blancco
CERTIFIED DATA ERASURE

Datenlösch-Management im Unternehmen:

AUTOMATISIERTE PROZESSE GARANTIEREN HÖCHSTE WIRTSCHAFTLICHKEIT

Blancco White Paper

Veröffentlicht am 16. Oktober 2013

Einführung

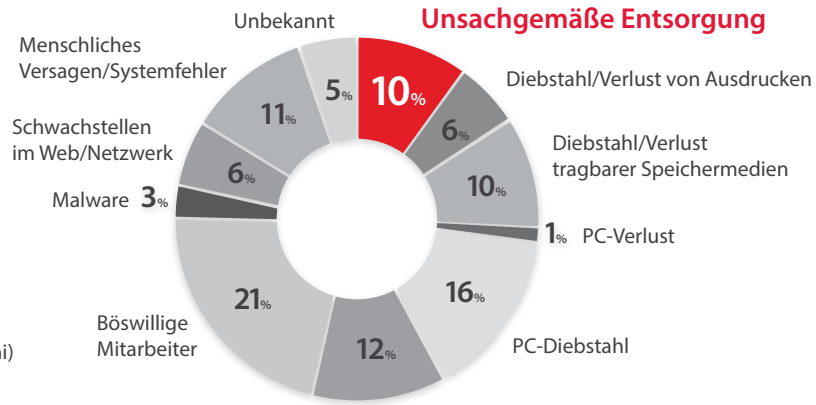
IT-Leiter (Chief Information Officer), Datenschutzbeauftragte (Corporate Security Officer) und IT-Asset-Manager sehen sich zunehmend mir Herausforderungen konfrontiert, die ihre anspruchsvolle Aufgaben zusätzlich erschweren. Als Verantwortliche für die Sicherheit und den Betrieb der IT-Infrastruktur tragen sie wesentlich zur Verfügbarkeit und zum Schutz geschäftskritischer Daten innerhalb von Unternehmen oder Behörden bei.

Weniger Personal und immer knappere Budgets sind heute nur einige der Herausforderungen des IT-Managements. Von IT-Leitern und ihren IT-Abteilungen wird erwartet, dass sie trotz schrumpfender finanzieller und personeller Ressourcen bestehende Zielvorgaben und Benchmarks so effizient und kostengünstig wie möglich erfüllen. Eine Entwicklung die heute die Anforderungen an die IT-Abteilungen permanent erhöht.

Ein wichtiger Bestandteil jeder IT-Richtlinie bei Unternehmen und Behörden ist eine solide und bewährte Datensicherheitsstrategie. Dies gilt insbesondere vor dem Hintergrund der weltweit starken Zunahme von Datensicherheitsverletzungen und Datendiebstahl. Die Festlegung und Umsetzung von Verfahren zur nachweisbaren Löschung von Daten auf Speichermedien, die wiederverwendet, gespendet oder entsorgt werden sollen, gehört zu den zentralen Aspekten einer solchen Strategie. Voraussetzung ist eine Lösung, die ein breites Spektrum an Hardware unterstützt, angefangen von Smartphones bis hin zu High-End-Servern, und die sowohl für das tägliche Datenlösch-Management als auch für individuelle Löschprozesse im Lebenszyklus eines Datenträgers einsetzbar ist. Dabei muss genau erfasst werden, welche Daten gelöscht wurden und von wem dies duchgeführt wurde.

Während die Datenlöschung zu den wichtigen “Best Practises” einer ganzheitlichen Datensicherheitsstrategie gehört, haben IT-Manager in ihrem Alltag trotzdem mit sinkenden Budgets und fehlenden Ressourcen zu kämpfen. Um die Datenlöschung effizient und wirtschaftlich umzusetzen, helfen moderne Datenlöschsystem mit einem zentralen Datenlösch-Management und schnellen, automatisierten und sicheren Abläufen. Gleichzeitig tragen solche Systeme zur Reduzierung der Kosten und Ressourcen bei. Automatisierte Funktionen beschleunigen den Löschprozess und ermöglichen die Anpassung der Lösch- und Berichtsprozesse an die Bedürfnisse der Unternehmen.

Inhalt



Ursachen:
Anzahl der Vorfälle im Jahr 2010 in Prozent dargestellt (Januar – Juni)

Quelle: KPMG International, Oktober 2010

Gefahr durch unsachgemäß entsorgte IT-Geräte

Während Unternehmen die Gefahren von Datenverlust häufig mit gestohlenen Laptops oder anderen tragbaren Speichergeräten assoziieren, wird eine andere, viel subtilere Ursache meist vernachlässigt: Die unsachgemäße Entsorgung von IT-Geräten durch die Unternehmen selbst. Laut einer internationalen Studie von KPMG aus dem Jahr 2010[1] sind zehn Prozent aller Fälle von Datenverlust auf eine unzureichende Datenvernichtung zurückzuführen; mit gravierenden Folgen für das Image des Unternehmens und empfindlichen Geldstrafen, infolge zunehmend schärferer Datenschutzbestimmungen. Berichten zufolge, darunter eine Studie von Kessler International[2] aus dem Jahr 2009, befinden sich auf rund 40 Prozent aller Festplatten, die gebraucht verkauft werden, sensible Daten.

Die Datenlöschung nutzt ein softwarebasiertes Verfahren zum Überschreiben und vollständigen Löschen aller, häufig sensibler elektronischer Informationen, die sich auf einer Festplatte oder auf einem anderen digitalen Speichermedium befinden, das für die Entsorgung oder Wiederverwendung vorgesehen ist. Diese Form der Datenvernichtung geht weit über einfache Befehle zum Löschen von Dateien, mit denen lediglich die direkten Verweise zu Datenträgersektoren entfernt werden und die mit gängigen Software-Tools problemlos wiederhergestellt werden können, hinaus. Bei einer professionellen Datenlöschung hingegen werden alle Informationen vollständig und sicher entfernt, ohne die Funktionsfähigkeit des Datenträgers zu zerstören. Löschberichte mit detaillierten Angaben zur Hardware und dem gelöschten Medium dienen als Nachweis für die erfolgreiche Datenlöschung.

