Neues aus Weingarten

Radfahrerin stürzt und verletzt sich schwer

WEINGARTEN (sz) - Bei einem Ausweichmanöver ist am Mittwochmorgen in Weingarten eine 71-jährige Radfahrerin gestürzt und hat sich dabei schwere Verletzungen zugezogen. Wie aus dem Polizeibericht hervorgeht, querte ein 72-Jähriger mit seinem Opel von der Wildeneggstraße kommend die vorfahrtsberechtigte Wolfegger Straße und übersah dabei die Richtung Stadtmitte radelnde Frau. Ohne dass es zu einer direkten Berührung mit dem Opel kam, stürzte diese und musste mit schweren Verletzungen in ein Krankenhaus transportiert werden. Laut Polizei hatte sie keinen Schutzhelm getragen. Den entstandenen Sachschaden am Fahrrad geben die Beamten mit rund 100 Euro an.

Kabarett-Duo gastiert in der „Linse“

WEINGARTEN (sz) - Tina Häussermann und Fabian Schläper, bekannt als das Duo „Zu Zweit", kommen heute ins Kulturzentrum Linse nach Weingarten. „Ich war's nicht!“ heißt ihr derzeitiges Programm, das quer durch Deutschland führt. Und das sich lustvoll an den Unwegsamkeiten des Daseins festhält: Wer hat den Hamster bestattet, obwohl der nur Winterschlaf gehalten hat? Wer hat die rote Badehose bei 90 Grad gewaschen? Wer hat auf dem Sitzrasenmäher das Autofahren gelernt? Fragen über Fragen, die nur eine Antwort kennen: Ich war's nicht! Häussermann und Schläper haben als Duo schon mehrere Kleinkunstpreise erhalten. Ihr Auftritt in Weingarten beginnt um 20 Uhr. Karten gibt es ab 17.30 Uhr im Kulturzentrum Linse; Reservierungen sind nicht möglich.

Polizei stoppt Raser – Motorradfahrer fährt 137 km/h

WEINGARTEN (sz) – Einige Raser sind der Verkehrspolizei Ravensburg bei Geschwindigkeitsmessungen im Stadtgebiet Weingarten am Donnerstag aufgefallen. Den traurigen Rekord erzielte ein 22-jähriger Motorradfahrer, der mit seiner Maschine zum Saisonabschluss noch einmal fahren wollte und hierbei bei erlaubten 50km/h mit 137 Stundenkilometern gemessen wurde. Im droht jetzt ein Bußgeld von mindestens 1200 Euro und ein dreimonatiges Fahrverbot. Etwa eine Stunde nach diesem Vorfall wurde ein 18-jähriger Fahranfänger gestoppt, der bei erlaubten 50km/h 110km/h auf dem Tacho hatte. Auch ihm droht ein saftiges Bußgeld, ein Fahrverbot sowie eine Nachschulung.

Ausstellung zeigt neue Arbeiten von Thom Barth

WEINGARTEN (sz) - „Von Lalibela nach Aleppo“: Unter diesem Titel werden neue Arbeiten von Thom Barth in der Akademie der Diözese Rottenburg-Stuttgart im Kloster Weingarten gezeigt. Zur Vernissage am Sonntag um 11 Uhr sprechen Ilonka Czerny, Referentin für Kunst an der Akademie, und Herbert Köhler, Kunst- und Kulturpublizist, Ravensburg. Die Ausstellung wird dann bis 26. Januar im Tagungshaus der Akademie in Weingarten gezeigt.

Interview

„Dass die NSA alles abhört, weiß man schon lange“

Wolfgang Ertel, Informatik-Professor an der Hochschule Ravensburg-Weingarten, über Datenschutz im Internet

Die beispiellose Schnüffelei der NSA schlägt große Wellen. Nicht erst, seit bekannt wurde, dass auch Bundeskanzlerin Angela Merkel im Fadenkreuz des US-Geheimdienstes steht. Wolfgang Ertel, Professor für Informatik an der Hochschule Ravensburg-Weingarten, ist Experte für Kryptografie, der Lehre von der Datenverschlüsselung. Im Interview mit SZ-Redakteur Daniel Drescher spricht er darüber, wie der Einzelne sich vor Datendieben schützen kann, wie sicher Internetkommunikation überhaupt ist – und warum jeder Informatikstudent E-Mails mitlesen kann.

