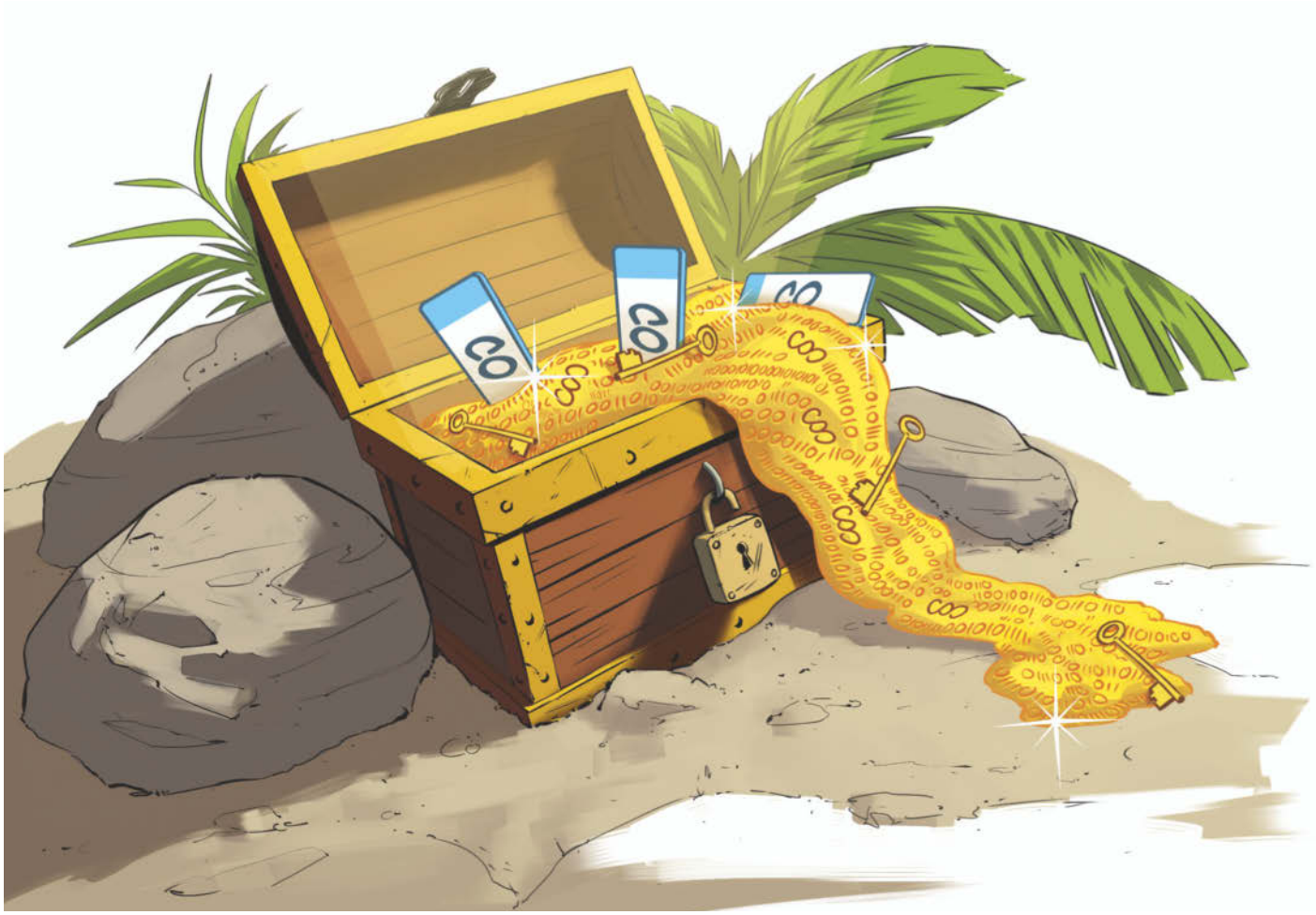

Bild: Albert Hulm

Daten-Schatzkiste

SSD mit Daten aus dem Jugendamt und der Kfz-Zulassungsstelle im Handel

Arbeitet eine Behörde mit persönlichen Daten von Bürgern, ist sie zur besonderen Sorgfalt verpflichtet. Dennoch tauchte eine SSD mit Zehntausenden Bürgerdaten aus der Kfz-Zulassungsstelle und dem Jugendamt der Stadt Coburg im Sortiment eines Händlers bei eBay als vermeintlich neuwertiges Laufwerk auf.

