Vorlage Federführende Dienststelle: Fachbereich Personal und Organisation Beteiligte Dienststelle/n:	Vorlage-Nr: FB 11/0210/WP16 Status: öffentlich AZ: FB 11 Datum: 23.09.2013 Verfasser: Herr Kinny

Ratsanfrage Fraktion "DIE LINKE" vom 11.Juli 2013, (E-Mail) Verschlüsselung ermöglichen

Beratungsfolge: **TOP:__**

Datum	Gremium	Kompetenz
20.11.2013	PVA	Kenntnisnahme

Beschlussvorschlag:

Der Personal- und Verwaltungsausschuss nimmt den Sachstand zur Kenntnis

Finanzielle Auswirkungen:

Keine

Erläuterungen:
Die Ratsfraktion "DIE LINKE" hat mit Datum 11. Juli 2013 nachfolgenden Ratsantrag Herrn Oberbürgermeister übergeben:
Die Verwaltung wird beauftragt, die Rechner der Stadtverwaltung schrittweise mit GnuPG³ oder einem anderen Programm auszustatten, welches den Bürger/innen eine OpenPGP-verschlüsselte Kommunikation ermöglicht. Begründung: Nachdem kürzlich bekannt wurde, dass Kommunikation per E-Mail im Regelfall von unbefugten Dritten mitgelesen wird, halten wir es für dringend notwendig, den Bürgerinnen und Bürgern eine sichere E-Mail-Kommunikation mit der Stadtverwaltung zu ermöglichen. Bei OpenPGP² handelt es sich um ein freies und standardisiertes Protokoll, welches für alle Aachener/innen, die über E-Mail verfügen nutzbar ist. Zudem handelt es sich um freie Software, so dass nur geringe Kosten entstehen.

Die E-Mail hat sich in den letzten Jahren zu einem beliebten und oft genutzten Kommunikationswerkzeug entwickelt, nicht nur zwischen Freunden, Bekannten und Familienangehörigen, sondern auch in der Geschäftswelt ist die E-Mail eine wichtiger Bestandteil vieler, ja fast aller Prozesse. Richtig ist, sowie im Ratsantrag beschrieben, dass die Mail relativ einfach mitgelesen werden kann, ja es ist so, als würde man eine Postkarte, eben nur ist in diesem Fall elektronisch, verschicken.

Das hat vor vielen Jahren auch der Gesetzesgeber erkannt und mit dem Verwaltungsverfahrensgesetz (VwVfG) entsprechende Regelungen für rechtsverbindliche elektronische Nachrichten (§ 3 a Verwaltungsverfahrensgesetz NW) geschaffen. Dies bedeutet konkret, dass eine Kommune in NRW auf der Homepage den Zugang für rechtsverbindliche elektronische Nachrichten (gem. § 3 a Verwaltungsverfahrensgesetz NW) eröffnen muss. Dem sind bisher nur wenige Städte in NRW- und dies nur eingeschränkt- gefolgt.

Die Stadt Aachen hat den elektronische Zugang zur Verwaltung - insbesondere die Übermittlung elektronischer Dokumente - für eine rechtsverbindliche elektronische Kommunikation zwischen Bürgern und Bürgerinnen, juristischen Personen des privaten und öffentlichen Rechts und der Verwaltung im Sinne des § 3 a Abs. 1 Verwaltungsverfahrensgesetz (VwVfG) ausdrücklich nicht eröffnet. Die Einschränkung gilt vor allem für die Zugänge per Email-Adresse, für Email-Kontaktformulare als auch für jede Art von Web-Formularen und sonstigen Zugängen. Das bedeutet, dass der heute gelebte Mail-Verkehr zwischen Bürgerinnen und Bürgern keinen rechtsverbindlichen Status besitzt.

