RUHR-UNIVERSITÄT BOCHUM

RUBBITS

INFORMATIONSTECHNISCHE DIENSTLEISTUNGEN AN DER RUHR-UNIVERSITÄT BOCHUM

RUBENS-BEILAGE | Als PDF- Dokument im Internet: http://www.ruhr-uni-bochum.de/RUBbits | NR. 25, MAI 2010

Bilder: istock / Montage: Sponheuer

EDITORIAL

IT-SICHERHEIT IST PFLICHT

Im modernen Universitätsbetrieb ist eine zuverlässig funktionierende IT-Infrastruktur zur Unterstützung der Arbeitsabläufe unerlässlich. Mit Blick auf die E-University werden administrative Aufgaben wie Raum-, Vorlesungs- und Prüfungsplanung, Finanzmanagement, Mitarbeiter- und Studierendenverwaltung virtuell abgebildet, Online-Lern- , Klausur- und Arbeitsplattformen stehen Lehrenden und Lernenden rund um die Uhr zur Verfügung und Forschungsaktivitäten werden international vernetzt. Der Einsatz von IT-Systemen führt dabei zu einer Rationalisierung des Arbeitsaufwands bei gleichzeitig deutlich verbessertem Dienstleistungsangebot.

Anders als in einem Unternehmensnetzwerk muss der Zugang zu einem universitären Datennetz jedoch flexibel und offen gestaltet sein: Das Netzwerk wird von den unterschiedlichsten Benutzergruppen, vor Ort oder Remote mit dienstlichen oder privaten Systemen genutzt. Das oft mangelnde Sicherheitsbewusstsein der Endnutzer macht das breitbandige, offene Datennetz zu einem Ziel lohnender Attacken. Im Intranet der Ruhr-Universität finden sich laufend neue Systeme, die von Viren befallen oder von Angreifern übernommen sind und diesen die Ausführung krimineller Aktivitäten erleichtern. Passwort-Phishing, Bot-Netzwerke, illegale Verkaufsshops sind nur einige der Stichworte in diesem Zusammenhang. Mögliche Folgen sind die Beeinträchtigung der Verfügbarkeit einzelner Dienste oder der IT-Infrastruktur insgesamt, der Verlust vertraulicher Informationen oder auch Schäden, die Dritten zugefügt werden und für die die Universität haften muss.

Im Spannungsfeld zwischen größtmöglicher Handlungsfreiheit für Forschung und Lehre und der unabdingbaren Pflicht, die IT-Infrastruktur mit der gebotenen Sorgfalt zu betreiben, muss nach geeigneten, beiden Seiten gerecht werdenden Lösungen gesucht werden. Jeder Endnutzer kann dabei durch Achtsamkeit und Anwendung geeigneter Grundschutzmaßnahmen zur Sicherung der IT-Infrastruktur insgesamt beitragen.

Die Awarenesskampagne „Sicher gehts besser“ hat die Aufmerksamkeit auf die Problematik der IT-Sicherheit an der Hochschule gelenkt und den Dialog darüber in der Breite angestoßen. Universitätsangehörige aus allen Bereichen haben zahlreich und interessiert an den Veranstaltungen teilgenommen oder sich Online über die Kampagnen-Webseite informiert. Nun gilt es, sich der Verantwortung für die Sicherung der IT an der Hochschule zu stellen und entsprechend zu handeln.

Rektor Prof. Dr. Elmar Weiler

Foto: Pressestelle / RUB

WAS IT-EXPERTEN ZUR VERZWEIFLUNG TREIBT

Der IT-Sicherheitsexperte an sich hat es nicht leicht. Nicht nur, dass er ständig den neuesten Angriffsmethoden und Sicherheitslücken hinterher rennen muss. Nein, insbesondere der Anwender steuert sein Übriges bei. Fröhlich werden Daten im Internet verteilt, Passwörter aus möglichst wenigen Zeichen zusammengestellt und dann auch noch mehrfach verwendet. Aber wirkliche Verzweiflung kommt auf, wenn ein Anwender bewusst Sicherheitsmechanismen umgeht oder ausschaltet „weil er doch nichts zu verbergen hat“!

Diese Aussage ist ein perfektes Beispiel dafür, dass sich noch keine Sicherheitskultur für das Internet, bzw. die digitale Welt entwickelt hat. Natürlich hat der Anwender etwas zu verbergen. Ein unverschlüsseltes WLAN beispielsweise bedeutet, dass ein Angreifer sämtliche unverschlüsselte Kommunikation mitlesen kann. Das Surfverhalten, die übermittelten Daten und die versendeten E-Mails sind sehr wohl schützenswertes Gut. Außerdem muss auch in die andere Richtung gedacht werden: Der Angreifer kann das WLAN auch verwenden, um gefährliche oder illegale Inhalte ins oder aus dem Internet zu laden, und dies fällt auf den WLAN-Betreiber zurück (s. S. 3). Das Ergebnis sind dann z.B. Rentner, die vor Gericht stehen, weil sie Lieder von Bushido heruntergeladen haben, bzw. – eher wahrscheinlich – ihr offenes WLAN von unbekannten Dritten dazu genutzt wurde.

Autoschlüssel rückt keiner raus

Ähnliche Beispiele lassen sich überall in der digitalen Welt finden. Ein Passwort ist ähnlich wichtig wie ein Wohnungsschlüssel in der realen Welt. Ihre Schlüssel geben wohl die wenigsten in fremde Hände. Auch die PIN – nichts Anderes als ein (sehr kurzes) Passwort – ihrer EC-Karte geben die wenigsten heraus. Anders bei Passwörtern: Vor ein paar Monaten sind wir – mit Radiomoderator und versteckten Mikrofon – als vermeintliche Mitarbeiter des Instituts für die deutsche Sprache durch eine Fußgängerzone gelaufen und haben Passwörter gesammelt. Grund sei die Überprüfung der These, dass Passwörter unsere schöne Sprache kaputt machen, weil hier ja keine normalen Wörter mehr verwendet werden dürfen. Die Folge war erneut ein verzweifelnder Sicherheitsexperte, denn von über 90% der angesprochenen Passanten haben ein oder mehrere Passworte genannt und teilweise auch noch die zugehörigen Dienste. Noch bedenklicher war, dass für das angeblich dazugehörige Gewinnspiel einige Passanten zusätzlich bereit waren, ihre Adressdaten beizusteuern.

Bezeichnend war die Gegenprobe, bei der wir als ADAC-Tester versucht haben den Passanten für einen angeblichen Sicherheitstest kurz den Autoschlüssel zu entlocken – klares Ergebnis: Den Autoschlüssel rückt der gute Bürger nicht mal eben so raus. Dieses Selbstverständnis, diese Kultur muss sich auch für die digitalen Dienste durchsetzen.

