AGENTENJÄGER IN DEN SCHALTKREISEN

Zum Max-Planck-Direktor auf dem zweiten Bildungsweg, das dürfte die Ausnahme sein. Doch so geht die Geschichte von Christof Paar, der zu den Gründern des Max-Planck-Instituts für Cybersicherheit und Schutz der Privatsphäre in Bochum gehört und dort heute unter anderem Hardwaretrojaner auf Computerchips aufspürt.

TEXT: KLAUS JACOB

An den Bau des Kölner Fernmeldeturms Colonius erinnert sich Christof Paar gerne. 1980 musste der Feuerwehrschacht, ein hohes Treppenhaus, mit Lautsprechern bestückt werden: alle zehn Höhenmeter vier Boxen. Eine Fleißarbeit für einen Azubi im ersten Lehrjahr – für Christof Paar. Inzwischen ist der einstige Fernmeldemechaniker in der Wissenschaft weit nach oben geklettert: Er ist einer der Gründungsdirektoren des Bochumer Max-Planck-Instituts für Cybersicherheit und Schutz der Privatsphäre. Die Forschung, die er dort betreibt, hat auch große politische Relevanz. So ist er ein guter Ansprechpartner, wenn es um das Thema Huawei und 5G-Netze oder um die Sicherheit von Unternehmen vor Hackern geht.

Der Weg Christof Paars zum Max-Planck-Direktor erinnert an die Story vom Tellerwäscher zum Millionär. Das wird deutlich, wenn man den einzelnen Etappen seines Lebenslaufs folgt. Dabei begann es erst einmal nicht ganz so vielversprechend. Weil Christof Paar Probleme mit Sprachen hatte, wechselte er vom Gymnasium an die Realschule und machte dort die Mittlere Reife. Wenn er über die anschließende Lehre spricht, klingt es aber nicht, als bedauere er den Weg ins Handwerk. Er habe schon als kleiner Junge gerne geschraubt und gebastelt, sagt er, sei technikverliebt gewesen. Und die Eltern akzeptierten den Lehrberuf sogar mit einem gewissen Wohlwollen, obwohl der Vater Akademiker war. Zur Wissenschaft kam Paar von dort über ein paar Zwischenstationen. Denn vom Handwerk in eine akademische Laufbahn zu wechseln, war damals, vor fast 40 Jahren, schwieriger als heute. Paar absolvierte zunächst ein Jahr lang die Fachoberschule und arbeitete dann noch ein halbes Jahr als Geselle in einem kleinen Dreimannbetrieb. „Mit dem Motorrad fuhr ich zu den Baustellen." Dann überlegte er – „wochenlang", wie er sagt –, ob er den Handwerksmeister machen oder in ein Studium wechseln sollte. Sein Chef drängte ihn zu bleiben: Aus seiner Sicht war eine Karriere als Meister viel sicherer als eine Ingenieurslaufbahn. Schließlich entschied sich Paar aber für den akademischen Weg und schrieb sich an der Fachhochschule Köln für Nachrichtentechnik ein. „Es war eine Vernunftentscheidung", sagt er. Den Ausschlag habe die Aussicht auf bessere Verdienstmöglichkeiten gegeben.

Bei den Schlenkern durch den zweiten Bildungsweg erfüllte Paar schon manche Erwartung an den Direktor eines Max-Planck-Instituts: Er glänzte durch Bestleistungen. Das lag nicht zuletzt daran, dass er sich für sein Fach begeisterte – und immer noch begeistert. Seine Augen leuchten, wenn er von schnellen Mikroprozessoren oder dem Kampf gegen Hacker erzählt. Im Umgang mit Menschen ist er unkompliziert, redet ebenso gerne wie viel und lacht dabei häufig. Wenn er als 57-jähriger Institutsleiter im Meeting mit seinem Team sitzt, diskutiert er mit seinen meist jungen Mitarbeitenden auf Augenhöhe, lässt sich kritisieren und ist mit allen per du. In Runden mit ihm herrscht eine entspannte studentische Atmosphäre, Pizza und

→

BESUCH BEI

CHRISTOF PAAR

FOTO: LARA WITTHAUT, FOTO-OSTERMANN.DE FÜR MPG

Spaß an der Technik: Christof Paar fahndet nach Sicherheitslücken in Computerhardware.

