

Ist die Datenhaltung des Grundbuches bzw. des Hauptbuches einer Bank auf root-Plattformen grundgesetzkonform?

Günter Nauheimer *

5. Oktober 2016

Das Betreiben der Datenhaltungsschicht des Grund- bzw. Hauptbuches einer Bank auf root-Plattformen gefährdet das Recht zur freien Entfaltung der Persönlichkeit, das Recht auf Eigentum, die Gewaltenteilung, die Parteienfinanzierung und das Wahlrecht. In diesem Umfeld sind also root-Plattformen nicht verfassungskonform und untergraben die rechtsstaatlichen Prinzipien der Gewährleistung von Rechtssicherheit, der Garantie gleicher persönlicher Freiheit, der Sicherung materieller Gerechtigkeit und der Gewährleistung elementarer Menschenrechte.

*<https://sieben-und-fuenf.org>

Erläuterungen

Mit *Datenhaltung* ist das Datenbankmanagementsystem (DBMS) und die Datenspeicher in der elektronischen Datenverarbeitung (EDV) der Bank gemeint. Geschrieben wird hier also über die Datenhaltungsschicht wie sie innerhalb einer Drei-Schichten-Softwarearchitektur bestehend aus Datenhaltungs-, Geschäftslogik- und Präsentationsschicht betrachtet wird. Die beiden letzten Schichten und weitere Komponenten einer IT-Landschaft sollen in weiteren Artikeln besprochen werden.

Mit *Grundbuch* bzw. *Hauptbuch* sind die Kontostamm-, Kontobewegungs- und Bilanzdaten der Bank gemeint. Die Paragraphen 675d Abs. 2, 675w Satz 1 und 676 BGB erlegen die Beweislast zum Nachweis der ordnungsgemäßen Aufzeichnung und Verbuchung den Zahlungsdienstleistern (i.w. Banken) auf. Im Streitfall über einen Tatbestand muß es möglich sein den Tathergang in objektiver Weise nachzuprüfen. Die objektive *Nachprüfbarkeit* ist nicht gegeben, wenn eine Person den Tathergang spurlos manipulieren kann. Auch muß nach den „Grundsätzen zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff“ (GoBD) das zum Einsatz kommende DV-Verfahren die Gewähr dafür bieten alle Informationen, die in den Verarbeitungsprozess eingeführt werden, erfasst werden und zudem nicht mehr unterdrückt werden können. Diese Gewährleistung kann auf root-Plattformen (s.u.) nicht gegeben werden.

Das Grundgesetz spielt eine Rolle bei der Auswahl des DBMS mit den Artikeln

Artikel 2 Abs. 1 *Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.*

Artikel 14 Abs. 1 *Das Eigentum und das Erbrecht werden gewährleistet. Inhalt und Schranken werden durch die Gesetze bestimmt.*

Artikel 20 Abs. 3 *Die Gesetzgebung ist an die verfassungsmäßige Ordnung, die vollziehende Gewalt und die Rechtsprechung sind an Gesetz und Recht gebunden.*

Artikel 21 Abs. 1 *Die Parteien wirken bei der politischen Willensbildung des Volkes mit. Ihre Gründung ist frei. Ihre innere Ordnung muß demokratischen Grundsätzen entsprechen. Sie müssen über die Herkunft und Verwendung ihrer Mittel sowie über ihr Vermögen öffentlich Rechenschaft geben.*

Artikel 38 Abs. 1 *Die Abgeordneten des Deutschen Bundestages werden in allgemeiner, unmittelbarer, freier, gleicher und geheimer Wahl gewählt.*

Mit *root-Plattform* ist ein Betriebssystem (OS) gemeint, welches ein allgemein bekanntes Benutzerkonto hat, dem alle Rechte (Erzeugen, Ändern, Löschen und Ausführen) an

sämtlichen Ressourcen (z.B. Daten und Prozesse) des Systems zugeordnet sind und dessen Benutzer im Namen aller anderen Benutzerkonten handeln darf (im folgenden wird dieses Benutzerkonto als *Superuserkonto* bezeichnet). Unter einem Benutzerkonto kann sich eine natürliche Person an dem Betriebssystem anmelden um damit zu arbeiten. Benutzer, die unter einem Superuserkonto arbeiten, werden als *Superuser* bezeichnet. Der *Verfügungsbereich* eines Benutzers ist die Summe aller Berechtigungen der ihm verfügbaren Benutzerkonten, die auch auf verschiedenen Systemen liegen können. Andere hochprivilegierte Benutzerkonten, z.B. des DBMS, die ebenfalls Auswirkung auf meine Grundrechte haben, bleiben hier der Einfachheit halber außen vor.

Eine Auflistung der Eigenschaften *digitaler Daten* (d.D.) verdeutlicht die besondere Kritikalität des Superuserkontos.

- es gibt kleinste Einheiten, Bits genannt
- es können Bit für Bit exakte Kopieen d.D. angefertigt werden

Auf les-/beschreibaren Medien (R/W Medien) gilt zusätzlich

- Bits sind beliebig manipulierbar
- makroskopische Mengen (bedeutungstragende Menge) von Bits sind mit vernachlässigbarem Zeit- und Energieaufwand änderbar

Digitale Daten besitzen im Gegensatz zu analogen Daten keine Individualität, womit der Unterschied zwischen Original und Fälschung entfällt, und sind auf R/W Medien beliebig formbar. Digitale Daten sind keine Sachen. Nur eine lückenlose Betrachtung der Sicherheit vom Chip bis zum Endbenutzer kann also Aufschluß geben über das erreichte Sicherheitsniveau.

Die genannten Eigenschaften d.D. führen mit der zunehmenden Digitalisierung der Datenverarbeitung zu zwei entgegengesetzten Entwicklungen bei dem Risiko. Es ist einerseits möglich zufällige Fehler weitestgehend auszuschließen (ein Programm macht immer exakt dasselbe), andererseits werden systematische Fehler ermöglicht, die prinzipiell unmöglich sind mit analogen Daten (z.B. spurlose Manipulation). Das systematische Risiko ist aber für die Auswirkung auf meine Grundrechte der entscheidende Aspekt. Für einen Banker, der beim Verkaufen eines Kredites unterschiedliche Risiken über den Preis (Zinsen) bewertet, wird das Risiko der verschiedenen Plattformen über deren Marktpreis offensichtlich.

Auch endet für d.D. der Prüfprozess des „genauer hinschauens“, im Gegensatz zu analogen Daten, auf der Ebene der kleinsten Einheiten, den Bits.

These

Die Datenhaltung des Grundbuches bzw. des Hauptbuches einer Bank auf einer root-Plattform ist nicht vereinbar mit den oben genannten Artikeln des Grundgesetzes und

untergräbt die rechtsstaatlichen Prinzipien der Gewährleistung von Rechtssicherheit, der Garantie gleicher persönlicher Freiheit, der Sicherung materieller Gerechtigkeit und der Gewährleistung elementarer Menschenrechte. Insbesondere sind Willkürfreiheit und Nachprüfbarkeit notwendige Eigenschaften von Daten, die über meine Grundrechte entscheiden um Rechtssicherheit zu bieten. Auch das in einem demokratischen Rechtsstaat notwendige Organisationsprinzip „Machtkontrolle durch Machtteilung“ wird durch ein Superuserkonto in diesem Umfeld verletzt.

Begründung

Da dem Superuserkonto alle Rechte (Erzeugen, Ändern, Löschen und Ausführen) an sämtlichen Ressourcen der Plattform zugeordnet sind und dessen Benutzer im Namen aller anderen Benutzerkonten handeln darf, kann der Superuser alle digitalen Daten beliebig und nicht nachprüfbar manipulieren. Die Nicht-Nachprüfbarkeit folgt aus verschiedenen Mechanismen: Erstens kann eine in sich stimmige und glaubhafte Änderung prinzipiell nicht als Manipulation erkannt werden, weil ein Rückgriff auf grundlegendere Daten (analoge Trägerschicht) wegen der eingesetzten Speichertechnologien, die die Austauschbarkeit der Festplatten im laufenden Betrieb erlauben und die Reorganisation der d.D. durch die Speicheralgorithmien mit Löschen und Wiederbeschreiben der physischen Trägerschicht durchführen, nicht sinnvoll, d.h. mit der notwendigen zeitlichen Stabilität, durchgeführt werden kann. Ein Rückgriff auf die analoge Trägerschicht läuft auch der Abstraktion „digitale Daten“ entgegen, die ja zwecks leichteren Gebrauchs eingeführt wurde. Die vollständige Rekonstruktion der bilanzwirksamen d.D. aus dem Bezeichneten, der Vorgang der Inventur, ist wegen der großen Menge und dem hohen Grad der beleglosen Verarbeitung nicht möglich. Die Inventur einer Bank ist im wesentlichen eine Buchinventur. Zum zweiten sind alle Prozesse auf dem System, die die d.D. der unmittelbaren Anschauung zuführen, unter der Willkür des Superusers (Rootkits).

