Berichtsvorlage

LWL
Für die Menschen.
Für Westfalen-Lippe.

Federführende Abteilung:	**Datum:**	**DrucksacheNr.:**
LWL.IT Service Abteilung	20.06.2017	**14/1231**

Status:	**Datum:**	**Gremium:**	**Berichterstattung:**
Ö	11.07.2017	Personalausschuss	Herr Dr. Lunemann

Betreff:
Antwort der Verwaltung auf die Anfrage der Gruppe LWL-Piraten betreffend Ransomware Angriffe auf öffentliche Infrastruktur (Drucksache Nr.: 14/1189)

1	Ergebnis- und/oder zahlungsrelevante Auswirkungen?		x	nein		ja
	Im Haushaltsplan vorgesehen?			nein		ja, im Hpl.
	Im Wirtschaftsplan vorgesehen?			nein		ja, im Wi-Plan
2	Die Leistungen sind		**3**	**Rechtsgrundlage/Ausschussbeschluss:**		
		freiwillig				
		durch Gesetz/Verordnung pp. bestimmt				
		durch Ausschussbeschluss des LWL bestimmt				

4	Investitionskosten/einmalige Auszahlungen:		**5**	Jährliche ergebnisrelevante Folgekosten:		**6**	Hinweise
Insgesamt:		EUR	Insgesamt:		EUR		Ergänzende Darstellung zu den ergebnis- und/oder zahlungsrelevanten Auswirkungen (Investitionskosten, Folgekosten, Finanzierung pp.) siehe in der Begründung unter Ziffer
Beteiligung Dritter:		EUR	Beteiligung Dritter:		EUR		
LWL-Mittel:		EUR	Belastung LWL:		EUR		

Die Vorlage 14/1231 wird zur Kenntnis genommen.

1. Ausgangssituation

Nachdem Bekanntwerden der Cyber-Angriffe am 12.5.2017 hat die Gruppe LWL-Piraten am 16.5.2017 mit der Drucksache 14/1189 eine Anfrage betreffend Ransomware-Angriffen auf die öffentliche Infrastruktur beim LWL gestellt. In der Anfrage wurden folgende Fragen gestellt, die im Kapitel 2 beantwortet werden.

1. Sind LWL-Einrichtungen Ziel des Hackerangriffs am 12. und 13. Mai 2017 gewesen?
    a. Waren diese Angriffe erfolgreich?
        i. Inwieweit wurde der LWL beeinträchtigt?
2. Ist der LWL in den letzten 16 Monaten Ziel von Cyberangriffen gewesen?
    a. Wann?
    b. Inwiefern?
    c. Waren die Angriffe erfolgreich?
        i. Inwieweit wurde der LWL beeinträchtigt?
    d. Falls nein, geht der LWL davon aus, dass es unwahrscheinlich ist, Ziel solcher Angriffe zu werden?
        i. Falls nein, geht der LWL davon aus, gut gewappnet zu sein?
            1. Wenn ja, warum?
3. Wie hoch war der Arbeitsmehraufwand bei den Bediensteten in Folge jedes Angriffs?
4. Mussten Überstunden geleistet werden aufgrund der Angriffe?
5. Ist der Arbeitsaufwand für Mitarbeiter des LWL aufgrund von Cyberangriffen gestiegen?
6. Ist mehr Personal für die Cybersicherheit des LWL seit den ersten Angriffen eingestellt worden?
    a. Wenn ja, wieviel in welchem Umfang und mit welcher Qualifikation?
7. Wurde in Betracht auf die mögliche Nutzung von Open-Source-Software eine Kosten-Nutzen-Analyse erarbeitet?
    a. Welche Kriterien wurden angelegt?
    b. Wenn nein, warum nicht?

