Ein Ausweg aus dem Gedränge

Foto: APA

Beim Wiener Marathon sind bis zu 400.000 Menschen auf der Straße, die den Läufern zujubeln oder auf andere Art an dem Spektakel Anteil nehmen. Eine App, die an der Johannes-Kepler-Universität Linz entstanden ist, erhebt, verstreut in der Menge, Daten über die Personendichte und hilft damit den Menschenmassen, sich besser zu koordinieren.

Das Smartphone kann auch als Sensor für Menschenmassen dienen. Linzer Forscher haben den Wiener City Marathon mit einem Werkzeug ausgestattet, das Besuchern hilft, Massendrängereien aus dem Weg zu gehen.

Alois Pumhösel

Wien – Wie jedes Jahr waren beim vergangenen Vienna City Marathon (VCM) am 12. April bis zu 400.000 Menschen auf den Beinen. Sie säumen die Strecke, fahren mit Öffis kreuz und quer durch die Bezirke. Sie feuern ihre Angehörigen an, holen sie vom Ziel ab. Gerade um den Wiener Heldenplatz herum ballt sich die Menge oft gewaltig zusammen. Menschenansammlungen dieser Größe bergen eine Gefahr in sich. Zuletzt hat das das Unglück bei der Loveparade 2010 in Duisburg bewiesen, bei dem 21 Menschen in der Menge erdrückt wurden.

Die Menschenschwärme scheinen nicht so wie jene des Tierreichs zu funktionieren. Laut Studien passen dort Fische, Insekten oder Fledermäuse Geschwindigkeit, Richtung und Abstand an ihre Nachbarn an. Der Homo sapiens mit seinen rationalen Plänen und spontanen Entscheidungen neigt bei Zusammenkünften hingegen dazu, sich selbst unwissentlich zu gefährden.

Mit der richtigen Art von Vernetzung ließe sich die Selbstorganisation von Menschenmassen aber verbessern, ist Alois Ferscha vom Institute for Pervasive Computing der Johannes-Kepler-Universität Linz überzeugt. Er ist einer der Entwickler eines Systems, das den Teilnehmern von Großveranstaltungen mehr Überblick über die Verteilung der Menschenmenge verleihen soll – und das in Echtzeit. Die Technik, die den Marathonveranstaltern gleichzeitig als Frühwarnsystem für Gefahrensituationen durch unvorhersehbares Massenverhalten dient, ist als Teil der Marathon-App im Einsatz.

„Die Frage, mit der wir uns beschäftigt haben, ist, wie man in einer realen Situation die Dichte in Menschenmengen messen kann und ab welcher Konzentration diese kritisch für die Sicherheit des Einzelnen wird", erläutert der Computerwissenschafter. Laut Studien komme es ab durchschnittlich 3,5 gehenden Menschen pro Quadratmeter zu ersten unabsichtlichen Körperkontakten, ab einem Wert von 5,5 wird es gefährlich, erläutert Ferscha. Bei stehenden Personen wird es ab einem Wert von 7,1 pro Quadratmeter kritisch. Die Konzentrationsmessung erfolgt in vielen Fällen mithilfe von Sensoren und Kameras, die an öffentlichen Plätzen, Fahrzeugen oder Drohnen montiert sind. Anstelle dieser Beobachtung „von außen" hatten Ferscha und Kollegen die Idee, dass sich Menschenmengen selbst organisieren, indem sie die Daten bezüglich der sozialen Dichte selbst kooperativ erheben und untereinander teilen. Als Sensorplattform sollte dazu das Smartphone dienen. Die Grundlagen wurden im Rahmen des EU-Projekts Socionical (Complex Socio-Technical System in Ambient Intelligence) gemeinsam mit Partnern wie der ETH Zürich, des Deutschen Forschungszentrums für Künstliche Intelligenz und der TU München geschaffen.

Smartphone als Sensorstation

Die Technik, so wie sie nun beim Wiener Marathon zur Anwendung kam, beruht darauf, dass sich Benutzer der App dafür entscheiden, anonymisierte Sensordaten ihres Smartphones zur Verfügung zu stellen. Von Jahr zu Jahr steigen die Nutzerzahlen, heuer waren es knapp 20.000. Jedes der aktivierten Geräte nutzt die Bluetooth-Funktion, die üblicherweise Datenübertragungen auf kurzen Distanzen – etwa für ein Headset – möglich macht, um die Signalstärke benachbarter, ebenfalls aktivierter Geräte zu messen, sagt Ferscha. Durch die Analyse des Verhältnisses von Funksignal und Hintergrundrauschen, der Signal-to-Noise-Ratio (SNR), wird die Entfernung zu weiteren Smartphones in der unmittelbaren Umgebung abgeschätzt.

Gemeinsam mit den GPS-Positionen werden diese Daten zur Auswertung an einen Server gesendet. Dort werden sie ins Verhältnis mit der erwarteten Gesamtanzahl der Menschen gesetzt und mit farblichen Abstufungen auf einem Stadtplan veranschaulicht. Grüne Flächen bedeuten eine bereits dichte Menschenansammlung, bei Gelb und Rot wird es kritisch. Ein Vorteil des Systems sei zudem, dass es bereits gut funktioniere, wenn nur wenige Prozent der Menschen ihre Daten zur Verfügung stellen. „Mit den 20.000 Nutzern kann man eine verlässliche, statistisch signfikante Schätzung der aktuellen sozialen Dichte erreichen", so Ferscha.

