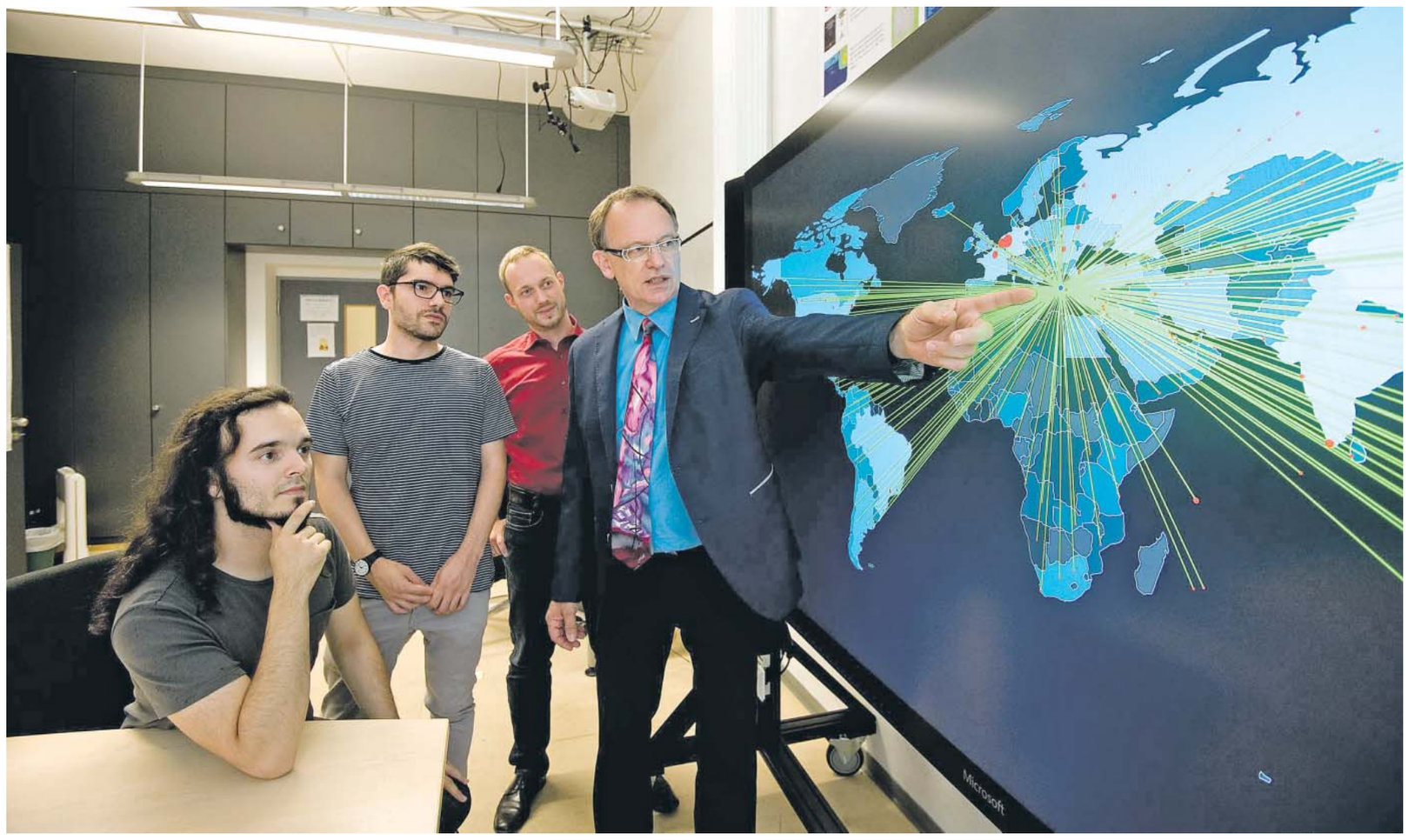
Mit Honigtöpfen gegen Cyber-Attacken

An der TU Darmstadt haben Forscher Köder ins Netz gestellt, um gezielt Cyber-Angreifer anzulocken. So wollen sie herausfinden, wie Hacker arbeiten.

