STUTTGART

Behördlicher Beauftragter für
Datenschutz und IT-Sicherheit
AK/DSB

Bericht
2013/2014

Datenschutz und IT-Sicherheit

Impressum

STUTTGART

Behördlicher Beauftragter
für Datenschutz und IT-Sicherheit
der Landeshauptstadt Stuttgart

Eberhardstraße 6a, 70173 Stuttgart
Telefon 0711 216-88387
Telefax 0711 216-950106

Redaktionsschluss: Dezember 2014

Inhalt

1 Vorwort

Die letzten Monate waren folgenreich für die Wahrnehmung der IT-Sicherheit. Wir haben erfahren, dass persönliche Gespräche oder vertrauliche E-Mails keinesfalls – egal ob im privaten oder geschäftlichen Kontext – vor Dritten geschützt sind oder sogar geschützt werden können.

Diese Enthüllungen über das Abhören von Daten und die immer wieder auftretenden Meldungen über Datenschutzlecks und Datenschutzskandale werfen die Frage auf, ob Datenverkehr heute überhaupt noch sicher gewährleistet werden kann. Wir müssen uns als Kommune, der die Bürgerinnen und Bürger Ihre Daten – z. T. unfreiwillig aufgrund gesetzlicher Verpflichtung – anvertraut haben, fragen, wie wir gegenüber den Betroffenen den Schutz dieser Daten sicherstellen und vor allem darstellen können.

Technische Innovationen und neue Formen des Arbeitens (z. B. mobiles Arbeiten und Telearbeit) entwickeln sich und müssen auch unter dem Aspekt des Datenschutzes betrachtet und beherrscht werden. Die Landeshauptstadt Stuttgart als moderner und innovativer Arbeitgeber, kann und darf sich diesen neuen Arbeitsformen nicht verschließen. Die Konkurrenz am Arbeitsmarkt erfordert hier aktives Agieren und nicht nur Reagieren.

Der Spagat zwischen dem Schutz unserer Daten und der Nutzung des technischen Fortschritts wird in den nächsten Jahren für uns alle eine große Herausforderung. Eine mittelalterliche Datenfestung ist zwar wünschenswert, aber nicht mehr zeitgemäß.

Angesichts der scheinbar übermächtigen Fähigkeiten der Geheimdienste die Hände in den Schoss zu legen, wäre sicher die falsche Konsequenz. Auch wenn ein Angriff auf die IT-Infrastruktur der Landeshauptstadt Stuttgart durch Geheimdienste nicht besonders plausibel erscheint, so gibt es jedoch auch andere Angreifer, die über ebenfalls mächtige Instrumente zum Eindringen in unsere Infrastruktur verfügen. Wir dürfen deshalb jedwedem Angreifer unsere Daten nicht auf dem silbernen Tablett präsentieren.

Sicherheit gibt es aber nicht zum Nulltarif, deshalb benötige ich Ihre Unterstützung und die der Fachverwaltung.

2 Aufgaben des Behördlichen Beauftragten für Datenschutz und IT-Sicherheit

2.1 Gesetzliche Aufgaben

Nach § 10 Abs. 4 Landesdatenschutzgesetz Baden-Württemberg (LDSG) hat der behördliche Datenschutzbeauftragte die Aufgabe, die öffentliche Stelle bei der Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu unterstützen. Zu seinen Aufgaben gehört es insbesondere,

1. auf die Einhaltung der Datenschutzvorschriften bei der Planung, Einführung und Anwendung von Verfahren, mit denen personenbezogene Daten automatisiert verarbeitet werden, hinzuwirken,
2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz und den besonderen Erfordernissen des Datenschutzes in ihrem Tätigkeitsbereich vertraut zu machen sowie
3. das Verfahrensverzeichnis gemäß § 11 LDSG zu führen.

Der behördliche Datenschutzbeauftragte ist vor dem Einsatz oder der wesentlichen Änderung eines automatisierten Verfahrens rechtzeitig zu unterrichten.

2.2 Vom Oberbürgermeister übertragene Aufgaben

Mit der Geschäftsanweisung Datenschutz und IT-Sicherheit für die Landeshauptstadt Stuttgart (Mitteilungen des Bürgermeisteramts, Folge 9, Nr. 13/2006) wurden AK/DSB weitere Aufgaben übertragen, insbesondere der im LDSG nicht geregelte Verantwortungsbereich IT-Sicherheit.

AK/DSB hat die Aufgabe – unbeschadet der eigenen Verantwortung für Datenschutz und IT-Sicherheit der Behördenleitung (OB, Referate, Ämter und Eigenbetriebe) – auf die Einhaltung der Datenschutzvorschriften und der IT-Sicherheit bei der Landeshauptstadt Stuttgart hinzuwirken und zu beraten.

Im Bereich Datenschutz gehören vor allem zu seinen Aufgaben:

- Bearbeitung von datenschutzrechtlichen Grundsatzfragen,
- Beratung bei ämterübergreifenden Datenschutzangelegenheiten,

- Kontrolle der Einhaltung der Vorschriften des LDSG und anderer Vorschriften über den Datenschutz in der Stadtverwaltung,
- Erarbeitung oder Mitwirkung bei der Erstellung von Richtlinien, Rundschreiben, Dienstvereinbarungen, Satzungen u. Ä., die den Umgang mit personenbezogenen Daten betreffen,
- Unterstützung der Datenschutzbearbeiterinnen und Datenschutzbearbeiter in den Ämtern und Eigenbetrieben,
- Beteiligung und Beratung bei Planung und Durchführung von Maßnahmen, Projekten der Informations- und Kommunikationstechnik und automatisierter Verfahren,
- Information und Schulung städtischer Mitarbeiterinnen und Mitarbeiter,
- Führung des städtischen Verfahrensverzeichnisses nach § 11 LDSG,
- Prüfung des Ergebnisses der Untersuchung und dessen Begründung nach § 12 LDSG (Vorabkontrolle),
- Erstellen eines Berichts zum Datenschutz und zur IT-Sicherheit für den Verwaltungsausschuss alle zwei Jahre,
- Ansprechpartner für Anfragen von Bürgerinnen und Bürgern.

Zu den Aufgaben von AK/DSB im Bereich der IT-Sicherheit gehören vor allem:

- Beratung der Behördenleitung,
- Leitung des IT-Sicherheitsmanagementteams,
- Zentrale Anlaufstelle für alle Belange der IT-Sicherheit,
- Erstellen und Fortschreiben zentraler Richtlinien und Regelungen,
- Fortschreibung des IT-Sicherheitskonzepts,
- Unterstützung bei der Erstellung und Fortschreibung von Notfallvorsorgekonzepten und Notfallplänen,
- Fortschreibung des Realisierungsplans für Sicherheitsmaßnahmen und Kontrolle der Umsetzung,
- Unterstützung bei der Anwendung des IT-Grundschutzes und die Durchführung von Risikoanalysen zur Erstellung des IT-Sicherheitskonzepts,
- Kontrolle von IT-Sicherheitsmaßnahmen,
- Untersuchung sicherheitsrelevanter Vorfälle und Unterstützung bei der Behebung und künftigen Vermeidung,
- Vorbereitung und Durchführung von Dienstbesprechungen mit den IT-Sicherheitsbearbeiterinnen und IT-Sicherheitsbearbeitern,
- Schulungsmaßnahmen zum Thema IT-Sicherheit.

3 Datenschutz in den Berichtsjahren

3.1 Anfragen des Landesbeauftragten für den Datenschutz

In den Berichtsjahren 2013 und 2014 erreichten uns wieder eine Vielzahl von Anfragen des Landesbeauftragten für den Datenschutz Baden-Württemberg (LfD) nach § 28 LDSG.

In Ziffer 2.4.3 der Geschäftsanweisung Datenschutz und IT-Sicherheit (GA-DS/IT-S) ist dem Datenschutzbeauftragten eindeutig die Federführung für die Kontakte zum LfD übertragen. Folgerichtig sollten alle vom LfD eingehenden Datenschutzanfragen zunächst an uns und erst dann an die Fachverwaltung gehen. Der vorgeschriebene Rückweg ist der gleiche. Die Fachverwaltung erstellt einen Entwurf, wir prüfen diesen und schlagen gegebenenfalls Änderungen vor. Diese klare und sinnvolle Vorgabe der Geschäftsanweisung wurde in der Realität leider nicht immer eingehalten. Einige Beschwerden gingen direkt in den betroffenen Ämtern oder Eigenbetrieben ein und wurden sodann dort ohne unsere Mitwirkung bearbeitet. Auf diese Art und Weise kann es natürlich nicht gelingen, mit einer einheitlichen Datenschutzmeinung der Landeshauptstadt Stuttgart gegenüber dem LfD aufzutreten.

Bei bestimmten Referenten des LfD ist eine neue Qualität und Quantität der Anfragen festzustellen. Trotz umfassender Stellungnahmen unsererseits wird nochmals mehrere Male schriftlich nachgefragt. Die Beantwortung in Zusammenarbeit mit der Fachverwaltung ist dadurch erheblich aufwändiger geworden.

Positiv sollte erwähnt werden, dass auch in den Berichtsjahren 2013/2014 keine formelle Beanstandung des LfD nach § 30 LDSG zu verzeichnen ist. Hinweise und Kritik gab es durchaus, dies ist aber häufig auch einer unterschiedlichen Rechtsansicht geschuldet. Wir sehen die Dinge meist pragmatisch und weniger dogmatisch. In der Diskussion mit der Fachverwaltung ergeben sich manchmal Lösungswege, die sich aus akademischer Sicht eher nicht aufdrängen.

Nur ein Beispiel: Die Thekenlösung in den Bürgerbüros ist sicher die zweitbeste Lösung zu Bürgergesprächen in Einzelbüros. Gleichwohl meinen wir, eine moderne Verwaltung kann sich nicht "einschließen", sie muss offen und kommunikativ auf die Bürger zugehen. Man darf deshalb aber auch nicht die Augen davor

verschließen, dass aus dieser offenen Lösung Konflikte und Datenschutzeingaben resultieren können, z. B. beim Mithören von Gesprächen.

WAS IST ZU TUN?
Wir haben bei der Dienststelle des LfD und den betroffenen Ämtern und Eigenbetrieben im allseitigen Interesse nochmals nachdrücklich um Beachtung unserer Zuständigkeit gebeten. Es liegt nun vor allem an den Fachdienststellen, die Vorgaben der GA-DS/IT-S auch einzuhalten. Gemeinsam suchen wir eine Lösung der Konflikte im allseitigen Interesse.

3.2 Datenschutzbeschwerden, ein heikles Thema

Ein häufiges Ärgernis bei Datenschutzbeschwerden ist die Instrumentalisierung des Datenschutzes für eigentlich andere Anliegen. Vielfach ist es der Fall, dass vor Eingehen einer Datenschutzbeschwerde bereits eine Dienstaufsichtsbeschwerde eingelegt oder Vorgesetzte bis hin zur Amtsleitung angeschrieben wurden. Dem Betroffenen geht es also eigentlich gar nicht um die Wahrnehmung seines informationellen Selbstbestimmungsrechts, vielmehr will er über den Hebel Datenschutz etwas ganz anderes erreichen, beispielsweise Auskünfte nicht zu geben, zu denen er eigentlich verpflichtet ist.

Obwohl wir uns mit jeder Beschwerde individuell befassen, haben sich im Lauf der Zeit typische, aber höchst unterschiedliche Fallkonstellationen herauskristallisiert:

1. Berechtigte, belegbare Beschwerden zum ungesetzlichen oder unfairen Umgang mit den Daten von Betroffenen,
2. Vermutete Verstöße gegen Datenschutz oder IT-Sicherheit,
3. Beschwerden, die vorgetäuscht oder aufgebauscht sind, um Vorteile herauszuschlagen,
4. Beschwerden, die bei näherem Hinsehen irrational wirken (Beispiel nach diesem Artikel).

In allen Fällen ist der Beauftragte für Datenschutz und IT-Sicherheit verpflichtet, gründlich zu recherchieren, um was es eigentlich geht. Ziffer 1 signalisiert ernsthaften Handlungsbedarf, während Ziffer 4 auf Menschen hindeutet, die für vernünftige Argumente eher unzugänglich sind.

Manche Vorwürfe und Bedrohungen, mit denen Sachbearbeiterinnen und Sachbearbeiter – und in der Folge der Datenschutzbeauftragte – in der Praxis kon-

frontiert werden, sind erschreckend und fallen unter das Szenario Ziffer 4. Wenn ein Beschwerdeführer aggressiv wird und mit Körperverletzung droht, dann sind unvorbereitete Sachbearbeiterinnen und Sachbearbeiter damit häufig mental überfordert. Völlig legale Datenverwendungen können bei bestimmten Persönlichkeitsstrukturen dazu führen, dass sich jemand eingeengt fühlt und den vermeintlichen Verursacher massiv bedroht. Wir raten den besonders gefährdeten Bereichen mit Publikumsbetrieb im Jugendamt, Sozialamt, Jobcenter und bei den Bürgerbüros deshalb zum Besuch von Seminaren, bei denen deeskalierende Strategien vermittelt werden. Hierfür eignet sich hervorragend das von unserem städtischen Weiterbildungszentrum angebotene Seminar "Professioneller Umgang mit Beleidigungen und Bedrohungen am Arbeitsplatz" (Seminar Nr. AG 440). Dort werden unter anderem Methoden der Eigensicherung, zur Einschätzung der Gefährdung und geeignete Maßnahmen aufgezeigt. Ebenfalls angeboten werden die Inhouse-Seminare "Deeskalationsstrategien im Umgang mit schwierigen Klientinnen und Klienten" (Seminar Nr. inhouse 400) als Grundlagenseminar und ein Aufbauseminar mit dem Schwerpunkt Selbstschutz (Seminar Nr. inhouse 420).

WAS IST ZU TUN?

Durch proaktive Aufklärung und rechtzeitige Beratung der Bürger können in der Bearbeitung zeitaufwändige Beschwerden bereits im Vorfeld abgefangen werden.

Der erfolgreiche Umgang mit aggressiven Beschwerdeführern gelingt nur bei rechtzeitiger Schulung.

[redacted]
Stuttgart

Meldestelle
Bürgerbüro
[redacted]
Stuttgart

[redacted] 2014
Landeshauptstadt Stuttgart
Amt für öffentliche Ordnung
Bürgerbüro [redacted]

[redacted]

Stuttgart, 21. Dezember 2014

Datenübermittlung aus dem Melderegister

Sehr geehrter Damen und Herren,

von einem Frau [redacted] habe ich eine Antwort auf meinen Brief vom Juli 2014 erhalten. In diesem untersage ich Ihnen weiterhin und erneut die Weitergabe meiner personenbezogenen Daten an jedwede Stelle oder Person.

Ich habe einem Herrn [redacted] bereits geschrieben, dass ich sicher bin, das der Paragraph 32 aus dem Meldegesetz des Landes Baden-Württemberg keine Anwendung findet, da das Recht auf informationelle Selbstbestimmung ein höheres Rechtsgut ist, als Ihr Landesmeldegesetz. Falls dies nicht so sein sollte, bitte ich Sie mir entsprechende Referenzurteile und Gesetzestexte (wie z.B. „Landesgesetz bricht Bundesrecht") zu übersenden. Falls Sie dies nicht können, bitte ich Sie die Situation von einem Gericht beurteilen zu lassen. Eine einfache Bestätigung im Tenor „das hat schon alles seine Richtigkeit" kann ich nicht akzeptieren. Der Satz „Ich kann Ihnen jedoch versichern, dass die Datenübermittlung entsprechend den gesetzlichen Vorgaben erfolgt." lässt sich gerichtlich klären. Bitte tun Sie dass, oder untermauern Sie Ihre Behauptung mit entsprechenden Referenzurteilen und Gesetzestexten.

Interessanterweise listet Herr [redacted] mehrere Stellen auf, mit denen ein „regelmässiger" Datenaustausch stattfinden würde. Ist das so, dass Sie meine Daten einfach so, ohne meine Zustimmung weitergeben? An wen haben Sie wann und warum meine personenbezogenen Daten weitergegeben? In jedem Fall verlange ich eine detaillierte schriftliche Aufstellung wem, wann, und wieso meine personenbezogenen Daten übergeben werden. Ich hatte Ihnen mehrfach angeboten, dass Sie meine Daten nach persönlicher Rücksprache mit mir weitergeben können. Eine Weitergabe ohne vorherige Information meiner Person hat zu unterbleiben.

Das Recht auf informationelle Selbstbestimmung ist zwar auch im Volkszahlungsurteil eingeschränkt, jedoch nur wenn „die Datenübermittlung" durch ein Gesetz legitimiert ist und die Personengruppe jeweils eingeschränkt ist.

Bitte teilen Sie mir mit welchem Gesetz die Weitergabe meiner personenbezogenen Daten an die Bundeszentrale für Steuern legitimiert wird. Ich bezweifele, dass dies eine abgeschlossene Personengruppe ist. Bitte teilen Sie mir die genaue Grösse dieser Personengruppe mit. Bitte teilen Sie mir die Namen aller dieser Personengruppe zugehörigen Personen mit.

Bitte teilen Sie mir mit welchem Gesetz die Weitergabe meiner personenbezogenen Daten an die Datenstelle der Rentenversicherungsträger legitimiert wird. Ich bezweifele, dass dies eine abgeschlossene Personengruppe ist. Bitte teilen Sie mir die genaue Grösse dieser Personengruppe mit. Bitte teilen Sie mir die Namen aller dieser Personengruppe zugehörigen Personen mit.

