

## Richter auf der Suche nach der Doktorwürde

**Freiburg** Der Skandalphysiker Jan Hendrik Schön kämpft um seinen Titel. Von Frank van Bebber

Was wird aus jemand, den die wissenschaftliche Gemeinschaft als Fälscher aus ihrer Mitte verbannt hat? Zumindest darauf hat das Freiburger Verwaltungsgericht bereits eine Antwort gefunden. Jan Hendrik Schön, erst Starphysiker, dann tief gefallener Skandalphysiker, arbeitet als Prozessingenieur in Deutschland. „Die Firma wusste von Anfang an Bescheid, das war kein Problem“, sagt Schön den drei Richtern und zwei Schöffen bei der Verhandlung, die bis in den Mittwochabend dauerte.

Erstmals seit Aufwiegen seiner Machenschaften in den amerikanischen Bell-Labors im Jahr 2002 zeigte sich Schön wieder öffentlich. Er selbst hat den Prozess angestrengt: Der Physiker klagt gegen die Entscheidung der Universität Konstanz, ihm wegen unwürdigen Verhaltens nachträglich seinen Dokortitel zu entziehen – obwohl die Doktorarbeit selbst gar nicht bemängelt wird. „Ich sehe nicht, warum ich das aufgeben sollte“, sagt er.

In den Labors der Hochschule am Bodensee hatte Schöns Höhenflug einst begonnen. Mit einem Konstanz-Dokortitel wechselte Schön 1998 an die Bell-Labors in den USA. Der redegewandte Physiker publizierte eine Flut bahnbrechender Ergebnisse. Schön, Jahrgang 1970, galt als künftiger Nobelpreisträger.

Doch nach ersten Zweifeln entdeckten Bell-Gutachter in seinen US-Arbeiten dreiste Manipulationen. Seine Arbeiten wurden zurückgezogen, Schön ins wissenschaftliche Nichts entlassen. Er selbst erklärt die falschen Zahlen bis heute mit Schlamperei. Doch weitere Gutachter, auch der Deutschen Forschungsgemeinschaft, bestätigten die Manipulationsvorwürfe.

Vor Gericht ist für den früheren Konstanz-Juraprofessor Dieter Lorenz, der für seine Universität spricht, der Fall darum klar: ein Dokortitel mag gesellschaftlich nicht mehr viel bedeuten, in der wissenschaftlichen Gemeinschaft begründet er die Pflicht zu wissenschaftlich korrektem Verhalten. Die Universität beruft sich dabei auf einen wenig beachteten Passus im Hochschulgesetz, der auf ein Reichsgesetz von 1939 zurückgeht. Demnach ist der nachträgliche Titelerwerb wegen unwürdigen Verhaltens möglich, selbst wenn die Doktorarbeit selbst korrekt war. Der Anwalt Schöns hält den Begriff der Würde für so willkürlich auslegbar, dass der Passus schlicht verfassungswidrig sei. Für niemanden wäre vorhersehbar, wann ihm ein Titelerwerb drohe, sagt er. Zudem treffe ein Entzug Schöns nicht nur wissenschaftlich, sondern auch gesellschaftlich – lebenslang.

Die Nachfragen der Freiburger Richter machen deutlich, dass auch sie die Konstanz-Argumentation nicht immer entwirren können: So kann nach der Uni-Lesart des Gesetzes ein Doktor seine Würde nur nachträglich verlieren. Käme Schön heute mit einer neuen Doktorarbeit, dürften seine früheren Verfehlungen dagegen keine Rolle spielen – die Universität müsste ihn als Doktoranden annehmen.

