



## DER DIGITALE RADIERGUMMI IM UNTERNEHMEN

Meinungsecke zum Dilemma um das Vergessen, Löschen oder Ausradieren von Daten

Begleitet von großem Medienecho präsentierte das Verbraucherschutzministerium das durch ein Team von Prof. Dr. Michael Backes entwickelte Programm „X-Pire!“ – den so genannten digitalen Radiergummi (siehe Box). Darauf folgten kurzfristig kritische Kommentare [1] und skeptische Analysen [2] des Programmes.

In dieser Meinungsecke werden wir die grundlegenden Probleme und Lösungsansätze diskutieren, die sich hinter dem digitalen Radiergummi verbergen. Weiterhin werden wir die Bedeutung eines solchen Werkzeugs für Unternehmen erläutern.

### Das Dilemma der verlustfreien Vervielfältigung

X-pire ist eine Instanz des „digitalen Rechtemanagements“ (DRM). Die „Probleme“, die mit DRM adressiert werden sollen, sind in aller Regel die folgenden:

1. Elektronisch repräsentierte Daten lassen sich beliebig oft verlustfrei vervielfältigen.
2. Daten altern nicht (Datenträger allerdings schon).

**Funktionsweise von „X-Pire!“** – Der Benutzer, der ein Bild veröffentlichen möchte, lässt das Bild von X-Pire verschlüsseln und veröffentlicht anschließend das verschlüsselte Bild. Der Schlüssel wird zusammen mit einem „Verfallsdatum“ auf einem X-Pire Server hinterlegt. Wenn ein anderer Benutzer das Bild betrachten möchte, muss er zuvor den Schlüssel von diesem Server abrufen. Der Server liefert den Schlüssel nur, wenn das Verfallsdatum nicht überschritten ist. Außerdem muss der Betrachter noch ein Captcha lösen – damit soll ein automatisiertes Auslesen der Bilder verhindert werden (siehe <http://www.x-pire.de>).

**Probleme der Funktionsweise von „X-Pire!“** – Das Programm kann nicht verhindern, dass die Schlüssel der geschützten Bilder gespeichert und weitergegeben werden. Mit einem

gespeicherten Schlüssel kann das Bild auch nach Ablauf des „Verfallsdatums“ noch betrachtet werden. Das Programm verhindert ebenfalls nicht, dass ein einmal entschlüsseltes Bild auch über das „Verfallsdatum“ hinaus gespeichert oder weiterverbreitet wird.

Zugleich wird der ehrliche Betrachter durch das ständige Lösen von Captchas gestört. Würden Sie sich die Urlaubsbilder eines Freundes ansehen, wenn sie dabei ständig unleserliche Texte abschreiben müssten? Schließlich kann der Schlüsselservers(betreiber) in die Privatsphäre der Betrachter eindringen, da er detailliert protokollieren kann, wer, wann und wie oft welches Bild betrachtet hat.

3. Wir haben hochleistungsfähige Suchverfahren, mit denen sich Daten schnell auffinden lassen. Die werden in den kommenden Jahren voraussichtlich noch besser (z. B. in Bezug auf Bilder- und Tonsuche).

Zum Problem werden diese für sich positiven Eigenschaften nur, falls die Verbreitung eines Datums nicht gewünscht oder an Voraussetzungen (z. B. Lizenzgebühren) geknüpft ist. Dabei sind zumindest die ersten beiden genannten Eigenschaften nicht neu und auch nicht auf elektronisch repräsentierte Daten beschränkt, sondern zeichnen sich seit der Erfindung der Schriftsprache bereits für Texte ab, jedoch in deutlich abgeschwächerter Form. Sie wur-

nicht noch ein weiteres Duplikat übersehen wurde. Die unter Punkt 3 genannten hochleistungsfähigen Suchverfahren mögen dabei helfen, die Daten zu finden, das ist jedoch nur bei Datenspeichern möglich, die einer Durchsuchung zur Verfügung stehen.

Die Anfertigung von Duplikaten lässt sich auch nicht wirkungsvoll verhindern: Nach der Erfindung von Schriftsprache, Fotografie, Fonografie, Cinemation, Fotokopie etc. kann daran kein Zweifel mehr bestehen. Jeder Kopierschutz und jedes digitale Rechtemanagement ist am Ende nichts anderes als eine mehr oder weniger nachdrücklich vorgebrachte Bitte an den Hörer oder Betrachter, von einer Vielfältigung abzusehen.

