Und Orwell hatte doch recht – Warum Palladium und TCPA so gefährlich sind

Christoph F.-J. Goetz
Leiter Telemedizin/EDV in der Arztpraxis
Kassenärztliche Vereinigung Bayern, Arabellastraße 30, 81925 München

Auf leisen Sohlen schleicht die neue Computerrevolution heran. In einer von Terror gebeutelten Welt machen sich ernsthafte Anwender so ihre Gedanken über die Gefahren im World Wide Web, über den Schutz eigener Rechnersysteme und über die grundsätzliche Zuverlässigkeit jener Technologie, der die ganze Welt ihr gesamtes Wissen, ihre vollständige Kommunikation, ja ihren wirtschaftlichen Lebensnerv zunehmend anvertraut.

Führte die Vergangenheit noch Kriege über Land und Besitz, gegen Menschen und Meinungen so dreht sich heute immer mehr um die Kontrolle von Information. Diese Entwicklung hat das Potenzial, sich zu einer Art neuzeitlichem Totalitarismus auszuwachsen – und keiner will es kommen gesehen haben.

Die neue Heilslehre:

Die weltweit bekannte Raumausstatterin, die Firma Klein & Weich, stellt vor den Häusern aller ihrer Kunden automatisch einen eigenen Wachmann auf, sobald man dort Möbel kauft. Dieser kontrolliert jeden der das Haus betreten will an der Türe und hält so Unbefugte fern. Noch besser, er schaut sogar in alle Tüten und Beutel und sichert so die Bewohner vor unliebsamen, potenziell gefährlichen Mitbringseln.

Zunächst verbreitet dieses Bild ein wohliges Gefühl der Sicherheit. Warm und behütet kann es sich nun jeder in seiner eigenen Behausung gemütlich machen. Doch irgendwann, langsam aus dem Unterbewusstsein, beginnen Zweifel an diesem bukolischen Bild zu nagen. Wurde nicht allzu leichtfertig, allzu viel aufgegeben?

Während Virenangriffe, untergeschobene Fremdprogramme und andere zweifelhafte Errungenschaften der elektronischen Welt bisher erträglich selten bezifferbare Verluste verursachten, so ist zwischenzeitlich der Finanzeinsatz, eigentlich das ganze bedrohte Kapital so immens, dass selbst einfache Gemüter sich ihre Gedanken machen. Das gesamte Schadenspotenzial lässt selbst abgebrühte Realisten grübeln. Daher will jeder sich, seinen Rechner, sein Wissen schützen. Ein Trend, den die Software- und Computerindustrie gerne bedienen will und muss.

In bemerkenswerter Synchronizität lässt sich eine weitere Strömung der Zeit erkennen. Viele Menschen sind jetzt anscheinend bereit, ihr kreatives Schaffen neuzeitlichen Medienkonzernen in den Rachen zu werfen. Damit wollen sie Urheberechtsschutzprobleme im Elektronikzeitalter vordergründig lösen, statt ihr eigenes Gedankengut selbst zu vertreten. Dabei vergessen sie, Wissen ist Macht und vor allzu viel Macht in der Hand eines immer größer werdenden Bruders haben schon die alten weisen Denker gewarnt.

Die Fakten sind leider eckig und spröde. Doch gerade deswegen sollte sich jeder seine eigene Meinung bilden. Die Geschichte geht so:

- „Palladium“ (benannt nach einem katalytischen Metall der Platingruppe) ist eine Software, die Microsoft in alle ihre kommenden Windows-Versionen integrieren will. Dort verankert, teilt Palladium künftig die Anwendungen in zwei Klassen auf: Standard oder sicher. Nur die „sicheren“ Programme erhalten direkten Zugriff auf den ganzen Rechner.
  Da die Bezeichnung Palladium durch Kontroversen und diverse Sicherheitslücken inzwischen „Flecken bekommen hat“, prägte das Unternehmen aus Redmont kürzlich das längere und noch undeutlichere Begriffsungetüm „Next Generation Secure Computing Base“ (NGSCB, „Sichere Rechnerbasis der nächsten Generation“). Die Microsoft-Techniker haben zur Umsetzung dieser Konzepte eine Software-Maschine mit dem Namen Nexus programmiert, die künftig im Herz jedes Betriebssystems regieren soll.

Der privilegierte Kern kommender Windows-Betriebssysteme soll dann auch noch in der Hardware des Computers durch einen auf dem Motherboard integrierten Chip fest verankert werden, der jedem Rechner seine eigene unverwechselbare Identität verleiht.

- Der neue Anker setzt dabei auf der „Trusted Computer Platform Alliance“ (TCPA, Allianz für vertrauenswürdige Computerplattformen) auf, einer vom Chip-Hersteller Intel und weiteren Initiativträgern geplanten speziellen Erweiterung des Prozessorkerns. Hier werden neue Sicherheitsfunktionen, privilegierte Befehle und Speicherbe-

Autor: Christoph F.-J. Goetz
Titel: Warum Palladium und TCPA so gefährlich sind
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Ober-Mörlen, Ausgabe 2004
Seite: 284-286

reiche fest im Silizium „verdrahtet“, natürlich zusammen mit einer weltweit eindeutigen Seriennummer. Diese wird integriert in eine Signatur, die auf der Hardware des Rechners basiert und jede Konfigurationsänderung sofort erkennt. Auch in dieser Entwicklung blieben Dissonanzen nicht aus. Trotz ihrer Mitbegründerschaft an TCPA will Intel nun einen Schritt weiter gehen und forciert eine eigene Lösung, die „ein wenig“ besser ist unter der Bezeichnung „LaGrande“.