2. Beantwortung der Anfrage

2.1 <u>Zu Frage 1:</u> Cyber-Angriff WannaCry

Mit WannaCry wird ein Cyber-Angriff bezeichnet, der am 12.5.2017 begann und die Erpressung von Lösegeld nach einer Verschlüsselung von Daten zum Ziel hatte. Die Schadsoftware machte sich eine Schwachstelle im Windows-Betriebssystem zunutze, die die nationale Sicherheitsbehörde der USA (NSA) seit mehr als 5 Jahren für eigene Zwecke ausgenutzt hatte. Nachdem die NSA erfahren hatte, dass das Wissen über die EternalBlue genannte Schwachstelle durch Hacker gestohlen worden war, informierte sie Microsoft. Am 12.3.2017 veröffentliche Microsoft einen Patch für die noch unterstützten Betriebssysteme, später, mit dem WannaCry-Ausbruch, auch für die veralteten und regulär nicht mehr unterstützten Betriebssystemversionen Windows XP und Windows 2003. Die WannaCry-Angriffswelle führte zu Ausfällen bei zahlreichen Organisationen z.B. im britischen Gesundheitswesen, bei der Deutschen Bahn, beim spanischen Telekommunikationskonzern Telefónica, beim US-Logistikunternehmen FedEx oder beim russischen Innenministerium.

Für WannaCry wurden kurz nach Bekanntwerden des Angriffs von den Virenschutzherstellern spezielle Virenkennungen bereitgestellt, die beim LWL zeitnah verteilt wurden.

Cyber-Angriffe sind auch beim LWL permanent zu verzeichnen. Es wurden aber keine Angriffe registriert, die der WannaCry-Angriffswelle konkret zugeordnet werden können.

2.2 Zu Frage 2 a-c: Cyber-Angriffe in den letzen 16 Monaten

Häufig sind beim LWL Angriffe über schädliche SPAM-E-Mails zu verzeichnen. Mit verschiedenen Tricks sollen Beschäftigte dazu gebracht werden, Dateianhänge (mit Schadsoftware) zu öffnen, Links anzuklicken (die auf mit Schadsoftware verseuchte Internetseiten führen) oder Zugangsdaten auf fremden Seiten einzugeben (Identitätsdiebstahl). In der letzen Zeit ist eine immer stärkere Individualisierung von Angriffe zu erkennen, die für die Empfänger schwer zu erkennen sind. So gingen im Dezember 2016 fingierte Bewerbungen auf ausgeschriebene Stellen beim LWL ein. Diese E-Mails enthielten Office-Dokumente als Mail-Anhang, die schädliche Makros enthielten. Von echten Bewerbungen können diese gefälschten Bewerbungen durch die Sachbearbeiter nur schwer erkannt werden. Beim LWL wurde die Schadsoftware in diesen Fällen nicht aktiv, da eine vorher bereits umgesetzte Maßnahme alle Makros aus Office-Dokumenten in E-Mail-Anlagen entfernt.

Weitere Angriffe erfolgen durch auf Internetseiten platzierte Schadsoftware. Dies kann auch renommierte Internetseiten betreffen, z.B. weil Schadsoftware in Werbebannern versteckt wird. Auch das automatisierte systematische oder manuelle Suchen nach Sicherheitslücken an den LWL-Internetzugängen ist permanent zu verzeichnen.

Ein Großteil der Angriffe wird durch verschiedene Maßnahmen wie Firewall, Spam-Filter, Virenschutz, Entfernen von Makros aus Office-Dokumenten oder Entfernen von ausführbaren Dateien aus Mail-Anhänge abgewehrt. In Einzelfällen gelangte dennoch Schadsoftware in beschränktem Umfang auf Rechner im LWL. Größere Schäden wurden nicht bekannt.

In den letzten 16 Monaten hatte der LWL auch zwei gezielte Angriffe auf die Verfügbarkeit des Internetzugangs zu verzeichnen: Am Samstag, 4.6.2016 / Sonntag, 5.6.2016 und am Freitag, 9.7.2016. Hierbei wurde durch Überlastungsangriffe der Internetzugang beeinträchtigt. Die Auswirkungen blieben überschaubar, da die Angriffe nur am Wochenende bzw. in Randzeiten erfolgten.

