Kreuzlingen

Stadtrat

Sperrfrist für alle Medien
Veröffentlichung erst nach der Medienkonferenz zur Gemeinderatssitzung

Beantwortung

Schriftliche Anfrage „Informationssicherheit in der Stadtverwaltung Kreuzlingen“

Am 15. Dezember 2016 reichte Gemeinderat Alexander Salzmann, Fraktion FDP/EVP, eine schriftliche Anfrage betreffend „Informationssicherheit in der Stadtverwaltung Kreuzlingen“ ein (Beilage).

Der Stadtrat beantwortet die Fragen wie folgt:

1 Wie hoch erachtet die Stadt das Risiko des Datenverlusts, der Datenmanipulation oder des Datendiebstahls von Daten der städtischen Verwaltung (inkl. Technischer Betriebe)? Bitte um entsprechende Begründung.

Stadtverwaltung
Das Risiko eines Datenverlustes wird als gering eingestuft. Alle Systeme sind in sich redundant. Das Risiko einer externen Datenmanipulation wird ebenfalls als gering eingestuft. Die Stadt wird durch die Firewall über das Amt für Informatik des Kantons Thurgau (AFI) und durch eine eigene Firewall geschützt. Der gesamte Internetverkehr wird nach Malware und Viren gescannt.

Die Stadt schützt sich im Rahmen der technischen Möglichkeiten gegen Datendiebstähle. Generell können jedoch Datendiebstähle nie vollständig ausgeschlossen werden.

Technische Betriebe Kreuzlingen (TBK)
Dieser Teil der Antwort bezieht sich nur auf die Datensysteme der TBK ausserhalb des städtischen Netzwerks. Die Systeme der TBK, wie das ERP System Abacus zur finanziellen Abbildung aller Geschäftsprozesse, die Energieverrechnungssoftware ISE und das Netzinformationssystem GeoNis werden durch die städtische IT betrieben. Die TBK nutzen das Dateisystem der Stadt auch zur Ablage von Daten und deren Archivierung.

Ausserhalb der städtischen IT-Umgebung bestehen die Leitstelle Strom und Gas sowie die Rundsteueranlage. Diese Systeme erzeugen und speichern Protokolle. Sie steuern bzw. schalten Komponenten des Netzes.

Die TBK sehen das Risiko bei dieser IT-Infrastruktur als klein an, da die Systeme in einem nur für diese Anwendung erstellten Netzwerk betrieben werden (Direktverbindung über Lichtwellenleiter oder Kupferkabel). Die Verbindung nach aussen ist lediglich für Wartungszwecke über einen durch eine Firewall gesicherten, zugriffsgeschützten Zugang durch den Systemlieferanten möglich. Physikalisch sind Leitstelle und Rundsteueranlage in einem rund um die Uhr verschlossenen und nur für Befugte zugänglichen Raum untergebracht. Sollten Daten verloren gehen, ist dies für den Betrieb der Anlagen nicht risikobehaftet, da die Daten nur der laufenden Steuerung dienen.

Die Speicherung von Daten dient nur der Plausibilisierung aggregierter Messdaten (Zusammenfassung von Einzelwerten) oder dem Nachweis der Einhaltung von Normen. Eine Datenmanipulation könnte sich entsprechend nur auf die Daten der Vergangenheit auswirken. Problematischer könnte ein Angriff sein, der eine Übernahme der Netzsteuerung anstrebt. Die Vorkehrungen gegen einen solchen Angriff sind eine Benutzerverwaltung/Zugriffskontrolle und eine Firewall, wobei nur eine Verbindung nach aussen zu Wartungszwecken besteht.

Im Weiteren gibt es Datensysteme, die Verbrauchsdaten übermitteln und halten. Es handelt sich um die Zählerfernauslesung und das Energiedatenmanagementsystem. Diese Prozesse sind ausgelagert.

Bei Datensystemen, die Verbrauchsdaten übermitteln und halten, wird das Risiko als höher erachtet. Die Datenverbindungen der Zählerfernauslesung erfolgt über ein Mobilfunkprotokoll der Swisscom zu den von den TBK beauftragten Unternehmen für Energielogistik. Das Energiedaten-Managementsystem wird durch diese Unternehmen betrieben. Nach Plausibilitätsprüfung erhalten die TBK die Verrechnungsdaten per E-Mail zugestellt.