FOTOS: LARA WITTHAUT, FOTO-OSTERMANN.DE FÜR MPG

Jugendlich fit: Nicht zuletzt durch sein Karatetraining dreimal in der Woche dürfte Christof Paar so gut in Form sein.

Kaffee griffbereit. Er selbst wirkt viel jünger, als er ist, was auch an seinem drahtigen Körper liegt. Mit Karate, dreimal die Woche, hält er sich fit.

Das FH-Studium beendete er als Jahrgangsbester – und als einer von einer Handvoll Kommilitonen schloss er es in der Regelstudienzeit ab. Er fand Studienkollegen, die einander zu Hochleistungen anspornten: „das A-Team“, wie er schmunzelnd sagt. Schon damals entdeckte er als Tutor für Mathematik seine Leidenschaft und sein Talent für die Lehre. In der Diplomarbeit entwickelte er eine Ansteuerungselektronik für die Anzeigetafeln etwa in Bussen. Viele winzige Täfelchen, die auf Schwarz oder Weiß klappen können, ergänzen sich zu den Namen der jeweiligen Haltestellen. Auf einer großen Version dieser Anzeige erfahren Händler an der Frankfurter Börse heute noch die aktuellen Kurse. Bei dieser Technik – damals Hightech – handelt es sich um ein sogenanntes eingebettetes System, also eine Verbindung von Computer und physikalischem Gerät – genau das Forschungsgebiet, mit dem sich Paar heute noch beschäftigt. Und schon damals, mit 24 Jahren, wusste er genau, wie seine berufliche Zukunft aussehen sollte: „Ich wollte Professor werden, ganz klar.“ Allerdings war seine Hauptmotivation damals die Lehre.

Vorher musste er freilich promovieren. Und das war zu jener Zeit an einer Fachhochschule nicht möglich. So wechselte er – zusammen mit dem A-Team – an die Uni Siegen, wo ihm zumindest das Grundstudium weitgehend erspart blieb. Doch zunächst musste er als anerkannter Kriegsdienstverweigerer seinen Ersatzdienst absolvieren – und hatte Glück. Der Audiologe Hasso von Wedel, der sich als Tinnitusforscher einen Namen gemacht hatte, hatte zwei forschungsnahe Zivi-Stellen an der Uniklinik Köln. Paar erhielt eine davon und war fortan für die Technik der Versuche zuständig. So profitierte er sogar beruflich von der Zwangs-

pause. Während des Zivildiensts belegte er zunächst Vorlesungen in Physik und Mathematik an der Uni Köln, und gegen Ende begann er an der Universität Siegen bereits sein Studium.

Von Siegen wechselte er für die zweite Diplomarbeit, diesmal an der Uni, in die USA, an die Michigan Technological University. Aber warum geht jemand, der wegen Problemen mit Fremdsprachen von der Schule geflogen ist, freiwillig in die USA? „Natürlich spielte Abenteuerlust eine Rolle“, sagt Paar. Zudem war er schon während der FH-Zeit zweimal durch die USA getrampt, wo er im Gespräch mit Amerikanern die Sprache wesentlich leichter erlernte als an der Schule. Mehr noch: Paar hat später sogar eine Amerikanerin geheiratet. „Meine Englischlehrerin würde sich ziemlich wundern“, sagt er mit einem Lachen.

Einen kalten Winter lang arbeitete Paar in Michigan an seiner Diplomarbeit. Das Thema lag – wieder einmal – auf der Höhe der technischen Entwicklung: aktive Schallfeldunterdrückung. Ein Gegenschall schaltet dabei unerwünschten Lärm aus, eine Technik, die etwa für Autos gedacht ist. In seinen Arbeiten hat Paar immer verschiedene Gebiete zusammengebracht: Physik mit Computertechnik, Ingenieurswissen mit Mathematik, klassische Hardware mit Software. Auch seine Doktorarbeit an der Uni Essen ist dafür ein Beispiel: Es ging um Fehlerkorrekturen in der Digitaltechnik. Man verwendet diese Technik etwa bei der Datenübertragung von Satelliten zur Erde oder im CD-Spieler. Kaum jemand, der eine CD laufen lässt, ahnt, welche raffinierten Mechanismen greifen, um zu garantieren, dass auch verkratzte CDs ohne Fehler abgespielt werden. So kann man ein bis zu drei Millimeter großes Loch in die Scheibe bohren und wird dann doch nicht in seinem Hörgenuss gestört. Paar vereinfachte die Algorithmen für die Echtzeit-Fehlerkorrektur, die direkt in speziellen Hardwareschaltungen umgesetzt werden, sodass diese deutlich kleiner, schneller und energieeffizienter wurden – eine Methode, die später auch kommerziell eingesetzt wurde.