Von Georg Schnurer

Ende Oktober war Daniel R. auf der Suche nach einer günstigen SSD für seinen PC. Dabei stolperte er bei eBay über das Angebot der Peperit GmbH aus Reutlingen: Die bot insgesamt 19 SSDs von Silicon Power mit einer Kapazität von 256 GByte zum Stückpreis von knapp 30 Euro an. Die Laufwerke sollten laut Beschreibung neuwertig sein und aus Kundenretouren innerhalb des Widerrufsrechts stammen. Alle SSDs seien geprüft und getestet worden und befänden sich in einwandfreiem Zustand.

Klingt doch nicht schlecht, dachte sich Daniel D., und orderte am 31. Oktober ein Exemplar. Der Händler bestätigte den Kauf und kurz darauf traf die SSD beim Kunden ein. Schon beim Auspacken wurde dieser stutzig: Die vermeintlich „neuwertige“ SSD zeigte deutliche Nutzungsspuren und Beschädigungen im Bereich der Befestigungsschrauben.

Schlimmes ahnend schloss Daniel D. die SSD erst einmal an seinen Linux-PC an und mountete das Gerät im Read-only-Modus. Ein Blick auf den Betriebsstundenzähler der SSD bestätigte seine Befürchtungen: Das Teil hatte bereits mehr als 2500 Stunden in einem PC gearbeitet und war mehr als 560 Mal ein- und ausgeschaltet worden. Im bisherigen Leben der SSD hatte diese gut 4200 GByte Daten geschrieben (NAND-Schreibvorgänge) – zu einer vorgeblich aus einem Widerruf stammenden SSD passte das so gar nicht.

Nicht neu!

Daniel D. warf noch einen schnellen Blick auf die Partitionierung der SSD und traute seinen Augen kaum: Auf dem Laufwerk war eine komplette Windows-10-Installation mit allen im Laufe von knapp zwei Jahren Betrieb gesammelten Daten. Bei den Daten, das stellte Daniel D. sofort fest, handelte es sich um Informationen zu typischen Verwaltungsakten einer Zulassungsstelle. Behördendaten auf einer angeblich neuwertigen SSD vom eBay-Händler? Das war Daniel D. dann doch nicht geheuer. Unverzüglich informierte er die c’t-Redaktion und bat uns, die Sache genauer unter die Lupe zu nehmen. Damit die SSD mit den sensiblen Daten nicht in falsche Hände

gerät, brachte Daniel D. sie persönlich in die Redaktion und nahm dafür auch eine längere Zugfahrt aus der Gegend um Nürnberg nach Hannover in Kauf.

Datenhalde mit Sprengstoff

Wir versuchten zunächst ein Image zu erstellen, um die Daten auf der SSD nicht zu verfälschen. Dabei stellte sich heraus, dass die SSD offensichtlich beschädigt war: Nach einiger Zeit hängte sich das Laufwerk auf und ein Zugriff war nicht mehr möglich. Das Linux-Tool DDRescue verhalf uns aber dennoch zu einem vollständigen Image. Die Original-SSD landete im Datentresor und alle weiteren Untersuchungen konzentrierten sich auf das Image.

Wie sich schnell herausstellte, stammten die meisten Daten aus dem Zweckverband Zulassungsstelle Coburg. Gut 20 Mitarbeiter hatten mit dem Rechner gearbeitet. Die dabei auf der SSD angefallenen Daten lieferten einen detaillierten Einblick in die Arbeitsweise der Zulassungsstelle. Anscheinend wurden dort Unterlagen zu An-, Ab- und Ummeldungen von Fahrzeugen aller Art zunächst eingescannt. Eine Software namens „komXpdf“ wandelt dann alle zu einem Vorgang gehörenden Dokumente in ein PDF-Dokument um. Anschließend scheinen die Daten an das Dokumentenmanagement-System der Behörde übergeben zu werden – allerdings ohne die zuvor lokal gespeicherten Daten nach erfolgreicher Übertragung zu löschen. So sammelt sich über die Zeit eine stattliche Datenhalde an. Wir entdeckten auf der SSD gut 12.750 solcher Dokumente. Da sich darin jede Menge persönlicher Daten von Bürgern befinden, birgt so eine lokale Datensammlung auf einem Arbeitsplatz-Rechner ein enormes Missbrauchspotenzial.

