Edda-Müller-Archiv

www.bayerischer-anwaltverband.de

Sicherheit in der Informationstechnik (2007)

Professor Dr. Edda Müller , Vorstand des Verbraucherzentrale Bundesverbandes (vzbv) e.V.

Statement anlässlich der internationalen Konferenz zum Thema „Sicherheit in der Informationstechnik" am 04. Juni 2007 im Auswärtigen Amt in Berlin
Motto des Panels: Shared responsibility among various players
Thema des Statements: The public´s responsibility

Sehr geehrte Damen und Herren,

über die Chancen und Risiken der Informationstechnik, speziell des Internets gibt es hier im Saal sicherlich keine unterschiedlichen Meinungen.

Bürgern und Verbrauchern bietet das Internet nahezu unbegrenzte Möglichkeiten zur Informationsbeschaffung, zum bequemen und jederzeitigen Einkauf und für den Meinungsaustausch etwa über die Qualität einer gekauften Ware oder einer genutzten Dienstleistung.

Wenn es um das Beherrschen der Risiken der Informationstechnik geht, postulieren die Veranstalter zu Recht eine geteilte Verantwortung des Staates, der Wirtschaft und der Nutzer.

Mir haben Sie den Part zugedacht, über die Verantwortung und den Beitrag der privaten Nutzer zur Gewährleistung der IT-Sicherheit zu sprechen. Ich stelle mich dieser Aufgabe gern.

Lassen Sie mich einleitend feststellen:
Verantwortung können Verbraucher nur für solche Risiken übernehmen, die sie zur Risikovermeidung und – Risikominimierung tatsächlich auch beeinflussen können.

Zur Verdeutlichung, was in diesem Sinne machbar ist und was nicht, will ich ein paar **gebräuchliche Praktiken und Gefahren** aufzeigen, mit denen Verbraucher bei der Internet-Nutzung konfrontiert werden. Dabei will ich mich nicht auf rein technisch bedingte Risiken beschränken:

- Es beginnt damit, dass Internetnutzer die wahre **Identität eines Online-Anbieters** oder die **Authentizität einer Internetseite** nicht ohne Weiteres zweifelsfrei erkennen können.
  Das macht vor allem den **Passwort-Klau** (engl. **Phishing**) oder das **Spammen** so leicht.

- Beim **Phishing** werden vorzugsweise Online-Bankkunden mittels eMail kontaktiert, um sie auf gefälschte Webseiten zu führen und so an Kontonummern und Zugangsdaten heranzukommen.

- Eine besondere Variante des Phishing ist der sogenannte „**Identitätsklau**". Dabei versuchen Kriminelle, an sensible Daten heranzukommen, die einer bestimmten Person zugeordnet sind. Das können Kreditkartendaten, Sozialversicherungsnummern oder – mit Blick in die Zukunft – Daten biometrischer Merkmale sein. Mit diesen Daten können dann auf Kosten der Betroffenen dubiose Geschäfte gemacht oder Personen gezielt diskreditiert oder gar erpresst werden.

- Beim **Spammen** wird sehr häufig der Absender einer Mail und der wirkliche Betreff verschleiert. Damit soll der Adressat zum Öffnen der Nachricht animiert werden. Gehen die Angeschriebenen darauf ein, finden sie im günstigsten Fall ein Angebot zum Kauf dubioser Produkte. Viele Empfänger von Spam-Mails sind auch schon auf gefälschte Rechnungen hereingefallen. Oder sie haben sich mittels eines vorschnellen Mausklicks ein Schad- oder Spionageprogramm einge-

fangen.

- Eine unseriöse Geschäftspraktik, mit der sich der Verbraucherzentrale Bundesverband und die Beratungsstellen der Verbraucherzentralen bis heute beschäftigen, sind **Abo-Fallen im Internet**. Da werden von windigen Firmen Dienste angeboten, deren Nutzung auf den ersten Blick kostenfrei erscheint. Wer gutgläubig auf ein solches Angebot eingeht, erkennt meist erst anhand einer später eintreffenden Rechnung, dass er ein völlig überteuertes Jahresabonnement eingegangen ist. Nicht nur viele Kinder und Jugendliche, sondern auch Erwachsene sind schon auf diesen Trick hereingefallen.

- Die digitale Revolution im Medienbereich hat zu einer zunehmend einseitigen Gestaltung des **Urheberrechts** zu Lasten der Nutzer geführt. Immer mehr Internet-Nutzer, darunter vor allem Kinder und Jugendliche, verstricken sich unbeabsichtigt im solchermaßen verschärften Regelwerk. Beispielsweise bei der unbeabsichtigten Nutzung illegaler Musik- oder Videoplattformen im Internet. Oder beim Einstellen von nicht unmittelbar erkennbarer urheberrechtlich geschützter Inhalte auf die eigene Webseite. Manche Eltern sahen sich daraufhin schon mit zum Teil horrenden Schadenersatzforderungen von Rechteinhabern und deren Anwälten konfrontiert.

Dies exemplarisch zu den Risiken und Nebenwirkungen einer an sich **wertfreien Technik**, die in ihrer praktischen Anwendung jedoch mit **erheblichen Risiken** und mit zum Teil **weitreichender Intransparenz** für die Nutzer verbunden ist.

Was Verbraucher tun können, um die IT-Sicherheit positiv zu beeinflussen

Zu einem gewissen Grad können private Internetnutzer ihre Hard- und Software durch zusätzliche Maßnahmen schützen. Auch sollten sie sich **risikobewusst im Internet bewegen**. Dies setzt **öffentliche Aufklärung** und **individuelle Information** voraus: Aufklärung durch Anbieter von Hard- und Software, durch Internet-Service-Provider, aber auch durch Behörden und Verbraucherorganisationen.

Diese Aufklärung wirkt allerdings nur dann im gewünschten Sinne, wenn der Nutzer informationswillig und bereit ist, in grundlegende Schutzmaßnahmen wie **Anti-Viren Programme**, **Firewall, Spam- und andere Filter** zu investieren. Auch sollte er nicht

leichtfertig auf unbekannte Webseiten oder intransparente Angebote klicken. Schließlich sollte er verantwortungsbewusst mit seinen persönlichen Daten, Passwörtern und vergleichbaren Zugangsdaten umgehen. Dies erfordert allerdings eine umfassende Transparenz über die Datenschutzpolitik der Anbieter.

Besonderen Schutz bei der Internetnutzung bedürfen Kinder und Jugendliche. Sei es vor der Datensammelwut wissbegieriger Unternehmen, vor unseriösen Diensteanbietern, vor entwicklungsbeeinträchtigenden Inhalten, vor Kontaktversuchen Krimineller in Chatrooms oder Foren und – derzeit besonders aktuell - vor einem unbeabsichtigten Verstoß gegen Urheberrechte Dritter. Daher sind die Eltern und Erzieher gefordert, zunächst sich selbst und dann die Kinder über die wesentlichen Risiken in der Online-Welt zu informieren. **Kinder sollten vor dem Bildschirm nicht allein gelassen,** und es sollte für einen **ausreichenden Zugangsschutz** durch wirksame **Filtersoftware** gesorgt werden.
Die Schulen wiederum haben eine wichtige Funktion in der Vermittlung einer **umfassenden Medienkompetenz**.

Maßnahmen zum Schutz von Kindern und Jugendlichen bei der Internetnutzung sehen wir als Teil einer optimierten IT-Sicherheit an. Daher begrüßen wir ausdrücklich das Projekt „**Ein Netz für Kinder**", eine gemeinsame Initiative der Bundesregierung und der Wirtschaft, und vergleichbare Projekte.

Was Verbraucher nicht tun können

Bei der Bewertung dessen, was private Internet-Nutzer zur Verbesserung der IT-Sicherheit beitragen können, dürfen wir nicht vergessen, dass wir es mit **informationstechnischen Laien** zu tun haben. Was die Verbraucher nicht kennen können, was sie als selbstverständlich voraussetzen oder worauf sie keinen unmittelbaren Einfluss haben, zu dessen Sicherheit können oder werden sie durch eigenes Zutun auch nichts beitragen.