2.3 Zu Frage 2 d: Aktuelle Sicherheitsvorkehrungen

Insgesamt haben sich die in den letzten Jahren umgesetzten Sicherheitsvorkehrungen der LWL.IT grundsätzlich bewährt. Zur Strategie der LWL.IT gehört eine zentrale Betriebsführung, um zeitnah aktuelle Sicherheits-Patches auf Clients und Servern einzuspielen. Außerdem werden Sicherheitseinstellungen der jeweiligen Bedrohungslage angepasst. Bereits vor WannaCry mit dem Bekanntwerden der ersten Welle von Ransomware, hat die LWL.IT Sicherheitsmaßnahmen zur besseren Absicherung von Netzwerken und Systemen ergriffen; so wurden z.B. der Adobe Flash-Player deinstalliert, der Download von Software für Nutzerinnen und Nutzer unterbunden und das Berechtigungskonzept für Admin-Kennungen der neuen Bedrohungslage angepasst.

Diese Maßnahmen führen bei dem betroffenen Personal zu Einschränkungen in den gewohnten Arbeitsabläufen; hier ist das Bewusstsein und das Verständnis für die Informationssicherheit zu schärfen. Weiterhin bleibt auch die Sensibilisierung von Mitarbeiterinnen und Mitarbeitern, keine unbekannten E-Mail-Anhänge zu öffnen und in Verdachtsfällen umgehend die Sicherheitsteams zu informieren, weiterhin eine wichtige Strategie. Andererseits sind die Möglichkeiten der Erkennung von Schad-Emails für Nutzerinnen und Nutzer auch begrenzt, da der Trend zunehmend in Richtung spezieller, auf den Empfängerkreis zugeschnittener

Schad-E-Mails geht (siehe angebliche Bewerber-E-Mails). Auch tauchen immer häufiger E-Mails auf, deren angeblicher (gefälschter) Absender dem Empfänger bekannt ist.

2.4 Zu den Fragen 3 bis 6: Arbeitsaufwand

Die Abwehr und Behandlung von Cyber-Angriffen führt regelmäßig zu erhöhten Aufwänden in der LWL.IT. Dabei ist der Aufwand abhängig vom Einzelfall. Die LWL.IT-internen Aufwände betrugen in den letzten 16 Monaten zwischen einer 1 Stunde und 50 Stunden pro Fall. Darüber hinaus entstand Aufwand in den Einrichtungen insbesondere durch die Nichtverfügbarkeit einzelner Rechner, der durch die LWL.IT nicht näher beziffert werden kann. Die Größenordnung der Beeinträchtigung entsprach der eines technischen Defektes. Bisher konnten die anlässlich der Sicherheitsvorfälle angefallenen Aufwände im Rahmen der normalen Arbeitszeitregelungen des LWL erledigt werden.

Zusätzliches Personal für den Bereich Informationssicherheit wurde bisher nicht eingestellt. Deshalb geht die für die Bearbeitung von Cybersicherheitsvorfällen erforderliche Zeit zu Lasten anderer Aufgaben. Insbesondere bleibt für die systematische Bearbeitung von Sicherheitsthemen und Zertifizierungen zu wenig Zeit.

2.5 Zu Frage 7: Einsatz von Open-Source-Software

Der Einsatz von Open-Source stellt nicht grundsätzlich einen besseren Schutz vor Cyberangriffen dar. So wurde beispielsweise am 26.5.2017 bekannt, dass es eine zu WannaCry vergleichbare gefährliche Schwachstelle auch in der unter dem Open-Source-Betriebssystem Linux gerne eingesetzten Open-Source-Software Samba gibt, die nun SambaCry genannt wird.

Bezüglich der Sicherheitsaspekte von Open-Source-Software sowie der Open-Source-Strategie wird auf die Vorlage 14/0343 – „Einsatz von Open-Source-Software beim LWL" vom 23.06.2015 verwiesen.

