19 Hightech-Steganografie

Am 10. Mai 1979 gegen 22 Uhr stieg der 45-jährige Nathan Allen nach Ende seiner Schicht in einem Stahlwerk in Maryland (USA) in sein Auto. Kurz nachdem er den Motor gestartet hatte, explodierte eine im Wagen angebrachte Bombe. Allen starb sofort, sein Beifahrer wurde leicht verletzt.

19.1 Klein aber wichtig: Mikrotaggants

Bei der Aufklärung des Verbrechens tappte die Polizei zunächst im Dunkeln. Doch als ein Sprengstoff-Experte die Tatortspuren unter dem Mikroskop betrachtete, kam Bewegung in den Fall. Ihm fielen winzige Plastikkörner auf, die sich nahezu überall am Tatort nachweisen ließen. Diese Körner bestanden aus Schichten unterschiedlicher Dicke und Farbe. Der Experte wusste sofort: Er war auf so genannte Mikrotaggants (Identifizierungsmarker) gestoßen. Mikrotaggants können Sprengstoff oder anderen Gütern bei der Herstellung zugesetzt werden, um sie identifizierbar zu machen. Jede Schicht eines Mikrotaggants kodiert durch ihre Dicke und Farbe einen Buchstaben oder eine Zahl. Im vorliegenden Fall ergab sich die Zeichenfolge 8DEO2A146.

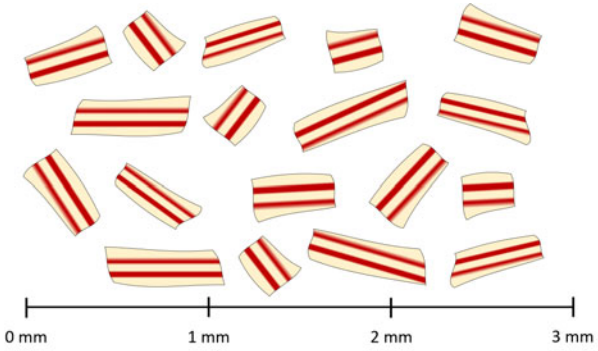

Abb. 78 Mikrotaggants sind mikroskopisch kleine Körner, die aus verschiedenen Schichten bestehen. Die Dicke und die Farbe der Schichten kodieren eine Botschaft.

Anhand der Zeichenfolge 8DEO2A146 stellte der Experte fest, dass es sich um Sprengstoff der Sorte Tovex 220 von DuPont handelte. Beim Hersteller erfuhr die Polizei anschließend, dass die fragliche Charge am 2. Dezember 1978 im Werk Martinsburg (West Virginia) hergestellt worden war. Ein Teil davon ging an den Einzelhändler Lawrence Jenkins, der ebenfalls in Martinsburg ansässig war. Jenkins hatte vorschriftsmäßig die Personalien seiner Kunden notiert. Es zeigte sich: Auf Jenkins' Liste stand auch James McFillin, der Onkel des Mordopfers. Der Rest war kriminalistische Routinearbeit. Schnell wurde klar, dass McFillin ein Motiv, aber kein Alibi hatte. Auf Grund weiterer Beweise wurde er überführt und zu einer lebenslangen Haftstrafe verurteilt.

Die Polizei hatte großes Glück, dass sie im Fall Nathan Allen auf Mikrotaggants gestoßen war, denn eine solche Markierung von Sprengstoffen gab es damals nur in Form eines Pilotversuchs. Nur etwa ein Prozent des auf dem Markt erhältlichen Sprengstoffs enthielt Mikrotaggants. Trotz dieses Fahndungserfolgs haben sich Mikrotaggants in Sprengstoffen nicht durchgesetzt. Nur in der Schweiz sind sie heute vorgeschrieben. In anderen Ländern betrachtet man den Aufwand als zu groß im Vergleich zum Nutzen und verzichtet auf entsprechende Vorschriften (vermutlich hat auch Lobbyismus der Hersteller eine Rolle gespielt).