Handys sind kleine Computer

Eine echte Herausforderung in der digitalen Welt ist das extreme Tempo, in dem neue Entwicklungen auf den Markt kommen. Ein Beispiel sind mobile Geräte wie Handys. Die sind zum Glück von Natur aus sicher – jedenfalls muss man das glauben, wenn man den Anwendern zuschaut. Das Problem: Viele aktuelle Handys sind kleine Computer, erfüllen schon heute viele Funktionen von Desktop-PCs und besitzen mittlerweile ein ähnliches Gefahrenpotential. So erlauben Trojanische Pferde, das Telefon als Wanze zu benutzen, Gespräche abzuhören, SMS zu lesen und das Handy zu orten.

In der Wirtschaftsspionage sind solche Möglichkeiten wohl genauso gern gesehen wie in Beziehungsfragen. So wirbt ein Trojaner mit dem Werbespruch: „Dank FlexiSPY habe ich letztendlich entdeckt, dass meine Frau mich mit meinem Bruder betrog. Ich hatte schon mehr als ein Jahr ein schlechtes Gefühl dabei. Seit der Scheidung ist mein Leben so viel besser. Danke FlexiSPY! Ich bin wieder frei!“. Hier soll noch einmal darauf hingewiesen werden, dass der versteckte Einsatz in beiden Fällen strafbar ist.

Es ist klar, dass sich eine Sicherheitskultur wie in der realen Welt noch nicht in der digitalen durchgesetzt haben kann. In der realen Welt lernen wir von Kindesbeinen an, was wir beachten müssen und wie gefährlich welche Situationen sind: Die Haustür wird abgeschlossen und der Gurt angelegt!

Um uns, unsere Kinder und unsere Werte zu schützen, ist es notwendig, dass wir uns mit den aktuelle Technologien und Möglichkeiten des Internets auseinander setzen und besonnen damit umgehen. Um die Sicherheitskultur zu fördern, gibt es inzwischen viele Webseiten und Hilfen, um sich zu informieren, damit Sicherheitsexperten nicht mehr verzweifeln.

Wir plädieren also: Habt ein Herz für IT-Sicherheitsexperten und haltet Euch an die wichtigsten Regeln im digitalen Leben!

Marian Jungbauer, Markus Linnemann

DIE AUTOREN

Marian Jungbauer und Markus Linnemann arbeiten im Institut für IT-Sicherheit der Fachhochschule Gelsenkirchen. Markus Linnemann ist Mit-Autor des Buchs „Sicher im Internet – Tipps und Tricks für das digitale Leben“, Infos: s. Linkslage.

Die Nutzung fremder Werke in Lehrmaterialien

WAS DARF ICH KOPIEREN?

In Lehrmaterialien an der Universität werden häufig Werke anderer Autoren zur Veranschaulichung eingebunden. Um etwaige Urheberrechte an den genutzten Werken zu wahren, gelten einige Grundregeln.

Zuerst ist zu klären, ob verwendetes Material urheberrechtlich geschützt ist. Das sind Werke der Literatur, Wissenschaft und Kunst, in denen sich ein verkörperter geistiger Inhalt sowie die Individualität des Urhebers ausdrücken. Erfasst sind z.B. Sprachwerke (etwa Monografien, wissenschaftliche Buchausgaben, Lexikonartikel), Musikwerke (ggf. auch kurze Tonfolgen), Werke der bildenden Künste, Lichtbild- und Filmwerke, Darstellungen wissenschaftlicher oder technischer Art, unter Umständen auch Kartenmaterial, Sammelwerke, Datenbanken oder Multimediawerke. Sie sind in der Regel bis 70 Jahre nach dem Tod des Urhebers geschützt. Frei nutzbar sind hingegen amtliche Werke, z.B. Gesetze, amtliche Bekanntmachungen oder Gerichtsentscheidungen – aber Sammlungen oder Bearbeitungen solcher Werke können wiederum geschützt sein.

Da die Rechte zur Nutzung eines geschützten Werkes (etwa durch Vervielfältigung, Verbreitung – einschließlich Weitergabe an andere, öffentliches Zugänglichmachen, z.B. in einer Lehrveranstaltung – oder durch Veröffentlichung von Umgestaltungen) primär dem Urheber zustehen, sind derartige Nutzungen des Werkes durch andere nur mit Erlaubnis des Urhebers oder kraft Gesetzes zulässig.

Faustregel: Weniger als 10%

Unproblematisch ist also die (evtl. entgeltliche) Verwendung eines geschützten Werkes mit Einverständnis des Urhebers. Dieses kann sich ggf. aus Indizien, wie z.B. der Bereitstellung zum Download, ergeben; allein das Einstellen eines Werkes in das Internet bedeutet aber noch nicht, dass der Urheber in alle technisch realisierbaren Nutzungsarten eingewilligt hat.

Von den gesetzlichen Erlaubnissen zur Nutzung geschützter Werke spielt für die Lehre vor allem das Recht der öffentlichen Zugänglichmachung nach § 52a UrhG eine Rolle: Zulässig ist es, veröffentlichte kleine Teile eines Werkes (Faustregel: weniger als 10 % des Gesamtumfangs), Werke geringen Umfangs sowie einzelne Zeitungs- oder Zeitschriftenbeiträge im Unterricht einem bestimmt abgegrenzten Kreis von Unterrichtsteilnehmern öffentlich zugänglich zu machen (und dafür zu vervielfältigen), soweit dies zu dem jeweiligen Zweck geboten und zur Verfolgung nicht kommerzieller Zwecke gerechtfertigt ist; die Quelle ist anzugeben. Viele Einzelheiten sind allerdings umstritten, z.B. ob das Zugänglichmachen zur Vor- und Nachbereitung eingeschlossen ist, wie der Teilnehmerkreis abzugrenzen ist (im Internet ist mindestens ein Passwortschutz erforderlich) und wie sich die Beschränkung auf nichtkommerzielle Zwecke etwa auf kostenpflichtige Weiterbildungsstudiengänge auswirkt.

Besser verlinken

Zusätzliche Einschränkungen gelten bei Werken für den Unterrichtsgebrauch an Schulen und bei Filmen. Dagegen dürfen einzelne Zeitungsartikel und Rundfunkkommentare, die politische, wirtschaftliche oder religiöse Tagesfragen betreffen und nicht mit einem Vorbehalt der Rechte versehen sind, sowie vermischte Nachrichten tatsächlichen Inhalts und Tagesneuigkeiten, die durch Presse oder Funk veröffentlicht worden sind, in der Regel vervielfältigt, verbreitet und öffentlich wiedergegeben werden. Der sicherste (wenn auch urheberrechtlich nicht ganz bedenkenfreie) Weg bei der Heranziehung fremder Online-Inhalte zu Lehrzwecken ist, sie nicht in die eigenen Lehrmaterialien einzubinden, sondern einen Link auf die entsprechende Internetseite zu setzen. Dieser sollte sich in einem neuen Fenster (in dem die geschützten Inhalte legal angeboten werden) öffnen; Frame- oder Inline-Links auf urheberrechtlich geschützte Inhalte sind unzulässig. Schließlich dürfen – soweit erforderlich – Vervielfältigungsstücke von kleinen Werkteilen, Werken geringen Umfangs oder einzelnen Zeitungs- oder Zeitschriftenbeiträgen (nicht aber von Werken speziell für den Unterrichtsgebrauch an Schulen) zu Prüfungszwecken hergestellt werden.