Von Alexander Jürgs



Achtung, Angriff: *Carlos Garcia Cordero, Emmanouil Vasilomanolatis, Florian Volk und Max Mühlhäuser (von links) erforschen Strategien gegen Cyberkriminalität.* Foto Wohlfahrt

DARMSTADT. Ein wuchtiger LED-Bildschirm steht in einem Raum im Erdgeschoss des Robert-Piloty-Gebäudes an der Technischen Universität in Darmstadt. Er ist mehr als zwei Meter breit und zeigt eine Weltkarte. Die einzelnen Länder sind türkis markiert, daneben gibt es zwei blaue und unzählige rote Punkte. Plötzlich erscheint kurz eine hellgrüne Linie zwischen einem der roten und einem der blauen Punkte. „Sehen Sie, das ist ein Angriff, genau in diesem Moment“, sagt Florian Volk von der Telecooperation Group. Das Institut gehört zum Fachbereich Informatik an der Darmstädter Hochschule. Die Wissenschaftler dort untersuchen Cyber-Angriffe.

Sie wollen so genau wie möglich herausfinden, wie Hacker vorgehen, um bessere Verteidigungsstrategien gegen die Attacken im Internet zu entwickeln. Darum zeichnen sie die virtuellen Angriffe auf. Und sie stellen die Daten, die sie dabei sammeln, anderen zur Verfügung. Über die Website *tracingmonitor.org* kann jeder diese Cyber-Attacken live verfolgen oder die Codes der Angriffe studieren.

Florian Volk nennt sich Research Strategy Coordinator, was bedeutet, dass er bei Forschungsprojekten der Telecooperation Group die Fäden zusammenhält. Jetzt wechselt er auf dem großen Bildschirm den Darstellungsmodus. Angezeigt werden alle bisherigen Angriffe des Tages: Es ist ein unüberschaubares Dickicht aus grünen Linien, denn: Cyber-Attacken sind im Internet alltäglich, sie laufen rund um die Uhr und millionenfach.

Um an diese Daten zu kommen, haben die Wissenschaftler Köder ausgesetzt, sogenannte „Honeypots“. Eigentlich sind derlei Honigtöpfe dazu da, um Hacker abzulenken. Ihren Namen verdanken sie der Idee, dass man Bären durch das Aufstellen von Honigtöpfen auf eine falsche Fährte locken könnte. Bei den Honeypots, die in der IT-Sicherheit eingesetzt werden, handelt es sich um Computerprogramme oder Server, die so tun, als seien sie der Netzwerkdienst eines einzelnen Rechners oder eines ganzen Netzwerks an Computern. So locken sie Cyber-Angreifer an und dienen dem Ziel, andere Systeme vor Attacken zu schützen.

Denn mit den Honigtöpfen sammeln die Wissenschaftler nicht nur in Darmstadt, sondern auch in Athen und Malaysia Daten, die der Forschung dienen. „Wir wollen besser lernen, wie die Angreifer vorgehen, wir wollen überprüfen, ob unsere Angreifermodelle stimmen“, erklärt Max Mühlhäuser, der das Fachgebiet Telekooperation leitet.

„Natürlich laufen wir den Angreifern hinterher und können nur reagieren, mit diesem Projekt aber rücken wir deutlich näher an sie heran“, sagt Mühlhäuser. Seine Abteilung ist Teil des Centers for Research in Security and Privacy, dem laut eigener Aussage größten Forschungszentrum für Cyber-Sicherheit in Europa. Die TU Darmstadt, die Hochschule Darmstadt sowie die Fraunhofer-Institute für Sichere Informationstechnologie und für Graphische Datenverarbeitung haben sich dazu zusammengeschlossen. Mehr als 450 Wissenschaftler forschen in Darmstadt über Cyber-Sicherheit.

Mit Hilfe von Smartphones werde die Anzahl der Honeypots erhöht, sagt Mühlhäuser. Eine von den Wissenschaftlern in Darmstadt entwickelte App ermöglicht auch die Registrierung privater Mobiltelefone als Honeypot, womit im Grunde jeder, der möchte, Teil des Forschungsprojekts werden könne. „So erreichen wir mehr und bessere Ergebnisse.“

Die Taktiken der Hacker haben sich in den vergangenen Jahren stark gewandelt, erklärt Mühlhäuser: Verfolgten sie früher meist das Ziel, Computern durch Viren direkt zu schaden, geschehen die Angriffe heute oft unbemerkt, ohne dass die Infizierung sofort auffällt. Die Hacker versuchen stattdessen, aus möglichst vielen gekaperten Maschinen Netzwerke zu bilden. Botnetze werden diese Netzwerke genannt, weil die dabei verknüpften Rechner von den Cyber-Kriminellen aus der Ferne über Schadprogramme, die Bots (von Roboter) heißen, gesteuert werden. Solche Netze haben mittlerweile riesige Ausmaße erreicht: Dass etwa 40 Prozent aller deutschen Computer mit Viren infiziert und so zu Bestandteilen von Botnetzen gemacht worden sind, schätzt zum Beispiel der Internetverband Eco.