Das mit dem grössten Teil der Energielogistik betraute Unternehmen EBM Energie AG (in der Nachfolge der Swisspower Energy AG) äussert sich zur Fragestellung wie folgt: „Wir erachten das Risiko des Datenverlusts, Datendiebstahls oder

der Datenmanipulation durch Externe als gering. Unser Rechenzentrum entspricht einem Tier 3-Rechenzentrum und verfügt über die notwendigen Schutzfunktionen (Biometrische Zutrittskontrolle, Videoüberwachung, Firewall-Systeme, Multi Netzwerk Segmentierung etc.). Zudem sind wir SAP-zertifizierter Hoster und werden regelmässig durch PwC, Deloitte wie auch KPMG auditiert."

2 Nach welchen Standards der Informationssicherheit betreibt die Stadtverwaltung (inkl. TBK) ihre IT? Hat sie die Informationssicherheit an andere Organisationen ausgelagert, wenn ja an wen?

Stadtverwaltung
Um alle Daten angemessen zu schützen, wird ein IT-Grundschutz betrieben. Die Informationssicherheit ist teilweise ausgelagert. Steuer- und Finanzdaten sind im Rechenzentrum der Verwaltungsrechenzentrum AG St. Gallen (Informationssicherheits-Managementsystem mit ISO/IEC 27001:2005 bzw. Produktion mit ISO 9001:2008 zertifiziert) und im AFI (ebenfalls mit ISO 9001 und 27001 zertifiziert) gespeichert.

TBK
Energiedatenmanagementsysteme und Zählerfernauslesung sind ausgelagert. Die reguläre Zählerfernauslesung aller Industrie- und Gewerbekunden sowie der Betrieb des zugehörigen Energiedaten-Managementsystems erfolgt bei EBM Energie AG. Die EBM Energie AG äussert sich zur Fragestellung wie folgt: „Unsere Rechenzentren entsprechen dem Tier-3-Standard. Zudem sind wir SAP-zertifizierter Hoster und in der Erstellung des ISAE3402 Prüfberichts (verfügbar Ende Q4 2017). Unsere Prozesse basieren auf ITIL-Standards und sind in unserem internen System dokumentiert und transparent nachvollziehbar."

Technisch begründet bestehen zwei weitere ausgelagerte Messdatenprozesse. Die bestehende Smart Meter Pilotinstallation der TBK (ca. 90 Zähler) wird bei SWIBI AG verarbeitet. Die Messdaten werden lediglich im Zuge der Weiterführung der Pilotinstallation erhoben. Die Verrechnungsdaten werden aber aus Effizienzgründen (sehr kleine Anzahl Zähler) auf konventionellem Weg durch Vor-Ort-Ablesung erhoben.

Die GWF AG betreibt die Zählerfernauslesung für Mengenumwerter bei etwa 10 grossen Erdgaskunden. Die Abrechnungsdaten werden im Verrechnungssystem nochmals plausibilisiert. Eine Vor-Ort-Ablesung wäre im Falle des Zweifels an Verrechnungsdaten nach wie vor möglich.

3 Bitte beschreiben Sie die Regeln und Verfahren für den Austausch, Spiegelung, Speicherung und der sicheren Beseitigung der betroffenen Datenträger. Erachten Sie die Regeln sowie deren Einhaltung als genügend? Sofern nein, welche Massnahmen sind vorgesehen?

Stadtverwaltung
Der Austausch der Daten erfolgt per Mail, Memorystick oder über unser Fileshare System (verschlüsselte Übertragung). Vertrauliche Daten der Sozialen Dienste werden über eine externe verschlüsselte Plattform ausgetauscht. Es wird eine tägliche Datensicherung ausgeführt. Die Daten werden getrennt aufbewahrt (Stadthaus, TBK und Banksafe). Auf dem Datenstorage (Speicherlösung) wird alle zwölf Stunden, zusätzlich zur Datensicherung, ein Snapshot des ganzen Datenbestandes erstellt. Defekte Datenträger und alte Hardware werden mechanisch unbrauchbar gemacht. Es sind keine weiteren Massnahmen vorgesehen.

