Die Referenten vom Chaos Computer Club Mannheim bei ihrem Vortrag

Online-Nutzerdaten als sicherheitspolitische Herausforderung

Der Facebook-Skandal um das Datenanalyseunternehmen Cambridge Analytica im Frühling dieses Jahres hat offenbart, dass womöglich mit Online-Nutzerdaten Präsidentschaftswahlen manipuliert werden können. Daher stellt sich mehr denn je die Frage: Was wissen andere über mich, wenn ich im Internet unterwegs bin?

Der Vorstand der Hochschulgruppe für Außen- und Sicherheitspolitik der Universität Mannheim

Um diese Frage zu beantworten und auch kleine Empfehlungen zur Selbstverteidigung im Netz zu geben, hat die Hochschulgruppe für Außen- und Sicherheitspolitik der Universität Mannheim zwei Mitglieder des Chaos Computer Club (CCC)Mannheim eingeladen.

Gemäß den Referenten, die in der Hacker-Szene auf die Namen „stean“ und „HASH1“ hören, ist die anlasslose Daten- und Informationssammlung über Bürger an sich kein neues Phänomen. Denn schon im Deutschen Kaiserreich seien Informationen gesammelt worden, zum Beispiel in Form von Listen über Homosexuelle im Land. Diese sogenannten Rosa-Listen galten zunächst als unbedenklich, bis sie in Nazi-Deutschland zur Verfolgung und Vernichtung eingesetzt wurden. Mit diesem erschreckenden Beispiel verdeutlichten die Referenten die Brisanz der digitalen Datenspeicherung. Was zunächst nach unwichtigen Daten aussieht, könnte in ein paar Jahren für ungeahnte Dinge verwendet werden.

Der größte Unterschied zur damaligen Zeit sei „stean“ und „HASH1“ zufolge, in welcher Größe und Menge Informationen gespeichert werden können. Während die vom Ministerium für Staatssicherheit der DDR gesammelten Daten ausgedruckt etwa 48 000 Aktenschränke entsprächen, sei die National Security Agency der USA im Besitz von fünf Zettabytes Daten. Professor Dr. Mathias Ludwig vom Institut für Didaktik der Mathematik und der Informatik an der Goethe-Universität Frankfurt am Main verbildlicht diese astronomische Zahl mit einem Flächenvergleich: Würde man fünf Zettabytes an Daten auf Din-A4-Papier ausdrucken, könnte die Erde mit der damit ausgedruckten Blattmenge 150 Mal zugeklebt werden.

Die zuvor genannten Beispiele sind Programme von staatlicher Seite. Doch wie verhält es sich mit kommerziellen Beobachtern, wie Facebook einer ist? „Während der Staat zur Datensammlung einen enormen Aufwand betreibt, sitzen Social-Media-Unternehmen direkt an der Quelle“, sagte einer der Referenten. Diese seien weniger an der direkten Überwachung, als an sogenannten Meta-Daten interessiert. Es würden keine direkten Inhalte gespeichert, sondern vielmehr Daten über die Daten, also wo, wann und wie die Nachricht verfasst wurde. Am Beispiel eines Instant-Messaging-Dienstes zeigten die Referenten, was alles beobachtbar ist. Von Abrufzeiten über Konversationen, bis hin zu Arbeitszeiten, all diese Informationen ließen sich aus den Daten gewinnen. „Durch eine Analyse der Nachrichtenseite Spiegel kannte ein CCC-Hacker am Ende die gesamte Belegschaft, ohne jemals mit ihnen in Kontakt gewesen zu sein“, merkte einer der beiden Chaos Computer Club-Mitglieder an.

Eine zusätzliche Gefahr gehe zudem von Beobachtern dritter Art aus. Durch Phishing E-Mails versuchen kriminelle Banden, Geld von ahnungslosen Nutzern zu bekommen. Wie leicht so etwas geht, zeigten die Referenten direkt vor Ort. Mithilfe eines selbstgeschriebenen Programms bekam die ausgewählte E-Mail-Adresse binnen Sekunden eine Nachricht von Angela Merkel angezeigt. Dass die Nachricht ein Fake war, sei nur auf den zweiten Blick ersichtlich gewesen.

Neben all den Beispielen, die die Gefahren der Datenspeicherung verdeutlichen, gaben die Referenten eine Empfehlung, wie solche Risiken minimiert werden können. Unmittelbar an den theoretischen Teil anknüpfend, erläuterte „stean“ die Funktionsweisen der asymmetrischen Verschlüsselung beim E-Mail-Verkehr und wie man sie nutzen kann. Schritt für Schritt installierte sich jeder Besucher daraufhin das Programm Enigmail, das vor Fake-Emails schützen kann.

Jonas Verch