Prüfung der IT Infrastruktur der Stadt Sprockhövel

1	**Prüfungsauftrag** Der Sonderprüfungsauftrag ergibt sich aus dem Beschluss des Haupt- und Finanzausschusses vom 31. August 2017 sowie des Ratsbeschlusses vom 28. September 2017.
2	**Prüfungsgegenstand, -umfang und –verfahren** Gemäß der Beschlussfassung des Haupt- und Finanzausschusses und des Rates ist mit Hilfe eines Externen Gutachters die Entstehung der IT Infrastruktur der Stadt Sprockhövel zu rekonstruieren und aufzuzeigen. Auf Grundlage der vorhandenen schriftlichen Unterlagen, die die Mitarbeiter der EDV dem RPA und dem EDV Sachverständigen freiwillig zur Verfügung gestellt haben, wurde eine grobe Auswahl der Prüfschwerpunkte getroffen. Diese Schwerpunkte dienten dazu, die Prüfung besser zu koordinieren und einen Einblick in die Struktur der Entstehung des Zustandes der EDV zu erhalten. Da auf Grund fehlender Festplatten sowie des Postgeheimnisses kein Zugang zu allen Daten möglich war, konnte nur auf Sicherungsdateien zurückgegriffen werden. Die Stadtverwaltung Sprockhövel besaß eine Dienstvereinbarung, in der private E-Mails generell untersagt wurden, und daher das Postgeheimnis solange für die E-Mails nicht existierte, bis diese Dienstvereinbarung nicht mehr gültig war. Ein genauer Zeitpunkt für das Ablaufen der Dienstvereinbarung liegt nicht vor. Mit Schreiben vom 20.03.2014 (Anlage 1) hat der Personalrat dem Bürgermeister mitgeteilt, dass er die Verhandlungen über eine neue Dienstvereinbarung als gescheitert erklärt. Der Personalrat wollte eine neue Dienstvereinbarung beschließen, da in der gelebten Praxis private E-Mails von den städtischen Mitarbeitern bestehen, und dieses stillschweigend bis heute geduldet wurde. Deshalb gehen die Prüfer davon aus, dass generell in den E-Mail Postfächern auch private Mails enthalten sein können, so dass aus datenschutzrechtlichen Gründen ein Zugriff auf diese Mailkonten den Prüfern nicht gestattet ist. Zusätzlich wurden dem RPA freiwillige Besprechungsprotokolle der EDV übergeben. Aus denen ist ersichtlich, dass die Struktur und Lizenzprobleme innerhalb der EDV und auch bei den Vorgesetzten bekannt waren. Zu klären ist auch, wann und wer was offiziell erfahren hat und in wie weit die jeweiligen Personen im Rahmen ihrer Tätigkeiten gegen die Struktur vorgegangen sind. Um die Prüffeststellungen zu untermauern, werden in dem Prüfbericht als Information die gesondert hier zitierten Berichte, Auszüge und Kopien von E-Mails, Protokollen und Vermerken aufgeführt.
3	**Prüfer** Die Rechnungsprüfer der Stadt Sprockhövel und Herrn Tolj von der Firma ITTCOM - Thomas Tolj, aus Hamburg