3. Strategische Ausrichtung des Informationssicherheitsmanagements

Eine hundertprozentige Sicherheit gibt es nicht und wird es auch nie geben, denn es werden auch bei sorgfältigster Planung und IT-Betrieb immer wieder neue Sicherheitslücken bekannt werden. Deshalb ist es umso wichtiger, organisatorisch so aufgestellt zu sein, dass Risiken und Sicherheitslücken frühzeitig erkannt und abgestellt werden können. Für eine größere Organisation wie den LWL ist es deswegen sinnvoll, ein Informationssicherheitsmanagementsystem (**ISMS**) einzuführen, welches sich am Stand der Technik orientiert. Hierzu gehört, dass eine umfassende Betrachtung aller Sicherheitsaspekte gewährleistet ist. Bereiche mit hohen Risiken sind zu identifizieren und es sind angemessene Risikobehandlungsmaßnahmen festzulegen.

Beispiele für Aspekte, die betrachtet werden müssen sind Zugangsschutz für Anwendungen, Kommunikationssicherheit, Physische Sicherheit, Schulung und Sensibilisierung von Personal, Handhabung von Informationssicherheitsvorfällen und Notfallplanung. Eine wesentliche Aufgabe ist auch die regelmäßige Überprüfung der Wirksamkeit und Angemessenheit von Sicherheitsmaßnahmen.

Die Leitlinie für Informationssicherheit des IT-Planungsrates, die für Bund und Länder verbindlich gilt, empfiehlt den Kommunen die Anwendung dieser Leitlinie. In der Leitlinie wird die Empfehlung gegeben, ein ISMS aufzubauen, welches sich am IT-Grundschutz-Standard

des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der ISO/IEC 27001 orientiert. Als erster Schritt genügt laut Leitlinie des IT-Planungsrates ein ISMS nach ISO/IEC 27001.

Der Deutsche Landkreistag hat zusammen mit dem Deutschen Städtetag, dem deutschen Städte- und Gemeindebund und der Arbeitsgemeinschaft der Kommunalen IT-Dienstleister in Deutschland (VITAKO) im März 2017 eine „Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen" veröffentlicht. Hier wird darauf verwiesen, dass bei ebenenübergreifenden Verfahren (z.B. Land – Kommune) die Leitlinie auch im kommunalen Bereich zu berücksichtigen sei.

Die LWL.IT prüft aktuell in Abstimmung mit der LWL-Leitung, ob und unter welchen Rahmenbedingungen das ISMS im LWL an einem anerkannten Standard ausgerichtet werden kann. Mehrere andere kommunale Rechenzentren haben diesen Weg inzwischen beschritten. So sind derzeit von den 32 Mitgliedern im Dachverband kommunaler IT-Dienstleister (KDN) bereits 8 zertifiziert, einige Rechenzentren bereiten eine Zertifizierung vor oder orientieren sich zumindest an einem anerkannten Standard.

Mit der derzeit für den Bereich Informationssicherheit vorhandenen Personalressource (eine Person; der Informationssicherheitsbeauftragte) wird dies jedoch kaum möglich sein, da diese vorhandene Person schon mit dem Tagesgeschäft ausgelastet ist. So nimmt der Informationssicherheitsbeauftragte derzeit u.a. die Funktion eines internen CERT (Computer Emergency Response Team) war. Hierzu gehören u.a. die Analyse von Meldungen anderer CERT-Dienste und Presse-Mitteilungen sowie die Organisation der Prüfung von Maßnahmen zur Risikominimierung. Weiterhin ist heute ein großer Teil der Kapazität durch die Einbeziehung bei Beschaffungen/ Ausschreibungen, Verfahrenseinführung, externe und interne Prüfungen und sonstige Fragen zur Informationssicherheit gebunden. Hinzu kommen Aufwände für die Erstellung von Richtlinien, Konzeption und Abstimmung von Sicherheitsmaßnahmen sowie die steigenden Aufwände für den Informationsaustausch und Abstimmungen innerhalb von Verbänden wie dem KDN oder der VITAKO. Ein angemessenes Informationssicherheitsmanagement ist mit der derzeitigen Organisation und Ressourcenausstattung im Bereich Informationssicherheit nicht zu leisten.