Insgesamt sind viele Einzelheiten rechtlich noch nicht abschließend geklärt. Als „Faustregel“ lässt sich aber festhalten, dass die urheberrechtlichen Restriktionen strenger sind als angesichts der heutigen technischen Möglichkeiten vielfach angenommen wird. *Prof. Dr. Renate Schaub*

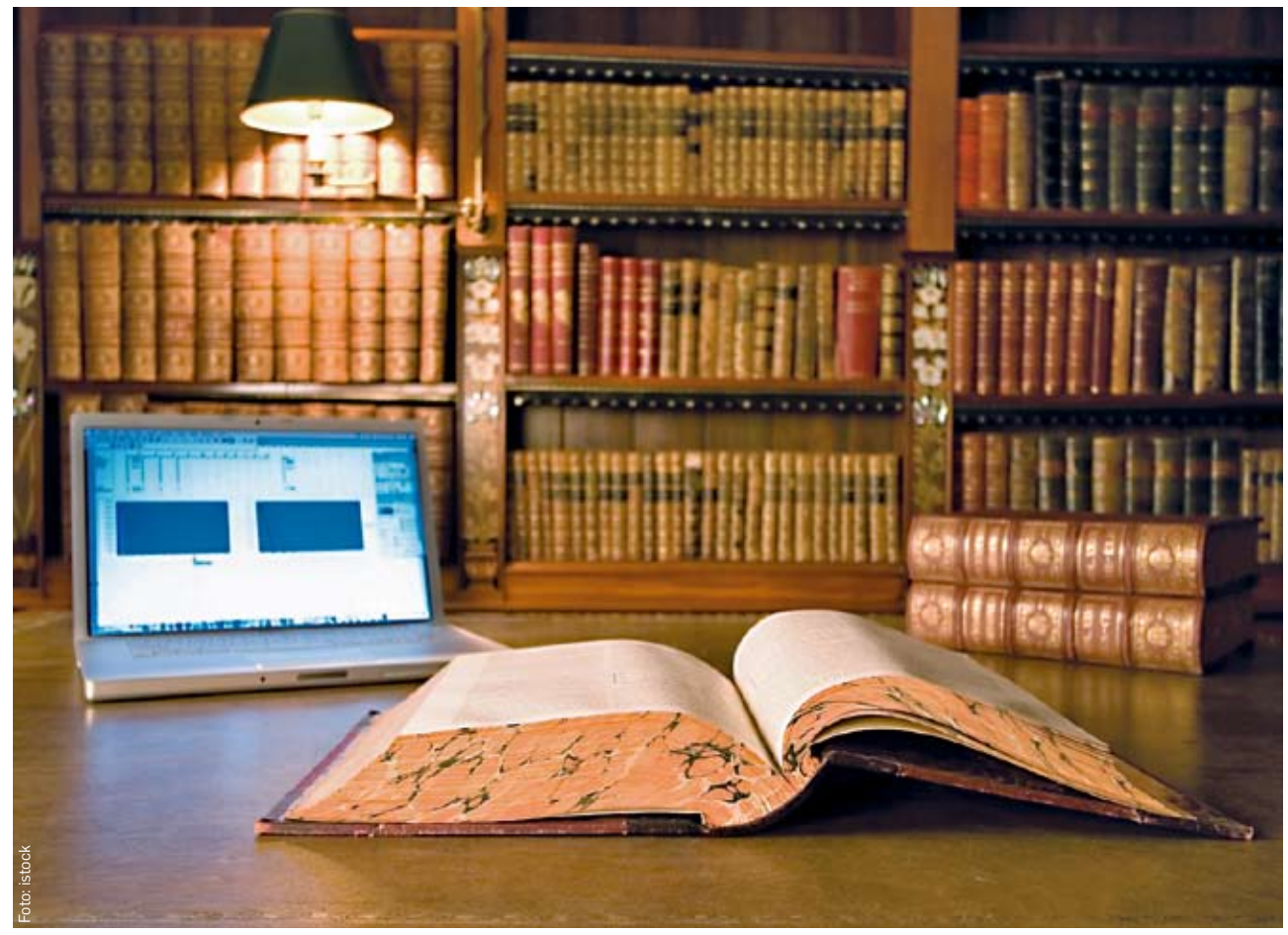


Foto: istock

DIE AUTORIN

Prof. Dr. Renate Schaub ist Inhaberin des Lehrstuhls für Bürgerliches Recht, Internationales Privatrecht und Rechtsvergleichung, Handels- und Wirtschaftsrecht der Ruhr-Universität.

LINKSLAGE

NÄHERE INFOS ZU DEN ARTIKELN IM WEB

Informationen zur IT-Sicherheit:
http://itsb.rub.de

Arbeitsgruppe Urheberrecht der UAMR
http://urheberrecht.uamr.de/

Institut für IT-Sicherheit der Fachhochschule Gelsenkirchen
http://www.internet-sicherheit.de/

Buch „Sicher im Internet“
http://www.internet-sicherheit.de/buch-sicher-im-internet/

Webseite von Prof. Dr. Hendrik Speck
http://www.hendrikspeck.com/

Lehrstuhl Prof. Schaub
http://www.ruhr-uni-bochum.de/ipr/

Arbeitsgruppe Identitätsschutz im Internet ai3
https://www.a-i3.org/

Auftritt von Tobias Schrödel zum Auftakt der IT-Awareness-Kampagne
http://sicher-gehts-besser.rub.de/v1.html

Aktuelle und historische Bücher über Kryptographie
http://www.sichere.it

Details zur Vigenère Verschlüsselung und den Methoden sie zu knacken
http://www.sichere.it/vigenere.php

Details zur Playfair Chiffre
http://www.sichere.it/playfair.php

Dienstanweisung „Geheimschrift innerhalb des Heeres
http://www.sichere.it/crypto_book_detail.php?bookid=308

Software CrypTool
http://www.cryptool.org

Gastkommentar

VON RUDERBOOTEN UND MEHR MERKWÜRDIGKEITEN

Die griechische Mythologie überliefert die Legende des Ruderschiffs von Theseus, mit dem er nach Kreta gefahren war, um die athenischen Geiseln aus dem Labyrinth des Minotaurus zu retten. Aus Dankbarkeit wurde das Schiff alljährlich von den Athenern für Prozessionen zur Insel Delos genutzt. Um das Schiff fast tausend Jahre lang zu erhalten, wurden verrottete Planken durch neue ersetzt. Mit jedem Jahr erhöhte sich der Anteil des Neuen am so konservierten Boot.