Wolfgang Ertel von der Hochschule Ravensburg-Weingarten war nicht sonderlich überrascht vom NSA-Skandal. Vor elf Jahren veröffentlichte der Informatik-Professor bereits einen Artikel im Hochschulmagazin, in dem es auch um die technischen Möglichkeiten des US-Geheimdienstes ging. FOTO: DANIEL DRESCHER

Herr Ertel, vor elf Jahren haben Sie im Hochschulmagazin „Konzepte“ einen Artikel über Internet-Überwachung veröffentlicht, in dem es auch um die NSA ging. Damals sagten Sie, es gebe viele Möglichkeiten geheimer Kommunikation im Internet. Gilt das heute immer noch – nach allem, was wir durch die Enthüllungen Edward Snowdens über die massenhafte Netz-Überwachung erfahren haben?
Natürlich. Es gibt kryptografische Verfahren, bei denen sich die Experten einig sind, dass man sie gegenwärtig nicht knacken kann. Was in 20 Jahren ist, weiß man nicht. Ich weiß auch nicht, was die NSA tut. Das ist ein Geheimdienst und den Namen trägt er nicht umsonst. Die Mitarbeiter dürfen nicht über ihre Arbeit reden. Wir haben im Fall Snowden gesehen, welche Schwierigkeiten er bekommen hat. Wir wissen nicht, auf welchem Stand die NSA ist. Aber wir wissen, dass sie mit extrem viel Geld, großer Rechnerleistung und exzellenten Leuten ausgestattet ist. Die NSA ist auf dem Stand der Kunst und vielleicht sogar dem Rest der Welt etwas voraus. Allerdings sicher nicht um Jahrhunderte, sondern um ein kleines bisschen. Aber das heißt nicht, dass der Geheimdienst alles knacken kann, was wir für sicher halten.

Was macht Sie da so sicher?
Ein praktisches Beispiel aus der Vergangenheit: In den 70er-Jahren wurden die Public-Key-Kryptografieverfahren erfunden. 1977 zum Beispiel mit dem RSA ein ganz wichtiges Verfahren. Genau 20 Jahre später stellte sich heraus, dass der britische Geheimdienst dieses Verfahren schon vier Jahre vorher erfunden hatte. Aber die Briten durften es nicht publizieren. Vier Jahre sind in der Wissenschaft nicht viel. Das gibt mir Vertrauen: Die NSA ist uns sicher nicht meilenweit voraus. Natürlich wird sie versuchen, die besten Köpfe aus der Wissenschaft abzuschöpfen. Aber nicht jeder exzellente Wissenschaftler will bei so einer Organisation arbeiten. Auch außerhalb der NSA gibt es kluge Köpfe.

Waren Sie davon überrascht, als der NSA-Skandal von Edward Snowden öffentlich gemacht wurde?
Überhaupt nicht. Das ist nichts Neues. Ich war eher über den Rummel überrascht, den es gab. Dass die NSA alles abhört was geht, weiß man schon lange. Vor etwa 20 Jahren wurde bekannt, dass die NSA sich in Frankfurt über einem Stockwerk eingemietet hatte, in dem ein zentraler Netzknoten betrieben wurde. Ein seltsamer Zufall, oder? Die NSA ist mächtig und hat die besten Techniken. Natürlich versuchen die Amerikaner es, aber sie können nicht alles abhören. Die gute Nachricht: Es gibt sehr sichere Verschlüsselungen, zum Beispiel beim E-Mail-Verkehr. Das kann ich auch nur jedem empfehlen. Wer es nicht tut – da muss man sagen, selber schuld. Jeder Informatikstudent, der sich mit Netzwerktechnik auskennt, ist in der Lage, E-Mails abzufangen.

