Fotos: Meinrad Hofer für DIE ZEIT; Intel Corporation (u.)

Daniel Gruss an der TU Graz, auf diesem Bild ausnahmsweise ohne Cola und in einem T-Shirt ohne Logo

Der Kernschmelzer

Daniel Gruss hat eine schwere Sicherheitslücke in Computerchips entdeckt. Warum gelingt dem Informatiker, woran die Hersteller scheitern? VON JENS TÖNNESMANN

Zwei Dinge fallen auf, wenn man Daniel Gruss an der Technischen Universität Graz trifft. Erstens: Gruss wirkt hellwach, dabei müsste er todmüde sein. Seit Wochen ist er unterwegs, sitzt in Flugzeugen, spricht auf Konferenzen, gibt Interviews. An diesem Wintertag ist der 31-Jährige seit acht Uhr im Büro, obwohl er es erst sechs Stunden vorher verlassen hat. Was ihn aufputscht, kann nicht allein die Cola sein, die sich sixpackweise in einer Ecke türmt. Da muss es noch etwas anderes geben.

Zweitens fällt auf: Gruss trägt oft dasselbe T-Shirt. Man sieht es auf Fotos, auf YouTube, auch heute hat er es an. Auf der Brust zeigt es ein schildförmiges Wappen, das tropft, als würde es schmelzen. Auf dem Rücken fünf Zeilen Computercode, »byte [rcx]« steht da zum Beispiel, und »qword [rbx + rax]«.

Das sind jene fünf Codezeilen, die Daniel Gruss und seine beiden Forscherkollegen Moritz Lipp und Michael Schwarz zu Berühmtheiten gemacht haben – in IT-Zirkeln und darüber hinaus. »Die jungen Genies«, titelte die *Kleine Zeitung* aus der Steiermark, die bei Gruss auf dem Schreibtisch liegt. Mit den fünf Zeilen wiesen die Forscher dem 50 Jahre alten Chiphersteller Intel eine der größten Sicherheitslücken der Geschichte nach. Bekannt geworden ist sie als »Meltdown«, Gruss hat sich den Namen ausgedacht. Man kann ihn mit »Kernschmelze« übersetzen oder auch mit »Nervenzusammenbruch«. Beides passt, denn Millionen von Computerchips waren von der Sicherheitslücke betroffen; das ließ nicht nur die Anwender, sondern auch die Manager und Aktionäre von Intel ziemlich zittrig werden.

Die fünf Zeilen Programmcode von Daniel Gruss und seinen Kollegen stehen aber nicht nur für den Krisenfall eines Konzerns und den Erfolg eines Forscherteams. Positiv betrachtet sind sie ein Beispiel dafür, wie gut Wissenschaftler und Wirtschaft heute zusammenarbeiten, wenn es um das Aufklären und Schließen von digitalen Sicherheitslücken geht.

Gruss und seine Kollegen erforschen in Graz gezielt, wie sich die physikalischen Eigenschaften von Hardware von Angreifern ausnutzen lassen. Dass die Prozessoren anfällig sind, darüber hatten sie schon früher mit anderen Forschern diskutiert. Gruss erzählt das, wenn man mit ihm in Graz im Computerlabor steht, wo er die Angriffe demonstriert – und dabei so schnell in die Tasten tippt und mit der Maus herumfährt, als müsse er bei einem Computerspiel den Endgegner besiegen. 2017 dann gelang es ihnen hier, die Lücke zu finden; daraufhin meldeten sie sich erst bei dem Konzern. Dann gaben sie dem Unternehmen monatelang Zeit, die Schwachstellen zu beheben, bevor sie die Öffentlichkeit informierten. »Responsible Disclosure« nennt man das in IT-Sicherheitskreisen, »verantwortungsvolle Offenlegung«. So kann die Schwachstelle behoben werden, bevor mögliche Angreifer davon erfahren und sie ausnutzen.

Dass akademische Sicherheitsforscher auf diese Weise Wirtschaftsunternehmen helfen, ist keine Seltenheit. Der deutsche Informatiker Vincent Haupert von der Uni Erlangen-Nürnberg etwa hat schon mehrfach Sicherheitslücken bei Banking-Apps für Smartphones ermittelt, und ein Forscher von der Uni Leuven sorgte vergangenes Jahr für Schlagzeilen, als er auf eine erhebliche Schwachstelle von WLAN-Routern hinwies. Solche Forscher seien heute »absolut vital«, sagt zum Beispiel die sozialliberale Europaabgeordnete Marietje Schaake, die in Brüssel einer Taskforce vorsitzt, die den richtigen Umgang mit IT-Schwachstellen ergründen will. »Software, die hundertprozentig sicher ist, ist eine Utopie«, sagt sie.