TBK
Bei den eigenen Systemen der TBK, wie Leitstelle und Rundsteueranlage, besteht keine Notwendigkeit für Austausch, Spiegelung oder Speicherung von Daten.

Zum Energiedaten-Managementsystem und zur Zählerfernauslesung äussert sich die EBM Energie AG wie folgt: „Abhängig vom Service Level Agreement (SLA) für den jeweiligen Service spiegeln wir die Systeme synchron in unser zweites Rechenzentrum (ca. 10 km) entfernt oder haben die Spiegelung auf der Stufe der Applikation synchron implementiert (z. B. SQL AlwaysOn). Das Backup erfolgt mittels professioneller Backup Software (TSM – Tivoli Storage Manager) jeweils ins andere Rechenzentrum. Die Beseitigung von Datenträgern erfolgt mittels verschlossenen Datareg Containern, die abgeholt und der Inhalt professionell beseitigt wird. Wir erachten die Regeln und die Systeme als genügend.“

4 Bitte beschreiben Sie die Verfahren zur Sicherstellung der kritischen Prozesse im Falle eines grossflächigen IT-Ausfalls. Erachten Sie die Regeln sowie deren Einhaltung als genügend? Sofern nein, welche Massnahmen sind vorgesehen?

Stadtverwaltung
Bei einem grossflächigen Ausfall der IT-Systeme (insbesondere Netzausfall) können die Rechenzentren - bei denen geschäftskritische Applikationen betrieben werden - nicht mehr erreicht werden. Der Handlungsspielraum der Stadt ist gering. Es kann angenommen werden, dass bei diesem Katastrophen-Szenario im Interesse sämtlicher Nutzerinnen und Nutzer der Wiederherstellung der Betriebsbereitschaft höchste Priorität beigemessen wird. Die Stadtverwaltung betreibt zudem keine Internetseiten, von denen sie abhängig ist. Im Werkhof werden Anlagen ferngesteuert und kontrolliert. Diese Steuerungen können manuell geprüft und eingestellt werden.

TBK
Der kritischste Prozess der TBK ist die Steuerung der Netze im Falle eines IT-Ausfalls. Damit müsste vor Ort in den Stationen geschaltet werden, es wäre keine zentrale Steuerung mehr vorhanden. Alle Mitarbeitenden der TBK, die Pikettdienst leisten, sind in der Lage, diese Schaltungen auszuführen. Dennoch wäre eine verlängerte Reaktionszeit die Folge.

Zum Energiedaten-Managementsystem und zur Zählerfernauslesung äussert sich die EBM Energie AG wie folgt: „Im Falle eines Desasters eines Rechenzentrums verfügen wir abhängig vom SLA des jeweiligen Services über eine synchrone Spiegelung im zweiten Rechenzentrum wo der Betrieb weiterhin sichergestellt ist. Zusätzlich sind sämtliche Massnahmen und Prozeduren im Business Continuity und Desaster Recovery Handbuch niedergeschrieben. Ebenfalls prüfen wir regelmässig die Dieselgeneratoren durch simulierte Stromausfälle. Wir erachten die Massnahmen und Systeme als genügend, was uns die externen Audits bestätigen."

5 Gab es in den letzten 24 Monaten Hacker-Angriffe auf die Stadt (Server) bzw. TBK (z. B. Steuerungskomponenten auf Netzinfrastrukturen)? Wenn ja, welche Dateneinsicht erhielt der Hacker und welche konnte er verändern?

Stadtverwaltung
Hackerangriffe auf das Kantonsnetz finden dauernd statt. Die umfangreichen Sicherheitssysteme des AFI schützen die Stadt gegen diese Attacken. Hackerangriffe auf die Stadtverwaltung sind nicht bekannt.

TBK
Angriffe auf die eigenen Systeme der TBK oder ihrer Dienstleister sind nicht bekannt.

6 Zum Testen der eigenen Informationssicherheit kann sporadisch eine spezialisierte Firma beauftragt werden, zu versuchen, das Netzwerk des Auftraggebers zu hacken. Hat die Stadt einen solchen Auftrag jemals vergeben und was war das Resultat? Wenn nein, warum nicht?