**Digitales Rechtemanagement (DRM)** – Digitales Rechtemanagement bezeichnet Technologien, mit denen die Verwendung elektronischer Daten trotz Veröffentlichung eingeschränkt werden kann. Beispiele für Anwendungen von DRM sind:

**PDF-Dateien**, die zwar betrachtet, aber nicht (ohne Weiteres) gedruckt werden können.

**Digitale Wasserzeichen**, mit denen die Urheberschaft an einer Datei nachgewiesen oder auch der Verbreitungsweg unerwünschter Kopien nachvollzogen werden kann.

**Musik- und Film-Dateien**, von denen der Kunde nur eine beschränkte Anzahl von Kopien anfertigen kann (Filme bei iTunes, bis 2009 auch Musik bei iTunes entsprechend geschützt).

Digitales Rechtemanagement wird sehr kontrovers gesehen. Einerseits ist der Schutz, den es bei gezieltem Vorgehen bietet beschränkt, andererseits behindert es in vielen Fällen auch die legitime Verwendung der durch DRM geschützten Daten. Ferner wird die Begriffswahl kritisiert, da eher Restriktionen als Rechte (bzw. Berechtigungen) verwaltet werden.

den seitdem bis zum heutigen Stand konsequent verstärkt, durch die Erfindung des Buchdrucks mit beweglichen Lettern, später durch die Erfindung von Kopiergeräten. Und genau wie den mittelalterlichen Zensurbestrebungen keine Erfindung zur Hilfe kam, mit der alle Exemplare eines einmal verbreiteten Druckwerkes auf einfache Weise zurückgeholt werden konnten, wird auch dem gegenwärtigen Verbraucher oder Unternehmer keine Erfindung helfen können, einmal verbreitete Daten vollständig zu tilgen.

Wer ein Datum aus der Welt schaffen möchte, muss alle noch erhaltenen Duplikate finden und vernichten. Und selbst dann gibt es keine Sicherheit, ob

## Herausforderungen aus Unternehmenssicht

Geringfügig anders kann es in der IT-Landschaft von Unternehmen aussehen. Dort kann die Wirksamkeit von DRM durch eine strenge Beschränkung der eingesetzten Hard- und Software gefördert werden. Es gibt eine Reihe von Situationen, in denen Unternehmen sich einen digitalen Radiergummi wünschen könnten. In jedem Fall ist zu unterscheiden, ob ein Gegner aktiv versucht, das Löschen zu verhindern, oder ob es nur Zufälle und Versehen sind, gegen die der Radiergummi helfen soll.

Folgenden Herausforderungen sehen sich Unternehmen gegenüber:

1. Im Unternehmen liegen Daten vor, die zuverlässig gelöscht werden sollen, zum Beispiel nach Ablauf einer Lagerfrist, nach dem Ende eines Kundenverhältnisses oder aufgrund der Bestimmungen des Bundesdatenschutzgesetzes (insb. § 35).

Dieser Fall ist recht einfach zu lösen: Es gibt zahlreiche Programme, welche die Daten physisch überschreiben, sodass das Wiederherstellen der Daten unmöglich wird. (Bei aktuellen Magnet-Festplatten genügt technisch gesehen ein einfaches Überschreiben, siehe [3]. Das zuverlässige Löschen von Solid-State-Laufwerken (SSD) ist Gegenstand aktueller Forschung, siehe [4]. Allerdings müssen auch eventuell angefertigte Sicherheitskopien berücksichtigt werden und das kann schwierig sein, wenn sie nicht ausschließlich systematisch angelegt und gelagert wurden.

2. Ein Unternehmen möchte sicherstellen, dass bestimmte Daten nicht unberechtigt oder unbemerkt kopiert werden können, oder es möchte alle Daten zentral verwalten und löschen können sowie feingranular festlegen können, wer Daten abrufen und wer sie drucken darf, etc.

Solche Fälle können bis zu einem gewissen Grad tatsächlich durch digitales Rechtemanagement (und die noch weitergehenden Überwachungsfunktionen des so genannten „Trusted Computing“) gelöst werden. Wenn das Rechtemanagement wirkungsvoll sein soll, erfordert es sehr weitreichende organisatorische und technische Maßnahmen. Das wird allerdings die Produktivität der Mitarbeiter verschlechtern, da zwangsläufig auch legitime Tätigkeiten blockiert oder behindert werden. Einem gezielt und mit krimineller Energie vorgehenden Mitarbeiter kann es dennoch gelingen, geschützte Dokumente beispielsweise zu fotografieren.

