BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG

20. Wahlperiode

Drucksache 20/

Antrag

des Abgeordneten Farid Müller, … (GRÜNE) und Fraktion

zur Drs. 20/11300

Betr.: Datenverkehr innerhalb der Hamburger Verwaltung und mit den Bürgerinnen und Bürgern durch Verschlüsselung sicherer machen!

Im Jahr 2008 informierte Microsoft die Stadt Hamburg, dass das bisher verwendete Verschlüsselungsprogramm „erweiterte Sicherheit“ im neuen Exchange Server 2010 nicht mehr zur Verfügung steht. Microsoft gab diese Information mit einem Vorlauf von über einem Jahr bekannt, die der Senat nicht nutzte, um eine gleichwertige Verschlüsselung der bis dahin ca. 16.000 Arbeitsplätze, die mit personenrelevanten oder anderen sensiblen Daten umgehen, auszurüsten. Offenbar konnte Dataport als IT-Dienstleister der Stadt Hamburg in diesem Zeitraum kein Angebot abgeben, so dass sich die Finanzbehörde gezwungen sah, ein anderes Schutzprogramm namens RMS einzusetzen. Dieses funktionierte aber erst im Juni 2011, so dass die Senats- und Parlamentsverwaltung ohne ein Schutzsystem dastand. Aber auch ab Juni 2011 stellte sich heraus, dass das Programm RMS nicht in der Lage war, Nicht-Microsoft-Dateiformate, wie zum Beispiel die in der Hamburger Verwaltung üblichen PDF-Formate, sicher zu verschlüsseln. Dieser gravierende Mangel führte nun dazu, dass auch RMS nicht flächendeckend für die o.g. 16 000 Arbeitsplätze eingeführt wurde.

Aktuell muss nun also die Hamburger Senats- und Parlamentsverwaltung ohne eine Ende zu EndeVerschlüsselung datensensible Kommunikation betreiben. Dieser Zustand ist weder verantwortbar für die dem Senat und der Bürgerschaft überlassenen Daten, noch technisch erklärbar und schon gar nicht finanziell begründbar.

Wenig verständlich ist, dass E-Mails nicht mindestens bei der Übertragung zwischen der Stadt zu anderen E-Mail-Providern mittels „ESMTPS“ verschlüsselt werden. Die dafür notwendige Technologie ist seit langem etabliert und wird bspw. vom Berliner E-Mail-Anbieter Posteo und auch von Google unterstützt. Im Oktober 2013 aktivierten große deutsche E-Mail-Anbieter wie die Telekom, Web.de und GMX im Rahmen der Kampagne „E-Mail made in Germany“ diese Verschlüsselung.

Zudem muss die Stadt mit freier Software und offenen Standards den Bürgerinnen und Bürgern ein sicheres Angebot machen, um sensible Personendaten oder andere Vorgänge bestmöglich zu schützen.

Im FDP-Antrag (Drs. 20/11300) sind konkrete Lösungen für diese Probleme im Auftrag an den Senat nicht benannt worden. Da der Senat nun aber seit Jahren hier keine Lösung anbietet, ist es seitens der Bürgerschaft angebracht, konkrete Lösungswege vorzuschlagen.

Dies vorangeschickt möge die Bürgerschaft daher beschließen:

1. Der Senat wird aufgefordert, entweder schnellstmöglich die frei und kostenlos allgemein anerkannte, verfügbare und auch schon vom Bundesamt für Sicherheit in der Informationstechnik und beim Hamburger Datenschutzbeauftragten benutzten E-Mail-Verschlüsselung PGP oder S/MIME einzuführen oder eine funktionstüchtige Alternative einzurichten.

2. Der Senat wird aufgefordert, in seinen Vertragsbeziehungen mit Dataport, soweit sie Datenspeicherung und Emailverkehr betreffen, Verschlüsselung als wesentlichen Bestandteil mit aufzunehmen.

3. Der Senat wird aufgefordert zu klären, inwieweit das bereits bestehende Angebot vom Bundesamt für Sicherheit und Informationstechnik (BSI) an die Bundesländer in Hinblick auf eine Schlüsselverwaltung mit eigenem Server (Public-Key-Infrastruktur) für Hamburg zu nutzen ist.

4. Der Senat wird aufgefordert, auch eine Ende-zu Ende-Verschlüsselung für die Email-Kommunikation zwischen Bürgerinnen und Bürgern und den Behörden sowie der Bürgerschaft zu gewährleisten.

5. Der Senat wird aufgefordert, zu klären, wie Microsoft in die Vertragspflicht genommen werden kann, um eine entsprechende Unterstützung an den Arbeitsplätzen der Stadt einzurichten

6. Die Bürgerschaft beschließt, ebenfalls schnellstmöglich auf eine E-Mail-Verschlüsselung analog der Senatsverwaltung zu dringen.