Es gibt mehrere Hersteller, die Microtaggant-Produkte am Markt anbieten – beispielsweise die Firmen Secutag und Microtrace. Deren Produkte werden nicht nur verwendet, um Sprengstoff zu markieren. Man kann sie auch in Kunststoff, Farbe, Chemikalien, Munition und andere Dinge einbringen. Sie kommen dabei zur Verbrechensaufklärung, zur Verhinderung von Fälschungen und zur Bekämpfung von Produktpiraterie zum Einsatz. Die Hersteller halten sich sehr bedeckt, wenn es um dieses Thema geht – man will Fälscher, Produktpiraten und Attentäter nicht unnötig warnen.

19.2 Steganografie mit Chemie und Physik

Der durch Mikrotaggants aufgeklärte Mord von Maryland zeigt: Mit moderner Technik lassen sich völlig neue Varianten der Steganografie realisieren. Neben der Computertechnik, auf die ich noch in Kapitel 20 eingehen werde, spielen hierbei die Chemie und die Physik eine wichtige Rolle. Bereits im Kalten Krieg war es beispielsweise möglich, Menschen und Gegenstände radioaktiv zu markieren. Unter anderem nutzte die Staatssicherheit (Stasi) in der DDR diese Technik – obwohl sie äußerst gefährlich war.

Eines der Stasi-Opfer war der Schriftsteller Rudolf Bahro[1]. Dieser hatte in konspirativer Arbeit ein kritisches Buch über die damaligen Zustände in der DDR verfasst, das kurz darauf im Westen von einem Verlag veröffentlicht wurde. Zusätzlich wollte er einige Kopien des Buchs in der DDR verteilen, was er einem Freund erzählte. Dummerweise arbeitete dieser als Stasi-Spitzel und verriet Bahros Plan umgehend an seinen Kontaktmann. Die Stasi reagierte prompt. Sie verschaffte sich Zugang zu Bahros Bücherversteck und versetzte die Manuskripte mit einer radioaktiven Substanz. Ansonsten ließ sie den Schriftsteller erst einmal gewähren.

Durch die radioaktive Markierung ließen sich die Bücher bei der Kontrolle der Post leicht ausfindig machen. Die Stasi ließ die Manuskripte unauffällig aussortieren und erfuhr obendrein, wer die geplanten Empfänger waren. Rudolf Bahro, der die verstrahlten Manuskripte eigenhändig verpackt und verschickt hatte, starb 20 Jahre später an Krebs. Ein Zusammenhang ist nicht ausgeschlossen.

Die Stasi nutzte die radioaktive Markierung noch deutlich öfter:

- 1978 übergab die Stasi dem als Spion verdächtigten Physiker Manfred Ludwig eine radioaktiv markierte Akte. Dieser gab sie jedoch vorschriftsgemäß an seinen Chef weiter.
- 1985 markierte die Stasi Geldscheine, um den Diebstahl von Westgeld in einer Postfiliale aufzuklären. Das Ergebnis dieser Aktion ist nicht bekannt.
- 1987 plante die Stasi einen Einsatz gegen Zwillingsschwestern, die beide als Models arbeiteten. Eine der beiden hatte eine Genehmigung zu einer Westreise erhalten. Die Stasi fürchtete, die beiden könnten ihre Identitäten tauschen. Mit einer radioaktiven Lösung markierte ein Stasi-Mitarbeiter ein Kleidungsstück der einen Schwester. Auch hier ist der weitere Lauf der Ereignisse nicht bekannt.

Zum Glück ist die radioaktive Markierung von Gegenständen inzwischen aus der Mode gekommen. Es gibt heute bessere und weniger gefährliche Methoden. So ist es beispielsweise möglich, bestimmte Substanzen auf Molekül-Ebene zu kennzeichnen – mit Hilfe der so genannten Isotopen-Markierung. Als Isotope bezeichnet man in der Chemie Atome, die zwar gleich viele Protonen, aber unterschiedlich viele Neutronen haben. Isotope unterscheiden sich zwar in ihrer Masse, verhalten sich chemisch aber nahezu gleich. Isotope gibt es von nahezu jedem chemischen Element, allerdings sind viele davon nicht

1) Stefan Berg: *Die Spur der Strahlen. http://www.spiegel.de/spiegel/print/d-15985956.html*

stabil. Manche Elemente kommen in der Natur nur als Mischung aus zwei oder mehr Isotopen vor.