Diese beiden Komponenten sollen künftig in jedem Computer eine Systemumgebung bilden, die verhindert, dass ein Angreifer (oder der Anwender) auf dem Rechner laufende Anwendungen oder verbaute Hardware manipulieren kann. Rechner und Betriebssystem erhalten so einen Schutz vor unberechtigten Zugriffen und natürlich auch vor dem, was die Hersteller als unberechtigten Zugriff durch den eigenen User erachten. Gab es da nicht einmal die Begriffe von „Besitz“ und „Eigentum“?

Praktisch gesehen soll also künftig eine Art „Wach und Schließgesellschaft“ in jedem Rechner Aufsicht führen, die z.B. überwacht: Ist das gerade gestartete Programm bei mir als „sicher“ registriert? Ist der gerade aufgelegte Song auch wirklich für „mich“ freigegeben? Windows führt dann nur noch solche Programme im gesicherten Kern aus, die vom System zuvor als unbedenklich erklärt wurden und relegiert alle anderen Programme in die eingeschränkte „Ersatzverarbeitung“. Dass die technischen Schergen der zweiten Klasse nur noch eingeschränkten Zugriff auf die Systemressourcen haben versteht sich eigentlich von selbst.

Diese eben beschriebenen technischen Schergen stehen aber im Computer nicht sinnlos herum, sie sind Dreh- und Angelpunkt eines in aller Stille durchgeschobenen, heute schon weltweit verbindlichen Gesetzeswerks.

- So beschloss 1994 die Welthandelsorganisation „geistiges Eigentum“, wie jedes materielle Eigentum, als gewöhnliche Handelsware zu definieren. In der „Richtlinie zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Rechte der Informationsgesellschaft“ übernahm dann im Sommer 2001 die EU diese Vorgaben, die bis zum 22.12.2002 von allen Mitgliedsstaaten in gültiges Recht umgesetzt werden sollten. Nur Deutschland war bislang noch säumig.
- Konkret gilt dabei folgendes: Auf dieser Rechtsgrundlage soll geistiges Eigentum zum individuierbaren Gegenstand gemacht werden, der nur mit Zustimmung des Eigentümers verwendet werden darf von einem dem Eigentümer namentlich bekannten Kunden. Dazu sollen globale Schutzmechanismen geschaffen werden. Deren Betreiber dürfen das gesamte System kontrollieren und gerichtlich gegen alle Verstöße vorgehen. Dabei dürfen sie dem Delinquenten auch den Internetzugang verwehren und sogar mittels Eingriff in dessen Rechner den Zugang zu diesem Diebesgut versperren.

Und so werden die spröden Ecken und Kanten von vorher jetzt plötzlich wieder rund!

Die praktischen Anwendungsmöglichkeiten von Palladium (NGSCB) und TCPA (LaGrande) sind vielfältig, häufig komplex, manchmal sogar hinreißend, hinterlassen aber im Rudel einen doch fauligen Geschmack:

- Als zunächst offensichtliche Anwendung leuchtet der wirksame Schutz vor Angreifern aus dem feindlichen Umfeld des Internets sofort ein. Wie schön wäre das Ende aller Viren und Trojaner!
- Die gleichen Prinzipien bieten sich aber auch an für das „Digital Rights Management“ (DRM, Verwaltung digitaler Urheberrecht). Hier gerät die arg geschundene Musikindustrie in verzücktes Strahlen. Der Rechner selbst kontrolliert, wer hat welche Lizenz zum Anhören welcher Musik erworben!
- Dies wiederum stellt ein El Dorado für Demographen, Meinungsforscher und Industriemanager dar, eröffnet sich doch aus dem so entstehenden Datenverkehr die Möglichkeit, jeden „Kunden“ künftig noch besser zu kennen und noch individueller bedienen zu können. Wer legt denn im Zeitalter aller dieser verflochtenen Credit- und Payback-Karten schließlich noch Wert darauf, dass sein Einkaufsverhalten Privatangelegenheit bleibt?
- Endlich können „gute“ von „schlechten“ Programmen wirksam unterschieden werden. Dabei spielt es dann doch eher eine geringe Rolle, wer diese Entscheidung letztendlich fällt und damit bestimmt, was auf welchem Rechner laufen darf.