4	**Prüfungsergebnis**
4.1	**Microsoft Lizenzen** Nach Rückfrage bei der Firma Cancom zu der getroffenen Aussage in dem vorläufigen Ergebnisbericht, welche Gründe zu dem in dem Bericht enthaltenen Vorwurf der „vorsätzlichen Handlung" geführt haben, hat Herr Schmidt von der Firma Cancom dem Leiter der EDV per Mail am 26. September 2017 (Anlage 2) mitgeteilt, dass er eine erhebliche Unterlizensierung festgestellt habe. Daher geht er davon aus, „dass hier nicht zufällig gehandelt wurde." Durch die Firma ITTCOM - Thomas Tolj wurde während der 38. KW die Analyse und das professionelle Reporting aller Software Lizenzen im Rahmen der Ist-Analyse aufgenommen. Als Ergebnis ist festzuhalten: Es wurden insgesamt 179 Windows und Microsoft Serverlizenzen sowie 38 Office-Lizenzen für das Rathaus ermittelt. In dieser Analyse fehlen noch sämtliche Außenstellen (Schulen, Kitas, etc), weil sie mit der Reportingsoftware nicht erreicht werden können. Für eine Prüfung müssten diese Außenstellen aufgesucht werden. Dieses wurde bisher aus zeitlichen Gründen nicht durchgeführt, wird aber seitens der Prüfer als dringend notwendig erachtet. In einer Aufstellung des EDV-Leiters, die letztmalig im ersten Quartal 2017 aktualisiert worden ist, sind folgende Unterlizensierungen ermittelt worden: • Microsoft Windows Arbeitsplatzlizenzen: 80 • Microsoft Server Lizenzen: 8 • Microsoft Office: 80 In diesen Aufstellungen wurden die käuflich erworbenen Lizenzen von der Firma PC-Fritz nicht berücksichtigt. Die Prüfer gehen daher davon aus, dass zum damaligen Zeitpunkt (2/2016) mindestens Zweifel an der Legalität dieser Lizenzen bei der EDV vorhanden waren. Ein früherer Nachweis von Zweifeln an der Rechtmäßigkeit dieser Lizenzen lässt sich aus den vorhandenen Unterlagen nicht nachweisen. **Ob bei der Nichtverfolgung dieser Zweifel bei der EDV rechtlich ein Vorsatz oder eine Fahrlässigkeit vorliegt, vermögen die Prüfer nicht zu beurteilen.** Wären die vorstehenden 80 Lizenzen gültig gewesen, hätte sich bei den Arbeitsplatzlizenzen keine Unterlizensierung ergeben. Die vorstehende Unterlizensierung der Server- und Office-Lizenzen ist von den PCFritz-Lizenzen nicht betroffen. Im Zuge unserer Legalitätsprüfung wurde ein Mitarbeiter der EDV-Abteilung zu diesem Beschaffungsvorgang befragt. Er teilte mit, dass damals die Beschaffung durch den damaligen EDV-Leiter vorgenommen worden ist. Zu diesem Zeitpunkt wurden von mehreren Händlern die Lizenzen preisgünstig angeboten. Die Preise lagen damals bei 25 – 30 Euro, so dass das Angebot von der Firma PC Fritz über 19,90 € pro Lizenz damals beauftragt worden ist. Die Rechnung über den erfolgten Kauf der Lizenzen lag der Rechnungsprüfung vor. Im Zuge der Prüfung hat Herr Rose einen Vergabevermerk eingesehen, der damals der Rechnungsprüfung vorgelegen hat. Es wurden vor der Auftragsvergabe von Lizenzkäufen entweder entsprechende Vergleichsangebote von mehreren Rahmenvertragshändlern, auf Grund des zwischen dem Bund und der Firma Microsoft verhandelten Rah-

menvertrages, von der Fachabteilung eingeholt bzw. auf Grund des vorstehenden Rahmenvertrages bestellt. Die eingeholten Vergleichsangebote liegen der Rechnungsprüfung ebenfalls vor. Die Bestellscheine wurden der Rechnungsprüfung ordnungsgemäß vorgelegt.

Es wurde dem RPA eine Komplettsicherung von File- und Mail-Servern ausgehändigt. Die Sicherung betrifft nach Auskunft des EDV-Leiters die Jahre 2004 – 2015. Sie wurde vom RPA im Tresor eingeschlossen. Die Rücksicherung wurde inzwischen von einem externen Dienstleister wieder hergestellt und ist damit technisch wieder verfügbar. Vor einer Analyse ist allerdings eine datenschutzrechtliche Prüfung erforderlich, da eventuell auch personenbezogene Daten sichtbar werden würden. Hier wird auf die eingangs aufgeführte Problematik mit der Dienstvereinbarung zum Datenschutz verwiesen.

Hinsichtlich der Frage der Unterlizensierung hat die Firma ITTCOM - Thomas Tolj geprüft, ob es sich bei denen mit Rechnungsdatum vom 25.07.2013 für den Preis von 19,90 € bei der Firma PCFritz gekauften 80 Lizenzen Windows 7 Professional um Original Recovery-DVD's und entsprechenden OEM-Lizenzen von PC-Herstellern wie Dell handelt, oder ob es sich hierbei um Fälschungen im großen Stil handelt.

Die Firma ITTCOM - Thomas Tolj hat Kontakt mit Microsoft aufgenommen und hat eine der damals gekauften 80 Lizenzen zur Prüfung an die Firma Microsoft übersandt.

Am 6. November 2017 hat die Firma Microsoft folgende Rückmeldung gegeben:
„Ich habe mir das Produkt (COA (Echtheitszertifikat englisch Certificate of Authenticity) + DVD) angeschaut. Der Anfangsverdacht hat sich bestätigt. Es handelt sich um eine Fälschung. Sowohl das COA als auch die DVD sind gefälscht." (Anlage 3)
Als Ergebnis bleibt festzuhalten, dass die mit Rechnungsdatum vom 25.07.2013 mit der Re-Nr. 84379 bei der Firma PC Fritz gekauften 80 Windows Pro Lizenzen gefälscht sind.