Wie bitte?
Das ist keine geheime Kommunikation. Eine E-Mail ist wie eine Postkarte. Jeder, der sie rumliegen sieht, kann sie lesen. Mails sind nicht verschlüsselt, sie gehen offen übers Netz. Wer sich in Netzwerktechnik gut auskennt, kann alles im Klartext mitlesen. Vielleicht ist es gut, dass das durch die Presse jetzt mal publik wird.

Wie kann sich der Einzelne dann schützen?
Nur durch Verschlüsseln der E-Mail. Es gibt kostenlose Software dafür. Eine sehr gute ist GPG, Gnu Privacy Guard. Das ist ein offenes, frei verfügbares und kostenloses System. Dass es offen ist, das ist ganz wichtig, wenn es um Sicherheitsstandards geht. Denn nur dann können Kryptanalytiker versuchen, die Verschlüsselungstechniken zu knacken. So wird heute die Sicherheit bewiesen – oder widerlegt.

Wie einfach oder aufwendig ist es, Mails zu verschlüsseln?
Das ist eine kleine Hürde, die man bewältigen muss. Wenn man Mails verschlüsselt, muss man sie mit einem passenden Schlüssel des Empfängers codieren. Diesen Schlüssel muss er mir zukommen lassen. Das ist eine Hemmschwelle. Für eine sichere Kommunikation müssen also meine Gesprächspartner mitmachen. Wir bräuchten eine Public-Key-Infrastruktur, die müsste man aufbauen. Das sage ich seit Jahrzehnten. Dafür wäre der Staat verantwortlich. Insbesondere wenn das Innenministerium findet, dass wir einen Bundestrojaner brauchen. Auch hier ein Beispiel: Der elektronische Personalausweis ist eine gute Sache. Ich fand das toll, weil ich dachte: Endlich sorgt der Staat für die längst überfällige Infrastruktur für Verschlüsselung und digitale Signatur. Auf dem Ausweis ist ein Chip, ein kleiner Computer, der Algorithmen zur Ver- und Entschlüsselung eingebaut hat. Leider ist durch einen Designfehler bei der Entwicklung des neuen Ausweises die digitale Signatur bis heute immer noch nicht realisiert. Immerhin gibt es nun eine Pilotstudie, an der Bürger teilnehmen können.

Aber dass ich meine Mails verschlüssele, bringt nichts, wenn es mein Gegenüber nicht auch tut, oder?
Da brauchen wir einen Standard. Das kann Generationen dauern, bis es einen gibt. Der Staat müsste hier durch eine passende Infrastruktur dafür sorgen, dass sich ein Standard durchsetzt. Das ist Aufgabe des Staates. So ein Standard könnte von mehreren Playern gesetzt werden. Staat, Firmen, Banken. Banken tun das schon, beim Online Banking. Aber sie haben sich nie geeinigt, jede Bank hat eine eigene Signatur. Firmen interessiert in erster Linie, dass sie mit Partnerfirmen kommunizieren können. BASF hat eine Public-Key-Infrastruktur aufgebaut, basierend auf PGP, dem Vorgänger von GPG.

Was ist mit populären Diensten wie Whatsapp für Smartphones oder Googlemail? Darf man die überhaupt nutzen, wenn man nicht überwacht werden will?
Whatsapp verschlüsselt zwar die Nachrichten, aber leider sehr unsicher. Die Whatsapp-Verschlüsselung ist zu einfach und wurde auch schon geknackt. Für E-Mails gilt: Mit einem auf dem Rechner installierten E-Mail-Client wie Thunderbird kann man komfortabel und sicher verschlüsseln. Bei einem Mail-Anbieter mit Web-Interface geht das nicht oder nicht sicher genug. Wichtig ist: Die Voreinstellung bei allen Email-Programmen ist die, dass nicht verschlüsselt wird. Denn beim Verschlüsseln müssen Sender und Empfänger zueinander passende Schlüssel und Verschlüsselungssoftware verwenden. Darum muss sich der Anwender kümmern.

Nehmen es nur Privatnutzer nicht so genau mit Verschlüsselung? Wie machen es Unternehmen, die ein Interesse an abhörsicherer Kommunikation haben müssen?
Ich war im Jahr 2000 für ein Forschungssemester im Silicon Valley. Dort haben wir ein Patent entwickelt. Als ich mit Patentanwälten redete und meinte, dass ich die Mails verschlüsselt schicken will, waren die überrascht: Das hätten sie noch nicht gemacht. Ich kenne viele Firmen, die schicken alle Mails unverschlüsselt. Das Problem ist: Informatik ist eine abstrakte virtuelle Welt. Wenn ein Terrorist eine physikalische Bombe hochgehen lässt, steht es am nächsten Tag in der Zeitung. Aber wenn eine virtuelle Bombe hochgeht und die Firma deshalb bankrott geht, wird es niemand erfahren. Sonst gehen die Aktienkurse runter. So etwas wird nie publiziert. Deshalb haben viele Firmenchefs vor Cyber-Angriffen immer noch wenig Angst.

Wenn ich als normaler Kunde beispielsweise in den Handyladen gehe, bekomme ich Standardware, und kein Kryptohandy. Was kann man hier tun?
Was wir auf jeden Fall tun können: Als Kunden mehr Sicherheit einfordern. Die Industrie baut alles, was der Kunde will. Aber da heute praktisch kein Kunde Sicherheit verlangt, wird sie nicht angeboten. Es gibt heute schon Verschlüsselungsverfahren für Handytelefonate und SMS. Zum Beispiel die kostenlose App „redphone“ für Android verschlüsselt Telefonate. Die Sprachqualität ist zwar nicht besonders hoch. Und es müssen natürlich beide Gesprächspartner diese App benutzen. Das ist der Preis den wir für die Sicherheit zahlen müssen.

Warum ist es unverhältnismäßig, diese Massenüberwachung zu betreiben – und inwiefern schadet es der Demokratie?
Das ist meine persönliche Meinung: Bundestrojaner und solche Dinge – das ist nicht der richtige Weg. Denn mit riesigem Aufwand verunsichert der Staat gigantisch viele unschuldige Bürger, macht ihnen Angst. Das darf man in einer Demokratie nicht tun. Der Staat hat natürlich die Aufgabe, die Bürger zu schützen. Jeder will sicher leben. Deshalb gibt's die Polizei. Und man muss etwas gegen Terroristen tun. Aber selektiv und nur bei entsprechendem Verdacht. Wenn ein Grund da ist soll durchaus die Kommunikation Einzelner überwacht werden, auf Anweisung des Staatsanwalts, ähnlich einem Durchsuchungsbefehl. Aber in dieser Breite alles abzuhören, halte ich für Unsinn. Egal ob BND oder NSA. Was man stattdessen mit dem Geld machen sollte, das kann ich Ihnen sagen. Die Polizei braucht viele sehr gute Informatiker. Leute, die sich im Netz mindestens so gut auskennen wie die Terroristen. Solche Leute werden zum Beispiel an unserer Hochschule ausgebildet. Um die Terroristen zu fangen, brauchen wir kluge Köpfe mit entsprechendem Fachwissen.

Zur Person

Wolfgang Ertel ist seit 1994 an der Hochschule Ravensburg-Weingarten. Sein Schwerpunkt ist die künstliche Intelligenz. Aber auch mit Kryptografie, der Wissenschaft von der Verschlüsselung von Daten, kennt er sich aus. **2001** veröffentlichte er sein **Buch „Angewandte Kryptografie“**. Ertel ist **Datenschutzbeauftragter** der Hochschule. Er hat in Konstanz Physik und Mathematik studiert, an der TU München promovierte er. (sz)

Informatiker erklärt, wie man seine Daten schützt

Thomas Sick informiert über die Tricks der Geheimdienste und über gute Verschlüsselungen

Von Victoria Grenz

WEINGARTEN - Passwort oder Fingerabdruck, das ist die Frage des Abends. Und auf die hat Informatiker Thorsten Sick, der bei einer Sicherheitsfirma arbeitet, am Mittwochabend in der Pädagogischen Hochschule Weingarten nur eine Antwort: Fingerabdrücke sind nicht sicher, um die eigenen Daten zu schützen. An diesem Abend geht es vor allem um digitale Selbstverteidigung und darum, wie Daten im Internet überhaupt geschützt werden können.

