Wir leben nicht in einer perfekten Welt

Muß der Staat bei elektronischen Geschäftsprozessen reglementieren oder bieten die Unternehmen schon ein angemessenes Maß an Vertrauenswürdigkeit für unsere Informations- und Wissensgesellschaft

Wir leben nicht in einer perfekten Welt, das wissen wir. Aber wir haben gelernt, mit dieser Tatsache in der realen Welt verantwortungsvoll umzugehen und uns ein grundlegendes Maß an Sicherheit zu schaffen.
Doch was müssen wir tun, um in der neuen 'elektronischen Welt' eine äquivalente Sicherheit zu bekommen, damit wir die Chancen, die die neuen Konzepte uns bieten, sinnvoll nutzen können?

Eine perfekte Welt gibt es nicht.

In einer perfekten Welt würden Vertrauen und Freundlichkeit regieren, wären alle Informationen frei für jeden verfügbar, würde sich niemand zu Lasten anderer bereichern, würden alle Kunden den gewünschten und angemessenen Preis für Waren und Dienstleistungen gern zahlen, wäre der Wettbewerb transparent, fair und ausgeglichen.

Die reale Welt sieht anders aus: Information und Wissen – und damit Macht – sind ungleich verteilt, Einbruch und Diebstahl gefährden Eigentum, Betrug und Verrat gehören zum Geschäftsleben, Terror und Gewalt bedrohen unseren Alltag. Aber wir haben im Laufe der Zeit gelernt, damit umzugehen und uns angemessen zu schützen.

Wie schützen wir uns in der realen Welt?

Pförtner sorgen dafür, dass kein Unbefugter ein Firmengelände betritt, verschlossene Schränke und Safes dienen zur sicheren Aufbewahrung wertvoller Güter (Geld, Sachwerte, Informationen und sonstige Unternehmenswerte), Sicherheitstransporter schützen die Werte während des Transports.

Standes- und Einwohnermeldeämter sichern die eindeutige und überprüfbare Identität von Personen: Das Standesamt sorgt dafür, dass wir über unseren Vor- und Nachnamen, den Geburtsort und das Geburtsdatum eindeutig identifizierbar sind. Das Einwohnermeldeamt gibt Ausweise heraus, die es ermöglichen, diese eindeutige Identität zweifelsfrei zu beweisen.

Verschlossene Briefumschläge sorgen für den vertraulichen Austausch von Information, eigenhändige Unterschriften für ihre Verbindlichkeit. Wir wissen, dass diese Verbindlichkeit sich auch auf Handlungen erstreckt, die durch ein Schreiben ausgelöst oder vollstreckt werden, z.B. im Geschäfts- oder Rechtsverkehr.

Reale versus elektronische Geschäftswelt

Ein besonders wichtiger Punkt in einer funktionierenden Gesellschaft ist die Vertrauenswürdigkeit – in der Geschäftswelt wie im alltäglichen Umgang miteinander.

In der realen Welt haben wir von klein auf gelernt, welche Bedeutung eine eigenhändige Unterschrift hat und wie wir mit Hilfe persönlicher Kontakte und intuitiver Einschätzung Vertrauenswürdigkeit bewerten, um mehr Sicherheit zu erlangen.

In der elektronischen Welt können wir auf die bewährten Mechanismen nicht zurückgreifen, da wir indirekt über Netze wie z.B. das Internet kommunizieren. Wir wissen nicht sicher, mit wem wir kommunizieren und wer möglicherweise die Kommunikation abhört oder manipuliert. Das heißt, dass wir die grundlegenden Sicherheitsbedürfnisse anders befriedigen müssen als in der realen Welt.

Welchen neuen Herausforderungen stehen wir in der elektronischen Welt gegenüber?

Wir erleben zurzeit einen fundamentalen Wandel zur Informations- und Wissensgesellschaft. Wir müssen uns bewusst werden, dass immer mehr Geschäftsprozesse mit Hilfe von IT-Systemen über das Internet abgewickelt werden. Damit nimmt auch die Notwendigkeit zu, IT-Sicherheitsmaßnahmen in angemessener Weise zu verwenden, damit in der elektronischen Welt eine Basis der Vertrauenswürdigkeit herrschen kann.

Eine weitere Herausforderung ist das häufig mangelnde Unrechtsbewusstsein in der elektronischen Welt. Wer in der realen Welt Unternehmenswerte entwenden will, der muss über Zäune klettern, Türen und Fenster aufbrechen, vielleicht sogar Tresore sprengen. Jedem, der so etwas tut, ist bewusst, dass er eine Straftat begeht! In der elektronischen Welt sitzen die Hacker bzw. Cracker mit Kaffee und Keksen vor dem Bildschirm und tun das Gleiche, aber sie haben dabei häufig nicht das Gefühl, etwas Unrechtes zu tun. Die Hemmschwelle ist niedriger, dadurch steigt die Wahrscheinlichkeit von Angriffen.

Wie können wir uns in der elektronischen Welt angemessen schützen?

