

Datendiebstahl in Bundesbehörden

29.04.2008, Alexander Schminke/Bruchlinien.de

Nach einer Anfrage des Bundestagsabgeordneten Carl-Ludwig Thiele¹ (FDP) gab das Bundesministerium des Inneren den Verlust zahlreicher Computer und Datenträger aus Bundesbehörden bekannt. Nicht nur den „meisten Bundesbehörden“ sind sensible und geheime Daten abhanden gekommen, sondern auch einigen im Ausland eingesetzten Diplomaten. Über das tatsächliche Ausmaß des Datenverlustes kann das Bundesinnenministerium keine Angaben machen. Der Bundesdatenschutzbeauftragte Peter Schaar² fordert deshalb weitere Aufklärung und eine verbesserte Erfassung solcher Low-Tech-Vorfälle.

Carl-Ludwig Thiele, stellvertretender Vorsitzender der FDP-Bundestagsfraktion, ist um die Datensicherheit in Bundesbehörden besorgt. Auslöser seiner Besorgnis sind die unfassbaren Datenlecks in Großbritannien und ein Einbruch in die Berliner Wohnung von Bundesjustizministerin Brigitte Zypries, bei dem Ende Januar 2008 zwei Laptops gestohlen wurden.

Massive Datenverluste britischer Behörden

Britische Behörden sehen sich seit Monaten mit einem Datenverlust unvorstellbaren Ausmaßes konfrontiert. Begonnen hatte die Pannenserie im Mai 2007.³ Der *Driver and Vehicle Licensing Agency* ist eine Festplatte mit Daten von drei Millionen Fahrschülern gestohlen wurden. Der Diebstahl ereignete sich im US-Unternehmen *Pearson Driving Assessment*, das Datenmaterial im Auftrag der britischen Zulassungsbehörde bearbeitet und verwaltet. Während die Verkehrsministerin Ruth Kelly dem Unterhaus Bericht erstattete⁴, gab sie außerdem den Verlust von 7500 Fahrzeughalterdaten bekannt, die postalisch von Nordirland nach Wales verschickt worden waren.

Dass der Postweg für den Versand personenbezogener Daten höchst ungeeignet erscheint, musste *HM Revenue and Customs* am 18. Oktober 2007 erfahren.⁵ An diesem Tag verlor die Steuerbehörde auf einen Schlag 25 Millionen Datensätze britischer Kindergeldempfänger.⁶ Zwecks Überprüfung wurden die auf zwei CDs gespeicherten Informationen auf dem vom Expressdienstleister TNT betriebenen internen Postweg an das *National Audit Office* verschickt und - erreichten nie Ihren Empfänger.

Die darauffolgende Sicherheitsüberprüfung aller Behörden deckte ein neues Datenleck auf.⁷ Den neun Verwaltungszentren des britischen Gesundheitssystems (NHS) fehlten plötzlich Patientendaten. Unter anderen sind die Datensätze von 160.000 Kindern, die ein Krankenhaus angefordert hatte, auf dem Lieferweg abhanden gekommen.⁸

Der massive Datenverlust britischer Behörden setzte sich auch im neuen Jahr fort.⁹ Der Verteidigungsminister Des Browne klärte am 21. Januar 2008 das Unterhaus über den Diebstahl unverschlüsselter Daten von 153.000 Rekruten und Militärdienstbewerbern sowie Bankverbindungen von 3.700 Personen auf.¹⁰ Über Nacht hatten Unbe-

kannte auf einem bewachten Militärgelände der Royal Navy ein Laptop geraubt, den ein Jungoffizier auf dem Beifahrersitz seines verschlossenen PKWs hatten liegen lassen. Brown ergänzte seinen Bericht mit dem Eingeständnis, dass das Militär bereits 2005 zwei Laptops auf ähnliche Art und Weise verloren hatte, auf denen die Daten von lediglich 500 Personen gespeichert wären.

Der zuletzt bekannt gewordene Datenverlust betrifft das britische Innenministerium, das nach Informationen des *Guardian* einen Low-Tech-Vorfall untersucht.¹¹ Demnach hatte eine Computerwerkstatt den Auftrag erhalten, einen bei eBay erworbenen Laptop wieder flott zu machen. Am 25. März entdeckte ein Techniker unter der Tastatur des Laptops eine CD mit der Aufschrift "*Home Office Confidential*". Nach Aussage eines Sprechers des Innenministeriums seien sowohl Laptop als auch CD verschlüsselt gewesen.