Seinen Einstieg in die Hochschullaufbahn nach der Promotion plante Paar in den USA. Denn er wollte zu seiner Freundin, die er zwei Jahre zuvor kennengelernt hatte und später heiratete. „Zwei Jahre Fernbeziehung waren genug.“ 1995 bekam er eine Stelle als Assistant Professor am Worcester Polytechnic Institute in Massachusetts, einer Privatuniversität, die von Studiengebühren lebt und daher großen Wert auf verständliche Vorlesungen legt. Paar musste also nicht nur einen Forschungs-, sondern auch einen Lehrvortrag halten – und mit dem stach er seine Konkurrenten aus. Als Professor genoss er nun viele Freiheiten, die er nutzte, um an der Hochschule ein neues Fach einzuführen: die Kryptografie.

Paar arbeitet an der Umsetzung neuer Verschlüsselungsmethoden in Hard- und Software. Er gehört zu den Experten, die dieses Forschungsgebiet etabliert haben.

Bei Kryptografie denkt man unwillkürlich an Geheimcodes, die jedes Kind faszinieren, oder an Enigma, die Chiffriermaschine der Nazis, die von den Alliierten geknackt wurde. Doch in der Forschung fristete die Disziplin in den 1990er-Jahren noch ein Schattendasein. Es gab nur ein einziges, damals ganz neues Lehrbuch, und nur wenige Unis boten das Fach an. Paar hatte auf das richtige Pferd gesetzt. „Mir half dabei auch Glück“, sagt er: Damals nahm der Internetboom richtig Fahrt auf, sodass Kryptografie und Datensicherheit immer wichtiger wurden. Das liegt auch an Fällen wie jenem des Whistleblowers Edward Snowden. Er zeigte, wie dreist Geheimdienste Daten abgreifen, und wie wichtig es ist, diese zu schützen. Eines

→

von unzähligen Beispielen ist auch der Skandal um die Krypto AG, eine Schweizer Firma, die während des Kalten Krieges Verschlüsselungsgeräte herstellte. Später wurde bekannt, dass sie im Auftrag von CIA und BND manipulierte Geräte verkaufte, womit die Geheimdienste in mehr als 100 Ländern spionierten.

Paar entwickelt allerdings in erster Linie keine neuen Verschlüsselungsmethoden, sondern arbeitet an deren Umsetzung in Hard- und Software. Er gehört zu den Experten, die dieses Forschungsgebiet überhaupt erst etabliert haben. Zusammen mit seinem Kollegen Çetin Koç rief er 1999 die Kryptografiekonferenz CHES (Cryptographic Hardware and Embedded Systems) ins Leben. Sie war eigentlich als relativ kleiner Workshop gedacht. Doch schon zur ersten CHES kamen mehr als 150 Fachleute aus Wissenschaft und Industrie, und sogar die *New York Times* berichtete darüber. Inzwischen ist die CHES eine der wichtigsten internationalen Kryptografiekonferenzen.

zweisprachig aufgewachsen und kamen erst hier in die Grundschule, die jüngste Tochter, Flora, wurde in Deutschland geboren. Für Paars Frau war der Wechsel beruflich schwieriger. Sie hatte in den USA an einem Community College unterrichtet, einer Hochschulform, die es in Deutschland nicht gibt. Mittlerweile arbeitet sie aber als Lehrbeauftragte für Biologie an der Ruhr-Universität Bochum. „Diese Tätigkeit gibt ihr viel Befriedigung", erzählt Christof Paar.

Für ihn läuft es ohnehin gut: Nicht zuletzt wegen des Horst Görtz Instituts gehört Bochum mit 1000 Studierenden in der IT-Sicherheit zu den weltweit führenden Standorten auf diesem Gebiet. Nicht nur in der Forschung sorgte das Institut 2008 für einiges Aufsehen. Paar und seinen Kollegen war es gelungen, einen elektronischen Türöffner, wie er millionenfach für Garagentore und Autotüren verwendet wird, zu knacken. Dafür mussten sie die Elektronik zunächst mit dem Reverse Engineering analysieren – ein sehr aufwendiger Schritt. Mit dem, was die

Es reicht oft aus, einige Transistoren subtil zu manipulieren, um wichtige Sicherheitsfunktionen abzuschalten.