Heutzutage ist es möglich, die in einer Substanz vorkommenden Anteile bestimmter Isotope beliebig festzulegen.[2] Hier setzt die Isotopen-Markierung an. Das Verhältnis der jeweiligen Anteile kann man als Code verwenden, der beispielsweise den Hersteller der Substanz identifiziert. Besonders geeignet sind die Elemente Kohlenstoff oder Stickstoff. Die Isotopen-Anteile lassen sich mit Geräten wie einem Massenspektrometer oder einem Gaschromatographen ermitteln.

Nach dem Bombenanschlag von Oklahoma City im Jahr 1995 kam die Isotopen-Markierung erstmals in die öffentliche Diskussion. Anders als im Mordfall Nathan Allen hätte eine Markierung von Sprengstoff – egal ob mit Microtaggants oder mit Isotopen-Markierung – hier nichts gebracht, denn der Attentäter hatte seine Bombe aus Kunstdünger hergestellt. Eine viel diskutierte Frage war daher, ob Kunstdünger per Isotopen-Markierung gekennzeichnet werden sollte. Doch die Hersteller derartiger Produkte hatten kein Interesse an einer solchen Maßnahme und schafften es, entsprechende Pläne zu verhindern.

Eine weitere Technik zur Markierung von Substanzen sind fluoreszierende Taggants. Dabei handelt es sich um fluoreszierende Stoffe, die in kleinen Mengen den entsprechenden Substanzen beigemischt werden. Durch die Leucht-Eigenschaften der Taggants (Wellenlänge, Stärke, Lichtabsorption) lassen sich genug Informationen kodieren, um beispielsweise den Herstellernamen und das Herstellungsjahr festzuhalten.

Eine interessante Anwendung der beschriebenen Techniken ist das Markieren von Medikamenten. Damit kann man gefälschte Medikamente von echten unterscheiden. Interessant sind entsprechende Markierungen auch in der Doping-Bekämpfung. Das Kalkül: Wenn ein Sportler ein gekennzeichnetes Medikament zum Dopen verwendet, lässt sich dies später in einer Blut- oder Urinprobe nachweisen. 2008 erklärte John Fahey, der damalige Präsident der Welt-Anti-Doping-Agentur WADA, beim EPO-Präparat CERA sei bereits eine Markierungstechnik im Einsatz (leider ist nicht bekannt welche).[3] Die entsprechenden Markierungen hätten dazu geführt, dass drei Radprofis bei der Tour de France des Dopings überführt werden konnten. Der Herstel-

2) John P. Jasper, Larry E. Weaner, John M. Hayes: *Process Patent Protection: Characterizing Synthetic Pathways by Stable-Isotopic Measurements*. *http://www.naturesfingerprint.com/pdfs/PharmTechPPP.2007f.pdf*

3) Pharmakonzern dementiert Epo-Markierung, Rasmussen will Geld. *http://www.spiegel.de/sport/sonst/radsport-pharmakonzern-dementiert-epo-markierung-rasmussen-will-geld-a-568221.html*

ler von CERA widersprach dieser Darstellung jedoch. Das Medikament enthalte keine Markierungen, hieß es in einer Stellungnahme.

Der Nürnberger Biochemiker und Anti-Doping-Experte Fritz Sörgel sprach sich derweil generell gegen markierte Medikamente aus: »Man kann nicht wegen vielleicht 200 bis 400 Personen, die in Deutschland EPO zu Dopingzwecken zu sich nehmen, in die Körper von 10.000 bis 15.000 Patienten, die EPO dringend zum Überleben benötigen, Stoffe einführen, die aus medizinischer Sicht nicht gebraucht werden. Keine Arzneimittelbehörde der Welt würde ein Medikament mit diesen Risiken zulassen.«

Ebenfalls in die physikalisch-chemische Trickkiste griff 2015 ein Team von Wissenschaftlern, um ein steganografisches Verfahren zu entwickeln, bei dem wiederum die Fluoreszenz (also die Leuchtkraft) einer flüssigen Substanz eine Rolle spielt.[4] Um das Verfahren anzuwenden, benötigt man eine Flüssigkeit (unter anderem sind Cola, Olivenöl oder Kaffee geeignet) sowie eine Chemikalie (unzählige Metalle und organische Substanzen können verwendet werden). Diese Substanz schüttet man in die Flüssigkeit und misst anschließend deren Fluoreszenz für verschiedene Wellenlängen. So ergibt sich beispielsweise eine Fluoreszenz von 5349 für 500 Nanometer, 4923 für 510 Nanometer, 4801 für 520 Nanometer und so weiter.

