahndungsmöglichkeiten. Ein EU-Forschungsprojekt bestätigt Erfolge im Einsatz von „Social Media“.

Die Tendenz der internetlastigen Kommunikation stellt die Polizeiarbeit vor neue Herausforderungen. Im Rahmen des EU-Forschungsprojekts „Composite“ (Comparative Police Studies in the EU) wurden Spezialisten im Bereich Informations- und Kommunikationstechnik (IKT) von Polizeiorganisationen in zehn europäischen Ländern interviewt, und zwar in Belgien, Deutschland, Frankreich, Großbritannien, Italien, Mazedonien, den Niederlanden, Rumänien, Spanien und Tschechien. Darüber hinaus wurden Verantwortliche von 20 IKT-Firmen befragt, die in diesen Ländern die Polizeibehörden ausrüsten. Das Projekt wird von der Europäischen Union im Rahmen des FP7-Forschungsrahmenprogramms gefördert und hat eine Laufzeit von 48 Monaten. Der Startschuss dazu fiel im August 2010.

Den Auslöser des Projekts bildeten Überlegungen zur Integration neuer Technologien und Medien in die Polizeiarbeit. Laut dem *Fraunhofer-Institut für Angewandte Informationstechnik (FIT)* galt es, Möglichkeiten zu finden, um die Öffentlichkeit verstärkt in polizeiliche Tätigkeiten einzubinden, Polizeiaktionen transparenter zu gestalten sowie das Vertrauen der Beamten in die eigene Arbeit zu erhöhen.

Großbritannien als Vorbild. „Soziale Medien werden laut der Studie besonders in den Niederlanden und Großbritannien bereits aktiv genutzt“, sagte Sebastian Denef, Wissenschaftler am FIT. „Alle Länder sehen Social Media aber als zentrale Herausforderung der Zukunft und glauben, dass solche Werkzeuge die Polizeiarbeit nachhaltig verändern werden.“ Als Musterbeispiel gilt Großbritannien. Dort fanden bereits mehrere Tests statt, im Zuge derer einzelne Polizeistationen stündlich über ihre Arbeit berichteten – via „Twitter“, einer Kommunikationsplattform, die ihren Nutzern erlaubt, Textnachrichten mit maximal 140 Zeichen zu versenden. Die Aussendungen stießen auf großes Interesse in der Bevölkerung. Zudem werde laut Denef durch eine solche Einbeziehung der

Großbritannien: Polizeistationen berichten über ihre Arbeit via „Twitter“.

Öffentlichkeit eine engere und vertrauensvollere Beziehung zwischen der Polizei und der Bevölkerung gefordert.

IT-Trends der Polizei in Europa. Seit dem Beginn von „Composite“ wurden sechs IT-Trends identifiziert, die alle befragten Behörden beschäftigen – Systemintegration, erhöhte Mobilität, Überwachungstechnologie, digitale Biometrie, Probleme mit der Nutzerakzeptanz und „Social Media“. Aufbauend auf diesen Grundelementen sollen in den kommenden Jahren die Polizeieinheiten der am Projekt beteiligten Länder stärker miteinander verknüpft werden; auch über Landes- und Staatsgrenzen hinweg. Laut FIT ist beispielsweise für das Dreiländereck Deutschland/Belgien/Niederlande ein „Intranet“ geplant. Ein weiteres Thema des Projekts ist der Umgang mit Geo-Daten, wie GPS-Koordinaten von Streifenwagen und der Einsatz von mobilen Fingerabdruck-Scannern, um die Koordination und den Ablauf von Einsätzen effizienter zu gestalten. Auch die Nutzung von Hilfssystemen bei der Videoüberwachung wird im Zuge des Projektes diskutiert.

In einem nächsten Schritt soll das Projekt auf die gesamteuropäische Ebene ausgeweitet werden. Dazu ist ein europaweiter Workshop zum Thema „Social Media“ mit Experten der Polizei und Zulieferfirmen geplant.

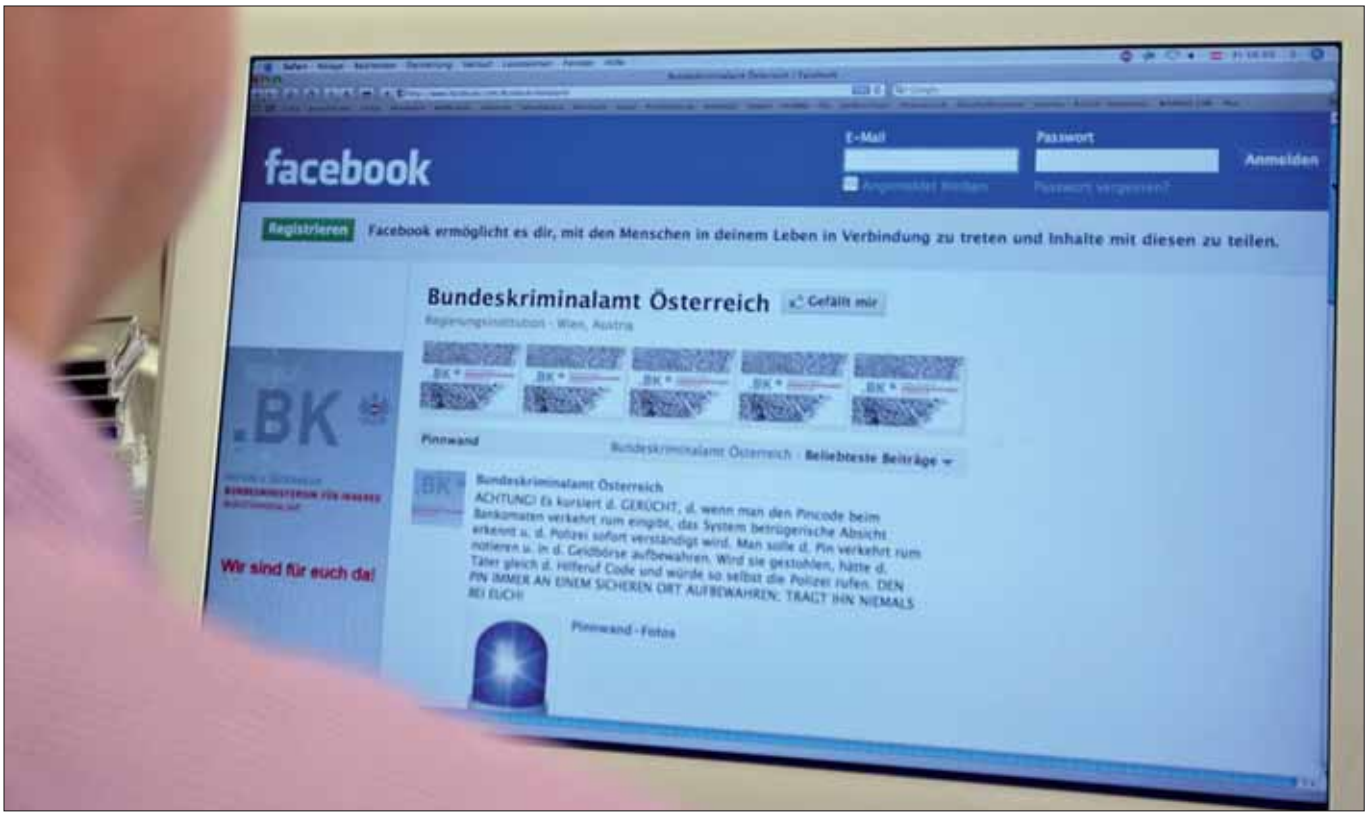
„Facebook“ im Dienst. Auch in Österreich soll die Bevölkerung verstärkt in polizeiliche Arbeiten eingebunden und über deren Fortschritte informiert werden. Das Bundeskriminalamt (BK) nutzt beispielsweise die Internet-Plattform „Facebook“ für die Information und Prävention. Das Bundesministerium für Unterricht, Kunst und Kultur betreibt als erstes österreichisches Ministerium seit August 2010 eine eigene „Facebook“-Seite.

Risiken und Nebenwirkungen sozialer Netze. In den Anfängen bestand das Internet hauptsächlich aus statischen HTML-Seiten mit Text und Bildern. Heute gilt Interaktivität, die vorwiegend in sozialen Netzwerken gelebt wird – und der Cyberkriminalität neue Wege öffnet.

„Gefällt mir“ nennt sich der wohl bekannteste „Button“ in der Welt des Internets. Auf der Plattform „Facebook“ betätigen ihn stündlich mehrere Hundert Nutzer, um ihr Gefallen, ihre Unterstützung oder schlicht ihre Präsenz auszudrücken. Was harmlos wirkt, kann schlimme Konsequenzen haben. So wollte die Engländerin Rebecca J. im September 2010 per „Facebook“ 15 Freunde zu ihrer Geburtstagsfeier einladen. Beim Versenden der Nachricht machte sie allerdings einen Fehler, sodass sich rund 21.000 „Freunde“ zu der Feier anmeldeten, berichtete der britische „Telegraph“. Die Polizei wurde alarmiert, das Fest abgesagt.