Zurück zu Christof Paars Weg vom Lehrjungen zum Max-Planck-Direktor: Sieben Jahre lang blieb er in den USA. Angebote, sich an Start-ups zu beteiligen, lehnte er ab. Denn er mochte den Universitätsbetrieb mit seiner Kombination aus Forschung und Lehre. Außerdem befürchtete er, nicht mehr genug Zeit für Frau und Kinder zu finden. 2001 kehrte er dann nach Deutschland zurück, weil er näher bei seinen alten Eltern sein wollte, aber auch weil er an der Ruhr-Universität Bochum das „Horst Görtz Institut für IT-Sicherheit" mit aufbauen konnte. Die Initiative dazu ging vom Mittelständler Horst Görtz aus, der während des Dotcom-Booms viel Geld mit IT-Sicherheit verdient hatte und nun mit seiner Stiftung eine starke Forschungsstätte in Deutschland anstoßen wollte. Paars beiden älteren Kindern, Noah und Maja, fiel der Wechsel nach Deutschland leicht; sie waren bereits von Anfang an

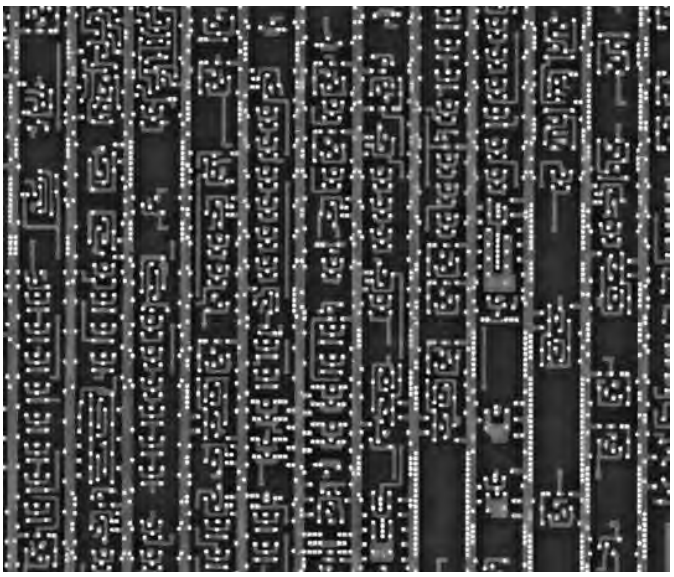
Forschenden dabei herausfanden, fertigten sie eine Art Universalschlüssel an, um Garagentore sowie die Türen mancher Autos zu öffnen – für die Medien eine große Nachricht: „Die Journalisten rannten uns über Wochen die Bude ein", sagt Paar.

Solche Hackeraktionen gehören für ihn zum Forschungsalltag. Denn wer die Sicherheit verbessern möchte, muss die Angriffspunkte in den Systemen kennen. Paar geht noch einen Schritt weiter: Er will auch wissen, wie Hacker ticken, wie ihre mentalen Prozesse ablaufen und wo ihre Schwachstellen sind – und hat damit ein neues Forschungsgebiet erschlossen. Dafür hat er sich mit der Kognitionsforscherin Nikol Rummel zusammengetan. Die beiden standen allerdings vor einem Problem: Profihacker sind scheu. Sie lassen sich selbst dann nicht in die Karten schauen, wenn sie im Auftrag von Unter-

→

FOTO: LARA WITTHAUT, FOTO-OSTERMANN.DE FÜR MPG

Sichere Überwachung: Christof Paars Team entwickelt eine Technik, mit der sich überprüfen lässt, ob Atomsprengköpfe sicher gelagert werden. Weil sie dabei eine spezielle elektromagnetische Signatur des Aufbewahrungsortes aufzeichnen, kann die Überwachung nicht unterlaufen werden. Der Blick auf physikalische Eigenschaften verbindet das Projekt mit der Forschung an Computerhardware.