Gezielter Einbruch bei Justizministerin Zypries

Ende Januar brachen Unbekannte in die Steglitzer Wohnung von Brigitte Zypries (SPD) ein. Die Bedingungen für diesen Einbruch waren äußerst günstig: sobald die Bundesjustizministerin sich außer Haus und nicht mehr im Bezirk befand, wurde von einer Bewachung ihrer Wohnung abgesehen. Den Tätern schien diese Praxis bekannt gewesen zu sein. Mit "chirurgischer" Präzision konnten sie ihre Tat verüben, wobei sie es ausschließlich auf die elektronischen Datenträger der Ministerin abgesehen hatten. Die zwei fehlenden Laptops, die zum Tatzeitpunkt keine sensiblen Daten enthalten haben sollen, bemerkte Zypries erst Tage später. "Ein Einbruch bei einer solch einflussreichen Frau", erläuterte ein Beamter gegenüber der Berliner Morgenpost, "wird nicht aus einer Laune heraus begangen. Man kann nicht ausschließen, dass es sich um eine politisch motivierte Tat handelt"¹².

Low-Tech-Bedrohungen

Geht es um den Datenschutz, denken viele Anwender zunächst an High-Tech-Bedrohungen, wie zum Beispiel Bots, Malware, Trojaner, Würmer u.a.. Doch der Diebstahl sensibler oder geheimer Informationen über das Internet, der sogenannte Online-Identitätsdiebstahl, wird überschätzt. Weitaus häufiger sind Low-Tech-Bedrohungen. "Die meisten persönlichen Daten werden auf ganz traditionellem Weg gestohlen", erklärt Ken Hunter¹³, Präsident des *Better Business Bureau*, das mit dem US-Marktforschungsunternehmen *Javelin Strategy & Research* eine Studie zu diesem Thema veröffentlicht hat.¹⁴ Beim Offline-Identitätsdiebstahl geht es um den Diebstahl unbeaufsichtigter oder fahrlässig transportierter Notebooks, Handheld-Organizer und Smartphones; das Abfangen verschickter Datenträger auf ungeschützten Lieferwegen; das Abfischen von achtlos entsorgten und nicht unkenntlich gemachten Informationen aus dem Hausmüll (*Dumpster Diving*); das Ausspähen gutgläubiger Menschen (*Social Hacking*); oder den Identitätsdiebstahl aufgrund verloren gegangener oder gestohlener Brieftaschen.

Datenlecks in Bundesbehörden

"Wie ist es um die Sicherheit der Daten in Deutschland bestellt?" Diese Frage stellte sich der stellvertretende Fraktionsvorsitzende der FDP, Carl-Ludwig Thiele, und richtete am 6. März 2008 zwei Fragen an die Bundesregierung.¹⁵ Er wollte wissen, ob und wie viele Computer in Bundesbehörden bislang abhanden gekommen sind und in welchen Behörden sich möglicherweise diese Hardware-Verluste ereignet haben. Die Antwort kam als Kurzmitteilung aus dem Bundesinnenministerium. In den letzten drei Jahren seien rund 500 Notebooks und Computer in den "meisten" Bundesbehörden "gestohlen worden, verloren gegangen oder unauffindbar". Exakte Verlustzahlen zu benennen, sei der kurzfristigen Anfrage wegen nicht möglich gewesen. Die Antwort hat Thiele dennoch verblüfft: "Die Anzahl der PC-Verluste zeigt, dass in Bundesbehörden unverantwortlich mit Datenträgern umgegangen wird."¹⁶ Die Zusicherung des Bundesinnenministeriums, dass die Daten auf den verschwundenen Datenträgern "absolut sicher geschützt" seien, klingt eher wie eine obligatorische Beschwichtigungsformel. Weitere Aufklärung sei deshalb dringend geboten, so Thiele. Um den Diskurs zu forcieren, legte er am 28. März 2008 der Bundesregierung eine kleine Anfrage mit 28 Fragen vor.¹⁷