Um sich dieser wichtigen Aufgabe zukünftig intensiv widmen zu können, ist eine Vollzeitkraft in die Stellenplanung 2018 eingebracht worden.

Anlage:

Vorlage 14/0342 – „Einsatz von Open-Source-Software beim LWL"

Berichtsvorlage

LWL
Für die Menschen.
Für Westfalen-Lippe.

Federführende Abteilung:	**Datum:**	**DrucksacheNr.:**
LWL.IT Service Abteilung	27.05.2015	**14/0342**

Status:	**Datum:**	**Gremium:**	**Berichterstattung:**
Ö	23.06.2015	Personalausschuss	Herr Dr. Lunemann
Ö	26.06.2015	Landschaftsausschuss	Herr Dr. Lunemann

Betreff:
Einsatz von Open-Source-Software beim LWL

1	Ergebnis- und/oder zahlungsrelevante Auswirkungen?		x	nein		ja
	Im Haushaltsplan vorgesehen?			nein		ja, im Hpl.
	Im Wirtschaftsplan vorgesehen?			nein		ja, im Wi-Plan

2	Die Leistungen sind		**3**	**Rechtsgrundlage/Ausschussbeschluss:**
		freiwillig		
		durch Gesetz/Verordnung pp. bestimmt		
		durch Ausschussbeschluss des LWL bestimmt		

4	Investitionskosten/einmalige Auszahlungen:		**5**	Jährliche ergebnisrelevante Folgekosten:		**6**	Hinweise
Insgesamt:		EUR	Insgesamt:		EUR	Ergänzende Darstellung zu den ergebnis- und/oder zahlungsrelevanten Auswirkungen (Investitionskosten, Folgekosten, Finanzierung pp.) siehe in der Begründung unter Ziffer	
Beteiligung Dritter:		EUR	Beteiligung Dritter:		EUR		
LWL-Mittel:		EUR	Belastung LWL:		EUR		

Die Vorlage 14/0342 wird zur Kenntnis genommen.

Begründung:

In der Sitzung des Landschaftsausschusses am 13.03.2015 hat die Fraktion Bündnis 90/Die Grünen den Antrag 14/0312 betr. Open Source eingebracht. Es bestand Einvernehmen, den Antrag nach vorheriger Beratung im Personalausschuss in einer der nächsten Sitzungen des Landschaftsausschusses zu behandeln.

Mit dieser Berichtsvorlage gibt die Verwaltung einen Überblick über den Einsatz von Open-Source-Software beim LWL.

1. Hintergründe

Open-Source-Software basiert im Kern auf der Überzeugung, dass im Gegensatz zur kommerziellen Software, bei dem der Quellcode als gut gehütetes Geheimnis unter Verschluss bleibt, bessere Software entsteht, wenn die Programmquellen von jedermann gelesen, neu verteilt und modifiziert werden können. Gemäß der Ende 1998 gegründeten Open Source-Initiative (OSI) gibt es folgende Kernelemente von Open Source:

- Freie Weiterverbreitung: Jeder darf Open-Source-Software nutzen und beliebig weiterverteilen.
- Verfügbarkeit des Quellcodes: Das Softwarepaket muss den Quellcode enthalten oder angeben, an welcher frei zugänglichen Stelle dieser zu erhalten ist.
- Änderungen am Quellcode: Der Quellcode darf an eigene Bedürfnisse angepasst und in dieser veränderten Form weitergegeben werden.

Die zunehmende Beherrschung des Softwaremarktes insbesondere durch große IT-Konzerne (u.a. Microsoft) und der wachsende Kostendruck bei Softwarelizenzen haben auch in der öffentlichen Verwaltung (und beim LWL) zu einer dauerhaften Auseinandersetzung mit Open-Source-Software geführt.