STÄRKEN UND SCHWÄCHEN VON DATENSCHUTZ-TECHNOLOGIEN

Die physikalische Vernichtung, die Entmagnetisierung, die Verschlüsselung, die Neuformatierung und der Einsatz einfacher Software zum Überschreiben von Speichermedien sind Beispiele für eine Vielzahl von Technologien zum Schutz und zur Vernichtung von Daten, die eines gemeinsam haben: Jede dieser Lösungen hat Nachteile. So führt beispielsweise die physikalische Vernichtung und Entmagnetisierung von Laufwerken dazu, dass diese unbrauchbar werden und weder weiterverkauft noch wiederverwendet werden können, mit negativen Auswirkungen bezüglich Nachhaltigkeit und Umwelt. Gleichzeitig bietet die physikalische Vernichtung keinen verlässlichen Schutz, da hier nicht die Daten selbst, sondern nur die Datenträger-Grundlage zerstört wird und selbst kleinste Partikel aus-

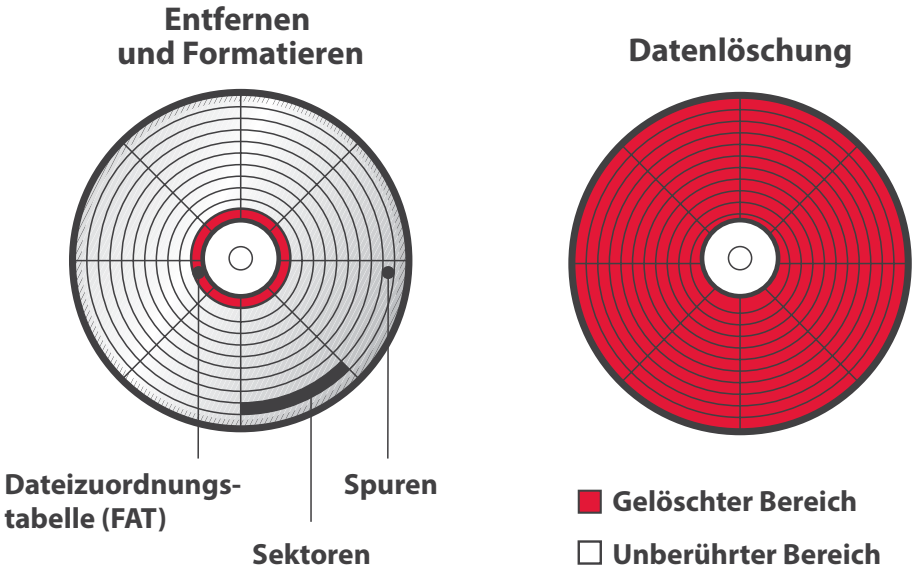
gelesen werden können. Ein weiterer Nachteil sind die hohen Anschaffungskosten für professionelle Anlagen zur Vernichtung von Festplatten. Ein Grund, weshalb dieser Vorgang in der Regel an externe Dienstleister ausgelagert wird. Ein gesicherter Transport verringert die Gefahr, dass Datenträger und Daten beim Transport verloren gehen.

Auch andere Datenschutzstrategien haben ihre Schwächen. Beispielsweise ist der Einsatz softwarebasierter Verschlüsselungsverfahren in bestimmten Situationen ein effizientes Mittel, das zeitaufwändig und rechenintensiv ist und insbesondere bei inaktiven Geräten weder absolute Sicherheit bietet noch eine überprüfbare Datensicherung ermöglicht. Das Löschen von kryptografischen Schlüsseln am Ende des Lebenszyklus von verschlüsselten Datenträgern bietet keinerlei Kontrollmöglichkeiten. Die Nachteile liegen auf der Hand: die Gefahr von Anwendungsfehlern und das Fehlen jeglicher Prüfnachweise. Aktive und inaktive Systeme, bei denen Verschlüsselungstechnologien zum Einsatz kommen, ohne regelmäßig aktualisiert zu werden, sind anfällig für Angriffe. Sollte der Schlüssel in die falschen Hände gelangen, die Verschlüsselung geknackt oder eine andere Schwachstelle genutzt werden, ist der Weg frei für einen Zugriff auf die gesamten Daten.

Ebenso werden beim Formatieren von Laufwerken nicht alle Daten gänzlich unbrauchbar gemacht. Beim Einsatz nicht ausgereifter Überschreibtechnologien besteht die Gefahr, dass nicht genügend Überschreibvorgänge durchgeführt werden und der Anwender keine Löschberichte erhält, die den gesetzlichen Vorschriften entsprechen. Detaillierte und überprüfbare Berichte werden bei kostenlosen Programmen nicht erstellt; die Wirksamkeit einer solchen Software wurde bisher von keiner unabhängigen Stelle bestätigt.

Ein Datenlösch-Management, das auf fortschrittliche Löschtechnologien setzt, ist die beste Möglichkeit, um sensible Daten sicher von Geräten zu entfernen.

Andererseits bietet ein modernes Datenlöschmanagement, das auf fortschrittliche Löschtechnologien setzt, die Sicherheit, dass sensible Daten nachweisbar vernichtet wurden. Durch die Automatisierung des kompletten Datenlöschprozesses, bei dem automatisch detaillierte Prüfberichte erstellt werden, können Unternehmen darauf vertrauen, dass ihre Daten geschützt sind. Weitere Vorteile bei der Wirtschaftlichkeit, der Nachhaltigkeit und bei der gesamten Nutzung sprechen für sich.



Aktuelle Herausforderungen des Datensicherheits-Managements

IT-Organisationen werden jeden Tag mit einer wachsenden Zahl neuer Herausforderungen konfrontiert. Trotz sinkender Budgets und begrenzten Personalressourcen wird von der IT erwartet, mit „weniger mehr zu erreichen", während gleichzeitig Netzwerke einen steigenden Datenverkehr mit zunehmend anspruchsvollen Anwendungen bewältigen müssen.