Das Interessante daran ist: Führt eine andere Person den gleichen Vorgang mit der gleichen Flüssigkeit und der gleichen Chemikalie durch, dann erhält sie die gleichen Messwerte. Von der Substanz werden nur geringe Mengen benötigt, die sich beispielsweise auf einen Brief aufbringen lassen. Das Verfahren lässt sich laut seinen Erfindern nutzen, um einen kryptografischen Schlüssel zu übertragen. Diesen können Sender und Empfänger dann für die verschlüsselte Kommunikation per Internet verwenden.

19.3 DNA-Steganografie

Die DNA (englische Abkürzung von »Desoxyribonukleinsäure«) ist bekanntlich der Träger der Erbinformation in der Zelle eines Lebewesens. Sie ist in Form einer Doppelhelix aufgebaut. Chemisch besteht sie aus vier verschiedenen Bausteinen, die als A, T, G und C bezeichnet werden. Diese Bausteine bilden lange Ketten, die quasi den Bauplan für ein Lebewesen bilden.

Heutzutage ist es möglich, DNA-Stränge künstlich herzustellen. Es liegt nahe, diese Technik zur Kodierung beliebiger Botschaften zu verwenden. Dies

4) Mark Lorch: *Code-a-cola: Scientists find a way to hide secret messages using FIZZY DRINKS. http://www.dailymail.co.uk/sciencetech/article-3574082/Code-cola-Scientists-way-hide-secret-messages-using-FIZZY-DRINKS.html*

bezeichnet man auch als DNA-Steganografie. In der DNA-Steganografie bietet es sich an, jeden Buchstaben des Alphabets mit Hilfe von drei DNA-Bausteinen zu kodieren, beispielsweise A=CGA, B=ATG, C=GTT, D=TTG, E=GGC und so weiter. Da ein Strang sehr klein ist, werden im Synthetisierungsprozess sehr viele identische Stränge hergestellt. Vor und hinter der eigentlichen Nachricht muss sich im Strang eine bestimmte Bausteinfolge (Primer-Target) finden.

Abb. 79 DNA-Stränge können heute künstlich hergestellt werden. Man kann in ihnen eine Botschaft kodieren.

Einen Sinn hat dieses Kodieren jedoch nur, wenn die entsprechend kodierten DNA-Stränge versteckt werden. Dazu stellt man mit Hilfe von Ultraschall eine Flüssigkeit her, die aus DNA-Bruchstücken besteht, die etwa die gleiche Länge wie die kodierten Stränge haben. Diese verschwinden dadurch in Millionen von anderen Strängen. Die richtigen kann man mit Hilfe des Primer-Targets herausfiltern. Falls man dieses geheim hält, dient es gleichzeitig als Schlüssel, ohne den man kaum eine Chance hat, die Nachricht zu lesen.

Seit den Neunzigerjahren gibt es Forschungen auf dem Gebiet der DNA-Steganografie. Eine 2001 veröffentlichte Arbeit berichtet beispielsweise, wie die Nachricht JUNE6_INVASION:NORMANDY in DNA-Flüssigkeit kodiert wurde. Beim Auslesen der Nachricht mit dem Primer-Target ergab sich JUNE6_INVASION:NORM?Z??. Das Experiment war damit zwar nicht vollständig gelungen, zeigte aber, dass das Verfahren funktionierte.

Inzwischen hat die DNA-Steganografie deutliche Fortschritte gemacht. Mittlerweile sind Produkte auf dem Markt, die es ermöglichen, dass man eine farblose Flüssigkeit mit dem entsprechenden DNA-Code mit einem Pinsel oder einer Sprühdose auf einen Gegenstand aufbringt. Dadurch wird dieser Gegenstand identifizierbar, was beispielsweise gegen Produktpiraterie hilft.

Die entsprechende Flüssigkeit ist nach dem Trocknen nahezu unsichtbar, und es ist schwierig, sie vollständig abzuwaschen. Sofern das Primer-Target geheim gehalten wird, ist die Flüssigkeit kaum zu fälschen.