Bitte teilen Sie mir mit welchem Gesetz die Weitergabe meiner personenbezogenen Daten an die Bundesagentur für Arbeit legitimiert wird. Ich bezweifele, dass dies eine abgeschlossene Personengruppe ist. Bitte teilen Sie mir die genaue Grösse dieser Personengruppe mit. Bitte teilen Sie mir die Namen aller dieser Personengruppe zugehörigen Personen mit.

Bitte teilen Sie mir mit welchem Gesetz die Weitergabe meiner personenbezogenen Daten an die Landesrundfunkanstalt legitimiert wird. Ich bezweifele, dass dies eine abgeschlossene Personengruppe ist. Bitte teilen Sie mir die genaue Grösse dieser Personengruppe mit. Bitte teilen Sie mir die Namen aller dieser Personengruppe zugehörigen Personen mit.

Bitte teilen Sie mir mit welchem Gesetz die Weitergabe meiner personenbezogenen Daten an Statistische Landesamt legitimiert wird. Ich bezweifele, dass dies eine abgeschlossene Personengruppe ist. Bitte teilen Sie mir die genaue Grösse dieser Personengruppe mit. Bitte teilen Sie mir die Namen aller dieser Personengruppe zugehörigen Personen mit.

Bitte teilen Sie mir mit welchem Gesetz die Weitergabe meiner personenbezogenen Daten an die Polizei legitimiert wird. Ich bezweifele, dass dies eine abgeschlossene Personengruppe ist. Bitte teilen Sie mir die genaue Grösse dieser Personengruppe mit. Bitte teilen Sie mir die Namen aller dieser Personengruppe zugehörigen Personen mit.

Bitte teilen Sie mir mit welchem Gesetz die Weitergabe meiner personenbezogenen Daten an das Meldeportal legitimiert wird. Ich bezweifele, dass dies eine abgeschlossene Personengruppe ist. Bitte teilen Sie mir die genaue Grösse dieser Personengruppe mit. Bitte teilen Sie mir die Namen aller dieser Personengruppe zugehörigen Personen mit.

Bitte teilen Sie mir mit welchem Gesetz die Weitergabe meiner personenbezogenen Daten an die LRA Kfz-Zulassung und FS-Behörde legitimiert wird. Ich bezweifele, dass dies eine abgeschlossene Personengruppe ist. Bitte teilen Sie mir die genaue Grösse dieser Personengruppe mit. Bitte teilen Sie mir die Namen aller dieser Personengruppe zugehörigen Personen mit.

Nach Paragraph 33 Ihres Landesmeldegesetzes kann auch eine Auskunftssperre eingetragen werden. Ich habe Herrn [redacted] bereits Tatsachen vorgebracht, die auf eine 'Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen' hindeuten. Ich habe bereite mehrfach erläutert, dass ich mein Grundrecht auf informationelle Selbstbestimmung eingeschränkt sehe. Dieses ist nach dem Volkszählungsurteil eng mit der persönlichen Freiheit (GG, Artikel 2) verknüpft, d.h. ich kann bestimmen wer wann und warum meine persönlichen Daten übermittelt bekommt. Somit liegt eine Einschränkung meiner persönlichen Freiheit – sogar auf der Grundlage des von Ihnen vorgebrachten Gesetzestextes – vor. Ich bitte Sie, dass nicht nur die komplette Weitergabe meiner personenbezogenen Daten zu unterlassen ist, sondern auch eine Auskunftssperre nach Paragraph 33 zu meinen Daten eingetragen wird.

Falls Sie oder das Meldeamt das Gefühl haben meine Daten weiterhin weitergeben zu wollen, dann können Sie bitte gerichtlich klären lassen, ob Ihre Interessen, bzw. das Meldegesetz von Baden-Württemberg ausreichend ist, um Einschränkungen an meinen Grundrechten zu erlauben. Bis dahin hat eine Weitergabe meiner personenbezogenen Daten zu unterbleiben.

Falls Sie mein Recht auf informationelle Selbstbestimmung nicht garantieren können, bitte ich Sie meine Daten umgehend und vollständig aus Ihren Registern zu löschen. Der obenstehende Text gilt auch fuer meine gesamte Familie [redacted].

[redacted]

3.3 Aus den Augen, aus dem Sinn? Der Postausgang

Jede verantwortliche Stelle versendet Briefe und Pakete. Aber ist ihr bewusst oder bekannt,

- was nach der Aufgabe der Sendung bei der Post oder nach dem Einwurf in einen Postkasten damit geschieht,
- durch wessen Hände sie läuft,
- wer sie schließlich ausliefert oder
- was mit ihr im Fall der Unzustellbarkeit passiert?

Früher war alles ganz einfach: Es gab die Deutsche Bundespost. Sie hatte das Brief- und Paketbeförderungsmonopol. Ihre Mitarbeiter waren Beamte, und so musste man darauf vertrauen, dass bei der Postbeförderung schon alles mit rechten Dingen zuging. Heute ist das anders: Das Beförderungsmonopol existiert längst nicht mehr. Dafür gibt es einige große und viele kleine bis ganz kleine Postdienstleister, und bei der Beförderung geht die Sendung durch die Hände mehrerer selbstständiger Unternehmen. Derzeit sind über 5.000 Subunternehmer für andere Postdienstleister tätig.

Vor diesem Hintergrund drängt sich die Frage nach der Sicherheit beim Verschicken förmlich auf. Genaue Zahlen, wie viele Postsendungen nicht beim Empfänger ankommen, gibt es nicht. Dass die Inhalte der Postsendungen und die näheren Umstände des Postverkehrs, also die Verbindungsdaten (von wem, wann, wie oft, auf welchem Wege, mit welchen Zusatzleistungen, an wen), in der Regel durch das Post- und Briefgeheimnis und durch strafrechtliche Normen geschützt sind, ist ein schwacher Trost.

Natürlich gibt es auch einen zivilrechtlichen Schutz der Postbeförderung aufgrund der vertraglichen Pflichten des Beförderers. Dass dieser sorgsam mit den Sendungen umgehen und auch den Datenschutz wahren muss, sind Nebenpflichten aus dem Beförderungsvertrag. Zudem gibt es für den Datenschutz die Postdienste-Datenschutzverordnung. Aber wie in der gesamten Wirtschaft gibt es auch im Postsektor Schwächen bei der Umsetzung und Kontrolle des Datenschutzes. Das Versenden von sensiblen Sendungen auf dem Postweg muss daher als unsicher bezeichnet werden.

Im Herrschaftsbereich der verantwortlichen Stelle unterliegen die Inhalte von Postsendungen dem Datenschutz nach den bekannten Datenschutzvorschriften. Muss die verantwortliche Stelle aber den Schutz der Daten auch sicherstellen,

wenn diese ihren Herrschaftsbereich verlassen? Ja, denn sie muss auch für den sicheren Transport zum Empfänger sorgen (sogenannte Weitergabekontrolle bei der Übermittlung und Weitergabe im Rahmen einer Auftragsdatenverarbeitung).

Die Versendung von Daten an den Betroffenen selbst ist zwar keine Übermittlung, da er nicht als Dritter gilt. Aber zum einen gebietet es die Sorgfaltspflicht, auch die Daten bei der Übersendung an den Betroffenen zu schützen. Zum anderen ist die Übersendung an den Betroffenen als Datennutzung anzusehen. Und damit gilt auch hier § 9 LDSG mit seiner Maßgabe, die erforderlichen Schutzmaßnahmen in einem angemessenen Verhältnis zum angestrebten Schutzzweck zu ergreifen.

Da der Postdienstleister auf die Inhalte der Postsendungen grundsätzlich nicht zugreifen darf, liegt bezüglich der Inhalte keine Übermittlung an den Postdienstleister vor. Der Absender muss allerdings dafür Sorge tragen, einen Postdienstleister einzusetzen, bei dem eine bestimmungsgemäße Leistungserbringung und gesetzeskonformer Umgang mit den Postsendungen zu erwarten sind. Ansonsten kann doch eine Übermittlung vorliegen.

Die Empfänger- und ebenso die Absenderadresse enthalten sehr häufig personenbezogene Daten (Namen, Titel, Funktion, Privatanschrift). Auch hier muss beim Postversand daran gedacht werden, dass es sich um schutzwürdige Daten handelt. Bei Absendern wie Gesundheitsamt, Jugendamt, Sozialamt oder Jobcenter sind es sogar sensible Daten. Schutzwürdig ist z. B. schon allein die Tatsache, dass jemand Klient beim Sozialamt ist. Hier sollten neutrale Briefumschläge mit dem unverfänglichen Absender "Landeshauptstadt Stuttgart" zum Einsatz kommen.

WAS IST ZU TUN?

Datenschutz beginnt im Kleinen. Es gilt, jederzeit wachsam zu sein. Auch ein unbedacht adressierter Briefumschlag kann schon eine unzulässige Datenübermittlung darstellen.

3.4 Datenlöschung in der Personalverwaltungssoftware dvv.Personal

Personaldaten müssen sachgerecht gelöscht werden, wenn sie nicht mehr benötigt werden. Für die neue Personalverwaltungssoftware dvv.Personal gab es die-

se Möglichkeit bisher noch nicht. Inzwischen ist dvv.Personal seit einigen Jahren im Einsatz und daher rücken die Stichtage näher, zu denen erstmalig Daten aufgrund der ablaufenden Aufbewahrungsfristen gelöscht werden müssen. In einer Arbeitsgruppe unter Leitung der Datenzentrale Baden-Württemberg, in der neben Vertretern verschiedener Gemeinden, dem KDRS und der Gemeindeprüfanstalt auch die Landeshauptstadt Stuttgart mit AK/DSB, Personalverwaltung und SAP - Competence Center Stuttgart (CCS) mitwirken, wurde mit der Planung der erforderlichen Löschprozeduren begonnen.

In dvv.Personal werden alle Daten eines Mitarbeiters gespeichert, welche eine ordnungsgemäße Personalverwaltung mit sich bringen. Dazu ist eine hochkomplexe Datenstruktur mit unzähligen Datenverknüpfungen erforderlich. Dies geht über den Namen und die Personalnummer weit hinaus und reflektiert den gesamten beruflichen Werdegang eines Mitarbeiters. Für alle diese unterschiedlichen Datenarten wurden in den verschiedenen Gesetzen und Vorschriften auch unterschiedliche Aufbewahrungsfristen definiert, die bei der Löschung berücksichtigt werden müssen.

Diesem dichten Datengeflecht wird nun mit SAP Lifecycle Management zu Leibe gerückt. Das Werkzeug lässt sich gut an die jeweiligen Anforderungen anpassen. Auf keinen Fall darf die Löschung von Personalfällen dazu führen, dass einzelne Abrechnungsdaten oder andere Angaben zu diesen Mitarbeitern im System verbleiben. Gleichzeitig dürfen keine Angaben gelöscht werden, die beispielsweise noch für Zwecke der Haushaltsrevision oder für externe Prüfungen vorgehalten werden müssen. Zusätzlich muss sichergestellt sein, dass die Löschprozesse nur mit entsprechenden Berechtigungen ausführbar sind.

In der Arbeitsgruppe wurden zunächst drei Fallgruppen identifiziert, für welche die Löschung als erstes in Angriff genommen werden soll. An diesen Rahmen passte die Datenzentrale das Programm an. Die Kommunen, welche dvv.Personal nutzen, müssen diesen Rahmen nur noch an die lokalen Anforderungen angleichen und der Löschprozess sollte erfolgreich ablaufen. Die ersten Tests wurden im Herbst 2014 ausgeführt. Die Ergebnisse lagen zum Zeitpunkt der Erstellung des Tätigkeitsberichts noch nicht vor. In der Projektgruppe ist man jedoch zuversichtlich und hofft darauf, dass im nächsten Jahr an der Umsetzung der übrigen Fälle weitergearbeitet werden kann.

WAS IST ZU TUN?

Zweifelsohne handelt es sich bei Personaldaten um besonders schützenswerte Daten. Dies erfordert besondere Sorgfalt im Umgang und bei der Verarbeitung der Daten. Die Vorarbeiten für die gesetzlich vorgesehene Datenlöschung benötigen Zeit und genaueste Analyse der Ausgangssituation. Die aufgefundenen Sachverhalte sind gegen sachliche und rechtliche Vorgaben abzugleichen, dann ist der erforderliche Verarbeitungsprozess exakt zu planen und umzusetzen. Gründlichkeit ist hierbei oberstes Gebot, denn nur so werden die Grundlagen für dauerhafte, sichere Prozesse geschaffen.

3.5 SAP TwoGo – Mitfahrbörse aus der Wolke

Im September 2014 konnten wir der Presse die groß aufgemachte Meldung entnehmen, dass kompromittierende Bilder von Prominenten aus der sogenannten Cloud gestohlen und unrechtmäßig im Internet verbreitet wurden. Dabei steht der Begriff Cloud für eine IT-Strategie mit verteilten Hard- und Software-Ressourcen, die von einem oder mehreren Providern im Internet bereitgestellt und auf Anforderung genutzt werden können. Diese Meldung zeigt uns, dass personenbezogene Daten in der Cloud entgegen den Beteuerungen der Betreiber nicht immer sicher sind.

Wenige Monate zuvor haben das Land Baden-Württemberg und die Landeshauptstadt Stuttgart sich zu einer Pilotphase mit SAP TwoGo entschieden. Im Rahmen eines allgemeinen Präsentationstermins wurde uns die Anwendung vorgestellt, mit der die Landeshauptstadt Stuttgart ihren Beschäftigten eine weitere Möglichkeit zur Bildung von Fahrgemeinschaften eröffnen möchte. Wir waren gebeten worden, für diese Applikation eine Beurteilung aus datenschutzrechtlicher Sicht abzugeben.

Die Anwendung präsentiert sich modern und zweckmäßig. Die erstmalige Registrierung funktioniert problemlos und einmal angemeldet, lässt sich die Suche nach einer Mitfahrgelegenheit recht einfach bewerkstelligen. Nebenbei und ganz im Stile von Social Media Netzwerken bekommt der Anwender danach ständig Neuigkeiten aus der gesamten Community angezeigt. Alle Teilnehmer bewegen sich hierbei innerhalb ein und derselben Cloud. In diesem Pilotprojekt wird der Service im Auftrag der Landeshauptstadt Stuttgart betrieben, was an der automatischen Einbindung der dienstlichen E-Mail-Adresse sichtbar wird. Wer bei dieser Mitfahrbörse registriert ist, nutzt sein Postfach automatisch auch privat, was nach

der Dienstvereinbarung zur E-Mail-Nutzung gewisse Einschränkungen des Zugriffs nach sich zieht.

SAP TwoGo ist als klassischer "Software as a Service" realisiert worden. Dieses Cloud-Modell basiert auf dem Grundsatz, dass die Software und die IT-Infrastruktur bei einem externen IT-Dienstleister betrieben und vom Kunden als Service genutzt wird. Das Rechenzentrum befindet sich derzeit bei SAP in Walldorf und wird dort, folgt man den Beschreibungen, nach den gängigen Sicherheitsprinzipien betrieben. Es liegt somit der klassische Fall der Funktionsübertragung auf einen Dritten vor, bei der ein Einfluss der Landeshauptstadt Stuttgart als Auftraggeber auf den Betriebsablauf jedoch nicht gegeben ist. Bei dieser Form der Datenverarbeitung gibt es kein gesetzlich vorgeschriebenes Kontrollrecht des Städtischen Beauftragten für den Datenschutz und IT-Sicherheit. Ein Weisungsrecht zum technischen Betriebsablauf fehlt ebenfalls. Vertragliche Anpassungen, wie sie mit anderen Auftragnehmern durchaus üblich sind, sind schwierig zu verabreden. Die Orientierungshilfe des Düsseldorfer Kreises zum Thema Datenverarbeitung in der Cloud listet neben diesen Punkten noch eine ganze Reihe weiterer Kriterien auf, welche eine derartige Verarbeitung an weitere Bedingungen knüpft.

Die Lektüre der Datenschutzbestimmungen und der Beschreibung der gespeicherten, personenbezogenen Daten bei SAP TwoGo lassen nicht wirklich Hoffnung aufkeimen. Der einzelne Benutzer hat das Recht, den Vorgaben von SAP zu folgen und kann den Dienst nutzen, oder er stimmt dem nicht zu, dann nimmt er auch nicht teil. Einschränkungen lassen sich nicht formulieren. Darüber hinaus behält sich SAP vor, übrigens wie die meisten anderen Anbieter von Cloud-Services ebenfalls, die Datenschutzbestimmungen oder die Nutzungsbedingungen nach eigenem Erfordernis zu verändern. Für uns besteht Erklärungsbedarf, warum und wie lange manche Benutzerdaten überhaupt gespeichert werden. Diese Fragen wurden von uns gestellt, die Antworten befriedigten letztlich nicht.

Trotzdem hat sich AK/DSB dazu entschlossen, einem Probebetrieb keine Hindernisse in den Weg zu stellen. Schließlich wird Datenverarbeitung in der Cloud andernorts zunehmend genutzt und man wird sich dem Trend mit datenschutzrechtlichen Bedenken nicht dauerhaft entgegenstemmen können. Wir halten es aus diesen Gründen durchaus für geboten, dass Erfahrungen mit dieser Technologie gesammelt werden, um hier für die Zukunft entsprechend gewappnet zu sein. Allerdings verbinden wir diese vorübergehende Nutzung mit der Forderung, die Zweifel bis zum Ende des Probebetriebs vollkommen auszuräumen, eine

vertragliche Basis für diese Auftragsdatenverarbeitung vorzubereiten sowie einige Forderungen zum technisch-organisatorischen Datenschutz zu erfüllen.

WAS IST ZU TUN?

AK/DSB unterstützt und begleitet die Erprobung neuer Technologien. Dies setzt allerdings voraus, dass wir rechtzeitig eingebunden und umfassend informiert werden. Nur mit dem Blick aufs Ganze können wir rechtzeitig und umfassend beraten.