Dieter Lorenz von der Uni Konstanz will sich darauf nicht einlassen. Er betont die Doktorpflichten: „Der wissenschaftliche Fortschritt ist ausgeschlossen, wenn manipuliert wird.“ Hätte er solche klaren Worte schon vor einigen Jahren gefunden, der Universität wäre der Prozess womöglich erspart geblieben. Doch ausgerechnet Lorenz war auch Vorsitzender jener Kommission, die nach dem Skandal Schöns Doktorarbeit untersuchte. Außer ein paar Schlampereien mochte sie nichts finden. Als die Kommission dann noch erklärte, eine „gewisse Glättung der Darstellung“ sei nicht in jedem Fall verwerflich, schlug der Universität zunehmend Kritik entgegen. Als letzten Ausweg fand sie den Würde-Passus im Gesetz, um ein öffentliches Zeichen für korrektes wissenschaftliches Arbeiten zu setzen. Am Montag wollen die Richter ihre Entscheidung verkünden.

### Kontakt

**Redaktion Wissenschaft**  
Telefon: 07 11/72 05-11 31  
E-Mail: wissenschaft@stz.zgs.de

## Der „digitale Erstschlag“ und seine Folgen

**IT-Sicherheit** Ein Computervirus greift weltweit Industrieanlagen an. Sind auch deutsche Firmen bedroht? Von Steffen Haubner

Der Krieg der Zukunft findet im Internet statt. Diese Prophezeiung vieler Experten ist seit kurzem Realität. Wann und wo der „digitale Erstschlag“ erfolgt ist, weiß derzeit allerdings niemand. Doch für die Experten ist klar: Er hat stattgefunden.

Alles fing mit einer Warnung vor einer Schadssoftware an, die in großem Umfang PCs in aller Welt infizierte. Im digitalen Zeitalter hat man sich an solche Meldungen gewöhnt. Der Schädling geht professionellen Virenjägern irgendwann ins Netz, wird analysiert und die so identifizierten Sicherheitslücken geschlossen. Der PC-Nutzer aktualisiert seine Sicherheitssoftware und geht zur Tagesordnung über.

Doch diesmal war alles anders. Der sogenannte Trojaner, ein Programm, das unbemerkt auf den Rechner gelangt, um zu einem bestimmten Zeitpunkt die Kontrolle zu übernehmen, nutzte nämlich gleich vier Sicherheitslücken im Betriebssystem Windows. Solche noch unentdeckten Lecks sind für Cyberkriminelle ausgesprochen wertvoll. So viel Aufwand zu betreiben, nur um ein paar sensible Nutzerdaten auszuspionieren, ist ungewöhnlich.

Zudem richtete Stuxnet, wie er mittlerweile von Sicherheitsexperten getauft wurde, auf den befallenen Rechnern keinen Schaden an. Auch das legte den Verdacht nahe, dass private Rechner gar nicht das Ziel des Angriffs waren. Eine eingehendere Analyse brachte kurz darauf Erstaunliches zutage: In den Tiefen der Software schlummerte nämlich ein Code, der offensichtlich die Aufgabe hatte, sich in der Steuerungssoftware von hochkomplexen Industrieanlagen einzunisten.

