PKI in der Datenschutzpraxis

Kerstin Blossey[1], Christian Weber[2]

Verimax GmbH, Bereich Datenschutz

[1]kerstin.blossey@verimax.de

Verimax GmbH, Bereich PKI-Lösungen

[2]christian.weber@verimax.de

Zusammenfassung

PKI in der Datenschutzpraxis ist die Philosophie einer heute bereits verfügbaren Technologie, um die scheinbar konträren Aspekte Informationsfreiheit und Sicherung von Daten und Informationen in Form sinnvoller Zugriffs- und Verarbeitungsregelungen miteinander zu verbinden. Leistungsfähigkeit und duale Sicherheit (Sicherheit des Systems und seiner Benutzer) sind nach Dierstein gleichrangige Konstruktionsprinzipien sicherer IT-Systeme. Die vielfältigen Einsatzmöglichkeiten zertifikatsbasierter Lösungen in Industrie, Wirtschaft, Medizin, Verwaltung und den fast allen anderen Disziplinen können nicht nur wirksame Hilfe bei der Umsetzung gesetzlicher Datenschutzvorschriften sein:

IT-Sicherheitselemente wie die Verschlüsselung vertraulicher Personen- oder Unternehmensdaten schützen geldwerte Informationen vor den neugierigen Augen von Mitbewerbern oder unloyalen Mitarbeitern. Der Risikofaktor Mensch, wie Kevin Mitnick ihn in unzähligen Praxisbeispielen umreißt, kann als Leck in der Wertschöpfungskette empfindlichen Schaden anrichten. Absolute Daten- und IT-Sicherheit gibt es nicht, jedoch kann ein sinnvolles Schutzziel mit angemessenen Maßnahmen, etwa einer niederschwelligen PKI-Lösung, erreicht werden, bevor der Schadensfall eintritt und der erforderliche aktuelle Notfallplan fehlt. Schaden vermeiden sollte die Devise sein, gerade nach den Anforderungen des Bundesdatenschutzgesetzes. Daten signieren, bei Bedarf verschlüsseln, stellt für Sender und Empfänger zugleich Authentizität, Vertraulichkeit, Integrität und Nichtbestreitbarkeit sicher.

Der voraus denkende Geschäftsleiter kann mit Blick auf die Nachvollziehbarkeit digitaler Geschäftsprozesse mit der Einführung einer PKI die Weichen im Unternehmen für die Zukunft richtig stellen. Arbeiten Datenschutzbeauftragter und IT-Sicherheits-Beauftragter kooperativ zusammen, entsteht als Produkt der beweisfähige Workflow - im Sinne des nach KonTraG längst eingeforderten Riskmanagements. Dies ist ein entscheidendes Element für die Geschäftsleitung, um die Zukunftssicherheit des Unternehmens zielorientiert und nachhaltig zu fördern, vor allem in seiner Bonität.

Der in vielen Bereichen inzwischen bevorzugte elektronische Weg zur Abwicklung von Verträgen und Verwaltungsakten erfordert darüber hinaus einen adäquaten Ersatz zur handschriftlichen Unterschrift im Sinne des BGB, welche ebenfalls via einer Public-Key-Infrastruktur in weiten Bereichen mit geringem Risiko realisierbar ist. Eine Wandlung im Bereich der Verwaltungsvorgänge im eGovernment ist bereits in der öffentlichen Diskussion, z.B. die sichere Übertragung von Steuer- und Finanzdaten. Der verantwortungsbewusste Umgang mit sensiblen Personen- und Unternehmensdaten ist nicht länger Fleißaufgabe, sondern Kennzeichen von Seriosität und Vertrauenswürdigkeit.

1 Hinführung zum Thema ... 3
1.1 Datenschutz – Grundlagen ... 4
1.1.1 Personenbezogene Daten und ihre Verarbeitung ... 4
1.1.2 Schutz personenbezogener Daten ... 4
1.2 Datenschutz und Datensicherheit ... 4
1.3 Datenschutz – warum jetzt? ... 5
2 Public-Key-Infrastruktur (PKI) ... 5
2.1 Skizzierung des generellen Verfahrens ... 6
2.2 Elektronische Signaturen ... 6
2.2.1 Signatur-Modelle ... 6
2.2.2 Zertifizierungsdienste-Anbieter ... 8
2.2.3 Sicherheitsanforderungen an technische Komponenten ... 8
2.3 PKI – warum jetzt? ... 9
3 PKI als praktizierter Datenschutz ... 10
3.1 Aus Sicht des Verbrauchers ... 10
3.2 Aus Sicht des Anbieters ... 11
3.3 Aus Sicht der Geschäftsleitung ... 13
3.3.1 Technikfolgenabschätzung ... 14
3.3.2 Aufwandsabschätzung und Wettbewerbsvorteil ... 14
4 Fazit und Ausblick ... 15

1 Hinführung zum Thema

„Es ist sicherer, zu wenig als zu viel zu wissen.

– Mit Sicherheit war der Urheber dieses Zitates kein IT-Sicherheits-Spezialist“.

Dieses Zitat ist auf einer Internetseite aus der IT-Branche zu lesen. Die Reaktionen auf diese These(n) werden sich in mindestens drei Lager spalten:

- Die Pragmaten („Was ich nicht weiß, macht mich nicht heiß…“),
- die Sammler („Es ist mein Job, jederzeit über möglichst viele Sachverhalte aktuelle Informationen zu verfügen.“) und
- die Engagierten („Nicht alle Informationen dürfen uneingeschränkt jedermann zu jedem Zweck verfügbar sein oder gemacht werden.“).

Die unternehmensspezifische Wirtschaftlichkeitsbetrachtung gibt einen anderen Maßstab vor: Jeder muss jederzeit genau auf die Daten und Informationen Zugriff haben, die er für seine Arbeit benötigt.

Die Aspekte Nichtbestreitbarkeit, Integrität, Vertraulichkeit und Authentizität sind es, auf die Unternehmen öffentlicher oder privater Natur aufbauen und deren Sicherung das Bundesdatenschutzgesetz (BDSG) einfordert. Geschäftsprozesse müssen flexibel sein, anpassungsfähige Strategien sind eine Voraussetzung für wirtschaftlichen Erfolg. Die automatisierte Verarbeitung von Personen- und Unternehmensdaten ist hierfür ein wichtiges Medium. „Schutzziel versus Kostenmatrix“ lautet die Formel, nach der die nachhaltig orientierte Geschäftsleitung vorzugehen hat – neben der IT-Sicherheit immer auch betriebswirtschaftliche Anforderungen im Blick, nicht zuletzt auf Grund des vielfach über Kreditmittel entscheidenden Rankings und des von den Kreditinstituten hoch bewerteten Riskmanagements.

Wie also soll man mit Informationen und Daten verfahren, um den gesetzlichen Anforderungen ebenso wie den wirtschaftsökonomischen Ansprüchen und privaten Interessen angemessen gerecht werden zu können? Das BDSG – flankiert von einer Fülle an Verordnungen, länder- und bereichsspezifischen Gesetzen und Vorschriften, ist der rechtliche Maßstab, wie allen Beteiligten und Betroffenen genüge zu tun ist, wenn es um personenbezogene Daten geht.

Wie gelingt der Spagat zwischen dem Aufgabenprofil eines IT-Sicherheits-Spezialisten und dem eines Datenschutzbeauftragten, also einerseits der sorgfältige sparsame Umgang mit allen personenbezogenen Daten und andererseits die optimale Nutzung – ebenso personenbezogener Daten – zu Unternehmenszwecken wie der Personalverwaltung, Kostenerhebung, Leistungsprofile, Markt- und Verbraucherverhaltensanalysen und vieler anderer Möglichkeiten, die moderne Informationstechnologien zur Selbstverständlichkeit werden lassen?

Neben vielen anderen Aspekten des Datenschutzes ist ein produktiver und zeitgemäßer Ansatz für eben diese Problemstellung der Einsatz einer Public-Key-Infrastruktur (PKI). Die Signierung und gegebenenfalls Verschlüsselung von Daten ist eine Alternative, die - längst einsatzbereit, bedienbar und bewährt – alle datenschutzrechtlichen Erfordernisse nach §9 BDSG erfüllt, aber vielfach nicht etabliert ist, weil der Wert von Daten noch immer nicht in Verbindung mit ihrem Schutz im Sinne einer sicheren Informationsübermittlung gebracht wird.

1.1 Datenschutz – Grundlagen

Das Bundesdatenschutzgesetz (BDSG) regelt bereits seit der Novellierung von 2001, wie mit personenbezogenen Daten automatisiert zu verfahren ist. Es gibt länder- und bereichsspezifische Vorschriften, Kontrollinstanzen, fachlich spezialisierte Dienstleister und eine Vielzahl von Hilfestellungen zur Umsetzung der gesetzlichen Anforderungen in öffentlichen wie nichtöffentlichen Einrichtungen und Unternehmen. Auch die Konsequenzen, die eine Missachtung der gesetzlichen Vorgaben hat und welche unabdingbaren Rechte der Betroffene hat, sind klar definiert. Sehen wir uns daher ein paar Aspekte des Datenschutzgesetzes genauer an.

1.1.1 Personenbezogene Daten und ihre Verarbeitung

Als personenbezogene Daten werden nach §3 BDSG solche Daten bezeichnet, die „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“ sind. Information dieser Art fallen in jedem Unternehmen und jeder Institution an, ob Behörde, Firma, Arztpraxis oder Verein.

Als automatisierte Verarbeitung im Sinne des BDSG sind sowohl die Verarbeitungsvorgänge in elektronischen Systemen als auch nichtelektronische Aufbewahrungsformen definiert, wenn sie automatisiert sind, wie etwa in strukturierten Karteien. Unter Verarbeitung versteht der Gesetzgeber die Erhebung, Verarbeitung (Speicherung, Veränderung, Übermittlung, Sperrung und Löschung) und Nutzung. Der Begriff der „Speicherung“ beinhaltet laut BDSG das „Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger“.

1.1.2 Schutz personenbezogener Daten

Der Begriff „Datenschutz“ ist mittlerweile mehrfach belegt, so dass eine eindeutige Definition generell nicht vorausgesetzt werden kann. Nach BDSG bedeutet er sowohl den verfahrensmäßigen, als auch den informationstechnischen (§9 und Anlagen) Schutz personenbezogener Daten vor Missbrauch. Zugleich wird das Recht des Bürgers geregelt, selbst über Preisgabe und Verwendung seiner Personendaten zu entscheiden.

Zur Umsetzung angemessener Datenschutzmaßnahmen nach BDSG sind alle Unternehmen, Vereine und weiteren Einrichtungen verpflichtet. Sind mehr als vier Mitarbeiter mit der Nutzung personenbezogener Daten beschäftigt, ist sogar die Bestellung eines fachkundigen, zuverlässigen Datenschutzbeauftragten vorgeschrieben. Werden besondere Arten personenbezogener Daten nach §9 Abs. 9 verarbeitet (z.B. ethnische Herkunft, politische Meinung oder philosophische Überzeugung), gelten noch strengere Vorschriften. Verstöße gegen das BDSG und flankierende Gesetzgebung werden mit Schadensersatz, Bußgeldern bis hin zu Strafen und Freiheitsentzug nach StGB geahndet (§43 ff).

1.2 Datenschutz und Datensicherheit

Mit dem sozialökonomischen Schutz personenbezogener Informationen und Daten ist es jedoch im Sinne des BDSG nicht getan. Der Gesetzgeber schreibt zugleich technische Sicherheitsmaßnahmen vor, insbesondere im bereits erwähnten §9 sowie der zugehörigen Anlage, die im Grunde einen kompletten Überblick über den Bereich IT-Security gibt, wie folgende Grafik zeigt:

Abb. 1: Datensicherheitsanforderungen nach §9 BDSG

1.3 Datenschutz – warum jetzt?

Das rechtswirksame BDSG stammt bereits von 2001, doch diverse Gründe ließen das Thema nur wenig publik werden, insbesondere bei Unternehmen. Mangelnde Kontrollen unterstützten die Untätigkeit. Oft wurde auch die in §45 BDSG festgelegten Übergangsfristen (z.B. der 23. Mai 2004) zur Einführung erforderlicher datenschutzrechtlicher Maßnahmen vorgeschoben. Viele sahen daher bisher keinen Handlungsbedarf. Doch aktuelle Trends machen erforderlich, dass die Geschäftsleitungen tätig werden und prüfen, in welchem Maß das eigene Unternehmen zum Datenschutz verpflichtet ist und diese Maßnahmen auch realisieren.

Die Frage muss daher nicht lauten: „Warum Datenschutz jetzt?“, sondern viel mehr: „Warum bisher *kein* Datenschutz?“.

2 Public-Key-Infrastruktur (PKI)

Der Begriff „Public-Key-Infrastruktur“ (PKI) ist längst kein Fremdwort mehr für IT-Sicherheits-Spezialisten. Gerade mit der zunehmenden Verlagerung vieler Geschäftsprozesse auf digitale Wege wird es immer wichtiger, die Kommunikation über ein unsicheres Medium sicher zu gestalten. Um Dienste wie E-Mail oder Internet – ebenso wie unternehmensinterne Abläufe – möglichst beweisfähig und rechtssicher zu gestalten, müssen Vertraulichkeit der Nachricht, die Integrität des Inhalts sowie Authentizität der am Prozess Beteiligten gewährleistet sein. PKI ist hierfür praxistaugliche und finanziell interessante Lösung, die auch Medienbrüche der Vergangenheit angehören lässt.

2.1 Skizzierung des generellen Verfahrens

Hinter der Bezeichnung „PKI“ (Public Key Infrastructure) steckt der Gedanke, dass ein Benutzer sich gegenüber einer vertrauenswürdigen anerkannten Stelle – landläufig „Trustcenter“ genannt – authentifiziert, welche ihm daraufhin einen öffentlichen und einen privaten digitalen Schlüssel zum Beispiel auf einer Smartcard aushändigt. Die Karte wiederum schützt den Zugriff auf den privaten Schlüssel durch eine PIN. Der öffentliche Schlüssel wird - wie auch das Zertifikat in der PKI-Lösung - veröffentlicht. Eine Liste der gesperrten Zertifikate wird ebenfalls veröffentlicht.

Der „private key“ wird ausschließlich vom Eigentümer genutzt. Er dient zum Entschlüsseln empfangener, mit dem öffentlichen Key verschlüsselter, Nachrichten ebenso wie zur digitalen Unterschrift. Aus diesem Grund muss der private digitale Schlüssel unbedingt vor Dritten sicher verwahrt werden. Darüber hinaus muss sichergestellt werden, dass auch Trustcenter und weitere beteiligte Regulierungsstellen keinen Zugriff auf diesen Schlüssel haben, um einen Missbrauch von möglichst jeder Seite ausschließen zu können.

Der öffentliche Schlüssel wird neben der Verschlüsselung von Nachrichten an den Eigentümer auch zur Überprüfung der digitalen Signatur benutzt. Das Zertifikat ist das Pendant zu einer persönlichen Identifikationskarte wie etwa einem Personalausweis. Es enthält eine eindeutig zuordenbare Seriennummer und den amtlich beglaubigten Namen des Inhabers, den public key sowie die digitale Unterschrift eines vertrauenswürdigen anerkannten Dritten, - in der Regel eines Trustcenters.

Mittels Verschlüsselung und qualifizierter Zertifizierung durch ein anerkanntes Trustcenter kann aber nicht nur das Lesen online verschickter Nachrichten reguliert werden. Die PKI-Lösung ermöglicht zugleich eine digitale Unterschrift, mit der auch elektronische Vertrags-, Zahlungs- oder Verwaltungsvorgänge einer bestimmbaren Person zuordenbar gemacht werden können. Damit sind die zertifikatbasierten Lösungen rund um PKI ein interessantes Werkzeug für den Schutz sensibler Daten.

2.2 Elektronische Signaturen

Analog zur Bedeutung und dem Wert von Informationen gibt es Unterschiede in der Qualität von Signaturen. Diese Unterschiede sind in der Art der Signatur als auch in der verwendeten Hard- und Software begründet. Mit einer sorgfältigen Wahl der Qualitätsstufe kann ein angemessenes Schutzniveau erreicht werden, ohne unnötige Kosten durch oversized-Lösungen.

2.2.1 Signatur-Modelle

Die elektronische Signatur definiert sich nach §2 SigG als „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen“. Folgende verschiedenen Arten der elektronischen Signatur werden in der Praxis unterschieden:

Abb. 2: Vergleich der Signaturarten

- **Einfache Signatur**

Einfache elektronische Signatur sind Angaben des Signaturerstellers über seine Identität. Das heißt, bereits bei der Angabe der Informationen zum Namen und der Firmenzugehörigkeit des Absenders im Footer oder Anhang einer E-Mail handelt es sich um eine einfache Form der digitalen Signatur. Hier ist noch keine zusätzliche Hard- und Software zum Erstellen notwendig.

- **Fortgeschrittene Signatur**

Bei fortgeschrittenen elektronischen Signaturen müssen nach §2 SigG folgende Kriterien erfüllt sein:

Die digitale Signatur muss

- ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sein,
- die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
- mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann und
- mit den Daten, auf die sie sich bezieht, so verknüpft sein, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Bei fortgeschrittenen Signaturen ist also bereits vom Gesetzgeber eine Messlatte angebracht worden, die in der Praxis als Maßstab für die Qualität einer digitalen Unterschrift gilt. Um dieses Niveau zu erfüllen, wird eine fortgeschrittene Signatur ausschließlich mit einer geschützten Hardware erstellt und über eine Software so implementiert, dass eine Veränderung des Dokumentes und der Signatur eindeutig nachvollzogen werden kann.

- **Qualifizierte Signatur**

Der Unterschied zwischen einer fortgeschrittenen elektronischen und einer qualifizierten Signatur liegt in der Anforderung des Gesetzgebers nach einem zum Zeitpunkt der Erzeugung des gültigen qualifizierten Zertifikats für den Signaturinhaber. Bei der Erstellung einer qualifizierten Signatur muss sich der Antragsteller daher mit einem entsprechenden amtlichen Ausweisdokument identifizieren, damit ein Zertifikat erstellt werden kann.

