Security by obscurity im Bundestag

Der Bundestag bietet an, den Abgeordneten verschlüsselte E-Mails senden zu können. Das hört sich gut an, funktioniert aber nicht: Kaum ein Abgeordnetenbüro weiß damit umzugehen. Bei technischen Fragen geht man zudem nach dem Motto vor: Security by obscurity.

Die rot-grüne Bundesregierung hat am 22. Januar 2002 die Telekommunikations-Überwachungsverordnung (TKÜV) erlassen. Seitdem wird die Kommunikation aller Bundesbürger komplett überwacht. Die Technik – eine Echtzeit-Schnittstelle – muss von den Telekommunikationsanbietern eingerichtet und selbst finanziert werden. Nur kleine Provider sind davon ausgenommen. Wer seine elektronische Kommunikation verschlüsselt, kann natürlich nicht belauscht werden. Was liegt also näher, auch bei vertraulichen Nachrichten an einen Abgeordneten des Bundestages kryptografische Verfahren zu verwenden.

Es scheint zunächst einfach zu sein: Unter der Überschrift „Senden verschlüsselter E-Mails an Mitglieder oder Mitarbeiter des Deutschen Bundestages“ kann sich jeder über die Grundlagen asymmetrischer Kryptografie informieren. Man wird auch hinreichend über die Methode aufgeklärt:

„Für die Verschlüsselung von E-Mails muss der jeweilige Absender den öffentlichen Schlüssel des Empfängers in seinen E-Mail Client einbinden. Der öffentliche Schlüssel für die jeweilige E-Mail Adresse der Abgeordneten und Verwaltungsmitarbeiter ist automatisch in jeder signierten E-Mail des Abgeordneten oder Mitarbeiters enthalten. Gegebenenfalls bitten Sie Ihren Kommunikationspartner im Deutschen Bundestag Ihnen eine signierte E-Mail zu senden, um ihm verschlüsselt antworten zu können.“

Vor das Verschlüsseln hat die Verwaltung des Bundestags eine hohe Hürde gestellt: Die E-Mail-Adressen, die man benötigt, um seinen eigenen öffentlichen Schlüssel an die Abgeordneten zu senden, werden nicht verraten, sondern stattdessen jeweils ein Kontaktformular angeboten. Viele Abgeordnete haben zwar eine Website, die muss man aber in jedem Fall einzeln und mühsam selbst recherchieren. Ob das zu erwartende System vorname.nachname@bundestag.de funktioniert, erfährt man auch nicht.

Selbst bei Jörg Tauss (SPD), der bei Internet-Themen als relativ kompetent gilt, ist von einem öffentlichen Schlüssel nichts zu sehen. (Dafür begegnet man aber auf seiner Website dem „Regenzauber“, gegen Spam das @ verklausuliert (a) zu schreiben, wodurch man gezwungen ist, die E-Mail-Adresse mühsam von Hand einzutippen, statt im Quellcode zum Beispiel schlicht Unicode zu benutzen, um es den Spambots nicht ganz so einfach zu machen)

Man muss also zuerst die real existierende E-Mail-Adresse erfragen, auf eine signierte Antwort hoffen, das Zertifikat des Bundestags in den eigenen E-Mail-Client implementieren, die Signatur der empfangenen E-Mail überprüfen, den darin

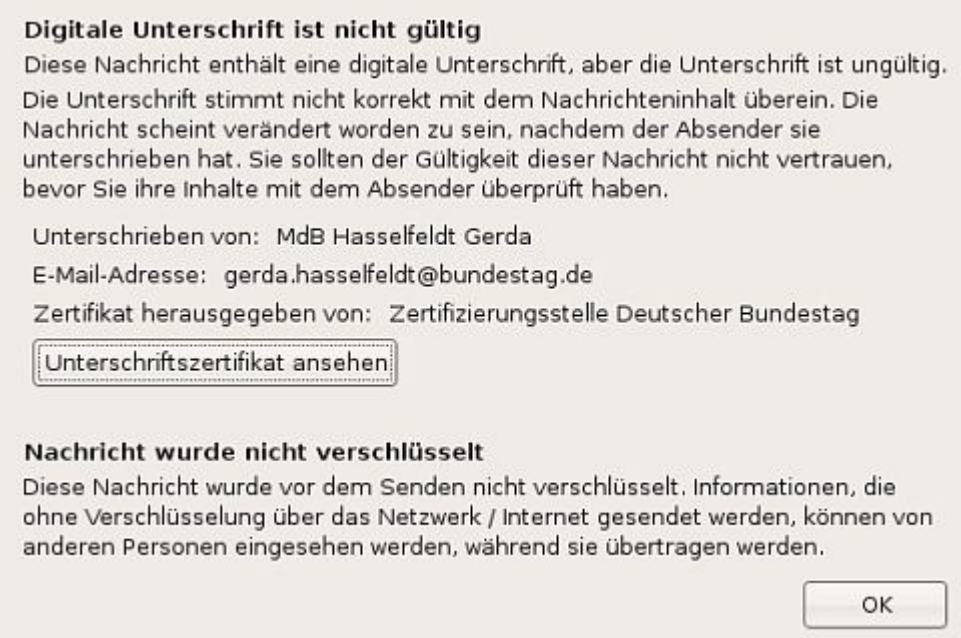
enthaltenen Schlüssel einbinden, dann mit einem eigenen Zertifikat signieren und mit dem öffentlichen Schlüssel des Abgeordneten verschlüsseln – und hoffen, dass der Empfänger die gleiche Methode anwendet und dann endlich auch verschlüsselt schreiben kann.