3.6 Verarbeitung personenbezogener Daten von Bäderkunden im Ausland

Im Rahmen unserer beratenden Tätigkeit sind wir darauf aufmerksam geworden, dass der Eigenbetrieb Bäderbetriebe Stuttgart einen Teil der Daten zum Betrieb seiner elektronischen Schließanlage in Schweden speichern und verarbeiten will. Hintergrund der Auslagerung ist, dass der PC, auf dem das System seit der Inbetriebnahme des Schließanlagensystems installiert war, im Eigenbetrieb ohne ausreichende Sicherungsmaßnahmen lief.

Um diesem schon längere Zeit andauernden Versäumnis abzuhelfen, hat man nach Lösungsalternativen gesucht. Auch der Betrieb eines Servers im städtischen Serverraum war in die Überlegungen mit einbezogen worden. Die Entscheidung fiel jedoch zugunsten eines Anbieters aus Schweden, weil sich herausstellte, dass das Angebot des Cloudbetreibers nur ein Fünftel des Preises ausmachte, der für eine eigene, innerstädtische Lösung angefallen wäre.

Bei den verarbeiteten Datenarten handelt es sich zwar nur um die Vor- und Nachnamen eines eingeschränkten Personenkreises und die Betroffenen wurden vorab um ihre Einwilligung gebeten. Für diese Daten leitet sich auch kein besonderer Schutzbedarf ab, so dass an den Cloud-Anbieter keine erhöhten Anforderungen in Bezug auf eine sicherheitstechnische Zertifizierung zu stellen sind. In diesem Fall kann aus datenschutzrechtlicher Sicht die Verarbeitung der Daten im europäischen Ausland nicht untersagt werden. Ob der gewählte Anbieter dem Vergleich mit den verbindlichen Service-Level-Agreements und den hohen Sicherheitsstandards des eigenen Serverparks standhalten kann, entzieht sich allerdings unserer Kenntnis.

Grundsätzlich ist bei der gewählten Cloud-Lösung weiterhin zu beachten, dass ein Vertrag nach § 7 LDSG zur Datenverarbeitung im Auftrag abgeschlossen werden muss.

Im Allgemeinen sind wir weiterhin der Meinung, dass die Verarbeitung von personenbezogenen Daten grundsätzlich in der städtischen Infrastruktur erfolgen sollte, weil hier beste datenschutzrechtliche Bedingungen gegeben sind und der IT-Sicherheit besondere Bedeutung eingeräumt wird.

WAS IST ZU TUN?

Die handelnden Personen müssen sich gewahr sein, dass wir alle der "Konzern" Landeshauptstadt Stuttgart sind. Unseres Erachtens ist es widersinnig, eine hervorragend aufgestellte IT bei der Abteilung IuK des Haupt- und Personalamts zu betreiben und andererseits bei neuen Aufträgen auf den kleinen finanziellen Vorteil externer Dienstleister zu setzen.

3.7 SoJuHKR löst Verfahren WAUS ab

Viele Jahre wurden Leistungen aus der kommunalen Sozialkasse mit dem zum Finanz- und Rechnungswesen (FIWES-Classic) gehörenden Verfahren für wiederkehrende Ausgaben (WAUS) abgewickelt. In der Finanzbuchhaltung hat inzwischen SAP und die doppische Buchhaltung das alte Verfahren abgelöst. Da auch das Verfahren WAUS vom Dienstleister nicht länger unterstützt wurde, konnte es bei der Landeshauptstadt Stuttgart nicht weiter betrieben werden. Die Abwicklung der Sozial- und Jugendbuchhaltung (SoJuHKR) erfolgt nun mit unserer betriebswirtschaftlichen Standardsoftware SAP im Rahmen der Geschäftspartnerbuchhaltung Public Sector Vertragskontokorrent (PSCD).

Damit die vielen Rädchen richtig ineinander greifen, wird ein erhebliches Maß an gemeinsamen Anstrengungen aller Beteiligten benötigt. So sind die Schnittstellen für den Datenaustausch bereitzustellen, die Prozessabläufe an die neuen Strukturen anzupassen und jede Menge Sand im Räderwerk der Aufgaben beim Fachamt, der Stadtkasse sowie dem Dienstleister und dessen zahlreichen beteiligten Stellen zu beseitigen.

Bei dieser Art von Leistungen werden auch besonders sensible Daten verarbeitet, für die besondere Sicherungsmaßnahmen zu ergreifen sind. So war sicherzustellen, dass die Daten nur verschlüsselt übertragen und auf den Zielsystemen bis zur Verarbeitung gespeichert werden. Die Zugriffsrechte mussten auf das gerade noch erforderliche Maß eingeschränkt werden. Gleichzeitig war zu prüfen, welche Daten unbedingt für die weitere Verarbeitung gebraucht wurden und zu übertragen waren bzw. welche Angaben im Vorverfahren verbleiben mussten. Gerade bei diesen Fragen war unser Rat, aber auch der mahnende Fingerzeig, besonders wichtig.

WAS IST ZU TUN?

Besonders sensible Daten sind zwingend verschlüsselt zu übertragen. Der sendende und der empfangende Server sind ebenfalls gegen unberechtigte Zugriffe zu sichern. Es sollte sich von selbst verstehen, dass die Dateien auf den Servern gelöscht werden, sobald sie nicht mehr erforderlich sind.

3.8 Blitzermarathon oder der rasende Motorradfahrer

Quelle: Stuttgarter Nachrichten vom 25.10.2013

Ein Motorradfahrer wurde im Stadtgebiet von Stuttgart elfmal geblitzt, zum Teil sogar posierend, etwa wie abgebildet mit hochgerissenen Armen. Das Blitzerfoto

nebst Sachverhalt mit diversen Zusatzangaben zum Fahrer und seinem Motorrad konnte den Stuttgarter Nachrichten entnommen werden.

Zumindest der Freundes- oder Bekanntenkreis des Beschuldigten kann ihn aufgrund der zahlreichen Zusatzangaben im Zeitungsartikel identifizieren. Eine Übermittlungsgrundlage für Blitzerfoto und Zusatzangaben an die Öffentlichkeit gibt es nicht.

Was war geschehen? Unsere Bußgeldstelle beim Amt für öffentliche Ordnung hatte nur das Blitzerfoto an die Zeitung übermittelt und zudem einige typische Merkmale auf dem Motorrad verpixelt. Damit wähnten sie sich auf der sicheren Seite. Die Zeitung hatte aber von der Sprecherin der Polizei die personenbeziehbaren Merkmale des Motorradfahrers erhalten und in ihren Artikel aufgenommen.

WAS IST ZU TUN?

Das Amt für öffentliche Ordnung hat zugesichert, künftig bei Presseauskünften grundsätzlich und ausnahmslos keine Fotoaufnahmen von Blitzern herauszugeben.

3.9 Übermittlungen aus dem Pass- und Ausweisregister

In den Pass- und Ausweisregistern werden über jeden Bürger wichtige Daten zu seiner Person gespeichert. Dies sind unter anderem sein Name, ggf. eine Anschrift und vor allem auch dessen Passfoto. Diese Daten sind aktuell, vollständig und wegen biometrischer Angaben für die Identifikation besonders geeignet. Nicht verwunderlich ist es daher, dass andere Ämter häufig und gerne auf diese Daten zugreifen und in der Stadtverwaltung vielfach Direktzugriffe von Sachbearbeitern auf beispielsweise das Melderegister bestehen.

Diesen Begehrlichkeiten stellen das Melde-, Pass- und Personalausweisgesetz klare Regeln entgegen. Hier ist klar geregelt, unter welchen Voraussetzungen andere Fachämter der Landeshauptstadt Stuttgart Auskünfte aus dem Passregister oder dem Ausweisregister einholen können. Die ersuchende Behörde trägt die Verantwortung dafür, dass diese Voraussetzungen auch erfüllt sind.

Das Amt für öffentliche Ordnung muss ein Auskunftsersuchen nur dahingehend abschätzen, ob die Anfrage nicht offensichtlich grober Unfug ist und von einem durch die Behördenleitung besonders ermächtigten Bediensteten gestellt wurde.

Aus Sicht von AK/DSB ist die Auskunftserteilung ohne Ermächtigung nicht zulässig.

WAS IST ZU TUN?

In den Fachämtern muss geprüft werden, ob eine entsprechende Ermächtigung für die betroffenen Mitarbeiter bereits erstellt wurde. Falls nicht ist dies unverzüglich nachzuholen. Zudem sollte man in den Fachämtern vor jeder Abfrage aus den Pass- und Ausweisregistern prüfen, ob die gesetzlichen Erfordernisse gegeben sind.

3.10 Digitalisierung von Wahlscheinanträgen

Erstmalig wurden für die Bundestagswahlen 2014 im Statistischen Amt die Wahlscheine vor der weiteren Bearbeitung digitalisiert. Zur Einordnung sei erwähnt, dass je nach Wahl deutlich über 90.000 Anträge beim Statistischen Amt und den Bürgerbüros eingehen, die alle rechtzeitig zur Wahl zu bearbeiten sind. Bisher waren die Wahlscheine stets nach der Bearbeitung in Ordner einsortiert worden, in denen die Dokumente bei Rückfragen mühsam herausgesucht werden mussten. Das war zeitaufwändig, erforderte viele Räume und Regalflächen sowie erheblichen logistischen Aufwand. Für den Bürger bedeutete es zumeist lange Wartezeiten, bevor ihm seine Fragen beantwortet werden konnten.

Wertvolle Arbeitszeit, die bisher für aufwändiges Suchen nach dem Originalantrag verbraucht wurde, konnte mit Hilfe der Entscheidung gewonnen werden, die Wahlscheinanträge sogleich nach dem Eingang zu digitalisieren. Neben einem geeigneten Scanner war eine Software zu beschaffen, welche die Barcodes auf den Wahlunterlagen erkennt, die Dateinamen um die eindeutige Wählernummer mit dem Wahlkreis ergänzt und in ein gesichertes Verzeichnis ablegt. Bei Bürgernachfragen konnten die Dokumente bereits während des Gesprächs eingesehen und die Anfrage sofort bearbeitet werden. Soweit die grobe Beschreibung des Verfahrens.

Wir waren bereits früh im Umsetzungsprozess beteiligt worden. So konnten wir rechtzeitig auf die Gefahr einer doppelten Datenhaltung hinweisen und dafür sorgen, dass nicht mehr benötigte Papierunterlagen nach dem Scannen des Originals datenschutzgerecht vernichtet wurden. Kein Wahlschein, keine Bürgerstimme darf verloren gehen; nur die erforderlichen Daten durften gespeichert werden; die gesetzlichen Löschfristen waren einzuhalten. Gemeinsam mit den Verant-

wortlichen haben wir die notwendigen Sicherungsmaßnahmen in den Prozessablauf integriert.

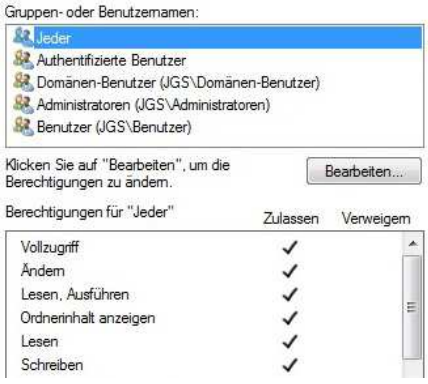
WAS IST ZU TUN?

Die Übertragung eines Schriftstücks in ein digitales Dokument zieht stets die Notwendigkeit nach sich, das Original nach erfolgreicher Übertragung zu vernichten. Die Datei ist ebenso gesichert zu behandeln wie das Original. Mittels geeigneter technisch-organisatorischer Maßnahmen ist sicherzustellen, dass keine weiteren Kopien angefertigt und unkontrolliert gespeichert werden können. Vorteile für den Bürger und die einfachere Vorgangsbearbeitung auf der einen Seite erzwingen verantwortungsbewusstes und verantwortungsvolles Handeln, damit das Vertrauen des Bürgers nicht verloren geht.

3.11 Vertrauliche Personal- und Schülerdaten für jederman zugänglich

Auf dem Windows-Server einer Stuttgarter Schule wurden Verzeichnisse mit teilweise vertraulichen Personal- und Schülerdaten für das gesamte städtische Netzwerk freigegeben. Darin befanden sich einige dienstliche Beurteilungen von Lehrern und umfangreiche Zeugnislisten der Schüler.

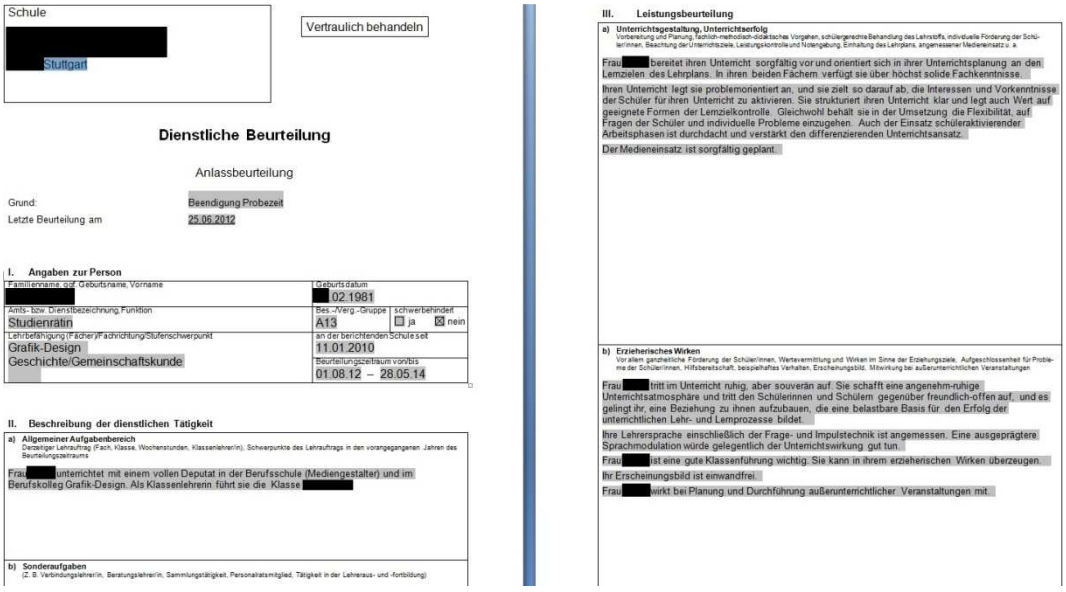
Der Server war nicht in die übliche hierarchische Domänenstruktur des städtischen Netzwerks integriert, daher wirkten die Zugangsbeschränkungen nicht. Bei der Inbetriebnahme wurde offensichtlich mangels Kenntnis des Dienstleisters oder zur Vereinfachung kurzerhand eine Vertrauensstellung mit der Funktion "Jeder hat alle Rechte" eingerichtet.



Durch die noch nicht stadtweit vorhandene Netzwerkzugangskontrolle (siehe auch Abschnitt 5.8) hätte diese Konfigurationslücke auch durch Dritte ausgenutzt

werden können. Dafür hätte der Zugang zu einer beliebigen Netzwerkdose genügt, wie sie beispielsweise auf öffentlichen Fluren oder in Kopiererräumen der Stadtverwaltung anzutreffen sind.

Auf unseren Hinweis hin konnte das Schulverwaltungsamt die viel zu großzügig erteilten Zugriffsberechtigungen auf den tatsächlich benötigten Nutzerkreis einschränken.



Schule
[redacted]
Stuttgart

Vertraulich behandeln

Dienstliche Beurteilung

Anlassbeurteilung

Grund: Beendigung Probezeit
Letzte Beurteilung am: 25.06.2012

I. Angaben zur Person

Familienname, ggf. Geburtsname, Vorname	Geburtsdatum
[redacted]	[redacted].02.1981
Amts- bzw. Dienstbezeichnung, Funktion: Studienrätin	Bes.-/Verg.-Gruppe: A13 / schwerbehindert: ☐ ja ☒ nein
Lehrbefähigung (Fächer)/Fachrichtung/Stufenschwerpunkt: Grafik-Design, Geschichte/Gemeinschaftskunde	an der berichtenden Schule seit: 11.01.2010
	Beurteilungszeitraum von/bis: 01.08.12 – 28.05.14

II. Beschreibung der dienstlichen Tätigkeit

a) Allgemeiner Aufgabenbereich
Derzeitiger Lehrauftrag (Fach, Klasse, Wochenstunden, Klassenlehrer(in). Schwerpunkte des Lehrauftrags in den vorangegangenen Jahren des Beurteilungszeitraums

Frau [redacted] unterrichtet mit einem vollen Deputat in der Berufsschule (Mediengestalter) und im Berufskolleg Grafik-Design. Als Klassenlehrerin führt sie die Klasse [redacted]

b) Sonderaufgaben
(z. B. Verbindungslehrer/in, Beratungslehrer/in, Sammlungstätigkeit, Personalratsmitglied, Tätigkeit in der Lehreraus- und -fortbildung)

III. Leistungsbeurteilung

a) Unterrichtsgestaltung, Unterrichtserfolg
Vorbereitung und Planung, fachlich-methodisch-didaktisches Vorgehen, schülergerechte Behandlung des Lehrstoffs, individuelle Förderung der Schülerinnen, Beachtung der Unterrichtsziele, Leistungskontrolle und Notengebung, Einhaltung des Lehrplans, angemessener Medieneinsatz u. a.

Frau [redacted] bereitet ihren Unterricht sorgfältig vor und orientiert sich in ihrer Unterrichtsplanung an den Lernzielen des Lehrplans. In ihren beiden Fächern verfügt sie über höchst solide Fachkenntnisse.

