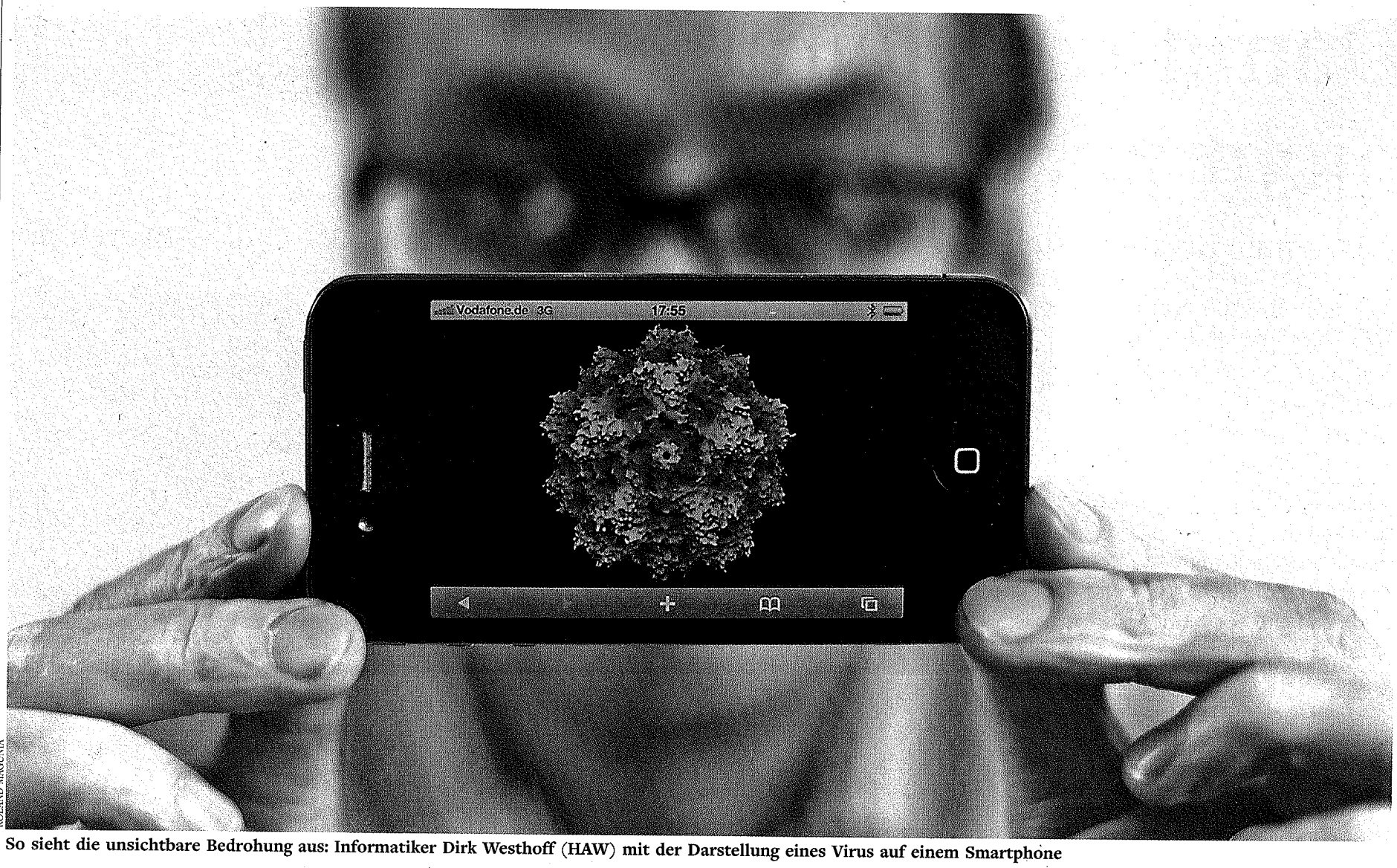

ROLAND MAGUNIA

So sieht die unsichtbare Bedrohung aus: Informatiker Dirk Westhoff (HAW) mit der Darstellung eines Virus auf einem Smartphone

Impfung gegen Angriffe aus dem Nichts

Hamburger Informatiker entwerfen Immunsystem für Smartphone und Co.

■ Das Projekt SKIMS zielt darauf ab, ein einheitliches Sicherheitssystem für mobile Geräte zu entwickeln.

GISELA SCHÜTTE

Die neuen Smartphones sind das Vergnügen ihrer Anwender, die damit telefonieren, fotografieren, navigieren, Musik hören, im Internet surfen und Spiele spielen können. Sie sind die Freude der Hersteller und Anbieter, die damit glänzende Geschäfte mit guten Zukunftsaussichten machen. Und sie sind von wachsendem Interesse für Kriminelle, die mit den mobilen Alleskönnern der anderen Geschäfte machen wollen: Nutzer des mobilen Internets werden zunehmend zum Ziel für großflächige Angriffe aus dem Netz.

Mit genau dieser Problematik befasst sich jetzt ein Forschungsprojekt an der Hochschule für Angewandte Wissenschaften (HAW). Unter dem Namen „Schichtenübergreifendes kooperatives Immunsystem für mobile mehrseitige Sicherheit" (SKIMS) werden die Wissenschaftler für 30 Monate unterstützt bei der Suche nach einem Konzept zur Sicherung des mobilen Internets.

SKIMS wird mit knapp einer Million Euro vom Bundesministerium für Bildung und Forschung im Rahmen der Schwerpunktmaßnahme „Sicherheit in unsicheren Umgebungen" gefördert. Der Projektleiter für SKIMS an der HAW ist Professor Dirk Westhoff. Ebenfalls mit von der Partie ist Professor Thomas Schmidt, der gegenwärtig auch ein Projekt zur Erforschung eines mobilen und servicefreundlichen Internets leitet. Um den komplexen Bedrohungen wirksam begegnen zu können, hat das Team, das sich aktuell in der Startphase befindet, starke Partner an seiner Seite.

Das sind der Mobilfunkexperte und Leiter des Berliner Forschungsforums Öffentliche Sicherheit, Professor Jochen Schiller von der Freien Universität, das DFN-CERT, ein Dienst des Deutschen Forschungsnetzes im Hinblick auf Sicherheitsprobleme im Datennetz, die Escrypt GmbH (ein Systemhaus) sowie der internationale Elektronik- und Software-Riese NEC Europe als assoziierter Partner aus der Wirtschaft, der den Blick auf die Marktrelevanz der Konzepte hält. Es ist ein renommiertes Projekt, das die Wissenschaftler an die HAW holten. Denn das Team setzte sich gegen hochrangige nationale Konkurrenz durch. Insgesamt hatten sich mehr als 50 Konsortien beworben.

Der Neu-Hamburger Dirk Westhoff stammt aus dem Ruhrgebiet. Nach Studium und Promotion arbeitete er zehn Jahre lang in einem Forschungslabor in Heidelberg bei der Firma NEC, zuletzt als „Chief-Researcher". Bereits in der Pfalz hatte er sich mit Sicherheitsfragen im Zusammenhang mit der Datenerhebung befasst, zum Beispiel im Zusammenhang mit Sensorknoten, die in den Weinbergen die Bodenfeuchtigkeit überwachten. Auch dabei geht es um verfügbare Datenübertragung, Robustheit und nicht zuletzt Datensicherheit. 2009 folgte der Informatiker dem Ruf an die HAW. „Die Angriffsmöglichkeiten werden allgegenwärtig", sagt Dirk Westhoff. Ursache seien die zahlreichen Geräteschnittstellen sowie die Verbindung zum Internet. Die neuen Geräte wie die Smartphones nutzen UMTS, WLAN und/oder Bluetooth.

Gleichzeitig wachse der Markt mit den Geräten rasant und damit der Anreiz für Unbefugte, auf die Systeme zuzugreifen. Bald aber werde es so viele Mobilgeräte mit Internetzugang geben, dass sich an öffentlichen Plätzen meist ganze Gruppen in WLAN- beziehungsweise Bluetooth-Funkreichweite zueinander befinden. Unterdessen sind diese Mobiltelefone leistungsschwächer und häufig schneller verwundbar als Standard-PCs. Sie haben nicht die Rechenkapazitäten, um sich durch herkömmlichen Virenschutz zu sichern.

Genau so eine Immunisierung gegen die Angriffe aus der Luft wird nun aber gesucht, damit sensible Daten nicht zur leichten Beute für Unbefugte werden. „Heute müssen wir Adressbuch und Kalender auf dem Handy schützen. In naher Zukunft, wenn wir per ‚Near Field'-Kommunikation mit dem Handy bezahlen, könnten ohne den Einsatz von Schutzsystemen Passanten unsere elektronische Geldbörse angreifen", so Westhoff.

> „Die Herausforderung liegt darin, mit geringem Aufwand unbekannte Angriffe zu blockieren"
>
> **Professor Thomas Schmidt**

Deshalb müssen Smartphones und Co. lernen, Angriffe aus der Luft zu erkennen und abzuwehren. „Die Herausforderung liegt darin, mit geringem Aufwand unbekannte Angriffe zu blockieren", sagt auch Professor Thomas Schmidt. Eine präventive Möglichkeit sei die Entwicklung sogenannter mobiler Honeypots. Das sind kleine Programme, die Angreifer ausspähen und in die Irre leiten. „Mit einfachen Strukturanalysen der empfangenen Daten sind wir bereits in der Lage, normale Web-Seiten von schädlichen Programmen zu unterscheiden", so Schmidt weiter. Diese neuen Methoden wollen er und sein Team ausbauen und verfeinern.

Ein weiteres Forschungsfeld sind Maßnahmen gegen Angriffe bei der Übermittlung von Updates für den Betrieb der mobilen Geräte. Dabei werden Datenmengen, die für viele Empfänger bestimmt sind, im Rahmen sogenannter Fontänencodes zerhackt und dann am Bestimmungsort wieder zusammengesetzt. Die Übertragung, so Westhoff, sei robuster gegen Störquellen. Allerdings sind auch hier noch Schutzmaßnahmen gegen Manipulationen zu erarbeiten.

Dirk Westhoff und Thomas Schmidt konzentrieren sich mit dem Hamburger Modul des Forschungsprojekts an der HAW auf das Thema „Verteilte Angriffserkennung und Abwehr". Dabei geht es darum, gegen bekannte Angreifer und gegen verdächtige Software vorzugehen. Dabei stellt sich die Frage, ob sich mobile Endgeräte gemeinschaftlich gegen Angriffe schützen können oder ob man mobile Sicherheit als sogenannten Dienst in der Cloud auffasst und damit auf eine Prüfung via Festnetz setzt.