Nach den Akten informiert der EDV-Leiter mit Mail vom 15.02.2017 die Fachbereichsleiterin, dass der Händler PCFritz vermutlich mit illegalen Kopien gehandelt hat. Ob diese Informationen bei der Stadt Sprockhövel bereits zu einem früheren Zeitpunkt bekannt waren, ist anhand der bisher geprüften Unterlagen nicht ersichtlich.

Ein weiterer Hinweis auf Unterlizensierung ist im vorläufigen Ergebnisbericht der Firma Cancom (ohne Datum) auf Seite 4 Unterpunkt 2.2 zu finden.

Generell ist festzustellen, dass nach Aktenlage und Gesprächsprotokollen der damalige Kämmerer und Hauptamtsleiter das seit langem praktizierte Vorgehen von **Einrichten der Server und Computer mit Microsoft-Betriebssystemen ohne Lizenzen** gebilligt hat. Mit Mail vom 15.06.2015 des EDV-Leiters wurde der Kämmerer über fehlende Lizenzen informiert (Anlage 4). So wurde z. B. in einer EDV-Besprechung am 26.06.2015 auf Vorschlag der EDV erneut entschieden, dass damals die Serverlizenzen erst nach dem Erscheinen der Windowsserver 2016 beschafft werden sollten. In der Besprechung wurde klar dargelegt, dass hier das Risiko, von Microsoft überprüft zu werden, als gering eingestuft worden ist und daher eingehbar sei (vgl. Protokoll dieser Besprechung; Anlage 5). In der Dienstbesprechung wurde laut dem damaligen Protokollant durch den Fachbereichsleiter entschieden, entsprechend zu

verfahren. Dies ist als Entscheidung in der Besprechung dem o.g. Protokoll zu entnehmen.

Aktuelle Situation bei den Lizenzen:
Am 31.10.2017 wurde ein Enterprise Agreement zwischen der Stadt Sprockhövel und der Firma Microsoft abgeschlossen. Dieses umfasst insbesondere die fehlenden Lizenzen. Es handelt sich hierbei um die Lizenzen für Server, Windows 10 und Microsoft Office. Für das Jahr 2017 muss eine Gesamtsumme von ca. 63.000 € incl. Umsatzsteuer gezahlt werden. Mit einem Betrag in gleicher Höhe ist auch für die Jahre 2018 und 2019 zu rechnen.

Inzwischen wurden die beauftragten Lizenzen von der Firma Microsoft bereitgestellt. Diese Lizenzen müssen noch auf der jeweiligen Hardware durch die EDV installiert werden. Diese Arbeiten werden voraussichtlich noch bis zum 1. Quartal 2018 andauern. **Dann ist die bisher bestehende Unterlizensierung von Microsoft-Lizenzen nicht mehr vorhanden.**

Die Stadt Sprockhövel ist bei dem abgeschlossenen Agreement verpflichtet, zukünftig einmal im Jahr eine Meldung über die tatsächlich eingesetzten Server und Office Standard Produkte abzugeben, wenn sich die Anzahl der installierten Lizenzen gegenüber der letzten Meldung erhöht hat. Dabei bleiben unterjährige Veränderungen laut dem Agreement unberücksichtigt. Die Rechnungsprüfung wird zukünftig eine Kopie der durchgeführten Meldung bzw. die Mitteilung der EDV, dass eine Erhöhung der installierten Lizenzen gegenüber dem letzten Jahr nicht vorliegt, bekommen. Die nächste Aktualisierung erfolgt dann Ende September 2018. Die Rechnungsprüfung wird die Einhaltung dieses Termins über Wiedervorlage überwachen.
Für den Bildungsbereich wurden weitere Lizenzen in einem Umfang von 5.000 € gekauft.

4.2 **Kostenentwicklung in der EDV/ Haushalt und Investitionen**
Im Haushalt der Stadt Sprockhövel werden die Mittel für den Bereich der EDV in dem Produkt 01.05.04 Telekommunikation, IT und Druckerei abgebildet.
Die Rechnungsprüfung stellt nachfolgend die Entwicklung der bereitgestellten Mittel für die einzelnen Haushaltsjahre dar und vergleicht diese mit den tatsächlich in diesem Jahr angefallenen Rechnungsergebnissen. Nach Rücksprache mit der EDV sind die von dort gemeldeten Ansätze nicht mehr vorhanden.
Für die einzelnen Haushaltsjahre wurden folgende Ergebnisse festgestellt:
Produkt: 01.05.04 Telekommunikation, IT und Druckerei:

Ergebnisplan:

