

## Beantwortung einer Anfrage nach § 4 der Geschäftsordnung öffentlicher Teil

Gremium	Datum
Ausschuss Allgemeine Verwaltung und Rechtsfragen / Vergabe / Internationales	11.12.2017

### Beantwortung der Anfrage der Ratsgruppe BUNT AN/1723/2017 Sicherheitslücke Ratsinformationssystem

#### Anfragetext:

1. Gibt es Kenntnisse über Sicherheitsprobleme des Kölner RIS, und wenn ja: Welche Schlüsse zieht die Verwaltung daraus?
2. Plant die Stadtverwaltung alle Passwörter zurückzusetzen und z. B. durch zufallserzeugte zu ersetzen?
3. Wie werden Bezirksvertreter\*innen mit dem RIS-System vertraut gemacht?
4. Welche Erfahrungen hat die Stadt Köln mit der Umsetzung der Standardisierung des RIS gemacht?
5. Wann kann mit einer RIS-App und der E-Mail-Benachrichtigung je Ausschuss gerechnet werden, und welche weiteren Optimierungen sind geplant?

#### Stellungnahme der Verwaltung:

Zu 1.: Die diversen Presseartikel, die sich mit der Sicherheit von Ratsinformationssystemen und möglichen Schwachstellen beschäftigen, sind den beteiligten Ämtern der Stadtverwaltung bekannt.

Aufgrund der Berichterstattung hat die Stadtverwaltung eine Stellungnahme des Herstellers angefordert, der wie folgt geantwortet hat:

Bei den von dem renommierten Sicherheitsanalysten Martin Tschirsich untersuchten Ratsinformationssystemen verschiedener Herstellerfirmen wurde eine Reihe von Schwachstellen aufgedeckt. Diese lassen sich nach Auskunft von der Fa. Somacos in drei Kategorien zuordnen:

- Produktsicherheit, hier konkret die WEB-Anwendung „Ratsinformationssystem“ in Verantwortung des Herstellers.
- Technisch, organisatorische Maßnahmen durch den Endkunden
- Technisch, organisatorische Maßnahmen durch den Betreiber / Hosting Partner

#### Zur Produktsicherheit:

Alle möglichen Schwachstellen in Informationssystemen, die bekannt waren, wurden mit dem Release Stand SessioNet 4.8.4 am 26.06.2017 beseitigt. Diese aktualisierte Version wurde

durch die Stadt Köln aus Sicherheitsgründen produktiv gesetzt.

Diese Schwachstellen sind Somacos entweder selbst im Rahmen von Maßnahmen der Produktentwicklung bzw. durch externe Sicherheitstests bekannt geworden. Das Verfahren wird periodisch durch Externe überprüft. Die Prüfung von Schwachstellen basiert dabei auf den neuesten Best-Practices. (OWASP-Empfehlungen 2017

<https://www.heise.de/developer/meldung/Schwachstellen-in-Webanwendungen-OWASP-Top-10-ist-2017-staerker-von-der-Community-gepraegt-3894946.html>).

### **Technisch, organisatorische Maßnahmen durch die Stadt Köln (als Betreiber und Endkunden):**

Die Stadt Köln betreibt das Ratsinformationssystem auf eigener Infrastruktur (Server, Firewalls, Netze) und hat damit die verwendeten Komponenten des RIS im Blick. Die Systeme werden laufend mit Sicherheitsupdates versorgt und entsprechend der aktuellen Anforderungen an die Sicherheit konfiguriert und aktualisiert.

Als zusätzlicher Schutz dient die Veröffentlichung der RIS-Website über ein redundantes Reverse Proxy System. Der Client kommuniziert dadurch nie direkt mit dem Webserver.

Zudem wurde vor ca. 2 Jahren der unverschlüsselte Zugriff mittels „http“ auf das RIS abgeschaltet und Nutzer zur Verwendung von „https“ automatisch umgeleitet.

Ergänzend dazu pflegt die Stadt Köln kontinuierlich die verwendbaren „https“-Verschlüsselungsalgorithmen – so wurde SSLv3 seinerzeit deaktiviert (Stichwort: Poodle-Lücke).

Damit „nicht-öffentliche“ Dokumente im Falle eines Problems bei der Produktsicherheit durch das reine Ausprobieren von Dokumentennummern nicht erreicht werden können, befinden sich referenzierte öffentliche Dokumente des RIS in einem separaten Ablageort.

Der Stadt Köln sind mit heutigem Stand keine aktuellen Sicherheitsprobleme des Kölner RIS bekannt. Sobald die Stadt Köln Schwachstellen des Systems findet oder Hinweise darauf erhält, wird die Stadt Köln schnellstmöglich eine Härtung der Sicherheitsmaßnahmen einleiten.

Zu 2.: Das über die Internetseite der Stadt Köln zugängliche Portal (<https://buergerinfo.stadt-koeln.de>) erfordert keine Anmeldung, weil ausschließlich öffentliche Informationen bereitgestellt werden. Die beiden Portale für den Zugriff auf nicht-öffentliche Informationen (Mitarbeiter- und Gremieninformationssystem) sind aus dem Internet nicht frei zugänglich.