Kritisch kann man aber auch fragen: Warum finden Forscher, die aus EU-Mitteln finanziert werden, solche Sicherheitslücken in Computerchips? Warum ist nicht Intel selbst darauf gestoßen, ein Konzern, der im vergangenen Jahr einen Rekordumsatz von 62 Milliarden Dollar und einen operativen Gewinn von 17 Milliarden Dollar eingefahren hat?

Gruss könnte viel Geld verdienen, wenn er seine Erkenntnisse verkaufen würde

Die Frage führt zurück ins Büro von Daniel Gruss, wo jetzt sein Kollege Michael Schwarz in der Tür steht. »Was machst du gleich in der Vorlesung?«, fragt der. »Ich werde natürlich übers Kochen reden!«, sagt Gruss. Kochen? Gruss läuft los, Treppe runter, einmal quer durch die Hochschule. Unterwegs ein »Hallo« hier und ein »Wie läuft's?« dort, dann die Betriebssysteme-Vorlesung in Raum I13, für Studenten im vierten und fünften Semester. In dieser Vorlesung beginnt man zu verstehen, was Gruss antreibt – und warum er kein Problem darin sieht, bei reichen Konzernen kostenlos Sicherheitslücken zu stopfen.

Ein Vortrag von Daniel Gruss ist unterhaltsam, auch für Nichtinformatiker. Er zeigt zum Beispiel gerne eine Szene aus der US-Serie *Game of Thrones,* in der ein Drache eine meterhohe Eiswand Feuer speiend wegschmilzt. So ähnlich ist das nämlich bei Meltdown. Der Arbeitsspeicher eines Computers ist aufgeteilt in zwei Bereiche, der eine ist für das Betriebssystem reserviert, der andere für Anwendungen des Nutzers. Die Bereiche sind wie mit einer Wand getrennt, um sensible Bereiche vor schädlicher Software schützen. Bei Meltdown aber schmilzt sie weg.

Was dann passiert, erklärt Daniel Gruss metaphernreich, indem er übers Kochen redet. Was tun, wenn man in der Küche stets zu spät merkt, dass Zutaten fehlen? Was läuft falsch, wenn man erst am Ende des Rezepts merkt, dass man den fertigen Braten mit gegarten Kartoffeln servieren soll, die Kartoffeln aber nicht mal vorbereitet hat? »Du solltest das Rezept durchlesen, bevor du anfängst«, ruft ein Student in den Saal, »und dir schon mal die Zutaten rauslegen.« Das Bild stimmt: So arbeiten viele Mikroprozessoren. Die Chips versuchen, die nächsten Schritte eines Programms vorherzusehen, und legen sich dafür schon mal Daten zurecht. Das macht sie schneller, aber auch unsicherer: Schadprogramme können die Daten abgreifen und daraus zum Beispiel Passwörter ableiten, die Nutzer eingegeben haben. Bei Meltdown, erklärt Gruss, sei es so, als würde einem jemand in der Küche über die Schulter schauen und von den auf dem Tisch ausgebreiteten Zutaten naschen. Das ist Gruss' großes Talent: Mit Bildern und Analogien macht er komplizierte Fragen der Technik verständlich.

Als nächstes erklärt Gruss ein Programm, das er mit seinen Kollegen entwickelt hat und mit dem sich die Intel-Sicherheitslücke schließen lässt. »Kaiser« haben sie es genannt und der Industrie kostenlos zur Verfügung gestellt. Es hat allerdings einen Nachteil: Wo Kaiser läuft, werden viele Prozessoren langsamer. In der Welt der Chiphersteller war das bisher keine Option. Die Anwender wollten immer schnellere Prozessoren, nicht sicherere. Sollten die Hersteller nun umdenken, dürfte das auch an Gruss liegen.

Wenn Gruss vorträgt, merkt man, was sein Aufputschmittel ist: Er läuft herum, blendet Fotos und Videos ein, erklärt und erklärt. Ein »pädagogisches Talent« nennt ihn sein Student Johannes Spöcklberger. Der studiert Softwareentwicklung bei Gruss, und er hat in der Vorlesung gefragt: »Sag mal, Daniel, bleibst du nach deinem großen Erfolg mit Meltdown eigentlich hier?« Ein anderer Kommilitone hat gerufen: »Oder gehst du zum amerikanischen Geheimdienst?«

Daniel Gruss hat gelacht und geantwortet, dass er Letzteres sicher nicht tun werde: »Ich will unterrichten!« Ein Erfolg wie Meltdown helfe ihm, Beiträge zu publizieren, was ihm wiederum Einladungen zu wichtigen Konferenzen verschaffe, weswegen er später leichter Fördermittel einwerben könne, um damit Doktoranden zu bezahlen, die dann die nächste Sicherheitslücke aufspüren. Das ist aber nur ein Grund, warum er sich Sicherheitslücken vornimmt. Auch sportlicher Ehrgeiz spielt eine Rolle: der Erste zu sein, der eine Lücke findet und schließt. Und es sei schon »ziemlich big«, wenn die eigenen Erkenntnisse in Wikipedia-Artikel oder Fernsehbeiträge münden.