Verlust geheimer Regierungsdaten

Das zwei Wochen später dem Parlamentsekretariat zugestellte Antwortschreiben des Bundesinnenministeriums¹⁸ informiert zunächst über die Anzahl der in allen deutschen Behörden eingesetzten Computer. Demnach sind insgesamt 314.000 stationäre sowie 53.600 mobile Computer in Gebrauch. Da es zur Zeit keine zentrale Erfassung von Computer- und Datenträgerverlusten gibt, beruhen die Angaben über die Anzahl gestohlener oder unauffindbarer Hardware auf die kurzfristige Recherche des Bundesinnenministeriums. "Geräte- sowie Datenträgerverluste [werden] eigenständig innerhalb der betroffenen Behörde bzw. dem betroffenen Geschäftsbereich erfasst." Aufgrund dieser aus den einzelnen Behörden erhobenen Informationen ergibt sich folgendes Bild: "In den Jahren 2005 – 2007 [sind] in deutschen Bundesbehörden rd. 189 stationäre Personal Computer, rd. 326 tragbare Computer (Notebooks), rd. 38 Memory-Sticks, CDs und DVDs sowie 271 Mobilfunktelefone und Taschenrechner ("Handheld-Organizer") gestohlen worden, abhanden gekommen bzw. unauffindbar". Über den Informationsgehalt der dabei verloren gegangenen Daten macht das Bundesinnenministerium keine Angaben. In dem Schreiben wird lediglich betont, dass dabei "überwiegend »offene« Daten, die nicht sensibel oder besonders schützenswert waren wie bspw. Präsentationen und Statistiken", abhanden gekommen sind. Ein Grund zur Entwarnung stellt dieser angebliche Befund nicht dar. Denn in den darauffolgenden Sätzen deutet das Bundesinnenministerium einige schwerwiegende Datenpannen an.

Auf Anfrage hat das Bundesministerium der Verteidigung mitgeteilt, dass derzeit in fünf Fällen wegen des Verlustes von Datenträgern, die Informationen mit der "Einstufung VS-Vertraulich und höher" enthielten, ermittelt werde. Personenbezogene Daten sollen angeblich nur auf einem dieser verschwundenen Datenträger gespeichert sein.

Etwas konkreter äußerte sich das Bundesamt für den Zivildienst zu eigenen Datenpannen. Demnach ist der Behörde ein Laptop gestohlen worden, auf dem sich 1.200 verschlüsselte Adressdaten von Zivildienstleistenden einer Betreuungsregion befunden haben.

Auch dem Bundesministerium der Justiz ist ein Laptop gestohlen worden. Auf diesem befanden sich "Verbindungsdaten für die Einwahl in dessen Local Area Network (LAN)". Nach Aussage der Behörde sei eine "Einwahl in das LAN nicht mehr möglich", da eine sofortige Sperrung der UMTS-Karte veranlasst wurde.

Verlustreiche Dienstreisen

Laut Bundesinnenministerium gingen im Ausland 46 Notebooks verloren. Über den Status dieser Geräte (Stand-by-Modus oder Power-off-Modus) zum Zeitpunkt ihres Verschwindens sowie über das auf den Festplatten gespeicherte Datenmaterial erteilt das Papier keine Auskunft. Es wird lediglich erläutert, wie Laptops bei Auslandsreisen mitgeführt werden. Da immer die Möglichkeit unbeobachteter Zugriffsversuche durch Dritte bestehe, schreiben interne Dienstanweisungen das Mitführen von Laptops grundsätzlich als Handgepäck vor. Ob verschlüsselte Festplatten ins Ausland mitgenommen werden können, wird von den jeweiligen Einreisebestimmungen abhängig gemacht. In Fällen, in denen die Offenlegung von Passwörtern, eine Beschlagnahme sowie Kopie der Festplatten durch die Zollbehörden des Ziellandes drohen (s. Einreisemodalitäten der USA)¹⁹, werden Dienstreisende, insbesondere Militärangehörige, mit diplomatischer Immunität versehen.