Haushaltsjahr	Haushaltsansatz	Sollbuchung
2007	448.090 €	367.553,55 €
2008	470.800 €	383.747,29 €
2009	493.350 €	387.069,93 €
2010	573.780 €	357.449,04 €
2011	392.290 €	364.239,80 €
2012	467.330 €	414.993,56 €
2013	487.220 €	442.331,11 €
2014	493.060 €	393.614,15 €
2015	462.550 €	505.874,82 €
2016	547.110 €	548.728,21 €

Es bleibt als Ergebnis festzuhalten, dass die für dieses Produkt im Ergebnisplan bereitgestellten Mittel mit einer Ausnahme im Jahr 2015 auskömmlich gewesen sind. Die Überschreitung des Ansatzes im Jahr 2015 ist durch die Buchungsstelle 01.05.04.501200 – Dienstbezüge an tariflich Beschäftigte begründet. Hier sind Mehrausgaben in Höhe von rund 58.000 € bei den Sollbuchungen entstanden.

Am 16. November 2017 hat die Gemeindeprüfungsanstalt NRW (GPA) nach mehrfacher Aufforderung der Prüfer die erbetenen Vergleichszahlen für das Jahr 2016 mitgeteilt. Danach ergibt sich in der Größenklasse der Stadt Sprockhövel ein Minimalwert vom 523.940 €. Der Maximalwert liegt bei 1.408.520 € und der Durchschnittswert bei 942.770 €. Hier zeigt sich, dass die Aufwendungen bei der Stadt Sprockhövel im EDV-Bereich im Landesvergleich als viel zu gering angesehen werden können. Weitere Vergleichszahlen aus den Vorjahren können laut Auskunft der GPA nicht zur Verfügung gestellt werden.

Finanzplan:

Haushaltsjahr	Haushaltsansatz	Sollbuchung
2007	98.300 €	111.723,88 €
2008	81.900 €	88.874,22 €
2009	64.700 €	46.715,76 €
2010	82.530 €	40.038,85 €
2011	81.600 €	75.492,70 €
2012	118.640 €	89.729,14 €
2013	51.590 €	28.779,04 €
2014	42.380 €	33.851,08 €
2015	30.700 €	87.419,62 €
2016	53.200 €	51.948,51 €

Es bleibt als Ergebnis festzuhalten, dass in den Haushaltsjahren 2007,2008 und 2015 die im Finanzplan bereitgestellten Ansätze nicht ausgereicht haben. Ab dem Haushaltsjahr 2013 wurden deutlich geringere Ansätze im Finanzplan gebildet.

4.3 Personalentwicklung in der EDV sowie deren Organisation

Die personelle Situation in der EDV-Abteilung ist den Beteiligten bekannt und ist mehrfach auch in den politischen Gremien ausführlich besprochen worden.

4.3.1 Personalentwicklung

Seit Anfang November steht ein neuer Mitarbeiter in der EDV zur Verfügung. Ein zum 31.12.2017 ausscheidender Mitarbeiter wird durch den zum 01.01.2018 kommenden weiteren Mitarbeiter ersetzt.

4.3.2 Arbeitsabläufe im Sachgebiet I.1

Auf Grund von Mitteilungen seitens des Personalrates an den damaligen Bürgermeister der Stadt Sprockhövel vom 16.04.2013 (Anlage 6) und die Antwort des damaligen Kämmerers und Fachbereichsleiters vom 22.04.2013 (Anlage 7) geht hervor, dass Maßnahmen in der EDV ohne Berücksichtigung des Landespersonalvertretungsgesetzes (LPVG NRW) und damit des Personalrates durchgeführt worden sind.

Im Schreiben des Personalrates an den damaligen Bürgermeister wurde auch darauf hingewiesen, dass zwei der drei Mitarbeiter der EDV nicht ausreichend