Das Schiff beschreibt die Abhängigkeit des Originalen oder der Identität, von Zeit, Weiterentwicklung und Veränderung. Schon Plutarch berichtet von philosophischen Diskussionen: Für die einen blieb das Schiff immer dasselbe, für die anderen verlor es seinen originären Charakter und wurde etwas Neues.

Die Veränderungen unserer Lebens- und Arbeitswelten haben, verbunden mit dem mediendemografischen Wandel, längst ihre Spuren in unserem Medienkonsum, aber auch in unserem Selbstverständnis, unserer Vorstellung von Privatsphäre und Öffentlichkeit hinterlassen. Für Zeitungen und Zeitschriften wird auch im Lande der Dichter und Denker in wenigen Jahren keine Druckerpresse mehr angeworfen. Für jüngere Generationen existiert das Wort Bibliothek nur noch als Rechtschreibrätsel. Ihre Musikvorlieben genießen sie unter dem mobilen Soundschirmchen ihrer MP3-Player und Mobiltelefone, den Verlust von Moderatoren, Stimmen und Stimmungen als übergreifender Klammer gesellschaftlicher Normenvermittelung kompensieren sie durch automatisierte Konsumempfehlungen.

Parallelwelt entsteht

Ein solcher Wandel muss nichts Schlechtes bedeuten: Mobiltelefone erhöhten die Erreichbarkeit, E-Mails sind schneller als die Serviceangebote der Post, Informationen sind unmittelbar zugänglich, das Internet schafft neue Varianten der Meinungsäußerung und eröffnet breiten Bevölkerungsschichten neue Zugänge. Die Verlagerung hin zur Dienstleistungsgesellschaft, der zunehmende Einsatz computervermittelter Angebote für Unterhaltung, Information und Kommunikation hinterlassen ihre Spuren in den von der Verwertungsindustrie zur Verfügung gestellten Datenabwurfplätzen. Eingefangen und profiliert beteiligt sich der Nutzer gerne an den vermeintlich sozialen Netzwerken, pflegt seine Kontakte, archiviert seine Fotos, kommentiert die Selbstdarstellungen anderer, nimmt am Aufmerksamkeitswettbewerb teil, überträgt seine Nutzungsrechte an die jeweiligen Plattformen und genießt die auf sein Profil zugeschnittene Werbung.

Handy telefoniert nach Hause

Unsere Identität verhält sich dabei ähnlich wie das Schiff des Theseus. Mit jeder Webseite, die uns mit einem Cookie entgegen lächelt; jedem Werbebanner, welches wir aus Versehen bestaunen; jeder Gruppe, der wir digital beitreten; jedem „Freund”, den wir auf Facebook erhören; jeder E-Mail die wir auf Gmail beantworten; jedem verlinkten Gesicht im Gruppenbild, jeder Nachricht im Gästebuch verraten wir mehr über uns, und wir können uns sicher sein: Unsere digitalen Zerrbilder lächeln zurück.

Mit ihrem enzyklopädischen Anspruch wächst die Bedeutung dieser aus Informationshäppchen konstruierten Modelle der Identitäten und Aufmerksamkeiten aus der reinen Datenebene hinaus. Steuernummern, Einkommensregister, Verkehrszentralregister, Versicherungsrankings, Krediturteile, Soziale Netzwerke und Personensuchmaschinen, sie alle lösen die Datenhoheit aus den Händen der Erfassten und schaffen durch ihre Aggregation auf Verlinkungen und Assoziationen beruhende Identitätsmodelle und Parallelwelten.

Nutzer können dabei die Kontrolle verlieren: Die informationelle Selbstbestimmung des Einzelnen wird erschwert, wenn Identitätsbildung zunehmend fremdgesteuert und dezentral stattfindet. Verzeihen oder Vergeben, die Möglichkeit einer zweiten Chance erscheinen obsolet, wenn eine zweite Festplatte billiger ist als ein Löschverfahren, viel preiswerter jedenfalls als Datensparsamkeit, Datensicherheit, Verfallsdatum, Korrektheit oder Relevanz.

Die individuelle und gesellschaftliche Teilhabe am Digitalen, die Verwertungsbestrebungen des Sozialen sowie Nutzer mir ihrer Mischung aus Naivität, Zukunftsvertrauen und Medieninkompetenz schaffen für die Identitätsbildung ein spannendes Ereignisfeld, in dem nicht sicher ist, welche Auswirkungen die Verschiebungen von Datenschutz und Privatsphäre haben werden.

Wenn mobile Endgeräte die Bewegungsprofile der Nutzer nach Hause telefonieren, wenn auf ihnen der Schwerpunkt der sozialen Interaktion stattfindet, wenn sie Rechner, Medienplattform, Kamera und Adressbuch in sich vereinen, dann gewinnen Stimmen an Bedeutung, die fragen, ob eine darauf basierende Profilierung zur Auflösung des selbstbestimmten Individuums führen kann, ob die Grenzflächen zwischen Privatsphäre und Öffentlichkeit verschwinden, ob sich Identität zum Referenzmodell entwickelt, was passiert, wenn mehr und mehr „Planken” unseres Selbst durch Andere bestimmt werden, wenn der Kern des Individuellen, des Einzigartigen, Privaten und Intimen verschwindet und dem nicht mehr als Gegenpol entgegengehalten werden kann.

Kein Gegenpol zum neuen Selbst

Die technische Evolution erscheint irreversibel: Jugendliche zur Datensparsamkeit aufzurufen, ist wie Eulen nach Athen tragen. Plattformbetreiber unterliegen einem zunehmenden Verwertungs- und Verdrängungswettbewerb, aber auch die Jahrzehnte alten Schutzzäune der Datenschutzgesetze rotten langsam vor sich hin und verbleiben auf diesem Auge systemblind. Ihr Fokus ist immer noch mehrheitlich auf das Bedrohungsszenario des Big Brother ausgerichtet, die mittlerweile viel umfangreicheren Datensammlungen der unzähligen kleinen Schwestern werden bestenfalls peripher wahrgenommen. Eine Veränderung ist nicht in Sicht: Von politischer Seite ist eine konsequente Weiterentwicklung zukünftiger Leitmedien nicht erkennbar, ein Verständnis für die komplexen Herausforderungen zukünftiger Technologien nicht zu erwarten.

Theseus konnte noch auf den Faden der Ariadne zurückgreifen. Auf ein solches Navigationssystem brauchen wir nicht zu hoffen. Von deutschen Politikern kommen im besten Fall Zensurgesetze.

Die gesellschaftlichen und individuellen Navigationssysteme taugen nur noch zur Baustellenumfahrung, ohne Medienkompetenz werden die Wandlungsprozesse sicher spannend verlaufen. *Prof. Dr. Hendrik Speck*

DER AUTOR

Prof. Dr. Hendrik Speck ist Inhaber des Lehrstuhls für Informatik und Mikrosystemtechnik an der Fachhochschule Kaiserslautern.