Um Geld aber geht es Gruss nicht. Dabei könnte er sicher gut verdienen, wenn er sich nicht in den Dienst der Wissenschaften stellen würde. Sein Doktorvater Stefan Mangard nennt Gruss seinen »größten Glücksgriff«. Und er vermutet auch: Wenn man Meltdown verkauft hätte, hätte man dafür vielleicht eine Million Dollar bekommen können von Unternehmen, die mit solchen Lücken Geschäfte machen. Aber selbst wenn das legal wäre, sei es doch »moralisch höchst fragwürdig«, sagt Mangard, »unser Einkommen ist unser wissenschaftliches Standing«.

Immerhin 5000 Dollar bekamen die Grazer Forscher von Intel aus einem Prämientopf für die Fehlerjagd (siehe Kasten). Manche Unternehmen gehen einen anderen Weg und stellen selbst Hacker ein. Einen von ihnen hat Gruss später an diesem Tag an seine Uni eingeladen: Thomas Dullien, der bei Google arbeitet. Bevor dessen Vortrag beginnt, muss der Vorlesungssaal gewechselt werden: zu großer Andrang.

Dann erklärt Dullien den Studenten: Die Risiken von Angriffen auf die moderne Computertechnik wüchsen, weil die Technologie exponentiell komplexer werde. Meltdown sei dafür ein Paradebeispiel: Die Schwachstelle sei bereits in den 1990er Jahren entstanden, als die ersten Prozessoren lernten, im Voraus zu denken. Erst durch die Vernetzung der Computer aber wurde sie zur echten Gefahr. Leute wie Gruss würden künftig mehr gebraucht denn je.

Im Studium haben Gruss viele Vorlesungen gelangweilt – das will er besser machen

Gruss weiß, wie man Studenten motiviert, sich auf diese neue Welt der Computerunsicherheit vorzubereiten. Als es dunkel wird über Graz, sitzt er in einem Seminarraum, umgeben von jungen Leuten. Auf den Tischen stehen Energiegetränke wie Mate und Red Bull, er selbst hat Cola dabei. Tagelang haben die Studenten in seinem Seminar selbst Betriebssysteme programmiert; jetzt machen sie Testläufe, um zu sehen, ob sie wirklich funktionieren. Zwischendurch erzählt Gruss davon, wie er schon als Grundschüler in Bad Münstereifel anfing zu programmieren. Er fand damals Spaß daran, sich den Kopf zu zerbrechen, bis ein Programm funktionierte. Fürs Studium zog er nach Graz, zu seiner Freundin, die er übers Internet kennengelernt hat und mit der er gerne Computerspiele zockt. Im Studium merkte er dann, dass viele Vorlesungen ihn überhaupt nicht begeisterten – und er beschloss, die Lehre besser zu machen. Vor allem: spielerischer.

So wie das Finale dieses Tages in einer Kneipe. Im Office Pub zwängen sich die Studenten an Holztische. Es gibt Bier und Nachos. Auf einer Leinwand werden die Ergebnisse der Studententeams eingeblendet, die ihre Betriebssysteme ausprobieren; es ist wie bei einem Skirennen, aber ohne Sport und für Nerds.

Wann immer ein Betriebssystem einen Durchlauf absolviert hat, reiht es sich in die Ergebnisliste ein. Erst tief in der Nacht steht ein Gewinner fest. Gruss bleibt noch länger. Dann schläft er ein bisschen und steigt bald ins Flugzeug. 15 Flüge stehen bis Ende April an, hat Gruss gezählt, einer führt nach Kalifornien. Zu Apple, wo man ihn kennenlernen will.

Kampf gegen die digitalen Gefahren

Hohe Schäden
Der Digitalverband Bitkom schätzt, dass 53 Prozent der deutschen Unternehmen in den vergangenen zwei Jahren Opfer von Datendiebstahl, Wirtschaftsspionage oder Sabotage per Computer wurden. Dabei seien rund 55 Milliarden Euro Schaden entstanden.

Prämienjäger
Viele Unternehmen in der IT-Branche loben Prämien für Hacker aus, wenn diese sie auf Sicherheitslücken hinweisen. Diese Prämien werden Bug-Bounties genannt. Die US-Firma Bugcrowd zählte 2017 doppelt so viele Bug-Bounty-Programme wie noch 2016; inzwischen seien mehr als sechs Millionen Dollar ausgezahlt worden. Auch Chiphersteller Intel lockt mit Bug-Bounties.

Was tun, wenn man ein Hacker ist?
Es gibt keine einheitlichen Vorgaben dafür, wie ein Hacker Sicherheitslücken offenlegen soll, wenn er welche entdeckt. Die sozialliberale Europaabgeordnete Marietje Schaake kritisiert das und macht sich für europäische Regeln stark, nach denen Sicherheitsforscher ihre Erkenntnisse mitteilen können und dabei vor Strafverfolgung geschützt sind.