	von der EDV-Leitung über beabsichtigte und durchgeführte Änderungen in der Serverlandschaft und den Betriebssystemen informiert wurden. Durch diese fehlende Information ist eine Unterhaltung und Betreuung der EDV Infrastruktur durch das eigene EDV-Personal nur sehr eingeschränkt möglich. Weshalb dieser unzureichende Informationsfluss erfolgte, kann nicht ermittelt werden. Hier wird jedoch auf die beabsichtigte Privatisierung der EDV verwiesen. Aus einer Nachricht an den Kämmerer und Fachbereichsleiter vom 11.09.2015 geht hervor, dass die vorhandene Organisationsstruktur innerhalb der EDV von einem Mitarbeiter nicht anerkannt bzw. akzeptiert wird. Schriftliche Hinweise auf die Beantwortung oder Regelung von Seiten des Fachbereichsleiters sind nicht zu erkennen. Hier liegt ein Versagen der Führungsaufgaben vor, da für einen längeren Zeitraum dieser Mangel regelmäßig dem Fachbereichsleiter zur Kenntnis zugesendet wurde. Nach mündlicher Auskunft des jetzigen EDV Leiters wurde von Seiten des damaligen Kämmerers sogar über eine Auslagerung des Zuständigkeitsbereiches eines EDV Mitarbeiter nachgedacht. Demnach wollte der Kämmerer, in Absprache mit dem Bürgermeister, erreichen, dass der EDV Leiter keine Weisungsbefugnis zu dem EDV Mitarbeiter besitzt. Dies hätte die bisher mangelhafte Organisations- und Arbeitsabläufe zusätzliche negativ beeinflusst.
4.4	**Beabsichtigte Privatisierung in der EDV** Im Jahr 2011 wurden Überlegungen angestellt, eine umfassende Dokumentation über alle im Einsatz befindlichen Programme sowie der eingesetzten Technik zu erstellen. Außerdem sollte die Möglichkeit der kompletten Übernahme und der Betreuung der hier vor Ort befindlichen Technik geprüft werden. Eine endgültige Auftragserteilung ist nicht erfolgt.
4.5	**Sicherheit und Datenschutz in der EDV** Im HFA wurden mehrere Schwachstellen durch den Gutachter erläutert. Das RPA hat die Verwaltung aufgefordert, die von Herrn Tolj ermittelten Schwachstellen sofort zu beheben. Bereits im Juli 2015 wurde von der Citkomm ein Security Checkup für die Stadt Sprockhövel erstellt. Adressat dieses Ergebnisberichts der Phase 1 – Ist-Aufnahme und Risikoanalyse war der Verwaltungsvorstand der Stadt. Weitere Ausführungen zu den Ergebnissen sind der gesamten Verwaltungsspitze mitgeteilt worden. **Am 18.09.2015 wurde den Führungskräften der Stadtverwaltung dieser Bericht des Security-Checks vorgestellt. Spätestens seit dem sind allen damaligen Führungskräften die im Sicherheitscheck festgestellten Probleme bekannt.** Im dem Bericht wurde unter Punkt 7. Risikobewertung auf den Seiten 26 bis 30 darauf hingewiesen, dass in der Stadtverwaltung Sprockhövel eine Reihe teilweise gravierender Risiken festgestellt worden sind, die strukturiert angegangen werden müssen. Leider ist hier als Ergebnis festzuhalten, dass die damals festgestellten Risiken auch bei dem vom dem Gutachter der Firma ITTCOM - Thomas Tolj gemachten Sicherheitscheck im Oktober 2017 wieder als Risiken aufgefallen sind. Gemeinsam mit der Firma Citkomm wurde damals (im Jahr 2015) eine Maß-

	nahmentabelle erarbeitet. Nach Rücksprache mit Teilnehmern der Arbeitsgruppe ist die Umsetzung damals an finanziellen und persönlichen Ressourcen gescheitert, so dass im Ergebnis nur einer der in der Tabelle aufgeführten Punkte erledigt worden ist. Die Abarbeitung der damals aufgezeigten und aktuell immer noch bestehenden Mängel ist aus Sicht der Prüfer zwingend kurzfristig erforderlich. Dass die Verwaltungsleitung aufgrund der Feststellungen keine konkreten Maßnahmen zur Behebung der festgestellten Mängel unter Terminsetzung veranlasst und die Abarbeitung nicht kontrolliert hat, wird von den Prüfern bemängelt. Es wird vorgeschlagen, die damals bereits gebildete Arbeitsgruppe wieder zu aktivieren. Als Problem hat sich herausgestellt, dass die Arbeitsgruppe damals nicht direkt an den Verwaltungsvorstand angebunden worden ist. Im Zuge unserer Untersuchungen wurde auch festgestellt, dass die vorhandene Back-up Lösung (Fa. Acronis) nicht ordnungsgemäß funktioniert hat (siehe dazu auch das Protokoll vom 29.02.2016 FB I.1 (EDV)). Das größte Problem bestand darin, dass ein Back-up auf Bändern nicht erfolgt ist und somit eine Datensicherung nicht so wie rechtlich vorgeschrieben ausgelagert werden konnte. Laut Rechnung der Firma ADN mit der Rechnungsnummer 5249212 vom 27.07.2012 wurde die Acronis Software mit der Produktbezeichnung Acronis Backup & Recovery 11 Advanced Server 27.07.2012 geliefert. Es bleibt festgehalten, dass die Datensicherung des Exchange-Servers (Mailservers) über Jahre nicht ordnungsgemäß erfolgt ist. **Hierbei handelt es sich um ein gravierendes Datensicherheitsproblem.** Die Produkte der Firma Acronis hat die Stadt Sprockhövel über die o.a. Firma erworben (siehe Kapitel 4.6). Inwieweit hier der Mangel an Firma Acronis angezeigt worden ist, ist aus den vorliegenden Unterlagen nicht ersichtlich. Auch ist eine Schadensersatzforderung aus den Unterlagen nicht erkennbar. Inzwischen wurde mit Unterstützung des Herstellers die Reparatur des Systems veranlasst. Die endgültige Fertigstellung einschließlich der Schulung der EDV-Mitarbeiter soll noch in diesem Jahr abgeschlossen werden. Als Ergebnis ist festzuhalten: Seit dem Oktober 2017 werden regelmäßige Datensicherungen durchgeführt. Die vorgesehene Auslagerung der Bänder in den Tresor der Sparkasse Sprockhövel soll wieder ab Ende November 2017 durchgeführt werden. Vorher erfolgt noch eine entsprechende Mitarbeiterschulung und die Neuinstallation durch den Hersteller (Fremdfirma) muss dazu noch abgeschlossen werden. Durch die Firma ITTCOM - Thomas Tolj wurden bei der Schwachstellenanalyse inzwischen folgende sicherheitsrelevante Schwachstellen festgestellt: • Eine IT Dokumentation mit einem Lizenzmanagement ist nicht vorhanden. Dieses ist ein wichtiger Aspekt, um viele Probleme nicht aufkommen zu lassen, wie z. B. zu wenig oder doppeltvergebene Lizenzen. Hier empfiehlt der Gutachter, das Lizenzmanagement mit Einsatz der Software Dokusnap durchzuführen. • Weiterhin ist eine Übersicht aller Anwendungen in der IT-Umgebung erforderlich. Hier empfiehlt der Gutachter den Einsatz der Software Dokusnap.