Ende des Jahres 2016 kam mit dem Thema mobile Gremienarbeit und den Zugriffen über die iPad App Mandatos eine weitere Zugriffsvariante auf das RIS hinzu. Neben einem Benutzernamen und einem selbst festgelegten Passwort (nach zufallsgenerierten Initialpasswort) sichert ergänzend ein zweiter Faktor (z.B. VPN-Verbindung) den Zugang zum System ab.

Zusätzlich zu den vorgenannten Sicherheitsmerkmalen werden die für den Zugriff berechtigten iPads in einem Mobile Device Management geführt und die Verwendung eines Gerätecodes als weiteren Authentifizierungsschritt vorgeschrieben (alternativ können Fingerabdruck oder Gesichtserkennung genutzt werden, sofern das Gerät dies unterstützt). Durch die Verwendung der iPad Sicherungsmechanismen wird der Zugang zu Mandatos schneller und komfortabler als zuvor. Die Anmeldedaten für den SessionNet Zugang (Username und Dauerpasswort) werden in dem Fall zwischengespeichert und erst nach einer manuellen Änderung oder Sperre wieder abgefragt. Bei Verwendung der biometrischen Möglichkeiten steigt der Schutz nochmals.

Unabhängig von der iPad Lösung, hat jede Mandatsträgerin und jeder Mandatsträger die Möglichkeit, selbst sein Kennwort in einem beliebigen Intervall am städtischen PC zu ändern. Nach zu vielen Fehleingaben erfolgt automatisch eine Sperre des Kontos (um z.B. Brute-Force Attacken zu verhindern) - zusätzlich können Konten durch die Stadt Köln manuell gesperrt werden.

Die momentane Lösung, die Passwörter der Mandatsträgerinnen und Mandatsträger der Stadt Köln nicht ablaufen zu lassen – ist ein Kompromiss aus Sicherheit und Sicherung der Arbeitsfähigkeit, um einen komfortablen Zugriff zu gewähren und damit die papierlose Arbeit zu etablieren.

Mit steigender Erfahrung und Sensibilisierung der Anwenderinnen und Anwender für die neuen Arbeitsmittel können in Zukunft weitere Maßnahmen zur Erhöhung der Sicherheit umgesetzt werden.

Zu 3.: Die Bezirksvertreterinnen und Bezirksvertreter werden, in einem persönlichen Termin bei der Einrichtung und Übergabe des iPads für die digitale Gremienarbeit von dem Mobile Support der Stadt Köln mit dem Gerät und dem RIS vertraut gemacht. Darüber hinaus werden Schulungen angeboten, die auch Sicherheitsrelevante Informationen zum Inhalt haben. Sowohl das Büro der Oberbürgermeisterin (OB/2-22 Digitales Gremienmanagement) wie auch der Mobile Support stehen telefonisch und persönlich für Hilfestellungen und Beratungen zur Verfügung.

Warum die Berliner Bezirksverordneten keine Sicherheitseinweisung erhalten haben ist hier nicht bekannt. In Köln werden alle Mandatsträgerinnen und Mandatsträger sowohl bei Ausgabe der Geräte wie auch bei der anschließenden Schulung auf die sicherheitsrelevanten Aspekte hingewiesen.

Zu 4.: Diese Frage wurde bereits am 16.06.2017 unter der Vorlagennummer 1773/2017 beantwortet (siehe Antwort zu Frage 5 im folgenden Dokument: <https://ratsinformation.stadt-koeln.de/getfile.asp?id=615849&type=do&> ).

Zu 5.: Die Stadt Köln wurde vom Bundesministerium des Innern im Rahmen eines bundesweiten Wettbewerbs als eine von neun Modellkommunen für Open Government in Deutschland ausgewählt. Im Projekt soll das Kölner Ratsinformationssystem zu einem umfassenden Serviceportal weiterentwickelt und mit interaktiven nutzerfreundlichen Funktionen versehen werden. Als Basis dienen Offene Daten, die aus dem Kölner Ratsinformationssystem generiert und über die OParl-Spezifikation produktiv eingebunden werden sollen. Das Anforderungsprofil für das neue Serviceportal wird zurzeit in einem offenen Prozess gemeinsam mit der Zivilgesellschaft entwickelt.  
Ein Zeitplan der Umsetzung einzelner Funktionen ist Stand heute nicht möglich.

Die Möglichkeit, sich über aktuelle Vorlagen eines Ausschusses per Mail informieren zu lassen, gibt es derzeit nicht. Im Rahmen der Verwaltungsreform soll dies jedoch bei einem zu entwickelnden „ServicePortal“ berücksichtigt werden.

Aus technologischer Sicht ist es möglich, die erweiterten Services über eine mobilfähige Webanwendung umzusetzen. Die Entwicklung einer eigenen RIS-App ist daher nicht unbedingt erforderlich.

**gez. Reker**