Genutzt werden können diese Netze für unterschiedliche kriminelle Aktionen: für das heimliche Versenden von Spam-Mails über infizierte Rechner genauso wie für Großangriffe auf Firmennetzwerke, Streamingdienste und Behörden. „Hacken ist heute eine Industrie“, sagt Florian Volk. Die Botnetze haben sich zu wahren Goldgruben entwickelt. „Da ist ein unüberschaubarer Untergrundmarkt entstanden, auf dem die Netze zur Miete oder zum Kauf angeboten werden. Für wenige hundert Dollar erhalten Sie dort Netzwerkkapazitäten, die ausreichen, um eine mittelständische Firma komplett aus dem Internet zu entfernen.“

Dabei greifen die Hacker mittlerweile viel seltener klassische Computer an. Und sogar die Attacken gegen Smartphones gehen anscheinend zurück. Neues Ziel der Cyber-Kriminellen ist das Internet der Dinge. Immer mehr Geräte des Alltags sind über das Netz verknüpft. Heizungen oder Kühlschränke lassen sich per Internet steuern. Die Geräte, die diese Alltagsgegenstände lenken, sind aber meistens schlechter gegen Hackerangriffe gesichert als ein Computer oder ein Smartphone. Das macht sie für Kriminelle attraktiv.

Würden Hacker also zum Beispiel die intelligente Heizungssteuerung angreifen, würde der Nutzer zunächst gar nichts davon merken, so Volk. „Da machen Sie auch nie Updates. Die läuft rund um die Uhr und hat immer Internetverbindung.“ Eine Phalanx aus solchen Geräten werde heute genutzt, um Konzerne wie Amazon anzugreifen.

Die Wissenschaftler in Darmstadt sind überzeugt: Gegen diese Angriffe, die von unzähligen, miteinander verbundenen Maschinen ausgeführt werden, können sich die Angegriffenen nur wehren, wenn sie sich ebenfalls zusammenschließen. „Wir brauchen eine kollaborative Verteidigung“, sagt Max Mühlhäuser. Wie diese funktionieren könnte, daran forscht aktuell der Doktorand Carlos Garcia Cordero. Der Mexikaner will Methoden entwickeln, wie Anomalien aus dem Netz noch schneller als bös- oder gutartig eingestuft und wie diese Informationen so effizient wie möglich ausgetauscht werden können, auch die über Fehlalarme. Denn nicht alles, was nach einem Cyber-Angriff aussieht, ist auch wirklich eine gefährliche Attacke. Wenn etwa jemand mehrfach versehentlich ein falsches Passwort am Firmen-PC eingibt, dann werden die Mitarbeiter in der IT-Sicherheitsabteilung sofort alarmiert, denn: Manchmal wirken einfache technische Probleme wie ein Angriff durch Hacker.

Das öffentliche Bewusstsein für Cyber-Sicherheit ist noch immer nicht besonders ausgeprägt. Angriffe werden gerne verdrängt, solange sie einen nicht selbst betreffen. Und natürlich ist das Thema komplex und somit für Nichtinformatiker kaum zu durchdringen. Ein Problem sei aber auch, dass den Nutzern lange ein Maß an Sicherheit versprochen worden sei, das es gar nicht gebe, so Mühlhäuser. „Wir haben jahrelang falsch über IT-Sicherheit gesprochen“, sagt der Informatiker. Den Nutzern habe man den Glauben verkauft, mit bestimmten Sicherheitssystemen geschützt zu sein. „Doch diese absolute Sicherheit gibt es nicht, es gibt nur mehr oder weniger Sicherheit.“

Mühlhäuser zieht einen Vergleich zum Schutz vor Einbrüchen. Auch dort könne man einiges unternehmen, um seine Wohnung oder sein Haus sicherer zu machen. „Doch wenn jemand wirklich eindringen will, dann können Sie das nicht unmöglich machen – und so ist es bei der IT-Sicherheit leider auch.“

Wie ist das, wenn man sich tagtäglich mit Hackerangriffen beschäftigt? Will man das nicht auch einmal ausprobieren? „Es ist eine Gewissensentscheidung, ob man auf der guten oder bösen Seite arbeitet“, sagt Florian Volk. „Was die Hacker machen, das können hier alle. Mit dem Wissen, das man mit einem Informatik-Studium erwirbt, wäre es ein Leichtes, auch für die Bösen zu arbeiten, wo man mit sehr viel weniger Aufwand sehr viel mehr Geld verdienen würde.“

Eine frühere Mitarbeiterin der Telecooperation Group arbeitet seit einiger Zeit schon als Hackerin – auf der guten Seite. Sie ist bei einer Firma untergekommen, die im Auftrag von Unternehmen gezielt Cyber-Angriffe gegen deren Internetseiten ausführt. Die Attacken sollen Sicherheitslöcher identifizieren, um sie zu stopfen – nicht, um dadurch Viren einzuschleusen. Im Kampf gegen die bösen Hacker braucht es heute auch gute Hacker.

Nicht so schlimm, wie alle denken

Fake News sind gefährlich und können Schaden anrichten / Mainzer Professor gibt für Deutschland derzeit eher Entwarnung

MAINZ. Was vor 20 Jahren in der Zeitung stand oder im Fernsehen lief, galt als wahr. Heute erscheint die Welt der Informationen durch das Internet und angekurbelt durch die sozialen Netzwerke unübersichtlicher, die Quellen einer Nachricht sind schwieriger zu prüfen. Das allgemeine Misstrauen gegenüber der Berichterstattung wächst und kulminiert in dem Begriff „Fake News“: die bewusst gestreute Falschmeldung, um Klicks im Internet zu gewinnen oder gar Meinungen, Themen und sogar Wahlkämpfe zu manipulieren.

Christian Schemer hat keine Angst davor. „Wenn man sich die etablierten Parteien und Medien in Deutschland anschaut, dann gibt es niemanden, der so ein Geschäft betreiben würde“, sagt der Professor für Kommunikationswissenschaft an der Mainzer Johannes-Gutenberg-Universität. Dadurch sei die Gefahr, dass Fake News einen spürbaren Einfluss auf die Politik haben könnten, eher gering. Außerdem zeigt eine Studie zum Medienvertrauen, die Schemer mit vier Wissenschaftlern seiner Uni verfasst hat, dass die Nutzung „klassischer Medien“ stabil bleibt.

Welchen enormen Einfluss Fake News haben könnten, lässt sich etwa an zwei Beispielen der jüngeren Geschichte aufzeigen. So grassierten in den Vereinigten Staaten beim vergangenen Wahlkampf erfundene Meldungen über einen Kinderpornoring, den Hillary Clinton von einer Pizzeria aus steuern würde. Durch Großbritanniens Medien geisterten vor der Brexit-Abstimmung enorme Geldsummen, die das Königreich im Falle eines EU-Austritts einsparen würde, die sich aber als haltlos erwiesen. „Fake News haben zwei entscheidende Vorteile gegenüber korrekten Nachrichten“, sagt Schemer. Man müsse sie erstens nicht überprüfen, bevor man sie veröffentliche, weshalb sie sich schneller verbreiten könnten als seriöse Nachrichten, deren Wahrheitsgehalt immer erst durch weitere Quellen auf die Probe gestellt werden muss. Zweitens seien Fake News oft so skurill, dass Rezipienten sie im Internet weiterverbreiteten – selbst wenn sie diese gar nicht glaubten. Eine biedere Nachrichtenmeldung teilen hingegen die wenigsten im Netz.

Fake News können sich gegen Politiker richten und diese verunglimpfen, aber auch Presseorgane können Zielscheibe sein, zumal den Medien auf Internetseiten wie „KenFM“ und den „Nachdenkseiten“ ohnehin schon grundsätzlich Unglaubwürdigkeit vorgeworfen wird. Allerdings sei die Zahl der Menschen, die ausschließlich auf solchen Internetseiten verkehrten und damit für dort verbreitete, falsche Nachrichten besonders anfällig seien, hierzulande eher gering,

Foto Michael Kretzer

Christian Schemer

sagt Schemer. Allgemeinen Befürchtungen zum Trotz hält der Professor auch das Einmischen russischer Akteure in den aktuellen Bundestagswahlkampf für unwahrscheinlich.

Aber ist es nicht denkbar, dass Plattformen wie die bereits reüssierenden amerikanischen „Breitbart News“ sich auch hierzulande noch stärker behaupten? Die dort publizierten Nachrichten bestehen aus verkürzten Meldungen und gelegentlichen Verschwörungstheorien – und betreffen auch Deutschland. Im sogenannten „Fall Lisa“ war es ein Journalist des russischen staatlichen Fernsehsenders „Erster Kanal“, der davon berichtete, dass das russlanddeutsche Mädchen Lisa in Deutschland von drei Männern, die als Flüchtlinge aus dem Nahen Osten dargestellt wurden, entführt und dreißig Stunden lang immer vergewaltigt worden sei. Diese Meldung löste vorübergehend Proteste aus und nötigte den amtierenden Außenministern Deutschlands und Russlands Stellungnahmen ab. Doch am Ende entpuppte sich die Geschichte als Falschmeldung.