	Die Bestellung des vorgeschlagenen Programms Dokusnap ist Anfang November 2017 durch die EDV erfolgt. • Der DNS-Server sollte auf dem aktuellsten Stand sein, da der Gutachter bei der Analyse noch alte Einträge von Geräten gefunden hat, die nicht mehr im Einsatz sind. Die „Pflege" der alten Einträge ist von der EDV nicht erfolgt. Die Aktualisierung wird von der EDV noch im Jahre 2017 durchgeführt. • Eine Passwortrichtlinie ist nicht vorhanden. Die Passwörter von Mitarbeitern, Administratoren und Datenbanken müssen in regelmäßigen Abständen geändert werden. Mittlerweile wurde eine Passwortrichtlinie eingeführt. Jeder Beschäftigte muss alle sechs Monate sein Passwort ändern. Die Benutzerkennworte wurden bereits geändert. • USB Ports müssen auf jedem Arbeitsrechner und allen Servern gesperrt werden. Bei dem Ortstermin des Gutachters Herrn Tolj in der 40. KW wurde zugesagt, dass die Sperrung von der EDV veranlasst wird. • Arbeitsrechner müssen beim Verlassen des Arbeitsplatzes gesperrt werden. Inzwischen wurde durch die EDV eine automatische Sperrung nach acht Minuten eingerichtet. • Büroräume müssen beim Verlassen des letzten Mitarbeiters verschlossen werden. Die Mitarbeiter müssen für dieses Thema sensibilisiert werden. • Eine Festplattenverschlüsselung auf allen Arbeitsplätzen ist erforderlich, um keinen Datenverlust an Dritte zu erleiden, wenn ein Rechner abhanden kommt. Die Umsetzung des Vorschlages wird von der EDV geprüft. • Alte Betriebssystem wie z. B Windows XP, Windows Server 2000, Windows Server 2003 und Windows Server 2008 dürfen nicht mehr eingesetzt werden. So ist aktuell in der Bücherei ein Windows Server 2003 mit einer alten Version des eingesetzten Programms „Bibliotheka" im Einsatz, die nicht mehr supportet wird und somit leicht durch Dritte angreifbar ist. Die Verantwortlichkeit für die Basisstruktur (Server, PC) liegt generell bei der EDV. Die Verantwortung für den Kauf von Fachsoftware und deren Betreuung liegt aber in den einzelnen Fachbereichen. Dieses hat zum Teil dazu geführt, dass notwendige Updates für die Software von den Fachbereichen nicht veranlasst worden sind. Dieses Verfahren sollte zukünftig geändert werden. Für das hier eingesetzte Programm „Bibliotheka" ist die Neuinstallation noch für das Jahr 2017 geplant. • Alle Unternehmensanwendungen müssen stets auf dem vom Hersteller unterstützten Stand sein. Nicht mehr vom Hersteller unterstützte Software, die auf Servern und Arbeitsrechnern vorhanden ist, muss unwiderruflich