Kein Grund zur Panik

Den Grundtenor des Papiers in Bezug auf den Datenschutz gedeutet, besteht nach Ansicht des Bundesinnenministeriums kein Grund zur Panik. Die meisten gestohlenen, verloren gegangenen oder unauffindbaren Computer und Speichermedien hätten nicht nur für Dritte uninteressante Daten enthalten, sondern auch aktivierte Festplattenverschlüsselungen, die das Ausspähen von Informationsinhalten unmöglich machten. Dass es zum Beispiel Techniken gibt (s. die Forschungsarbeit des *Center for Information Technology Policy* der *Princeton University*)²⁰, mit denen die Schlüssel für die Chiffrierungen ausgekundschaftet werden können, wird im Papier nicht angesprochen.

Thiele: "Ein handfester Skandal"

Es sei handfester Skandal, bemängelte Thiele, "wenn die Regierung noch nicht einmal für die Sicherheit ihrer Informationen sorgen kann, die sie mit ihrer grenzenlosen Datensammelwut zusammen trägt"²¹. Die stellvertretende Vorsitzende der Bundestagsfraktion DIE LINKE und Vizepräsidentin des Deutschen Bundestages, Petra Pau, äußerte sich besorgt über die Datenlecks in Bundes- und Verwaltungsbehörden: "Der materielle Schaden von 540.000 Euro ist fatal, aber überschaubar. Der damit verbundene Datenverlust indes ist unberechenbar und daher verantwortungslos."²² Verant-

wortungslos sei auch der bisherige Umgang mit dieser Problematik, so Thiele, und forderte weitere Aufklärung: "Die 14 zum Teil sehr kurzen und ausweichenden Antworten auf die 28 Einzelfragen der Kleinen Anfrage lassen darauf schließen, dass sich die Bundesregierung selbst erst über die Geschehnisse informieren musste und über das Ausmaß der Verluste bis zu der Anfrage der FDP-Bundestagsfraktion überhaupt nicht im Bilde war."²³ Die Haltung der Bundesregierung mache deutlich, dass eine zentrale Erfassung aller Datenpannen dringend erforderlich sei. Der Datenschutzbeauftragte Peter Schaar unterstützt nach Angaben seines Sprechers, Dietmar Müller, die Forderung des FDP-Abgeordneten: "Die Vorfälle zeigen, wie wichtig, eine Meldepflicht für solche Datenverluste ist, damit wir ermitteln können."²⁴

¹ Internetseite des stellv. Vorsitzenden der FDP-Bundestagsfraktion, Carl-Ludwig Thiele. Online in Internet: URL: <http://www.carl-ludwig-thiele.de/> [Stand 28.04.2008]

² Internetseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Peter Schaar. Online in Internet: URL: <http://www.bfdi.bund.de/> [Stand 28.04.2008]

³ Vgl. Heise online, Britischen Behörden gehen erneut Millionen Daten verloren, 18.12.2007. Online in Internet: URL: <http://www.heise.de/newsticker/meldung/100742> [Stand 28.04.2008]

⁴ Statement by the Secretary of State for Transport on Data Security, 17.12.2007. Online in Internet: URL: <http://www.dft.gov.uk/press/speechesstatements/statements/datasecurity> [Stand 28.04.2008]

⁵ Vgl. Heise online, Millionen Briten von Datenpanne betroffen, 21.11.2007. Online in Internet: URL: <http://www.heise.de/newsticker/meldung/99315> [Stand 28.04.2008]

⁶ Vgl. BBC News, Q&A: Child benefit records lost, 22.11.2007. Online in Internet: URL: http://news.bbc.co.uk/2/hi/uk_news/politics/7103828.stm [Stand 28.04.2008]

⁷ Vgl. Heise online, Daten von hunderttausenden Patienten sind in Großbritannien verloren gegangen, 23.12.2007. Online in Internet: URL: <http://www.heise.de/newsticker/meldung/101035> [Stand 28.04.2008]

⁸ Vgl. Sunday Mirror, 9 trust lose files, 23.12.2007. Online in Internet: URL: <http://www.sundaymirror.co.uk/news/sunday/2007/12/23/9-trusts-lose-files-98487-20264126/> [Stand 28.04.2008]

⁹ Vgl. Heise online, Datenpannen beim britischen Militär und US-Kreditkartenunternehmen, 19.01.2008. Online in Internet: URL: <http://www.heise.de/newsticker/meldung/102065> [Stand 28.04.2008]