„Ich glaube, es wird immer wieder Wellenbewegungen geben, in denen das Thema Fake News wichtiger wird“, sagt Schemer. „Das hängt mit der Konjunktur von Themen zusammen, die manchen Parteien Zulauf bescheren.“ Das habe etwa auf die Flüchtlingsthematik zugetroffen, die dem rechten Rand durch Verschwörungstheorien und drastisch überspitzte Meldungen zusätzliches Interesse sicherte.

Am Diskurs über Fake News lässt sich laut Schemer aufzeigen, „was korrekte Nachrichten sind und dass ein guter Journalist sauber recherchiert und mehrere Quellen prüft“. Immer noch seien Menschen überzeugt: Journalisten bekommen von jemandem gesagt, was sie zu schreiben haben. Dennoch glaubt er nicht, dass Fake News derzeit in Deutschland erheblichen Schaden anrichten könnten: „In der momentanen Situation würde ich Entwarnung geben.“ SHEA WESTHOFF

AUF EIN WORT

Foto Wolfgang Eilmes

Kia Baniashraf, *21 Jahre, Justus-Liebig-Universität Gießen, 2. Semester Moderne Fremdsprachen, Kulturen, Wirtschaft*

Besucht lieber Freunde

Was liegt an in dieser Woche?

Ich werde vier Klausuren schreiben. Das Schwierigste wird sein, dass ich mich durchgehend konzentriere. Aber in der Klausurenphase habe ich eh nur die Uni im Kopf.

Was gefällt Ihnen an dem Fach, das Sie studieren?

Vorher hatte ich angefangen, Englisch und Geschichte auf Lehramt zu studieren. Das hat mir nicht so gefallen. Mit Englisch wollte ich aber schon weitermachen. Mein derzeitiges Studium ist ja eine Mischung aus BWL und Sprachen, in meinem Fall Französisch und Englisch. Französisch hatte ich schon sechs Jahre lang in der Schule. Sprachen liegen mir eigentlich.

Und was stört Sie?

BWL fällt mir schwer, weil ich es nicht so mit Zahlen habe. Aber wenn man gut lernt und die richtige Nachhilfe hat, kann man das hinkriegen. Die Englisch-Seminare finde ich teilweise eintönig.

Was wollten Sie Ihrem Hochschulpräsidenten schon immer mal sagen?

Da fällt mir nichts ein. Ich studiere hier, ich sehe hier Freunde, ansonsten habe ich keine so enge Bindung zur Uni.

Ihr Lieblingsort an der Hochschule?

Die Mensa, das ist ein guter Treffpunkt. Ich bin auch gerne in der „Cubar“, dem Café in der Uni-Bibliothek.

Und wohin gehen Sie auf keinen Fall, wenn Sie nicht müssen?

Vielleicht in die große Bibliothek, weil sie manchmal voll und stickig ist.

Wo ist an der Hochschule der beste Ort, um zu flirten?

Keine Ahnung, das habe ich hier noch nicht gemacht. Wahrscheinlich in der „Cubar“. Aber theoretisch ist das ja auch gar nicht schwer, es sind ja lauter junge Leute hier. Du gehst hin, fragst: „Was studierst du?“ Und dann: mal schauen.

Wie wohnen Sie?

Ich wohne in einer Wohngemeinschaft in der Innenstadt.

Wie finanzieren Sie Ihr Studium?

Hauptsächlich durch Bafög, teilweise durch meine Eltern. Außerdem mache ich ab und zu Messearbeit und helfe manchmal bei der Fußballschule des FSV und FFH in Frankfurt aus.

Wo gehen Sie abends am liebsten hin?

Am liebsten gehe ich zu Freunden. Da chillen wir, schauen Filme, spielen Playstation oder kochen. Clubs reizen mich nicht sonderlich, höchstens mal mit einer großen Gruppe.

Was gefällt Ihnen an Gießen, was nicht?

Mir gefällt, dass es viele junge Leute gibt. Das ist in meiner Heimatstadt Bad Nauheim anders. Und hier gibt es eine Vielfalt an Leuten. Wohnen und Verpflegung sind hier echt günstig. Bisher gibt es eigentlich nichts, was ich an Gießen nicht mag.

Was wollen Sie nach dem Studium machen?

Langsam Fuß fassen im Leben und arbeiten. Allerdings bin ich mir noch unsicher, ob ich nicht vielleicht doch noch den Master mache.

Aufgezeichnet von **Shea Westhoff**

Besserer Schutz

Ameisen mit Tarnkappe auf Raubzug

Unter den Ameisenarten sind sklavenhaltende Ameisen besonders heimtückisch. Sie legen sich chemische Tarnkappen an, um auf ihrem Raubzug durch fremde Nester nicht erkannt zu werden, wo sie die Brut stehlen und anschließend in ihrem eigenen Bau versklaven. Eine Arbeitsgruppe aus Biologen um Susanne Foitzik geht an der Uni Mainz der Frage nach, welche Faktoren die Kohlenwasserstoffe beeinflussen, die für den Erfolg der Tarnkappe verantwortlich sind. Sie befinden sich auf der Haut der Ameisen, die einander hauptsächlich über ihren Duft erkennen. Die Mainzer Evolutionsbiologen interessiert besonders, warum sich die Kohlenwasserstoffprofile bei parasitären Ameisen wie den Sklavenhaltern anders entwickelt haben als bei anderen Arten. Dabei fanden sie heraus, dass die Parasiten weniger von jenen Signalstoffen aufweisen, die zur Erkennung dienen – und deshalb auch in unterschiedlichen Nestern mit verschiedenen Duft-Profilen unentdeckt bleiben können. *ddt.*

Foto epd

Rückläufige Zahlen

Weniger tödliche Tierversuche an Unis

Rückläufige Zahlen bei den tödlichen Tierversuchen, dafür mehr vielversprechende Alternativen: Für die Forschung an den hessischen Universitäten starben zuletzt weniger Tiere. In den vergangenen zwei Jahren waren es jeweils 37 000, zuvor, im Jahr 2014, waren es noch 50 000 gewesen, heißt es in einer Antwort von Wissenschaftsminister Boris Rhein (CDU) auf eine Anfrage der Grünen-Abgeordneten Ursula Hammann.

Auch die Zahl der Tierversuche wäre in der Summe rückläufig, gäbe es an der TU Darmstadt nicht stark steigende Versuchszahlen im Fachbereich Biologie. Rhein wies jedoch darauf hin, dass die Hochschule „jedes verbrauchte Tier als Tierversuch zähle“ und es sich größtenteils um tier- und umweltschutzbezogene Versuche an Fischen handele. Diese kämen nicht zu Schaden, sondern würden nach Ende des Versuchs wieder in die Freiheit entlassen. Die Darmstädter Forscher wollen herausfinden, wie Wanderfische besser geschützt und unterstützt werden können. Rhein zufolge ließen sich dennoch „in den letzten drei Jahren auch bei der Zahl der durchgeführten Tierversuche Reduktionen erkennen“.

An den hessischen Universitäten nutzen Wissenschaftler die Tierversuche hauptsächlich für ihre Grundlagenforschung. Wer mit Tieren arbeitet, muss nachweisen, dass es dazu keine Alternative gibt. *lhe.*

Neue Erkenntnis

Der Arterienbildung auf der Spur

Die Bildung von Arterien ist während der Entwicklung von Menschen, aber auch bei Erwachsenen von großer Bedeutung. Auch bei lebensbedrohlichen Herz-Krankheiten könnte die Bildung neuer Arterien großen therapeutischen Nutzen haben. Allerdings sind die molekularen Mechanismen der Arterienbildung noch weitgehend unbekannt.

Einem Forscherteam um Tilman Borggrefe vom Biochemischen Institut der Uni Gießen und seinem Kollegen Ralf Adams vom Max-Planck-Institut für molekulare Biomedizin in Münster ist nun ein wichtiger Schritt bei der Erforschung der Arterienbildung gelungen. Die an den Studien beteiligten Forscher kombinierten bei ihren Arbeiten genetische Experimente mit pharmakologischen Methoden. Dabei fanden sie heraus, dass einem Rezeptor namens Notch in diesem Prozess eine wichtige Rolle zukommt. Einer Mitteilung der Universität zufolge könnten die Erkenntnisse die Grundlage dafür sein, neue therapeutische Ansätze für die Bildung neuer Arterien nach Organverletzungen zu entwickeln. *ddt.*

Foto dpa