Doch damit nicht genug: Anscheinend arbeitet die Zulassungsstelle Coburg mit Outlook 2016, das so konfiguriert wurde, dass stets lokale Kopien der E-Mail-Postfächer in OST-Dateien angelegt werden. In diesen, mit vielen Freeware-Programmen auslesbaren Dateien fanden wir Tausende von empfangenen, versendeten und vermeintlich gelöschten E-Mail-Nachrichten. Darunter nicht nur jede Menge interner Behördenkommunikation, sondern auch Nachrichten und Mail-Anhänge mit Bürgerdaten. Da waren dann Vollmachten, Versicherungsdaten, Handelsregisterauszüge, Zulassungen, aber eben auch Stilllegungsverfügungen, Bußgeldbenachrichtigungen, Zwangsversteigerungen und andere amtliche Zwangsverfahren zu finden.

Geradezu sorglos scheint man in der Zulassungsstelle Coburg mit Passwörtern umzugehen. Wir entdeckten haufenweise Nachrichten mit Zugangsdaten zu den verschiedensten behördlichen Servern. Darunter waren so spannende Dinge wie das europäische Fahrzeug- und Führerscheininformationssystem EUCARIS, das Zentralregister des Kraftfahrt-Bundesamtes REGINA und eVB-Zugangsdaten, um nur einige der Dienste zu nennen. Auch der Zugriff auf die DEKRA-Gutachten-Datenbank, die Rechtsdatenbank Wolterskluwe-online und andere Dienste waren vertreten.

Weitere strukturelle Datenschutzrisiken entdeckten wir bei einem Blick auf die Spuren, die der behördeninterne Brief-Generator hinterlassen hat: Das System wird anscheinend von den Mitarbeitern mit Auszügen aus der zentralen Datenbank gefüttert. Die Datenbank hinterlegt auf dem Rechner des Verwaltungsmitarbeiters eine Datei mit der Endung .db. Dabei handelt es sich um eine Datei im CSV-Format, die jeweils eine Deskriptorenzeile und einen Bürgerdatensatz enthält. Daraus generiert das System dann einen Brief und legt diesen im RTF-Format im Userverzeichnis des Mitarbeiters ab. Nach erfolgtem Druck wird aber weder die CSV- noch die RTF-Datei gelöscht – und wieder entsteht eine Datenhalde, die zu allerlei Missbrauch einlädt.

Daten vom Jugendamt

Aber es kommt noch schlimmer: Eine der Mitarbeiterinnen der Zulassungsstelle hat wohl einen Arbeitsvertrag, bei dem sie einen Teil ihrer Arbeitszeit auch für das Jugendamt des Landratsamts Coburg aufwendet. Die Arbeit für das Jugendamt scheint am gleichen PC zu erfolgen wir die für die Zulassungsstelle. Folgerichtig entdeckten wir im E-Mail-Verkehr der Mitarbeiterin auch jede Menge hochsensibler Korrespondenz in Jugendamtsangelegenheiten, darunter auch Daten zu Betreuungsverhältnissen, Heimunterbringungen und Unterhaltsfragen. So etwas gehört unter keinen Umständen unverschlüsselt auf den lokalen PC eines Verwaltungsmitarbeiters und natürlich erst recht nicht auf eine bei eBay verkaufte SSD.

Angesichte der bereits entdeckten Daten fällt es kaum noch ins Gewicht, dass sich auf der SSD auch Dokumente zu internen Abläufen der Behörde fanden. So etwa die im Amt als „Bibel“ bezeichnete Dokumentation aller Handlungsabläufe der Zulassungsstelle. Aus den in den jeweiligen Nutzerverzeichnissen hinterlegten Cookies und Surf-Verläufen lässt sich auch das private und dienstliche Surfverhalten der einzelnen Mitarbeiter nachvollziehen. Doch wer da wo und wann nach Urlaubsreisen, Kochrezepten oder Hochzeitssprüchen gesucht hat, ist weit weniger brisant als die vielen Daten der Bürger.

Spurensuche

Doch wie kommt eine SSD mit sensiblen Behördendaten in das Angebot eines eBay-Händlers? Das Datenschutzrecht schreibt vor, dass Datenträger mit sensiblen Informationen entweder fachgerecht vernichtet oder zumindest zuverlässig gelöscht werden müssen. Über die Löschung beziehungsweise Vernichtung muss die Behörde einen entsprechenden Beleg erhalten, andernfalls verhält sie sich rechtswidrig.