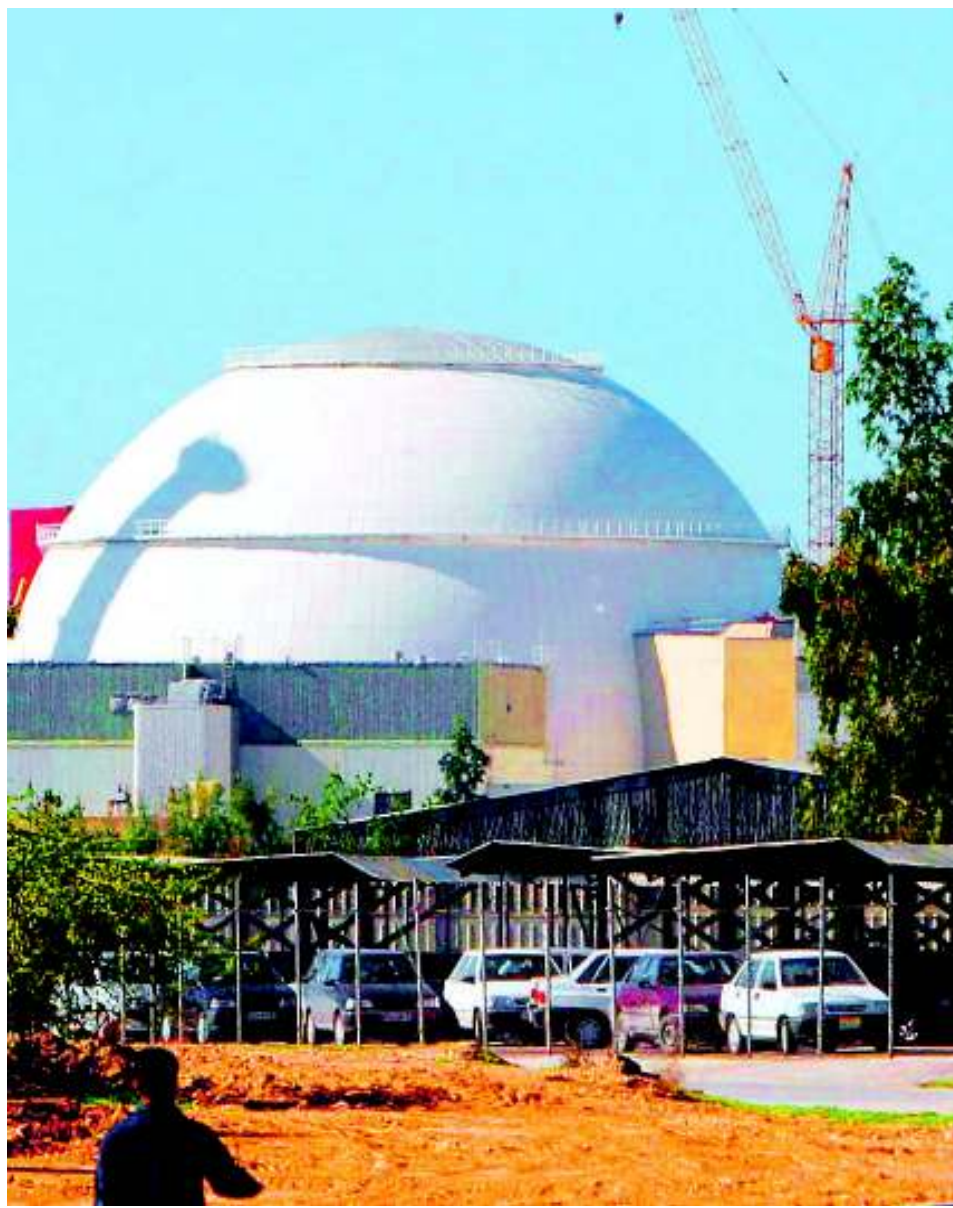
„Solche Systeme sind eigentlich in sich geschlossen“, sagt Stefan Wesche von der Security-Firma Symantec, die Stuxnet als eines der ersten Unternehmen entdeckte. Die Raffinesse, mit der sich das Virus dort trotzdem Zugang verschaffte, verblüffte die Experten. Die massenhafte Verbreitung war offenbar nur Mittel zum Zweck gewesen. Sein ganzes Potenzial entfaltet der Schädling nämlich erst dann, wenn er auf eine jener Anlagen stößt, auf die er offenbar angesetzt wurde. Eingeschleust über einen simplen USB-Stick oder eine E-Mail, gelang er schließlich in die Computersteuerung der Anlage und wartet dort auf weitere Befehle. „Es ist der erste bekannte Schadcode, der zu so etwas in der Lage ist“, so Wesche.

Doch wer ist der Urheber dieser Attacke und gegen wen war sie gerichtet? Darüber wird in Fachkreisen derzeit noch wild spekuliert. Fest steht, dass ausschließlich Anlagen betroffen sind, die mit einem bestimmten Programm der Firma Siemens arbeiten.

„Es ist der erste Code, der zu so etwas in der Lage ist.“

Stefan Wesche, Firma Symantec

Lebensmittelherstellern oder Stahlfirmen, aber auch bei Pipelines oder Atomkraftwerken. Sie werden überall dort gebraucht, wo der Mensch die komplexen Mess- und Steuerungsmechanismen nicht mehr allein überblicken kann. Stuxnet hatte also die Aufgabe, eine Art Fernsteuerung zu in-



Die iranische Atomanlage Buschehr könnte das Ziel von „Stuxnet“ gewesen sein. Foto: dpa

stallieren, mit der sich Industrieanlagen aller Art beeinflussen lassen.

Der Hamburger Security-Experte Ralph Langner, dessen Unternehmen auf die Sicherheit solcher Anlagen spezialisiert ist, steuerte weitere wichtige Teile des Puzzles bei. „Für diese Attacke war eine unglaubliche Menge von Know how erforderlich“, so der Experte. „Das war kein einzelner Hacker im Keller seines Elternhauses.“ Eine abschließende Auswertung ist laut Langner nur eine Frage der Zeit. Das wiederum lasse zwei Rückschlüsse zu: Zum einen mussten die Angreifer damit rechnen, dass

man ihnen irgendwann auf die Spur kommt. Die damit drohende Gefängnisstrafe scheint die Betroffenen aber nicht zu beeindrucken. Waren hier also staatliche Organisationen am Werk? Zum anderen sei Stuxnet durch seine Entdeckung praktisch wertlos geworden. Auch damit mussten die Urheber rechnen.

Damit sei es wahrscheinlich, dass es sich bei Stuxnet um eine „Ein-Schuss-Waffe“ handelt, die auf ein außerordentlich lohnendes Ziel gerichtet gewesen sei. Langners Fazit: „Ich nehme an, dass der Angriff bereits stattgefunden hat.“

### Kommentar

## Die Utopie wird Wirklichkeit

**Attacke** Ein Computervirus von bisher nicht gekannter Durchschlagskraft alarmiert die Experten – und wirft Fragen zur Sicherheit auch von Atomanlagen auf. Von Klaus Zintz

Die Fachwelt ist sich einig: das Virus namens Stuxnet war hochprofessionell gemacht – und viel zu aufwendig für einen simplen Hackerangriff. Außerdem galt die Attacke nicht irgendwelchen Privatrechnern oder sozialen Netzwerken, sondern sollte offenbar gezielt Industriesysteme lahmlegen. Noch ist völlig ungewiss, wer die Erschaffer von Stuxnet waren – und ob es sich womöglich um eine gezielte Attacke westlicher Geheimdienste handelt, die es speziell auf iranische Atomanlagen abgesehen hatte. Gänzlich aus der Luft gegriffen ist diese Vermutung aber keineswegs.

Klar ist, dass sich mit dem inzwischen entlarvten Virus eine ganz neue Qualität der digitalen Erstschlag ist, wie in der Hackerszene vermutet wird, oder „nur“ ein beson-

ders raffinierter Spionagevirus, sei einmal dahingestellt. Wichtig ist, dass eine so aggressive Cyberwaffe überhaupt entwickelt werden und sich offensichtlich erfolgreich in Industrieanlagen einnisten konnte.

Dies nährt die Befürchtung, dass derartige elektronische Angriffe, die mit einer simplen E-Mail oder einem USB-Stick gestartet werden können, weitaus schwerere Schäden anrichten können als bisher von den meisten Menschen vermutet. Wenn sich Industrieanlagen von solch einem Virus manipulieren lassen, warum nicht auch Kernkraftwerke? Westliche Atommeiler seien sicher, heißt es immer. Aber die Strategie von Terroristen ist bekanntlich, sich neue, bisher nicht gekannte Angriffswege auszudenken. Stuxnet zeigt, wie verheerend eine solche Cyberattacke sein könnte.