3. Ein Unternehmen möchte Daten, die es selber irrtümlich im Internet veröffentlicht hat, wieder zurücknehmen. Die Daten müssen nicht nur von der eigenen Website gelöscht werden, sondern es müssen auch Suchmaschinen- und Archivbetreiber aufgefordert werden, die betroffenen Daten aus ihren Zwischenspeichern zu entfernen. Das ist auf Anfrage möglich, kann jedoch einige Zeit in Anspruch nehmen.

Auf den ersten Blick können DRM-Techniken wie X-Pire in solchen Situationen helfen, da sie verhindern, dass Suchmaschinen und Archive die fraglichen Daten überhaupt erst erfassen. Tatsächlich existiert eine wesentlich einfachere Möglichkeit, mit der Suchmaschinen- und Ar-

**Radiergummi oder Verfallsdatum?** – Das Verbraucherschutzministerium spricht im Zusammenhang mit Datenschutz im Internet seit einiger Zeit von einem „Digitalen Radiergummi“ der benötigt würde, um unerwünschte Daten aus dem Internet auszuradiieren. Die Wortwahl ist ungünstig, denn schon wesentlich länger firmieren Programme, die gelöschte Daten physisch überschreiben, um ein Wiederherstellen zu verhindern, unter der Bezeichnung „Radiergummi“ (bzw. häufiger auf Englisch „Eraser“). Andererseits ist die Wortwahl

ungewollt treffend, da herkömmliche Radiergummis genau wie ihre elektronischen Pendanten immer nur das vorliegende Dokument bearbeiten und nie zuvor erzeugte Duplikate. Die Bezeichnung „elektronisches Verfallsdatum“ ist für das, was X-Pire tun soll, treffender: Ein herkömmliches Verfallsdatum ist auf eine Verpackung aufgedruckt und fordert den Verbraucher auf, das Produkt nach dem Datum nicht mehr oder nur vorsichtig zu verwenden. Es verhindert die Verwendung jedoch nicht.

chivbetreiber von der eigenen Seite oder auch von bestimmten Dokumenten, die sich darauf befinden, fern gehalten werden können. Alle seriösen Anbieter können mit einer einfachen Textdatei in der Domain, der „robots.txt“, dazu gebracht werden, eine Website nur teilweise oder überhaupt nicht zu erfassen.

4. Ein Unternehmen möchte Daten, die jemand anderes im Internet veröffentlicht hat, entfernt wissen.

In diesem Fall ist eine technische Lösung nicht Erfolg versprechend – selbst wenn das fragliche Dokument durch DRM geschützt war, ist nach der Veröffentlichung davon auszugehen, dass der Schutz bereits umgangen wurde. Ein juristisches Vorgehen gegen die Veröffentlichung ist möglich, allerdings kann es passieren, dass damit zusätzliche Aufmerksamkeit auf die fraglichen Daten gelenkt wird. Dieser Umstand wird im Internet als Streisand-Effekt bezeichnet. Er wird dadurch verstärkt, dass verschiedene Gruppen reflexhaft auf alles reagieren, was als Zensur des Internets interpretiert werden könnte. Um diesen Effekt zu vermeiden, kann eine gütliche Einigung mit der Person, die die Daten veröffentlicht hat, eine bessere Strategie sein – insbesondere wenn die Person offenkundig nicht aus Böswilligkeit, sondern aus Unwissenheit gehandelt hat.

### Die gereizte Reaktion der Netzwelt

Obwohl eine abschließende Lösung der Probleme einer ungewünschten Vervielfältigung oder Verbreitung mit technischen Mitteln nicht möglich ist, reagiert ein großer Teil der Netzgemeinschaft ablehnend oder sogar feindlich auf entsprechende Ansätze. Die zentrale Sorge ist, es könne eine wirkungsvolle Zensurinfrastruktur entstehen, die später zur Durchsetzung fragwürdiger wirtschaftlicher und

gesellschaftlicher Interessen missbraucht werden könnte, denn auch wenn DRM-Techniken nie perfekt werden können, sind sie keineswegs wirkungslos. Sie zu umgehen erfordert Werkzeuge oder Kenntnisse, die nicht jedem zur Verfügung stehen. Außerdem besteht die Möglichkeit, dass technische Unzulänglichkeiten durch Gesetze kompensiert werden. Genauso, wie die Umgehung von sogenannten wirksamen technischen Kopierschutzvorrichtungen (§95a Urheberrechtsgesetz) in Deutschland bereits unter Strafe steht, könnte auch die Wirksamkeit eines elektronischen Radierers durch Verbote und Vorschriften flankiert werden.