Auf Daten, die der willkürlichen und nicht nachprüfbaren Manipulation unterworfen sind, kann keine allgemeinverbindliche, willkürfreie Interpretation aufgebaut werden.

In dem hier besprochenen Umfeld werden die d.D. als Geld interpretiert. Der Funktion von Geld als Zwischentauschmittel gemäß liegt der Wert des Geldes zwischen den Personen. Damit diese Daten in ihrer Funktion als Geld genutzt werden können, ist es also notwendig eine allgemeinverbindliche, willkürfreie Interpretation aufbauen zu können. Insbesondere sind auf Basis von digitalen Daten, die im Verfügungsbereich eines Superusers gehalten werden, keine Beweise nach den Paragraphen 675d Abs. 2, 675w Satz1 oder 676 BGB möglich.

Meine oben genannten Grundrechte und Artikel des Grundgesetzes sind durch folgende Mechanismen in Gefahr.

Artikel 2 Abs. 1

In unserer hochgradig arbeitsteiligen Gesellschaft ist Geld das hauptsächliche Mittel um seine Wünsche zu verwirklichen. Gibt man dieses Geld (bzw. die Daten, welche das Geld repräsentieren) in die Willkür eines Superusers, dann kann man nicht mehr von einem garantierten Grundrecht reden. Zum großen Teil hinge meine persönliche Entfaltungsfreiheit also von des Superusers Gnaden ab.

Artikel 14 Abs. 1

Mein Eigentum ist durch die Haltung meiner Kontodaten auf einer root-Plattform durch drei Mechanismen gefährdet. Erstens könnte mein Kontosaldo auf nicht-nachprüfbare, willkürliche Weise zu meinem Nachteil manipuliert werden. Zweitens könnte zu Gunsten Dritter Geld in praktisch beliebiger Menge geschöpft werden, was eine Inflation verursachen würde. Und Drittens würde langfristig das Vertrauen der Menschen in das Geld untergraben, weil ein DBMS auf einer root-Plattform dem Drucken von Geldscheinen auf Normalpapier durch die EZB gleichkäme. Weil das weitaus meiste Geld im Umlauf aber von Banken geschöpftes Geld ist, ist ein DBMS auf einer root-Plattform noch folgenschwerer.

Artikel 20 Abs. 3

Im Artikel 20 Abs. 3 werden die drei Gewalten Gesetzgebung, vollziehende Gewalt und Rechtsprechung juristisch aus der Taufe gehoben. Das in einem demokratischen Rechtsstaat geltende Organisationsprinzip „Machtkontrolle durch Machtteilung“ findet darin seinen Ausdruck. Die im Artikel 21 Abs. 1 juristisch akzeptierte Verbindung zwischen Geld und Macht, legt es nahe dieses Organisationsprinzip auf die Hauptquelle des Geldes, das meiste Geld wird von Banken geschöpft, zu übertragen.

Ein Superuserkonto im DBMS läuft dem Organisationsprinzip „Machtkontrolle durch Machtteilung“ zuwider.

Artikel 21 Abs. 1

Im Artikel 21 Absatz 1 wird eine Verbindung zwischen Geld und Macht juristisch akzeptiert und soweit problematisiert, daß Parteien über ihr Vermögen öffentlich Rechenschaft abgeben müssen. Weil die Daten in der Willkür des Superusers liegen, verliert jedes Reden darüber (insbesondere Reden zur Abgabe von Rechenschaft) seine Substanz. Es könnte einer Partei nicht-nachprüfbar Vermögen entzogen bzw. hinzugefügt werden. Auch wären Parteien gefährdet durch sichtbar gemachtes zusätzliches Vermögen und die damit einhergehende öffentliche Diskussion. Es wäre somit willkürlich möglich Parteien in den finanziellen oder politischen Ruin zu führen.