Ihren Unterricht legt sie problemorientiert an, und sie zielt so darauf ab, die Interessen und Vorkenntnisse der Schüler für ihren Unterricht zu aktivieren. Sie strukturiert ihren Unterricht klar und legt auch Wert auf geeignete Formen der Lernzielkontrolle. Gleichwohl behält sie in der Umsetzung die Flexibilität, auf Fragen der Schüler und individuelle Probleme einzugehen. Auch der Einsatz schüleraktivierender Arbeitsphasen ist durchdacht und verstärkt den differenzierenden Unterrichtsansatz.

Der Medieneinsatz ist sorgfältig geplant.

b) Erzieherisches Wirken
Vor allem ganzheitliche Förderung der Schülerinnen, Wertevermittlung und Wirken im Sinne der Erziehungsziele, Aufgeschlossenheit für Probleme der Schülerinnen, Hilfsbereitschaft, beispielhaftes Verhalten, Erscheinungsbild, Mitwirkung bei außerunterrichtlichen Veranstaltungen

Frau [redacted] tritt im Unterricht ruhig, aber souverän auf. Sie schafft eine angenehm-ruhige Unterrichtsatmosphäre und tritt den Schülerinnen und Schülern gegenüber freundlich-offen auf, und es gelingt ihr, eine Beziehung zu ihnen aufzubauen, die eine belastbare Basis für den Erfolg der unterrichtlichen Lehr- und Lernprozesse bildet.

Ihre Lehrersprache einschließlich der Frage- und Impulstechnik ist angemessen. Eine ausgeprägtere Sprachmodulation würde gelegentlich der Unterrichtswirkung gut tun.

Frau [redacted] ist eine gute Klassenführung wichtig. Sie kann in ihrem erzieherischen Wirken überzeugen.

Ihr Erscheinungsbild ist einwandfrei.

Frau [redacted] wirkt bei Planung und Durchführung außerunterrichtlicher Veranstaltungen mit.

Jahreszeugnis
2. Ausbildungsjahr
Beruf: Buchbinder
Klasse: [redacted]
Klassenlehrer: [redacted]

				Zeugnisnoten								Eingabenoten								
			Fach	Rel	D	Gk	Wi	T	TM	TP	∅	Rel	D	Gk	Wi	TM	T1	T2	T4	TP	T
			Lk									Hp	Hl	De	De	Ci	Ci	Ci	Si/Ki		
Nr.	Nachname	Vorname	Gew.f.														5	7	3		15
1	[redacted]			t	3	3	4	5	5	4	4,0	t	3	3	4	5	5,3	4,3	4,4	4,0	4,6
2				t	1	1	2	1	1	2	1,3	t	1	1	2	1	1,4	1,4	1,0	2,0	1,3
3				nt	3	3	3	3	4	3	3,1	nt	3	3	3	4	3,8	2,9	2,0	3,0	3,0
4				nt	3	2	3	2	3	2	2,5	nt	3	2	3	3	2,8	2,1	2,9	2,0	2,4
5				t	2	1	2	2	3	3	2,1	t	2	1	2	3	2,3	2,2	1,5	3,0	2,0
6				nt	3	3	3	3	4	2	3,0	nt	3	3	3	4	4,3	2,7	2,4	2,0	3,1
7				nt	6	5	6	5	6	3	5,1	nt	6	5	6	6	6,0	3,8	6,0	3,0	4,9
8				t	3	4	4	4	5	3	3,8	t	3	4	4	5	4,9	2,9	2,9	3,0	3,5
9				t	3	2	3	3	3	2	2,6	t	3	2	3	3	3,7	2,8	3,0	2,0	3,1
10				nt	2	3	3	3	4	3	3,0	nt	2	3	3	4	3,7	2,8		3,0	2,5
11				nt	2	2	4	2	2	3	2,5	nt	2	2	4	2	2,1	1,9		3,0	1,5
12				nt	1	1	2	1	2	2	1,5	nt	1	1	2	2	2,3			2,0	0,7
13				t	3	2	2	2	2	2	2,1	t	3	2	2	2	2,6	1,8		2,0	1,7
14				t	3	3	2	2	3	3	2,6	t	3	3	2	3	3,6	2,5		3,0	2,3
15				t	3	3	4	3	5	3	3,5	t	3	3	4	5	4,4	3,5		3,0	3,1
16				nt	2	2	3	3	3	3	2,6	nt	2	2	3	3	4,1	3,1		3,0	2,8
17				t	3	4	4	3	5	3	3,6	t	3	4	4	5	5,0	3,8		3,0	3,4
18				nt	4	4	4	3	5	4	4,0	nt	4	4	4	5	3,3	3,9		4,0	2,9

WAS IST ZU TUN?

Es muss regelmäßig geprüft werden, ob Administratoren oder externe Dienstleister Freigaben auf Systemen eingerichtet und diese auf den benötigten Nutzerkreis beschränkt haben. Nur dann kann eine eventuelle Fehlkonfiguration zeitnah behoben werden.

In künftigen Ausschreibungen muss darauf geachtet werden, dass die anzuschaffenden Geräte in der vorhandenen Infrastruktur ordnungsgemäß verwaltet werden können. Zur Abnahme ist es erforderlich, Systeme auf Schwachstellen zu untersuchen und eventuell entdeckte Fehlkonfigurationen vom Auftragnehmer kostenneutral vor Übernahme in den Regelbetrieb beheben zu lassen. Um die Administration zu vereinheitlichen und Fehlern bei manuellen Konfigurationsänderungen vorzubeugen, ist eine zentrale Verwaltung der Server anzustreben.

3.12 Entbindung von der Schweigepflicht

Vom Sozialamt wurden wir um eine datenschutzrechtliche Einschätzung zum Thema Entbindung von der Schweigepflicht gebeten.

Ein freier Träger wollte Heimbewohner beim Abschluss des Heimvertrags unterschreiben lassen, dass er Auskunft über den Betroffenen beim Sozialamt erhält. Dazu wollte er im Heimvertrag folgende Formulierung aufnehmen:

„Im Falle eines Sozialhilfebezugs: Ich entbinde das Sozialamt gegenüber dem Träger der Einrichtung von seiner Schweigepflicht. Ich ermächtige das Sozialamt, Kopien der jeweiligen Bescheide an den Träger der Einrichtung weiterzugeben."

Aus unserer Sicht ist das Vorgehen aus folgenden Gründen nicht zulässig:

Daten sind grundsätzlich beim Betroffenen zu erheben. Die rechtlichen Voraussetzungen zur Erhebung der Daten an anderer Stelle sind in diesem Fall nicht gegeben. Weder macht die zu erfüllende Verwaltungsaufgabe die Erhebung bei anderen Stellen erforderlich noch erfordert die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand.

Davon abgesehen war die Form der geplanten Einwilligungserklärung untauglich. Im Formular wurden sogar noch weitere Einverständniserklärungen abgefragt. Beispielsweise, ob der Betroffene damit einverstanden ist, dass Fotos von ihm

zur Wunddokumentation erstellt oder ob in der Hauszeitung Beiträge veröffentlicht werden dürfen, in denen der Betroffene erwähnt wird.

Erstaunlicherweise wurde dem Betroffenen für die letzten zwei Punkte ein Entscheidungsrecht eingeräumt, -das heißt er konnte wählen, ob er damit einverstanden ist oder nicht, wohingegen keine Wahlmöglichkeit für die Schweigepflichtentbindung gegeben war.

Der Punkt zur Schweigepflichtentbindung hätte wesentlich deutlicher hervorgehoben werden müssen.

Zudem muss konkret beschrieben werden, für welche Daten die Schweigepflichtentbindung gilt. Die Beschreibung "Kopien der jeweiligen Bescheide" ist zu allgemein.

Wirksam kann nur eingewilligt werden, wenn der Betroffene versteht, in was er einwilligt und die Folgen abschätzen kann, die durch die Einwilligung entstehen. Das heißt, dass beispielsweise demente Menschen häufig nicht wirksam einwilligen können. Der Vertrag kann nur wirksam unterschrieben werden, wenn entweder der Betroffene die Voraussetzungen erfüllt, die für eine wirksame Einwilligungserklärung notwendig sind oder er einen Betreuer hat, den man nach den erforderlichen Informationen fragen kann, wenn dieser entsprechend berechtigt ist. Wenn das alles nicht zutrifft und der Betroffene nicht wirksam einwilligen kann, dann hilft dem Träger eine Unterschrift auf dem Formular nichts.

Letztlich muss bei der Unterschrift der Einwilligung die Freiwilligkeit gegeben sein. Die Voraussetzungen der Freiwilligkeit bezweifeln wir allerdings ebenfalls. Wie auch das Sozialamt halten wir es für wahrscheinlich, dass Betroffene im Zuge der Heimaufnahme fast alles unterschreiben, um einen der begehrten Heimplätze zu erhalten.

WAS IST ZU TUN?

Einwilligungserklärungen sind auf folgende Punkte kritisch zu durchleuchten:

- **Ist die Einwilligung schriftlich dokumentiert?**
- **Ist deren Zweck hinreichend genau beschrieben?**
- **Sind die Daten ausnahmslos zur Aufgabenerfüllung erforderlich?**
- **Sind die Folgen der Unterschrift für den Betroffenen abschätzbar?**
- **Ist deutlich hervorgehoben, für was der Betroffene die Einwilligungserklärung unterschreibt?**

- **Gibt es einen Hinweis auf die Möglichkeit zum Widerspruch und werden die Folgen im Falle des Widerspruchs dargelegt?**

3.13 Software Prosoz Open

Seit November 2013 begleiteten wir die Einführung eines webbasierten Fachverfahrens für die sozialen Dienste im Jugendamt.

Die Software soll die Fachkräfte der Beratungszentren Jugend und Familie in ihrer prozessorientierten Einzelfallarbeit zur Wahrnehmung der Aufgaben nach dem Achten Buch Sozialgesetzbuch, also in der Diagnostik zur Gefährdungseinschätzung von Kindeswohlgefährdungen unterstützen. Ein heikles Thema mit besonders sensiblen Daten.

Die Herausforderung bestand darin, verschiedene Anforderungen an die geplanten Auswertungen zum notwendigen Ausgleich zu bringen. Auf der einen Seite sind personenbezogene Auswertungen notwendig, die sich auf einen eher kurzen Zeitraum beziehen. Auf der anderen Seite wird ein Berichtswesen benötigt, für das Daten über eine lange Zeitspanne anonymisiert auswertbar sein müssen.

Um in allen Fällen datenschutzkonform zu handeln, hat der Hersteller zusammen mit dem Jugendamt große Anstrengungen unternommen und das Produkt wurde im Sinne des Datenschutzes erheblich weiterentwickelt. Im Ergebnis gibt es nun zwei große Datenbestände, die jeweils in separaten Datenbanken gehalten werden. Über einen Datenbestand werden die kurzfristigen personenbezogenen Auswertungen durchgeführt, in dem die nicht mehr erforderlichen personenbezogenen Daten gelöscht werden. Im zweiten Datenbestand werden die Daten anonymisiert, so dass langfristige Statistiken möglich sind.

Bei diesem Projekt ist besonders das große Engagement der Beteiligten des Jugendamts hervorzuheben, mit dem sie die Einführung des Verfahrens begleiteten. Der Datenschutz ist bei diesem Projekt immer auf ein offenes Ohr gestoßen, obwohl unsere Empfehlungen sicher mit einem erhöhten Aufwand verbunden waren. Wir sind beispielsweise dem Wunsch des Herstellers nicht nachgekommen, ihm den bestehenden produktiven Adressdatenbestand zu Testzwecken zu überlassen.

WAS IST ZU TUN?

An der einen oder anderen Stelle sind noch Kleinigkeiten innerhalb des Projekts offen, die wir weiterhin im Auge behalten werden. Aber vor allem gilt ein besonderer Dank an alle Beteiligten im Jugendamt. Wir freuen uns auf die weitere Zusammenarbeit.

3.14 Unsichere Kommunikation mit Bürgern

Das Baurechtsamt fordert Bürger auf, Bauakten zur Einsicht zwingend vorab per E-Mail anzufordern, da diese teilweise durch ausgefallene Aktenpaternoster in das Lager eines externen Dienstleisters verlegt werden mussten. Wir sehen die ungesicherte und unverschlüsselte Übertragung von personenbezogenen Daten per E-Mail als unzulässig an.

Um herauszufinden, ob die betreffende Akte im Amt vorrätig ist oder vorab angefordert werden muss, soll der Bürger eine über 300 Seiten umfassende Liste betroffener Straßenabschnitte in Stuttgart herunterladen und durchsuchen – was ebenfalls wenig bürgerfreundlich wirkt.


Alle ausgelagerten Daten sind in folgendem Dokument gelistet. Bitte überprüfen Sie, ob Ihre Bauunterlagen hier aufgeführt sind:

Ausgelagerte Akten (PDF - 4,8 MB)

Auf unseren entsprechenden Hinweis nimmt das Amt immerhin den Hinweis auf den unsicheren Übertragungsweg in sein Internetangebot auf und bietet nun doch einen alternativen Weg der Aktenanforderung über Telefax und per Briefpost an.

Es gilt ein weiteres grundsätzliches Problem zu beachten. Schon der Transport von Akten durch einen Dienstleister ist ohne Vertrag zur Auftragsdatenverarbeitung nicht zulässig. Der gesetzlich vorgeschriebene Vertrag nach § 7 LDSG liegt uns bis heute nicht vor.

Unsere Vorschläge zur datenschutzkonformen Übertragung mittels abgesichertem Kontaktformular und Datenbankabgleich wurden von der internen IT-Abteilung des Baurechtsamts bisher nicht realisiert. Unsere Empfehlung hätte eine verschlüsselte Kommunikation sichergestellt und die große Adressliste obsolet gemacht.

Verfügbarkeit von ausgelagerten Akten aus dem Baurechtsamt

Weil einige Aktenpaternoster des Baurechtsamts defekt sind, wurden Akten teilweise zu einer Fremdfirma ausgelagert. Diese Akten sind künftig nicht mehr im Bürgerservice Bauen in der Eberhardstraße sofort greifbar. Außerdem ergeben sich einige organisatorische Änderungen im Baurechtsamt. Wir haben hier die wichtigsten Änderungen für Sie zusammengefasst:

Wie kann ich Bauunterlagen einsehen?

Die Bauakten können künftig **nur nach vorheriger schriftlicher Anforderung** per E-Mail eingesehen werden. Bitte schreiben Sie an

- BSBauen@stuttgart.de

Alternativ können Sie das folgende Formular ausdrucken und per Fax an den Bürgerservice Bauen schicken:

- Antragsformular für die Bereitstellung von Bauakten/ Statik (PDF - 72 KB)
- Fax-Nr: 0711/216-60101

Wir weisen darauf hin, dass die eingetragenen Daten im Antragsformular derzeit ungeschützt sind. Ein verschlüsseltes Antragsformular steht demnächst zur Verfügung.

Foto: covision.de

WAS IST ZU TUN?

Mit der Eröffnung einer Gefahrenquelle durch die Aufforderung, per E-Mail zu kommunizieren, müssen die Bürger deutlich auf den ungesicherten Kommunikationsweg hingewiesen werden.

3.15 Androhung einer Abmahnung unserer Internetseite

Im Mai 2014 erreichte die Landeshauptstadt Stuttgart ein interessantes Schreiben. Es war die Androhung einer Abmahnung der Wettbewerbszentrale wegen dem angeblich lückenhaften Impressum unserer Internetseite (siehe unten).

Die erste Frage, die sich einem sofort aufdrängt, ist natürlich, warum wir als Kommune von der Wettbewerbszentrale angeschrieben werden. Die Wettbewerbszentrale ist die größte und einflussreichste bundesweit und grenzüberschreitend tätige Selbstkontrollinstitution zur Durchsetzung des Rechts gegen den unlauteren Wettbewerb. Grundlage ihrer Tätigkeit ist die Verbandsklagebefugnis gemäß § 8 Abs. 3 Nr. 2 Gesetz gegen den unlauteren Wettbewerb und § 33 Abs. 2 Gesetz gegen Wettbewerbsbeschränkungen. Geht es bei diesem Schreiben mit rechten Dingen zu, mit wem sollen wir denn im Wettbewerb stehen? Falls nein, könnte man das Schreiben beruhigt zur Seite legen bzw. die Androhung mit Gelassenheit zurückweisen. Eine kurze Recherche ergab dann leider das ungute Ergebnis, dass wir mit unserem Internetangebot weltweit mit allen anderen Webseitenbetreibern im Wettbewerb stehen. Hier geht es nicht um den Kernbereich kommunaler Tätigkeit, sondern wir sind im Internet gleichbe-

rechtigter Anbieter mit allen daraus folgenden Pflichten. Damit war dieser einfache Ausweg verbaut und wir mussten uns inhaltlich mit dem Schreiben auseinandersetzen.

Wir verwenden auf unseren Internetseiten unter www.stuttgart.de das im Gegensatz zu Google Analytics datenschutzfreundlichere Analysetool Piwik. Im Vergleich zu dem bekannteren Google Analytics hat Piwik den Vorteil der Speicherung von sensiblen Logdaten auf dem eigenen Server der Landeshauptstadt Stuttgart. Dagegen ist bei Google Analytics eine Datenübertragung an Google als Dritten zwingend notwendig. Alles richtig gemacht oder doch nicht?

Nach Ansicht der Wettbewerbszentrale klären wir die Nutzer über die Verwendung des Analysetools Piwik nicht hinreichend auf. Klingt zunächst einfach. Etwas komplizierter wird es, weil es nicht eine Seite www.stuttgart.de gibt, sondern sich hinter der Einstiegsseite zahlreiche weitere Unterseiten befinden. Richtig kompliziert wird der Vorgang aber erst dadurch, dass im Laufe der Jahre viele Seiten mit www.stuttgart.de verlinkt wurden, z. B.