Der Bundestag verwendet nicht die Open-Source-Methode GNU Privacy Guard (GnuPG) oder gar die kommerzielle Version Pretty Good Privacy (PGp) wie etwa das Bundesverfassungsgericht, sondern verschlüsselt über Secure/Multipurpose Internet Mail Extensions (S/MIME).

Diese Methode hat ihre Tücken: Benutzerfreundlich ist sie nicht, denn kaum ein Computer-Laie wird wissen, wie er oder sie an ein S/Mime-Zertifikat kommen kann und wie das anzustellen sei. Außerdem vertragen sich bei den meisten gängigen E-Mail-Programmen die beiden Verschlüsselungs-Methoden nicht. Thunderbird zum Beispiel arbeitet zuerst die S/Mime-Routinen ab, dann GnuPG. Wenn man eine E-Mail mit S/Mime signiert, kann man GnuPG nicht parallel verwenden, da eine anschließende Verschlüsselung die Mail verändern würde und die Signatur ungültig wäre. Es gibt auch keine Möglichkeit, für bestimmte Empfänger festzulegen, welche S/MIME-Funktion angewendet werden soll. Es ist also immer mühsame Handarbeit angesagt. Das weiß offenbar auch die Pressestelle des Bundestags, die auf Anfrage dazu etwas vage antwortet: „Der Deutsche Bundestag hat sich nur für eine der beiden Alternativen entschieden, da die parallele Verwendung zu technischen und organisatorischen Problemen führen könnte.“ Der Bundestag hat das zusätzliche Problem, dass er nur eine deutsche Zertifizierungsinstanz benutzen kann. Er ist zwar Certification Authority, kann aber das – auch aus Kostengründen – nicht in gängige Browser und Mail-User-Agenten implementieren lassen.

Am 19. Januar wurden 46 (von 613) nach dem Zufallsprinzip ausgewählte Abgeordnete angeschrieben mit der Bitte: „Bitte schicken Sie mir eine signierte E-Mail zu.“ Nach einer Woche

(!) hatten nur sieben geantwortet, von dem angeschriebenen Abgeordneten der Partei „Die Linke“ reagierte sogar niemand. Das Büro von Michael Glos (CSU) war mit am schnellsten: Man wusste offenbar sofort, worum es ging, jedoch fehlte die Signatur. Dafür erfährt man immerhin bei jeder Antwort die eigene IP-Adresse, die man beim Abschicken der E-Mail verwendet hatte – warum auch immer: „Diese Nachricht wurde im Internet des Deutschen Bundestages erfasst – Sa Jan 19 18:03:31 2008 – Externe IP-Adresse: 217.83.70.227.“ Auf Nachfrage reagierte Glos‘ Büro dann nicht mehr.



Eine Mitarbeiterin Volkmar Vogels (CDU) rief sogar an, um sich erklären zu lassen, um welchen unverständlichen Sachverhalt es sich in der fraglichen E-Mail gehandelt habe. Danach scheint das Interesse am Thema aber erloschen zu sein – eine elektronische Antwort kam nicht. Auch das Büro des Bundesinnenministers Wolfgang Schäuble (CDU) schwieg eisern. Zugunsten Schäubles muss erwähnt werden, dass die Standard-Signatur des Autors vermutlich sehr abschreckend wirkt: „Please note that according to the German law on data retention, information on every electronic information exchange with me is retained for a period of six months.“

Gerda Hasselfeldt, CDU/CSU, Petra Bierwirth (SPD), Lydia Westrich (SPD) und Miriam Gruß (FDP) antworteten kurzfristig