- **Akkreditiert qualifizierte Signatur**

Die akkreditierte, qualifizierte elektronische Signatur unterscheidet sich von der qualifizierten elektronischen Signatur durch die gehobenen gesetzlichen Ansprüche nach SigG an den Zertifizierungsdiensteanbieter: Eine Akkreditierung wird nur dann erteilt, wenn der Zertifizierungsdiensteanbieter nachweist, dass die Anforderungen nach dem Signaturgesetz und der Signaturverordnung erfüllt sind.

Zur Erfüllung der Anforderungen muss das Sicherheitskonzept der Zertifizierungsstelle durch eine Bestätigungsstelle auf seine Eignung und die korrekte praktische Umsetzung geprüft und bestätigt sein. Das heißt, der Vorgang der Zertifikatserzeugung ist vom Ausfüllen des Antragsformulars, der Überprüfung des amtlichen Ausweisdokumentes, der Antragsannahme, der Schlüsselgenerierung bis hin zum endgültigen Erzeugen des Zertifikates kontrolliert und akkreditiert worden. Diese Prüfung und Bestätigung ist nach sicherheitserheblichen Veränderungen sowie in regelmäßigen Zeitabständen zu wiederholen.

2.2.2 Zertifizierungsdienste-Anbieter

Je nach gewünschter Qualitätsstufe der elektronischen Signatur für ein formuliertes Einsatzgebiet stellt sich im Anschluss die Frage nach dem richtigen Zertifizierungsdiensteanbieter. Für die Auswahl, ob hier eine unternehmensinterne PKI, eine externe Full-Service-PKI oder ein Zertifikat von einem akkreditierten Zertifizierungsdiensteanbieter benötigt werden, ist eine Analyse der Anforderungen des Unternehmens im jeweiligen Einzelfall erforderlich. Eine akkreditiert qualifizierte Signatur ist natürlich auf Grund ihres hohen Sicherheitsniveaus in allen Fällen einsetzbar, bedeutet jedoch unter Umständen einen höheren Kostenfaktor als für den konkreten Einsatz der Signatur nötig wäre.

2.2.3 Sicherheitsanforderungen an technische Komponenten

Die technische Sicherheit elektronischer Signaturen beruht vor allem auf

- dem verwendeten kryptografischen Verfahren,
- der Einmaligkeit der Signaturschlüsselpaare,
- der zuverlässigen Bindung des geheimen privaten Signaturschlüssels an den Inhaber,
- dem Ausschluss nicht gewollter digitaler Signaturen,
- der zuverlässigen Überprüfung der Gültigkeit des Zertifikats.

Die Eignung jeder Signaturkomponente wird durch eine Prüfung nach den Sicherheitskriterien "Common Criteria for Technology Security Evaluation" (CC) oder nach den "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik" (ITSEC) bestätigt.

2.3 PKI – warum jetzt?

Das BDSG sieht eine ganze Reihe datensicherheits- und datenschutztechnischer Regelungen vor. Zum einen muss der Verlagerung rechtsverbindlicher geschäftlicher Transaktionen auf die digitalen Medien und Kommunikationswege, wie sie bereits im Jahrbuch der Technikfolgenabschätzung 2002-2003 formuliert wurde, Rechnung getragen werden. Den Gefahren durch Datenmanipulation, -missbrauch oder –diebstahl wird, wie die aktuelle kes/Microsoft-Sicherheitsstudie von 2004 zeigt, eine größere Bedeutung zugemessen als je zuvor. Neben Schadsoftware wie Viren, Würmer und Trojanern gilt die Sorge der Unternehmen vor allem Irrtümern und der Nachlässigkeit eigener Mitarbeiter (51% der 90 Befragten). Unbefugter Kenntnisnahme, dem Informationsdiebstahl und der Wirtschaftspionage messen die Teilnehmer der Studie in der Bedeutung für das Unternehmen Rang 3 zu. Besondere Beachtung muss auch der Datenübermittlung an Dritte und ins Ausland gezollt werden, was auch datenschutzrechtlich ein wichtiger Aspekt ist, in dem PKI einfach und unkompliziert wirken kann.

Ein weiterer Grund sind betriebswirtschaftliche Argumente. Die Optimierung von Prozessen kann durch rein in der IT abgebildete Arbeitsabläufe ohne Medienbrüche, also den Wechsel des Informationsmediums, mit sicherem Zugriff vieler Personen auf kritische Daten durch PKI-Lösungen verwirklicht werden. Für Wirtschaftsunternehmen relevante Stellen fordern inzwischen ebenfalls Sicherheitsmaßen ein, namentlich ein ganzheitliches Risikomanagement. Unternehmen, die Kreditmittel einplanen, müssen sich schon heute mit beweisfähigem Workflow, nachweisbaren Sicherheitsvorkehrungen nach §9 BDSG, der elektronischen, rechtsverbindlichen Unterschrift, eCommerce, eGovernment und viele weitere, auf die digitale Ebene verlagerte Geschäftsprozesse, einstellen.

In vielen Punkten ist dies kein Problem: E-Mail-Agents bedienen, das Flug- oder Bahnticket online buchen, gezielt Informationen aus dem Internet beziehen und sich das Lieblingstrikot des favorisierten Fußballclubs zu ordern, ist nicht schwer. Der Umkehrschluss ist jedoch, dass sich in der Gemeinde der E-Medien-Nutzer eine rege Sorglosigkeit breit gemacht hat, mit der man unbedacht seine persönlichen Daten preisgibt, samt Kreditkartennummer, Geburtstag und Bankverbindung. Fotos sind in Businessforen obligatorisch. Ist es da nicht nahe liegend, dem Geschäftspartner Zukunftspläne und Unternehmensdaten unverschlüsselt und in blindem Vertrauen über eine einfache Telefonleitung zu schicken?

3 PKI als praktizierter Datenschutz

Die vorhergehend beschriebenen Aspekte aus der gängigen Praxis zeigen, von welch entscheidender Bedeutung es inzwischen ist, als Unternehmen anfallende Daten zu schützen – vor Übergriffen von extern ebenso wie vor unachtsamem Umgang oder bewusstem Missbrauch durch Personal und mit dem Unternehmen vertraute Personen.

Abb. 3: Zunehmende Relevanz elektronischer Zertifikate

Elektronische Signaturen, und bei gesteigertem Schutzniveau auch die Verschlüsselung von Daten, können hier in einem weiten Feld wirtschaftlich und effektiv helfen:

- Richtigkeit und Unversehrtheit übermittelter Daten(Daten-Integrität)
- Sicherstellung des Absenders (Urheber-Authentizität)
- Vertraulichkeit der Informationen (durch Verschlüsselung der Daten)
- Verfügbarkeit/Nichtbestreitbarkeit (elektron. Vertragsabschluss/Verwaltungsvorgang)

Die generelle Aufgabenstellung praktizierten Datenschutzes ist es, bei allen digitalen Informationsverarbeitungsvorgängen sicherzustellen, dass personenbezogene Daten im Sinne des BDSG vom Benutzer über eine vorhandene Plattform eingeben und übertragen werden können, ohne dass der Benutzer selbst in seiner Arbeit behindert wird oder sensible Personendaten unberechtigt eingesehen oder genutzt werden können. Ein Praxisbeispiel hierfür soll im Weiteren genauer betrachtet werden: die Abwicklung eines eCommerce-Vorgangs.

3.1 Aus Sicht des Verbrauchers

Folgendes Beispiel sei hierzu gewählt: User „Otto Normalverbraucher“ hat im Internet den Online-Shop „E-Kauf“ entdeckt und möchte ein dort angebotenes Produkt erwerben – ohne lästigen Austausch papierener Dokumente und dennoch möglichst rechtssicher.

Die Anmeldung des Users Otto ist bereits ein entscheidender Schritt im Prozess des digitalen Kaufprozesses: Otto möchte Produkte an seine Adresse zugestellt bekommen und zugleich sicherstellen, dass niemand anderes auf seinen Namen einkaufen kann und niemand anderes als „E-Kauf“ das Geld erhält, das Otto dem Online-Shop als Bezahlung zukommen lassen wird. Eine PKI-Lösung kann hier sowohl die Authentizität des Endnutzers Otto und des E-Shops im Sinne des BDSG sicherstellen, als auch die Korrektheit des Bestell- und Liefervorgangs, da beider Identität durch qualifizierte Trustcenter sichergestellt ist und die Anonymität jeweils dennoch gewahrt bleibt.

Der Kaufvertrag wird mittels der digitalen Signatur der PKI-Lösung unterschrieben und damit das Zustandekommen der Willenserklärung verifiziert. Das bedeutet eine rechtliche Absicherung der Transaktion, insbesondere wenn die übertragenen Daten verschlüsselt oder über eine sichere Verbindung ausgetauscht werden, für beide Seiten. Dies ermöglicht ein großes Maß an Rechtsverbindlichkeit im virtuellen Raum des Internets, insbesondere wenn weitere Identifikations- und personalisierte Bestätigungsinstrumente wie etwa die TAN (**T**rans**A**ktions-**N**ummern) zum Einsatz kommen. Neben der Authentizität der Vertragspartner kann auch die Integrität der Vertragsdaten sichergestellt werden.

Aus Datenschutzsicht ist es unbegreiflich, dass so unsichere Systeme wie Kreditkarten, bei denen alleine die Bekanntgabe der Kreditkartennummer und Laufzeit ausreichen, um sie als Zahlungsmittel zu missbrauchen, immer noch einer wesentlich sicherere Alternative in Form einer qualifizierten digitalen Signatur vorgezogen werden. Österreichische Kreditinstitute haben längst die Geschäftsabwicklung per qualifizierter digitaler Signatur realisiert – während in vielen anderen Ländern Risikopotential und Umständlichkeit in der Handhabung mit PIN und TAN in Kauf genommen werden oder zusätzlich weitere HBCI-Karten hierfür ausgegeben werden.

Fazit: Der Einsatz zertifikatsbasierter Lösungen im E-Commerce ebenso wie in anderen Online-Prozessen, die auf Rechtssicherheit und Beweisfähigkeit angewiesen sind, ist eine praktikable sinnvolle Methode für alle Beteiligten. Missbrauchsmöglichkeiten werden von vorneherein minimiert. PKI wird jedoch bisher immer noch viel zu selten genutzt wird – zugunsten eines allzu hohen Risikofaktors für alle Beteiligten.

3.2 Aus Sicht des Anbieters

Die Einsatzmöglichkeiten von PKI-Lösungen gehen noch viel weiter und können durchaus auch die weiteren Erfordernisse an Datensicherheit nach §9 BDSG erfüllen. Betrachten wir als zweites Beispiel die Firma „Innovativ“, die strikt alle anfallenden personenbezogenen – und natürlich auch unternehmenssensiblen- Daten nach den gesetzlichen Anforderungen schützt. Die Perspektive des Anbieters wird der Vereinfachung halber gleichgesetzt mit der des Datenschutz- und IT-Sicherheits-Beauftragten, die die im Unternehmen vorhandenen Geschäftsprozesse sorgfältig auf datenschutzrechtliche und sicherheitstechnische Korrektheit überprüfen.

Das Unternehmen hat für jeden Mitarbeiter eine Smartcard samt Lesegerät der Klasse 2 (für optimalen Schutz der ausgetauschten Daten auf Seiten des Mitarbeiters) zur Verfügung gestellt. Hierfür hätte theoretisch eine interne Zertifizierung der Keys genügt, jedoch will der Arbeitgeber auf Nummer sicher gehen und bietet daher qualifizierte Zertifikate an, die durch ein akkreditiertes Trustcenter jeweils Identität und Authentizität des Inhabers bestätigen.

Mit dieser Smartcard können Mitarbeiter Zutritt zu den Räumlichkeiten erhalten, die sie jeweils benötigen. Bestimmte Örtlichkeiten können eindeutig definierten Benutzergruppen und Einzelpersonen zugeordnet werde. Beispielsweise können zum Aktenarchiv der Personalabteilung ausschließlich die Geschäftsführung, befugte Mitarbeiter der Personalabteilung und weitere klar definierte Personen z.B. aus der Hausmeisterdienste-Gruppe zugelassen werden. Ebenso können Abteilungen untereinander abgegrenzt, der Zutritt zum Serverraum - dem Herzstück vieler IT-Unternehmen - restriktiv definiert werden. Doch nicht nur die Räumlichkeiten, sondern auch der Zugang zu den (Rechner-)Systemen des Unternehmens können mit der Smartcard der Mitarbeiter geregelt werden, mittels der hierfür erforderlichen Authentifizierung und Identifizierung des jeweiligen Mitarbeiters. Der Zugang zur entsprechend sensiblen Infrastruktur ist also zusätzlich gesichert. Dabei wird – ganz nebenbei – eine weitere Anforderung des BDSG erfüllt: Die Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden (Anlage zu §9 Punkt 8 BDSG).

Die Sicherstellung der Verfügbarkeit personenbezogener und sensibler Daten kann zum Teil ebenfalls mittels PKI reguliert werden: Durch die kontrolliert begrenzten Zugriffsmöglichkeiten auf die Informationen wird das Datenverlustrisiko durch unsachgemäße, unaufmerksame oder bewusst fahrlässige Nutzung bereits bedeutend reduziert. Mit Hilfe der Nachvollziehbarkeit von Modifikationen an Dateien und Daten kann rekonstruiert werden, wer für den Verlust von Daten im Notfall verantwortlich war – dies fördert zusätzlich die Motivation der Mitarbeiter, mit Informationen dieser Art bewusster und verantwortlicher Umzugehen.

Dasselbe gilt für den Datentransfer und –austausch, wo mit Hilfe des Zertifikats kontrolliert werden kann, dass eine Weitergabe sensibler Informationen nur an solche Personen erfolgt, die von Unternehmensseite hierfür vorgesehen sind. Insbesondere die Datenübermittlung an Dritte zu Zwecken der Auftragsdatenverarbeitung im Sinne des §11 BDSG oder der Datentransfer ins Ausland erfordern besonderer Sorgfalt im Bezug auf den Schutz personenbezogener Daten. Dasselbe gilt durchaus auch für die sensiblen weiteren Unternehmensdaten, die nicht an jeder beliebigen Zwischenstation abgegriffen werden können sollen.

Doch was ist mit der Integrität der Daten? Mittels der digitalen Unterschrift, die jeder Mitarbeiter durch die Daten auf seiner Smartcard leisten kann, kann jede Eingabe, also jeder digitaler Arbeitsschritt, bei Bedarf in einem Geschäftsprozess nachverfolgt werden. Jede Modifikation von Informationen könnte also – wenn nötig – jederzeit nachvollzogen und einer Person zugeordnet werden. Auf diese Weise ist auch die korrekte Erfüllung der Aufgabenstellung durch die Mitarbeiter gewährleistet. Es kann also die Auftragskontrolle gemäß BDSG durchgeführt werden und eine eventuell erforderliche Nachbesserung an den entsprechenden Stellen im Unternehmen erfolgen.

Letztlich muss schließlich auch noch die Privatsphäre der Mitarbeiter geschützt werden. Eine Speicherung von Prozessablaufdaten kann – und sollte anonymisiert bzw. pseudonymisiert zu erfolgen, um einer Erstellung von datenschutzrechtlich nicht akzeptablen Leistungsprofilen der Mitarbeiter wirksam zu begegnen. Auch hier kann die PKI-Lösung nützlich sein, weil die Signatur in Verbindung mit einer Laufnummer statt des Mitarbeiternamens bereits eine Pseudonymisierung darstellt, ohne großen Aufwand vom Betreiber zu fordern.

Andererseits wird gleichzeitig die Sensibilisierung aller Personen, die mir personenbezogenen Daten zu tun haben, wird durch die PKI-Lösung unterstützt: Der Mitarbeiter erhält nicht nur

einen Usernamen und ein Passwort, welche er einfach weitersagen oder unachtsam ablegen kann, er gibt mit der Weitergabe seiner Smartcard auch gleichzeitig seine Identität im System aus der Hand und kann selbst in der Zeit nicht arbeiten.

Für den Einsatz von PKI in der Datenschutzpraxis sprechen viele Punkte, sofern die Sicherheitsmaßgaben im Bezug auf Erstellung elektronischer Signaturen und die Geheimhaltung des personalisierten Schlüssels hierfür vor unbefugten Zugriffen wirksam geschützt ist.

3.3 Aus Sicht der Geschäftsleitung

Jede Partei, die am elektronischen Kommunikationsalltag teilnimmt, ist zugleich Verbraucher und Anbieter, sei es ein Unternehmen, eine Behörde, ein Verein oder eine Privatperson. Jeder Beteiligte nimmt mit seinem Handeln Einfluss auf unzählige Schnittstellen im System:

- Ist der Virenscanner untauglich oder nicht vorhanden, werden zum Beispiel Mails an alle Adressaten im digitalen Mailer-Adressbuch mit verseuchtem Inhalt versandt.
- Werden in einem Massenmailing alle Empfänger im „To“-Feld eingetragen, haben sämtliche Beteiligten des Adressbuches einen kostenlosen Kontaktpool frei Haus.
- Befinden sich die Systempasswörter des Geschäftsführers unter seiner Tastatur, in der obersten Schreibtischschublade oder im aufgeklappten Organizer, öffnet er damit Missbrauch Tor und Tür.

Im letzten Punkt geht der Geschäftsführer mit schlechtem Beispiel voran, weil er signalisiert, dass er den Wert des Unternehmenssystems samt aller vorhandenen Daten und Informationen selbst nicht ernst genug nimmt, um verantwortungsbewusst mit diesem Grundkapital umzugehen. Der gezielte Einsatz von PKI-Lösungen in den genannten Qualitätsabstufungen je nach erforderlichem Schutzniveau der Daten kann mit wenig Aufwand und sehr effektiv helfen ein derartiges Fehlverhalten auf ein Minimum zu reduzieren.