	deinstalliert werden. • Alle Betriebssysteme in der IT-Landschaft müssen immer auf dem aktuellen Stand sein. Dafür ist ein Patchmanagement erforderlich. Für die in Sprockhövel eingesetzten Microsoft Produkte ist ein Update-Server im Einsatz (WSUS). Für Standardprogramme wird zukünftig von der EDV eine Lösung angeboten. • An den Netzwerkdosen sind nicht belegte Ports (freie Ports) vorhanden, jedoch sind diese in der IT-Landschaft gepatcht. Damit kann sich jeder einen Zugang an die Unternehmensdaten und die IT-Landschaft verschaffen, z. B., wenn ein fremdes Notebook im Flur an einer Netzwerkdose angeschlossen wird. • Der Gutachter schlägt vor, dass alle Netzwerkdosen überwacht werden müssen, damit kein Fremder sein Gerät anschließen kann, um sich damit einen Zugang an die Unternehmensdaten zu verschaffen. Dafür ist eine Netzwerk-Kontrolllösung erforderlich. Die Überwachung soll laut EDV im Rahmen der Neuverkabelung umgesetzt werden. Eine Schwachstellenanalyse in den beiden IP Netzen des Rathauses 192.168.160.0/24 und 192.168.161.0/24 ergab eine sehr große Anzahl von Schwachstellen auf Rechnern, Servern, Druckern und Switchen, die einen Zugriff von Dritten ermöglichen, durch den ggf. auch unerwünschte Schadsoftware aufgespielt werden kann, um einen Zugriff auf die Daten der Gemeinde zu erlangen. Die vorhandenen Schwachstellen sind entstanden durch den Einsatz veralteter Software und fehlender Aktualisierungen bzw. nicht regelmäßig installierter Updates. Eine detaillierte Liste der Schwachstellen wurde der EDV zur Behebung übergeben. Die Prüfer haben eine Dokumentation eines Sicherheitsvorfalles vom 18.08.2015 entdeckt. Hierbei handelte es sich um eine Infektion durch einen Kryptovirus. Über diesen Sicherheitsvorfall wurden Bürgermeister und Kämmerer per E-Mail (siehe Anlage 8) vom EDV Leiter am 21.08.2015 um 08:51 Uhr informiert, und beide erhielten so Kenntnis über gravierende IT-Sicherheitsmängel, unter anderem auch über die nicht ausreichende, gesetzeskonforme Datensicherung. **Besonders wichtig wird von den Prüfern die Überarbeitung und saubere Dokumentation von Domänen-Administrator-Passworten angesehen.** Auf die Ausführungen im vorläufigen Ergebnisbericht der Firma CANCOM unter Punkt 2.5 wird dazu verwiesen. • **Alle Mitarbeiter müssen mindestens einmal im Jahr in Form einer Schulung sensibilisiert werden.** Der Schulungsbedarf wird ebenfalls von der EDV als notwendig angesehen. Eine Konzeption soll entwickelt werden.
4.6	**Geschäftsbeziehung mit der Firma eines EDV-Mitarbeiters** Ein Mitarbeiter der EDV-Abteilung führt einen Gewerbebetrieb für IT-Beschaffungen. Die Nebentätigkeit ist bei der Stadt Sprockhövel bekannt. Zu der Geschäftsbeziehung gibt es einen Mailverkehr zwischen IT-Leiter und