2. Aktuelle Situation LWL.IT

Der LWL setzt seit Jahren in verschiedenen Bereichen Open-Source- Software in u.a. folgenden Bereichen ein:
Schüler-Netze mit u.a.

- ODS-Server (Linux-basierend)
- 7-ZIP (Datenkomprimierung)
- Thunderbird (Mail-Client)
- Sunbird (Terminverwaltung)
- Video-LAN-Client (Multimedia-Anzeige)
- Open Office Org (Textverarbeitung, Tabellenkalkulation)

- Web-Server, Mail-Server, Datenbank-Server mit u.a.
  - SUSE, Debian u. OpenSuse Linux (Betriebssystemdistributionen)
  - VNC (Fernwartung)
  - Apache (Web-Server)
  - Tomcat (Applicationsserver)
  - Squid (Web-Proxy-Server)
  - mySQL (Relationales Datenbankmanagementsystem)
  - PostgreSQL (DB - z.B. Produktiv im Kulturatlas)
  - Postfix (Mailserver)
  - Piwik (Website-Statistik)
  - Spamassassin (SPAM-Filterung)
  - Filezilla (FTP-Client)
  - Ready! basiert auf ZOPE (Redaktionssystem des LWL)
- Anwendungsentwicklung mit u.a.
  - Eclipse (JAVA-Anwendungsentwicklungsumgebung)

    - Hibernate, Spring, ZK, Wicket (Frameworks)
    - PostgreSQL (Datenbank)
    - deegree (Java-Framework - Verwaltung und Darstellung von geographischen Daten (z.B Kulturatlas))
    - Subversion (Versionsverwaltung von Sourcen/Quellcode)
- APC mit u.a.
    - Firefox (Browser)
    - 7-ZIP (Datenkomprimierung)
    - SSH, TeraTerm (Shell, verschlüsselte Netzwerkverbindung, Terminal-Emulator)
    - FreePDF
- File-Server, File-Server, DHCP- und DNS-Server, Depot-Server mit u.a.
    - SUSE Linux Enterprise Server OES2
- Monitoring von Servern mit Nagios / Icinga

Von 1453 Servern laufen 628 unter dem Open-Source-Betriebssystem Linux und (nur) 562 unter Windows. Die vorstehende Aufzählung der beim LWL eingesetzten Open-Source-Software ist nicht vollständig; es handelt sich durchaus um nennenswerte Produkte, die im täglichen Betrieb an strategisch wichtigen Stellen oder besonders häufig eingesetzt werden.

Im Bereich der großen strategischen Verfahren hat der LWL strategische Entscheidungen für Marktanbieter wie
- ANLEI (Verfahren in Einzelfallsachbearbeitung der Abt. 50, 60 und 61),
- SAP (u.a. Finanzwesen, Controlling, Bestellwesen, Personalwesen),
- NEXUS/KIS (Krankenhausinformationssystem) und
- SER (Dokumentenmanagementsystem)

getroffen und hat deren Closed-Source-Software lizenziert. In diesen Bereichen gibt es keine gleichwertige Open-Source-Software. Hinzu kommt, dass diese Verfahren hinsichtlich des Formularwesens und der Textverarbeitung meist technisch sehr eng mit Produkten von Microsoft verzahnt sind, so dass sich hieraus weitere Abhängigkeiten (Windows 7, Office 2007/2010 etc.) ergeben. Auch Produkte von Oracle, Adobe, Citrix oder Betriebssysteme wie AIX und Windows Server sind z.Zt. unverzichtbare kommerzielle Standard-Softwareprodukte beim LWL.

3. Generelle Überlegungen und Maximen

Zukunftssicherheit:
Im Grunde gilt bei Open-Source-Software, genauso wie bei jeder anderen Software auch, vor dem Einsatz ist zu prüfen, ob diese neben den fachlichen Anforderungen auch langfristig Bestand haben kann. Dabei muss geprüft werden, wie viele Entwickler die Software entwickeln und wie die Community aussieht, die das Produkt unterstützt.