- stuttgart.de/baeder
- stuttgart.de/komm-zu-uns
- stuttgart.de/stadtbibliothek
- wolfgang-schuster.info
- fritz-kuhn-ins-rathaus.de
- planetarium-stuttgart.de
- stadtmuseum-stuttgart.de
- bewegungsnetz-stuttgart.de
- stuttgarter-stadtteile.de
- kids-initiative-stuttgart.de
- see-stuttgart.de
- sia-projekt.de
- buergerhaushalt-stuttgart.de
- leben-und-wohnen.de
- feuerwehr-stuttgart.de

Diese verlinkten Seiten pflegen ihren Datenschutzhinweis bisher selbst. Dadurch wird natürlich keine Einheitlichkeit erreicht und der Nutzer ist einer Vielzahl an Hinweisen abweichenden Inhalts ausgesetzt. Künftig soll nur noch eine Datenschutzerklärung in allen Internetangeboten unter der Domain "stuttgart.de" verwendet werden. Dies wird erreicht, indem mit einem Link auf das Impressum der

Einstiegseite verwiesen wird, wodurch automatisch immer dieses Impressum angezeigt wird.

Nachdem in herausragender Zusammenarbeit mit der Abteilung Kommunikation (L/OB-K) und der Abteilung eGovernment beim Haupt- und Personalamt (10-6) der Datenschutzhinweis zu Piwik in kürzester Zeit angepasst und durch die Fachverwaltung auch mit ihren Seiten verlinkt wurde, konnte Entwarnung gegeben werden. Die drohende Abmahnung der Wettbewerbszentrale war abgewehrt und ein weiteres Schreiben hat uns von dort nicht mehr erreicht.

WAS IST ZU TUN?

Alle neu hinzukommenden Internetseiten müssen mit dem Datenschutzhinweis unter www.stuttgart.de verlinkt werden. Beim Einsatz abweichender Analysetools zu Piwik, also z. B. Google Analytics, muss ein zusätzlicher Hinweis an den Besucher der Seite erfolgen.

Wettbewerbszentrale

Landeshauptstadt Stuttgart
70151 Stuttgart

F 7 0118/14
Landeshauptstadt Stuttgart

Assin. [redacted]
Telefon 06172-[redacted]
29. April 2014

Sehr geehrte Damen und Herren,

die Wettbewerbszentrale ist eine gemeinnützige Selbstkontrollinstitution der deutschen Wirtschaft. Zur Förderung eines lauteren Wettbewerbs hat sie unter anderem die Aufgabe, wettbewerbswidrige Rechtsverletzungen im gewerblichen Bereich auszuräumen. Als Verband zur Förderung gewerblicher Interessen im Sinne des Gesetzes gegen unlauteren Wettbewerb ist die Wettbewerbszentrale nach ständiger Rechtsprechung des Bundesgerichtshofs berechtigt, bei Rechtsverletzungen Abmahnungen auszusprechen und Klage zu erheben. Informationen zur Wettbewerbszentrale erhalten Sie unter www.wettbewerbszentrale.de.

Wir haben eine Beschwerde darüber erhalten, dass Sie auf der von Ihnen betrieben Internetseite www.stuttgart.de das Analyse-Tool Piwik nutzen, ohne den Nutzer der Internetseiten hierauf klar und zuverlässig wahrnehmbar hinzuweisen.

Die Nutzung des Analysewerkzeuges Piwik, mit dem das Nutzungsverhalten auf Ihrer Internetseite analysiert wird, ergibt sich aus dem Quellcode der oben genannten Internetseite (siehe hierzu beigefügten Screenshot). Über die Nutzung dieses Tracking-Tools wird der Nutzer Ihrer Internetseite an keiner Stelle informiert. Zwar halten Sie eine Datenschutzerklärung vor, doch auch hier finden sich keine Informationen zu dem genutzten Tool.

§ 13 Abs. 1, 2 TMG verlangt, dass bei personenbezogenen Daten der Nutzer über Art, Umfang und Zweck der Erhebung und Verwendung unterrichtet und eine Einwilligung in die Nutzung erteilt wird. Daraus ergibt sich die Verpflichtung, über die Datenverarbeitung durch Piwik aufzuklären und die Einwilligung des jeweiligen Nutzers einzuholen.

Zentrale zur Bekämpfung unlauteren Wettbewerbs Frankfurt am Main e.V.
Landgrafenstraße 24 B
61348 Bad Homburg v. d. H.
Postfach 2555
61295 Bad Homburg v. d. H.
Telefon: 06172-12150
Telefax: 06172-84422
mail@wettbewerbszentrale.de
www.wettbewerbszentrale.de
Postbank Frankfurt
IBAN: DE 79500100600059419[illegible]
BIC: PBNKDEFF
AG Frankfurt am Main 75VR 64[illegible]
Steuernummer 005 250 99268

Piwik kann jedoch auch so eingesetzt werden, dass nur pseudonymisierte Daten erhoben werden. Doch selbst wenn das Trackingprogramm nur pseudonyme Nutzungsprofile der Webseitenbesucher erstellt, ist der Webseitenbetreiber verpflichtet den Nutzer zu Beginn des Nutzungsumfanges und später jederzeit abrufbar auf die Widerspruchsmöglichkeit nach § 15 Abs. 3, 13 Abs. 1 TMG hinzuweisen. Dieser Hinweises muss klar, zuverlässig wahrnehmbar und zu Beginn des Nutzungsvorgangs erteilt werden (siehe hierzu: LG Frankfurt, Urteil vom 18.02.2014, Az. 3-10 O 86/12).

Das ist auf Ihrer Internetseite gerade nicht der Fall. An keiner Stelle weisen Sie den Nutzer auf sein Widerspruchsrecht hin.

Ein Verstoß gegen die Vorschriften des Telemediengesetzes (TMG) stellt zugleich einen Wettbewerbsverstoß nach §§ 3, 4 Nr. 11 UWG dar, da die Vorschriften geeignet sind, das Marktverhalten zu regeln (siehe hierzu: Urteil des OLG Hamburg vom 27.06.2013, Az. 3 U 26/12; LG Frankfurt, Urteil vom 18.02.2014, Az. 3-10 O 86/12).

Wir haben zunächst davon abgesehen, eine kostenpflichtige Abmahnung auszusprechen. Wir geben Ihnen Gelegenheit zur Stellungnahme und zur Ausräumung des Wettbewerbsverstoßes bis zum

13. Mai 2014.

Mit freundlichen Grüßen
DIE GESCHÄFTSFÜHRUNG
im Auftrag [redacted]

[redacted]
Assessorin

4 Fachübergreifende Projekte bei der Landeshauptstadt Stuttgart

4.1 Einführung eines Dokumentenmanagementsystems

Wir haben das Pilotprojekt eines Dokumentenmanagementsystems (DMS) der Firma PDV-Systeme GmbH aus Erfurt befürwortet. Der Einsatz eines DMS kann eine datenschutzkonforme Verarbeitung von personenbezogenen Informationen unterstützen, insbesondere wenn die Daten nicht in Fachverfahren gespeichert werden, sondern in Text- oder Tabellendateien auf vorher nicht festlegbaren Laufwerken.

Bei der eingesetzten Dokumentenmanagementsoftware "PDV VIS 5.1" halten wir es aus Datenschutzsicht für sehr ungünstig, dass zum vollständigen Betrieb des Systems zusätzlich die Webanwendung gepflegt werden muss. Bestimmte Funktionen wie Löschen der Papierkörbe, die Aussonderung, die Rücknahme von Rechten in PDV sind nur in der Webanwendung verfügbar. Aus unserer Sicht führt dies dazu, dass die momentan eingesetzte Version für einen stadtweiten Einsatz nicht geeignet ist.

Die Aufbewahrungsfrist einer Akte wird über das zugehörige Aktenzeichen gesteuert. Ein der Akte untergeordneter Vorgang "erbt" die Aufbewahrungsfrist der Akte. Dem Vorgang kann durch den Standardnutzer keine andere Aufbewahrungsfrist zugeordnet werden. Die Vergabe einer anderen Aufbewahrungsfrist für ein einzelnes Objekt ist dem Administrator vorbehalten. Wenn jedoch Dokumente mit personenbezogenen Daten im DMS abgelegt werden sollen, dann ist auf die Einhaltung der spezifischen Aufbewahrungsfristen zu achten. Die Vergabe der Aufgabenfristen führt dazu, dass die Nutzer in ihrer Gestaltungsmöglichkeit der Aktenführung im DMS eingeschränkt werden. Innerhalb einer Akte dürfen dann nur Vorgänge mit einheitlicher Aufbewahrungsfrist abgelegt werden. Damit stellt sich die Frage, ob letztendlich mehrere gleichlautende Aktenzeichen angelegt werden müssen, für die verschiedene Aufbewahrungsfristen festgelegt werden.

Im Stadtarchiv hat der Aussonderungstest stattgefunden. Dabei haben sich weitere datenschutzrechtliche Aspekte ergeben, die noch der Klärung bedürfen.

Die Nutzung der Adressen wurde im Piloten nicht organisatorisch geregelt. Aus unserer Sicht ist deshalb eine datenschutzkonforme Nutzung der Adressen problematisch und sollte bis zur Klärung technisch unterbunden werden.

Während des Pilotbetriebs hat die Projektlenkung administrative Aufgaben übernommen. Das ist nur während der Pilotphase aus sicherheitstechnischer Sicht tolerabel. Wenn nach der Pilotphase der Produktivbetrieb beginnt, kann nur eine mit ausreichenden Personalressourcen bestückte Administration für die Verfügbarkeit des Systems sorgen. Zu klären sind des Weiteren die Zuständigkeiten der Fachadministratoren.

Einen großen Mehrwert beim Einsatz eines DMS stellt die Volltextsuche über den kompletten Bestand der Akten und Vorgänge dar. Der Bestand ist natürlich nur dann vollständig, wenn auch die papiergebundenen Unterlagen in einem durchsuchbaren Format zum Vorgang eingescannt wurden. Die Projektleitung hat deshalb angeregt, dass bei auslaufenden Leasingverträgen die Funktion „Texterkennung“ mit in die Verträge aufgenommen wird. Aus datenschutzrechtlicher Sicht ist es hingegen empfehlenswert, das Einscannen der Unterlagen durch den zentralen Posteingang durchführen zu lassen. Wenn die Unterlagen dezentral gescannt werden, besteht die Gefahr, dass personenbezogene Daten gleich mehrfach abgelegt werden (elektronisch und papiergebunden) und die erforderliche Löschung der Daten dadurch noch schleppender – weil unübersichtlicher – realisiert wird. Hinzu kommt, dass solange bei der Landeshauptstadt Stuttgart keine Regelungen über eine elektronische Aktenführung getroffen wurden, die Akten nach der Aktenordnung zwingend in Papierform zu führen sind. Deshalb ist es aus datenschutzrechtlicher Sicht ohnehin problematisch, Dokumente mit personenbezogenen Informationen einzuscannen und doppelt abzulegen.

WAS IST ZU TUN?

Aus unserer Sicht ist die Einführung eines stadtweiten Dokumentenmanagementsystems sehr empfehlenswert. Die Vorteile für den Datenschutz und die IT-Sicherheit ergeben sich allerdings nur, wenn nicht nur ein technisches Produkt eingeführt wird, sondern auch die gegebenenfalls notwendigen organisatorischen Änderungen umgesetzt werden. Beispielsweise können Löschfristen zentral verwaltet werden, womit ein regelmäßiger automatischer Löschlauf möglich ist.

4.2 Single Sign-on – ein Schlüssel, viele Türen

Mit Single Sign-on (SSO) wird die einmalige Authentifizierung für mehrere Rechner und Dienste bezeichnet. Übersetzt bedeutet der Begriff "Einmalanmeldung". Wer sich am Morgen oder den Tag über an vielen Anwendungen jeweils mit Benutzerkennung und Kennwort anmelden muss, der wird eine solche Einrichtung sicher sehr rasch zu schätzen wissen. Zumal dann, wenn jede Anwendung mit separatem komplexem Kennwort gesichert wurde. Zumindest in kleinem Rahmen wollte man in einem gemeinsamen Pilotprojekt mit dem Zweckverband Kommunale Datenverarbeitung Region Stuttgart (KDRS) Single Sign-on für die städtischen SAP-Anwendungen ermöglichen. Zunächst sollte für das SAP - Competence Center Stuttgart eine Plattform bereitgestellt werden, mit dem sich die Anwender dort nur noch einmal anmelden müssen. Danach werden die Anmeldeinformationen automatisch zur nächsten Anwendung durchgeschleust. Lokale Anmeldeinformationen über Netzwerkgrenzen hinweg zu transportieren, diese auch zu verifizieren, dahinter verbarg sich mehr als kurz die Tür zur eigenen Wohnung aufzuschließen. Immerhin hatte man bis dahin keine Tür, kein Schloss, keinen Schlüssel, keinen Schlüsselbund, der Hauszugang musste noch freigeräumt werden, und wie alles zusammengehört oder eingebaut wird, das war ebenfalls unbekannt.

Praktischerweise erledigt das Betriebssystem mit dem Active Directory (Verzeichnisdienst und Benutzerverwaltung von Microsoft) nicht nur die Erstanmeldung ans System, sondern liefert auch einen Kerberos-Schlüssel mit (verteilter Authentifizierungsdienst für offene und unsichere Computernetze wie z. B. das Internet), mit dem sich der Benutzer gegenüber anderen Anwendungen authentifizieren kann. Voraussetzung dafür ist allerdings, dass die Anwendung eine Anmeldung mit Kerberos überhaupt unterstützt. Was für SAP theoretisch möglich ist, geht leider nicht bei allen anderen in der Landeshauptstadt Stuttgart genutzten Anwendungen. Eine entsprechende Portalanwendung steht für SAP auch zur Verfügung. Also alles schlüsselfertig?

Würde man alles in eigener Hand betreiben, keine Subunternehmer beschäftigen und das eigene Netzwerk nicht verlassen, käme man leichter über die Hindernisse hinweg. Nicht so in diesem speziellen Fall. Einige Fragen waren rasch zu klären, wie jene der Verbindung der beiden Netze oder wie die Oberfläche am Portal aussehen und welche Anwendungen erreicht werden sollten. Die Kernfrage, die nach dem Zugangsschlüssel, bereitete indes einiges Kopfzerbrechen.

Nun ist Kerberos seit 1993 im Internet anerkannter Standard. Die vorliegende Implementierung von SAP stützt sich auf diesen Standard. Die letzte Aktualisierung des Kerberos-Standards datiert aus dem Jahre 2012. Obwohl die Anmeldeinformationen mit Kerberos-Ticket übergeben werden, verifiziert SAP die Benutzerkennung nochmals im Active Directory. Bei diesem Zugriff sind systembedingt alle Angaben des Verzeichnisses sichtbar, obwohl nur die Daten eines Benutzers, nicht aber der gesamte Datensatz, benötigt werden. Hierzu könnte man sich überlegen, den Umfang der gelesenen Informationen zu reduzieren, indem man das Verzeichnis hierarchisch strukturiert und die Information in einer tieferen Ebene eingliedert.

Auf unser konsequentes Hinterfragen hin hat SAP nun weitere Wege aufgezeigt, wie SAP Single Sign-on auch ohne Zugriff auf fremde Datenquellen funktionieren sollte. Diese Wege sind im Moment noch in der Erprobungsphase. Über den Ausgang kann noch nichts gesagt werden.

Genug Zeit, um sich dem Thema Sicherheit der Netze im Umgang mit Single Sign-on zu befassen. Ohne dieses Verfahren werden die einzelnen Anwendungen mit je einem eigenen Zugriffscode gegen unberechtigte Benutzung abgesichert. Diese Sicherung entfällt, wenn sich der Benutzer nur noch ein Mal am System anmeldet und danach ohne weitere Anmeldung automatisch auf andere Anwendungen weitergeleitet wird. Damit wird der Schutzmechanismus für die Anwendungsdaten zu einem großen Teil ausgehebelt. Deswegen empfiehlt die Konferenz der deutschen Datenschutzbeauftragten in ihrer Orientierungshilfe zum Thema Single Sign-on ausdrücklich, eine Zwei-Faktor-Authentifizierung einzuführen. Dabei wird dem Benutzer ein weiteres Identifikationsmerkmal an die Hand gegeben, mit dem er sich identifizieren muss. Beispielsweise nutzt er eine persönliche Smartcard sowie eine geheime PIN, um sich am System anzumelden.

Eng verbunden mit dem Begriff Authentifizierung ist das Thema Identitätsmanagement. In diesem Projekt wurde vor geraumer Zeit eine Lösung erarbeitet und bereitgestellt. Leider wurden die Ergebnisse dieses Projekts bisher nie umgesetzt. Das städtische Netzwerk wäre so um einiges besser abgesichert und Single Sign-on müsste deutlich weniger Hürden überwinden. In der bestehenden Form ohne Zwei-Faktor-Authentifizierung konnten wir nur der testweisen Einführung im Rahmen des Pilotprojekts zustimmen. Die Chance, neue Erfahrungen zu sammeln und technische Innovationen zu erproben, sollte nicht von vornherein verbaut werden.

WAS IST ZU TUN?

Manchmal braucht es etwas Risikobereitschaft, um neue Technologien zu erproben. Technische Veränderungen im Bereich der Informationstechnik entwickeln sich stürmisch. Wer die IT-Sicherheit in der Landeshauptstadt Stuttgart verantwortet, muss daher mit dieser Entwicklung Schritt halten und darf nicht einzelne Schritte auslassen, die aufeinander aufbauen und sich bedingen. Fehlt dieser Schritt, dann ist die weitere Entwicklung gehemmt und die IT-Sicherheit ruht auf tönernen Füßen. So ist ein funktionierendes Identitätsmanagement Voraussetzung für sicheres Single Sign-on.