Die digitalen Datenmengen, die Netzwerke jeglicher Art durchlaufen, haben sich laut einer Studie von EMC/IDC Digital Universe aus dem Jahr 2011[3] zwischen 2005 und 2010 fast verzehnfacht. Anzeichen für ein Nachlassen des Datenverkehrs gibt es nicht. Im Gegenteil: Die Zahlen haben sich zwischen 2010 und 2012 verdoppelt und werden sich Prognosen zufolge bis 2015 erneut mehr als verdoppeln.

UNTERNEHMEN SEHEN SICH EINER WACHSENDEN FLUT VON VORSCHRIFTEN GEGENÜBER

Weltweit wurden etliche strenge, branchenspezifische Standards und Vorschriften eingeführt, um das Risiko des Verlustes vertraulicher Daten zu minimieren, einschließlich Vorschriften für das Gesundheitswesen, für Finanz- und Kreditinformationen. Zu den aktuell geltenden Vorschriften mit expliziter Anforderung zur Löschung von Daten gehören das Bundesdatenschutzgesetz

> *Gesetze und rechtliche Anforderungen zum Thema Datenschutz konfrontieren Unternehmen mit zusätzlichen Vorgaben, die erfüllt werden müssen.*

in Deutschland, der Health Insurance Portability and Accountability Act (HIPAA), der Fair and Accurate Credit Transactions Act aus dem Jahr 2003 (FACTA), der Payment Card Industry Data Security Standard (PCI DSS) in den USA sowie der UK Data Protection Act aus dem Jahr 1998. Umfassende Regelungen einschließlich Vorgaben zum Löschen von Daten werden derzeit in den USA im Rahmen der Consumer Privacy Bill of Rights und in Europa durch die EU-Gesetzgebung im Rahmen einer Reform des Datenschutzes erarbeitet.

US-INITIATIVEN

Durch die Verabschiedung von Gesetzen und neuen rechtlichen Anforderungen zum Thema Datenschutz, sehen sich Unternehmen heute konkreten Vorgaben gegenüber, die erfüllt werden müssen. US-Präsident Obama hat im Februar 2012 Rahmenbedingungen zum Datenschutz und zur Innovationsförderung in der globalen digitalen Wirtschaft veröffentlicht. Der Bericht befasst sich nicht nur mit dem Verbraucherdatenschutz, sondern formuliert insgesamt die Kernfragen, Trends, und Probleme im Zusammenhang mit digitalen Daten.

In dem Bericht wird festgestellt, dass es einerseits an eindeutigen Vorgaben zum Datenschutz in der Wirtschaft mangelt und andererseits ein nachhaltiges Bekenntnis aller Beteiligten zur Beantwortung datenschutzrechtlicher Fragen bei Entwicklungen innerhalb der IT und bei neuen Geschäftsmodellen fehlt.

Als Antwort darauf hat die Obama-Administration die „Consumer Privacy Bill of Rights"[4] verabschiedet, die ein dynamisches Modell zur Förderung ständiger Innovationen bei gleichzeitiger Wahrung eines strengen Datenschutzes unterstützt und konkrete Auflagen zum Löschen von Daten enthält. Mit diesen neuen Rahmenbedingungen werden eindeutige Grundsätze zum Datenschutz in der Wirtschaft geschaffen und alle

Beteiligten werden aufgefordert, aufkommende datenschutzrechtliche Fragen im Zuge der technologischen Entwicklung zu beantworten.

EU-DATENSCHUTZ-VERORDNUNG

Auch in Europa wurde eine Änderung des Datenschutzes vorgeschlagen, die nicht nur eine Überarbeitung der seit 1995 bestehenden Bestimmungen, sondern vor allem auch eine konsequentere und einheitlichere Anwendung von geltendem Recht vorsieht. Zwingend notwendig wurde eine Überarbeitung der EU-Datenschutzbestimmungen[5] auch aufgrund des technologischen Fortschritts der letzten Jahre, wie z. B. bei sozialen Netzwerken, Cloud-Computing, lokalen Dienstleistungen und Chipkarten. Ein Entwurf der Datenschutzverordnung wird derzeit von allen Mitgliedstaaten der EU geprüft. Die Verabschiedung dieser Vorlage, die auch Bestimmungen zum Löschen von Online-Daten und zur Nutzung auditierbarer Verfahren für datenverarbeitende Unternehmen vorsieht, ist geplant. Im Rahmen dieser Verordnung wird unter anderem der Einsatz von zertifizierten Tools und Verfahren empfohlen.

Bei Verstößen gegen die neuen EU-Bestimmungen sind Geldstrafen von 250.000 Euro bis zu 0,5 % des jährlichen Firmen-Umsatzes bei kleineren Vergehen und von 1 Million Euro bis zu 2 % des Firmen-Umsatzes bei schwerwiegenderen Verstößen, vorgesehen. Unternehmen mit Cloud-Dienstleistungen, die personenbezogene Daten von EU-Bürgern verarbeiten, sind – unabhängig davon, ob sich ihre Server innerhalb oder außerhalb der EU befinden – zur Einhaltung der Rechtsvorschriften verpflichtet.

Neben der wachsenden Zahl von Datenschutzbestimmungen und Branchenstandards sehen sich IT-Abteilungen einer immer breiter werdenden Palette von Geräten und Plattformen gegenüber, auf denen Daten gespeichert werden. Das bedeutet, dass heute das Sicherheitsmanagement für unterschiedlichste Geräte ausgelegt sein muss. Desktops und Laptops, Server und Speichermedien, mobile Endgeräte wie Smartphones, virtuelle Maschinen und komplexe Massenspeicher in Rechenzentren sind nur einige von vielen verschiedenen Arten von Datenspeichern, auf denen sich sensible Informationen befinden können. Angesichts, explodierender Datenmengen müssen Unternehmen zukünftig in der Lage sein, Daten von einer Vielzahl unterschiedlicher Geräte zu löschen, um ihren gesetzlichen Verpflichtungen und ihrer moralischen und treuhänderischen Verantwortung nachzukommen.