Unabhängig vom Janusgesicht aller dieser „Vorteile“ rückt hier fast unmerklich die Bedeutung der weltweiten Internets in den Brennpunkt des Geschehens. Alle genannten Anwendungen weisen eine zentrale Gemeinsamkeit auf: Die des „offenen“ Internets. Mittels Palladium oder TCPA gesicherte Programme können erst ihre volle Wirkung entfalten, wenn sie dauernd über das Internet mit ihren Autoren, Verantwortlichen oder Rechteinhabern Kontakt aufnehmen können. Als sogenannte „phone home“-Applikationen entfachen gesicherte Anwendungen einen ständigen Kommunikationsbedarf, den die Industrie sicher gerne nutzen wird. Die Logik ist unausweichlich: Irgend jemand muss schließlich die Sicherheitstabellen pflegen. Dieser Jemand bekommt alles mit. Er weiß, was jeder hat. Er kann jede Anwendung ein- oder ausschalten.

Wie fasste doch gleich wieder Orwell den Begriff des große Bruders?

Eine Erkenntnis wird unausweichlich: Bei der „Trusted Computing Platform“ bedeutet Vertrauen nicht, das der Benutzer nun seinem Computer vertrauen kann, sondern vielmehr umgekehrt, dass die TCP-Allianz dem Computer ihres Kunden vertraut und die Kontrolle über dessen Datenverkehr besitzt.

Dass es auch anders geht zeigt der zunehmende Erfolg von sogenannter „Open Source Software“ wie z.B. Linux. Bei diesem Betriebssystem ist jede Funktion, jede Zeile Code offen gelegt und wird von der User-Gemeinde nur dann freigegeben, wenn allen Nutzerhinweisen nachgegangen wurde. So ist ein Betriebssystem entstanden mit eingebautem „peer group review“, ein Konzept dass sich seit Anbeginn der Naturwissenschaft bewährt hat. Erkenntnisse über die Vorteile dieser Architektur schlagen sich gegenwärtig in

immer mehr Nutzerentscheidung nieder. Nach der Grundsatzentscheidung der Bundesverwaltung für Open Source Software hat jetzt z.B. auch die Stadt München sich für ihren gesamten kommunalen Bereich dieser Richtung angeschlossen.

Dabei lässt auch die Palette von Anwendungsprogrammen unter Linux inzwischen keine Wünsche mehr offen. So können z.B. sämtliche MS-Office-Dokumente 1:1 gelesen, verarbeitet oder produziert werden. Medienbrüche zwischen der Windows-Welt und Linux sind auch für Endanwender inzwischen nahezu vollständig ausgeräumt. Hinzu kommt, dass aus Gründen der Lizenzgebühren, der Zuverlässigkeit und der Wartungsfreundlichkeit viele Rechenzentren schon ihre Client-/Serverarchitektur ganz stillschweigend auf Open Source Software umgestellt haben.

Was könnten jetzt Palladium und TCPA für den medizinischen Bereich bedeuten?

Zunächst kann der potenzielle Sicherheitsgewinn dieser Entwicklung vordergründig nicht bestritten werden. Dabei ist aber fraglich, ob die damit etablierten Strukturen mit den Pflichten der Informationsverarbeitung im Gesundheitswesen grundsätzlich in Einklang gebracht werden können.

Die Einhaltung der ärztlichen Schweigepflicht ist bekanntlich nicht delegierbar. Jeder Arzt muss selbst dafür Sorgen, dass durch ihn verarbeitete Patientendaten nicht in unberechtigte Hände gelangen können. In diesem Sinn hat auch die 50. Konferenz der Bundes- und Landesbeauftragten für den Datenschutz festgestellt, dass keine zentralen Sammlungen von personenbezogenen Patientendaten entstehen dürfen. Während in Amerika also der Health Insurance Portability and Accountability Act (HIPAA) von 1996 die Grundlagen für elektronische Patientenakten in großem Stil schafft, steht diese Diskussion in Deutschland noch weit vor einem absehbaren Ende. Angesichts der Erfahrungen aus einer noch nicht lange abgelegten Vergangenheit erscheinen Behutsamkeit und Bedacht hier zwingendes Gebot.

Jeder Einzelne muss für sich selbst entscheiden, inwieweit er heute selbstverständliche Rechte abgeben will, um an der elektronischen Welt des World Wide Web von Morgen teilzunehmen. Was will der Mensch für seine Identität und seine Sicherheit künftig investieren? Was ist er bereit, von seiner Privatsphäre preiszugeben? In welche Instanz kann er sein Vertrauen setzen? Will er für sich wählen oder Vorgesetztes einfach konsumieren?

Antworten auf diese und ähnliche Fragen werden kommende Generationen bis ins Mark hinein prägen. Nur ist „Man on the Street“ keinesfalls klar, dass diese Entscheidungen schon heute gefällt werden. Das Interesse der Öffentlichkeit an der aktiven Gestaltung ihrer eigenen Welt von Morgen hält sich in sehr engen Grenzen. Mehr noch, in vollständiger Fehleinschätzung ihrer eigentlichen Kurzsichtigkeit wird es Technikern und Wirtschaftsunternehmen überlassen, Fakten zu Schaffen, die durch keine Abstimmung mit einem wirklich informierten Bürgern legitimiert sind.

Als ob's Orwell schon gewusst hätte, oder täuscht sich hier nur der Verfasser?