Als Geschäftsleitung muss man sich mehr denn je darüber informieren, welche Konsequenzen unterlassenes Handeln haben kann. Von Urheberrechtsklagen und Schadensersatzforderungen, verhängten Bußgeldern auf Grund von Versäumnissen, bis hin zum Verlust der Bonität des Unternehmens und sogar Freiheitsstrafen kann die Verletzung der Sorgfaltspflicht der Geschäftsleitung zur Folge haben. Wichtiger denn je ist es daher, sich im laufenden Betrieb Gedanken um IT-Sicherheit und Datenschutz zu machen. Das größte Schadenspotential wird laut der aktuellen kes/Microsoft-Sicherheitsstudie jedoch immer noch dem Ausfall der technischen Ressourcen – in welcher Weise auch immer – beigemessen. Den immensen „Wert der vorgehaltenen Informationen“ (s. WIK) im Unternehmen bei einem Schadensfall und dem damit verbundenen Verlust sämtlicher Unternehmensdaten definieren 9 von 90 Antworten als „’unbezahlbar’ oder legten nahe, dass dies den Geschäftsverlust zur Folge hätte. Die 81 quantifizierten Antworten ergaben einen mittleren Verlust-Wert von rund 281 Mio. €“ (s. WIK).

3.3.1 Technikfolgenabschätzung

Die juristischen Aspekte im Bezug auf die IT-Sicherheit im Unternehmen gewinnen also immer mehr an Bedeutung. Die zunehmende Vernetzung und damit die nahezu unüberschaubare Komplexität moderner Kommunikations- und IT-Systeme sorgt für ein stetig wachsendes Gefährdungspotential, dem Unternehmen Rechnung tragen müssen, wollen sie das Risiko eines Schadens im eigenen Haus nicht eingehen. Das Beispiel des Brandes bei einem Zulieferer namhafter Handyhersteller zeigt eindrücklich, wie wichtig ein IT-Sicherheitskonzept im Ernstfall sein kann: während der eine Konzern dank seines Notfallhandbuchs alternative Wege bei der Aufrechterhaltung seiner Geschäftsprozesse zielstrebig einschlagen konnte, musste der zweite Betroffene seinen Geschäftsbereich Mobiltelefongeräte einstellen.

In den meisten Unternehmen ist es den Mitarbeitern gestattet, privat das Internet zu nutzen. Welche Konsequenzen darauf für den Arbeitgeber ins Haus stehen, weil er damit zugleich unter das Teledienstemediengesetz fällt, ist kaum bekannt.

In einer Zeit, wo viele Konzernleitungen noch nicht abschätzen können, welche massiven Konsequenzen die Einführung von Softwarepatenten für die alltägliche Arbeit an und mit Hard- und Software haben wird, rückt die Eintrittswahrscheinlichkeit eines ersten Verstoßes gegen irgendein Urheberrecht aber mit jedem Tag näher. Das Patent auf den Doppelklick oder den Fortschrittsbalken, der den Status eines Speichervorgangs abbildet, sind nur zwei kleine Beispiele.

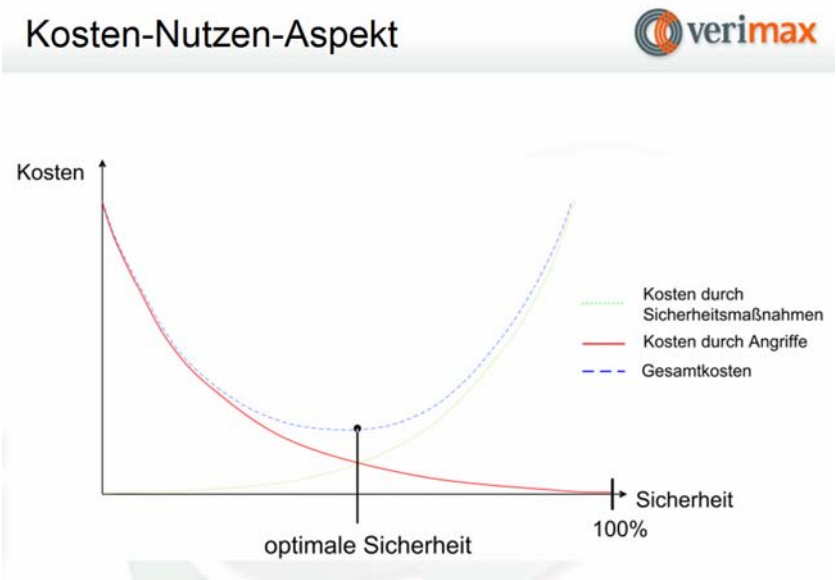

Abb. 4: Kosten-Nutzen-Abwägung im Bezug auf ein optimales Schutzniveau

3.3.2 Aufwandsabschätzung und Wettbewerbsvorteil

Die Umsetzung datenschutzrechtlicher Anforderungen ist keineswegs aufwändig und kompliziert, zudem stehen vielfältige Hilfsmittel in Form der Datenschutzbeauftragten und anderer Institutionen sowie kommerzielle Dienstleister bereit. Die informationstechnischen Standards bieten Möglichkeiten, Geschäftsprozesse ebenso effektiv wie datenschutzfreundlich zu gestal-

ten. Eine Form ist die Nutzung von PKI-Lösungen, also der Einsatz elektronischer Zertifikate und Verschlüsselung von sensiblen Personen- und Unternehmensdaten.

Der Aufwand für die Installation einer PKI-Lösung ist ebenfalls durchaus überschaubar. Je nach angestrebtem Schutzniveau ist neben der Ausrüstung der PC-Arbeitsplätze mit geeigneten Kartenlesern eine Smartcard mit Zertifikat für jeden Mitarbeiter erforderlich. Hinzu kommt eine Einführung in das Medium und seine Benutzung sowie die Erstellung einer Dienstanweisung, was im Falle beobachteter Unregelmäßigkeiten im Bezug auf die PKI im Unternehmen von den Mitarbeitern zu tun ist.

Alles in allem ist die Einführung einer PKI ein kaufmännisch überschaubarer Aufwand, der in keinem Verhältnis zum Schaden, der durch den Verlust von Daten, Industriespionage oder Bußgelder und Strafen, wie sie im BDSG und StGB geregelt sind, steht. Durch die Reduktion von Medienbrüchen kann ganz nebenbei die Prozessgeschwindigkeit im Unternehmen erhöht werden und dadurch auch der Kostenfaktor der einzelnen Prozesse minimiert werden.