Jeder verantwortet seinen Internetanschluss

HAFTUNG FÜR FREMDE TATEN

Das Internet kann leicht zur Haftungsfalle werden. Wer unachtsam ist, kann Opfer von Betrug oder unseriösen Geschäftspraktiken werden. Und mehr: Unter Umständen ist er auch noch für die Taten Anderer verantwortlich.

Verfügbarkeit, Anonymität, Rechtsverletzungen im Netz

Das Internet schafft eine einzigartige Sichtbarkeit und Verfügbarkeit von Information. Zugleich ist es angenehm anonym: „On the Internet noboby knows you‘ re dog“ – dieses Motto aus der Anfangszeit des Web bestimmt unser Verhalten im Netz.

Das World Wide Web ist Instrument für zahllose Verletzungen von Marken, Urheber- und Persönlichkeitsrechten. Es ist verständlich und legitim, dass die Inhaber von Schutzrechten, etwa die Musik- und Filmindustrie, dies nicht hinnehmen wollen. Jedoch sind die Rechtsverletzter meist nicht bekannt. Bekannt sind nur die IP-Adresse und der dahinterstehende Internetanschluss, über die die Rechtsverletzung erfolgte. Folglich können sich die Rechteinhaber an den Inhaber des Internetanschlusses halten.

Verantwortlichkeit für Kommunikationsräume

Die Nutzung des Internet entwickelte sich stark über Kommunikationsräume, die die Interaktion der Nutzer bündeln. Konkret sind dies Handelsplattformen wie eBay, soziale Netzwerke sowie Foren, Blogs etc. Diese Kommunikationsräume sind Gegenstand massiver Rechtsverletzungen. So wurden etwa Handelsplattformen zum Vertrieb von Plagiaten genutzt.

Das deutsche Recht enthält in hohem Maße Schutzpflichten, die Regelverstöße durch andere Personen verhindern sollen. „Eltern haften für ihre Kinder!“ – Dieser Grundsatz bezeichnet – missverständlich, aber plakativ – die Pflicht von Eltern, Dritte vor Regelverstößen durch ihre Kinder zu bewahren. Entsprechend haben Eigentümer von Sachen und Betreiber von Unternehmen die Pflicht, dafür zu sorgen, dass hiervon keine Gefahren für Dritte ausgehen.

Nach diesen Grundsätzen sind die Betreiber von Handelsplattformen verpflichtet, Rechtsverletzungen durch ihre Nutzer zu unterbinden, soweit möglich und zumutbar. Dasselbe gilt für Anbieter sonstiger Dienste. Diensteanbieter ist jeder, der einen Kommunikationsraum betreibt. Dazu gehören auch Foren oder Blogs, unabhängig von der Größe. Jeder Anbieter, und das kann im Web 2.0 fast jeder sein, hat also Schutzpflichten zugunsten Dritter.

Verantwortlichkeit für den Internetanschluss

Auch ein bloßer Internetanschluss ist schon eine Gefahrenquelle, die Schutzpflichten auslöst, da er für Rechtsverletzungen genutzt werden kann. Der Anschlussinhaber hat die Gefahr durch das Betreiben des Anschlusses geschaffen und kann sie kontrollieren. Folglich hat auch er Schutzpflichten zu erfüllen.

Diese betreffen etwa die Sicherung eines WLAN. Hier gilt: Ein privates WLAN muss grundsätzlich durch Passwort gegen den Zugriff unbefugter Dritter geschützt werden. Wer ein offenes WLAN betreibt, verletzt diese Pflicht und haftet auf Unterlassung, unter Umständen auch auf Schadensersatz.

Eine andere Fallgruppe, die auch bei geschützten WLAN eine Rolle spielt, betrifft die Verantwortlichkeit für Familienangehörige. Urheberrechtsverletzungen über Musiktauschbörsen werden häufig durch Kinder des Anschlussinhabers begangen. Bei Minderjährigen wird der Anschlussinhaber von den Gerichten häufig wegen unzureichender Beaufsichtigung der Kinder in Anspruch genommen. Hier verlangen die Gerichte teilweise eine Kontrolle der Internetnutzung. Andere Gerichte lehnen dies – zu Recht – ab, da die eigenständige Nutzung des Internet zur Entwicklung von Heranwachsenden gehört, und verlangen eine Kontrolle nur, wenn es zuvor schon Rechtsverletzungen gab. Bei volljährigen Kindern sind die Anforderungen an die Beaufsichtigung wesentlich geringer.

Wenn das Familienmitglied, das die Musiktauschbörse genutzt hat, bekannt ist, kann es vom Rechteinhaber selbständig in Anspruch genommen werden. Dies gilt auch bei Jugendlichen. Das LG Hamburg beispielsweise verurteilte einen 15-jährigen Schüler.

Wenn nicht bekannt ist, welches Familienmitglied die Rechtsverletzung begangen hat, bejahen einige Gerichte pauschal eine Schutzpflichtverletzung des Anschlussinhabers. Dies überzeugt nicht. Es muss eine konkrete Pflichtverletzung des Anschlussinhabers nachgewiesen werden.

Der Anschlussinhabers hat folgende Maßnahmen zu ergreifen: Er muss sein WLAN sichern, er muss alle Personen, die Zugriff auf das WLAN haben, hinsichtlich des Unterlassens von Rechtsverletzungen instruieren und er muss notfalls die Nutzung des Internets beaufsichtigen und Personen davon ausschließen.

Im Zusammenhang mit Urheberrechtsverletzungen durch Musiktauschbörsen hat sich als Geschäftsmodell von Anwälten die Abmahnung an Tauschbörsen etabliert. Die bekannten Musiktauschbörsen werden mit speziellen Programmen überwacht, die die IP-Adressen der Nutzer und der Umfang der Nutzung protokollieren. Anschließend wird der Inhaber des Internetanschlusses ermittelt und auf Unterlassen sowie Schadensersatz in Anspruch genommen. Meist werden Abmahngebühren und hoher Schadensersatz gefordert und ein Vergleich in Höhe von einigen tausend Euro angeboten.

Hier gilt Folgendes: Ein Anspruch auf Schadensersatz setzt Verschulden voraus, wofür der Anspruchsinhaber beweispflichtig ist. Dazu muss eine konkrete Pflichtverletzung bewiesen werden. Wenn unklar ist, wer den Anschluss nutzte, wird dies nicht in jedem Fall gelingen.

Praxis von Urheberrechtsverletzungen

Der Gesetzgeber hat die Höhe der Abmahnkosten beschränkt. Nach § 97a II UrhG sind die Abmahnkosten auf 100,- EUR begrenzt, wenn es sich um eine erstmalige Abmahnung in einfach gelagerten Fällen mit einer unerheblichen Rechtsverletzung im privaten Bereich handelt. Wann eine unerhebliche Rechtsverletzung vorliegt, ist sehr umstritten. Die Gerichte nehmen eine nicht unerhebliche Rechtsverletzung etwa an, wenn mehr als 1.000 Musikstücke betroffen sind. Die Rechtslage bei Verletzung von Urheberrechten im Internet ist komplex und im steten Fluss. Wer wegen Urheberrechtsverletzung auf höhere Beträge in Anspruch genommen wird, sollte daher Rat bei einem spezialisierten Rechtswalt suchen. *Prof. Dr. Georg Borges*

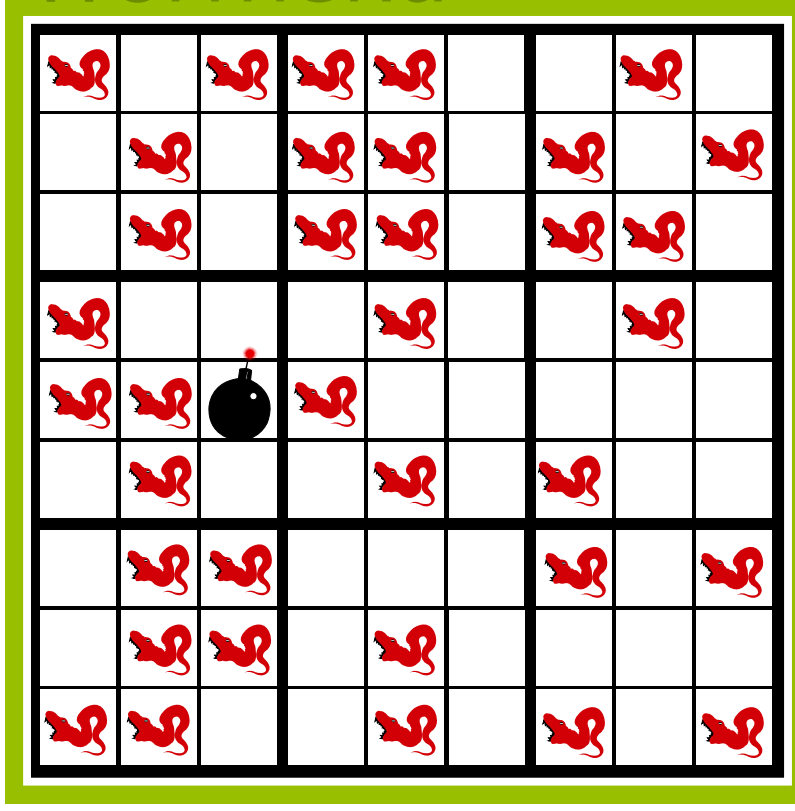
Foto: istock

DER AUTOR

Prof. Dr. Georg Borges ist Inhaber des Lehrstuhls Bürgerl. Recht, deutsches und internat. Handels- und Wirtschaftsrecht, insbes. Recht der Medien und der Informationstechnologie an der RUB und Sprecher des Vorstands der AG „Identitätsschutz im Internet“ ai3.

RÄTSELSPASS

Wormoku



Schon wieder hat ein Wurm Ihr System befallen. Sie können ihn stoppen, indem Sie in jeder Reihe, in jeder Spalte und in jeden der insgesamt neun 3x3 Blöcke genau ein (1!) Anti-Virus-Tool (Bombe) zeichnen. Ein Tool ist bereits vorgegeben. Es gibt nur (1!) Lösung.

§ RECHTSLAGE

FILME AUF KINO.TO & CO.

Das Herunterladen von Filmen aus Tauschbörsen ist rechtswidrig. Als Alternative bieten sich kino.to und andere Dienste an, die den Genuss des Films über Streaming vermitteln.

Streaming bezeichnet die Wiedergabe einer Audio- oder Videodatei direkt aus dem Internet, die ohne den vorherigen Download auf die Festplatte des Nutzers auskommt. Bei kino.to und ähnlichen Diensten handelt es sich um ein On-Demand-Streaming, bei dem die Wiedergabe bereitgehaltener Dateien auf Abruf erfolgt. Das Anbieten eines solchen Streams ist rechtswidrig.

Umstritten ist aber, ob das bloße Ansehen eines Streams, etwa eines aktuellen Kinofilms, urheberrechtlich zulässig ist. Beim Streaming werden keine Daten dauerhaft auf der Festplatte des Nutzers gespeichert. Jedoch wird eine Kopie des Werks im Arbeitsspeicher abgelegt. Darin liegt schon eine Vervielfältigung gemäß § 16 UrhG, die nur zulässig ist, wenn sie durch Gesetz erlaubt ist. Private Kopien von Werken sind zulässig (§ 53 I UrhG), es sei denn, die Vorlage ist offensichtlich rechtswidrig. Genau dies ist bei Streaming-Angeboten zu aktuellen Kinofilmen aber regelmäßig der Fall.

Eine Vervielfältigung von Daten im Arbeitsspeicher ist flüchtig und kann daher gerechtfertigt sein (§ 44a UrhG). Dies setzt jedoch voraus, dass die Speicherung eine erlaubte Werknutzung ermöglichen soll (§ 44a Nr. 2 UrhG). Entgegen einer in der Literatur vertretenen Ansicht ist dies der Fall. Das Urheberrechtsgesetz verbietet nicht den bloßen Werkgenuss, also das Ansehen oder -hören eines Werkes. Folglich ermöglicht eine temporäre Vervielfältigung eine rechtmäßige Nutzung, wenn sie nur dazu dient, eine bloße Werkrezeption zu ermöglichen.

Im Ergebnis ist also die Nutzung von Streaming-Angeboten urheberrechtlich zulässig.

Prof. Dr. Georg Borges

Drei Anekdoten der historischen Kryptographie

IDEENKLAU UND DEUTSCHES LIEDGUT

Die Geschichte der Kryptographie ist eine Geschichte voller Missverständnisse. Dem einen gelingt ein Durchbruch nach Jahrhunderten, keiner merkt es und dann war doch schon einer schneller. Ein anderer erfindet eine fast virtuos anmutende Verschlüsselung, zeigt sie einem Freund und prompt wird sie nach diesem benannt. Und wieder andere zeigen, dass sogar Minister lernfähig sind, wenn auch auf Raten und ohne Erfolg. Drei Anekdoten zur Verschlüsselung von Tobias Schrödel.

VIGENÈRE UND KASISKI

Als um 1540 Blaise de Vigenère nach Vorarbeit von Porta die nach ihm benannte Verschlüsselungsmethode beschrieb, dachte er an eine sichere Geheimschrift, die bis in alle Ewigkeit halten würde. Freilich ist eine Ewigkeit im ebenfalls ewigen Wettstreit der Kryptographen mit den Kryptoanalytikern ein hohes Ziel. Nichtsdestotrotz sollte die Vigenère-Verschlüsselung so lange als sicher gelten, wie keine andere zuvor und bis heute auch keine danach.