	Kämmerer, der mit einer Mail vom 28.07.2015 endet, in der es nicht als problematisch erachtet wird, mit der o.a. Firma Geschäftsbeziehungen zu unterhalten. Hierbei wäre auf folgendes zu achten: 1. Die allgemeinen Regeln der Auftragsvergabe sind einzuhalten. 2. Der EDV-Mitarbeiter darf nicht selber an der Beschaffung städtischerseits beteiligt sein. Insbesondere den zweiten Punkt sehen die Prüfer als problematisch an. Der EDV-Mitarbeiter hat Entscheidungen über einzukaufende Produkte, z.B. Kauf der DELL Server getroffen, die dann von der Stadt über seine Firma beschafft wurden. Darin sehen die Prüfer eindeutig eine Beteiligung des Mitarbeiters an dem Beschaffungsprozess und damit einen Verstoß gegen geltende Compliance-Regeln. Die aktive Beteiligung des Mitarbeiters zeigt sich auch in dem geprüften Mailverkehr in der Mail vom 11.09.2015 vom EDV Leiter an den Kämmerer (siehe Anlage 9) Danach wird noch einmal bestätigt, dass der Mitarbeiter sich sehr stark für die Anschaffung von den Produkten der Firma DELL eingesetzt hat. Bei der Planung von der Hardware und der Bewertung von Angeboten setzte er die Produkte der Firma DELL als Maßstab an. Inzwischen werden die DELL-Produkte von der Stadt Sprockhövel direkt von der Firma DELL bezogen. Dieser direkte Weg ist erfahrungsgemäß preisgünstiger. Aus fachlicher Sicht ist gegen die Anschaffung von DELL Produkten nichts einzuwenden. Dass seitens der Stadt regelmäßig Beschaffungen über die vorstehende Firma abgewickelt werden, ergibt sich aus den gesichteten Unterlagen. In mehreren Fällen wurden die Rechnungen mit Rechnungsanschrift der Firma des Mitarbeiters an die Stadt Sprockhövel direkt weitergeleitet und von dort aus auch bezahlt. Nach Rücksprache mit dem Leiter des Finanzmanagements wird dieses Verfahren seit Jahren praktiziert. Ihm wurde vom damaligen IT-Leiter und vom damaligen Kämmerer auf Nachfrage mitgeteilt, dass die Rechnungen, welche an die o.a. Firma ausgestellt wurden, seitens der Stadt Sprockhövel direkt bezahlt werden (siehe Anlage 10).
4.7	**Schadensermittlung** Als direkter Schaden ist der Kauf der PCFritz-Lizenzen für ca. 1.600 € einzustufen. Weiterhin ist hier der Aufwand für die sachverständige Unterstützung der Firma ITTCOM - Thomas Tolj anzusetzen. Eine Schlussrechnung hierzu liegt noch nicht vor. Ein Schaden durch Hacking auf die IT-Systeme der Stadt Sprockhövel auf Grund der vorliegenden Sicherheitslücken konnte bisher nicht nachgewiesen werden. Hierzu wäre eine gesonderte Überprüfung erforderlich. Die oben aufgeführten Lizenzkosten für das Enterprise Agreement mit Microsoft in Höhe von ca. 63.000 € pro Jahr sind nicht als Schaden einzustufen, da dieser Betrag für 2017 und Folgejahre berechnet wird. In den Vorjahren sind Aufwendungen für eine ordnungsgemäße Lizensierung nicht in voller Höhe entstanden.

5	**Zusammenfassung** Zur den Verantwortlichkeiten innerhalb der Stadtverwaltung wurden vorstehend folgende Feststellungen getroffen: **Lizenzen:** Eine Unterlizensierung bei der Stadtverwaltung Sprockhövel kann für die Vergangenheit festgestellt werden. Die Unterlizensierung war dem damaligen EDV-Leiter und dem damaligen Kämmerer bekannt. Der Kämmerer hatte sogar die Entscheidung getroffen, dass hier das Risiko von Microsoft bezüglich der fehlenden Lizenzen überprüft zu werden, als gering eingestuft wird und daher eingehbar sei (vgl. Protokoll der Besprechung vom 26.05.2015; Anlage 5) In Kenntnis der damaligen Unterlizensierung sind trotzdem ohne Vorliegen ausreichender Lizenzen weitere PC-Arbeitsplätze eingerichtet worden. Ob es sich hierbei rechtlich um einen Vorsatz oder eine Fahrlässigkeit handelt, vermögen die Prüfer nicht zu beurteilen. **Abarbeitung Sicherheitsmängel citkomm-Ergebnisbericht vom 02.06.2015** Am 18.09.2015 wurde den Führungskräften der Stadtverwaltung der Bericht des Security-Checks vorgestellt. Spätestens seitdem sind allen damaligen Führungskräften die im Sicherheitscheck festgestellten Probleme bekannt. Eine Behebung ist nicht erfolgt. Die Mängel sind durch die aktuellen sachverständigen Untersuchungen der Firma ITTCOM - Thomas Tolj erneut festgestellt worden. Für die nicht erfolgte Abarbeitung der Mängel wird wegen der Schwere der im Bericht festgestellten Mängel auch eine Verantwortung des damals zuständigen Verwaltungsvorstandes gesehen. **Nachbesetzung der Leitungsstelle in der EDV Abteilung** Das Rechnungsprüfungsamt (RPA) kann hinsichtlich der Eignung des neuen EDV-Leiters dahingehend eine Auskunft erteilen, dass durch den EDV-Leiter nun eine korrekte Dokumentation der vorhandenen Situation und Arbeitsabläufe entstanden ist. Hinsichtlich einer fachlichen Eignung als EDV-Leiter kann das RPA keine Aussage treffen.
6	**Bemerkungen** Die im Bericht aufgeführten Anlagen werden aus datenschutzrechtlichen Gründen nicht mit veröffentlicht. Sie werden von der Rechnungsprüfung vorgehalten und können bei Bedarf dort eingesehen werden.

Sprockhövel, den 17. November 2017

Tolj Rose Springer Hockelmann