Stadtverwaltung
Die Stadtverwaltung hat im Juli 2015 mit einem spezialisierten und zertifizierten Informatik-Sicherheitsunternehmen ein Premium Audit zur IT-Sicherheit durchgeführt. Zur weiteren Verbesserung wurde durch den Auftragnehmer eine Massnahmenliste definiert. Die Vorschläge wurden geprüft und grossmehrheitlich umgesetzt.

TBK
Mit kompletter Fertigstellung des Leitsystems wird eine spezialisierte externe Firma die Sicherheit von aussen überprüfen. Es haben hierzu bereits seit etwa anderthalb Jahren Gespräche zur Vorbereitung des Audits stattgefunden.

Kreuzlingen, 7. März 2017

Stadtrat Kreuzlingen

Andreas Netzle, Stadtpräsident

Thomas Niederberger, Stadtschreiber

Beilage
Schriftliche Anfrage „Informationssicherheit in der Stadtverwaltung Kreuzlingen“

Mitteilung an
- GR Alexander Salzmann, Ebenalpstrasse 41, 8280 Kreuzlingen
- Mitglieder des Gemeinderates
- Medien

FDP
Die Liberalen

EVP
Evangelische Volkspartei

FDP/EVP Fraktion
der Stadt Kreuzlingen
8280 Kreuzlingen

Fragesteller:
Alexander Salzmann
T +41 (0)79 654 22 48
alexander.salzmann@gmx.ch

Kreuzlingen, 15.12.2016

Schriftliche Anfrage zur Informationssicherheit in der Stadtverwaltung Kreuzlingen gemäss Art. 45 der Geschäftsordnung des Gemeinderats

In letzter Zeit wird immer mehr berichtet über erfolgreiches Eindringen in Datenbanken namhafter Firmen oder auch Gesellschaften mit wichtigen Infrastrukturen. Dazu gehört meines Erachtens vor allem, aber nicht nur, die Netzinfrastrukturen der Technischen Betriebe. Grundlage für die betriebliche Handlungsfähigkeit und den wirksamen Schutz von Informationen ist eine definierte, eindeutig zuweisbare und nachvollziehbare Verantwortlichkeit für Informationen bzw. Datenbestände und Applikationen.
Zur Stadtverwaltung (inklusive Technischer Betriebe) stelle ich hiermit im Namen der FDP/EVP-Fraktion folgende Fragen zur Informationssicherheit:

1. Wie hoch erachtet die Stadt das Risiko des Datenverlusts, der Datenmanipulation oder des Datendiebstahls von Daten der städtischen Verwaltung (inkl. Technischer Betriebe)? Bitte um entsprechende Begründung.

2. Nach welchen Standards der Informationssicherheit betreibt die Stadtverwaltung (inkl. TBK) ihre IT? Hat sie die Informationssicherheit an andere Organisationen ausgelagert, wenn ja an wen?

3. Bitte beschreiben Sie die Regeln und Verfahren für den Austausch, Spiegelung, Speicherung und der sicheren Beseitigung der betroffenen Datenträger. Erachten Sie die Regeln sowie deren Einhaltung als genügend? Sofern, nein, welche Massnahmen sind vorgesehen?

4. Bitte beschreiben Sie die Verfahren zur Sicherstellung der kritischen Prozesse im Falle eines grossflächigen IT-Ausfalls. Erachten Sie die Regeln sowie deren Einhaltung als genügend? Sofern, nein, welche Massnahmen sind vorgesehen?

5. Gab es in den letzten 24 Monaten Hacker-Angriffe auf die Stadt (Server) bzw. TBK (z.B. Steuerungskomponenten auf Netzinfrastrukturen)? Wenn ja, welche Dateneinsicht erhielt der Hacker und welche konnte er verändern?

6. Zum Testen der eigenen Informationssicherheit kann sporadisch eine spezialisierte Firma beauftragt werden, zu versuchen, das Netzwerk des Auftraggebers zu hacken. Hat die Stadt einen solchen Auftrag jemals vergeben und was war das Resultat? Wenn nein, warum nicht?

Mit freundlichen Grüssen

Alexander Salzmann, Gemeinderat FDP

A. Sal