„Gute Kryptologen, die gute Verschlüsselungen machen, sind paranoid“, sagt Thorsten Sick. Offenbar haben die genialen Mathematiker damit recht, denn fast täglich kommen neue Details an die Öffentlichkeit, wer noch alles auf der Überwachungsliste des amerikanischen Geheimdienstes NSA steht. Auf die Hersteller, die teilweise mit der NSA kooperieren, und Politik sei dabei kein Verlass, so Sick. Was wir uns abgewöhnen sollten, ist die Denke: 'Die werden das schon richtig machen'. „Nein werden sie nicht“, sagt er. Sein Fazit deshalb: Man muss selbst etwas tun.

Die einzige sichere Option sind für Sick Passwörter. „Fingerabdrücke hinterlässt man überall“, sagt er und erklärt, wie schnell so ein Abdruck mit einem Laserdrucker und etwas Leim rekonstruiert werden kann. Und dann darf das Passwort natürlich auch nicht abc123, sunshine oder 12345 lauten. Eine gute Möglichkeit, ein sicheres Passwort zu generieren, das auch nicht vergessen wird, ist, vier gewöhnliche Worte auszuwählen und diese dann zu kombinieren. Sicks Beispiel: richtig, Pferd, Batterie und Stapel. Mit einer kleinen ausgedachten Geschichte dazu leicht zu merken, dafür aber recht schwer zu erraten.

Das Nächste, was der private Internetnutzer zu Hause für seine Datensicherheit tun kann, ist auf sogenannte Open-Source-Programme zu setzen. Bei dieser Software sind die Baupläne öffentlich und sobald ein Fehler auftritt, kann der von jedem korrigiert werden. Bei Programmen der großen Hersteller dagegen sind die Baupläne unbekannt und es weiß niemand, ob nicht auch Dritte Zugriff auf die eigenen Daten haben. Sick rät zum Beispiel zu Firefox anstatt der gängigen Internetbrowser der großen Hersteller. Kombiniert man diese Programme noch mit zusätzlicher Verschlüsselungssoftware, sind die Daten recht gut geschützt. Zumindest brauche die NSA dann länger zum Entschlüsseln, so Sick.

Wie gute und auch schlechte Verschlüsselung im Internet funktioniert, erklärt Sick ganz einfach mit Briefumschlägen und Schachteln. Zwar sieht die Verschlüsselung so einfach und verständlich aus, bei der Umsetzung braucht es allerdings noch etwas Geduld. Manche der Verschlüsselungsprogramme sind nicht ganz einfach zu bedienen und brauchen etwas Zeit, bis sie tatsächlich auch installiert sind. Sick hofft, dass das so schnell wie möglich verbessert wird. Denn dann wäre es wesentlich wahrscheinlicher, dass in Zukunft hauptsächlich verschlüsselte E-Mails verschickt werden. Momentan hapert es nämlich daran, dass kaum einer die Verschlüsselung auch lesen kann.

Facebook-App löschen

Der Wermutstropfen des gut besuchten Vortrags, zu dem der Studiengang Medien- und Bildungsmanagement eingeladen hatte: Es ist schwer, gute Verschlüsselungsprogramme für Smartphones und Handys zu finden. Doch auch hier kann man zumindest die Facebook-App löschen. Die frisst, laut Sick, nicht nur enorm Akku, bei Facebook ist auch bekannt, dass die Daten bei der NSA landen.

Thorsten Sick beim Vortrag. FOTO: VICTORIA GRENZ