Es liegt auf der Hand, dass die Anlagenbetreiber es nicht an die große Glocke hängen, wenn sie Opfer eines solchen Angriffs geworden sind. Auch hier sind die Fahnder also auf Spurensicherung angewiesen. Symantec kam dabei zu interessanten Erkenntnissen. „Wir haben herausgefunden, dass Stuxnet in Indien, Pakistan und am meisten im Iran aufgetreten ist“, erklärt Stefan Wesche. Denkbar sei, dass die Angreifer das Virus gezielt dort einschleusen ließen, zum Beispiel über manipulierte E-Mails an hochrangige Mitarbeiter betroffener Firmen oder V-Männer vor Ort.

Damit liegt der Verdacht nahe, dass eine westliche Nation versucht haben könnte, militärische Ziele im Iran zu sabotieren. Dazu passen unbestätigte Meldungen, dass es Mitte vergangenen Jahres in einer iranischen Urananreicherungsanlage zu Störfällen gekommen sei. Kurze Zeit später trat der Chef der iranischen Atombehörde zurück. Auch Langner tippt auf den Iran als eigentliches Ziel. Auf der Konferenz Applied Control Solutions in Washington führte der Experte Mitte der Woche aus, dass nach seinen Erkenntnissen die Atomanlage in Buschehr am Persischen Golf von Stuxnet infiziert worden sei. Beweise für seine Theorie habe er allerdings nicht.

Doch was, wenn der Fernsteuerungscode unbemerkt in weiteren Anlagen schlummert? Und wie können sich Privatnutzer vor Stuxnet schützen? „Einen Windows-Rechner von dem Schädling zu säubern, ist kein Problem“, sagt Sicherheitsexperte Wesche. „Jeder, der einen vernünftigen Virenschutz hat, dürfte nun davon gefeit sein.“ Die beiden kritischsten Sicherheitslücken seien zudem von Microsoft gestopft worden. Viel schwieriger sei es, den Code aus bereits befallenen Anlagen zu entfernen. Das sei kostspielig und nur von Spezialisten durchzuführen. „Man kann nur hoffen, dass alle Betreiber entsprechende Maßnahmen getroffen haben. Denn falls nicht, sind die möglichen Auswirkungen unvorhersehbar.“

Sind solche Cyberangriffe demnach eine konkrete Bedrohung für die Anlagensicherheit in aller Welt und auch hierzulande? Schließlich waren laut Siemens auch deutsche Anlagen betroffen. „Stuxnet ist ein mit besonders großem Aufwand und Sorgfalt programmierter gezielter Angriff gegen Prozesssteuerungssysteme“, sagt Stefan Ritter, Leiter des Computer Emergency Response Team beim Bundesamt für Sicherheit in der Informationstechnik (BSI). „Diese Systeme werden in vielen Bereichen des täglichen Lebens eingesetzt, von kritischen Infrastrukturen wie Stromversorgung bis hin zur Klimatisierung von Büroräumen.“ Stuxnet sei der erste öffentlich bekannt gewordene Angriff auf Prozesssteuerungssysteme dieser Größenordnung. „Angriffe dieser Dimension waren bislang nur theoretisch denkbar und wurden daher als Restrisiko getragen. Durch das erste Auftreten wird hier eine Neubewertung notwendig.“

Die eigentliche Gefahr gehe jedoch weniger von diesem konkreten Angriff aus, sondern sei abstrakter zu betrachten: „Mit sehr hohem Aufwand und besonderen Kenntnissen, lassen sich auch besonders gut geschützte IT-Systeme angreifen.“ Anders ausgedrückt: niemand kann momentan sagen, wann der nächste Angriff dieser Art stattfinden wird und gegen wen oder was er sich richten wird. Von einem „Cyberkrieg“ mag Ritter dennoch nicht sprechen. „Wir haben es mit einem Angriff auf ein technisches System zu tun. Dies mit militärischen Angriffen in einem Krieg gleichzusetzen, wäre sicher zu weit gegriffen.“

„Das war kein Hacker im elterlichen Keller.“

Ralph Langner, Sicherheitsexperte

## Dem Asthma auf der Spur

**Medizin** Forscher haben unterschiedliche Genvarianten der Krankheit entdeckt und hoffen dadurch auf neue Heilungsmöglichkeiten.