¹⁰ Vgl. Statement by Des Browne, Defence Secretary, to House Of Commons, 21.01.2008. Online in Internet: URL: <http://www.mod.uk/DefenceInternet/DefenceNews/DefencePolicyAndBusiness/BrowneAnnouncesReviewOnModInformationSecurity.htm> [Stand 28.04.2008]

¹¹ Vgl. The Guardian, Laptop sold on eBay hid confidential Home Office disc, 28.02.2008. Online in Internet: URL: <http://www.guardian.co.uk/technology/2008/feb/28/politics.ebay> [Stand 28.04.2008]

-
- ¹² Berliner Morgenpost, Einbruch bei Ministerin Zypries, 02.02.2008. Online in Internet: URL: <http://www.morgenpost.de/content/2008/02/02/berlin/944763.html> [Stand 28.04.2008]
- ¹³ Stern.de, Die meisten Daten werden offline gestohlen, 05.02.2005. Online in Internet: URL: http://www.stern.de/computer-technik/computer/536169.html?nv=ct_mt [Stand 28.04.2008]
- ¹⁴ Vgl. Better Business Bureau, New Research Shows That Identity Theft Is More Prevalent Offline with Paper than Online, 26.01.2005. Online in Internet: URL: <http://www.bbb.org/alerts/article.asp?ID=565> [Stand 28.04.2008]
- ¹⁵ Vgl. Spiegel Online, Rund 500 Computer verschwunden, 20.03.2008. Online in Internet: URL: <http://www.spiegel.de/netzwelt/tech/0,1518,542632,00.html> [Stand 28.04.2008]
- ¹⁶ Ebenda.
- ¹⁷ Deutscher Bundestag, Kleine Anfrage, Computerverluste in Bundesbehörden, Drucksache 16/8673, 28.03.2008. Online in Internet: URL: <http://dip21.bundestag.de/dip21/btd/16/086/1608673.pdf> [Stand 28.04.2008]
- ¹⁸ Antwort der Bundesregierung auf die Kleine Anfrage des Abgeordneten Carl-Ludwig Thiele u. a. und der Fraktion der FDP, BT-Frucksache 16/8673, 14.04.2008. Online in Internet: URL: http://www.carl-ludwig-thiele.de/files/3185/Antwort_KIA_Computerverluste.pdf [Stand 28.04.2008]
- ¹⁹ Vgl. Spiegel Online, US-Zöllner durchstöbern Laptops und Handys, 07.02.2008. Online in Internet: URL: <http://www.spiegel.de/netzwelt/mobil/0,1518,533812,00.html> [Stand 28.04.2008]; vgl. Heise online, Verdachtsgrund Laptop, 08.04.2008. Online in Internet: URL: <http://www.heise.de/tr/Verdachtsgrund-Laptop--/artikel/106009> [Stand 28.04.2008]
- ²⁰ Vgl. J. Alex Halderman, Seth D. Schoen, Nadia Heninger u. a., Lest We Remember: Cold Boot Attacks on Encryption Keys, Princeton University 02.04.2008. Online in Internet: URL: <http://citp.princeton.edu/pub/coldboot.pdf> [Stand 28.04.2008]; Vgl. Internetseite des Center for Information Technology Policy der Princeton University. Online in Internet: URL: <http://citp.princeton.edu/memory/> [Stand 28.04.2008]
- ²¹ FDP-Bundestagsfraktion, Auch geheime Informationen vom Datenklau in Behörden betroffen, 21.04.2008. Online in Internet: URL: http://www.fdp-fraktion.de/webcom/show_article.php/c-334/nr-1304/p-1/i.html [Stand 28.04.2008]
- ²² Petra Pau, Datenverlust ist unberechenbar, Presseerklärung vom 20.04.2008. Online in Internet: URL: http://www.petrapau.de/aktuell/presse/080420_computer.htm [Stand 28.04.2008]
- ²³ FDP-Bundestagsfraktion, Auch geheime Informationen vom Datenklau in Behörden betroffen, 21.04.2008. Online in Internet: URL: http://www.fdp-fraktion.de/webcom/show_article.php/c-334/nr-1304/p-1/i.html [Stand 28.04.2008]
- ²⁴ Netzzeitung.de, Geheime Regierungsdaten sind weg, 19.04.2008. Online in Internet: URL: <http://www.netzzeitung.de/politik/deutschland/982977.html> [Stand 28.04.2008]