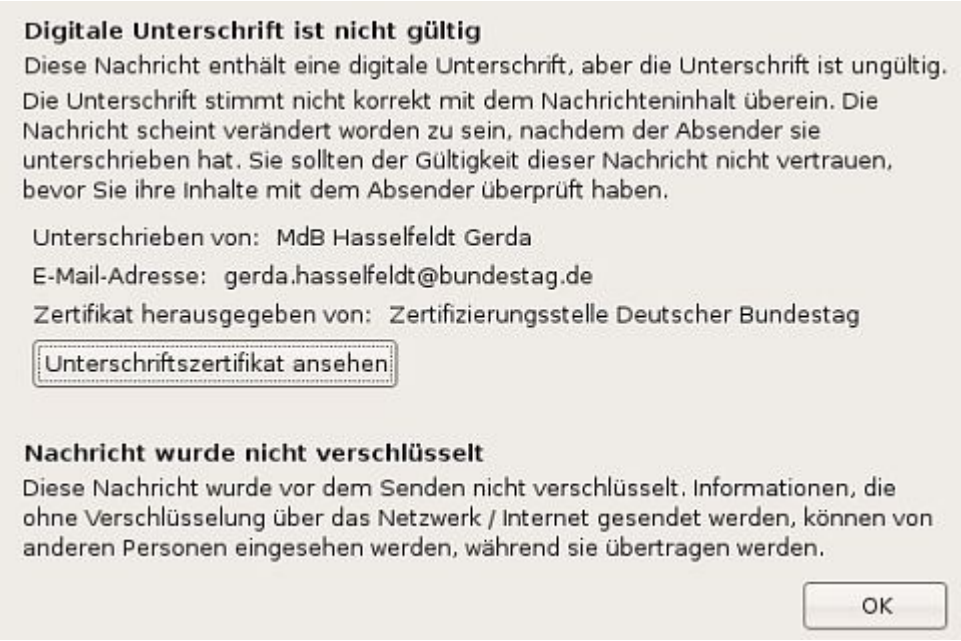
und korrekt signiert, jedoch nur zwei Männer: Markus Löning (FDP) und Hans-Christian Ströbele (Die Grünen). Das Büro Ströbeles, das offenbar zusätzlich die EDV im Bundestag bemühte, kommentierte: „Leider mussten die Techniker einräumen, dass das System noch nicht wirklich gut funktioniert.“ Nur sieben von 47 Mitgliedern des Bundestages reagieren also auf eine E-Mail, die um das bittet, was der Bundestag selbst empfiehlt – eine traurige Bilanz.

Der zweite Schritt gab auch den wenigen Abgeordneten, deren Mitarbeiter verstanden hatten, was eine elektronische Signatur ist, große Rätsel auf:
„Um nachzuprüfen, ob nicht nur die elektronische Signatur, sondern auch die Verschlüsselung funktioniert, bitte ich Sie um eine weitere kurze Mail, die Sie bitte an mich verschlüsseln. Mein öffentlicher Schlüssel (S/Mime) ist in meiner Signatur enthalten.“

Nur zwei Abgeordnete – Lydia Westrich und Markus Löning – meisterten diese Hürde und antworteten per verschlüsselter E-Mail. Das Büro von Miriam Gruß gab sich Mühe und kündigte an, man werde sich im Haus sachkundig machen – was aber seitdem offenbar noch nicht von Erfolg gekrönt war. Ein Verantwortlicher für die Technik im Bundestag verriet per verschlüsselter E-Mail, dass es für Probleme dieser Art sogar eine telefonische Hotline gebe und jederzeit Hilfe, falls ein Abgeordneter darum bäte.

Welche technischen Probleme Mitglieder des Bundestag daran hindern könnten, ihre Kommunikation zu verschlüsseln, war nicht zu erfahren. Einige Signaturen wiesen darauf hin, dass die Unterschrift ungültig sei. Das wird vermutlich daran liegen, dass verschlüsselte E-Mails an Bundestagsabgeordnete von einem zentralen Server entschlüsselt werden – ein Prinzip, dass der Idee widerspräche, dass nur der Empfänger einer kodierten Nachricht diese auch lesen sollte. Wie die Sicherheit der Kommunikation zwischen dem Server des Bundestags und Empfänger gewährleistet sei, darüber wollte man

keine Details preisgeben. Anna Rubinowicz-Gründler, Pressereferentin im Bundestag, antwortete: „Zu IT-sicherheitsrelevanten Fragen können wir keine Auskünfte erteilen.“ Auf die Frage, warum ein Kontaktformular, das Signieren und den Austausch von Schlüsseln per S/MIME nicht erlaubt, angeboten wird statt einer funktionierenden E-Mail-Adresse, verwies man darauf, dass „die in das Formular eingetragenen Daten (..) verschlüsselt über ‚HTTPS‘ übertragen“ werden. Das bedeutet in diesem Fall nichts, da offenbar niemand genau weiß, wer im Bundestag die Mails welcher Abgeordneten lesen kann. Die mangelnde Fähigkeit oder Bereitschaft der Abgeordneten, ihre E-Mails vor dem Zugriff anderer zu schützen zu wollen, mochte man ebenfalls nicht kommentieren: „Die Pressestelle des Deutschen Bundestages informiert über Sachverhalte, transportiert aber keine Meinungen.“



Über diesen Sachverhalt kann man geteilter Meinung sein. Dass ein Abgeordneter des Bundestages keinen technischen Sachverstand besitzt, ist verzeihlich. Dass sie oder er auf auf den Sachverstand verzichtet, der ihm innerhalb des Hauses gratis angeboten wird, ist einfach nur ignorant.

Dieser Artikel erscheint leicht verändert am 04.02.2008 auf Telepolis.