Eine Gruppe von Forschern hat mehrere Genvarianten entdeckt, die mit Asthma in Verbindung stehen und neue Heilungsmöglichkeiten eröffnen könnten. Bei der großangelegten, internationalen Studie stellte sich heraus, dass Asthma bei Kindern und die Form, die Betroffene erst als Erwachsene bekommen, zwei verschiedene Krankheiten sein könnten, erläuterten gestern Wissenschaftler vom Imperial College London. An der Untersuchung wirkten auch Forscher der Ludwig-Maximilians-Universität und des Helmholtz Zentrums in München mit.

Die Ursachen von Asthma sind noch nicht abschließend geklärt. Nach derzeitigem Forschungsstand wird die Atemnot durch eine Kombination aus genetischen und Umwelteinflüssen verursacht. In

Deutschland sind nach Angaben des Helmholtz Zentrums etwa fünf bis zehn Prozent der Bevölkerung an Asthma erkrankt. In den letzten beiden Dekaden sei die Zahl der Asthmapatienten stark angestiegen.

Für die Studie, deren Ergebnisse in der neuesten Ausgabe des „New England Journal of Medicine“ nachzulesen sind, wurden die Gene von 10 000 Kindern und Erwachsenen mit Asthma sowie 16 000 gesunden Menschen untersucht. „Asthma ist eine komplexe Krankheit, in die viele verschiedene Bereiche des Immunsystems mit hineingezogen werden können“, sagte William Cookson vom Imperial College. Die Organisation Asthma UK wies darauf hin, dass Wissenschaftler nun stärker auf die genetischen Vorgaben gerichtet forschen und Therapien entwickeln könnten. dpa

## Fruchtbare Feldhäsinen

**Biologie** Schwanger werden bei bestehender Schwangerschaft – das geht eigentlich nicht. Aber keine Regel ist ohne Ausnahme.

Das Lepus europaeus, der europäische Feldhase, ist weiß man ja schon lange. Und dass es schwangere Häsinen schaffen, gleichzeitig ein weiteres Mal schwanger zu werden, ist auch bekannt. Biologen nennen das Superfetation. Doch wie die Hasen dieses Kunststück fertig bringen, das haben jetzt Forscher am Leibniz-Institut für Zoo- und Wildtierforschung (IZW) herausgefunden – unter Einsatz von Vaterschaftstests und hochauflösender Ultraschallgeräte. Publiziert haben sie ihre Ergebnisse jetzt im Fachjournal „Nature Communications“.

Dabei zeigte sich, dass die Häsinen nicht etwa den Samen speichern, den der Rammler bei einem früheren Liebesakt hinterlassen hat. Vielmehr „bahnen sich die Samenzellen ihren Weg durch die Gebä-

mutter, in der sich noch der vorherige Wurf befindet“, wie es Kathleen Röllig vom IZW formuliert. So werden die Hasendamen noch während ihrer ersten Schwangerschaft befruchtet. Rund vier Tage vor der Geburt entwickelt sich dadurch eine zweite Schwangerschaft.

Die befruchteten Embryonen „warten“ dabei so lange im Eileiter, bis der vorangegangene Wurf geboren ist. Erst danach können sie sich in der Gebärmutter einnisten – allerdings ohne weitere Verzögerung. Somit verringert sich die Tragzeit von 42 auf 38 Tage. Mit dieser Fortpflanzungsstrategie bringen die Häsinen nach Angaben der Forscher bis zu ein Drittel mehr Nachwuchs zur Welt. Die Wissenschaftler halten daher die Superfetation für eine wichtige evolutionäre Anpassung. Zz