Wirtschaftlichkeit:
Ob sich Kostenersparnisse erzielen lassen hängt davon ab, ob und wenn ja welches kommerzielle Produkt durch welches Open-Source-Produkt ersetzt werden kann. Bei der wirtschaftlichen Betrachtung einer Softwarelösung ist dabei zu beachten, dass die zu entrichtenden Lizenzgebühren nur eine zu berücksichtigende Kostengröße darstellen. Der Aufwand für Einführung und Betrieb der Software liegt in der Regel um ein Vielfaches über dem der Lizenzkosten. Ebenfalls muss IT-Fachpersonal für Open Source Produkte vorgehalten werden.

Schnittstellen:
Daneben ist angesichts der heutigen Softwaredurchdringung der Aspekt der Schnittstellen zu beachten. Die Integration neuer Software und die Anpassung neuer Softwareversionen ist ein Kostenbestandteil, der gerade bei der Einführung oft ein wesentlicher Faktor ist. Er entsteht aber potentiell über den gesamten Softwarelebenszyklus und wird durch die

Upgrade-Zyklen noch getrieben. Angesichts der heutigen Kritikalität der Schnittstellen für die Geschäftsprozesse ist wegen der fehlenden vertraglichen Absicherung bei Open Source Produkten eine intensive Abwägung vorzunehmen.

Sicherheit:
Das Thema Sicherheit wird im Zusammenhang mit freier Software besonders intensiv diskutiert. Weit verbreitet ist die Annahme, freie Software sei per se sicherer als z.B. gekaufte Closed-Source-Software. Aus Sicht des LWL ist diese Vermutung jedoch nicht haltbar. Als Beispiel sei auf einen Fehler in der Open-Source-Software SSL hingewiesen, der jahrelang unentdeckt blieb und für eine unsichere https-Übertragung verantwortlich war (http://heise.de/thema/Heartbleed).
Grundsätzlich gibt es einen ganz wesentlichen Unterschied zwischen Open- und Closed-Source-Software: Während ein Sicherheitsproblem bei einer freien Software bis in den Quellcode hinein verfolgt werden kann und damit die Fehlerursache transparent ist, bleibt es bei der Closed-Source-Software intransparent. In einem Fall ist der Nutzer in der Abhängigkeit eines kommerziellen Produktes - im anderen Fall in der Abhängigkeit einer unbekannten Entwicklergemeinschaft, über deren Fortbestehen und Zielrichtungen man nur mutmaßen kann. Aber auch für die Sicherheitsanalysen bei Open-Source-Produkten wäre ein signifikanter Personalaufwand zu betreiben. De facto hat heute keine Verwaltung die Zeit, den offen gelegten Programmcode zu prüfen.

Beispiele München / Wien:
Die zitierten Beispiele der Stadtverwaltungen München und Wien weisen auf Umstellungsprojekte auf Open-Source-Software hin. Gleichwohl sind diese Vorhaben nicht unumstritten und weisen nicht unerhebliche Schwierigkeiten auf. Unseres Wissens wurde in Wien der flächendeckende Umstieg auf Open-Source-Software auf den Endgeräten 2009 aufgrund von Kompatibilitätsproblemen nicht weiter verfolgt. Hingegen sind nach Pressemitteilungen mehr als 80% der Arbeitsplätze in München umgestellt. Gleichwohl gibt es auch hier kritische Anmerkungen zur „Alltagstauglichkeit des Systems“.

4. IT-Strategie des LWL

Die IT-Strategie des LWL wird in den regelmäßig tagenden Sitzungen des IT-Steuerungsgremiums fortgeschrieben. Standardtagesordnungspunkte sind neue Projekte und Vorhaben, die alle einer Wirtschaftlichkeitsbetrachtung unterliegen, und die fortschreitende IT-Standardisierung. Die LWL.IT hat in einem Dokument alle aktuellen Standards dokumentiert und schreibt dies regelmäßig fort. Zusammenfassend ergibt sich aktuell aus Sicht der LWL.IT kein Handlungsbedarf für eine neue Open-Source-Software-Strategie.