4.3 Berechtigungsprüfung in SAP mit CheckAud

Die Arbeit der Benutzerverwaltung ist nie beendet. Neue Mitarbeiter kommen hinzu, andere verlassen uns. Veränderte oder neue Module erfordern neue Rollen, welche wiederum Benutzern zugewiesen werden müssen. Dies trifft für alle Anwendungen zu. Jetzt ist aber mit SAP ein System im Einsatz, dessen Rechteverwaltung unvergleichlich granularer aufgebaut ist und den Administratoren höchste Aufmerksamkeit abverlangt. Das Rechtegeflecht mit einem unabhängigen, objektiven Werkzeug zu überprüfen war Grund für den Einsatz des Tools CheckAud der Firma IBS Schreiber aus Hamburg. Wir erwähnten dies bereits in unserem letzten Bericht unter Ziffer 5.12.

Die Menge der durch das Tool gelieferten Ergebnisse war so groß, dass zunächst eine Struktur erarbeitet und die Treffer vorsortiert werden mussten, um überhaupt damit arbeiten zu können. In akribischer Kleinarbeit waren die Ergebnisse einzeln zu bewerten und fallbezogen darüber zu befinden, wie und an welcher Stelle nachjustiert werden musste. Die daraus entstandene Dokumentation diente anschließend den Modulbetreuern als Arbeitsgrundlage, um die notwendigen Korrekturen in das Berechtigungssystem einzuarbeiten.

Beispielsweise wurden Benutzer gefunden, bei denen eine Berechtigung zu entfernen war, weil diese inzwischen nicht mehr erforderlich ist. Auch die sehr große Anzahl von Benutzern des KDRS wird im Dialog mit dem Dienstleister zu reduzieren sein. Oder aus dem Ergebnis waren einzelne Tabellen ersichtlich, auf die ein Zugriff erforderlich ist, dies aber zu einem nicht gewollten Nebenrecht auf ein anderes Objekt führt. Um solche Nebeneffekte zu verhindern, wird es Zug um Zug notwendig sein, die Strukturen anders zuzuschneiden, damit diese weitestgehend ausgeschlossen werden können.

Mit der Durchführung einer Prüfung mit CheckAud gewinnt die Landeshauptstadt Stuttgart. Sie gewinnt Sicherheit darüber, dass

- in der SAP-Finanzverwaltung das Rechte- und Rollenkonzept nach objektiven Maßstäben überprüft wurde,
- erkannte Mängel beseitigt wurden und nicht zuletzt
- die Erweiterung der Fachkompetenz der eigenen Mitarbeiter im Umgang mit SAP und seinen Berechtigungsverfahren.

Für das Prüfen weiterer Applikationen mit CheckAud werden die Erfahrungen dieses Einsatzes auf jeden Fall mehr als wertvoll sein. Ohne die hervorragende Zusammenarbeit mit dem SAP – Competence Center wären die Prüfungsergebnisse nicht möglich gewesen. An dieser Stelle deshalb ein besonderer Dank für das Vertrauen und die Kollegialität.

WAS IST ZU TUN?

Nach der Prüfung ist vor der Prüfung. Daher ist eine erneute Prüfung des SAP-Mandanten für das Finanzwesen schon heute als erforderlich anzusehen. Einem solchen Auditing ist dvv.Personal ebenfalls zu unterziehen. Darüber hinaus empfehlen wir in vergleichbarer Form auch die Untersuchung der übrigen im Namen der Landeshauptstadt Stuttgart betriebenen Mandanten.

4.4 Hop oder Top – Online-Bewerbungsmanagement startet mit Hindernissen

Im November 2011 startete man mit der ambitionierten Vorgabe, elektronische Bewerbungen ab Herbst 2012 für die Ausbildungsstellen bei der Landeshauptstadt Stuttgart zu ermöglichen. Zu diesem Zeitpunkt gab es kein elektronisches Verfahren, man wusste nicht einmal, welches man beschaffen wollte und welche Fähigkeiten es mitbringen müsste. Im Herbst 2014 war es dann soweit. Die Auszubildenden des nächsten Jahrgangs konnten sich in einem Online-Verfahren bewerben.

Diese lange Zeitspanne bis zur Realisierung war durchaus erforderlich, denn es waren eine Vielzahl an technischen und organisatorischen Fragen zu bewältigen, bevor der erste Aspirant auf einen Ausbildungsplatz seine Bewerbung in einem elektronischen Verfahren abgeben konnte. Wo es letztendlich überall Probleme gab und was man hätte anders umsetzen können, das muss aus unserer Sicht nicht beurteilt werden.

Neben diesen Unwägbarkeiten, mit denen fast jedes Projekt in der einen oder anderen Form zu kämpfen hat, gab es dann doch einige Punkte, bei denen der Datenschützer die Stirn in Falten zog. Nachdem die vom Landesdatenschutzgesetz (LDSG) vorgeschriebene Vorabkontrolle nach § 12 LDSG unterblieben war (diese prüft, ob überhaupt oder unter welchen besonderen Sicherheitsmaßnahmen eine derartige Datenverarbeitung stattfinden darf), hätten wir vorgewarnt sein müssen. Obwohl wir bei unseren Mitwirken in der Projektarbeit stets darauf gedrängt haben, startete der Echtbetrieb auch noch ohne einen formal gültigen Eintrag in das Verfahrensverzeichnis nach § 11 LDSG. Zwei Verstöße gegen geltendes Datenschutzrecht, die leicht vermeidbar gewesen wären.

Die Verwaltung der Zugriffsberechtigungen für das Online-Bewerbermanagement ist technisch anders als gewohnt realisiert worden. Die verschiedenen Rechte an der einzelnen Bewerbung werden dynamisch je nach Stand des Bearbeitungsverfahrens erweitert oder wieder eingeschränkt. So hat die Fachabteilung nicht während der gesamten Bewerbungszeit Zugriff auf die einzelne Bewerbung, sondern nur für die Dauer der fachlichen Beurteilung. Für die Rechteverwaltung sind somit nur die Bedingungen definiert, unter denen der jeweilige Benutzer die Daten bearbeiten darf. Eine Funktion, die eingeschränkte Rechte für Kontroll- und Prüfzwecke beinhaltet, ist leider entgegen unserer Forderung zur Softwarebeschaffung nicht vorgesehen. Entweder man ist Administrator und sieht alles, oder man ist Funktionsträger innerhalb des Prozesses und sieht nur das, was man sehen soll.

Viel schwerer wiegt die Entscheidung der Verantwortlichen, die Daten länger zu speichern, als dies gesetzlich vorgesehen ist. Die Speicherdauer der Bewerberdaten wurde von der Fachabteilung aufgrund einer Beurteilung des Rechtsamts aus dem Jahre 2005 auf sechs Monate festgelegt, weil man bei eventuellen Klagen abgelehnter Bewerber noch auf die Unterlagen zurückgreifen wolle. Ein Jahr nach dem vorgenannten Schreiben wurde im neuen Allgemeinen Gleichbehandlungsgesetz für Einsprüche aus abgelehnten Bewerbungen eine Frist von zwei Monaten festgeschrieben. Wir haben auf diese Gesetzesänderung nach dem Rechtsamtsschreiben ausdrücklich hingewiesen, es wurde aber gebetsmühlenartig auf das Schreiben des Rechtsamts verwiesen. Aus Sicht des Datenschutzes dürfen Daten aber nur so lange gespeichert werden, wie sie erforderlich sind. Selbst wenn also eine Klage am letzten Tag der Frist eingereicht würde und man einen ganzen Monat für die innerbetriebliche Laufzeit hinzugibt, bis die Fachseite von einem anhängigen Verfahren Kenntnis erhält, dürften die von uns für praktikabel angesehenen drei Monate mehr als ausreichen. Man speichert also doppelt so lange aus dem einfachen Grund, weil man eine jener Akten unter den tausenden vielleicht doch noch einmal benötigen könnte. Das widerspricht geltenden Rechtsgrundsätzen und im schlimmsten Fall ist dies auch eine Missachtung der Rechte jener Menschen, die man doch so gerne in den eigenen Reihen

beschäftigen möchte. Eine Vorratsdatenspeicherung verstößt gegen das Grundrecht auf informationelle Selbstbestimmung und den verwaltungsrechtlichen Grundsatz der Verhältnismäßigkeit.

WAS IST ZU TUN?

Für elektronische Verfahren, in denen personenbezogene Daten verarbeitet werden, ist eine Vorabkontrolle nach § 12 LDSG zwingend durchzuführen. Dann kann auch der Eintrag in das Verfahrensverzeichnis nach § 11 LDSG rechtzeitig und einfach vor dem Echtbetrieb fertiggestellt werden.

5 IT-Sicherheit

5.1 Fernbetreuung und die bewegte Maus

Ursachen für nicht vom Benutzer ausgelöste Mausbewegungen gibt es viele. Beispielsweise können diese Bewegungen durch einen Schädling (Computervirus oder Ähnliches) auf dem Rechner, durch eine Fernbetreuungssitzung, durch die sogenannte Zeigerbeschleunigungsfunktion in Windows oder bei optischen Mäusen durch eine spiegelnde Oberfläche ausgeführt werden. Die Suche nach der Ursache kann aber auch zu einem unerwarteten Ergebnis führen.

Im Juli 2013 wunderte sich eine Benutzerin über eine offensichtlich nicht von ihr bewirkte Mausbewegung. Daraufhin wandte sie sich an den Benutzerservice mit der Bitte um Klärung. Nach ausführlicher Analyse des Rechners konnte ein Virenbefall oder Dergleichen ausgeschlossen werden.

Aufgrund der Protokollierung konnte auch eine Fernbetreuung zur maßgeblichen Zeit ausgeschlossen werden. Allerdings wurde festgestellt, dass zur Behebung einer vorhergehenden Störung im April 2013 beim eingesetzten Fernbetreuungswerkzeug die Option "Permission required" (Benutzerzustimmung) im Einvernehmen mit der Nutzerin abgeschaltet wurde. Zum damaligen Zeitpunkt funktionierte ihr Bildschirm nicht und dadurch konnte die Fernbetreuung nicht wie vorgegeben am PC freigegeben werden. Leider wurde nach Behebung der Störung vergessen, diese Option wieder zu aktivieren. Da bei der Deaktivierung der Benutzerzustimmung der Administrator über Fernbetreuung nur unter seiner eigenen Benutzerkennung arbeiten kann und nicht unter einer fremden, ist dieser Vorfall als geringfügig einzustufen. Er zeigt allerdings, wie Sicherheitsfunktionen ungewollt über einen längeren Zeitraum ausgehebelt werden können.

WAS IST ZU TUN?

Bei Störungen ist es akzeptabel, dass Sicherheitsfunktionen kurzzeitig deaktiviert werden. Allerdings muss darauf geachtet werden, dass diese sofort nach Störungsbehebung wieder aktiviert werden.

5.2 Mobile Geräte

Der Einsatz von dienstlichen Smartphones und Tablet-PCs ist auch bei der Landeshauptstadt Stuttgart aus der täglichen Arbeit vieler Mitarbeiter nicht mehr

wegzudenken. Ende 2014 hatte die Landeshauptstadt Stuttgart über 450 Smartphones und Tablet-PCs im Einsatz, bei denen es sich hauptsächlich um iPhones und iPads der Firma Apple handelt.

Wer die Vorteile in seinem privaten Umfeld bereits zu schätzen gelernt hat kann nachvollziehen, warum viele Mitarbeiter auf diese Weise mobil arbeiten möchten. Laut einer Statistik der Statista GmbH setzten bereits im August 2013 59,8 % aller Mobiltelefonbesitzer ein Smartphone ein. Unternehmer.de führt aus, dass 2013 über 100 Milliarden kostenpflichtige und kostenlose Apps (Anwendungssoftware im Bereich mobiler Betriebssysteme) installiert wurden.

Der Einsatz mobiler Geräte in der Landeshauptstadt Stuttgart verursacht allerdings einen hohen Administrationsaufwand. Es wurde eine Management-Konsole eingeführt, damit die Geräte zentral konfiguriert werden können. In der Praxis zeigt sich jedoch, dass die Updates, die von Apple regelmäßig zur Verfügung gestellt werden, wegen ihrer Größe (> 1 Gigabyte) nicht über die mobile Netzverbindung heruntergeladen werden können. Es bedarf einer Wireless Local Area Network - Verbindung (WLAN). Allerdings betreibt die Landeshauptstadt Stuttgart in ihren Gebäuden keine drahtlosen WLAN Internetzugänge. Eine Alternative wäre das Herunterladen der Updates über ein WLAN zuhause. Dies ist aus Sicht der IT-Sicherheit allerdings nicht zu empfehlen. Denn man hat keinen Einblick in die Konfiguration der privaten Netze und akzeptiert somit ein Sicherheitsrisiko für die städtische Infrastruktur, in der die mobilen Geräte anschließend wieder betrieben werden.

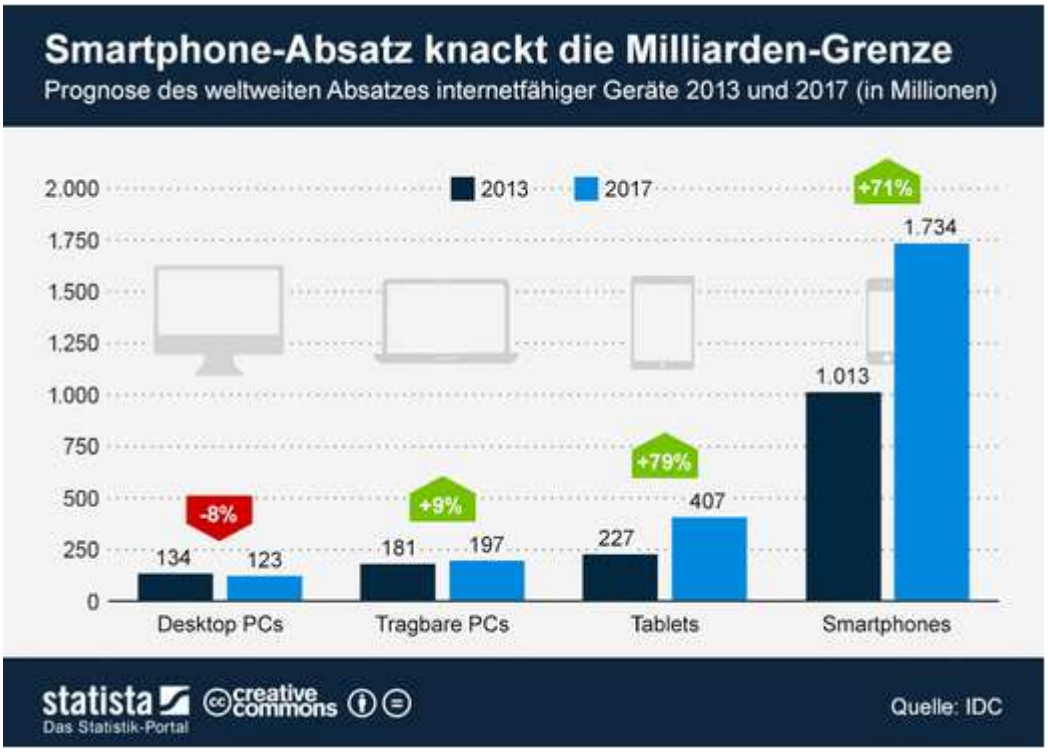
Die Nutzung von Apps stellt die beteiligten Stellen aber noch vor eine weit größere Herausforderung. Bedingt durch den Zugriff auf das Internet aus dem städtischen Netz heraus können die Geräte in der Standardkonfiguration nur die Apps herunterladen, die im eigenen stadtinternen App-Store zur Verfügung gestellt werden. Das ist aus sicherheitstechnischer Sicht sehr zu begrüßen, denn damit kann sichergestellt werden, dass eine App, bevor sie zur Verfügung gestellt wird, zunächst einer Sicherheits- und Lauffähigkeitsprüfung unterzogen wird. Leider wurden aber auch Ausnahmen von der Standardinstallation zugelassen. Das heißt gegen die Bezahlung eines Entgelts ist es einem kleinen Benutzerkreis gestattet, den App Store von Apple zu nutzen. Damit können alle Apps heruntergeladen werden, die dort zur Verfügung gestellt werden. Eine Sicherheitsüberprüfung vor dem Einsatz findet nicht statt. Vor diesem Hintergrund wird zu Beginn des Jahres 2015 ein Penetrationstest durchgeführt, der das Gefahrenpotential dieser Konfiguration untersucht. Wir sind jetzt schon gespannt auf das Ergebnis. Die Thematik bekommt zusätzlich besondere Brisanz, da geplant ist, al-

len Mitgliedern des Gemeinderats ein Smartphone zur Verfügung zur stellen und auch ihnen – falls gewollt – die Möglichkeit zur Privatnutzung zu geben.

In der Praxis lässt sich die Funktionsfähigkeit einer heruntergeladenen App nicht garantieren. Die Lauffähigkeit der App kann eingeschränkt sein, wenn diese beispielsweise Verbindungen in das Internet benötigt, die über das Standardprotokoll HTTP hinausgehen. Aber selbst wenn eine App über den städtischen App Store freigegeben wurde und zunächst funktioniert hat, kann es sein, dass es irgendwann zu Einschränkungen kommt, wenn der Anbieter die erforderlichen Verbindungen ändert. Man kann gut erkennen, dass der Aufbau unserer Infrastruktur gewisse Nachteile mit sich bringt. Wenn jedoch die dienstliche Nutzung im Vordergrund stehen soll, hat die Nutzung der Smartphones und Tablet-PCs über das städtische Netz große Vorteile in Bezug auf die Datensicherheit und Nutzung von städtischen Anwendungen wie beispielsweise die Bilddatenbank.

Grundsätzlich können Smartphones und Tablet-PCs auch in anderen Formen in die Infrastruktur eingebettet werden. Dann befinden sich die Geräte beispielsweise direkt im Internet, so wie dies im privaten Umfeld normalerweise der Fall ist. Jeder Nutzer verfügt in diesem Szenario über eine eigene Apple-ID und kann nach eigenem Gutdünken Apps herunterladen und installieren. Dienstliche Anwendungen laufen in diesem Fall in einer sogenannten Sandbox, das heißt sie sind abgekapselt von den restlichen Anwendungen auf dem Gerät.

Neben dem Penetrationstest wird ab Februar 2015 im Rahmen eines Projekts die netztechnische Ansiedlung von Smartphones und Tablet-PCs untersucht. Dabei sollen die verschiedenen Möglichkeiten mit ihren jeweiligen Gefahren, die zu ergreifenden Maßnahmen und die damit verbundenen Aufwände erfasst werden. Ziel ist es, der Führungsebene eine Empfehlung an die Hand geben zu können, damit diese auf einer möglichst umfassenden Wissensbasis eine Entscheidung über die künftige Strategie im Bereich der Smartphones und Tablets fällen kann.



WAS IST ZU TUN?

Aus unserer Sicht ist auf alle Fälle sinnvoll, all jene, die die Geräte privat nutzen dürfen, nochmal gesondert zu sensibilisieren. Beispielsweise ist auch darauf hinzuweisen, dass sie die Geräte nicht weitergeben dürfen und Tipps zu geben, auf was beim Herunterladen von Apps notwendigerweise zu beachten ist.

Wenn eine Änderung der Standardkonfiguration durchgeführt wird, die eine Gefahr für die städtische IT-Sicherheit bedeuten kann, ist vor der Änderung ein Test durchzuführen, um die möglichen Gefahren besser abschätzen zu können.

5.3 Festplattenverschlüsselung

Bei Notebooks sowie anderen mobilen Geräten und Datenträgern (z. B. Smartphones, externe Festplatten oder USB-Sticks) besteht ein erhöhtes Verlustrisiko. Mit der Hardware können auch Daten in unbefugte Hände gelangen. Derzeit werden die Daten auf den Geräten in der Regel unverschlüsselt abgelegt. Die Notebooks sind durch ein BIOS-Kennwort und das Domänenpasswort (Windowsanmeldung) vor fremdem Zugriff geschützt. Dieser Schutz ist allerdings nicht immer ausreichend.

Beim Jugendamt wurde deshalb eine Festplattenverschlüsselung eingeführt. Das eingesetzte Produkt lief nur unter dem inzwischen veralteten Betriebssystem Windows XP. Da die Wartung von Windows XP zum April 2014 eingestellt wurde (siehe Abschnitt 5.10), musste eine neue Festplattenverschlüsselungslösung her. Bei der Landeshauptstadt Stuttgart war zwar bereits eine weitere Festplattenverschlüsselungssoftware im Testbetrieb, dieses Produkt wurde aber abgekündigt. Somit musste Anfang 2014 kurzfristig eine neue Lösung ausgeschrieben werden. Unsererseits hatte diese Ausschreibung höchste Priorität, so dass nach erfolgreichen Tests die neue Festplattenverschlüsselungslösung in Verbindung mit Windows 7 bereits im Frühjahr 2014 beim Jugendamt eingeführt werden konnte.

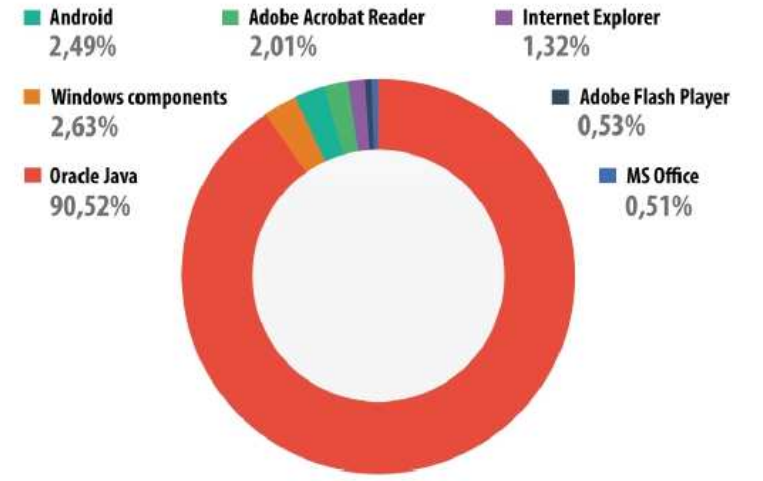
WAS IST ZU TUN?

Die bewährte Lösung muss auch auf andere schützenswerte Geräte der Stadtverwaltung ausgeweitet werden. Dazu sind personelle und finanzielle Ressourcen notwendig. Ebenso muss bei der Beschaffung von Produkten und Lösungen gewährleistet sein, dass diese über den gesamten Lebenszyklus lauffähig sind und vom jeweiligen Hersteller unterstützt werden.

5.4 Verbesserungen beim Patchmanagement der Internet-Browser

Bei der Landeshauptstadt Stuttgart wird der Internet-Browser "Mozilla Firefox" im sogenannten Extended Support Release (ESR) eingesetzt. Diese Variante des weit verbreiteten Browsers wird etwa ein Jahr lang mit Updates versorgt. Das ESR hat eine Überschneidung von 12 Wochen zwischen dem Zeitpunkt eines neuen Release und dem Ende der Unterstützung (end-of-life) des vorherigen Release. In dieser Zeit muss das neue Release getestet und auf alle Rechner verteilt werden.

Um die Funktionen des Browsers zu erweitern, werden sogenannte Plugins (z. B. Java-, Flash- und PDF-Plugin) genutzt. Diese Plugins müssen regelmäßig aktualisiert werden, da sie besonders häufig Schwachstellen aufweisen und für Angriffe missbraucht werden.



Verteilung der in Attacken von Cyberkriminellen verwendeten Exploits nach Typen der angegriffenen Anwendungen

Quelle: Kaspersky Security Bulletin 2014

In Zusammenarbeit mit der Abteilung IuK des Haupt- und Personalamts haben wir im Berichtszeitraum eine wesentliche Verbesserung des Patchmanagements erreicht. Es ist nun sichergestellt, dass ein Update auf eine neue ESR-Version vor Ende der Unterstützung der installierten ESR-Version erfolgt. Zudem wurden alle Browser so konfiguriert, dass die Sicherheitsupdates innerhalb des ESR automatisch eingespielt werden.

WAS IST ZU TUN?

Der Prozess muss weiter optimiert werden, um die Gefährdung für die Nutzer möglichst gering zu halten. Desweiteren sollte aufgrund der wachsenden Bedeutung dieser Softwarekomponente ein weiterer Internet-Browser in ähnlicher Weise auf aktuellem Stand gehalten werden. Nur dadurch kann die Unabhängigkeit von einzelnen Herstellern gewährleistet werden.

5.5 Soziales "Hacking" bzw. Manipulation

Der technische und organisatorische Schutz kann noch so gut sein – er wird nicht vollends greifen, wenn der "Faktor Mensch" unberücksichtigt bleibt. Gegen technische Angriffe wie Viren und Trojaner hat sich die Landeshauptstadt Stuttgart mittels Hard- und Software in angemessenem Umfang geschützt. Angriffe durch "Social Engineering" (soziale Manipulation) hingegen lassen sich nur abwehren, wenn alle Mitarbeiter mitdenken und mitwirken.

Unwissenheit, mangelndes Verständnis und ungenügendes Verantwortungsbewusstsein können zu erheblichen Problemen führen, die von der Entwendung von Daten bis zu technischen Ausfällen reichen. Die sicherste Informationstechnik kann ihren Schutz nicht entfalten, wenn Mitarbeiter fahrlässig agieren.

Das Bundeskriminalamt (BKA) sieht eine wachsende Gefahr durch Verbrecher im Netz. „Die Internetkriminalität ist weiterhin auf dem Vormarsch“, sagte der BKA-Präsident bei der Vorstellung des neuen "Bundeslagebilds 2013" zur Cyberkriminalität.

Das BKA zählte im vergangenen Jahr 64.426 Fälle von Cyberkriminalität in Deutschland. Das ist zwar nur etwa ein Prozent mehr als im Jahr zuvor. Doch seit 2009 stieg die Zahl der registrierten Fälle um mehr als 20 Prozent. So z. B. beim sogenannten Phishing (Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen): Hier verzeichneten die Ermittler einen Anstieg der Fälle um 20 Prozent gegenüber 2013. Mit dem Diebstahl digitaler Identitäten räumen Internetkriminelle wieder häufiger die Konten von Verbrauchern ab. Pro Fall entstand dabei ein durchschnittlicher Schaden von rund 4.000 Euro.

WAS IST ZU TUN?

Für das Jahr 2015 planen wir eine IT-Sicherheitskampagne. Die Mitarbeiter sollen geschult und sensibilisiert werden, damit sie informiert ihre Verantwortung erkennen und soziale Manipulationsversuche abwehren können.

5.6 Löschung alter Computerkonten

In Microsoft-Netzwerken entsprechen Computerkonten einer physikalischen Einheit, z. B. einem Computer oder einer Person und werden im sogenannten Active Directory verwaltet. Sie werden verwendet für die Authentifizierung eines Benutzers oder Computers, für Zugriffskontrollen auf Ressourcen im Netzwerk, die Verwaltung diverser Sicherheitsfunktionen oder für wichtige Überwachungsaufgaben. Computerkonten sind eine zentrale Einheit, in deren Datenbank eine Fülle an technischen Informationen verknüpft ist. Die Daten zu den Computerkonten sollten daher stets aktuell gehalten und eindeutig zugeordnet werden können. Veraltete oder inaktive Computerkonten sind eine unnötige Gefährdung für das ganze System.

Bis Oktober 2013 haben die Workstation-Administratoren der Ämter und Eigenbetriebe vom Windows-Serverteam der Abteilung IuK des Haupt- und Personalamts eine Übersicht der seit über sechs Monaten inaktiven Rechner ihrer Organisationseinheit zur Überprüfung bekommen.

Von dieser Übersicht wurde nicht von allen Organisationseinheiten regelmäßig Gebrauch gemacht, so dass die Zahl der "verwaisten" Computerkonten ständig anstieg. Deshalb wurde die Löschung dieser Konten automatisiert. Die Ämter und Eigenbetriebe wurden in einem Rundschreiben im August 2013 darüber informiert. Beim Durchlauf am 01.02.2014 wurden beispielsweise über 100 inaktive Konten entdeckt und gelöscht.

Neben einer Verbesserung des Lizenzmanagements wurde damit erreicht, dass keine veralteten und damit potentiell unsicheren Softwarestände (z. B. alte Virenschutzdefinitionen, fehlende Betriebssystemupdates usw.) auf den Arbeitsplatzrechnern verwendet werden können.

WAS IST ZU TUN?

Vorübergehend stillgelegte Rechner, welche beispielsweise als Reserve vorgehalten werden, müssen regelmäßig an das städtische Datennetz angeschlossen und aktualisiert werden. Nur so haben sie die notwendigen Sicherheitsupdates und sind im Bedarfsfall auch betriebsbereit.

5.7 Netzweite Dateifreigaben in der Stadtverwaltung

Auf einem Windows-Server wurden Verzeichnisse mit Buchungsdaten der Auszahlungsautomaten des Sozialamts für sämtliche Computer und Nutzer im städtischen Netzwerk sicht- und teilweise auch veränderbar bereitgestellt. Darunter war die Dokumentation sämtlicher Auszahlungen mit Angabe von Namen der Empfänger und erhaltenen Leistungen über mehrere Jahre.

Da der betriebene Server nicht vollständig in die Verwaltungsstruktur des städtischen Netzwerks integriert wurde, konnten die sonst üblichen Zugangsbeschränkungen nicht wirken. Bei der Inbetriebnahme wurde wohl zur Vereinfachung oder Beschleunigung des Prozesses kurzerhand eine Vertrauensstellung mit der Funktion "Jeder hat alle Rechte" eingerichtet.

Die dadurch erteilten Zugriffsberechtigungen wurden bereits von Mitarbeitern ausgenutzt, um eine gemeinsame Dateiablage ohne Größenbeschränkungen für Witze, Videodateien und ähnliches zu betreiben.

Durch die noch nicht stadtweit vorhandene Netzwerkzugangskontrolle (siehe auch Abschnitt 5.8) hätte die Schwachstelle auch durch Dritte ausgenutzt werden können. Dafür genügt der Zugang zu einer beliebigen Netzwerkdose, wie sie beispielsweise häufig auf Fluren oder in öffentlichen Bereichen der Stadtverwaltung anzutreffen sind.

Auf unseren Hinweis hin konnte das betroffene Amt die viel zu großzügig erteilten Zugangsberechtigungen auf den tatsächlich für den Betrieb nötigen Bereich einschränken und die Tauschplattform entfernen.

WAS IST ZU TUN?

Es muss regelmäßig geprüft werden, ob Administratoren oder externe Dienstleister Freigaben auf Systemen eingerichtet und diese auf den benötigten Nutzerkreis beschränkt haben. Nur dann kann eine eventuelle Fehlkonfiguration zeitnah behoben werden.

In künftigen Ausschreibungen muss darauf geachtet werden, dass die anzuschaffenden Geräte für den Betrieb im Netzwerk gehärtet und durch die vorhandene Infrastruktur ordnungsgemäß verwaltet werden können. Zur Abnahme ist es erforderlich, Systeme auf Schwachstellen zu untersuchen und eventuell entdeckte Fehlkonfigurationen vom Auftragnehmer kostenneutral vor Übernahme in den Regelbetrieb beheben zu lassen.

5.8 Netzwerkzugangskontrolle

Die meisten Gebäude der Landeshauptstadt Stuttgart sind selbstverständlich für unsere Bürger (und somit auch für andere) frei zugänglich. In diesen Gebäuden gibt es auch Netzwerkdosen in nicht abgeschlossenen Räumen (z. B. in Fluren, Besprechungszimmern und Druckerräumen). Wie schon im letzten Bericht erörtert, benötigen wir deshalb dringend eine technische Lösung, die unbekannten Geräten den Zugang zum städtischen Datennetz sperrt.

Im September 2013 begann der Test einer Netzwerkzugangskontrolllösung (Port Security) im Stadtmessungsamt. Diese erste Testphase wurde Anfang 2014 erfolgreich abgeschlossen. Ein weiterer Ausbau der Lösung im Stadtmessungsamt

war vorgesehen, wurde aber aufgrund eines Umzugs des Amts in ein anderes Gebäude nicht weiter verfolgt.

Das Haupt- und Personalamt hat beschlossen, diese Technologie im Rathaus einzuführen. Die dafür benötigten Lizenzen und Hardware wurden beschafft.

WAS IST ZU TUN?
Es ist gut, die Netzwerkzugangskontrolle zeitnah im Rathaus einzuführen. Nach erfolgreichem Pilotbetrieb sollten dann weitere städtische Gebäude mit Publikumsbetrieb abgesichert werden. Finanzielle und personelle Aufwendungen dürfen kein Hinderungsgrund sein.

5.9 Schnittstellenüberwachung an Computern

Sobald externe Geräte mit einem PC verbunden werden (über USB, Bluetooth, Firewire, PCMCIA usw.), beginnen diese Geräte sofort mit dem PC zu kommunizieren. Befindet sich auf dem externen Gerät beispielsweise Schadsoftware, so wird sie bereits beim Einstecken in den PC aktiviert. Dass dies nicht nur graue Theorie sondern raue Wirklichkeit ist, zeigte sich bei der Überprüfung städtischer Notebooks durch einen sogenannten Penetrationstest. Der Zugriffsschutz des Notebooks konnte über eine derartige Schnittstelle ausgehebelt werden.

Die bereits in mehreren Ämtern und Eigenbetrieben genutzte Software DeviceWatch ermöglicht das zentrale Management aller Schnittstellen und Geräte und kann so den Betrieb unerwünschter Geräte an einem PC verhindern. Die Software wurde nach Entdeckung der Sicherheitslücke auf sämtlichen Notebooks der Stadtverwaltung installiert.

WAS IST ZU TUN?
Bei Ablösung der bisher verwendeten Software sollte darauf geachtet werden, dass diese effektiver administrierbar und besser in andere Sicherheitsprodukte integrierbar ist.

5.10 Betriebssystemumstellung auf Windows 7

Seit Oktober 2009 ist das Betriebssystem Windows 7 von Microsoft auf dem Markt. Für die Ämter und Eigenbetriebe der Landeshauptstadt Stuttgart wurde

entschieden, sukzessive sämtliche Rechner auf das Betriebssystem Windows 7 umzustellen.

Das Betriebssystem Windows XP wurde nur noch bis zum 8. April 2014 gewartet und vom Hersteller mit Sicherheitsupdates versorgt. Da ein Betrieb von Rechnern mit Windows XP nach dem 8. April 2014 wegen der fehlenden Wartung mit beträchtlichen IT-Sicherheitsrisiken verbunden gewesen wäre, hatten die Ämter und Eigenbetriebe daher dafür Sorge zu tragen, dass die Ablösung aller XP-Systeme vor dem 8. April 2014 erledigt hätte sein sollen.

Nach einer Erhebung der Abteilung IuK des Haupt- und Personalamts vom April 2013 war bei den Ämtern und Eigenbetrieben noch immer eine Vielzahl von Rechnern mit Windows XP in Betrieb. Aufgrund dessen wurden die Ämter und Eigenbetriebe im Rundschreiben 015/2013 vom 07.07.2013 nochmals auf die Dringlichkeit der Umstellung hingewiesen. Zur Abkündigung von Windows XP im April 2014 waren gleichwohl noch ca. 2.000 Rechner nicht umgestellt.

Das IT-Sicherheitsmanagementteam unter unserer Leitung hat in seiner Sitzung am 16.04.2014 die Empfehlung ausgesprochen, zum Schutz des städtischen Netzes diese verbliebenen Geräte mit dem zu diesem Zeitpunkt unsicheren Betriebssystem Windows XP grundsätzlich von der Internetnutzung auszuschließen. Ab Mai 2014 wurden im Einzelfall einzelne PCs weiterhin zugelassen, wenn eine entsprechende Begründung für den Einzelfall vorlag und ein konkreter Plan mit überschaubarem Zeithorizont für die Umstellung der jeweiligen Systeme vorgelegt wurde.

Bis zum Jahresende 2014 wurden alle Rechner umgestellt.

WAS IST ZU TUN?

Der Betrieb von Rechnern erfordert von Zeit zu Zeit die eine oder andere Reparatur, wobei eine Reparatur an der Hardware teuer bezahlt werden muss. Die Reparatur an der Software hingegen, die regelmäßigen Sicherheitsaktualisierungen, sind kostenlos. So schleicht sich manchmal der Schlendrian ein, denn was man nicht bemerkt und nichts kostet wird ja auch nicht so wichtig sein. Für das derzeit aktuelle Betriebssystem Windows 7 gibt es noch bis zum Januar 2020 Sicherheitsupdates. Bis dahin muss also das Nachfolgeprodukt ausgewählt und flächendeckend installiert sein. Es sollte umgehend damit begonnen werden, denn die Zeit läuft.

5.11 Spionagesoftware auf Webserver

Seit vielen Jahren warnen wir vor den Gefahren aus dem Internet. Dass unsere Warnungen nicht aus der Luft gegriffen waren, zeigte sich im Herbst 2014 in einer nüchternen Information an die Landeshauptstadt Stuttgart durch das Bundeskriminalamt.

Mehrere Webserver, die für die Landeshauptstadt Stuttgart registriert und für die sie damit verantwortlich war, waren kompromittiert und mit einer Schadsoftware infiziert worden. Das Programm Turla, ein zur Spionage eingesetztes Trojanisches Pferd hatte die Server des Europäischen Städtenetzwerks "cities for children" befallen. Die Rechner unserer Bürger wurden dadurch bei einem Besuch der Webseite ebenfalls infiziert.

Einerseits war das Bundeskriminalamt daran interessiert, weitere Erkenntnisse zu sammeln und Aufschluss über eventuelle Hintermänner zu gewinnen. Andererseits galt es, unmittelbaren Schaden für die Landeshauptstadt Stuttgart und die Bürger, welche sich über das Europäische Städtenetzwerk Cities for Children informieren wollten, vor einer möglichen Infektion zu schützen. Daher entschloss man sich, nach der separaten Datensicherung für weitere polizeiliche Ermittlungen des Bundeskriminalamts, den Server still zu legen.

Die Infektion mit der Schadsoftware war aus mehreren Gründen möglich gewesen. Erstens war die Software zum Management der Webseiteninhalte längere Zeit nicht mehr aktualisiert worden. Zweitens waren die Webseiten seinerzeit von einem Drittanbieter entwickelt und installiert worden, der nach Projektende naturgemäß auch nicht mehr für die Landeshauptstadt Stuttgart tätig war.

WAS IST ZU TUN?

Auf Servern, die direkt mit dem Internet korrespondieren, sind alle Softwarepakete auf einem aktuellen Stand zu halten. Sofern Drittanbieter die Webserver gestalten, sind entweder städtische Standardprodukte zu wählen oder die dauerhafte Serverbetreuung ist anderweitig sicher zu stellen.
Das Notfallhandbuch aus dem letzten Jahrzehnt ist zu aktualisieren und kontinuierlich an die verschiedenen Bedrohungen anzupassen. Zudem müssen klar definierte Prozesse für die erforderlichen Schritte definiert und verfügbar gemacht werden.

Bundeskriminalamt

POSTANSCHRIFT Bundeskriminalamt · 53338 Meckenheim

Per E-Mail

An
Behördlicher Beauftragter für Datenschutz und IT-Sicherheit
Eberhardstraße 6A
70173 Stuttgart
z. Hd. [redacted]

HAUSANSCHRIFT Gerhard-Boeden-Str. 2, 53340 Meckenheim
POSTANSCHRIFT 53338 Meckenheim

TEL +49(0)2225 89[redacted]
FAX +49(0)2225 89[redacted]
BEARBEITET VON [redacted]
E-MAIL [redacted]
AZ ST 23[redacted]
DATUM 01. Oktober 2014

BETREFF **Hinweise auf kompromitierte Webseiten der Landeshauptstadt Stuttgart**

hier: Datenerhebung des betroffenen Webservers

Bezug: Ihr Telefonat mit Herrn [redacted] vom 01.10.2014

Sehr geehrter Herr [redacted]

unter Bezugnahme auf das mit Ihnen geführte telefonische Gespräch vom 01.10.2014 möchte ich Ihnen nachfolgende Erkenntnisse hinsichtlich der kompromittierten Webseiten mitteilen.

Dienstlich wurde bekannt, dass die Webseiten

- www.citiesforchildren.de
- www.citiesforchildren.eu
- www.citiesforchildren.com
- www.citiesforchildren.org

kompromittiert worden sein sollen und als Watering Hole für die Schadsoftware Turla dienen.

Die vier Domains www.citiesforchildren.de / .eu / .com / .org lösen auf die IP-Adresse 91.208.45.55 auf und konnten der

ZUSTELL- UND LIEFERANSCHRIFT BKA, Gerhard-Boeden-Str. 2, 53340 Meckenheim
ÜBERWEISUNGSEMPFÄNGER Bundeskasse Trier
BANKVERBINDUNG Deutsche Bundesbank
Filiale Saarbrücken (BBk Saarbrücken)
BIC MARKDEF1590
IBAN DE81 5900 0000 0059 0010 20

BKA

 Landeshauptstadt Stuttgart

Eberhardtstraße 6

70173 Stuttgart

zugeordnet werden.

In diesem Zusammenhang bitten wir um Kontaktaufnahme hinsichtlich der weiteren Vorgehensweise bezüglich der Erhebung und Sicherstellung von etwaigen Daten des kompromittierten Servers (mit IP-Adresse 91.208.45.55).

Mit freundlichen Grüßen

Im Auftrag

gez.

[redacted]

Bundeskriminalamt

POSTANSCHRIFT Bundeskriminalamt • 53338 Meckenheim

Per E-Mail

An
Behördlicher Beauftragter für Datenschutz und IT-Sicherheit
Eberhardstraße 6A
70173 Stuttgart
z. Hd. [redacted]

HAUSANSCHRIFT Gerhard-Boeden-Str. 2, 53340 Meckenheim
POSTANSCHRIFT 53338 Meckenheim

TEL +49(0)2225 89[redacted]
FAX +49(0)2225 89[redacted]
BEARBEITET VON [redacted]
E-MAIL [redacted]
AZ ST 23 - [redacted]
DATUM 07. Oktober 2014

BETREFF **Hinweise auf kompromitierte Webseiten der Landeshauptstadt Stuttgart**

hier: Sicherungen der betroffenen Server

Bezug: Ihr Telefonat mit Unterzeichner vom 01.10.2014

Sehr geehrter Herr [redacted]

Sehr geehrter Herr [redacted]

unter Bezugnahme auf unseren bisher geführten Schriftverkehr in puncto kompromittierte Server teilte mir Ihr Kollege Herr [redacted] mit, dass die Stadt Stuttgart beabsichtigt, diese vom Netz zu nehmen.

Herr [redacted] sicherte Unterzeichner die Aushändigung einer Sicherung des Web und Datenbankservers unter Einbindung des Behördlichen Beauftragten für Datenschutz und IT-Sicherheit zu.

Um eine zeitnahe Analyse der kompromittierten Daten durchführen zu können, bitten wir um Zusendung der Sicherungen per DVD oder Festplatte an die nachfolgende Adresse:

ZUSTELL- UND LIEFERANSCHRIFT: BKA, Gerhard-Boeden-Str. 2, 53340 Meckenheim
ÜBERWEISUNGSEMPFÄNGER: Bundeskasse Trier
BANKVERBINDUNG: Deutsche Bundesbank
Filiale Saarbrücken (BBk Saarbrücken)
BIC MARKDEF1590
IBAN DE81 5900 0000 0059 0010 20

BKA

Bundeskriminalamt Meckenheim

Gerhard-Boeden-Straße 2

53340 Meckenheim

z.Hd. Herrn [redacted]

Mit freundlichen Grüßen

Im Auftrag

gez.

[redacted]

6 Verzeichnis der Abkürzungen und Fachbegriffe

A

Active Directory	Active Directory (AD), der Verzeichnisdienst von Microsoft Windows Server. Dabei handelt es sich um eine Zuordnungsliste wie zum Beispiel bei einem Telefonbuch, das Telefonnummern den jeweiligen Anschlüssen (Besitzern) zuordnet. Den Benutzern des Netzwerks können Zugriffsbeschränkungen erteilt werden. So darf zum Beispiel nicht jeder Benutzer jede Datei ansehen oder jeden Drucker verwenden.
AK/DSB	Behördlicher Beauftragter für Datenschutz und IT-Sicherheit der Landeshauptstadt Stuttgart
App	Als App (Mobile App) wird eine Anwendungssoftware für Mobilgeräte bzw. mobile Betriebssysteme bezeichnet. Obwohl sich der Begriff App als Abkürzung von dem englischen Begriff Application Software auf jegliche Art von Anwendungssoftware bezieht, wird er im deutschen Sprachraum oft mit Anwendungssoftware für Mobilgeräte gleichgesetzt.
App Store	In Folge des großen Markterfolgs von Smartphones und Tablet-PC´s haben praktisch alle Hersteller mobiler Betriebssysteme eigene Online-Systeme entwickelt, um die für ihre jeweiligen Geräte entwickelten Apps zu vermarkten. Die Apps werden so über eine zentrale Vertriebsplattform angeboten und können von Kunden dort kostenlos oder kostenpflichtig heruntergeladen werden. Die erste dieser Vertriebsplattformen war der App Store von Apple, andere Hersteller folgten nach.
Apple-ID	Eine Apple-ID wird für alle Interaktionen mit der Firma Apple benötigt, beispielsweise um kostenpflichtige Dienste oder ein iPhone bzw. iPad nutzen zu können.

B

BIOS	Das BIOS ist eine direkt nach dem Einschalten ausgeführte und fest mit der Hardware verbundene Software. Aufgabe des BIOS ist es unter anderem, den PC zunächst funktionsfähig zu machen und im Anschluss das Starten eines Betriebssystems einzuleiten.

Bluetooth	Bluetooth ist ein in den 1990er-Jahren durch die Bluetooth Special Interest Group (SIG) entwickelter Industriestandard gemäß IEEE 802.15.1 für die Datenübertragung zwischen Geräten über kurze Distanz per Funktechnik.
Browser	Computerprogramm zur Darstellung von Internetseiten
BSI	Bundesamt für Sicherheit in der Informationstechnik

C

CheckAud	CheckAud ist eine Prüfsoftware für SAP-Systeme mit der Zielrichtung, das Berechtigungskonzept transparent abzubilden und kontrollierbar zu machen.
Client	Ein Client bezeichnet ein Computerprogramm, das auf dem Endgerät eines Netzwerks ausgeführt wird und mit einem Zentralrechner (Server) kommuniziert. Man nennt auch ein Endgerät selbst, das Dienste von einem Server abruft, Client.
Cloud	Unter Cloud Computing versteht man das Verarbeiten von Daten in einem entfernten Rechenzentrum.
Community	Eine Community-Plattform im Internet stellt grundlegende Werkzeuge bereit, um den Austausch zwischen ihren Mitgliedern zu ermöglichen und zu organisieren. Vorbedingung zur Nutzung ist fast immer eine Registrierung als Mitglied. Zur angemeldeten Teilnahme wird ein Benutzerkonto angelegt. In den meisten Fällen werden selbstgewählte Pseudonyme als Benutzernamen verwendet. Teilweise erhalten auch nicht angemeldete Gäste einen Zugang, aber meist sehr eingeschränkt.

D

DeviceWatch	Software für die Verwaltung von Schnittstellen
DMS	Dokumentenmanagementsystem
Düsseldorfer Kreis	Konferenz der Datenschutzbeauftragten des Bundes und der Länder im nicht öffentlichen Bereich
dvv.Personal	Neues Personalmanagementsystem des Datenverarbeitungsverbundes Baden-Württemberg

F

Firewire	Firewire, i.LINK oder IEEE 1394 ist eine Schnittstelle für die serielle Datenübertragung (urspr. entwickelt von Apple). In

	PC-Systemen entwickelte sich USB hingegen zum Standard.

G

GA-DS/IT-S	Geschäftsanweisung Datenschutz und IT-Sicherheit für die Landeshauptstadt Stuttgart vom 06. Juni 2006, veröffentlicht in Mitteilungen des Bürgermeisteramtes, Folge 6, vom 03. Juli 2006

H

HTTP	Das Hypertext Transfer Protocol (HTTP) ist ein Protokoll zur Übertragung von Daten über ein Rechnernetz. Es wird hauptsächlich eingesetzt, um Webseiten (Hypertext-Dokumente) aus dem World Wide Web (WWW) in einen Webbrowser zu laden.

I

Internet	Das Internet ist ein weltweites Netzwerk von Rechnern, durch das Daten ausgetauscht werden.
Intranet	Ein Intranet ist ein Rechnernetz, das im Gegensatz zum Internet nicht öffentlich ist.
IT	Informationstechnologie
IuK	Informations- und Kommunikationstechnik

K

KDRS	Zweckverband Kommunale Datenverarbeitung Region Stuttgart
Kerberos	Kerberos bezeichnet einen Authentifizierungsdienst für offene und unsichere Computernetze – z. B. das Internet. Der Name für den elektronischen Torhüter ist dem Wächter der Unterwelt entlehnt – offenbar ein Prädikat für die Unbestechlichkeit bei der Kontrolle des Computernetzes. Hier sind gewissermaßen der Client, der Server, den der Client nutzen will, und der Kerberos-Server die drei Köpfe

L

LDSG	Landesdatenschutzgesetz Baden-Württemberg
LfD	Landesbeauftragter für den Datenschutz Baden-Württemberg
Link	Ein Link oder Hyperlink ist ein Querverweis in einem elektronischen Dokument (z. B. einer Webseite) zu einem anderen elektronischen Dokument.

P

Patch	Korrekturauslieferung für Software oder Daten
PCMCIA	Die 1990 gegründete Personal Computer Memory Card International Association (PCMCIA) ist Namensgeber eines Standards für Erweiterungskarten mobiler Computer. Diese Karten sind unter den Namen PCMCIA-Karte oder PC Card bekannt. Diese Karten arbeiten stromsparend und unterstützen Hot-Plug, sind also im laufenden Betrieb wechselbar. Alle zur automatischen Konfiguration des Treibers nötigen Eigenschaften der Karte sind auf der Karte selbst abgelegt.
Phishing	Unter Phishing versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen.
PIN	Persönliche Identifikationsnummer, Geheimzahl
Plugin	Ein Plugin ist eine Programmerweiterung, die von einer Anwendung während ihrer Laufzeit eingebunden wird, um deren Funktionalität zu erweitern.

R

Release	Die fertige und veröffentlichte Version einer Software wird als Release bezeichnet. Damit geht eine Veränderung der Versionsbezeichnung, meist ein Hochzählen der Versionsnummer einher.
RFC	Die Requests for Comments (kurz RFC, zu Deutsch: "Bitte um Kommentare") sind eine Reihe von technischen und organisatorischen Dokumenten zum Internet und definieren anerkannt verbindliche Standards.

S

Sandbox	Sandbox bezeichnet in der Informationstechnologie einen isolierten Bereich, innerhalb dessen die Ausführung einer Programmfunktion keinerlei Auswirkung auf andere Anwendungen hat. Die Software wird vom Rest des Systems abgeschirmt.
SAP	Steht synonym für das Softwareprodukt der Firma, ein integriertes betriebswirtschaftliches Standardsoftwarepaket.
SGB	Sozialgesetzbuch
Smartcard	Eine Smartcard ist eine spezielle Chipkarte mit integriertem Schaltkreis, Speicher und einem Mikroprozessor, über den man auf die gespeicherten Daten zugreifen kann.
SQL	Structured Query Language SQL ist eine Datenbanksprache zur Definition von Datenstrukturen in relationalen Datenbanken sowie zum Bearbeiten und Abfragen von darauf basierenden Datenbeständen.

U

Update	Mit Update wird die Aktualisierung von Software oder Daten bezeichnet. Ein Software Update enthält in der Regel kleinere Verbesserungen wie etwa Optimierungen in der Programmausführungsgeschwindigkeit und beseitigt Fehler innerhalb eines bestimmten Softwarestands. Updates, die sich auf den Bereich der Computersicherheit beziehen, werden Security Updates genannt. Sie sorgen dafür, dass Sicherheitslücken in Programmen geschlossen werden.
USB	Der Universal Serial Bus (USB) ist eine Schnittstelle zur Verbindung eines externen Geräts mit einem Computer.

W

Web	Das Web ("World Wide Web" oder kurz "WWW") ist ein über das Internet abrufbares System von elektronischen Dokumenten, die durch sogenannte Hyperlinks miteinander verknüpft sind
WLAN	Wireless Local Area Network (Wireless LAN, WLAN) bezeichnet ein lokales Funknetz.