Die oben genannten Sicherheitsmechanismen, die wir aus der realen Welt kennen, sind analog auch in der elektronischen Welt verfügbar:

Es gibt Sicherheitsmechanismen, die jede Organisation in ihrer eigenen Verantwortung nutzen kann: Das sind:

Firewall- und PC-Sicherheitsysteme – als elektronische Pförtner – verhindern den unerlaubten Zugriff von außen auf die internen IT-Einrichtungen einer Organisation.

Datei- und Festplattenverschlüsselung sorgen als digitaler Tresor für eine sichere Aufbewahrung der elektronischen Informationen.

Sogenannte Virtual Private Networks (Kommunikationsverschlüsselungseinheiten) schützen sie, ähnlich wie ein Sicherheitstransporter, während der Übertragung vor Manipulation und unerlaubter Einsichtnahme.

Es gibt aber auch Sicherheitsmechanismen, die auf eine gemeinsame Infrastruktur zurückgreifen müssen. Das sind z.B.:

Public Key Infrastructures (PKIs) und deren Anwendungen sorgen wie Standes- und Einwohnermeldeämter für die eindeutige und sichere Identifikation von Geschäftspartnern im Internet.

Beispiele von PKI-Anwendung sind z.B.: Verschlüsselte E-Mails, welche einen vertraulichen 'Briefverkehr' ermöglichen. Elektronische Signaturen gewährleisten die Verbindlichkeit und damit eine höhere Rechtssicherheit.

In den letzten Jahren wurden in vielen großen Unternehmen PKIs eingerichtet. Zu Beginn dieser Entwicklung standen die PKI als Ziel beim Anwender im Vordergrund. Die PKI ist zwar vorhanden, aber hat in vielen Fällen nicht den gewünschten Nutzen erbracht. Probleme waren die technische sowie die organisatorische Interoperabilität sowie die richtige Strategie der Einführung.

Zwei Initiative, die pragmatisch die Interoperabilitätsprobleme lösen, sind: die Spezifikation ISIS-MTT auf technischer und die Initiative "European Bridge-CA" auf organisatorischer Ebene.

Die ISIS-MTT-Spezifikation basiert auf internationalen Standards (S/MIME, PKIX, PKCS, X.509, ETSI, CEN ESI etc.) Sie besteht aus einer Kernspezifikation, welche die Grundanforderungen aller Anwendungskategorien abdeckt, und Erweiterungen für die verschiedenen Anwendungen (z.B. elektronische Signatur, E-Mail-Verschlüsselung). Darin werden ausschließlich Festlegungen getroffen, die in den bestehenden Standards nicht hinreichend eindeutig geregelt sind (siehe www.teletrust.de)

Eine zweite wichtige Initiative ist die "**European Bridge-CA**", die sich das Ziel gesetzt hat, die Interoperabilität zwischen PKIs pragmatisch zu lösen. Die European Bridge-CA wird von der TeleTrusT betrieben und wir schon von über 20 großen Organisationen unterschiedlicher Industriezweige und der öffentlichen Verwaltung genutzt. Das Ziel der europäischen Bridge-CA ist es, eine "Brücke des Vertrauens" zwischen verschiedenen PKIs weltweit herzustellen, indem sie minimale Policy-Anforderungen und technische Vorbedingungen definiert, die eine sichere Kommunikation über organisatorische Grenzen hinweg erlauben.

Was kann oder muss der Staat tun?

Damit wird für den nächsten Schritt in die Informations- und Wissensgesellschaft mit einem angemessenen Risiko eintreten stellt sich die Frage, inwieweit der Staat hier reglementieren kann oder muß.

Soll die Sicherheitsinfrastruktur vom Staat gefördert werden?

Die Bundesregierung könnte z.B. durch die Ausgabe von Personalausweisen mit SmartCard dafür sorgen, das jeder Bürger in die Fähigkeit gebracht wird sich eindeutig und sicher in der elektronischen Welt, im Internet, darstellen und alle PKI-Anwendungen nutzen kann.

Anwendungen der Verschlüsselung und der elektronischen Signatur

Die Bundesregierung könnte ähnlich wie im Straßenverkehr durch die Anschallpflicht im Auto die Verschlüsselung von E-Mail fordern und die elektronische Signatur für bestimmte elektronische Geschäftsprozesse zwingend machen.

Durch solche Maßnahmen wird das Risiko für die Informations- und Wissensgesellschaft minimiert. Dies wird sich sicherlich auch auf den zurzeit schlechten Markt (E-Business, E-

Commerce) positiv auswirken, weil dann das potentielle Rationalisierungspotential risikoärmer durch die Unternehmen und Organisationen ausgeschöpft werden kann.

Zusammenfassung

Wenn wir die Vorteile der elektronischen Welt – der *Informations- und Wissensgesellschaft* – ausschöpfen möchten, müssen wir, ähnlich wie in der realen Welt, das Risiko begrenzen. Das heißt, wir müssen geeignete Sicherheitslösungen einsetzen und dafür sorgen, dass ihre Entwicklung der Risikobegrenzung mit der Entwicklung ihres Umfelds, dem Internet, Schritt hält. Die Bundesregierung kann hier durch geeignete Maßnahmen einen wichtigen Impuls setzen.

Autor:

Dr. Norbert Pohlmann
(Vorstandsvorsitzender von TeleTrusT e.V.,
Vorstand Utimaco Safeware AG)