

Mathe studiert – und dann?

Kristina Vaillant

Hackerangriffe auf Kommunikationsnetze werden immer professioneller – resümiert das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem Lagebericht für 2014. Für Mathematiker gibt es daher viel zu tun, denn sie arbeiten in Schlüsselbereichen des Amtes, so wie Andreas Könen. Der Mathematiker steht dem BSI seit Anfang 2013 als Vizepräsident vor. Seine Karriere begann mit der Entwicklung und Überprüfung kryptografischer Verfahren, dem klassischen aber nicht einzigen Arbeitsgebiet von Mathematikern am BSI.

Herr Könen, im aktuellen Lagebericht beklagt das BSI, dass Cyberkriminelle immer zielgerichteter vorgehen. Was kann das BSI dagegen unternehmen und warum braucht es dafür Mathematiker?

Ganz allgemein ist es das Ziel des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die IT-Sicherheit in Deutschland voranzubringen. Das heißt, wir untersuchen und bewerten bestehende Sicherheitsrisiken und schätzen die Auswirkungen neuer Entwicklungen auf diesem Gebiet ab. Auf dieser Grundlage informieren wir, geben Sicherheitsempfehlungen, beraten und zertifizieren. Hinsichtlich des Schutzes vor Cyberattacken geht es darum, dass Institutionen in ihren Kommunikationsnetzen besondere Sicherheitstrennungen einführen, dass sorgfältig nach Schadsoftware gesucht wird und dann innerhalb der Netze vor allem Verschlüsselung eingesetzt wird, um Daten, die besonderen Wert besitzen, gegenüber dem Zugriff Fremder zu schützen.

An wen richtet sich das BSI mit dem Angebot?

Wir sind in erster Linie der zentrale IT-Sicherheitsdienstleister für den Bund, aber wir wenden uns mit diesem Angebot auch an private und gewerbliche Nutzer, an Hersteller sowie Anbieter von Informationstechnik.

Wo kommt die Expertise von Mathematikern ins Spiel?

Ich habe im Grunde schon zwei Bereiche genannt, in denen Mathematiker am BSI eine ganz wichtige Rolle spielen. Beim Thema Kryptografie und bei der Sicherheit in Kommunikationsnetzen. Von Anfang an, seit es das BSI gibt, waren Mathematiker diejenigen, die mathematisch-kryptografische Verfahren eingeführt, geprüft und zusammen mit Technikern zur Einsatzreife gebracht haben. Und sie sorgen auch dafür, dass diese Verfahren später im Einsatz stark genug bleiben, um Angriffen zu widerstehen. Der andere Bereich ist die Sicherheit in Netzen. Welche Rolle Mathematiker da spielen, ist von außen nicht so offensichtlich. Aber allein schon wenn es um die Erkennung von Schadsoftware in Netzen geht, sind wir auf ihre Expertise angewiesen.

Inwiefern?

Es geht darum, wie man Schadsoftware findet, wie man Indikatoren entwickelt, mit deren Hilfe aus einem riesigen Datenaufkommen genau diese eine Mail herauspickselt werden kann, die mit Schadsoftware versehen ist. An solchen Aufgaben arbeiten bei uns Mathematiker gemeinsam mit Technikern und Informatikern. Und diese Aufgaben werden immer wichtiger. Wir müssen uns mit Big Data beschäftigen, wenn wir zukünftig Gefährdungen analysieren wollen.

Worum geht es – mathematisch gesehen – bei den kryptografischen Verfahren?

Kryptografie ist nichts anderes als die Entwicklung von Algorithmen. Es geht darum, mit mathematisch beweisbaren Methoden sicherzustellen, dass ein kryptografisches Verfahren, ein Public-Key-Verfahren, funktioniert und tatsächlich allen Angriffen standhält. Das ist eine echte mathematische Aufgabe. Die Mathematiker, die bei uns auf diesem Gebiet arbeiten, publizieren oft nebenher in wissenschaftlichen Fachzeitschriften, weil sie ihr Wissen permanent weiterentwickeln.

Wie sind Sie an das Bundesamt für Sicherheit in der Informationstechnik gekommen?

Ich bin seit 2006 am BSI und war zunächst Leiter des Stabes des Präsidenten. Danach habe ich mich in zwei verschiedenen Fachbereichen mit dem Schutz kritischer Infrastrukturen und der Beratung in der Informationssicherheit befasst. Vorher war ich in verschiedenen Bereichen der Bundesverwaltung in der Informationssicherheit tätig. Aber begonnen habe ich meinen Berufsweg tatsächlich mit der Entwicklung und Überprüfung von Kryptoverfahren und zwar bei der Vorläuferorganisation des BSI, der in den 50er Jahren eingerichteten Zentralstelle für das Chiffrierwesen, ZfCH, wie sie bis Ende 1988 hieß.

Haben Sie bereits während Ihres Studiums darauf hingearbeitet?