Die Konten von Parteien dürfen daher nicht auf root-Plattformen geführt werden.

Artikel 38 Abs. 1

Ein Superuserkonto könnte auch Abgeordneten und Wahlkreiskandidaten nicht-nachprüfbar Geld verfügbar machen oder entziehen. Damit gäbe es keine Chancengleichheit mehr zwischen den Kandidaten.

Gegenstrategien

Auf die drei Gegenstrategien „Verschlüsselung“, „organisatorische Maßnahmen“ und „nebengeordnete Daten“, die oft angewendet werden um die beliebige Formbarkeit d.D. zu mindern und deren Beweiskraft zu stärken, wird hier noch eingegangen und auf ihre Unzulänglichkeit hingewiesen.

Die Vorstellung die Daten vor Mißbrauch durch eine Verschlüsselung zu schützen, beruht auf der fehlenden Unterscheidung zwischen „Daten“ und „Information“ (eine typische Anthropomorphisierung, da bei Menschen, als biologische Einheiten, Datenverarbeitung und Informationsverarbeitung nicht trennbar ist). Ob die Daten nun verschlüsselt sind oder nicht, der Superuser kann in beiden Fällen jedem beliebigen Bit einen willkürlichen Wert geben. Die Verschlüsselung ändert also nichts an der Herrschaft über die Daten. Die Verschlüsselung verschärft dagegen das Problem der unabhängigen Nachprüfbarkeit (Beweiskraft), da jeder sinnvolle Gebrauch der Daten nun gezwungen wird durch das Nadelöhr der Entschlüsselung zu gehen. Eine Verschlüsselung bilanzwirksamer Daten schließt z.B. den in der Buchführung geforderten „sachverständigen Dritten“ aus bzw. zwingt ihn durch das Nadelöhr der Entschlüsselung. Die Verschlüsselung in der Datenhaltungsschicht kann also nicht einen angemessenen Zuschnitt der Berechtigungen auf dem System ersetzen. Die Verschlüsselung schränkt lediglich den Gebrauch der durch die Daten repräsentierten Information auf die Schlüsselberechtigten ein.

Organisatorische Maßnahmen, die vor Mißbrauch der d.D. schützen sollen, bedürfen sowohl aus systematischer als auch aus praktischer Sicht gleichlaufende, technische Maßnahmen.

Da d.D. nur über technische Mittel zugänglich sind, müssen Benutzer von der Bank berechtigt werden (Anlegen eines Benutzerkontos, Zuteilung von Rechten an das Benutzerkonto, Zuteilung des Benutzerkontos an den Benutzer) bevor sie im System etwas machen können. Der Superuser ist daher immer konfrontiert mit zwei gegensätzlichen Willensäußerungen der Bank: Die Rechte des Superuserkontos besagen „Du darfst alles und das auch im Namen aller Anderen.“ und die organisatorischen Maßnahmen besagen „Du darfst dies und das nicht.“. Weil die Berechtigungen über den Zugriff entscheiden, können diese juristisch nicht vernachlässigt werden. Anderenfalls würde man ja dem Aufbau einer Parallelwelt zusehen.

Mit der Entscheidung für eine root-Plattform in der Datenhaltungsschicht konterkariert die Bank daher ihre Dienstanweisungen zu einem ordnungsgemäßen Bankbetrieb.

Die gleiche Widersprüchlichkeit besteht zwischen den Verträgen zur Auslagerung des Betriebes von root-Plattformen und dem Inhalt der Superuserrechten, sei es durch die Zuteilung an externe Arbeiter oder durch die Auslagerung des Betriebes von root-Plattformen.

Die Auslagerung des Betriebes von root-Plattformen und die Zuteilung von Superuserrechten an externe Arbeiter ist in diesem Umfeld nicht in verantwortlicher Weise möglich.

Die praktische Sicht muß berücksichtigen die begrenzte Aufnahme-, Verarbeitungs- und Urteilsfähigkeit des menschlichen Bewusstseins, den Kostendruck auf dem Bankbetrieb, die typische Incidentrate eines Bankbetriebes und die Tatsache, daß niemand eine neutrale Haltung gegenüber Geld einnehmen kann. In diesem Arbeitsumfeld ist es nur eine (kurze) Frage der Zeit bis zu einem Zugriff mit Superuserberechtigung. Danach kann für die Integrität des Systems keine allgemeine Zustimmung mehr eingefordert werden.