19.4 Drucker-Steganografie

Im Jahr 2004 veröffentlichte die Zeitschrift *PC World* einen Artikel, der einiges Aufsehen erregte.[5] »Mehrere Drucker-Hersteller«, so hieß es darin, »kodieren die Seriennummer und die Herstellerkennung ihrer Farb-Laserdrucker und Farbkopierer auf jedes Dokument, das sie produzieren.« Durch diese Enthüllung wurde die heute wohl bekannteste Variante der Hightech-Steganografie populär: die Drucker-Steganografie.

Das Prinzip, das die *PC World* beschrieb, funktioniert wie folgt: Bedruckt ein Drucker oder Kopierer ein Stück Papier, dann fügt er winzige Punkte (Durchmesser etwa 0,1 Millimeter) hinzu, die mit bloßem Auge kaum zu erkennen sind. Diese Punkte kodieren eine Botschaft, die neben einer Seriennummer und der Herstellerkennung auch das Datum und die Uhrzeit des Druckvorgangs enthält. Wer den Code kennt, kann bei genauer Betrachtung eines bedruckten Stücks Papier feststellen, welcher Drucker es wann ausgedruckt hat. Dies ist ein Traum für einen Kriminalpolizisten – aber sicherlich nicht für einen Datenschützer.

Abb. 80 Viele Drucker und Kopierer fügen auf jedem Ausdruck winzige Punkte (Durchmesser etwa 0,1 Millimeter) hinzu, die mit bloßem Auge kaum zu erkennen sind.

Man kann die Punkte sichtbar machen, indem man eine Farbseite druckt bzw. fotokopiert und anschließend einen Ausschnitt davon mit einem Scanner mit hoher Auflösung (600 dpi oder mehr) einscannt. Zusätzlich sollte

5) Jason Tuohey: *Government Uses Color Laser Printer Technology to Track Documents*. *http://www.pcworld.com/article/118664/article.html*

man den gelben Farbkanal mit einem Grafikprogramm verstärken. Bei guter Beleuchtung kann auch eine Lupe ausreichen, um die winzigen gelben Punkte zu sehen.

Offensichtlich verwenden die diversen Drucker-Hersteller unterschiedliche Codes. Bei manchen sind die Punkte in Reihen und Spalten angeordnet, bei anderen bilden sie Wolken. Ein entsprechendes Muster nimmt nur wenige Quadratzentimeter in Anspruch und wiederholt sich ständig. Auf einem DIN-A4-Blatt erscheint derselbe Code dadurch etwa 150 Mal. Dadurch kann man den Code auch dann vollständig auslesen, wenn man nur einen kleinen Ausschnitt des bedruckten Blatts zur Verfügung hat.

Neu waren die gelben Punkte nicht mehr, als die *PC World* darüber berichtete. Eingeführt wurde die Technik spätestens Anfang der Neunzigerjahre. Erstaunlicherweise dauerte es bis 2005, ehe die Öffentlichkeit erstmals Notiz davon nahm. Vermutlich wurden die steganografischen Markierungen auf Drängen der NSA oder einer anderen US-Behörde eingeführt. Allerdings gibt es durchaus auch Farb-Laserdrucker, die keine gelben Punkte ausdrucken. Warum das so ist, ist nicht bekannt.

Nur zögerlich äußerten sich die Hersteller zur Drucker-Steganografie. Die Firma Xerox räumte immerhin ein, dass deren Produkte gelbe Punkte produzieren, und gab an, dass diese der Verbrechensbekämpfung dienen. Angeblich kennen die US-Geheimdienste den Code nicht selbst, sondern müssen bei Bedarf eine Anfrage an Xerox stellen, um einen bestimmten Ausdruck dekodieren zu lassen. Und angeblich liefert Xerox die Dekodierung nur in besonders wichtigen Fällen. Auch Hewlett Packard bestätigte die Existenz des Codes, ohne jedoch genauere Angaben zu machen.

Bis heute hat kein Druckerhersteller und keine Behörde irgendwelche Details zu den Markierungs-Codes veröffentlicht. Immerhin gelang es der Bürgerrechtsorganisation Electronic Frontier Foundation (EFF), den Code eines Xerox-Druckers größtenteils zu entschlüsseln (siehe Abb. 81). Demnach geben die gelben Punkte das Datum und die Uhrzeit des Druckvorgangs sowie die Seriennummer des Druckers im Binärformat an. Die EFF kündigte weitere Untersuchungen an und bat darum, Ausdrucke zur Untersuchung einzuschicken. Doch wie es scheint, verloren die Aktivisten der EFF schon bald das Interesse an diesem Forschungsvorhaben. In den letzten Jahren ist nichts wesentlich Neues zu diesem Thema veröffentlicht worden.

