SPD-Fraktion im Rat der Stadt Herten
Sozialdemokratische Partei Deutschlands

SPD-Fraktion im Rat
der Stadt HERTEN
Kurt-Schumacher-Str. 2
45699 Herten
Telefon: 02366/303546
Telefax: 02366/303636
E-Mail: info@hertenerspd.de

An den Bürgermeister der Stadt Herten
Herrn Matthias Müller
Kurt-Schumacher-Straße 2
45699 Herten

Herten, den 16.09.2021

Anfrage nach § 13 GO des Rates der Stadt Herten

Schutz sensibler Daten bei elektronischer Kommunikation (E-Mail) in der Stadtverwaltung

Sehr geehrter Herr Bürgermeister,

bislang gibt es in der Stadtverwaltung keine Vorkehrungen, den elektronischen Schriftverkehr zu schützen. Wir bitten daher um Darstellung, wie zukünftig sensible Daten von Bürger:innen (z.B. Gesundheits-, Steuer-, Sozial- und Personendaten) oder der Stadtverwaltung selbst in der externen elektronischen Kommunikation datenschutzrechtlich vor Zugriffen Fremder geschützt werden können.

Begründung:

Austausch von Nachrichten via E-Mails gehören zum normalen Geschäftsalltag. E-Mails sind vergleichbar mit Postkarten aus der klassischen Briefpost. Im Zuge der Digitalisierung der öffentlichen Einrichtungen werden immer mehr sensible und personenbezogene Daten ausgetauscht. Unbefugte, die sensible Nutzerdaten ausspionieren wollen, profitieren von Nachrichten im Klartext. E-Mails sind weiterhin das Haupteinfallstor für Cyberangriffe. Ohne wirkungsvolle Verschlüsselung können E-Mails im Zweifelsfall mitgelesen oder verändert und so missbraucht werden. Gerade vertrauliche Informationen müssen geschützt werden und es muss gewährleistet sein, dass die Inhalte verschickter Mails nicht auszulesen sind.

Viele Internet-Provider bieten online schon durch die SSL-/TLS-Verschlüsselung einen sicheren Transportweg und mehr Datenschutz. Das bedeutet aber nicht, dass die Nachrichten gänzlich vor fremden Blicken geschützt sind. Um dieses zu gewährleisten, gibt es verschiedene Verschlüsselungs-Verfahren: S/MIME und/oder PGP (Pretty Good Privacy = Echt gute Privatsphäre). Dabei werden die Nachrichten Ende-zu-Ende verschlüsselt.

Unter Ende-zu-Ende wird die Verschlüsselung übertragener Daten über alle Übertragungsstationen hinweg verstanden. Die zu übertragenden Daten werden auf Senderseite verschlüsselt und erst beim Empfänger wieder entschlüsselt. Durch Verschlüsseln wird ein „Klartext", also ein klar lesbarer Text, in einen „Geheimtext", also in eine unverständliche Zeichenfolge umgewandelt. Durch PGP und auch S/MIME ist es möglich, eine Nachricht im Ganzen (außer E-Mail-Kopf und Betreff), inklusive aller Dateianlagen zu verschlüsseln und zu signieren. Für beide Möglichkeiten der Verschlüsselung werden entsprechende Zertifikate benötigt, für die gewisse Registrierungen notwendig sind. Dabei wird zwischen einem öffentlichen und einem privaten Schlüssel unterschieden, die entsprechend zu generieren sind. Diese Funktionen sind mit allen Web-Services zu nutzen.

Mit freundlichem Glückauf

Regina Haastert

Regina Haastert