Unternehmen mit Cloud-Dienstleistungen, die personenbezogene Daten von EU-Bürgern verarbeiten, sind – unabhängig davon, ob sich ihre Server innerhalb oder außerhalb der EU befinden – zur Einhaltung der Rechtsvorschriften verpflichtet.

VOLLSTÄNDIG AUDITIERBARES LÖSCHMANAGEMENT

Ein erfolgreiches Löschen allein reicht nicht mehr aus, da heute ein eindeutiger Nachweis der Löschung notwendig ist. Bei einer professionellen Datenlöschlösung ist ein detaillierter und auditfähiger Datenlöschbericht für Revisionszwecke und für Audits gefordert. In diesem Report sind wichtige Information zu Gerätedaten festgehalten um Compliance-Regeln, erfüllen zu können.

Ein manipulationssicheres und nachvollziehbares Lösch-Reporting ist für die Erfüllung behördlicher und rechtlicher Vorgaben unverzichtbar. Eine Datenlöschlösung sollte über eine integrierte und umfassende Berichtsfunktion zum Erstellen auditfähiger Reports verfügen, die wichtige Informationen enthalten: Zustand der Hardware, Seriennummern und Typenbezeichnungen, Erfassung von Softwarelizenzen und wer beispielsweise die Löschung durchgeführt hat.

BYOD IST KEINE MODEERSCHEINUNG

Der BYOD-Trend („Bring Your Own Device“) stellt Unternehmen vor zusätzliche Herausforderungen. Laut einem kürzlich veröffentlichten Bericht von Juniper Research ist der BYOD-Trend nicht aufzuhalten. Aktuell werden weltweit rund 150 Millionen private Geräte von Mitarbeitern am Arbeitsplatz genutzt[6]. Allein die Zahl der privaten Smartphones, die auf der Arbeit genutzt werden, könnte bis 2014 die Marke von 350 Millionen übersteigen.[7]

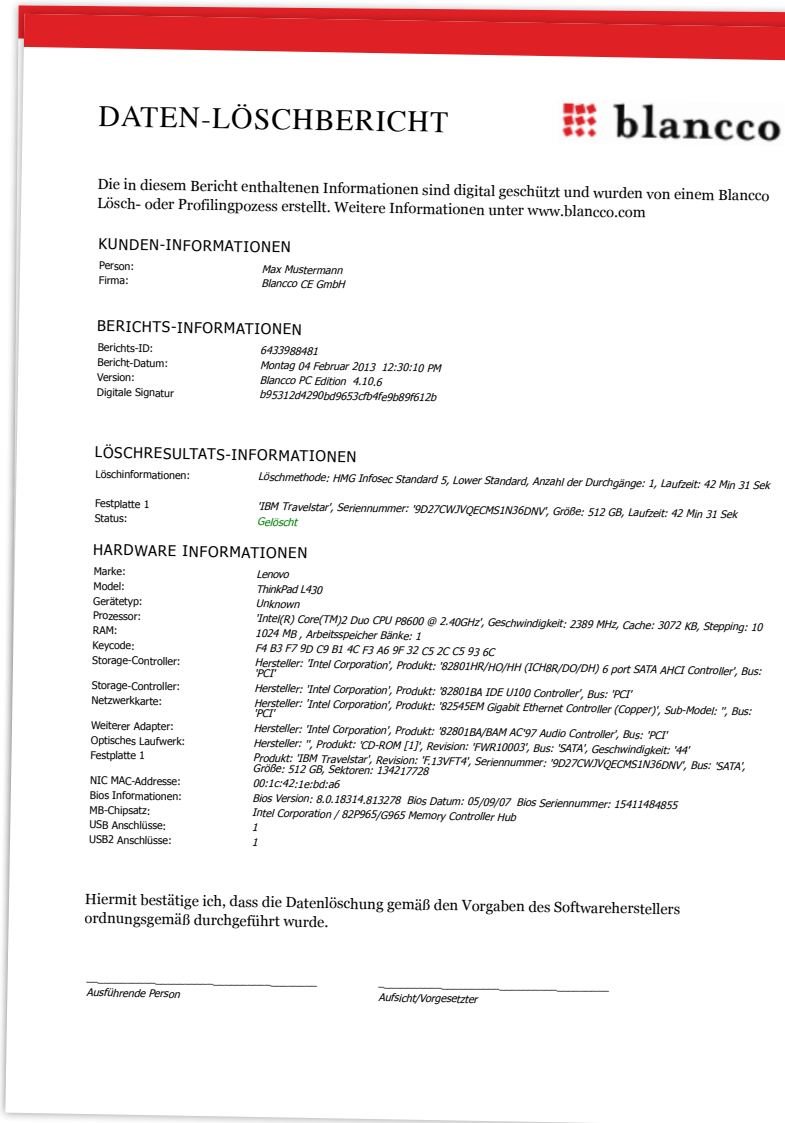
Mit einer Speicherkapazität von bis zu 64 GB enthalten mobile Endgeräte wie Smartphones und Tablets trotz ihrer Kompaktheit eine Fülle von Informationen. Je intelligenter diese speicherstarken Geräte werden und je häufiger sie für berufliche und private Zwecke eingesetzt sind, desto höher ist die Wahrscheinlichkeit, dass darauf E-Mails, Kundendaten, Passwörter und andere sensible Informationen gespeichert sind. Wenn diese Geräte entsorgt werden, ohne die darauf enthaltenen Informationen zuvor sicher und nachweislich zu löschen, kommt es zu Datenschutzverletzungen. Eine Studie aus dem Jahr 2009 hat gezeigt, dass 99 % der Menschen ihre Mobiltelefone für berufliche oder geschäftliche Zwecke nutzen. 77 % der Befragten haben auf ihren Mobiltelefonen Namen und Adressen von Geschäftskontakten gespeichert, 23 % Kundendaten und 17 % haben mit ihren Mobilgeräten Unternehmensinformationen wie Dokumente und Tabellen heruntergeladen.[8]

Während Datenrisiken im Zusammenhang mit mobilen Endgeräten wie Smartphones und Tablets häufig mit Malware sowie Phishing- und Spyware-Attacken in Verbindung gebracht werden, kann eine unsachgemäße Ausmusterung von Altgeräten ein noch viel größeres Sicherheitsrisiko darstellen. Organisationen wie die Europäische Agentur für Netz- und Informationssicherheit (ENISA) haben festgestellt, dass eine unsachgemäße Ausmusterung von Smartphones

infolge einer unvollständigen Datenlöschung eines der größten IT-Sicherheitsrisiken darstellt. Dennoch wird bei diesen Geräten – anders als bei gebrauchten Festplatten – nicht auf professionelle Löschprozesse zurückgegriffen, die heute zur Verfügung stehen.[9] Besonders besorgniserregend ist dies vor dem Hintergrund, dass Analysteneinschätzungen zufolge heute über 100 Millionen Mobiltelefone wiederverwendet werden.[10]

Ein Zurücksetzen auf den Fabrikzustand (factory reset) greift hier zu kurz. Die vermeintlich gelöschten Daten lassen sich mit leicht erhältlichen Tools problemlos wiederherstellen. Unternehmen sollten zur Unterstützung einer stabilen Sicherheitsstrategie für mobile Geräte sowie zur Einhaltung gesetzlicher Bestimmungen und zum Schutz vor Datenmissbrauch auf ein Datenlöschmanagement mit modernsten Löschtechnologien setzen, die einen überprüfbaren Nachweis der Datenlöschung bieten oder sich einen vertrauenswürdigen Partner für die Entsorgung von IT-Equipment suchen, der zertifizierte Verfahren und Löschprodukte nutzt. Mit den entsprechenden Fachkenntnissen, der richtigen Technologie oder dem richtigen Dienstleister können IT-Manager ihre Sicherheitsstrategien auf unternehmenseigene und auch auf private Mobilgeräte von Mitarbeitern individuell anpassen.

Unternehmen sollten im Sinne einer professionellen Sicherheitsstrategie für mobile Geräte und zum Schutz vor Datenmissbrauch ein Datenlösch-Management mit modernster Löschtechno-logie einsetzen, das zusätzlich einen überprüfbaren Nachweis der Löschung erstellt.



DATEN-LÖSCHBERICHT

blancco

Die in diesem Bericht enthaltenen Informationen sind digital geschützt und wurden von einem Blancco Lösch- oder Profilingpozess erstellt. Weitere Informationen unter www.blancco.com

KUNDEN-INFORMATIONEN

Person:	Max Mustermann
Firma:	Blancco CE GmbH

BERICHTS-INFORMATIONEN

Berichts-ID:	6433988481
Bericht-Datum:	Montag 04 Februar 2013 12:30:10 PM
Version:	Blancco PC Edition 4.10.6
Digitale Signatur	b95312d4290bd9653cfb4fe9b89f612b

LÖSCHRESULTATS-INFORMATIONEN

Löschinformationen:	Löschmethode: HMG Infosec Standard 5, Lower Standard, Anzahl der Durchgänge: 1, Laufzeit: 42 Min 31 Sek
Festplatte 1	'IBM Travelstar', Seriennummer: '9D27CWJVQECMS1N36DNV', Größe: 512 GB, Laufzeit: 42 Min 31 Sek
Status:	Gelöscht

HARDWARE INFORMATIONEN

Marke:	Lenovo
Model:	ThinkPad L430
Gerätetyp:	Unknown
Prozessor:	'Intel(R) Core(TM)2 Duo CPU P8600 @ 2.40GHz', Geschwindigkeit: 2389 MHz, Cache: 3072 KB, Stepping: 10
RAM:	1024 MB , Arbeitsspeicher Bänke: 1
Keycode:	F4 B3 F7 9D C9 B1 4C F3 A6 9F 32 C5 2C C5 93 6C
Storage-Controller:	Hersteller: 'Intel Corporation', Produkt: '82801HR/HO/HH (ICH8R/DO/DH) 6 port SATA AHCI Controller', Bus: 'PCI'
Storage-Controller:	Hersteller: 'Intel Corporation', Produkt: '82801BA IDE U100 Controller', Bus: 'PCI'
Netzwerkkarte:	Hersteller: 'Intel Corporation', Produkt: '82545EM Gigabit Ethernet Controller (Copper)', Sub-Model: '', Bus: 'PCI'
Weiterer Adapter:	Hersteller: 'Intel Corporation', Produkt: '82801BA/BAM AC'97 Audio Controller', Bus: 'PCI'
Optisches Laufwerk:	Hersteller: '', Produkt: 'CD-ROM [1]', Revision: 'FWR10003', Bus: 'SATA', Geschwindigkeit: '44'
Festplatte 1	Produkt: 'IBM Travelstar', Revision: 'F.13VFT4', Seriennummer: '9D27CWJVQECMS1N36DNV', Bus: 'SATA', Größe: 512 GB, Sektoren: 134217728
NIC MAC-Addresse:	00:1c:42:1e:bd:a6
Bios Informationen:	Bios Version: 8.0.18314.813278 Bios Datum: 05/09/07 Bios Seriennummer: 15411484855
MB-Chipsatz:	Intel Corporation / 82P965/G965 Memory Controller Hub
USB Anschlüsse:	1
USB2 Anschlüsse:	1

Hiermit bestätige ich, dass die Datenlöschung gemäß den Vorgaben des Softwareherstellers ordnungsgemäß durchgeführt wurde.

Ausführende Person

Aufsicht/Vorgesetzter

Weshalb ein Datenlösch-Management über den gesamten IT-Geräte-Lebenszyklus notwendig ist

Kunden und Mitarbeiter sind auf die Sicherheit ihrer persönlichen und geschäftlichen Daten angewiesen. IT-Geräte oder Speichermedien, die entsorgt werden, ohne dass die darauf enthaltenen Informationen sicher gelöscht wurden, können nicht nur der Marke und dem Image eines Unternehmens schaden, sondern auch fallende Aktienkurse, Verlust von Kunden und Geschäftspartnern und eine negative Presse zur Folge haben. Sorglos ausgesonderte Festplatten mit vertraulichen Informationen, die nicht gelöscht wurden, öffnen Tür und Tor für Datendiebstahl und bergen für Unternehmen Risiken einer negativen Publicity, kostspieliger Rechtsstreitigkeiten und gesetzlicher Strafen. Häufig wirkt sich dies auch negativ auf Mitarbeiter, den täglichen Geschäftsbetrieb und die interne Informationssicherheit aus.

Die Datenlöschung spielt auch in anderen Fällen eine wichtige Rolle. Falls Anwendung- und Systemsoftware auf Festplatten verbleiben, wenn die Geräte ausgemustert und weiterverkauft werden, werden vielfach Lizenzvereinbarungen der Softwarehersteller verletzt und können empfindliche Geldstrafen nach sich ziehen.

DATENSCHUTZ BEI AUSSERBETRIEBNAHME

Datensicherheit ist für Unternehmen selbstverständlich, um die auf IT-Equipment enthaltene Informationen während des gesamten Lebenszyklus zu schützen. Der Schutz dieser vertraulichen Daten im Zuge der Außerbetriebnahme von Geräten – oder wenn ein Rechner im Rahmen des Change-Management intern neu zugewiesen wird – ist ebenso wichtig, wird aber häufig außer Acht gelassen. Angesichts der großen Mengen vertraulicher Informationen, die auf diesen Geräten gespeichert sind, müssen alle Daten vollständig vernichtet werden, bevor die IT-Geräte ausgemustert, wiederverwendet, recycelt oder gespendet werden.

Ist ein durchgängiges Datenlösch-Konzept vorhanden, können IT-Geräte ohne Sorge um die ehemals vorhandenen sensiblen Daten weiterverkauft oder gespendet werden. In Kombination mit der Datenlöschung wird auch die physikalische Vernichtung zu einer praktikableren Lösung, da damit ein Höchstmaß an Sicherheit erreicht wird. Sollte die physikalische Vernichtung nicht erfolgreich oder es aufgrund technologischer Entwicklungen möglich sein, Daten selbst aus kleinen Teilen von Speichermedien auszulesen, garantiert die zuvor durchgeführte Datenlöschung trotzdem den nötigen Schutz.

DATEN AUF AKTIVEN SYSTEMEN

Aufgrund der Gesetze ist die Datenlöschung nicht nur am Ende des Life-Cycle von Bedeutung, sondern kann jederzeit erforderlich werden, beispielsweise wenn bestimmte personenbezogene Informationen auf einem aktiven System nicht länger benötigt werden. Moderne Datenlöschtools ermöglichen ein gezieltes Löschen und Vernichten einzelner Dateien und Ordner auf aktiven Systemen. Dieses Verfahren der permanenten Datenlöschung ist die ideale Lösung zum Entfernen vertraulicher Daten, die nur temporär benötigt werden, wie z. B. Angaben zu Kreditkarten, Kundeninformationen und geheime Geschäftsunterlagen. Ein modernes Datenlöschmanagement, das eine zeit- und ereignisgesteuerte Datenvernichtung unterstützt, bietet Datensicherheit für lokale oder dezentrale Server, Computer und für alle auf dem System befindlichen und individuell auswählbaren Dateien. Mehr noch, die Datenvernichtung im Alltag kann weitestgehend automatisiert werden und wird damit zum Kinderspiel.

Viele Unternehmen nutzen darüber hinaus in Rechenzentren kostenintensive und komplexe Systeme wie logische Laufwerke (LUN) und Speicher-Arrays. Da sich die Bereitstellung, Verwaltung und der Betrieb dieser Systeme von Desktops und Laptops grundsätzlich unterscheidet, besteht bei Löschvorgängen die Gefahr der Beeinträchtigung wichtiger Betriebsabläufe. Und weil Server oder Speicher-Arrays, auf denen geschäftskritische Anwendungen laufen, nicht ohne Weiteres abgeschaltet werden können und eine erneute Online-Schaltung nach einer Außerbetriebnahme immer mit einem erheblichen Zeit- und Kostenaufwand verbunden ist, bedarf es einer modernen Löschlösung, die in der Lage ist, definierte Daten, LUN oder Speicher-Arrays auf aktiven Systemen im laufenden Betrieb gezielt zu löschen.

DATENLÖSCHUNG VOR ORT

Unternehmen, die die Entsorgung von IT-Geräten auslagern wollen, sollten bei der Auswahl eines Dienstleisters darauf achten, dass dieser ein sicheres Löschverfahren mit vollständiger Informations- und Berichtsfunktion verwendet. Eine sichere Lösung ist vielfach die Datenlöschung vor Ort. Nur so wird gewährleistet, dass keine sensiblen Daten das Unternehmen oder ein bestimmtes Büro verlassen. Die International Association of IT Asset Managers (IAITAM)[11] empfiehlt einen dualen Ansatz. Im ersten Schritt werden die Daten vor Ort gelöscht, bevor die Altgeräte im zweiten Schritt an ein Entsorgungsunternehmen oder an ein Dienstleistungsunternehmen zur Löschung übergeben werden.

> *Die Datenlöschung ist nicht nur am Ende des Life-Cycle von Bedeutung, sondern wird immer dann erforderlich, wenn beispielsweise bestimmte vertrauliche Informationen auf einem aktiven System nicht länger benötigt werden.*

Strenge branchenspezifische und gesetzliche Vorschriften, monetäre Verluste, mögliche Imageschäden aufgrund von Datenschutzverletzungen und das Risiko dass Daten in fremde Hände gelangen könnten, sind gewichtige Gründe um ein professionelles Datenlösch-Management im Rahmen der IT-Sicherheitsstrategie umzusetzen. Ohne die erforderlichen Sicherheitsvorkehrungen drohen Unternehmen bei Datenschutzverletzungen Geldstrafen, angefangen von mehreren Zehntausend bis über 1 Million US-Dollar pro Verstoß.[12] In bestimmten Situationen setzen Unternehmen ihre Mitarbeiter durch ein Fehlen adäquater Sicherheitsmaßnahmen dem Risiko von Haftstrafen aus.

Vorteile einer zertifizierten, prozessorientierten Datenlöschsoftware

Obwohl viele Unternehmen mit dem Löschen von Daten bereits einen ersten Schritt auf dem Weg zur sicheren Entsorgung von Speichergeräten getan haben, bleibt der Einsatz von professionellen Lösungen, deren Leistungsfähigkeit und Sicherheit durch Zertifikate und Empfehlungen von unabhängigen nationalen und internationalen Organisationen bestätigt wurde, heute für Unternehmen und Behörden unerlässlich.

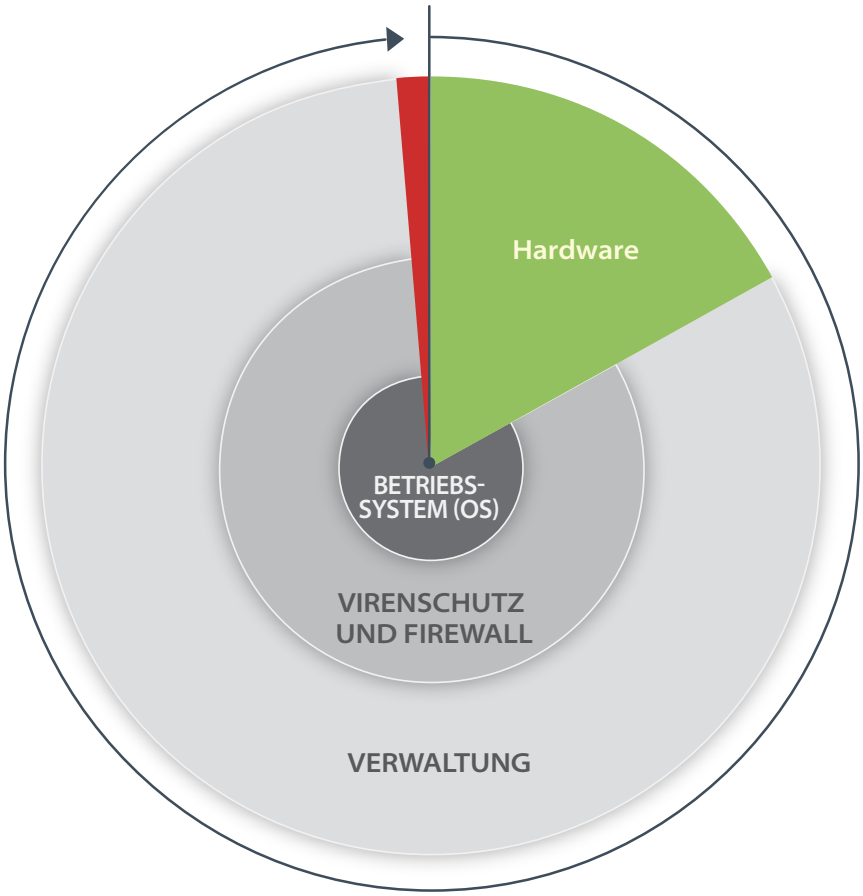
Der Einsatz einer zertifizierten Software, die neben einheitlichen und verlässlichen Ergebnissen auch Kontrollmöglichkeiten mittels Berichtsfunktion bietet, gibt Unternehmen, Behörden und anderen Einrichtungen erst die notwendige Sicherheit. Beispielsweise wird durch das international anerkannte Sicherheitszertifikat Common Criteria bestätigt, dass durch sorgfältige und unabhängige Tests die Eignung der Löschsoftware zum dauerhaften Löschen von Daten von Festplatten und anderen Speichermedien nachgewiesen wurde. Darüber hinaus wird durch das Zertifikat bestätigt, dass die Software den Standards der Internationalen Organisation für Normung entspricht (ISO-IEC 15408).

Der Einsatz einer prozessorientierten, zentral verwalteten und automati-sierten Datenlöschsoftware führt zu einer höheren Produktivität und Wirtschaftlichkeit.

Der Einsatz eines prozessorientierten, zentral verwalteten und automatisierten Datenlöschsystems führt außerdem zu einer Verbesserung der Produktivität und Effizienz. Dank einer zentralen Steuerung, Kontrolle und Prüfung, verbunden mit einem geringen manuellen Eingabeaufwand und der automatischen Bereitstellung aller Hardware- und Löschinformationen durch netzwerkbasierte Übertragung von Löschberichten, können menschliche Fehlerquellen nahezu ausgeschlossen werden. Gleichzeitig werden damit auch Prüfverfahren zur Erfüllung gesetzlicher Anforderungen einfacher und schneller durchführbar. Eine solche Lösung unterstützt nicht nur das sichere Löschen von Daten und Erstellen von Löschberichten, sondern auch eine Reihe umfangreicher automatischer und manueller Hardwaretests. Die Testprotokolle liefern die erforderlichen Informationen für eine Wiederverwendung und Weitervermarktung von IT-Geräten. Ein weiterer Vorteil einer solchen Lösung ist, dass im Vergleich zu herkömmlich angewendeten Verfahren bzw. Datenlöschlösungen, deutlich mehr IT-Geräte in kürzerer Zeit gelöscht werden können. Die Lösung lassen sich meist an die individuellen Anforderungen der Hardware- oder Netzwerkumgebungen von Unternehmen anpassen.

PROZESSMANAGEMENT

Eine umfassende und zentral gesteuerte Lösung für das automatisierte Datenlösch-Management vereinfacht den gesamten Prozess, vom Einschalten über die Rückmeldung an die Datenbank und die Initialisierung des Löschprozesses bis zum Ausschalten der Geräte. Eine Managementkonsole ermöglicht darüber hinaus die Fernkontrolle der Löschprozesse, die komplette Automatisierung mit minimaler Benutzerinteraktion und speichert zentral alle Datenlöschberichte, die zu Revisionszwecke leicht ausgewertet werden können. Damit ist im Vergleich zu anderen Verfahren eine Produktivitätssteigerung von 25% bis 30% möglich. IT-



Kosten des Datenlösch-Managements

Mitarbeiter sind mithilfe eines modernen Löschprozesses beispielsweise in der Lage, pro Server mehr als 200 Festplatten gleichzeitig zu löschen. Darüber hinaus ist auch die Remote-Kontrolle der Löschprozesse auf den verschiedenen Systemen jederzeit möglich.

Aufgrund der Effizienzvorteile, die sich durch die Zentralisierung und Automatisierung des Datenlöschverfahrens ergeben, ist der Investitionsaufwand für eine solche Software am Ende des Tages gering. Unter Berücksichtigung der Risiken, der möglichen Geldstrafen aufgrund von Datenschutzverletzungen und im Verhältnis zu den Gesamtgerätekosten, einschließlich Hardware, Software, Firewall und Virenschutz, ist der Anschaffungspreis für einen gesteuerten Datenlöschprozess minimal.

Operativ und ökonomisch entscheidend ist häufig auch, welche Möglichkeiten der nahtlosen Integration einer Datenlöschlösung in die bestehende IT-Infrastruktur gegeben sind. Dies beinhaltet die Kompatibilität mit anderen IT-Asset-Management-Lösungen und ERP-Suiten sowie die Möglichkeit des einfachen Datenimports und -exports und die Nutzung webbasierter Schnittstellen.

Fazit

Die Flut an Datensicherheits- und Datenschutzbestimmungen, das ständige Risiko von Datenlücken und die hohen Kosten im Zusammenhang mit Datenschutzverletzungen lassen keine Zweifel an der Notwendigkeit einer vollständigen und sicheren Vernichtung sensibler Daten. In vielen Fällen sind Datenschutzverletzungen nicht auf Hackerangriffe oder andere versteckte Aktivitäten zurückzuführen, sondern auf eine unsachgemäße Entsorgung von IT-Geräten. Studien zeigen, dass in zehn Prozent aller Fälle von Datenverlust eine falsche und unzureichende Datenlöschung die Ursache ist.[12]

Da die IT-Geräte von Unternehmen künftig immer größere Mengen vertraulicher Informationen enthalten werden, ist der Einsatz einer umfassenden Datenlöschlösung zum Schutz von Daten oberstes Gebot. Bevor IT-Geräte entsorgt, recycelt, wiederverwendet oder gespendet werden, müssen alle darauf gespeicherten Daten vollständig vernichtet werden. Darüber hinaus sind Unternehmen in vielen Fällen aufgrund der steigenden Zahl behördlicher und branchenspezifischer Standards und Vorschriften verpflichtet, eine sichere und nachweisbare Vernichtung sensibler Informationen zu gewährleisten. Andernfalls drohen erhebliche Strafen.

Mit einem modernen und zentralisierten Datenlöschsystem steht eine schnelle, automatisierte und sichere Lösung zum Schutz ihrer vertraulichen Daten zur Verfügung, mit der sich zudem Zeit und Kosten sparen lassen.

Die Datenlöschung zeichnet sich durch einen softwarebasierten Ansatz zum Überschreiben von Daten und zur Vernichtung aller elektronischen Informationen auf Festplatten oder anderen digitalen Speichermedien aus, ohne jedoch die Funktionsfähigkeit des Datenträgers zu zerstören. Moderne Datenlöschtools bieten verschiedene Konfigurationsmöglichkeiten, die ein gezieltes Löschen vertraulicher Daten auf aktiven Systemen unterstützen. Nicht zuletzt deshalb ist die Anschaffung einer Datenlöschsoftware eine Entscheidung, die nicht erst am Ende eines Lebenszyklus getroffen werden sollte, sondern bereits zum Zeitpunkt der ersten Inbetriebnahme eines IT-Geräts.

Mit einem modernen und zentralisierten Datenlöschsystem steht Unternehmen und Behörden ein schnelle, automatisierte und sichere Lösung zum Schutz ihrer vertraulichen Daten zur Verfügung, mit dem sich darüber hinaus Zeit und Kosten sparen lassen. Dank automatisierter Datenlöschfunktionen erhalten IT-Abteilungen eine Lösung, die sich wie keine andere an die individuellen Anforderungen anpassen lässt, und ein Maximum an Geschwindigkeit, Effizienz und Sicherheit beim Lösch-, Berichts- und Auditprozess bietet.

Quellen- und Literaturverzeichnis

[1] KPMG International, "Data Loss Barometer –Insights into Lost and Stolen Information in 2010," Issue 3, 2010

[2] Kessler International, "Is Your Confidential Information Being Sold on eBay?", February 2009, http://www.investigation.com/press/press75.htm

[3] IDC, sponsored by EMC Corporation, "Extracting Value from Chaos," June 2011, http://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf

[4] Obama Administration, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," February 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

[5] European Commission, January 2012, http://ec.europa.eu/justice/data-protection/index_en.htm

[6] MaaSters Blog, "Enterprise Mobility Update: 350 Million BYOD Smartphones by 2014," August 2012, http://www.maas360.com/maasters/blog/businessintelligence/ enterprise-mobility-350-million-byod-smartphones-2014/

[7] Juniper Research, August 2012, http://www.juniperresearch.com/viewpressrelease.php?pr=330

[8] *Government Technology*, "4.2 Million Cell Phone Users Leave Sensitive Data Unprotected," March 2009, http://www.govtech.com/security/42-Million-Cell-Phone.html

[9] ENISA, "Smartphones: Information Security Risks, Opportunities and Recommendations for Users," December 2010, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks/top-ten-smartphone-risks

[10] ABI Research, "Recycled Handset Shipments to Exceed 100 Million Units in 2012," December 2007, http://www.abiresearch.com/press/1015-Recycled+Handset+Shipments+to+Exceed+100+Million+Units+in+2012

[11] http://www.iaitam.org/

[12] *Dark Reading*, "$1.5M Fine Marks A New Era In HITECH Enforcement," March 2012, http://www.darkreading.com/database-security/167901020/security/vulnerabilities/232700031/1-5m-fine-marks-a-new-era-in-hitech-enforcement.html

Kroll Ontrack®

+49 (0)7031 644 290, software@krollontrack.de
www.krollontrack.de, www.krollontrack.ch