Die Verschlüsselung über OpenPGP Datenformate, so wie im Ratsantrag beschrieben, ist zwar grundsätzlich möglich, aber vom organisatorischen und technischen Aufwand nicht zu vertreten und nur schwer zu händeln. Angenommen, 40% der Aachener Bürger (derzeitige Quote der Online Nutzer Bewohnerparken) würden mit einem der über 2000 MitarbeiterInnen der Verwaltung kommunizieren wollen, könnte das bedeuten, dass theoretisch bis zu 100.000 Zertifikate (öffentliche Schlüssel) der Bürger von unserem Mailingsystem GroupWise pro User verwaltet werden müssten. Der Bürger die Bürgerinnen wiederum hätten es mit einer Vielzahl von öffentlichen Schlüsseln der von ihnen

kontaktierten VerwaltungsmitarbeiterInnen zu tun. Die jeweiligen Zertifikate würden im Arbeitsplatzrechner gespeichert und übernähmen vor dem Senden die Verschlüsselung der Mail bzw. die Entschlüsselung (privater Schlüssel) nach Erhalt der Mail (Ende-zu-Ende-Verschlüsselung).

Dies bedeutet konkret, dass auch jeder Bürger, der mit einem Partner verschlüsselt kommunizieren möchte, ein solches Schlüsselpaar genieren, verwalten und dem jeweiligen Partner bekannt geben (öffentlicher Schlüssel) müsste. Da die Schlüssel rechnerseitig abgelegt werden, müssten diese bei Rechnerwechsel, Neuinstallationen, verschiedenen Programmänderungen oder Anpassungen vom Benutzer gesichert bzw. neu erzeugt werden.

Dieser unbefriedigende o.b. Zustand der nicht verschlüsselten Mail ist der Verwaltung bewusst, an Lösungen wird seit längerer Zeit gearbeitet. In den nächsten Wochen fällt eine Systementscheidung für eine Portalsoftware (Inter- und Intranet) der Stadt Aachen. Portale zeichnen sich durch die Integration von Anwendungen, Prozessen und Diensten aus. Ein Portal stellt seinem Benutzer verschiedene Funktionen wie beispielsweise Personalisierung, Sicherheit, Navigation, Suche, Benutzerverwaltung, Payment-Funktionalitäten und Kommunikation zur Verfügung. Die Portalsoftware bietet u.a. auch ein Auftragsmanagement für Antragsteller und Sachbearbeiter an. Über einen gesicherten Zugangsweg (SSL) kann ein im Bürgerkonto registrierter Benutzer Anträge, Schreiben oder Formulare einreichen, diese werden dann dem zuständigen Sachbearbeiter zugewiesen und durch diesen bearbeitet. Nach Erledigung erhält der Bürger eine E-Mail, dass sein Anliegen erledigt ist und dass Dokumente im Bürgerportal wieder abgeholt werden können. Dies erfolgt auf dem gleichen gesicherten Weg wie die Einreichung.

Mit dem Aufbau und der Zugänglichkeit des Internetportals wird im 2. Quartal des nächsten Jahres gerechnet. Selbstverständlich sind alle Mails, die innerhalb der Verwaltung per GroupWise verschickt werden, verschlüsselt.

[2]OpenPGP ist ein standardisiertes (http://de.wikipedia.org/wiki/Standard) Datenformat für verschlüsselte und digital signierte Daten. Auch wird das Format von Zertifikaten (http://de.wikipedia.org/wiki/Digitales_Zertifikat) festgelegt, die landläufig auch als „Schlüssel (http://de.wikipedia.org/wiki/Schl%C3%BCssel_%28Kryptologie%29)“ bezeichnet werden. Es basiert auf dem Format, das von PGP (http://de.wikipedia.org/wiki/Pretty_Good_Privacy) 5 eingeführt wurde und ist im RFC 4880 (http://tools.ietf.org/html/rfc4880) standardisiert.
[3]GnuPG erlaubt die Verschlüsselung und Signierung von Daten und Kommunikation, ist mit einer vielseitigen Schlüsselverwaltung ausgestattet und verfügt über Zugriffsmodule für alle Arten von öffentlichen Schlüsselverzeichnissen. GnuPG, auch unter GPG bekannt, ist ein Kommandozeilenwerkzeug mit Eigenschaften, die eine leichte Integration in andere Anwendungen erlaubt.

Anlage/n: