Stadt Kitzingen

AMT:	1
Sachgebiet:	12
Vorlagen.Nr.:	2017/215
Datum:	21.09.2017

Sitzungsvorlage an den

Stadtrat	28.09.2017	öffentlich	zur Entscheidung

Kitzingen, 21.09.2017 ..... Amtsleitung	Mitzeichnungen:	Kitzingen, 21.09.2017 ..... Oberbürgermeister

Bearbeiter:	Wolfgang Zürrlein	Zimmer:	6.1
E-Mail:	wolfgang.zuerrlein@stadt-kitzingen.de	Telefon:	09321/20-1201
Maßnahme:			

Überörtliche Prüfung der Jahresrechnungen 2011 - 2015
Textziffern TZ 7 b; TZ 1 a; b; c; d; e; f; TZ 2 a; b; TZ 6 b; TZ 7 a bb; TZ 8 a; b; c, e

Beschlussentwurf:
Von Sachvortrag wird Kenntnis genommen

1. TZ 7 b) Online-Banking

   Es wird davon Kenntnis genommen, dass der Rechnungsprüfungsausschuss in seiner Sitzung am 18.07.2017 die Stellungnahme des SG12/IT ohne Änderungen anerkannt hat.

   Dieser Entscheidung des Rechnungsprüfungsausschusses wird zugestimmt.

2. TZ 1 a) Ungeeignete Absicherung administrativer Benutzerkonten im lokalen Netzwerk

   Es wird davon Kenntnis genommen, dass der Rechnungsprüfungsausschuss in seiner Sitzung am 18.07.2017 die Stellungnahme des SG12/IT ohne Änderungen anerkannt hat.

   Dieser Entscheidung des Rechnungsprüfungsausschusses wird zugestimmt.

3. TZ 1 b) Weitere Hinweise zur Benutzerkontenverwaltung über den Verzeichnisdienst Active Directory

   Es wird davon Kenntnis genommen, dass der Rechnungsprüfungsausschuss in seiner Sitzung am 18.07.2017 die Stellungnahme des SG12/IT ohne Änderungen anerkannt hat.

   Dieser Entscheidung des Rechnungsprüfungsausschusses wird zugestimmt.

4. TZ 1 c) Verbesserung beim Virenschutz

   Es wird davon Kenntnis genommen, dass der Rechnungsprüfungsausschuss in seiner Sitzung am 18.07.2017 die Stellungnahme des SG12/IT ohne Änderungen anerkannt hat.

   Dieser Entscheidung des Rechnungsprüfungsausschusses wird zugestimmt.

5. TZ 1 d) Überarbeitung der Verzeichniszugriffsberechtigungen

   Es wird davon Kenntnis genommen, dass der Rechnungsprüfungsausschuss in seiner Sitzung am 18.07.2017 die Stellungnahme des SG12/IT ohne Änderungen anerkannt hat.

   Dieser Entscheidung des Rechnungsprüfungsausschusses wird zugestimmt.

6. TZ 1 e) Fehlerhafte Datensicherung und Vergrößerung des Sicherungszeitraums

   Es wird davon Kenntnis genommen, dass der Rechnungsprüfungsausschuss in seiner Sitzung am 18.07.2017 die Stellungnahme des SG12/IT ohne Änderungen anerkannt hat.

   Dieser Entscheidung des Rechnungsprüfungsausschusses wird zugestimmt.

7. TZ 1 f) Smartphones und „Bring your own Device“

   Es wird davon Kenntnis genommen, dass der Rechnungsprüfungsausschuss in seiner Sitzung am 18.07.2017 die Stellungnahme des SG12/IT ohne Änderungen anerkannt hat.

   Dieser Entscheidung des Rechnungsprüfungsausschusses wird zugestimmt.

8. TZ 2 a) Direkter Zugriff auf die Datenbank des Verfahrens OK.EWO – Einwohnermeldewesen

   Es wird davon Kenntnis genommen, dass der Rechnungsprüfungsausschuss in seiner Sitzung am 18.07.2017 die Stellungnahme des SG12/IT ohne Änderungen anerkannt hat.

   Dieser Entscheidung des Rechnungsprüfungsausschusses wird zugestimmt.

9. TZ 2 b) Ungeeignete Absicherung der Datenbank TDV HKR

   Es wird davon Kenntnis genommen, dass der Rechnungsprüfungsausschuss in seiner Sitzung am 18.07.2017 die Stellungnahme des SG12/IT ohne Änderungen anerkannt hat.

   Dieser Entscheidung des Rechnungsprüfungsausschusses wird zugestimmt.

10. TZ 6 b) Zugriff auf die Personalakten

    Es wird davon Kenntnis genommen, dass der Rechnungsprüfungsausschuss in seiner Sitzung am 18.07.2017 die Stellungnahme des SG12/IT mit folgender Änderungen anerkannt hat: Die Datenschutzbeauftragte der Stadt Kitzingen ist zukünftig bei den Zugriffsrechten miteinzubeziehen.

    Dieser Entscheidung des Rechnungsprüfungsausschusses wird zugestimmt.

11. TZ 7 a) bb) Punktuelle Überarbeitung der Benutzerrechte im OK.FIS

    Es wird davon Kenntnis genommen, dass der Rechnungsprüfungsausschuss in seiner Sitzung am 18.07.2017 die Stellungnahme des SG12/IT mit folgendem Hinweis anerkannt hat, dass die Probleme von der AKDB nun bereinigt wurden.

    Dieser Entscheidung des Rechnungsprüfungsausschusses wird zugestimmt.

12. TZ 8 a) die eingesetzten automatisierten Verfahren waren noch nicht fachlich freigegeben

    Es wird davon Kenntnis genommen, dass der Rechnungsprüfungsausschuss in seiner Sitzung am 18.07.2017 die Stellungnahme des SG12/IT ohne Änderungen anerkannt hat.

    Dieser Entscheidung des Rechnungsprüfungsausschusses wird zugestimmt.

13. TZ 8 b) Maßnahmen zur Sicherstellung der Informationssicherheit

    Es wird davon Kenntnis genommen, dass der Rechnungsprüfungsausschuss in seiner Sitzung am 18.07.2017 die Stellungnahme des SG12/IT ohne Änderungen anerkannt hat.

    Dieser Entscheidung des Rechnungsprüfungsausschusses wird zugestimmt.

14. TZ 8 c) Effizientere Anbindung der Außenstellen

    Es wird davon Kenntnis genommen, dass der Rechnungsprüfungsausschuss in seiner Sitzung am 18.07.2017 die Stellungnahme des SG12/IT ohne Änderungen anerkannt hat.

    Dieser Entscheidung des Rechnungsprüfungsausschusses wird zugestimmt.

15. TZ 8 e) Dienstanweisung für den IT-Betrieb

    Es wird davon Kenntnis genommen, dass der Rechnungsprüfungsausschuss in seiner Sitzung am 18.07.2017 die Stellungnahme des SG12/IT ohne Änderungen anerkannt hat.

    Dieser Entscheidung des Rechnungsprüfungsausschusses wird zugestimmt.

Sachvortrag:
Zu
TZ 7 b): Online-Banking
(Prüfbericht BKPV Seite 31 – 32)

Die Kassenmitarbeiter besaßen administrative Rechte für das Online-Banking-Verfahren. Die Berechtigungen beschränken sich mittlerweile auf die Aufgaben des einzelnen Kassenmitarbeiters.

aa) Einsatz sicherer Signaturerstellungseinheiten

Der BKPV beanstandet, dass die Signaturschlüssel der einzelnen Mitarbeiter lokal auf Rechner gespeichert waren.

Die IT Abteilung hat den Signaturschlüssel nun im Mitarbeiterverzeichnis hinterlegt, sodass ausschließlich der einzelne Mitarbeiter auf seinen Signaturschlüssel zugreifen kann. Der zweite Sicherheitsfaktor ist der PIN, mit dem man den Transfer bestätigt. Zudem gilt das vier Augen Prinzip und ein zweiter Mitarbeiter muss diesen Vorgang in gleicher Weise bestätigen(Kassenleiterin). Somit ist die Beanstandung erledigt.

Die höchste Sicherheitsstufe ist über Smartkartenlesegeräte gewährt, die der BKPV vorschlägt. Die Eingabe eines PIN erfolgt über ein Lesegerät. Momentan ist diese Variante in der Prüfung, inwiefern eine Umsetzung organisatorisch möglich ist.

bb) Berechtigung in SFIRM

Bei dem Programm SFIRM besaßen die Kassenmitarbeiter einen administrativen Zugang von der Bank. Die Programmadministration (z. B. Zuteilung der Berechtigung) und die Ausführung im Programm (z. B. Tätigen der Transaktion) unterliegen mittlerweile einer Trennung.

Zu
TZ 1 a): Ungeeignete Absicherung administrativer Benutzerkonten im lokalen Netzwerk
(Prüfungsbericht BKPV Seite 15 – 16)

Der"jboss-service"-Benutzer, welcher seitens der AKDB eingerichtet wurde, wurde deaktiviert und wird nicht mehr benötigt.

Es wird ein IT-Service Benutzerkonto verwendet, dessen Passwort nur den Administratoren (IT) bekannt ist. Alle Systemkonten haben zudem ein festes kryptisches Passwort mit hoher Passwortsicherheit(z.B. $5tR5=7Dfs§2lö?\). In der Dienstanweisung zur Informationstechnik vom 01.12.2016 werden in Anlage 5 Hinweise zu einem sicheren Passwort und allgemein der Umgang mit Passwörtern gegeben.

Zu
TZ 1 b): Weitere Hinweise zur Benutzerkontenverwaltung über den Verzeichnisdienst Active Directory
(Prüfungsbericht BKPV Seite 16 – 17)

aa) Personenbezogene Benutzerkonten auch zur Administration

Das einzige Benutzerkonto Administrator splittet sich nun in Benutzerkonten pro Mitarbeiter auf, die administrative Rechte besitzen. So ist nachzuvollziehen welcher Mitarbeiter der IT als Administrator arbeitet.

bb) Fernwartung durch externe Dienstleister

Die Hinweise des Prüfers sind bekannt und werden beachtet.

cc) Verwendung privilegierter Benutzerkonten für die täglichen Arbeiten

Des Weiteren besitzen die Mitarbeiter der IT „normale“ Benutzerkonten ohne administrative Rechte, die sie in der täglichen Arbeit einsetzen.

dd) Verbindlichkeit der Kontorichtlinien.

Die Kennwortänderung beschränkt die IT auf max. 90 Tage. Außerdem sperrt sich der Bildschirm nach 15 Minuten. Umsetzung über flächendeckende Gruppenrichtlinien, welche von den Usern nicht umgangen werden können!

Zu
TZ 1 c): Verbesserungen beim Virenschutz
(Prüfungsbericht BKPV Seite 17)

Der Prüfer bemängelt, dass nicht alle Server mit einem ausreichenden Virenschutz ausgestattet sind. Dies hat den Hintergrund, dass nicht an allen Servern aktiv gearbeitet wird. Einige Server nutzt die Stadtverwaltung lediglich für die Bereitstellung von Daten.

Eine Optimierung des Virenschutzes versucht die IT stetig umzusetzen. Zum heutigen Zeitpunkt sind nahezu alle Server mit einem Virenschutz ausgestattet.

Zu
TZ 1 d): Überarbeitung der Verzeichniszugriffsberechtigungen
(Prüfungsbericht BKPV Seite 17 – 18)

Die Verzeichnisse aktualisiert die IT. Alle wichtigen Verzeichnisse mit verwaltungskritischen Daten sind nun über Sicherheitsgruppen abgesichert, so dass gewährleistet ist, dass nur berechtigte User Zugriff haben

Zu
TZ 1 e): Fehlerhafte Datensicherungen und Vergrößerung des Sicherungszeitraums
(Prüfungsbericht BKPV Seite 18 -19)

Durch die Beschaffung neuer Server im Jahr 2016 konnten die Sicherungsroutinen bereits umgestellt und verbessert werden. Die Backupkapazitäten sind erweitert und Sicherungsrichtlinien wurden fixiert. Die tägliche Sicherung erfolgt durch die IT. Der Sicherungszeitraum beträgt zum heutigen Zeitpunkt 3 Jahre. (Tagessicherung 3 Generationen / Wochensicherung 4 Wochen / Monatssicherung 12 Monate / Jahressicherung 3 Jahre)

Zu
TZ 1 f): Smartphones und „Bring your own Device”
(Prüfungsbericht BKPV Seite 19)

Bisher konnte die IT die größten Sicherheitslücken bei Verwendung der Smartphones schließen. Bei Smartphonenutzung muss eine bestimmte App auf dem Smartphone installiert werden, die u. a. ein Kennwort fordert. Ein Fernzugriff auf das betreffende Gerät ist ebenfalls vorhanden, so dass bei Verlust ein Fernmlöschen des Gerätes möglich ist.

Zu
TZ 2 a): Direkter Zugriff auf die Datenbank des Verfahrens OK.EWO – Einwohnermeldewesen
(Prüfungsbericht BKPV Seite 19 -20)

Die Änderungen des direkten Zugriffes auf die Datenbank erfolgt im Moment in Abstimmung mit der AKDB. Die Datenbanken haben viele Schnittstellen zu anderen Fachprogrammen, daher gestaltet sich die Änderung des Zugriffes schwierig. Bis Ende 2017 werden alle Änderung abgeschlossen sein.

Zu
TZ 2 b): Ungeeignete Absicherung der Datenbank von TDV HKR
(Prüfungsbericht BKPV Seite 20)

Die Datenbank betrifft ein Altverfahren. Die Absicherung der Datenbank wurde realisiert. Passwortänderung wurde vorgenommen..

Zu
TZ 6 b): Zugriff auf die Personalakten
(Prüfungsbericht BKPV Seite 29 – 30)

Den Zugriff für das Dokumentenmanagement schränkte die IT so ein, dass der Administrator in dem System nur auf die Benutzerverwaltung zugreifen kann. Ein Zugriff auf Dokumente ist durch den Administrator so nicht mehr möglich.

Der Rechnungsprüfungsausschuss erkennt die Stellungnahme der TZ 6 b) mit folgender Änderung an: Die Datenschutzbeauftragte der Stadt Kitzingen ist zukünftig bei den Zugriffsrechten miteinzubeziehen

Zu
TZ 7 a) bb): Punktuelle Überarbeitung der Benutzerrechte im OK.FIS
(Prüfungsbericht BKPV Seite 31)

Die Benutzerrechte des Sachbearbeiters in der Steuerverwaltung schränkte die IT ein. Nach der Einschränkung konnte der Sachbearbeiter seine Arbeitsabläufe nicht mehr vollziehen. Die AKDB bereinigte die Probleme, sodass nun eine ordnungsgemäße Sachbearbeitung mit Beschränkung der Benutzerrechte funktioniert.

Der Rechnungsprüfungsausschuss erkennt die Stellungnahme der TZ 7a) bb) mit dem Hinweis, dass die Probleme von der AKDB nun bereinigt wurden, an.

Zu
TZ 8 a): Die eingesetzten automatisierten Verfahren waren noch nicht fachlich freigegeben.
(Prüfungsbericht BKPV Seite 34 – 35)

Jedes automatisierte Verfahren muss fachlich freigegeben werden. Das Verfahrensverzeichnis führt die Datenschutzbeauftragte der Stadt Kitzingen (bisher im SG 12). Das Verzeichnis dokumentiert die Freigabe des Programms durch den Hersteller und die fachliche Freigabe durch die Mitarbeiter. Alle Programme müssen vor Einführung geprüft und begutachtet werden. Zukünftig wird dieses Verzeichnis die neue Datenschutzbeauftragte der Stadt Kitzingen weiterführen.

Zu
TZ 8 b): Maßnahmen zur Sicherstellung der Informationssicherheit

Ein Informationssicherheitsteam besteht aus dem Leiter der IT sowie der Datenschutzbeauftragten und weiteren Mitarbeitern aus der Verwaltung, die ein Informationssicherheitskonzept erarbeiten. Nach der Erstellung erfolgt eine stetige Fortschreibung bzw. Aktualisierung des Konzeptes.

Ein Informationssicherheitsbeauftragter für die Stadt Kitzingen ist bis zum heutigen Tag noch nicht benannt worden.

Zu
TZ 8 c): Effizientere Anbindung der Außenstellen
(Prüfungsbericht BKPV Seite 36)

Die Tourist-Info verfügt über eine Anbindung über Funk. Derzeit mietet die Stadtverwaltung Leitungen für die Anbindung der vhs und des Bauhofes. Langfristig plant die Stadtverwaltung eine Anbindung über Glasfaserverbindungen.

Zu
TZ 8 e): Dienstanweisung für den IT-Betrieb
(Prüfungsbericht BKPV Seite 36)

Die Dienstanweisung ist am 01.12.2016 in Kraft getreten. Eine stetige Aktualisierung ist geplant.

Anlagen: