



Über ENISA

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) ist eine Agentur der Europäischen Union, die zur Förderung des Binnenmarktes eingerichtet wurde. Die ENISA dient den Mitgliedstaaten und EU-Institutionen als Kompetenzzentrum für Netz- und Informationssicherheit, das Ratschläge und Empfehlungen gibt und als Schaltstelle für den Austausch von Informationen über bewährte Verfahren fungiert. Darüber hinaus knüpft die Agentur Kontakte zwischen den EU-Institutionen, Mitgliedstaaten sowie Vertretern von Privatwirtschaft und Industrie.

Kontaktangaben:

Wenn Sie Kontakt zu ENISA aufnehmen möchten oder allgemeine Fragen zum Thema Sensibilisierung für Informationssicherheit haben, wenden Sie sich bitte an:

Isabella Santa, Senior Expert Awareness Raising

E-Mail: awareness@enisa.europa.eu

Internet: <http://www.enisa.europa.eu/>

Rechtliche Hinweise

Bitte beachten Sie, dass diese Veröffentlichung die Ansichten und Auslegungen der Autoren und Herausgeber wiedergibt, sofern nicht anders angegeben. Diese Veröffentlichung ist nur dann als Veröffentlichung der ENISA oder von Einrichtungen der ENISA anzusehen, wenn sie gemäß der Verordnung (EG) Nr. 460/2004 zur Errichtung der ENISA angenommen wurde. Die vorliegende Veröffentlichung gibt nicht notwendigerweise den neuesten Stand wieder und kann von Zeit zu Zeit aktualisiert werden.

Drittquellen werden angegeben, soweit erforderlich. Die ENISA ist nicht verantwortlich für den Inhalt der externen Quellen, einschließlich externer Websites, auf die in dieser Veröffentlichung Bezug genommen wird.

Die vorliegende Veröffentlichung ist lediglich zu Aufklärungs- und Informationszwecken gedacht. Weder die ENISA noch Dritte, die in ihrem Auftrag handeln, haften für die mögliche Nutzung der in dieser Veröffentlichung enthaltenen Informationen.

Nachdruck mit Quellenangabe gestattet.

© Europäische Agentur für Netz- und Informationssicherheit (ENISA), 2008



Sicherer Umgang mit USB-Speichersticks

Juni 2008

Danksagung

Mehrere Personen haben auf unterschiedliche Weise direkt oder indirekt zu diesem Werk beigetragen.

Der Autor dankt insbesondere Dror Todress von SanDisk und Louis Marinos von ENISA für die zeitnahe Unterstützung, die wertvollen Beiträge und Materialien zur Anfertigung der vorliegenden Arbeit.

Ebenso möchte der Autor all denjenigen danken, die mit informellen Rezensionen, hilfreichen Erläuterungen und Beobachtungen, Anregungen und Lösungsvorschlägen zu dieser Veröffentlichung beigetragen haben und ohne deren wertvolle Hilfe dieses Dokument unvollständig und fehlerhaft wäre.

Inhaltsverzeichnis

ÜBER ENISA	2
DANKSAGUNG	4
ZUSAMMENFASSUNG	7
TEIL 1: USB-SPEICHERSTICKS UND DEREN SICHERHEIT	9
DER GEBRAUCH MOBILER GERÄTE.....	10
USB-SPEICHERSTICKS	11
EINE DEFINITION	11
EINIGE VORFÄLLE DER JÜNGEREN VERGANGENHEIT.....	13
DIE GRÖßTEN GEFAHREN BEI USB-SPEICHERSTICKS.....	14
UNTERNEHMENSBELANGE	15
FOLGEN FÜR DIE SICHERHEIT	16
RISIKEN UND BEDROHUNGEN.....	17
TEIL 2: LEITFADEN FÜR BEWÄHRTE VERFAHREN	19
UNSERE LEITLINIEN.....	20
EMPFEHLUNGEN SOWIE MÖGLICHE SOFTWARE- UND HARDWARELÖSUNGEN.....	20
CHECKLISTE	26
TEIL 3: SICHERHEITSTIPPS UND NUTZEFFEKTE FÜR UNTERNEHMEN	27
PRAKTISCHE TIPPS ZUR VERHINDERUNG DES DIEBSTAHLS VON USB-SPEICHERSTICKS	28
NUTZEFFEKTE	28
FAZIT	29
LITERATURANGABEN UND VERWEISE AUF WEITERE QUELLEN	30

Zusammenfassung

In den vergangenen Jahren ist es für Endbenutzer in Unternehmen immer wichtiger geworden, uneingeschränkt mobil zu sein und stets Anschluss zu haben, um berufliche Aufgaben ohne Abstriche an der Produktivität auch unterwegs oder von zu Hause aus erledigen zu können. Unternehmensmitarbeiter müssen in der Lage sein, Dateien zwischen einem Computer und einem mobilen Laufwerk zu synchronisieren, um wichtige Daten zu sichern und auf diese auch außer Haus bzw. auf anderen PCs zugreifen zu können⁽¹⁾. Entsprechend hat sich der Gebrauch mobiler Geräte, beispielsweise von Laptop- und Notebook-Rechnern, USB (Universal Serial Bus)-Speichersticks, PDAs (Personal Digital Assistants), Mobiltelefonen der neueren Generation und weiterer mobiler Kommunikationstechnik, in den letzten Jahren enorm entwickelt⁽²⁾.

Insbesondere sind Datenträger wie USB-Speichersticks, die mittlerweile über beträchtliche Speicherkapazitäten verfügen, aus dem geschäftlichen Umfeld praktisch nicht mehr wegzudenken⁽³⁾. Allerdings mangelt es derartigen Geräten gewöhnlich an Sicherheits-, Kontroll- und Managementtools und unterliegt ihre Nutzung zumeist nicht einer Unternehmenspolitik, die Audit, Datensicherung, Verschlüsselung bzw. Sachmittelverwaltung vorsieht.

Vorfälle der jüngeren Zeit ließen bei Unternehmen und Institutionen Bedenken aufkommen und gaben zu verstehen, dass es neuer Strategien und Technologien bedarf, um auf persönlichen USB-Speichersticks gespeicherte Daten zu sichern⁽⁴⁾. Häufig jedoch erweisen sich die von den Organisationen unternommenen Maßnahmen zur Sicherung der auf mobilen Geräten abgelegten Informationen als unzureichend. Unternehmen, deren Daten hoch sensibel sind bzw. strenger Regulierung unterliegen, sollten deshalb Kontrollmechanismen für den Gebrauch von Plug-and-Play-Geräten erwägen. Die erste Verteidigungslinie gegen Sicherheitsverletzungen ist indes die Sensibilisierung für Risiken und geeignete Sicherungsmaßnahmen⁽⁵⁾.

Der vorliegende Beitrag fasst im Überblick zusammen, welche geschäftlichen Daten anfällig für Sicherheitsverletzungen sind, und stellt die potenziellen Risiken im Zusammenhang mit dem unbedachten Gebrauch von USB-Speichersticks durch Unternehmensmitarbeiter oder der Nutzung für weniger legitime Zwecke wie dem Datenschmuggel heraus. Darüber hinaus werden Leitlinien für bewährte Verfahren aufgeführt, die dem Leser helfen sollen, Hindernisse in der eigenen Organisation zu überwinden. Der erste Schritt besteht darin, eindeutige Sicherheitsgrundsätze festzulegen und sie den Mitarbeitern zu vermitteln.

Diese Abhandlung richtet sich an IT-Abteilungen, insbesondere die für Informationstechnologie zuständigen Leitungs- und Fachkräfte, um sie in die Lage zu versetzen, Informationen im Intranet ihrer Organisation zu sichern und Möglichkeiten zu schaffen, auf mobilen Geräten in das bzw. aus dem Unternehmen gebrachte Daten sicher zu verwalten. Ebenso soll sie Endbenutzer im Unternehmensbereich ganz allgemein für die mit dem Einsatz von USB-Speichersticks verbundenen Risiken sensibilisieren.

Im vorliegenden Dokument bleiben die einschlägigen rechtlichen Aspekte unberücksichtigt. Ebenso wenig sollte diese Abhandlung als umfassende Informationsquelle zu sämtlichen Risiken bezüglich des Gebrauchs privater USB-Speichersticks zu beruflichen Zwecken oder aber als technischer Leitfaden für Sicherheitsstandards bzw. -lösungen angesehen werden.

⁽¹⁾ DataTraveler Secure and DataTraveler Secure — Privacy Edition White Paper, *Kingston Technology*, Rev. 2.0, Juni 2007.

⁽²⁾ Determine the appropriate level of ITAM controls for mobile assets, *Jack Heine, Gartner*, 15. November 2005.

⁽³⁾ Seven steps to secure USB drives, *SanDisk*, Juli 2007.

⁽⁴⁾ Seven steps to secure USB drives, *SanDisk*, Juli 2007.

⁽⁵⁾ Leitfaden für die Praxis: Wege zu mehr Bewusstsein für Informationssicherheit, *ENISA*, Juni 2006.

TEIL 1:

USB-Speichersticks und deren Sicherheit



Der Gebrauch mobiler Geräte

Im digitalen Zeitalter, das heute unser Leben und unsere Arbeit prägt, ist es für Endbenutzer aus dem Unternehmensbereich wichtig, mit wenig Ballast unterwegs und dabei überall entsprechenden Anschluss zu haben. Infolgedessen ist im geschäftlichen Alltag eine zunehmende Zahl mobiler Geräte wie Laptop- und Notebook-Rechner, USB (Universal Serial Bus)-Speichersticks, PDAs (Personal Digital Assistants), Mobiltelefone der neueren Generation und weitere mobile Kommunikationstechnik in Gebrauch.



Wenn Mitarbeiter mobile Geräte nutzen, mit Daten unterwegs sind und sich Arbeit mit nach Hause nehmen, sind Unternehmen dauerhaft vom Risiko ungeschützter Daten auf nicht gesicherten USB-Speichersticks betroffen. Die Folgen können verheerend sein: Rufschädigung, Verlust von Arbeitsplätzen, entgangene Gewinne⁽⁶⁾. Beispiele für Daten, die üblicherweise auf diesen Geräten gespeichert und transportiert werden, sind Kundendaten, Finanzzahlen, Geschäftspläne, Patientenakten und andere vertrauliche Informationen. Eine beträchtliche Zahl der Endbenutzer ist sich jedoch nicht bewusst, welchen Sicherheitsrisiken sie dabei ausgesetzt sind, wie jüngste Vorfälle deutlich gezeigt haben⁽⁷⁾.



So wurde einem Finanzamtsmitarbeiter im Vereinigten Königreich ein Laptop mit Daten von rund 2000 Bürgern mit steuerbegünstigten Sparkonten, sogenannten ISA-Konten, gestohlen; dem britischen Finanzamt kamen die personenbezogenen Daten von 6500 Empfängern von Privatpensionen abhanden; neun Versorgungswerke (Trusts) des britischen staatlichen Gesundheitsdienstes NHS verloren ihre auf CD gespeicherten Patientenakten; Personendaten von 1500 Studenten gingen auf dem Postweg verloren; in den USA kamen die Daten

⁽⁶⁾ DataTraveler for Enterprise, Kingston, 2008, abrufbar unter http://www.kingston.com/flash/DataTravelers_enterprise.asp (zuletzt aufgerufen am 30. Mai 2008).

⁽⁷⁾ McAfee encrypted USB – Data sheet, McAfee.

von drei Millionen britischen Fahrschülern abhanden ⁽⁸⁾; ein USB-Speicherstick mit den Namen, Noten und Sozialversicherungsnummern von 6500 ehemaligen Studenten wurde gestohlen ⁽⁹⁾; USB-Speichersticks mit geheimen Militärintformationen der US-Armee wurden auf einem Basar bei Bagram (Afghanistan) zum Kauf angeboten ⁽¹⁰⁾.

Die Tatsache, dass das Schadenspotenzial aus dem Verlust bzw. Diebstahl sensibler Unternehmensdaten Tag für Tag exponentiell wächst, unterstreicht die Forderung nach geeigneten Sicherungsstrategien, die diese kleinen mobilen Datenträger einbeziehen ⁽¹¹⁾. Der Verlust von Daten ist nicht nur ein IT- bzw. Sicherheitsproblem; er ist ein Geschäftsfaktor, der sich bis in den fernsten Winkel eines Unternehmens auswirkt ⁽¹²⁾.

Dem von McAfee in Auftrag gegebenen Datamonitor-Bericht zufolge gaben 60 % der 1400 weltweit befragten IT-Entscheidungsträger an, bereits ein Datenleck erlitten zu haben, wobei nur 6 % mit Sicherheit behaupten konnten, in den vergangenen zwei Jahren frei von Datenleck-Problemen geblieben zu sein. Zudem waren 61 % der Meinung, dass Datenlecks das Werk von Unternehmensangehörigen selbst sind ⁽¹³⁾.

USB-Speichersticks

Eine Definition

USB-Speichersticks sind Lösungen für das Speichern und Verwalten von Unternehmensdaten innerhalb und außerhalb des Unternehmensumfelds. Es handelt sich dabei um Plug-and-Play-fähige, tragbare Speichergeräte auf Basis eines Flash-Speichers, die sich dank ihrer geringen Größe und ihres geringen Gewichts an einem Schlüsselring befestigen lassen. USB-Sticks wurden erstmals im Jahr 2000 verkauft.

Für mobiles Fachpersonal aus Unternehmen und Verwaltungen sind USB-Speichersticks ein leistungsfähiges und beliebtes Werkzeug, das sich durch folgende Merkmale auszeichnet:

- ✓ klein und leicht
- ✓ hohe Übertragungsgeschwindigkeit — 24MB/s
- ✓ große Speicherkapazität
- ✓ niedriger Preis
- ✓ Plug-and-Play-Funktionalität.



Ihr Gebrauch verbreitet sich weiter und die Nachfrage nach neuen Geräten ist hoch. Im Jahr 2006 prognostizierte Gartner einen Anstieg der gelieferten Stückzahlen auf über 114 Millionen ⁽¹⁴⁾. 2007 wurden 85 Millionen Stück verkauft, wobei sich nur wenige der Käufer Gedanken über die

⁽⁸⁾ „Timetable of missing data blunders“, The Times, 20. Februar 2008; „Disc listing foreign criminals lost for year“, The Times, 20. Februar 2008.

⁽⁹⁾ „Small drives cause big problems“, John Swarts, USA Today, 16. Juni 2006.

⁽¹⁰⁾ „US military secrets for sale at Afghanistan bazaar“, Watson, Los Angeles Times, 10. April 2006.

⁽¹¹⁾ Seven steps to secure USB drives, SanDisk, Juli 2007 und Mobile device security in 2006, Forrester, Februar 2006.

⁽¹²⁾ Getting started with McAfee host data loss prevention, McAfee, 2008.

⁽¹³⁾ „New report chronicles the cost of data leaks“, Physorg.com, 2007, abrufbar unter <http://www.physorg.com/news96708147.html> (zuletzt aufgerufen am 2. Juni 2008).

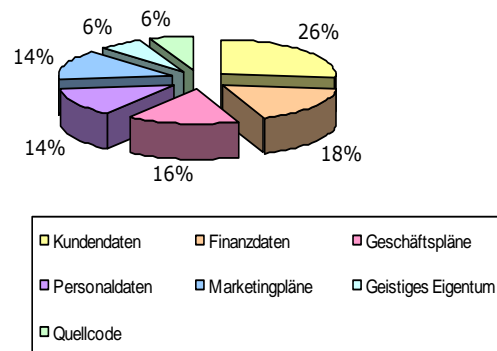
⁽¹⁴⁾ Dataquest insight: USB flash drive market trends, worldwide, 2001–2010, Joseph Unsworth, Gartner, 20. November 2006; Forecast: USB flash drives, worldwide, 2001–2011, Joseph Unsworth, Gartner, 24. September 2007.

Sicherheitsaspekte der Sticks machten ⁽¹⁵⁾. Eine Gartner-Untersuchung ergab, dass 22 % der USB-Speichersticks an Unternehmen verkauft werden und etwa 80–90 % über keine Verschlüsselung verfügen ⁽¹⁶⁾.

USB-Speichersticks sind eine preiswerte und praktische Methode, Daten aus dem Rechner zu übernehmen – weit einfacher, als einen Laptop oder ein Festplattenlaufwerk mitzuführen ⁽¹⁷⁾. Eine neuere Studie von SanDisk ergab Folgendes ⁽¹⁸⁾:

- ✓ Die meisten geschäftlichen Endbenutzer (77 %) haben bereits einen privaten USB-Speicherstick für berufliche Zwecke genutzt. Den Angaben zufolge ist sich nur jeder Fünfte von ihnen der Risiken bewusst, die ein Mitführen von Unternehmensdaten auf USB-Speichersticks birgt (21 %), was ein beträchtliches Potenzial für Datenverluste erkennen lässt.
- ✓ IT-Entscheidungsträger gehen davon aus, dass ca. 35 % der Belegschaft ihrer Organisationen private USB-Speichersticks zum Transport von Unternehmensdaten gebrauchen wird.
- ✓ Etwa 41 % IT-Entscheidungsträger sehen das gegenwärtige Ausmaß des Gebrauchs von USB-Speichersticks in ihrer Organisation mit Unbehagen.

Unternehmensdaten auf USB-Speichersticks



Einer Studie des Ponemon Institute zufolge kopieren mehr als die Hälfte aller Angestellten sensible Informationen auf USB-Speichersticks, obwohl in 87 % der befragten Unternehmen Leitlinien gelten, die ein solches Vorgehen verbieten ⁽¹⁹⁾. Diese Diskrepanz lässt erkennen, dass das Wissen der Mitarbeiter um die Grundsätze ihres Unternehmens zum Gebrauch von USB-Speichersticks sehr begrenzt ist. Ein Blick auf die Schulungen, die Unternehmen zu ihren Leitlinien im Zusammenhang mit der Nutzung von USB-Sticks anbieten, lässt uns zu der Überzeugung kommen, dass hier eine eindeutige Korrelation besteht. Wie die Untersuchung durch SanDisk zeigt, werden Mitarbeiter unterschiedlich oft zur Unternehmenspolitik hinsichtlich des Gebrauchs von USB-Speichersticks geschult, nämlich einmal jährlich (33 %); mehr als einmal im Jahr (24 %); nur, wenn sie neu in das Unternehmen kommen (22 %) bzw. wenn eine Schulung verlangt wird (17 %) oder aber überhaupt nicht (3 %) ⁽²⁰⁾. Daher ist unbedingt zu unterstreichen, dass sich Maßnahmen der Aufklärung und Sensibilisierung für die mit dem Einsatz von USB-Speichersticks verbundenen Risiken ganz wesentlich auf das Mitarbeiterverhalten auswirken, da sie einen sicheren Gebrauch im beruflichen Alltag fördern.

⁽¹⁵⁾ „Thumb drives are too often the victims of convenience“, John Zyskowski, GCN, 14. Dezember 2006, abrufbar unter http://www.gcn.com/online/vol1_no1/44136-1.html (zuletzt aufgerufen am 30. Mai 2008).

⁽¹⁶⁾ „Data breaches are 'everyday incidents'“, Matt Chapman, vnunet.com, 15. November 2007, abrufbar unter <http://www.vnunet.com/vnunet/news/2203540/security-breaches-everyday> (zuletzt aufgerufen am 30. Mai 2008).

⁽¹⁷⁾ „The portable risk of high capacity USB drives“, Allan Leinwand, GigaOM, 5. Dezember 2007, abrufbar unter <http://gigaom.com/2007/12/05/the-portable-risk-of-high-capacity-usb-drives/> (zuletzt aufgerufen am 30. Mai 2008).

⁽¹⁸⁾ SanDisk endpoint security survey, SanDisk, April 2008.

⁽¹⁹⁾ Survey of US IT practitioners reveals data security policies not enforced, Ponemon Institute and RedCannon Security, Dezember 2007, abrufbar unter http://www.ponemon.org/press/RC_PonemonSurvey_FINAL.pdf (zuletzt aufgerufen am 2. Juni 2008).

⁽²⁰⁾ SanDisk Endpoint Security Survey, SanDisk, April 2008.

Einige Vorfälle der jüngeren Vergangenheit

Auch in jüngerer Zeit kommt es wiederholt zu Vorfällen, da USB-Speichersticks immer wieder verloren, verlegt, ohne Erlaubnis ausgeliehen oder gar gestohlen werden⁽²¹⁾. Hier einige der Vorfallsberichte⁽²²⁾:

- ✓ Dem schwedischen Militär wurde ein an einem öffentlichen Rechner zurückgelassener USB-Speicherstick ausgehändigt. Ein Bürger hatte den Stick, auf dem sich zwei der Geheimhaltung unterliegende Dokumente befanden, in einem öffentlichen Computer-Center in Stockholm entdeckt. Ein Militärangestellter meldete, dass der verlegte USB-Speicherstick ihm gehöre. Der Stick enthielt sowohl nicht vertrauliche als auch geheime Informationen zu Bedrohungen durch unkonventionelle Spreng- und Brandvorrichtungen (USBV) und Minen in Afghanistan⁽²³⁾.
- ✓ Dem staatlichen britischen Gesundheitsdienst gingen zwei nicht verschlüsselte USB-Speichersticks mit den Krankendaten von 148 Patienten verloren. Erst kurz zuvor waren dem Finanzamt des Vereinigten Königreichs (HMRC) zwei unverschlüsselte CD-ROM mit Daten von 25 Millionen Steuerzahlern abhanden gekommen⁽²⁴⁾.
- ✓ Anfang Mai 2008 kam es zum Verlust eines USB-Speichersticks mit Krankenhausakten des Prince of Wales Hospital (PWH) Hongkong. Bei den darauf gespeicherten Dateien handelte es sich überwiegend um Arbeitsdokumente mit personenbezogenen Daten von Patienten wie Namen, Ausweisnummern und Laborwerten. Einer Schätzung zufolge waren 10 000 Krankenakten betroffen⁽²⁵⁾.
- ✓ Während des Urlaubs in Madagaskar verlor ein Mathematikprofessor einen USB-Speicherstick mit Informationen über 8000 Studenten der texanischen A&M University Corpus Christi. Auf dem USB-Stick befanden sich neben den Sozialversicherungsnummern der Studenten und weiteren Angaben auch Informationen über alle im Frühjahrs-, Sommer- und Herbst-Trimester 2006 von ihnen belegten Hauptfächer sowie die Einstufungen der Studenten. Das Laufwerk gehörte dem Chairman der Fakultät für Mathematik, der es auf seiner zweiwöchigen Urlaubsreise bei sich hatte und den Verlust erst beim Packen für die Heimreise bemerkte⁽²⁶⁾.
- ✓ USB-Speichersticks mit Geheiminformationen der US-Armee standen auf einem Basar am Rande der afghanischen Stadt Bagram zum Verkauf. Auf den Sticks befanden sich unter anderem Einsatzpläne und weitere Dokumente, denen sich die Namen und Sozialversicherungsnummern von nahezu 700 US-Militärangehörigen entnehmen ließen. Diebe von Identitätsdaten könnten diese Informationen dazu nutzen, auf den Namen von

⁽²¹⁾ DataTraveler Secure and DataTraveler Secure — Privacy Edition White Paper, Kingston Technology, Rev. 2.0, Juni 2007.

⁽²²⁾ Weiterer Lesestoff zu Sicherheitsvorfällen findet sich in „Educational security incidents (ESI) — Sometimes the free flow of information is unintentional“, abrufbar unter <http://www.adamdodge.com/esi/month/2008/01>; „Privacy and identity theft“, Dave Jevans, IronKey, abrufbar unter <http://blog.ironkey.com/?cat=9&paged=2> (zuletzt aufgerufen am 20. Mai 2008); und „Thumb drives are too often the victims of convenience“, John Zyskowski, GCN, 14. Dezember 2006, abrufbar unter http://www.gcn.com/online/vol1_no1/44136-1.html (zuletzt aufgerufen am 30. Mai 2008); Plugging the leaks: best practices in endpoint security, SanDisk, 2008.

⁽²³⁾ „Privacy and identity theft“, Dave Jevans, IronKey, abrufbar unter <http://blog.ironkey.com/?cat=9&paged=2> (zuletzt aufgerufen am 20. Mai 2008).

⁽²⁴⁾ „Privacy and identity theft“, Dave Jevans, IronKey, abrufbar unter <http://blog.ironkey.com/?cat=9&paged=2> (zuletzt aufgerufen am 20. Mai 2008).

⁽²⁵⁾ „Prince of Wales Hospital announced an incident of loss of USB flash drive containing hospital files“, Pressemitteilungen, 6. Mai 2008, abrufbar unter <http://www.info.gov.hk/gia/general/200805/06/P200805060232.htm> (zuletzt aufgerufen am 30. Mai 2008).

⁽²⁶⁾ „TAMU Corpus Christi prof loses flash drive with 8 000 student records“, Paul McCloskey, Campus Technology, 18. August 2007, abrufbar unter <http://campustechnology.com/articles/48635> (zuletzt aufgerufen am 30. Mai 2008).

- Soldaten Kreditkartenkonten anzulegen ⁽²⁷⁾.
- ✓ Rund 13 000 Mitarbeiter des Pharmakonzerns Pfizer Inc., darunter 5000 aus Connecticut, sahen ihre personenbezogenen Daten offengelegt, als ein Firmen-Laptop samt USB-Speicherstick gestohlen wurde. Die Datenschutzverletzung, die sich am 12. Mai 2008 ereignete, war bereits der zweite derartige Vorfall, der Mitarbeiter von Pfizer betraf, und der sechste, der im Zeitraum eines Jahres seit Mai 2007 an die Öffentlichkeit gelangte. Pfizer machte seinen Firmenangehörigen im vergangenen Jahr mehr als 65 000 Mitteilungen über Datenschutzverletzungen, wovon über 10 000 an Mitarbeiter in Connecticut gingen. Nach Aussage des Unternehmens waren auf dem Laptop keine Sozialversicherungsnummern gespeichert, doch wurden möglicherweise Namen, Wohnanschriften, private Telefonnummern, Mitarbeiternummern, Funktions- und Gehaltsangaben der Beschäftigten preisgegeben. Weitere womöglich verlorene Daten betrafen Angaben zu den Abteilungen, in denen die Firmenangehörigen eingesetzt waren, sowie Namen und Tätigkeitsbeschreibungen von Mitarbeitern und Vorgesetzten ⁽²⁸⁾.
 - ✓ Aus dem Auto einer Prüfungsorganisatorin der texanischen Schulorganisation Spring ISD wurde während eines kurzen Stopps auf der Heimfahrt von der Arbeit ein Laptop-Computer mit den personenbezogenen Daten von rund 8000 Schülern gestohlen. Neben dem Dienst-Laptop der Schulmitarbeiterin ließen die Täter auch einen externen USB-Speicherstick mitgehen. Auf dem USB-Stick waren die Sozialversicherungsnummern und personenbezogene Informationen der Schüler, ihre Geburtsdaten sowie Angaben zu den von ihnen besuchten Schulen und erreichten Noten gespeichert. Außerdem befanden sich auf dem Laufwerk die Ergebnisse des Leistungsvergleichs für Schüler im Bundesstaat Texas (Texas Assessment of Knowledge and Skills Test) ⁽²⁹⁾.
 - ✓ Am 26. Mai 2006 wurden nach dem Diebstahl des USB-Speichersticks eines Professors der University of Kentucky die Personendaten, darunter Namen, Noten und Sozialversicherungsnummern, von 6500 aktiven wie auch ehemaligen Studenten der Universität als gestohlen gemeldet. Der Stick wurde bisher nicht wieder aufgefunden, und die Universität überprüft derzeit ihre Verfahrensweisen für den Gebrauch von USB-Speichersticks ⁽³⁰⁾.
 - ✓ In Oktober 2005 teilte das Wilcox Memorial Hospital in Lihue, Hawaii, 120 000 aktuellen und früheren Patienten mit, dass ein USB-Speicherstick mit ihren Personendaten (Namen, Anschriften, Sozialversicherungs- und Krankenaktensnummern) verloren gegangen sei. Er hat sich bis heute nicht wieder angefangen. Der Gebrauch von USB-Sticks, die erst einige Monate zuvor im Krankenhaus eingeführt worden waren, ist seitdem verboten.

Auch wenn es sich um verschiedenartige Vorfälle handelt, war die Ursache stets dieselbe: ein unzureichendes Problembewusstsein bezüglich der Risiken, die der Gebrauch von USB-Speichersticks zum Transport sensibler Daten in sich birgt, und eine nicht bis zur Endbenutzerebene hin konsequente Sicherheitspolitik („Endpoint Security“).

Die größten Gefahren bei USB-Speichersticks

Der unkontrollierte Gebrauch von USB-Speichersticks ist eine wesentliche Gefahr, da er eine nicht quantifizierbare, aber dennoch signifikante Bedrohung der Vertraulichkeit von Informationen darstellt. Im Hinblick auf die Sicherung der in Unternehmen zur Anwendung kommenden USB-

⁽²⁷⁾ „Afghan market sells US military flash drives“, Paul Watson, Los Angeles Times, 18. April 2006, abrufbar unter <http://www.veteransforcommonsense.org/ArticleID/7120> (zuletzt aufgerufen am 28. Mai 2008).

⁽²⁸⁾ „Another laptop stolen from Pfizer, employee information compromised“, Lee Howard, 12. Mai 2008, abrufbar unter <http://attrition.org/dataloss/2008/05/pfizer01.html> (zuletzt aufgerufen am 30. Mai 2008).

⁽²⁹⁾ „Spring students' info at risk after laptop theft“, KHOU.com Korrespondentenbericht, 16. Mai, 2008, abrufbar unter <http://attrition.org/dataloss/2008/05/spring01.html> (zuletzt aufgerufen am 30. Mai 2008).

⁽³⁰⁾ „Small drives cause big problems“, Jon Swartz, USA Today, 16. August 2006, abrufbar unter http://www.usatoday.com/tech/news/computersecurity/2006-08-15-thumbdrives-stolen_x.htm (zuletzt aufgerufen am 27. Mai 2008).

Speichersticks sollten deshalb folgende Aspekte bedacht werden:

- ✓ Aufbewahrung: USB-Speichersticks werden gewöhnlich in Handtaschen, Rucksäcken, Laptop-Taschen, Jackett- oder Hosentaschen aufbewahrt oder aber unbeaufsichtigt am Arbeitsplatz zurückgelassen.
- ✓ Gebrauch: Unternehmensdaten werden auf privaten, nicht gesicherten Sticks abgelegt und befinden sich ständig in Bewegung. Mit der zunehmenden Akzeptanz von USB-Speichersticks bei den IT-Abteilungen von Organisationen wächst die Wahrscheinlichkeit von Sicherheitsverletzungen und Datenverlusten. Viele Geschäftsleitungen verfolgen eine strenge Politik bezüglich USB-Sticks; in einigen Unternehmen ist ihr Gebrauch sogar ganz verboten, um das Risiko zu minimieren. Einen Beitrag zur Risikominderung könnten Softwarelösungen liefern, die es gestatten, den Datenaustausch zwischen Speicherstick und PC bzw. Server aufzuzeichnen und in einer zentralen Datenbank zu protokollieren ⁽³¹⁾.
- ✓ Kosten: die durchschnittlichen Kosten je Datenschutzverletzung reichen von unter 100 000 USD bis zu rund 2,5 Millionen USD ⁽³²⁾.
- ✓ Art der gespeicherten Dokumente: öffentliche, interne, vertrauliche, eingeschränkt zugängliche und geschützte Dokumente. Je nach Wirtschaftsbranche (Banken, Versicherungen usw.) unterscheidet sich die Art der gespeicherten Informationen: Endbenutzer in Unternehmen legen auf den USB-Speichersticks zumeist Kundendaten ab (25 %), gefolgt von Finanzdaten (17 %), Geschäftsplänen (15 %), Personaldaten (13 %), Marketingplänen (13 %), geistigem Eigentum (6 %) und Quellcode (6 %) ⁽³³⁾.

Arten von Dokumenten

- ❖ *Öffentliche Informationen: sind jedermann zugänglich.*
- ❖ *Interne Informationen: bewegen sich frei innerhalb der Organisation.*
- ❖ *Vertrauliche Informationen: bewegen sich zwischen einzelnen Abteilungen und/oder Geschäftsbereichen und unterliegen einer Geheimhaltungsvereinbarung.*
- ❖ *Eingeschränkt zugängliche Informationen: werden nur zwischen ausgewählten Mitarbeitern des Unternehmens ausgetauscht.*
- ❖ *Geschützte Informationen: werden um jeden Preis gesichert.*

Unternehmensbelange

Im Folgenden sind einige der wichtigsten Aspekte aufgeführt, die Unternehmen im Zusammenhang mit dem Gebrauch von USB-Speichersticks berühren ⁽³⁴⁾.

- ✓ Datenlecks: Um Datenlecks einzugrenzen, sollten Organisationen den Gebrauch von USB-Speichersticks regulieren, um letztendlich nur die Verwendung vom Unternehmen selbst genehmigter USB-Sticks zuzulassen ⁽³⁵⁾.
- ✓ Einhaltung von Regulierungs- und Sicherheitsvorschriften: Unternehmen, die für einen sicheren Umgang mit USB-Speichersticks sorgen, wird es leichter fallen, den drei

⁽³¹⁾ USB flash drive market trends, worldwide, 2001–2010, Joseph Unsworth, November 2006, Gartner.

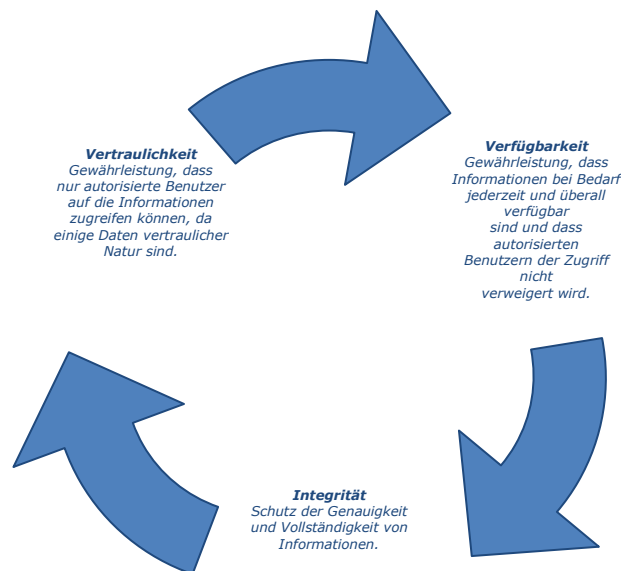
⁽³²⁾ SanDisk Endpoint Security Survey, SanDisk, April 2008.

⁽³³⁾ SanDisk Endpoint Security Survey, SanDisk, April 2008.

⁽³⁴⁾ Seven steps to secure USB drives, SanDisk, Juli 2007.

⁽³⁵⁾ USB flash drive protection, Ron LaPedis, SanDisk, Disk Encryption Forum, 13. Februar 2007.

Sicherheitsanforderungen (Vertraulichkeit, Verfügbarkeit und Integrität) sowie einer Reihe von Sicherheitsstandards bzw. Compliance-Regelwerken (z. B. Sarbanes-Oxley, PCI-Standard zum Schutz von Kreditkartendaten) zu entsprechen;



- ✓ Kosten bei Datenverlust und Supportleistungen: Eine geeignete Sicherheitspolitik könnte den Unternehmen helfen, ihre Daten in Fällen von Diebstahl oder Verlust – die selbst bei funktionierenden Sicherungsmaßnahmen nicht auszuschließen sind – wiederherzustellen, was sich in geringeren Betriebs- und Supportkosten auswirkt.

Folgen für die Sicherheit

Sobald Mitarbeiter geschäftliche Informationen auf privaten und ungesicherten USB-Speichersticks speichern, setzen sie ihren Arbeitgeber einem Risiko aus, selbst wenn sie sich im Firmengebäude aufhalten. Der Grad des Risikos und der möglichen Bedrohung ist jedoch noch höher, wenn sensible Informationen das Unternehmen verlassen, da sie dann noch leichter in falsche Hände geraten könnten ⁽³⁶⁾.

USB-Speichersticks sind ein wesentliches Sicherheitsrisiko, da sich Fälle von Verlust und Diebstahl häufen. Eine von der Sicherheitsfirma Vontu geförderte Studie zeigt auf, dass laut mehr als der Hälfte der 484 befragten Technologiefachleute USB-Sticks vertrauliche Informationen enthalten, die ungeschützt sind. Jeden Monat geht 20 % der Umfrageteilnehmer zufolge mindestens ein USB-Speicherstick mit Daten verloren. Für die Organisationen ist es dann eine schwere Aufgabe herauszufinden, wo sich die Daten befinden bzw. welchen Weg sie nehmen. Hinzu kommt, dass Mitarbeiter in den meisten Fällen gar nicht melden, dass sie einen Speicherstick vermissen. Ein Mitarbeiter kann Informationen im Wert von 25 Millionen USD auf einen USB-Stick



⁽³⁶⁾ Getting started with McAfee host data loss prevention, McAfee, 2008.

laden, der gerade einmal 25 USD kostet ⁽³⁷⁾.

Die von persönlichen Speichergeräten ausgehenden Sicherheitsbedrohungen lassen sich wie folgt klassifizieren ⁽³⁸⁾:

- ✓ Preisgabe von Daten durch Verlust, Diebstahl oder nicht korrekten Gebrauch der Geräte.
- ✓ unerlaubtes Auslesen von Daten.
- ✓ Einschleusen von Schadprogrammen.

Risiken und Bedrohungen

Betrachtet man den Gebrauch von ungesicherten privaten USB-Speichersticks und die Folgen der Übertragung und des Transports von Unternehmensdaten, geht die Zahl der Risiken und Bedrohungen nahezu ins Unendliche. Folgende Problemkreise lassen sich ausmachen:

- ✓ Datenlecks ⁽³⁹⁾: Welchen Schaden ein Unternehmen erleidet, wenn wertvolle Informationen nach außen dringen, lässt sich schwer abschätzen; sicher ist jedoch, dass das Problem zunimmt.
- ✓ Informationsverluste: USB-Speichersticks werden verlegt oder irgendwo vergessen. Mit hoher Wahrscheinlichkeit werden andere Personen, die zum Beispiel als vertraulich gekennzeichnete Informationen (wie Kunden- bzw. Mitarbeiterdaten) darauf sehen, sich diese für den privaten Gebrauch kopieren und den Stick schließlich neu formatieren, um ihn selber zu verwenden. Daraus könnte sich eine gesetzliche Haftung ergeben.
- ✓ Vertraulichkeit von Informationen: Geraten Informationen in die falschen Hände, erleidet ein Unternehmen Verluste, die weit über die reinen Wiederbeschaffungskosten für den Speicherstick hinausgehen.
- ✓ Integrität der Informationen: Inhalte werden geändert.
- ✓ Datenverfälschung: Wenn der USB-Speicherstick mit magnetischen Feldern in Berührung kommt oder nicht sauber vom Rechner entfernt bzw. abgemeldet wird. Im Normalfall wird es dem Betriebssystem gelingen, bei unerwartetem Verbindungsabbruch eine Beschädigung der Daten zu verhindern.
- ✓ Datensicherheit: Informationen werden aus dem Unternehmen geschmuggelt.
- ✓ Geschäfts-, Ruf- bzw. Imageschädigung: Ein gestohlener USB-Speicherstick kann dazu missbraucht werden, den Ruf, das Image bzw. das Geschäft eines Unternehmens zu beschädigen.
- ✓ Verlust der marktführenden Stellung.
- ✓ Infektion mit Viren/Würmern ⁽⁴⁰⁾: Werden Dateien zwischen zwei Rechnern ausgetauscht, besteht immer ein Risiko, dass auch Viren oder andere Schadprogramme übertragen werden. Im April 2008 lieferte HP eine Charge mit einem Virus infizierter USB-Speichersticks aus.
- ✓ Spyware ⁽⁴¹⁾: Der Host-Rechner kann von Programmen, die Daten ausspähen, befallen oder anderen Bedrohungen ausgesetzt sein. In diesem Fall ist eine softwarebasierte Sicherung, wie sie in handelsüblichen USB-Speichersticks mit Passwortschutz gebräuchlich ist, weniger verlässlich als eine hardwarebasierte Verschlüsselung, da ein Softwareschutz darauf

⁽³⁷⁾ „Small drives cause big problems“, Jon Swartz, USA Today, 16. August 2006, abrufbar unter http://www.usatoday.com/tech/news/computersecurity/2006-08-15-thumbdrives-stolen_x.htm (zuletzt aufgerufen am 27. Mai 2008).

⁽³⁸⁾ Seven steps to secure USB drives, SanDisk, Juli 2007.

⁽³⁹⁾ Understanding data leakage, Jay Heiser, Gartner, 21. August 2007; „Data-leak security proves to be too hard to use“, Infoworld.com, abrufbar unter http://www.infoworld.com/article/08/03/06/10NF-data-loss-prevention-problem_1.html (zuletzt aufgerufen am 2. Juni 2008).

⁽⁴⁰⁾ Im Rahmen der SanDisk-Erhebung zählten IT-Entscheidungsträger Viren bzw. Würmer zu den drei wichtigsten Sicherheitsbedrohungen, vgl.: SanDisk Endpoint Security Survey, SanDisk, April 2008. Siehe auch McAfee®VirusScan® USB — proven security that protects your USB drive against viruses, McAfee, 2006, abrufbar unter http://download.mcafee.com/products/manuals/en-us/vsusb_datasheet_2007.pdf (zuletzt aufgerufen am 30. Mai 2008).

⁽⁴¹⁾ Im Rahmen der SanDisk-Erhebung zählten IT-Entscheidungsträger Spyware zu den drei wichtigsten Sicherheitsbedrohungen, vgl.: SanDisk Endpoint Security Survey, SanDisk, April 2008.

- angewiesen ist, dass im Host-Rechner bestimmte Sicherheitsroutinen ablaufen;
- ✓ Schwachstellen in der Software ⁽⁴²⁾.
 - ✓ Betrug/Täuschung:
 - Erpressung;
 - Identitätsdiebstahl;
 - Diebstahl von geistigem Eigentum, Wirtschaftsgeheimnissen, geschützten Informationen.

⁽⁴²⁾ Im Rahmen der SanDisk-Erhebung zählten IT-Entscheidungsträger Softwareschwächen zu den drei wichtigsten Sicherheitsbedrohungen, vgl.: SanDisk Endpoint Security Survey, SanDisk, April 2008. Siehe auch New attacks: device vulnerabilities stand out, Avivah Litan, Don Dixon, Greg Young, Gartner, 21. Juni 2005.

TEIL 2:

Leitfaden für bewährte Verfahren



Unsere Leitlinien

Ausgehend von den ermittelten Daten und deren Auswertung enthält das vorliegende Dokument Leitlinien für bewährte Verfahren, die den Lesern und ihren Organisationen eine Hilfe bei der Minderung der Sicherheitsrisiken im Zusammenhang mit USB-Sticks sein können.

Der Leitfaden bewährter Verfahren setzt sich aus drei Teilen zusammen:

- ✓ Empfehlungen (*Recommendations*);
- ✓ mögliche Software- und Hardwarelösungen (*Software & Hardware solutions*);
- ✓ Checkliste (*Checklist*).



Empfehlungen sowie mögliche Software- und Hardwarelösungen

Eine Reihe Empfehlungen wie auch Software- und Hardwarelösungen sollen für einen sicheren Gebrauch von USB-Speichersticks sorgen.

- ✓ Führen Sie eine Methodik zur Risikobeurteilung ein, um die geeigneten Kontrollmechanismen zur Minimierung der Risiken über den gesamten Lebenszyklus der Geräte sicherzustellen⁽⁴³⁾. Anhand einer Risikobeurteilung wird es möglich, die Risiken und Kosten im Zusammenhang mit dem Gebrauch von USB-Speichersticks im Einzelnen zu verstehen und auf dieser Grundlage eine Strategie zum Schließen bestehender Lücken zu entwickeln⁽⁴⁴⁾;
- ✓ Führen Sie Sicherheitsgrundsätze bzw. -leitlinien für alle Aspekte der Nutzung von USB-Speichersticks sowie der Speicherung von Unternehmensdaten auf privaten USB-Sticks ein.

⁽⁴³⁾ Determine the appropriate level of ITAM controls for mobile assets, Jack Heine, Gartner, 15. November 2005.

⁽⁴⁴⁾ Mehr über Methoden des Risikomanagements bzw. der Risikobeurteilung finden Sie unter http://www.enisa.europa.eu/rmra/rm_ra_methods.html und http://www.enisa.europa.eu/rmra/rm_ra_tools.html

Meistens werden Maßnahmen als Reaktion auf einen Datenverlust ergriffen. Eine jüngere Untersuchung zeigt, dass 67 % der Organisationen die entsprechenden Grundsätze erst im Ergebnis einer in der Organisation bereits vorgefallenen Datensicherheitsverletzung eingeführt haben bzw. einführen⁽⁴⁵⁾. Sicherheitsstrategien sollten aber umgesetzt werden, bevor sich eine Verletzung der Datensicherheit bzw. des Datenschutzes ereignet. Entwickeln Sie für Ihr Unternehmen eine Sicherheitspolitik, die von jedem Mitarbeiter die Unterzeichnung einer Erklärung verlangt, einen privaten USB-Speicherstick weder an das Firmen-Intranet anzuschließen noch zum Transport von Firmendaten zu verwenden. Der Gebrauch unternehmenseigener USB-Speichersticks kann letztendlich gestattet werden, wobei jedoch Pflichten und Regeln der Mitarbeiter für den sicheren Gebrauch festzulegen⁽⁴⁶⁾ und Sticks, die keinen nachvollziehbaren geschäftlichen Nutzeffekt haben, zu sperren sind⁽⁴⁷⁾. In diesem Sinne ist zu definieren, welche Arten von Geräten für den Zugriff auf das Firmen-Intranet zugelassen sind.

Die Unternehmensgrundsätze sollten umfassend, aber nicht so restriktiv sein, dass sie die Produktivität der Mitarbeiter einschränken. Aus diesem Grund ziehen es viele Großunternehmen vor, den Zugriff auf sensible Dateien zu überwachen und zu protokollieren, statt ihn gänzlich zu verwehren⁽⁴⁸⁾. Die entsprechenden Regeln können je nach Funktion und Verantwortlichkeit eines Mitarbeiters variieren.

- ✓ Führen Sie ein Verfahren zur Beurteilung des Verlusts und/oder der Beschädigung unternehmenseigener Hardware, z. B. eines USB-Speichersticks, ein. Nutzen Sie gegebenenfalls Formblätter, um von beteiligten Mitarbeitern Informationen zu erfragen und auszuwerten.
- ✓ Führen Sie eine zentrale Politik für die Endpoint Security in Form einer eigens dafür konzipierten Lösung ein. Das organisationsweite Einrichten und Verwalten mobiler Datenträger kann kompliziert und kostspielig sein, wohingegen eine zentrale Verwaltungslösung es Organisationen Folgendes gestattet:
 - Verwaltung und gegebenenfalls. völlige Sperrung von Hardware-Schnittstellen (Ports), da selbst eine Verschlüsselungs- und Identitätsmanagementsoftware USB-Speichersticks nicht zu 100 % sicher machen wird. Überwachen Sie jeden Port an jeder Arbeitsstation und sperren Sie nicht zugelassene Geräte aus. Zudem ist es möglich, über ein Port-Audit den Anschluss von Geräten zu protokollieren bzw. von vornherein nur ausgewählte Geräte zuzulassen, z. B. verschlüsselte Sticks, die an bestimmte Mitarbeiter ausgegeben wurden⁽⁴⁹⁾;
 - Suche nach einem System, das es ermöglicht, den Offline-Gebrauch von USB-Speichersticks nachzuvollziehen, indem es die auf mobilen Geräten abgelegten Dateien mit den Originaldateien vergleicht, um festzustellen, ob Dateien geöffnet, verändert oder auf ein weiteres Gerät übertragen wurden;
 - zentrale Erfassung von Benutzerpasswörtern unter Anwendung eines Authentifizierungsverfahrens nach dem Challenge-Response-Prinzip;
 - zentrale Verwaltung unternehmenseigener USB-Speichersticks;
 - Nachweis der Einhaltung von Sicherheitsstandards;

⁽⁴⁵⁾ SanDisk Endpoint Security Survey, *SanDisk*, April 2008.

⁽⁴⁶⁾ Toolkit sample template: a sample employee agreement for the use of personal digital devices, *Jay Heiser, Gartner*, 1. Februar 2008. *SANS stellt eine Musterpolitik zur Kontrolle des Gebrauchs von mobilen Rechen- und Speichergeräten vor. Diese Musterpolitik ist abrufbar unter http://www.sans.org/resources/policies/Remote_Access.doc (zuletzt aufgerufen am 30. Mai 2008).*

⁽⁴⁷⁾ Getting started with McAfee host data loss prevention, *McAfee*, 2008.

⁽⁴⁸⁾ „Data-leak security proves to be too hard to use“, *Infoworld.com*, abrufbar unter http://www.infoworld.com/article/08/03/06/10NF-data-loss-prevention-problem_1.html (zuletzt aufgerufen am 2. Juni 2008).

⁽⁴⁹⁾ „Closed doors policy“, *Daniel Tynan, FedTech Magazine*, August 2007, abrufbar unter http://fedtechmagazine.com/article.asp?item_id=352 (zuletzt aufgerufen am 30. Mai 2008); „Thumb drives are too often the victims of convenience“, *John Zyskowski, GCN*, 14. Dezember 2006, abrufbar unter http://www.gcn.com/online/vol1_no1/44136-1.html (zuletzt aufgerufen am 30. Mai 2008); USB flash drive protection, *Ron LaPedis, SanDisk, Disk Encryption Forum*, 13. Februar 2007.

- Schutz von Sachwerten und Marken, da sich nachweisen lässt, dass Geräte zum Zeitpunkt des Verlusts verschlüsselt waren bzw. gestohlene Geräte einer umfassenden Auditierung unterlagen;
- ✓ Prüfen Sie die Sicherheitsstrategien und setzen Sie diese durch: Stellen Sie sicher, dass einmal eingeführte Regelungen auch befolgt werden. Entsprechende Überprüfungen können von der physischen Kontrolle der Büro-Arbeitsplätze (z. B. zur Überwachung des Gebrauchs von USB-Speichersticks in Ihrer Organisation, der letztendlich auf speziell vom Unternehmen zugelassene Datenträger beschränkt werden sollte) bis zu virtuellen Audits mithilfe netzbasierter Anwendungen reichen, die den Weg bestimmter Daten durch die gesamte Organisation verfolgen ⁽⁵⁰⁾. Eine Aufstellung von Unternehmensgrundsätzen, ohne Mittel und Methoden zu deren Durchsetzung bzw. zum Feststellen von Verletzungen vorzusehen, ist nutzlos ⁽⁵¹⁾.
- ✓ Sachmittelverwaltung: Überprüfen und Inventarisieren Sie alle Hardware bzw. tragbaren Geräte, mit denen Zugriff auf Ihr Intranet erfolgt. Nutzen Sie Programme, die alle Geräte ermitteln können, die zu beliebiger Zeit an Ihr Netz angeschlossen wurden. Anhand dieser Informationen wird es Ihnen möglich, geeignete Grundsätze zu formulieren, mit denen neben der Art von Geräten einschließlich USB-Speichersticks, deren Gebrauch im Unternehmen gestattet ist, auch festgelegt wird, welche Mitarbeiter diese Geräte verwenden dürfen und welche Sicherungsmaßnahmen dabei anzuwenden sind.
- ✓ Stellen Sie fest, inwieweit Ihr Unternehmen auf Datenverluste vorbereitet ist, sollten USB-Speichersticks verloren gehen bzw. gestohlen werden.

Einschätzung

- ❖ *Kennen Sie die für Dokumente bzw. Daten geltende Einstufung hinsichtlich der Sensibilität der Inhalte?*
- ❖ *Wissen Sie, welche sensiblen Geschäftsdaten und grundlegenden Informationswerte zu schützen sind?*
- ❖ *Wissen Sie, welche Benutzer/Abteilungen auf derartige Informationen zugreifen können bzw. auf welche Weise und wie oft?*
- ❖ *Wissen Sie, wer USB-Speichersticks nutzen darf, um Daten zu kopieren und zu transportieren? Wissen Sie außerdem, welchem Mitarbeiter zu diesem Zweck ein unternehmenseigener USB-Stick zur Verfügung gestellt wurde?*
- ❖ *Liegen schriftliche Sicherheitsgrundsätze bzw. -leitlinien vor, die den Gebrauch von USB-Speichersticks betreffen?*
- ❖ *Werden die Benutzer geschult und wie häufig erfolgt dies?*
- ❖ *Fertigen Sie Sicherungskopien der auf USB-Sticks abgelegten Daten an?*
- ❖ *Werden Sie von den maßgeblich Beteiligten unterstützt?*

- ✓ **Zugangsbeschränkung:** Gestatten Sie nur namentlich festgelegten Mitarbeitern den Zugriff auf bestimmte Arten und Mengen sensibler Daten. In komplexeren Organisationen sollten feste Regeln für den Datengebrauch genau festlegen, welche Mitarbeiter ermächtigt werden können, auf sensible Datenbestände zuzugreifen, welche Arten von Dateien auf tragbare Geräte kopiert werden dürfen und wie diese behandelt werden sollten. Installieren Sie Software, die diesen Prozess automatisieren kann, indem sie Dateien auf Netzlaufwerken

⁽⁵⁰⁾ „Closed doors policy“, Daniel Tynan, FedTech Magazine, August 2007, abrufbar unter http://fedtechmagazine.com/article.asp?item_id=352 (zuletzt aufgerufen am 30. Mai 2008).

⁽⁵¹⁾ Plugging the leaks: best practices in endpoint security, SanDisk, 2008.

- und Client-Rechnern scannt und dabei nach Schlüsselwörtern sucht⁽⁵²⁾.
- ✓ Befestigen Sie Ihre USB-Speichersticks an Schlüsselringen oder Tragebändern, um sie nicht zu verlieren; aufgrund ihrer geringen Größe gehen sie sehr leicht verloren oder können gestohlen werden, und größere Speicherkapazitäten erhöhen zugleich die potenziell dem Risiko eines unberechtigten Zugriffs ausgesetzte Datenmenge.
 - ✓ Legen Sie den Benutzern von USB-Speichersticks nahe, diese im Read-Only-Modus zu betreiben, um das Übertragen von Viren zu vermeiden: an einigen USB-Sticks befindet sich ein Schalter bzw. eine Verriegelung, um das Gerät in den Read-Only-Modus zu versetzen, der das Beschreiben des Laufwerks bzw. das Verändern darauf gespeicherter Daten durch den Host-Rechner verhindert.
 - ✓ Unterziehen Sie den USB-Speicherstick einem Anti-Virus-Scan, wenn Sie Dateien von einem nicht vertrauenswürdigen Rechner kopiert haben.
 - ✓ Richten Sie eine Authentifizierung für Benutzer ein. Verhindern Sie den unberechtigten Zugriff auf Daten, indem Sie ein Verfahren anwenden, das Benutzer auffordert, sich mittels Passwort bzw. Fingerabdruck anzumelden. Legen Sie eine maximale Anzahl von Wiederholungen der Passworteingabe bzw. der biometrischen Authentifizierung fest, um Umgehungsversuchen zu begegnen.
 - ✓ Nutzung von Verschlüsselungstechniken, entweder auf Software- oder auf Hardwareebene, die Daten so verändern, dass ein Zugriff ohne den korrekten Schlüssel nicht möglich ist⁽⁵³⁾. Die auf dem USB-Speicherstick gespeicherten Daten sind so lange nutzlos, bis der richtige Schlüssel eingegeben wird, und bleiben damit beim Transport stets gesichert. Eine Lösung besteht darin, das Ablegen sensibler Daten nur auf verschlüsselten Datenträgern wie speziell für den Unternehmenseinsatz konzipierten USB-Speichersticks zu gestatten, die alle Dateien obligatorisch mit einem Passwortschutz versehen. Eine weitere Möglichkeit, die weithin als eine der besten Lösungen gilt, ist der Einsatz von Speichergeräten mit Hardware-Verschlüsselung, die eine Kodierung der Daten im USB-Speicherstick selbst vornehmen. Der größte Vorteil der zugehörigen Hardware-basierten Schlüssel besteht darin, dass sie den USB-Speicherstick nie verlassen, gegen Angriffe von außen resistent sind und praktisch keine Leistungseinbußen verursachen⁽⁵⁴⁾. Letztendlich ist auch die Verschlüsselung der Daten selbst eine leistungsstarke Sicherungstechnologie, die als Hilfsmittel genutzt werden kann. Sie sollte immer dann eingesetzt werden, wenn Daten transportiert werden, für die keine ausreichend spezifischen Zugriffskontrollrechte existieren⁽⁵⁵⁾. Informieren Sie sich über Verschlüsselungs-Tools von Drittanbietern, die geeignete Sicherungsmechanismen für alle Risikosysteme bieten, insbesondere solche, auf denen sensible Daten gespeichert werden bzw. die entwendet und für Wirtschaftsspionage genutzt werden könnten⁽⁵⁶⁾.
 - ✓ Schützen Sie Ihre Infrastruktur vor Schadprogrammen. Verwenden Sie ein Virenschutzprogramm⁽⁵⁷⁾, um:
 - Virenangriffe zu unterbinden, da es den Zugriff von Viren und Trojanern auf USB-Speichersticks sperrt bzw. bereits infizierte Laufwerke säubert;

⁽⁵²⁾ Plugging the leaks: best practices in endpoint security, *SanDisk*, 2008.

⁽⁵³⁾ Use the three laws of encryption to properly protect data, *Rich Mogull, Gartner*, 24. August 2005; „Thumb drives are too often the victims of convenience“, *John Zyskowski, GCN*, 14. Dezember 2006, abrufbar unter http://www.gcn.com/online/vol1_no1/44136-1.html (zuletzt aufgerufen am 30. Mai 2008); Seven steps to secure USB drives, *SanDisk*, Juli 2007, und Assessing the security of hardware-based vs. software-based encryption on USB flash drive, *SanDisk*, Mai 2008.

⁽⁵⁴⁾ Assessing the security of hardware-based vs. software-based encryption on USB flash drive, *SanDisk*, Mai 2008.

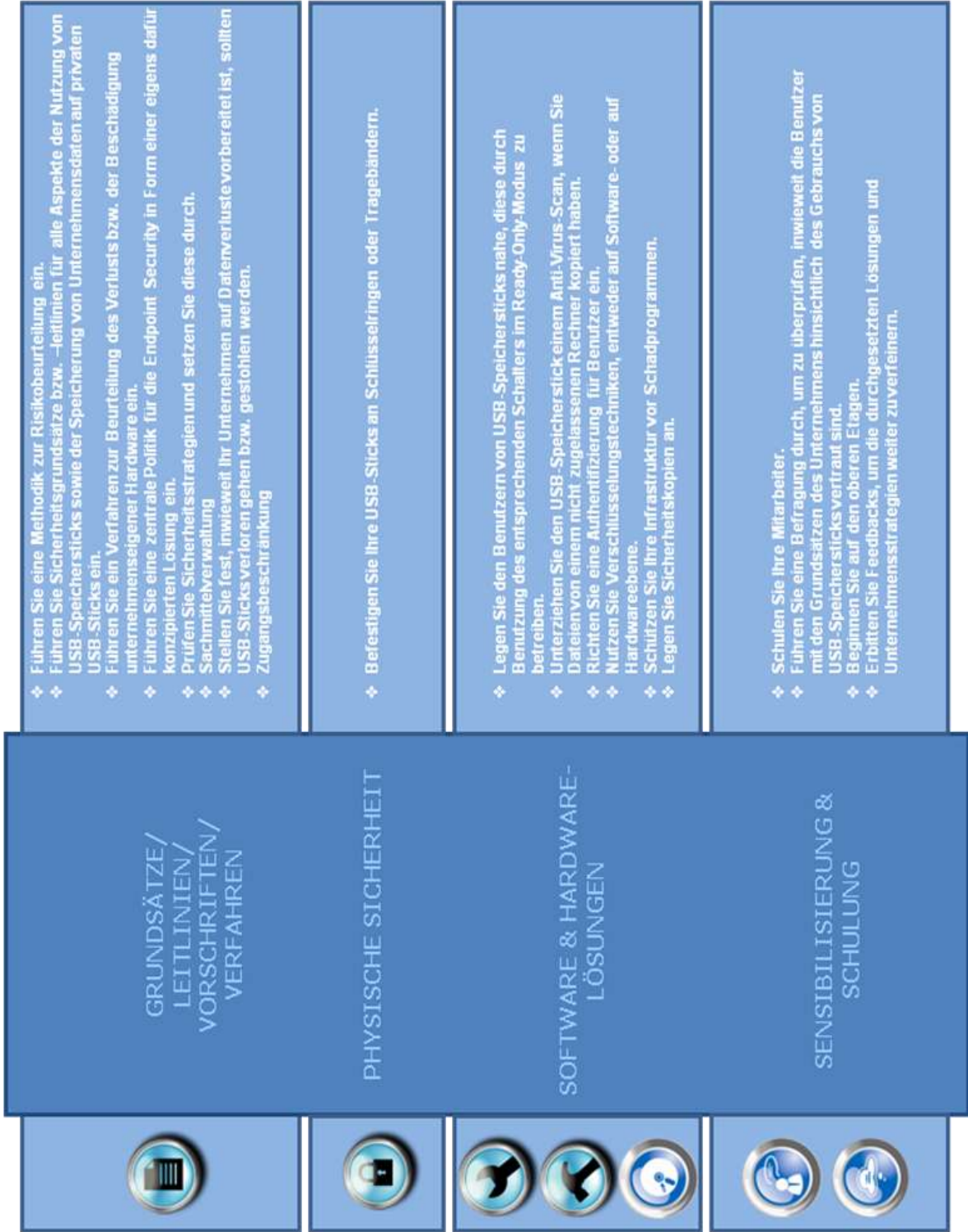
⁽⁵⁵⁾ Use the three laws of encryption to properly protect data, *Rich Mogull, Gartner*, 24. August 2005, und Prepare for DRAM threat to encrypted data storage, *John Girard, Ray Wagner, Eric Ouellet, Gartner*, 25. Februar 2008.

⁽⁵⁶⁾ Cyber-Spionage nimmt mittlerweile den dritten Rang in der SANS-Liste der zehn größten Cyber-Bedrohungen für 2008 ein. Weitere Einzelheiten finden sich in Top 10 cyber menaces for 2008, *SANS Institute*, abrufbar unter <http://www.sans.org/2008menaces/> (zuletzt aufgerufen am 2. Juni 2008).

⁽⁵⁷⁾ McAfee®VirusScan® USB – Sicherheit zum Schutz Ihres USB-Laufwerks, *McAfee*, 2006, abrufbar unter http://download.mcafee.com/products/manuals/de/vsusb_datasheet_2007.pdf.

- Ihre PCs zu schützen, da es verhindert, dass ein USB-Speicherstick als Überträger von Viren fungiert, sobald sie ihn an einen PC anstecken.
- ✓ Legen Sie Sicherheitskopien an, um auf USB-Speichersticks abgelegte Daten bei Bedarf wiederherstellen zu können.
- ✓ Mitarbeiterschulung: Schulen Sie Ihr Personal zu den Unternehmensgrundsätzen rund um den Einsatz von Informationstechnik, um sie für die Risiken im Zusammenhang mit Speicherung und Transport von Unternehmensdaten USB-Speichersticks zu sensibilisieren. Erläutern Sie, wie sich Datenlecks vermeiden lassen, und verlangen Sie, diesbezügliche Vorfälle zu melden. Halten Sie die Mitarbeiter über etwaige Änderungen der einschlägigen Grundsätze auf dem Laufenden und stellen Sie sicher, dass die Grundsätze in der täglichen Arbeit beachtet werden. Die Aufklärung und Sensibilisierung der Benutzer sowie deren Einsicht in die Notwendigkeit entsprechender Regelungen sind kritische Faktoren für den Erfolg einer jeden Sicherheitspolitik oder implementierten technischen Lösung.
- ✓ Führen Sie eine Befragung durch, um zu überprüfen, inwieweit die Benutzer mit den Grundsätzen ihres Unternehmens hinsichtlich des Gebrauchs von USB-Speichersticks vertraut sind.
- ✓ Beginnen Sie in den oberen Etagen! Instruieren Sie zuerst die Unternehmensleitung und diejenigen Mitarbeiter, die mit sensiblen Daten reisen, bevor Sie sich den übrigen Mitarbeitern zuwenden. Die beste Verteidigung gegen Datenlecks ist eine entsprechend aufgeklärte Belegschaft.
- ✓ Erbitten Sie Feedback, um die durchgesetzten Lösungen und Unternehmensstrategien weiter zu verfeinern, genau auf den Punkt zu bringen und eventuelle Verlaufsmuster zu erkennen, die das Datenverlustrisiko erhöhen.

In der folgenden Tabelle sind die gerade beschriebenen Empfehlungen sowie Software- und Hardwarelösungen noch einmal im Überblick dargestellt:



Checkliste

Die einzelnen Positionen der Checkliste können als Leitfaden für die wichtigsten Schritte eines Unternehmens bei Maßnahmen im Zusammenhang mit dem sicheren Gebrauch von USB-Speichersticks dienen. Wenn das Unternehmen die Bedeutung des Schutzes von Unternehmensdaten erkannt und die Daten entsprechend eingestuft hat, sollten folgende Hauptschritte absolviert werden:



TEIL 3:
Sicherheitstipps und Nutzeffekte für
Unternehmen



Praktische Tipps zur Verhinderung des Diebstahls von USB-Speichersticks

Tipps für die Praxis

- ❖ Sorgen Sie dafür, dass Mitarbeiter jeden Verlust oder Diebstahl eines USB-Speichersticks der IT-Abteilung melden.
- ❖ Nehmen Sie für jeden abhanden gekommenen USB-Speicherstick eine Schadensbeurteilung vor.
- ❖ Ermitteln Sie genau, wie und wo das Laufwerk abhanden gekommen ist
- ❖ Überprüfen Sie Ihre Leitlinien/Grundsätze um sicher zu gehen, dass die Hauptursachen für Verluste erfasst sind.
- ❖ Weisen Sie deutlich auf potenzielle Risiken hin, die sich aus dem unbedachten Gebrauch von USB-Speichersticks durch Mitarbeiter wie auch aus der Nutzung für weniger legitime Zwecke wie dem heimlichen Verbringen von Informationen aus dem Unternehmen ergeben.
- ❖ Führen Sie spezielle Maßnahmen für Abteilungen ein, die Umgang mit sensiblen Daten haben.
- ❖ Überwachen Sie den Datenverkehr und berichten Sie Vorfälle regelmäßig.
- ❖ Schulen Sie die Mitarbeiter und erinnern Sie sie regelmäßig an das Gelernte.
- ❖ Vergleichen Sie Ihre Sicherheitsbilanz mit der ähnlich gelagerter Unternehmen.
- ❖ Erbitten Sie Feedbacks, um die durchgesetzten Lösungen und Unternehmensstrategien weiter zu verfeinern, auf den Punkt zu bringen und eventuelle Muster zu erkennen, die das Datenverlustrisiko erhöhen.

Nutzeffekte

Eine Übersicht der vielen Vorzüge, die mit dem sicheren Gebrauch von USB-Speichersticks verbunden sind, soll Unternehmen behilflich sein, bessere Entscheidungen in dieser Angelegenheit zu treffen. Folgende Nutzeffekte geeigneter Sicherheitslösungen konnten ermittelt werden:

- ✓ Erhöhung der Mitarbeiterproduktivität durch Mobilität und Möglichkeit des Fernzugriffs auf Daten;
- ✓ Flexible und sichere Lösungen
 - schützen die Unternehmenswerte,
 - senken die Gesamtbetriebskosten (TCO),
 - sorgen dafür, dass Geräte bei Verlust oder Diebstahl verschlüsselt sind.
- ✓ Schutz des Unternehmens vor Datenlecks.
- ✓ Unternehmensweite Durchsetzung obligatorischer Sicherheitsgrundsätze.
- ✓ Schutz und Säuberung jedes Rechners an jedem Ort – nur zugelassene Geräte dürfen an einen PC angeschlossen werden;
- ✓ Ausweitung der Sicherheitspolitik über das Unternehmensgelände hinaus, denn
 - sämtliche Aktivitäten von USB-Speichersticks werden nachvollziehbar.

- ✓ Konsequente Beachtung der drei Säulen bzw. Anforderungen der Informationssicherheit – Vertraulichkeit, Verfügbarkeit, Integrität – und der geltenden Sicherheitsnormen.

Fazit

In Unternehmen der heutigen Zeit werden sensible Daten auf den verschiedensten mobilen Geräten, darunter USB-Speichersticks, gespeichert und ausgelesen. Der Gebrauch dieser Geräte hat enorm zugenommen, was unter anderem auf ihre hohe Speicherkapazität, ihren niedrigen Preis, ihre geringe Größe und Plug-and-Play-Fähigkeit zurückzuführen ist. Häufig befinden sich auf USB-Speichersticks Unternehmensdaten wie Finanzdaten, Formulare, Mitarbeiterinformationen und Kundendaten. Ein hoher Anteil dieser mobilen Geräte ist nach wie vor ungeschützt und unterliegt nicht der Kontrolle durch die IT-Abteilungen, was Unternehmen anfällig für Angriffe mit potenziell verheerenden Auswirkungen wie Rufschädigung, Arbeitsplatzverlust und Gewinneinbußen macht.

Der Verlust von Unternehmensdaten ist das Ergebnis fehlender Kenntnisse über die mit dem Gebrauch von USB-Speichersticks verbundenen Risiken bei den Mitarbeitern bzw. deren Bereitschaft, bestimmte Sicherheitsvorschriften zu umgehen, um produktiver arbeiten zu können. In diesem Sinne werden die meisten Vorfälle nicht vorsätzlich oder böswillig herbeigeführt, sondern eher versehentlich und unbeabsichtigt.

Trotz eines zunehmenden Bewusstseins für die Risiken und Kosten des ungesicherten Gebrauchs von USB-Speichersticks bleibt in dieser Richtung noch sehr viel zu tun. Von ganz entscheidender Bedeutung ist deshalb, dass die IT-Verantwortlichen sich und ihre Organisationen darauf vorbereiten, den Gebrauch von USB-Speichersticks zu regulieren, zu verwalten und zu prüfen, da es für jedes Unternehmen – ungeachtet seiner Größe und Reife – ausgesprochen wichtig ist, über Möglichkeiten zur Sicherung von Daten in seinem Intranet wie auch zur Verwaltung aller Daten, die in das Unternehmen kommen bzw. das Unternehmensumfeld verlassen, zu verfügen.

Angesichts der wachsenden Zahl mobiler Geräte, die zu geschäftlichen Zwecken, wenn Mitarbeiter reisen oder sich Arbeit mit nach Hause nehmen, genutzt werden, sollte ein sicherer Gebrauch von USB-Speichersticks und die Sensibilisierung für die damit verbundenen Risiken fester Bestandteil einer umfassenden Sicherheitsstrategie jedes Unternehmens sein.

ENISA hofft, den Unternehmen mit dem vorliegenden Beitrag ein wertvolles Werkzeug an die Hand zu geben, um bestehende Hindernisse überwinden zu können.

Literaturangaben und Verweise auf weitere Quellen

Leitfaden für die Praxis: Wege zu mehr Bewusstsein für Informationssicherheit, *ENISA*, Juni 2006.

„Afghan market sells US military flash drives“, *Paul Watson*, Los Angeles Times, 18. April 2006, abrufbar unter <http://www.veteransforcommonsense.org/ArticleID/7120> (zuletzt aufgerufen am 28. Mai 2008).

„Analysis of USB flash drives in a virtual environment“, *Derek Bem und Ewa Huebner*, Small Scale Digital Device Forensics Journal, Vol. 1, No 1, Juni 2007.

„Another laptop stolen from Pfizer, employee information compromised“, *Lee Howard*, 12. Mai 2008, abrufbar unter <http://attrition.org/dataloss/2008/05/pfizer01.html> (zuletzt aufgerufen am 30. Mai 2008).

„Closed doors policy“, *Daniel Tynan*, FedTech Magazine, August 2007, abrufbar unter http://fedtechmagazine.com/article.asp?item_id=352 (zuletzt aufgerufen am 30. Mai 2008).

„Data breaches are ‚everyday incidents‘“, *Matt Chapman*, vnunet.com, 15 Nov 2007, abrufbar unter <http://www.vnunet.com/vnunet/news/2203540/security-breaches-everyday> (zuletzt aufgerufen am 30. Mai 2008).

„Data-leak security proves to be too hard to use“, *Infoworld.com*, abrufbar unter http://www.infoworld.com/article/08/03/06/10NF-data-loss-prevention-problem_1.html (zuletzt aufgerufen am 2. Juni 2008).

Dataquest insight: USB flash drive market trends, worldwide, 2001–2010, *Joseph Unsworth*, Gartner, 20. November 2006.

DataTraveler for Enterprise, *Kingston*, 2008, abrufbar unter http://www.kingston.com/flash/DataTravelers_enterprise.asp (zuletzt aufgerufen am 30. Mai 2008).

DataTraveler Secure and DataTraveler Secure — Privacy Edition White Paper, *Kingston Technology*, Rev. 2.0, Juni 2007.

Determine the appropriate level of ITAM controls for mobile assets, *Jack Heine*, Gartner, 15. November 2005.

„Disc listing foreign criminals lost for year“, *The Times*, 20. Februar 2008.

Educational security incidents (ESI) — Sometimes the free flow of information is unintentional, abrufbar unter <http://www.adamdodge.com/esi/month/2008/01>

Forecast: USB flash drives, worldwide, 2001–2011, *Joseph Unsworth*, Gartner, 24. September 2007.

Getting started with McAfee host data loss prevention, *McAfee*, 2008.

Magic quadrant for mobile data protection, 2007, *John Girard*, *Ray Wagner*, Gartner.

McAfee Encrypted USB — data sheet, *McAfee*.

McAfee® VirusScan® USB — Sicherheit zum Schutz Ihres USB-Laufwerks, *McAfee*, 2006, abrufbar unter http://download.mcafee.com/products/manuals/de/vsusb_datasheet_2007.pdf.

New attacks: device vulnerabilities stand out, *Avivah Litan, Don Dixon, Greg Young, Gartner*, 21. Juni 2005.

„New report chronicles the cost of data leaks“, *Physorg.com*, 2007, abrufbar unter <http://www.physorg.com/news96708147.html> (zuletzt aufgerufen am 2. Juni 2008).

Plugging the leaks: best practices in endpoint security, *SanDisk*, 2008.

Prepare for DRAM threat to encrypted data storage, *John Girard, Ray Wagner, Eric Ouellet, Gartner*, 25. Februar 2008.

„Prince of Wales Hospital announced an incident of loss of USB flash drive containing hospital files“, *press releases*, 6. Mai 2008, abrufbar unter <http://www.info.gov.hk/gia/general/200805/06/P200805060232.htm> (zuletzt aufgerufen am 30. Mai 2008).

Privacy and identity theft“, *Dave Jevans, IronKey*, abrufbar unter <http://blog.ironkey.com/?cat=9&paged=2> (zuletzt aufgerufen am 20. Mai 2008).

Plugging the leaks: best practices in endpoint security, *SanDisk*, 2008.

SanDisk Endpoint Security Survey, *SanDisk*, April 2008.

Seven steps to secure USB drives, *SanDisk*, Juli 2007.

„Small drives cause big problems“, *Jon Swartz*, USA Today, 16. August 2006, abrufbar unter http://www.usatoday.com/tech/news/computersecurity/2006-08-15-thumbdrives-stolen_x.htm (zuletzt aufgerufen am 27. Mai 2008).

„Spring students' info at risk after laptop theft“, *KHOU.com staff report*, 16. Mai 2008, abrufbar unter <http://attrition.org/dataloss/2008/05/spring01.html> (zuletzt aufgerufen am 30. Mai 2008).

Survey of US IT practitioners reveals data security policies not enforced, *Ponemon Institute and RedCannon Security*, December 2007, abrufbar unter http://www.ponemon.org/press/RC_PonemonSurvey_FINAL.pdf (last visited 2. Juni 2008).

„TAMU Corpus Christi prof loses flash drive with 8 000 student records“, *Paul McCloskey*, Campus Technology, 18. August 2007, abrufbar unter <http://campustechnology.com/articles/48635> (zuletzt aufgerufen am 30. Mai 2008).

The portable risk of high capacity USB drives, *Allan Leinwand*, GigaOM, 5. Dezember 2007, abrufbar unter <http://gigaom.com/2007/12/05/the-portable-risk-of-high-capacity-usb-drives/> (zuletzt aufgerufen am 30. Mai 2008).

„Thumb drives are too often the victims of convenience“, *John Zyskowski*, GCN, 14. Dezember 2006, abrufbar unter http://www.gcn.com/online/vol1_no1/44136-1.html (zuletzt aufgerufen am 30. Mai 2008).

Timetable of missing data blunders“, *The Times*, 20. Februar 2008.

Toolkit sample template: a sample employee agreement for the use of personal digital devices, *Jay Heiser, Gartner*, 1. Februar 2008.

Top 10 Cyber menaces for 2008, *SANS Institute*, abrufbar unter <http://www.sans.org/2008menaces/> (zuletzt aufgerufen am 2. Juni 2008).

Understanding data leakage, Jay Heiser, *Gartner*, 21. August 2007.

„US military secrets for sale at Afghanistan bazaar“, *Watson*, Los Angeles Times, 10. April 2006.

USB flash drive market trends, Worldwide, 2001–2010, *Joseph Unsworth*, *Gartner*, November 2006.

USB flash drive protection, *Ron LaPedis*, *SanDisk*, *Disk Encryption Forum*, 13. Februar 2007.

Use the three laws of encryption to properly protect data, *Rich Mogull*, *Gartner*, 24. August 2005.

http://www.enisa.europa.eu/rmra/rm_ra_methods.html

http://www.enisa.europa.eu/rmra/rm_ra_tools.html

Assessing the security of hardware-based vs. software-based encryption on USB flash drive, *SanDisk*, Mai 2008.

Sicherer Umgang mit USB-Speichersticks

ISBN: 978-92-9204-010-9

Catalogue number: TP-30-08-571-DE-C



ISBN 978-92-9204-010-9