Dieses Beispiel illustriert die Entwicklungen des „Mitmach-Web“ in den vergangenen Jahren: Mittels Weblogs, Foren, Videoplattformen und sozialen Netzwerken haben Nutzerinnen und Nutzer die Möglichkeit, sich ohne großen Aufwand online zu präsentieren, Gleichgesinnte zu finden und sich mit ihnen auszutauschen. Laut einem Ratgeber der Arbeiterkammer Wien aus dem Jahr 2009 nutzten in Europa im Jahr 2008 rund 42 Millionen Menschen regelmäßig soziale Netzwerke im Internet – Tendenz steigend. Laut dem Themenportal „Europe’s Information Society“ zählten 2009 in Österreich die Internetauftritte „Youtube“, „Facebook“ und „MySpace“ zu den 20 meistbesuchten Seiten im World Wide Web.

FOTO: GREGOR WENDA



Das Bundeskriminalamt nutzt die Internet-Plattform „Facebook“ zur Information und für die Prävention.

Im Netz der Gefahren. Global agierende Hacker versuchen dieses Verhalten auszunutzen. Mit gefälschten E-Mails versuchen sie, sich persönliche Daten von Nutzern zu beschaffen („Phishing“). Auch unfreiwillige Verlinkungen („Social Bookmarks“) stellen ein Risiko dar – Bilder werden ohne Einflussnahme des Nutzers mit Links und Schlagwörtern versehen.

Zusätzlich könnten mit Softwareprogrammen online auffindbare Bilder einer Gesichtserkennung unterzogen werden – ein Abgleich mittels CBIR (Content Based Image Retrival) ermöglicht sogar die Ortung der abgebildeten Nutzer.

Derartige Praktiken können unter anderem zum „Cyber-Bullying“ führen – vergleichbar dem Mobbing am Arbeitsplatz. Praktiken, die verheerende Folgen haben können. So nahm sich in den USA im Jahr 2007 ein 13-jähriges Mädchen wegen Online-Mobbings das Leben. Auch Sexualstraftäter sind vermehrt in sozialen Netzen vertreten. Sie geben sich gegenüber Jugendlichen oder Kindern als gleichaltrige „Freunde” aus und arrangieren Treffen in der „realen Welt“.

Mobiltelefone im Visier. Von den Gefahren, die das Internet mit sich bringt, bleiben auch Smartphones nicht verschont – Mobiltelefone, die mit Zusatzdiensten wie Internetzugang, E-Mail-Postfach und Navigationsprogrammen ausgestattet sind. Immer häufiger werden sie zum Angriffsziel von Cyberattacken, wie der aktuelle „Internet Security Threat Report“ von *Symantec* zeigt. Besonders betroffen sind Nutzer von „Facebook“, „Twitter“ und dem Google-Handybetriebssystem „Android“. Für das Jahr 2010 machte *Symantec* weltweit über 286 Millionen neue Bedrohungen aus. Vor allem die Zahl von gezielten Attacken, bei denen spezielle Toolkits – Baukästen für Cyber-Attacken – verwendet werden, hat im Vergleich zu 2009 um 93 Prozent zugenommen.

In Europa gilt Deutschland bei Internet-Kriminellen als das beliebteste Land. In Österreich scheint die Tendenz leicht rückläufig: Laut dem *Symantec*-Bericht befand sich Österreich im Jahr 2009 noch auf dem 40. Platz im Ländervergleich; 2010 belegte es den 44. Rang. Hingegen nahmen Aktivitäten von Cyber-Kriminellen in den Niederlanden und Südkorea drastisch zu.

Unbekannt sicher. Um dennoch nicht gänzlich auf die neuen Medien verzichten zu müssen, raten Experten ein vernünftiges und vorausblickendes Verhalten im „Netz“. Das Verwenden unterschiedlicher Kennnamen, Passwörter und mehrerer E-Mail-Adressen spielt dabei eine wesentliche Rolle – Aktivitäten von Einzelpersonen können so schwieriger nachverfolgt werden.

Auch die Einrichtung einer wirksamen Internet-Security-Software ist ratsam, ebenso wie ein vorsichtiger Umgang mit Kontaktdaten und Bildern. Zudem sollten die Nutzungsbedingungen einzelner Plattformen unbedingt gelesen werden. *Hellin Sapinski*

Quellen:
Bauser Enterprises IT: www.bauserenterprises.com/html/web_2_0.html
Europe’s Information Society: http://ec.europa.eu/information_society/activities/social_networking/facts/index_en.htm
Fraunhofer-Studie: www.fit.fraunhofer.de/fb/ucc/projects/composite.html
Internet Security Threat Report: http://www.symantec.com/business/threatreport/index.jsp
Ratgeber der Arbeiterkammer: www.arbeiterkammer.at/bilder/d101/RatgeberSozialeNetzwerke.pdf
Telegraph:www.telegraph.co.uk/technology/facebook/8012043/Girl-14-fears-21000-party-guests-after-Facebook-invite-blunder.html
Zeit online: www.zeit.de/digital/2009-09/facebook-gaydar-myspace

Foto: Alexander Tuma