cebis
Landkreis Neu-Ulm

De-Mail, E-Postbrief etc.: Der Versuch, E-Mail sicher zu machen

Das Thema ist fast so alt wie die E-Mail selbst: Woher weiß ich, dass die E-Mail, die ich grade gelesen habe, von eben demjenigen stammt, der als Absender angezeigt wird. Oder anders herum: Wenn ich eine E-Mail verschicke, woher weiß ich dann, ob sie angekommen ist? Und bei wem? Und wer diese E-Mail noch alles mitgelesen hat ....

Im Prinzip sind diese Probleme ganz einfach lösbar: Die bereits 1997 gesetzlich geregelte digitale Signatur (http://de.wikipedia.org/wiki/Digitale_Signatur) erlaubt es etwa, eine Nachricht digital, d.h. ausschließlich am Computer und ohne Ausdrucken und manueller Unterschrift, zu unterschreiben; damit kann der Empfänger verlässlich nachprüfen, von wem die Nachricht stammt und er kann verhindern, dass sie von Unbefugten gelesen wird. Weil eine digitale Signatur viele Prozesse in Wirtschaft, Verwaltung und täglichem Leben erheblich beschleunigen und damit verbilligen würde, hat die Bundesregierung mit dem Signaturgesetz (http://de.wikipedia.org/wiki/Signaturgesetz_(Deutschland)) den rechtlichen Rahmen geschaffen, um dies auch für rechtsverbindliche Dokumente einsetzen zu können.

Doch "Grau, teurer Freund, ist alle Theorie". Oder verschicken Sie etwa schon seit über zehn Jahren alle Rechnungen, Steuererklärungen, Strafzettel, Mietverträge etc. elektronisch signiert? Wer kennt schon den Unterschied zwischen der einfachen und der qualifizierten elektronischen Signatur mit jeweils völlig unterschiedlichen Rechtsfolgen? Laut Wikipedia ist jedenfalls die am weitesten verbreitete Anwendung der elektronischen Signatur nicht die E-Mail, sondern das Elektronische Abfallnachweisverfahren (eANV) (http://de.wikipedia.org/wiki/Qualifizierte_elektronische_Signatur).

Die Alternativen

Die - im Übrigen technisch durchaus gut funktionierenden - Verfahren zur Absicherung von E-Mails werden von den wenigsten Anwendern akzeptiert. Was vielleicht auch daran liegt, dass kein einheitlicher Standard existiert: Es gibt

- eine Reihe von kommerziellen Angeboten zur Lösung dieser Probleme,
- Open-Source-Lösungen wie etwa PGP (http://de.wikipedia.org/wiki/Pretty_Good_Privacy),
- allgemeine E-Mail-Portale wie etwa von Google (http://www.google.com/postini/encryption.html) oder
- Spezialanwendungen wie elektronische Rechnungen etwa von den Sparkassen oder den VR-Banken (http://www.ebillsmore.com/de/).

Leider sind diese Verfahren alle nicht miteinander kompatibel. Weil zumindest öffentliche Stellen im Rahmen der Umsetzung der EU-Dienstleistungsrichtlinie elektronische Kommunikation akzeptieren müssen (http://www.presseanzeiger.de/meldungen/it-computer-internet/307319.php), muss ein allgemein akzeptierter Standard her, der das erlaubt und "so einfach ist wie E-Mail und dabei so sicher wie die Papierpost" (http://www.cio.bund.de/SharedDocs/Projekte/2008/dmail_projekt.html).

Versuche von Standards

In jüngster Zeit wurden vor allem folgende Standard-Vorschläge diskutiert:

- De-Mail – ein Projekt der Bundesregierung (http://de.wikipedia.org/wiki/De-Mail) - soll den verbindlichen und vertraulichen Austausch elektronischer Dokumente über das Internet ermöglichen und dabei die Kommunikationskosten für Verwaltungen und Unternehmen reduzieren. Umgesetzt wird De-Mail von Privatunternehmen und dabei im Wesentlichen von den großen E-Mail-Providern, also etwa der Telekom, gmx oder web.de. Dort kann man sich bereits vorregistrieren und eine De-Mail-Adresse reservieren. Das De-Mail-Gesetz ist allerdings noch nicht verabschiedet .....
- E-Postbrief (http://www.epost.de; http://de.wikipedia.org/wiki/E-Postbrief) wird von der Deutschen Post angeboten, die ursprünglich am De-Mail-Projekt beteiligt war, dort aber inzwischen ausgestie-

gen ist. Der Grund für ein eigenes Verfahren ist einleuchtend: Natürlich würde eine Umstellung auf die elektronische Zustellung der Post einen deutlichen Umsatzeinbruch bei der konventionellen Post bescheren; so ist die Deutsche Post immer noch von der Partie.