Nebengeordnete digitale Daten sind z.B. Logging, Backups, Kontrollkonten oder Abstimmlisten der liefernden Systeme. Nur wenn diese Daten außerhalb des Verfügungsgebietes eines (1) Superusers liegen, können sie zur Minderung der Willkürlichkeit des Grundbuches bzw. des Hauptbuches beitragen. Um den Wert von nebengeordneten d.D. einschätzen zu können, müssen daher die anderen Softwareschichten und Komponenten einer IT-Landschaft, wie z.B. Rechnerkommunikation und die liefernden Systeme, mit betrachtet werden. Rationalisierungsmaßnahmen zur Vereinheitlichung der IT-Plattformen und zur Personaleinsparung wirken der gegenseitigen Abschottung entgegen und mindern die sich gegenseitig stützende Aussagekraft der digitalen Daten. Auch haben diese nebengeordneten d.D. im allgemeinen eine geringere Schutzklasse und werden nur kürzer aufbewahrt. Ebenso liegt in der Entscheidung, welchen d.D. nun in der konkreten Situation getraut wird, eine gewisse Willkürlichkeit.

Schlußwort

Ich plädiere hier nicht dafür die Bücher einer Bank auf Tontafeln zu führen um sie 4000 Jahre später noch nachprüfen zu können. Eine kritische Einstellung zu den Berechtigungen an den Daten, die über meine Grundrechte entscheiden, ist aber notwendig. Daten, die über meine Grundrechte entscheiden, müssen in der EDV vernünftigerweise auf Plattformen ohne Superuserkonto gehalten werden, um den Forderungen nach Willkürfreiheit und Nachprüfbarkeit in einem demokratischen Rechtsstaat genügen zu können.

Folgende Denkanstöße noch zu allerletzt:

Welche Bedeutung hat ein Kontosaldo, welche Bedeutung hat die Bilanz der Bank, wenn der Superuser die Berechtigung hat die Daten des Grundbuches bzw. des Hauptbuches in eine digitale Repräsentation des Walt Disney Films “Das Dschungelbuch“ zu transformieren?

Wie passt die aktuelle Einführung von Geldscheinen mit stärkeren Sicherheitsmerkmalen durch die EZB zu der Entwicklung bei Banken ihre bilanzwirksamen Daten auf root-Plattformen, die eine minderwertige Sicherheit bieten, zu migrieren?

Wie passt es zusammen, daß der Gesetzgeber einerseits mit der Beweislastumkehr im Zahlungsverkehr zu seinem stärksten disziplinierenden Mittel greift, andererseits es den Banken erlaubt wird ihren Bankbetrieb auf root-Plattformen zu fahren, die die Zahlungsverkehrsdaten auf nicht nachprüfbare Weise (Rootkits) in die Willkür des Superusers legen?

Bei analogen Daten werden durch die unveränderbaren, allgemeingültigen Naturgesetze die möglichen Operationen und Zustände beschränkt, wodurch eine sinnvolle Kommunikation erst ermöglicht wird. Um auf Basis von digitalen Daten eine sinnvolle, allgemeingültige Kommunikation aufbauen zu können, ist die Fähigkeit entscheidend die möglichen Operationen und Zustände einschränken zu können.

Zu einer Einschätzung des Sicherheitsniveaus auf den verschiedenen IT-Plattformen kann man auch durch folgendes Experiment gelangen:

Man wähle aus den Benutzerkonten eines aus und gebe einem der zugeordneten Benutzer einen Beraterstab an die Hand, der für diesen Benutzer die Recherche nach Schwachstellen und den Bau von Kits (rootkits) übernimmt. Mit der Hand an der Tastatur tätig wird nur der eine Benutzer im Rahmen seines Verfügungsbereiches. Gelingt es dem Benutzer das Grund- und Hauptbuch unter seine Kontrolle zu bekommen, dann liegen meine o.g. Grundrechte in seiner Willkür.

Zu einer empirischen Einschätzung des Sicherheitsniveaus der verschiedenen IT-Plattformen kann man durch das Studium von Fehlerdatenbanken (z.B. <https://nvd.nist.gov/>) gelangen.