Interview Professor Michael Backes, Direktor des CISPA und Professor für Informationssicherheit und Privacy an der Universität des Saarlandes

Frage: *Herr Prof. Backes, könnten Sie zunächst einmal umreißen, was man alles unter IT-Sicherheit versteht?*

Prof. Backes: Ich kann es gerne versuchen. IT-Sicherheit ist ein sehr breites Thema, es hat viele Komponenten insbesondere zum Beispiel neue Algorithmen, die Verschlüsselungen aber auch generell Analyse von zum Beispiel Systemen und Anwendungen bis zu auch Analyse und Konstruktion von neuen Systemen mit neuen Sicherheitseigenschaften. Generell ist IT-Sicherheit eine Querschnittsdisziplin, das heißt wir haben Anknüpfungspunkte mit so ziemlich jeder anderen Disziplin in der Informatik, sei es mit der Konstruktion von Systemen, mit der Analyse von Algorithmen, sei es auch mit Computergrafik oder Bio-Informatik.

Frage: *Wir hören derzeit ständig davon, dass unsere Internetaktivitäten, unser E-Mail-Verkehr bis hin zu Telefonverbindungsdaten und vielleicht sogar die Telefonate selbst aufgezeichnet und von Firmen oder Geheimdiensten ausgewertet werden. Besteht aus Sicht der Forschung überhaupt eine Möglichkeit, derartige Aktivitäten zu unterbinden?*

Prof. Backes: Zum Teil ja, zum Teil hängt es stark an den Benutzern. Zum Beispiel, wenn sie E-Mails verschicken möchten oder einfach kommunizieren möchten, könnten sie zum Beispiel so genannte „Ende zu Ende-Verschlüsselung“ benutzen. Das würde in der Tat das Problem zu einem großen Teil lösen. Andere Dinge sind komplexer. Wenn sie zum Beispiel das Internet benutzen um zum Beispiel zu googlen, dann muss ihnen bewusst sein, dass die Daten, die sie bereitwillig preisgeben im Allgemeinen auch verloren sind, das heißt dort hilft eigentlich nur noch sich klar zu machen, was akzeptiere ich, wem vertraue ich, was toleriere ich und dementsprechend muss ich mich dann eben verhalten.

Frage: *Manche gerade jüngere Menschen gehen oft sehr sorglos mit ihren Daten um. Kann die Forschung Gefahren abwehren oder müssen die Menschen selber immer wieder darauf hingewiesen werden, keine wichtigen Daten im Netz preiszugeben.*

Prof. Backes: Sie brauchen beides. Im Endeffekt ist es so, das was Menschen bereitwillig preisgeben von sich, gegen das kann man sie eigentlich nicht schützen. Das ist ihre zum Teil bereitwillige Selbstentfaltung, das heißt, wenn Leute einfach gewisse Dinge teilen möchten, ist es ihr gutes Recht. Was die Forschung kann, zu mindestens prinzipiell, ist Konsequenzen aufzuzeigen, einfach bildlich zu demonstrieren, was mit den Daten passieren könnte, wer sie sehen könnte, was schlimmsten Falls eintreten könnte und den Benutzern zu mindestens die Möglichkeit geben zu entscheiden, ob dies akzeptabel ist oder nicht.

Frage: *Könnten Sie noch etwas dazu sagen, was man sich konkret unter IT-Sicherheitsforschung vorstellen kann. Geht es vor allem um Programmierung immer neuer Verschlüsselungen oder um Hardwareentwicklungen oder liegt der Schwerpunkt ganz wo anders?*

Prof. Backes: Es ist eigentlich eher woanders. Verschlüsselung war früher das ganz große Thema, inzwischen sind Verschlüsselungsalgorithmen sehr gut geworden. Natürlich programmieren sie auch, natürlich entwickeln sie auch Hardware. Typischerweise geht es aber um Systeme, um Software, das heißt wie kann man neue Systeme entwickeln, die gewissen Sicherheitsanforderungen haben oder wie kann man bestehende Systeme analysieren. Ein klassisches Beispiel, was momentan sehr on Vogue ist, ist zum Beispiel Mobilsicherheit also verstehen, wie zum Beispiel Apps auf ihre Daten zugreifen können, auf Ihr Mobiltelefon. Und wie sie dies eventuell unterbinden können, so dass die Apps immer noch das tut was sie sollen nur eben ohne ihre Daten abzugreifen und in die Welt zu schicken.