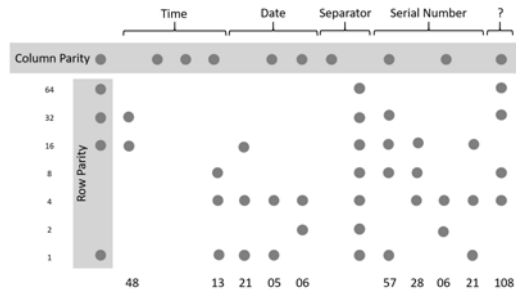

Abb. 81 So funktioniert der Code eines Xerox-Druckers. Das Blatt mit diesem Punktmuster wurde am 21.05.06 um 13:48 von einem Drucker mit der Seriennummer 21062857 ausgedruckt.

Klar ist, dass die kleinen gelben Punkte nach wie vor von vielen (wenn auch nicht allen) Druckermodellen verwendet werden. Allerdings gilt dies nur für Farb-Laserdrucker. Schwarz-Weiß-Drucker (die ohnehin keine gelben Punkte drucken können) sowie Tintenstrahl-Drucker sind nicht betroffen. Es ist durchaus möglich, dass solche Modelle andere Drucker-Markierungstechniken nutzen, ohne dass die Öffentlichkeit darüber Bescheid weiß.

So ist beispielsweise die DNA-Steganografie sehr gut für Tintenstrahl-Drucker geeignet, da man die entsprechende Flüssigkeit in die Tinte einbringen kann. Druckertinte mit Microtaggants, fluoreszierenden Taggants oder Isotopen-Markierung wird längst am Markt angeboten. Der offizielle Zweck dieser Produkte besteht darin, sie für das Drucken von Wertpapieren, Ausweisen und ähnlichen Produkten zu verwenden, um Fälschungen erkennen zu können. Von einer flächendeckenden Verwendung in Druckerpatronen ist bisher nichts bekannt. Darüber hinaus gibt es die Möglichkeit, Botschaften mit Grauabstufungen zu kodieren, was sich für Schwarz-Weiß-Drucker (egal ob Laser oder Tinte) nutzen lässt.

Es versteht sich von selbst, dass entsprechende Markierungen nicht nur für Drucker, Kopierer und Faxgeräte geeignet sind. Auch auf Kugelschreiber, Patronen für Füllfederhalter, Lacke, Textilien, Verpackungen und vieles mehr lässt sich diese Technik anwenden. Inwiefern das gemacht wird, ist nicht bekannt.

19.5 Ungewöhnliche Datenspeicher

Wie kann man größere Datenmengen bei sich tragen, ohne dass es bei einer Leibesvisitation auffällt? Heutige Speichermedien – beispielsweise USB-Sticks – sind teilweise so klein, dass die durchsuchende Person schon sehr genau hinsehen muss, um einen solchen zu finden, wenn er beispielsweise in der Kleidung versteckt ist. Doch es geht noch besser. 2005 zeigten japanische Wissenschaftler, dass man mit Hilfe von Laserstrahlen winzige Markierungen in menschliche Fingernägel brennen kann, die sich zum Speichern von Daten eignen.[6] Die mit bloßem Auge nicht sichtbaren Strukturen werden in drei Schichten angebracht. Etwa 800 Kilobyte lassen sich damit auf einem Fingernagel unterbringen. Nimmt man alle Fingernägel einer Person zusammen, dann reicht das, um ein ganzes Telefonbuch zu kodieren. Die Markierungen halten einige Monate, bevor sie durch das Nachwachsen der Nägel wieder verschwinden.

Leider hat die Fingernagel-Methode einen Nachteil: Das Anfertigen der Datenpunkte per Laser ist recht aufwändig. Gleiches gilt für das Auslesen, das ein Mikroskop erfordert. Noch ist es also nicht möglich, am Computer durch das Klicken von »Speichern unter« mal eben ein Textdokument auf dem Fingernagel abzulegen oder es mit »Öffnen« zu laden. Doch zukünftige Versionen dieser Technologie könnten deutlich praktikabler sein. Die Erfinder denken allerdings weniger an einen USB-Stick-Ersatz als an ein Gerät, das beispielsweise an Grenzübergängen genutzt wird. Ein auf die Fingernägel kodierter Code wäre als Alternative zu biometrischen Merkmalen wie Fingerabdruck oder Gesicht für eine Identifizierung vorstellbar.