Im Gegensatz zu De-Mail ist der E-Postbrief seit Mitte letzten Jahres verfügbar und hat inzwischen über eine Million Kunden. Die Post verfügt bereits über einen großen Teil der für ein solches Verfahren notwendigen Infrastruktur, etwa das Postident-Verfahren (http://de.wikipedia.org/wiki/Postident), und besitzt damit einen erheblichen Vorteil - den sie auch behalten will und sich deshalb weigert, diese Infrastruktur den De-Mail-Anbietern zur Verfügung zu stellen. Die ziehen dagegen vor Gericht (http://m.ftd.de/artikel/60016780.xml?v=2.0). Augenscheinlich kämpfen also die beiden Konkurrenten mit harten Bandagen. Wer letztlich gewinnt, bleibt abzuwarten; wer verliert, ist klar: Der Anwender, der auf einen einzigen Standard gehofft hat, auf den er ohne Risiko setzen kann, und jetzt wieder mehreren Standards gegenüber steht - und damit im Endeffekt keinem Standard.

Technische Probleme:

Obwohl der Bundesrat dies bereits letztes Jahr forderte, bieten De-Mail und E-Postbrief beide keine Ende-zu-Ende-Verschlüsselung, also eine Verschlüsselung durch den Absender, die nur durch den Empfänger wieder rückgängig gemacht werden kann. Stattdessen entschlüsselt der jeweilige Provider die Nachrichten (etwa um sie auf Viren zu scannen und zu archivieren), verschlüsselt dann wieder und stellt sie schließlich zu. Der Provider kann also alle Nachrichten mitlesen. Was er unter Umständen auch tun muss, wenn etwa Strafverfolgungsbehörden dies verlangen. Datenschützer warnen allerdings davor, dass hiermit das Briefgeheimnis in Frage gestellt wird (http://www.heise.de/newsticker/meldung/Kritik-am-E-Postbrief-waechst-1044814.html).

Das ist aber nicht nur für Datenschützer relevant; nach aktueller Rechtslage eignet sich ein solches Verfahren nicht, um die qualifizierte elektronische Signatur bei Rechnungen zu ersetzen (http://www.heise.de/artikel-archiv/ct/2011/4/146_kiosk). Das soll sich aber nach dem inzwischen beschlossenen Entwurf des Steuervereinfachungsgesetzes für Umsätze nach Ende Juni ändern (http://www.heise.de/ct/meldung/Zwang-zur-Rechnungssignatur-faellt-Ende-Juni-1183747.html).

Die AGBs der Post beinhalten noch weitere Feinheiten: Die Post fordert in ihren AGBs dazu auf, jeden Tag sein Postfach zu prüfen; ein E-Postbrief-Brief gilt nach einem Tag als zugestellt. Rechtsmittelfristen laufen dann, auch wenn eine Zustellung aus technischen Gründen nicht möglich war oder der Kunde schlicht im Urlaub ist und keinen Internet-Zugang hat. Die Beweislast wird praktisch umgekehrt: Ein Empfänger muss nachweisen, dass ihn eine Nachricht nicht erreicht hat, ein normaler Brief kann schon mal verloren gehen, hier muss der Absender die Zustellung beweisen. Aufgrund der massiven Kritik an diesen AGBs hat die Post zwar eine Website mit Erklärungen eingerichtet, die alle kritischen Punkte abschwächen sollen; die AGBs selbst bleiben aber in ihrer Substanz unverändert (http://www.E-Postbrief.de/privatkunden/footer/rechtliches/agb.html).

Bei einer Anhörung im Innenausschuss wurde erhebliche Kritik an De-Mail geübt, unter anderem sprach ein Vertreter des deutschen Notarvereins von einer "Mogelpackung" und "Bauernfängerei". Der Gesetzentwurf wird jedenfalls weiter überarbeitet; mal sehen, was dabei heraus kommt (http://www.heise.de/newsticker/meldung/Scharfe-Kritik-am-De-Mail-Gesetzentwurf-im-Bundestag-1184961.html).

Beide „Standards“ sind also "nicht ausgereift", so jedenfalls die Einschätzung der Stiftung Finanztest (http://www.test.de/themen/computer-telefon/meldung/Elektronischer-Brief-Postmodern-4132755-4132760/). Briefmarkensammler können also aufatmen; der Nachschub versiegt bis auf weiteres noch nicht und die Arbeitsplätze bei der Deutschen Post bleiben gesichert …

CEBIS hilft weiter

Unternehmen, die Informations- und Beratungsbedarf zu Chancen, aber auch Risiken von IT und Internet haben, können sich an CEBIS wenden. In Veranstaltungen und Einzelberatungen können Unternehmen Hilfestellung durch kompetente Experten erhalten. Informieren Sie sich auf der CEBIS-Website über die entsprechenden Termine und melden Sie sich möglichst frühzeitig an.

Tipp des Monats März 2011