Nein, ich bin über einen Umweg zu meinem Arbeitsgebiet gekommen. Ich habe Mathematik an der Universität zu Köln studiert und mich nach dem Grundstudium der Algebraischen Zahlentheorie zugewandt. Damals nahm ich an einem Oberseminar mit dem schönen, aber sehr abstrakten Thema „Konstruktive Galoistheorie“ teil. Und tatsächlich verbarg sich dahinter zu Teilen eine Auseinandersetzung mit den heute bekannten Public-Key-Verfahren wie RSA und Merkle-Hellmann-Verfahren. Damals, Anfang der 80er Jahre, wurden diese Technologien erstmals eingesetzt. Wir haben uns mathematisch damit auseinandergesetzt, und es war eine Riesenüberraschung, als wir merkten: Mit diesem abstrakten Thema kann man wirklich praktisch etwas anfangen! Dadurch bin ich auf



Andreas Könen (Foto: BSI)

die berufliche Schiene gekommen, die mich letztendlich ans BSI gebracht hat. Heute beruht der elektronische Personalausweis auf diesen Verfahren, und wir im BSI sind diejenigen, die diese mathematischen Verfahren algorithmisch und technisch umgesetzt haben.

Inzwischen sind Sie Vize-Präsident des BSI. Haben Sie im Arbeitsalltag noch mit Mathematik zu tun?

Nicht direkt. Die typische Rolle eines Vizepräsidenten besteht darin, die Aufgaben eines Amtes so zu gestalten und vorwärtszutreiben, dass sie in dem Sinne erledigt werden, wie die Bundesregierung es ihm zugedacht hat. Und wir haben das Glück, dass wir ein sehr lebendiges Aufgabengebiet haben. Jeder weiß, wie tief die Digitalisierung heute in unseren Alltag eindringt. Und zu erkennen, wo Sicherheit hier eine herausragende Rolle spielen muss, das ist die große Herausforderung für unser Amt.

Gibt es Aufgaben, die Ihnen besonders am Herzen liegen?

Ja, spannend wird es für mich besonders, wenn ganz konkrete Gefährdungen im Raum stehen – wie etwa der Stuxnet-Wurm vor einigen Jahren –, und dann zu beurteilen ist, wie wir uns vor Angriffen schützen. Und ich freue mich, wenn ich mich an der einen oder anderen Stelle doch wieder mit dem Einsatz kryptografischer Methoden auseinandersetzen kann, so wie in den letzten Wochen. Da hatte ich mit elliptischer Kurvenkryptografie zu tun. In solchen Momenten fühle ich mich als Mathematiker herausgefordert, das Thema dann auch wirklich zu durchdringen.

Warum steht das Thema elliptische Kurvenkryptografie auf der Tagesordnung?

Die elliptische Kurvenkryptografie ist ein besonderer Zweig der Public-Key-Kryptografie, der international gerade neu standardisiert wird. Wir als BSI spielen da eine wichtige Rolle, weil wir hier hohe Expertise besitzen. In unserem elektronischen Personalausweis haben wir beispielsweise elliptische Kurven als wesentliche Sicherheitsanker eingebaut.

Ist Mathematik für Sie in erster Linie Beruf – oder auch Berufung?

Es ist beides. Ich habe den Ehrgeiz, nebenher hin und wieder zu verfolgen, was in der Mathematik und speziell in der Zahlentheorie passiert. Das ist immer wieder faszinierend. Insofern ist es Berufung. Andererseits Beruf: Gerade die Fähigkeiten, die man im Mathematik-Studium erwirbt, also strukturiert zu denken und ein komplexes Problem so in kleinere lösbare Probleme aufzugliedern, dass sie doch eine Systematik besitzen, die den Blick auf das Ganze ermöglicht – diese Fähigkeiten nimmt man aus der Berufung mit in den Beruf.

Das BSI hat im vergangenen Jahr eine Kampagne gestartet, um Nachwuchsfachkräfte zu rekrutieren.

In der Tat. Wir haben 39 neue Stellen erhalten und die werden wir teilweise mit Mathematikern besetzen. Vor allem in den Bereichen Kryptografie und Cybersicherheit. Ein weiterer Einsatzbereich ist der, der sich mit elektronischen Identitäten befasst, also der Realisierung von sicheren, individuellen Identifikationsmöglichkeiten zum Beispiel im Internet. Wir sind ständig auf der Suche nach jungen, fähigen Absolventen, aber auch Kollegen, die schon eine gewisse Berufserfahrung haben.

Was sollten Bewerber mitbringen?

Neben einer guten fachlichen Qualifikation in Mathematik – die Spezialisierung ist zweitrangig – eine Offenheit für Themen der Informationssicherheit. Das können unmittelbar mathematische Fragestellungen sein, aber Bewerber sollten auch Interesse an gesellschaftlichen Fragestellungen haben. Zum Beispiel: Was bedeutet es, wenn Digitalisierung auch im Auto Fuß fasst? Welche sicherheitsrelevanten Fragestellungen bringt das mit sich? Und was kann ich mit Informationssicherheit und letztlich mit Mathematik leisten, damit wir am Ende nicht den „gläsernen Autofahrer“ haben. Es sind Fragen wie diese, die wir als BSI nach außen kommunizieren, und auch die Lösungen, die wir dafür entwickeln, müssen wir unseren Kunden verständlich machen. Mathematiker, die solche gesellschaftlichen Fragen mitdenken können, sind deshalb klar im Vorteil.

Kristina Vaillant ist freie Journalistin in Berlin und arbeitet regelmäßig für das Medienbüro der Deutschen Mathematiker-Vereinigung. <http://www.vaillant-texte.de>