Stratum 0 e. V.
Hamburger Straße 273a
D-38114 Braunschweig
E-Mail: kontakt@stratum0.org
Website: https://www.stratum0.org

Stratum 0 e. V., Hamburger Straße 273a, D-38114 Braunschweig

An den Rat der Stadt Braunschweig
Platz der Deutschen Einheit 1
38100 Braunschweig

26. März 2014

Stellungnahme zum Antrag 3171/14, "Prüfauftrag zu technischer und rechtlicher Machbarkeit und Kosten von verschlüsselter digitaler Kommunikation (z.B. GnuPG / GPG4Win) zwischen Einwohnern und der Stadt BS"

An den Rat der Stadt Braunschweig,

es ist realistisch davon auszugehen, dass Emails, wie wir sie heute und seit vielen Jahren versenden, auch in absehbarer Zukunft einen wichtigen Teil unserer Kommunikation ausmachen. Vertraulichkeit wie sie beim klassischen Brief durch das Postgeheimnis sichergestellt ist, ist in Kommunikation jeder Art ein Anliegen von zentraler Wichtigkeit. Spätestens die Veröffentlichungen im Rahmen des NSA-Skandals haben bewiesen, dass Verschlüsselung ein wichtiger Aspekt digitaler Kommunikation ist. Umso wichtiger ist sie beim Austausch persönlicher Daten, die bei der Kommunikation zwischen Stadt und Bürgern anfallen. Der Antrag zielt darauf ab, dem Bürger eine verschlüsselte und damit vertrauliche Kommunikation mit Ämtern und Behörden zu ermöglichen.

Der Antrag fordert im speziellen, eine verschlüsselte Kommunikation auf Basis anerkannter technischer Standards und mit freier Software zu ermöglichen. Dies unterstützen wir. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt[1] zu diesem Zweck ebenfalls das im Antrag vorgeschlagene Gpg4Win, welches auf dem seit fast 20 Jahren etablierten OpenPGP-Standard[2] beruht, die spezifische Software wurde außerdem vom BSI selbst ausgeschrieben. Für eine verschlüsselte Kommunikation ist es

[1] https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Datenverschluesselung/Praxis/Software/software_node.html
[2] http://en.wikipedia.org/wiki/Pretty_Good_Privacy

notwendig, dass die Ver- und Entschlüsselung auf Geräten stattfindet, die sich unter der Kontrolle des jeweiligen Benutzers befinden. Man spricht hier von Ende–zu–Ende Verschlüsselung. Nur diese Art von Verschlüsselung ermöglicht eine sichere Kommunikation, ohne dem Transportweg (Internet) vertrauen zu müssen.

Wie im Statement der Verwaltung erwähnt, sind Nachbesserungen an der De-Mail bezüglich einer Ende–zu–Ende Verschlüsselung vorgesehen. Das dabei aktuell vorgeschlagene Verfahren[3] verwendet wiederum das oben erwähnte Gpg4Win, welches mit der De-Mail auf identische Weise wie bei E-Mails angewendet werden soll. Dies zeigt, dass die De-Mail das Problem der vertraulichen Kommunikation nicht löst, und ihre Einführung schlussendlich nichts ändert an der im Antrag angeführten Notwendigkeit der Verwaltung, sich mit dem Thema der Ende–zu–Ende Verschlüsselung auseinanderzusetzen.

Die Ermöglichung der verschlüsselten Kommunikation zwischen Stadt und Bürgern auch mit klassischer E-Mail halten wir für realisierbar, umso mehr da die Verfahren sich nicht unterscheiden von denen, die auch mit der De-Mail eingeführt würden. Wir empfehlen daher, dem Antrag zuzustimmen und damit eine Prüfung dieser Möglichkeiten in die Wege zu leiten.

Mit freundlichen Grüßen,

Vincent Breitmoser
Lars Andresen
Matthias Uschok

Stratum 0 e. V.

[3] https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/KommunikationUeberInternet/De-Mail/VorteileundFunktionen/EndezuEndeVerschluesselung/endezuendeverschluesselung_node.html