Ebenfalls ungewöhnlich ist die Idee, Daten in einer Rolle Klebeband (z. B. Tesafilm) abzuspeichern.[7] Diese Idee präsentierten die Mannheimer Informatiker Steffen Noehte und Matthias Gerspach 1999 auf der Computermesse Cebit. Das Prinzip des Lese- und Schreibvorgangs ähnelt dem einer CD- oder DVD-ROM: Ein 170 Grad heißer Laserstrahl brennt die Informationen als kleine Punkte in die Klebeband-Rolle, die hierbei nicht aufgerollt werden muss. Beim Auslesen der Daten tastet ein Laserstrahl die Oberfläche der einzelnen Lagen wieder ab. Auf diese Weise soll es möglich sein, mehrere Gigabyte an Daten auf eine Klebebandrolle zu brennen.

---

6) *Fingernagel als Datenspeicher. http://www.n-tv.de/mediathek/bilderserien/technik/Fingernagel-als-Datenspeicher-article161470.html*

7) Michael Dreischulte, Markus Wick: *Tesa als Datenspeicher. http://winfwiki.wi-fom.de/index.php/Tesa_als_Datenspeicher*

Ende der Neunzigerjahre wurde die Idee, Klebeband-Rollen als billige und leistungsfähige Speichermedien zu verwenden (tesa-ROM), ernsthaft diskutiert. Eine CD-ROM kostete damals etwa doppelt so viel wie eine Rolle Klebeband, bot jedoch nur etwa 700 Megabyte Speicher. Die tesa-ROM brachte es aber nie zur Marktreife. Dies lag auch daran, dass etwa zur gleichen Zeit neue, billige Speichermedien aufkamen (insbesondere die DVD), wodurch die Klebeband-Speichertechnik an Attraktivität verlor.

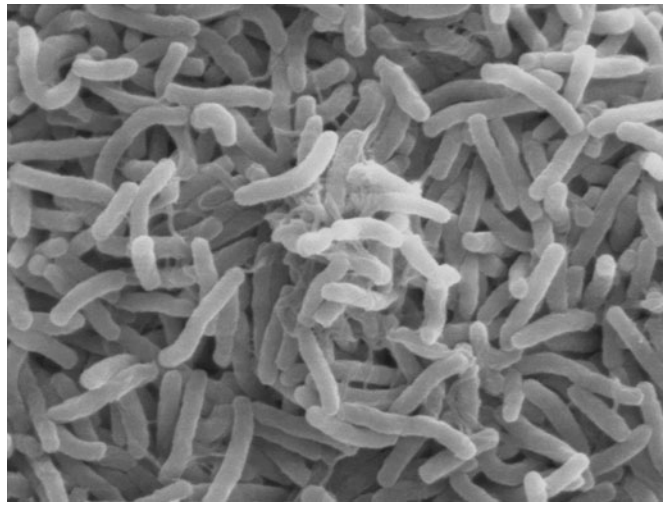

Abb. 82 Selbst Bakterien lassen sich zum Speichern von Daten verwenden – per Gen-Manipulation.

Möglich ist auch das Speichern von Daten in Bakterien.[8] Eine 2011 veröffentlichte Forschungsarbeit zu diesem Thema verspricht wahre Wunderdinge. In einem Gramm Bakterien soll man Tausende von Gigabyte an Daten speichern können. Diese Technologie wird auch als Biostorage bezeichnet. Die Speicherung erfolgt jeweils in der DNA der Bakterien. Anders als bei der DNA-Steganografie wird hier die DNA lebender Objekte manipuliert – es handelt sich also um eine Form der Gen-Manipulation. Dies wird die Marktchancen dieser Technologie sicherlich nicht erhöhen.

8) Darlene Storm: *Unhackable data in a box of bacteria: Future of InfoSec? http://www.computerworld.com/article/2470267/endpoint-security/unhackable-data-in-a-box-of-bacteria--future-of-infosec-.html*