GRAFIK: KRIMINALTECHNISCHES INSTITUT DES BKA - KT 52

Durchleuchtete Bauteile: Die Aufnahme eines Rastertunnelmikroskops zeigt Details in der Chipstruktur, die den Bochumer Forschern bei der Suche nach Hardwaretrojanern helfen.

nehmen nach Schwachstellen in deren Produkten suchen. Die Bochumer Uni-Forscher mussten sich mit Studierenden begnügen, die sich freiwillig beteiligten. So fanden sie heraus, dass die Geschwindigkeit, mit der ein Hacker vorankommt, mit der Größe seines Arbeitsgedächtnisses korreliert. Aus der Kognitionspsychologie weiß man, dass die meisten Menschen höchstens sieben Informationseinheiten gleichzeitig verarbeiten. Um Hackerangriffe zu verhindern, ist ein Ansatz daher, Hard- und Software so zu entwerfen, dass der Angreifer wesentlich mehr Information erfassen muss. Seit Mitte 2019 ist Christof Paar mit dem Franzosen Gilles Barthe Gründungsdirektor am neuen Max-Planck-Institut in Bochum. Nun kann er sich stärker um die Forschung kümmern, bei der er auch mit dem Bundeskriminalamt und Unternehmen wie Google zusammenarbeitet. Doch auf die Lehre will er nicht ganz verzichten. „Aber ich kann mir jetzt die Rosinen herauspicken“, sagt er. Dazu gehört die Einführungsvorlesung in Kryptografie, mit der er in den USA reüssiert hatte – natürlich in aktualisierter Form.

Wie wichtig sein Fachgebiet ist, zeigt sich zurzeit am Hickhack um Huawei. Die USA und Großbritannien verdächtigen das Unternehmen, für den chinesischen Staat zu spionieren, und schließen es beim Bau der 5G-Technik aus. Dass solche Manipulationen möglich sind, weiß Paar nur zu gut. Denn er beschäftigt sich auch mit Hardwaretrojanern, dafür hat er auch einen ERC Advanced Grant, eine der wichtigsten europäischen Forschungsförderungen. Hardwaretrojaner sind versteckte Schaltungen auf einem Chip, die zur Spionage genutzt werden können. Mit ihnen wäre es sogar möglich, komplette Industrieanlagen abzuschalten.

Der Laie denkt vielleicht, so schwer kann es doch nicht sein, solche Manipulationen zu finden. Ganz falsch. Denn Chips, wie sie in Smartphones oder in mit 5G-Technik vernetzten Computern stecken, enthalten viele Millionen nur wenige Nanometer große Transistoren, deren Bauplan strengstens gehütet wird. Christof Paar und sein Team haben herausgefunden, dass es oft ausreicht, einige dieser Transistoren subtil zu manipulieren, um wichtige Sicherheitsfunktionen abzuschalten. Um solche Schaltungen zu verstehen, müssen die Forscher den Chip Schicht um Schicht abtragen und aufwendig analysieren. Zumindest für die Untersuchung der Grobstruktur haben sie mittlerweile eine automatisierte Methode entwickelt. Damit lässt sich etwa herausfinden, in welchen Untereinheiten des Chips die Verschlüsselung stattfindet; diese Teile bieten sich für den Einbau von Trojanern besonders an. Solche Analysetechniken stehen bisher nur mächtigen Nachrichtendiensten und wenigen spezialisierten Firmen zur Verfügung. Paars Forschung hilft dagegen der gesamten internationalen Forschungsgemeinschaft, die Manipulationen der Hardware besser zu verstehen, sodass sich neue Schutzmaßnahmen entwickeln lassen.

Wie sich gerade Angriffe von staatlichen oder halbstaatlichen Organisationen parieren lassen, das ist Thema im Exzellenzcluster „Cybersicherheit im Zeitalter großskaliger Angreifer“, zu deren Sprechern Christof Paar zählt. „Wie wir aus Edward Snowdens Enthüllungen wissen, treiben die Nachrichtendienste dafür einen absurden Aufwand“, sagt er. Die Arbeit, so ist zu befürchten, wird ihm daher so schnell nicht ausgehen.

←

FORSCHUNG
LEICHT GEMACHT

Das Magazin der Max-Planck-Gesellschaft als **ePaper**:

www.mpg.de/mpf-mobil
www.mpg.de/mpforschung

KOSTENLOS DOWNLOADEN!