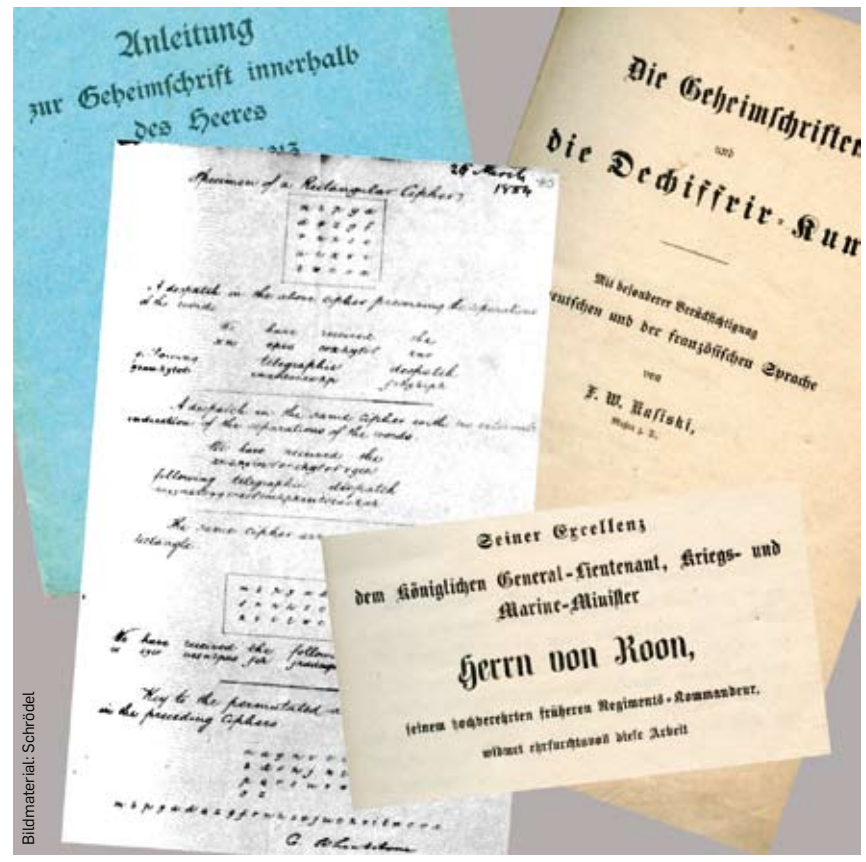
Erst 1864 nämlich, also mehr als 300 Jahre später, entdeckte der deutsche Major a.D. Friedrich Wilhelm Kasiski eine Schwäche darin und beschrieb diese in einem Büchlein, von dem er im Eigenverlag ein paar Dutzend drucken ließ. Im Vorwort grüßt er freundlich den Kriegsminister und ließ diesem sein famoses Werk auch gleich per Post zustellen. Das würde Orden hageln am Ende seiner Laufbahn, dessen war sich Kasiski sicher. Die Vigenère-Verschlüsselung war beim ausländischen Militär, gerade bei den Franzosen, noch immer im Einsatz, abgefangene Depeschen unlesbar und Kasiskis Entdeckung ein vielleicht entscheidender Vorteil, falls es Krieg gäbe. Kriegsminister von Roon erkannte die Tragweite von Kasiskis Entdeckung jedoch nicht. Es ist nicht einmal belegt, dass er das Buch überhaupt gelesen hat.

Friedrich Kasiski konnte sich über eine derartige Kurzsichtigkeit des Ministers, noch dazu ein Preuße wie er selbst, nur maßlos ärgern, ließ fortan das Dechiffrieren sein und widmete sich den Rest seines Lebens der Archäologie. Zum Glück erfuhr er niemals, dass man im Nachlass des umtriebigen britischen Erfinders Charles Babbage Aufzeichnungen fand, die belegen, dass dieser bereits zehn Jahre vor Kasiski die gleiche Schwachstelle gefunden, aber aus Faulheit nie veröffentlicht hatte. Kasiski hätte sich an einer seiner Ausgrabungsstätten wohl gleich selbst mit eingegraben.

Zwar existiert die gefundene Schwachstelle nur bei langen Texten, in Universitäten wird dem Major a.D. trotzdem gehuldigt, wenn vom Kasiski-Test die Rede ist. Die letzte Bastion von Vigenère fiel erst nach rund 450 Jahren im März 2008. Seitdem können auch kurze Chiffren gebrochen werden.

Details zur Vigenère Verschlüsselung und den Methoden sie zu knacken stehen im Internet, siehe Linkslage.

Tobias Schrödel



Bildmaterial: Schrödel

Dienstanweisung „Anleitung zur Geheimschrift innerhalb des Heeres“ in der Ausgabe von 1913 (links oben). Darüber eine Kopie der handschriftlichen Beschreibung der als „Playfair-Chiffre“ bezeichneten Verschlüsselung, datiert auf März 1854 und von ihrem Erfinder Charles Wheatstone unterzeichnet. Rechts das Titelblatt von Friedrich Wilhelm Kasiskis Buch über das Entziffern einer Vigenère-Verschlüsselung mit darüber gelegter Widmung der Folgeseite an den damaligen Kriegsminister.

DEUTSCHES LIEDGUT

Das Kriegsministerium des deutschen Staatenbundes brachte 1898 eine aktualisierte Version seiner Dienstanweisung zur „Geheimschrift innerhalb des Heeres“ heraus. Die vorgestellte Verschlüsselung ähnelt dem sog. Doppelwürfel (s. Info.). Diesen beschreibt Otto Leiberich, der erste Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI), noch 1999 in „Spektrum der Wissenschaft“ als unlösbar. Jedoch nur dann, so führt er aus, wenn sie richtig angewendet wird, was auch an der Wahl eines sicheren Schlüsselwortes liegt.

Rund 100 Jahre früher war das dem Kriegsministerium offenbar noch nicht so klar, denn man schrieb den Soldaten in die Anweisung: „Zum Schlüsseltext empfiehlt sich ein leicht zu behaltender Spruch oder Liedvers“. Ein Vorschlag, der heute noch jedem PC Benutzer die Haare zu Berge stehen lässt, weiß man doch, dass Hacker schon länger mögliche Schlüsselworte ausprobieren. Und was lag damals näher, als das Liedgut der feindlichen Kameraden?

Es ist daher auch gar nicht verwunderlich, dass man im nahen Ausland deutsche Funksprüche und Depeschen las. Nur in Berlin wunderte man sich immer wieder über die guten Informationen, die die Nachbarstaaten über die deutschen Truppenbewegungen hatten. Eine Idee, woran das liegen könnte, hatte man wohl, aber so richtig sicher, war man sich nicht. Beweis dafür ist die Neuauflage der Dienstanweisung von 1908: „Der Anfang eines Liedes ist zu vermeiden“ steht dort.