Der Forscher betont dabei die hohen Datenschutzstandards des Service: „Die Sammlung der Daten ist auf ein Zeitfenster zwischen acht und 16 Uhr beschränkt. Neben den relevanten Sensordaten wird lediglich eine Identifikationsnummer des Handys mitgeschickt. Keine Namen, keine sonstigen Informationen."

Gefahrenzonen entdecken

Die Besucher können dank der Visualisierung der „crowd density" dem dichten Gedränge vorausschauend aus dem Weg gehen. Das hilft bei der Selbstregulierung der Masse. Den Sicherheitskräften helfen die Daten bei der Abschätzung möglicher Gefahrenherde. Bei ihrem Einsatz 2013 habe die App etwa eine potenziell gefährliche Menschendichte für das Umfeld des Heldenplatztors beim Volksgarten angezeigt, weil viele herein- und hinausströmende Menschen aufeinandertrafen. Die Veranstalter setzten daraufhin dort mehr Personal ein, um die Personenströme zu regulieren.

Und noch eine weitere Art von „Schwarmverhalten" entdeckten die Forscher. „Wir wunderten uns, dass im Prater ein Platz noch gelb aufleuchtete, als der Marathontross längst weg war", erinnert sich Ferscha. „Dann wurde uns klar, dass das mit einem bekannten Gastgarten dort zu tun hat."

Den Datendiebstahl rechtzeitig erkennen

Niederösterreichs erstes Josef-Ressel-Zentrum konzentriert sich auf die Abwehr von Cyberspionage

Sankt Pölten – Eine Spionagesoftware, die in den vergangenen Jahren Informationen von Einzelpersonen, Behörden und Forschungseinrichtungen ausgespäht hat: das ist zum Beispiel Regin. „Ein hochkomplexer Trojaner, der von Experten für bestimmte Aufgaben in monatelanger Arbeit maßgeschneidert wurde. Code-Vergleiche legen nahe, dass es sich um ein Instrument der NSA handelt", erläutert Sebastian Schrittwieser, Dozent am Department Informatik und Security der FH Sankt Pölten. Nachdem Regin bekannt wurde, konnte er im Herbst 2014 auch auf Rechnern in Österreich identifiziert werden.

Um derartigen Angriffen in Zukunft besser begegnen zu können, startete nun an der FH Sankt Pölten das von Schrittwieser geleitete Josef-Ressel-Zentrum für die konsolidierte Erkennung gezielter Angriffe – das erste seiner Art in Niederösterreich.

Gemeinsam mit den Firmenpartnern Ikarus Security Software und SEC Consult sollen Strategien gefunden werden, um Spionage- und Sabotagesoftware frühzeitig zu erkennen. Im Rahmen von Ressel-Zentren fördert das Wissenschafts- und Wirtschaftsministerium anwendungsorientierte Forschungskooperationen zwischen FHs und Unternehmen. Vorbild sind die Christian-Doppler-Labore an Universitäten.

Konventionelle Viren sind auf eine rasche Verbreitung ausgerichtet. Sie sollen an möglichst vielen Computern Schaden anrichten. Einmal entdeckt, werden ihre Signaturen in die Datenbanken der Antivirenprogramme aufgenommen. Die Chance, spezialisierte Schadprogramme à la Regin zu enttarnen, ist aber durch deren geringe Verbreitung ungleich geringer, sagt Schrittwieser. In manchen Fällen werden sie etwa vor Ort per USB-Stick im gewünschten Netzwerk platziert. Außerdem sind die Trojaner natürlich darauf ausgerichtet, ihre Aktivitäten möglichst gut zu verstecken. Die konventionelle, signaturbasierte Methode greift bei diesen Attacken nicht.

„Wir müssen also dahin kommen, das schädliche Verhalten eines Programms aufgrund seiner Auswirkungen auf das System zu erkennen", so Schrittwieser. Eine einzelne Aktion des Programms – etwa das Anlegen einer Datei oder der Verbindungsaufbau zu einem Server im Internet – mag für sich noch unverdächtig sein. Aus dem Zusammenspiel vieler kleiner Einzelereignisse inmitten der zigtausenden Prozesse, die in einem Computersystem täglich ablaufen, könne man aber gegebenenfalls auf bösartige Absichten schließen. „Wenn ein Programm von einem USB-Stick gestartet wird und gleich danach Daten auf einen externen Server geschickt werden, könnte das auf eine Spionagesoftware hindeuten", gibt der Informatiker ein einfaches Beispiel. Derartige verdächtige Kombinationen sollen systematisch modelliert werden.

Gemeinsam mit dem Firmenpartner Ikarus konzentrieren sich Schrittwieser und Kollegen auf die Analyse von Ereignissen in Unternehmensnetzwerken, mit SEC Consult will man sich auf die Suche von Schwachstellen und Hintertüren in Softwaresystemen begeben. (pum)