Unser Versuch, den Weg der SSD zu eBay zu verfolgen, endete zunächst beim Händler. Um Stellungnahme gebeten, er-

Diese bei eBay gekaufte SSD enthielt als unerwartete Zugabe nicht nur zehntausende Bürgerdaten, sondern auch Zugangsdaten zu diversen Behörden- und Firmenserverdiensten.

Auf der Rückseite der SSD entdeckten wir einen Aufkleber des PC-Herstellers Hyrican. Er gab erste Hinweise auf den Weg des Datenspeichers zu eBay.

klärte Mathias Zweigle, Geschäftsführer der Peperit GmbH, dass die uns von Daniel D. übergebene SSD nicht von ihm stammen könne. Er habe nie eine SSD mit der zugehörigen Seriennummer eingekauft und könne sie folglich auch nicht verkauft haben, beteuerte Zweigle. Der Kunde wiederum schwört Stein und Bein, genau diese SSD von der Peperit GmbH zugeschickt bekommen zu haben. Seine Aussage stützt die von der Firma erhaltene Rechnung, die exakt eine SSD des uns übergebenen Typs beschreibt. Allerdings ist auf der Rechnung keinerlei Seriennummer hinterlegt – zweifelsfrei können wir dem Händler die Lieferung damit nicht nachweisen.

Behörde im Alarm-Modus

Doch damit waren unsere Recherchemöglichkeiten noch nicht erschöpft: Auch über die Zulassungsstelle Coburg sollte sich zumindest teilweise rekonstruieren lassen, wie die SSD und die darauf befindlichen Daten ihren Weg zu eBay genommen haben. Wir informierten das zuständige Landratsamt Coburg, den Datenschutzbeauftragen des Amtes und den bayrischen Datenschutzbeauftragten am Freitagnachmittag über die bei uns gelandeten Daten.

Die Reaktion der Behörde erfolgte unverzüglich: Der bayrische Datenschutzbeauftragte, Prof. Dr. Thomas Petri, leitete sofort eine Untersuchung des Vorfalls ein. Auch der Datenschutzbeauftragte des Landkreisamtes blieb nicht untätig und schaltete die Kriminalpolizei Coburg ein. Dort vermutete man zunächst, dass die SSD aus einem der vier Behördenrechner stammen könnte, die zusammen mit einem Beamer um Ostern herum bei einem Einbruch im Schulungszentrum der Zulassungsstelle gestohlen worden waren. Wir extrahierten daraufhin den Namen und die IP-Adresse des Rechners aus den Daten auf der SSD. Doch der PC mit der Bezeichnung „HY038“ stand nicht auf der Liste der entwendeten Geräte. Zudem nutzten die Mitbearbeiter den Rechner noch lange nach Ostern.

All das führte letztlich zu einer anderen Spur: Die Zulassungsstelle wird IT-technisch vom Fachbereich Informations- und Kommunikationstechnik des Landratsamts Coburg betreut. Zusätzlich fungiert die DiAL GmbH aus Eichenzell als externer Dienstleister. Der war auch für die Beschaffung der PCs in der Zulassungsstelle verantwortlich. Die DiAL GmbH hatte die Hyrican Informationssysteme AG mit der Lieferung der Rechner beauftragt. Im Juni 2019 gab es dann ein Problem mit der SSD in dem Rechner mit der Bezeichnung „HY038“. Daraufhin übernahm ein Techniker von Hyrican den Austausch der SSD. Nach Angaben der Behördenleitung hätte der Hyrican-Techniker auch eine Löschungsbescheinigung für die mitgenommene defekte SSD ausgestellt.

Löschen nach DoD

Doch wieso landete die SSD mitsamt den Daten dann bei eBay? Wir baten Christian Grimm, technischer Leiter bei der Hyrican Informationssysteme AG, um Stellungnahme. Laut Grimm wurde die von uns untersuchte SSD tatsächlich von einem Hyrican-Mitarbeiter in der Zulassungsstelle Coburg getauscht. Die SSD sei dann am 22. August zusammen mit 33 weiteren SSDs des gleichen Typs an den Distributor, die Api Computerhandels GmbH, zwecks Garantieleistung gesendet worden. Üblicherweise würden Laufwerke mit sensiblen Daten bei Hyrican mit einem speziellen Festplatten-Duplizier-system, dem Image MASSter 4000PRO, gelöscht. Der Imager bietet die Funktion WhipeOut DoD. Dahinter verbirgt sich ein vom amerikanischen Verteidigungsministerium entwickeltes Löschverfahren (DoD 5220.22-M), bei dem alle Daten auf einer Festplatte mehrfach mit diversen Bitmustern überschrieben werden.

Für Laufwerke mit magnetischer Datenspeicherung mag diese Löschmethode durchaus geeignet sein, für SSDs ist damit aber generell keine einhundertprozentige Löschung aller Daten möglich. Jede SSD besitzt interne Reservesektoren (Over-Provisioning), auf die der Controller im Rahmen des sogenannten Wear Leveling Daten von häufig genutzten Speicherzellen auslagert. Diese über die SATA-Schnittstelle nicht adressierbaren Reservespeicherzellen erreicht ein Löschverfahren nach DoD nicht. Für hochsensible Daten auf SSDs kommt deshalb nur die physikalische Zerstörung des Laufwerks infrage.

Die Daten der Coburger Zulassungsstelle klassifiziert die Behörde als „vertrauliches Material“ der Sicherheitsstufe 3. Hier wäre eine Löschung durch mehrfaches Überschreiben nach DoD also durchaus hinreichend – selbst auf einer SSD. Doch die in der Zulassungsstelle aufgrund eines Firmware-Fehlers ausgetauschten SSDs seien mit dem Image MASSter 4000PRO nicht mehr ansprechbar gewesen, teilte uns der technische Leiter von Hyrican mit.

Kein Festplattenverwurf

Doch warum wurden die vermeintlich defekten SSDs dann nicht vernichtet? Auch dafür hatte Hyrican eine Erklärung: Das Landratsamt hatte bei der Ausschreibung für die PC-Beschaffung explizit auf den sogenannten Festplattenverwurf verzichtet. Damit gehen defekte oder ausgetauschte Festplatten und SSDs in den Besitz des Lieferanten über – hier also Hyrican. Nur wenn in der Ausschreibung explizit „Festplattenverwurf“ vereinbart wurde, verbleiben ausgebaute Datenspeicher im Besitz der Behörde und werden dort dann üblicherweise direkt vernichtet.

Ohne Festplattenverwurf ging unsere SSD also zurück an den PC-Hersteller Hyrican. Von dort gelangte das Laufwerk zusammen mit 32 weiteren defekten SSDs des gleichen Typs an den Distributor Api. Natürlich baten wir auch dort um Stellungnahme. Wir wollten wissen, wie die von Hyrican zurückgeschickte SSD anscheinend ungeprüft und ungelöscht wieder in den Handel geraten konnte. Doch bei Api zeigte man sich wenig auskunftsfreudig: Man habe aktuell kein Interesse an einer Kommunikation mit der Presse, ließ man uns telefonisch mitteilen.

Trotzdem baten wir per Fax und E-Mail um Stellungnahme. Die Antwort kam dann in Form eines Anwaltsschreibens. Die Kanzlei ließ uns wissen, dass Api nach unserer Anfrage eine Verdachtsmeldung nach Artikel 33 DSGVO beim zuständigen Datenschutzbeauftragten für Nordrhein-Westfalen abgegeben habe. Nach dieser Vorschrift müssen Datenpannen vom Verantwortlichen binnen 72 Stunden nach Kenntnis der zuständigen Aufsichtsbehörde gemeldet werden. Geschieht dies nicht, drohen hohe Bußgelder. Weiter erklärten die Anwälte, dass Api die SSD einer einfachen, rein technischen Funktionsprüfung unterzogen habe. Nachdem dabei keine Fehler festgestellt worden seien, habe man die SSD als B-Ware an die ITK Computer GmbH, einer Tochtergesellschaft von Api, weiterverkauft. ITK habe die SSD wiederum an einen gewerblichen Händler als B-Ware veräußert. Nennen wollte das Unternehmen den Händler freilich nicht.

Dennoch scheint der Weg der SSD von der Coburger Zulassungsstelle zu eBay damit hinreichend geklärt zu sein: Auf Nachfrage bestätigte nämlich der eBay-Händler, dass er die von ihm angebotenen SSDs von der Api-Tochter erworben hatte.

Bild: JMR Electronics Inc

Zum Duplizieren von Festplatten-Images entwickelt, eignet sich der Image MASSter 4000Pro auch zum Löschen von Festplatten mit vertraulichem Material. Zum vollständigen Löschen von SSDs ist seine Funktion „WipeOut DoD" aber prinzipbedingt ungeeignet.

Polizeiarbeit

Parallel zu unseren Nachforschungen tat sich auch bei den Ermittlungsbehörden etwas: Die Zentralstelle Cybercrime Bayern mit Sitz in Bamberg übernahm das Ermittlungsverfahren von der Kriminalpolizei Coburg. Als erste Amtshandlung verfügte man eine Beschlagnahmung der SSD. Nachdem unsere Recherchen rund um die Daten und den Weg der SSD ohnehin abgeschlossen waren, gab es für die Redaktion keinerlei Gründe, hier nicht mit den Ermittlungsbehörden zusammenzuarbeiten.

Zwei Mitarbeiter der Kriminalpolizei besuchten wenig später die c't-Redaktion und nahmen das Corpus Delicti in Empfang – wir sind nun sehr gespannt, was die weiteren Ermittlungen der Zentralstelle Cybercrime Bayern ergeben und welche Konsequenzen das Datenleck für die Beteiligten haben wird.

Was nun, Landratsamt Coburg?

Unabhängig davon bleibt die Frage nach den Lehren, die die Zulassungsstelle und das Landratsamt Coburg aus dem Vorfall ziehen. Schließlich förderten unsere Recherchen einen geradezu leichtsinnigen Umgang mit den Daten von Bürgern zutage. Warum, so fragten wir uns, waren überhaupt Bürgerdaten auf den lokalen PCs der Mitarbeiter gespeichert? Warum erfolgte das auch noch unverschlüsselt, wo die verwendete Windows 10-Version (Windows 10 Enterprise 2016 LTSB, 6.3.14393) mit Bitlocker doch eine recht sichere Möglichkeit der Verschlüsselung bietet? Darüber hinaus erscheinen auch die internen Abläufe in der Zulassungsstelle und im Jugendamt nicht datenschutzkonform. Weder E-Mails noch Schreiben an Bürger gehören auf lokale Rechner und dass man Zugangsdaten nicht per unverschlüsselter E-Mail in der Behörde verteilt, sollte eigentlich klar sein.

Für den Fachbereich Informations- und Kommunikationsmanagement des Landratsamts Coburg ging Matthias Aust auf unsere Fragen ein. Die im Landratsamt verwendete Technik in Verbindung mit der in der Zulassungsstelle verwendeten Hardware lasse aktuell die Nutzung von Bitlocker nicht zu, da man den Software-Rollout derzeit nur im Legacy-Modus durchführen könne. Es gäbe Probleme mit dem TPM in diesem Betriebsmodus. Das klingt zwar nachvollziehbar, doch warum man dann komplett auf eine Verschlüsselung der lokalen SSDs verzichtet, leuchtet uns nicht so recht ein. Schließlich gibt es neben Bitlocker noch andere Verschlüsselungslösungen für Windows-PCs.

Die Nutzung des Exchange Cache Modus erklärt Matthias Aust mit der Umstellung des Mailservers von Outlook 2010 auf Outlook 2016. Beim Zugriff auf Mails habe es danach teils erhebliche Performanceprobleme bei der Kommunikation zwischen dem Server und den Clients gegeben. Da das Problem auch nach Hinzuziehung eines externen Systemhauses nicht in den Griff zu bekommen war, habe man sich notgedrungen für die lokale Zwischenspeicherung der Mails entschieden.

Wegen der Auffälligkeiten beim Dokumentenmanagement-System der Zulassungsstelle habe man den Hersteller der Software kontaktiert. Ein Ergebnis läge noch nicht vor.

Seit Jahresbeginn würde im Landratsamt Coburg an der Erarbeitung eines Informationssicherheitskonzepts nach ISIS12-Methodik (Informations-Sicherheitsmanagement-System in zwölf Schritten) gearbeitet. Der aktuelle Fall mache laut Aust deutlich, dass es richtig war, dem Thema Informationssicherheit einen höheren Stellenwert einzuräumen. Bei zukünftigen Ausschreibungen für Behörden-PCs, auf denen sensible Daten verarbeitet werden, werde man zudem wohl nicht mehr auf den „Festplattenverwurf" verzichten. *(gs@ct.de)* c't