### Die gesellschaftliche Komponente

Auch der Bundesdatenschutzbeauftragte Peter Schaar ist der Frage, wie das Löschen von Daten im Internet sichergestellt werden kann, in einem Beitrag [5] nachgegangen:

“Unabhängig davon überzeugen mich die technologischen Gegenargumente nicht. Selbst wenn die Löschung nicht garantiert werden kann, bedeutet dies nicht, dass man auf das Machbare verzichten muss. Auch in anderen Bereichen menschlichen Zusammenlebens lassen sich manche Ziele – auch solche, die allgemein akzeptiert sind – nicht hundertprozentig erreichen, was uns aber nicht daran hindert, entsprechende Regeln zu formulieren” – Peter Schaar.

Diese Aussage möchten wir hinterfragen: Der aktuelle Stand der Technik erlaubt es jeder und jedem, egal, ob es ein Konzern, ein Syndikat, eine Regierung oder eine Privatperson im Internetcafé ist, Daten zu vervielfältigen und zu speichern. Wenn digitale Radiergummis erst einmal allgegenwärtig sind, wird das anders.

Mit hinreichend Aufwand wird sich weiterhin alles, was einmal sichtbar oder hörbar war, persistieren lassen – beispielsweise durch abfotografieren. Die-

se Möglichkeit wird auch als analoge Lücke bezeichnet. Jedoch wird nicht mehr jeder in der Lage sein, diesen Aufwand zu erbringen. Möglich ist, dass eines Tages der durchschnittliche Privatanutzer, die NGO, oder der Whistleblower wirksam am Kopieren gehindert wird – bisweilen auch an der Weiterverarbeitung der eigenen Daten oder sogar einer Beweissicherung. Ein Beispiel wäre der Mittelständler, der gegen die unlauteren Online-Werbungen seines Wettbewerbers nicht vorgehen kann, da sein Wettbewerber die strittige Werbung einfach „digital ausradiert“ bevor ein Gericht sie zur Kenntnis nehmen kann. Noch drastischer wäre eine verbrecherische Organisation, die inkriminierendes Material trotz digitaler Löschung unbegrenzt vorhalten kann, während die Opfer nicht einmal ohne Weiteres in der Lage sind, die gegen Vervielfältigung geschützten Erpresserschreiben an die Polizei weiterzuleiten. Kurz gesagt könnte ein flächendeckender Einsatz von digitalem Rechtemanagement (und der weiterreichenden Variante des so genannten “Trusted Computing”) eine Asymmetrie schaffen, wo heute Gleichberechtigung herrscht.

---

Vincent Wolff-Marting

## Quellen

- [1] <http://www.heise.de/security/artikel/Bitte-vergessen-1167720.html>
- [2] <http://www.danisch.de/blog/2011/01/05/idiotische-kryptographie-made-in-germany/>
- [3] Craig Wright, Dave Kleiman und Shyaam Sundhar R.S.: Overwriting Hard Drive Data: The Great Wiping Controversy. In Lecture Notes in Computer Science, 2008, Volume 5352/2008, 243-257, DOI: 10.1007/978-3-540-89862-7\_21
- [4] Michael Wei, Laura Grupp, Frederick E. Spada und Steven Swanson: Reliably Erasing Data from Flash-Based Solid State Drives. 9th USENIX Conference on File and Storage Technologies, 15-17. Feb 2011, San Jose.  
[http://www.usenix.org/events/fast11/tech/full\\_papers/Wei.pdf](http://www.usenix.org/events/fast11/tech/full_papers/Wei.pdf)
- [5] [https://www.bfdi.bund.de/bfdi\\_forum/showthread.php?1697-Der-digitale-Radiergummi-und-das-Recht-vergessen-zu-werden](https://www.bfdi.bund.de/bfdi_forum/showthread.php?1697-Der-digitale-Radiergummi-und-das-Recht-vergessen-zu-werden)