Außerdem gewinnt das Unternehmen einen Imagevorteil durch eine Steigerung der Vertrauenswürdigkeit beim Kunden – ein nicht zu unterschätzender Vorteil im stetig härter werdenden Wettbewerb. Zudem wird man zu einem interessanteren Gesprächspartner für Banken und Kreditinstitute, von der Haftung der Geschäftsführer und Vorstände nach KonTraG ganz zu schweigen. Letztendlich erfüllen Unternehmen, die schon jetzt Datenschutzerfordernissen folgen, nicht nur die gesetzliche Verpflichtung zum sorgsamen Umgang mit personenbezogenen Daten, sondern erfüllen darüber hinaus wesentliche betriebswirtschaftliche Voraussetzungen:

- die Nachvollziehbarkeit von Datenmodifikationen zu jeder Zeit
- Beweisfähigkeit Workflow durch digital durchgeführter Prozessschritte
- Aspekte der dauerhaften Rechtssicherheit

Mittel- und langfristig muss es Ziel jedes Unternehmens sein, das Risikopotential der Nutzung von online-Kommunikationswegen und – Handelsplattformen so weit zu minimieren, dass potentiellen Kunden die absolute Vertrauenswürdigkeit des Unternehmens ersichtlich wird.

4 Fazit und Ausblick

Die vielfältigen Einsatzmöglichkeiten digitaler Signaturen in Industrie, Wirtschaft, Medizin und weit darüber hinaus können nicht nur eine wirksame Hilfe bei der Umsetzung gesetzlicher Datenschutzvorschriften sein, sondern zugleich die richtigen Weichen im Unternehmen für die Zukunft stellen: arbeiten Datenschutzbeauftragter und IT-Sicherheits-Beauftragter kooperativ zusammen, entsteht als Produkt auch der beweisfähige Workflow im Sinne des nach KonTraG längst eingeforderten Riskmanagements. Ein weiteres wichtiges Element für die Geschäftsleitung, um die Zukunftssicherheit des Unternehmens zielorientiert zu fördern. Die Bedeutung der Kundenbindung durch Vertrauensbildende Maßnahmen sind ein weiterer Aspekt, der die mittel- und langfristige Wettbewerbsfähigkeit steigern und erhalten kann. PKI in der Datenschutzpraxis kann hier viele wertvolle Beiträge liefern.

Künftig ermöglichen Public-Key-Infrastrukturen durch ihre vielseitigen Einsatzmöglichkeiten ungeahnten gesellschafts- und wirtschaftsökonomischen Fortschritt. Vor allem bietet sich die Zusammenlegung der unzähligen Smartcards an, die jeder von uns bisher mit sich herumträgt:

Bankkundenkarte, EC-Karte, Kreditkarte, Bonuspunktesystem-Karten, Krankenversichertenkarte, Führerscheinkarte, Parkkarte, Mitarbeiter-Kennkarte, Telefonkarte und so weiter…

Ein paar der vielen Vorteile dieser so genannten multifunktionalen Smartcard sind:

- Eine PIN für alle implementierten Anwendungen
- Konzentration aller benötigten Informationen auf einem Medium
- Zutritts-, Zugangs- und Zugriffsregelungen sind einfach verwaltbar
- Die Ablaufkontrolle in Geschäftsprozessen ist gewährleistet
- Bequeme Abwicklung digital gestützter Rechtsgeschäfte, bargeldloser Zahlungsverkehr
- Optimierte Personenidentifikation durch biometrische Zusatzmerkmale
- Effektive Senkung von Geschäftsprozesskosten

Längst nicht mehr Zukunftsmusik: In Kombination mit der RFID (Radio Frequency Identification)-Technologie ist der Einsatz eines funkgesteuerten und damit kontaktlos verwendbaren Datenchips als subkutanes Implantat denkbar und in Vorbereitung. Erste „Feldversuche“ finden derzeit schon an verschiedenen Orten statt, genannt sei stellvertretend die Anwendung in Diskotheken (u.a. in Berlin und auf Mallorca). Hier erhalten Personen, die sich einen solchen Chip als Identifikations- und Zahlungsinstrument unter die Haut spritzen lassen, VIP-Status.

Die Grenzen zwischen Informationsfreiheit, dem sinnvollen Einsatz von Informationstechnologien und dem Schutz der Privatsphäre des zivilisierten Menschen zerfließen unaufhaltsam. Daher gilt es, den großen Nutzen von PKI-Lösungen im Bereich Datenschutz so zu nutzen, dass die personalisierte Smartcard als personenbezogenes Element der digitalen Signatur ausschließlich in die Hände des Eigentümers gelangt, um Missbrauch zu verhindern. Zudem sind auch die weiteren, bereits mehrfach dargelegten, datenschutzrechtlichen Belange in solcher Weise zu berücksichtigen, dass am Ende aus dem fortschrittlichen Verbraucher nicht der so wahnsinnig zerbrechlichen gläsernen Menschen geschaffen wird, der wir nicht sein wollen.

Kerstin Blossey und Christian Weber, Wiesbaden 2005;

Verwendete Quellen

Literatur

Dierstein, Rüdiger: IT-Sicherheit und ihre Besonderheiten – Kursunterlagen zur Einführung in die IT-Sicherheit (Teil 4), Ulm 2004;

Kollmann, Tobias: Vertrauensmanagement – Erfolgsfaktoren für die Kundengewinnung im E-Business, Frankfurt am Main 2003;

Mitnick, Kevin; Simon William: Risikofaktor Mensch – Die Kunst der Täuschung, mitp-Verlag, Bonn 2003;

Niedermeier, Rober; Dr. Junker, Markus: Rechtliche Pflichten im Bereich der IT-Sicherheit, Broschüre der Heussen Rechtsanwaltsgesellschaft mbH, ohne Ort und Jahr;

Gesetzestexte

Bundesdatenschutzgesetz (BDSG) idgF;

Signaturgesetz (SigG) idgF;

Signaturverordnung (SigV) idgF;

Signaturverordnung (SigV) idgF;

Aktuelle Studien

eBusiness-Jahrbuch der deutschen Wirtschaft 2004/2005, herausgegeben von Wegweiser GmbH, Berlin 2004;

kes/Microsoft Sicherheitsstudie 2004, gelesen in der WIK – Zeitschrift für die Sicherheit der Wirtschaft, SecuMedia Verlags-GmbH – Ausgabe Nr. 5/2004, Ingelheim 2004;

Jahrbuch der Technikfolgenabschätzung 2002-2003, herausgegeben von der Akademie für Technikfolgenabschätzung, Stuttgart 2003;