1911, es wurde nicht besser, entschied man sich, die Soldaten gar nicht erst auf die Idee mit dem Liedvers zu bringen und empfahl schlicht „einige leicht zu behaltende Worte“. Die Ausgabe von 1913 bleibt dabei.

Erst vier Jahre später kam man darauf, dass Soldaten immer noch gerne singen und allen voran die französischen Kryptoanalytiker deutsche Schellackplatten auf ihren Grammophonen rotieren ließen. Sie wollten nicht mitsingen, nur den Liedtext verstehen. Nun wurde die Anweisung erneut geändert, der Zusatz lautet kurz und knapp: „Der Anfang eines Liedes ist verboten“.

Général Cartier, der für die französischen Truppen den gesamten ersten Weltkrieg hindurch deutsche Verschlüsselungen knackte, berichtete später, dass es ihm half, dass sehr oft der Anfang eines Gedichtes als Schlüsselwort verwendet wurde. Nun sind Gedichte ja keine Lieder, es fehlt schließlich die Melodie. Etwas anderes hätte ich im Land der Dichter und Denker auch nicht erwartet. Vorschrift ist Vorschrift.

Ausschnitte aus dem Buch, insbesondere die angesprochene Dienstanweisung im Internet: s. Linkslage. *Tobias Schrödel*

IDEENKLAU VON LORD PLAYFAIR

Charles Wheatstone nutzte für geschäftliche und private Korrespondenz, ebenso wie viele andere um 1850, eine einfache, weil schnelle Substitutionsmethode. Teilten die Beteiligten nicht nur geschäftliche Kontakte oder das Bett miteinander, sondern auch ein Schlüsselwort, so konnten sie damit das Alphabet sehr einfach, aber effektiv durchmischen und geheim kommunizieren.

Wheatstone tauschte die Buchstaben jedoch nicht nur fest verdrahtet aus, er ordnete das gemischte Alphabet in einem 5x5 Quadrat in Spalten und Zeilen an (glücklicherweise wurde das J erst später erfunden). Aus jeweils zwei aufeinander folgenden Buchstaben des Klartextes bildete er innerhalb dieses Quadrats die gegenüberliegenden Ecken eines gedachten Rechtecks. Die Buchstaben an den freien Ecken ergaben das verschlüsselte Buchstabenpärchen. Durch eine Häufigkeitsanalyse war dem geheimen Text nun nicht mehr zu Leibe zu rücken.

Er zeigte diese geniale Idee seinem Freund Baron Lyon Playfair. Dieser genoss seine Abende in weit feinerer Gesellschaft als Wheatstone und die Hoffnung war, dass er ihm half, den Ruhm und die Ehre des britischen Empires zu erlangen. Bei einem Dinner mit Prince Albert, dem Mann von Königin Victoria, konnte Playfair auch tatsächlich davon berichten. Der König war derart angetan von der Sicherheit dieser einfachen Methode, dass er sogleich seinen geheimen Kabinetten auftrug, die neue „Playfair-Chiffre“ zu verwenden. Sie wird heute noch gerne unter dieser Bezeichnung in Büchern oder Vorlesungen über historische Kryptografie beschrieben. Ganz gleich, ob Lord Playfair die Namensgebung des Königs unterstützte oder sich einfach nicht traute zu widersprechen: An so etwas gehen Männerfreundschaften zu Grunde.

Details zur Playfair Chiffre stehen im Internet, siehe Linkslage.

Tobias Schrödel

DER DOPPELWÜRFEL

Angeblich setzen Spione beim Verschlüsseln von Texten selbst heute noch den so genannten Doppelwürfel ein, wenn sie nur Stift und Papier zur Verfügung haben oder der Einsatz einer Verschlüsselungsmaschine oder -software zu auffällig ist. Das Verfahren war Anfang des 20. Jahrhunderts auch als Nihilistenwürfel bekannt.

Notwendig ist die Kenntnis eines Schlüsselwortes, unter das man den zu verschleiernden Text schreibt. (a) Nehmen wir als Schlüssel RUBBITS und als Text eine Zeile aus einem Lied, welche wir unter das Losungswort schreiben. (b) Nun sortiert man das Schlüsselwort alphabetisch und vertauscht so die Spalten. (c) Nun liest man den Text Spaltenweise aus. Mit einem neuen Schlüsselwort werden diese Schritte wiederholt, so dass aus dem einfachen Würfel, der Doppelwürfel wird. Dieser ist – angeblich – unlösbar, wenn der Würfel nicht voll gefüllt ist, also die Textlänge kein Vielfaches der Länge des Schlüsselwortes ist. Auch sollte das Schlüsselwort nicht zu erraten sein.

R	U	B	B	I	T	S
t	i	e	f	i	m	w
e	s	t	e	n	w	o
d	i	e	s	o	n	n
e	v	e	r	s	t	a
u	b	t				

B	B	I	R	S	T	U
e	f	i	t	w	m	i
t	e	n	e	o	w	s
e	s	o	d	n	n	i
e	r	s	e	a	t	v
t			u			b

eteetfesrinostedeuwonamwntisivb

DER AUTOR

Tobias Schrödel ist freiberuflicher Berater für IT Security & Awareness und arbeitet bei T-Systems als Consultant im Bereich ICT PreSales. Tipps zu historischen und aktuellen Büchern und Software zu Verschlüsselungsmethoden: s. Linkslage.

IMPRESSUM

Herausgeber: Pressestelle der Ruhr-Universität Bochum; Leiter: Dr. Josef König (v.i.S.d.P.);
Redaktion: Meike Drießen, md; Koordination: Meike Drießen, Rainer Wojcieszynski, RZ;
Redaktionsanschrift: Pressestelle der RUB, UV 3/366, 44780 Bochum, Tel.: 0234/32-26952, -22830, Fax: 0234/32-14136, Internet: http://www.ruhr-uni-bochum.de/pressestelle;
Layout und Satz: bsp_design, Babette Sponheuer, Bochum;
Anzeigenverwaltung und -herstellung: vmm Wirtschaftsverlag, Maximilianstraße 9, 86150 Augsburg, Tel.: 0821/4405-0
Anzeigenschluss für Ausgabe 26 (November 2010) ist der 11.10.2010; Mediadaten: http://www.ruhr-uni-bochum.de/rubens/mediadat.htm
RUBbits erscheint zweimal pro Jahr als Service-Beilage zu RUBENS, Zeitschrift der Ruhr-Universität Bochum (http://www.ruhr-uni-bochum.de/RUBbits).
Namentlich gekennzeichnete Beiträge geben nicht unbedingt die Meinung der Redaktion wieder. Anfragen und Mitteilungen per E-Mail: rubbits@ruhr-uni-bochum.de
Auflage: 13.200