In der realen Welt geht der Verbraucher von der **gesundheitlichen und wirtschaftlichen Unschädlichkeit** von Produkten oder Dienstleistungen aus. Bei der Nutzung von Informationstechnik und im Internet ist das anders. Da werden Produkte und Dienste angeboten, die ohne Nachrüstung durch den Nutzer ein **erhebliches**

Risikopotential beinhalten. Ich vergleiche das mit einem Autohersteller, der seine Fahrzeuge mit unzureichenden Bremsen ausrüstet und von den Käufern erwartet, dass sie die Fahrzeuge auf eigene Kosten entsprechend nachbessern. Die Mehrzahl der privaten IT-Nutzer verfügt aber weder über die Fähigkeiten noch hat sie erforderlichen Detailkenntnis, um Geräte, Programme gegen Attacken krimineller Angreifer wirksam zu schützen. Daher ist es zum Beispiel wichtig, dass Hard- und Software bei der Auslieferung mit **optimaler Sicherheitseinstellung** für die Online-Nutzung versehen sind.

Was wir von Wirtschaft und Politik erwarten

Manche IT- Produkte und -Systeme haben zweifellos Nachbesserungsbedarf in punkto IT-Sicherheit. Das gilt nicht nur für Softwarelieferanten. Erst kürzlich sind Sparkassen in Bezug auf die Sicherheit ihrer Webseiten in die Kritik von Sicherheitsexperten geraten. Nach dem Urteil der Experten sollen sich die überprüften Institute nicht genügend um die Sicherheit ihrer Banking-Portale gekümmert haben. Angesichts der Erfahrungen mit Phishing ist man da geradezu fassungslos. Dass die Kunden die finanziellen Konsequenzen einer unzureichenden Sicherheitspolitik ihrer Bank ausbaden sollen, ist für uns jedenfalls völlig inakzeptabel.

Positiv aufgenommen haben wir die Empfehlungen des nationalen IT-Gipfels vom Dezember 2006 zur IT-Sicherheit. Vorgeschlagen wurden dort unter anderem eine Verbesserung des Identitätsschutzes, die Anpassung des Computerstrafrechts an neue Bedrohungsszenarien und die Verbesserung der Datensicherheit und des Datenschutzes.

Besonders begrüßt haben wir die im März des Jahres vom Bundesverbraucherschutzministerium vorgestellte Charta der Verbrauchersouveränität in der digitalen Welt. In punkto IT-Sicherheit verpflichtet die Charta die Unternehmen insbesondere ...

- zur **größtmöglichen Risikominimierung** mittels Auswahl effektiver Sicherheitssysteme,

- zur **frühzeitigen Information der Kunden über aktuelle Sicherheitsrisiken** vor allem bei sensiblen Online-Geschäften,
- zum **effektiven Schutz vertraulicher und personenbezogener Daten** vor unbefugtem Zugriff.

Ich fasse zusammen: IT-Sicherheit und Datenschutz müssen permanent den veränderten Bedingungen in der digitalen Welt angepasst werden. Entwicklungen wie …

- das „**web2**" mit seinen virtuellen Welten,
- die **biometrische Identifikation,** vor allem dann, wenn die biometrische Daten in zentralen Datenbanken gespeichert und verarbeitet werden sollen,
- **RFID** oder das „**Internet der Dinge**"[1], bei dem vernetzte Computerintelligenz in Produkte des täglichen Lebens einziehen wird[2],

zeigen schon heute den diesbezüglichen Bedarf auf.

Vielen Dank für Ihre Aufmerksamkeit. Ich freue mich auf die Diskussion.

[1] engl. „internet of things" oder auch „ubiquitous computing"
[2] Beispiele hierfür sind das „intelligente", energieeffiziente und einbruchssichere Haus oder der „intelligente" Kühlschrank, der Lebensmittel selbstständig nachbestellt