blancco
CERTIFIED DATA ERASURE

Mobile Geräte am Arbeitsplatz:

DATENLÖSCHSTRATEGIEN FÜR UNTERNEHMEN

Blancco White Paper

Veröffentlicht am 17. Januar 2013

Einführung

Moderne mobile Endgeräte wie Smartphones und Tablets entwickeln sich immer mehr zu unverzichtbaren Werkzeugen, die sowohl die Zufriedenheit als auch die Produktivität von Mitarbeitern am Arbeitsplatz erhöhen. Einer kürzlich unter US-amerikanischen und europäischen Unternehmen durchgeführten Umfrage zufolge, stellen mittlerweile 77 % aller Unternehmen einem Teil ihrer Mitarbeiter Smartphones zur Verfügung.[1]

Während in der Vergangenheit überwiegend Mitarbeiter in leitender Funktion sowie im Vertrieb und Marketing von ihren Arbeitgebern mit Mobiltelefonen ausgestattet wurden, führt die BYOD-Revolution („Bring Your Own Device“) zu einer grundlegenden Veränderung des Arbeitsalltags, in dem diese Geräte von immer mehr Mitarbeitern in unterschiedlichsten Funktionen genutzt werden. Nach IDC-Prognosen sollen 2013 mehr als die Hälfte aller Business-Smartphones privat von Mitarbeitern gekauft werden.[2] Gartner geht von Schätzungen aus, wonach in diesem Jahr[1,2] Milliarden Smartphones und Tablets verkauft werden, und dass bis 2016 zwei Drittel aller mobilen Arbeitskräfte ein Smartphone besitzen werden.[3]

Unternehmen müssen im Rahmen einer professionellen Sicherheitsstrategie für mobile Endgeräte die Risiken kennen und minimieren, die mit einer unsachgemäßen Außerbetriebnahme einhergehen.

Zusammengenommen verfügen diese mobilen Endgeräte über Billionen von Gigabyte an Speicherkapazität. Angesichts des anhaltenden Drucks auf Unternehmen, das Arbeiten mit privaten Geräten (BYOD) zu gestatten und zu fördern, könnten sich auf diesen Geräten bald große Mengen an sensiblen Unternehmens-, Kunden- und Mitarbeiterdaten befinden. Eine vor kurzem durchgeführte Studie hat jedoch gezeigt, dass 71 % der Unternehmen, die BYOD gestatten, nicht über konkrete Strategien und Richtlinien zum Schutz dieser Daten verfügen.[4]

Selbst wenn das Thema Sicherheit angegangen wird, werden Sicherheitsbedrohungen meist nur in Form von Malware und Phishing- und Spyware-Attacken auf mobile Geräte gesehen. Eine unsachgemäße Außerbetriebnahme von Altgeräten kann allerdings ein noch größeres Sicherheitsrisiko darstellen, das jedoch häufig vernachlässigt wird.

Eine professionelle Sicherheitsstrategie für mobile Geräte erfordert, dass Unternehmen die Risiken kennen und berücksichtigen, die mit einer unsachgemäßen Außerbetriebnahme einhergehen, z. B. wenn ein Smartphone oder Tablet ausgemustert, einem anderen Nutzer zur Verfügung gestellt oder dem Recycling zugeführt werden soll. Unternehmen sollten bei einer Sicherheitsstrategie für mobile Geräte die Einhaltung gesetzlicher Vorschriften bei der Datenlöschung bzw. Entsorgung von IT-Geräten beachten. Um eine absolute Sicherheit für mobile Geräte gewährleisten zu können, sollten Unternehmen dabei auf die Implementierung professioneller Löschprodukte setzen, die einen überprüfbaren Nachweis der sicheren Datenlöschung bieten oder sich einen zuverlässigen IT-Remarketing Partner bzw. ein Recyclingunternehmen für mobile Geräte suchen, das eine solche Software einsetzt. Mit den entsprechenden Fachkenntnissen und der richtigen Technologie bzw. dem richtigen Technologieanbieter können IT Asset Manager Sicherheitsstrategien implementieren, die sowohl den Schutz von Daten auf firmeneigenen als auch auf privaten Mobilgeräten von Mitarbeitern gewährleisten.

Inhalt

Warum mobile Geräte löschen?

Neben der Ausbreitung von firmeneigenen und privaten mobilen Geräten am Arbeitsplatz gibt es weitere wichtige Gründe, die eine Sicherheitsrichtlinie für mobile Geräte, welche auch eine sichere Datenlöschung beinhaltet, notwendig machen. Dabei spielen die Art der Nutzung und die gesetzlichen Bestimmungen zum Schutz von Daten eine wichtige Rolle.

KLEINE GERÄTE – GROSSE RISIKEN

Mit mehr Rechenleistung als Apollo 11 bei der Mondlandung, enthalten mobile Geräte trotz ihrer Kompaktheit heute eine Fülle von Informationen. Einige Smartphones und Tablets verfügen sogar über eine interne Speicherkapazität von bis zu 64 GB. Je intelligenter diese speicherstarken Geräte sind und je häufiger sie für berufliche und private Zwecke eingesetzt werden, desto höher ist die Wahrscheinlichkeit, dass darauf E-Mails, Kundendaten, Passwörter und andere sensible Informationen gespeichert sind. Sollten diese Geräte entsorgt werden, ohne die darauf enthaltenen Informationen zuvor zu löschen, kommt es mit hoher Wahrscheinlichkeit zu Datenschutzverletzungen.

So hat eine Studie aus dem Jahr 2009 ergeben, dass 99 % der Personen 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.[5]

Mit zunehmender Entwicklungsgeschwindigkeit steigt auch das Risiko des Datenmissbrauchs. Studien zeigen, dass persönliche und geschäftliche Daten, die auf Smartphones und Tablets gespeichert sind, vielfach den Weg auf den Gebrauchtmarkt finden – wenn auch unbeabsichtigt. Eine Untersuchung aus dem Jahr 2008 hat herausgefunden, dass ein Fünftel aller mobilen Kommunikationsgeräte im Recyclingmarkt sensible Informationen enthielten.[6] Jüngere, informelle Studien kommen zu noch dramatischeren Ergebnissen, wonach der Anteil dieser Geräte zwischen 60% und 99% liegt.[7,8]

Bei einer in Großbritannien durchgeführten Umfrage gaben 81 % der Befragten an, vor dem Verkauf ihrer Mobiltelefone alle darauf befindlichen Daten gelöscht zu haben. Sechs von zehn Befragten waren sich sicher, die Daten unwiderruflich gelöscht zu haben.[9] Alarmierend ist, dass die Mehrheit derjenigen, die ihre Mobiltelefone gelöscht hatten, dies nach eigenen Angaben manuell getan hat. Derart gelöschte Daten können größtenteils mit einfachen Mitteln wiederhergestellt werden.

RECHTLICHE ASPEKTE

Die Folgen bei Datenpannen von einem Tablet oder Smartphone können genauso verheerend sein wie der Missbrauch von Daten von einem Server oder Laptop. Unternehmen riskieren im Falle von Datenmissbrauch nicht nur einen Imageschaden, sondern auch Geldstrafen aufgrund von Verstößen gegen branchenspezifische Vorschriften, wie z. B. Verstöße gegen die Bestimmungen zum Verbot der Offenlegung von Kreditkarteninformationen oder anderen personenbezogenen Kundendaten gemäß dem Payment Card Industry Data Security Standard (PCI DSS) oder gemäß dem Bundesdatenschutz oder in den Vereinigten Staaten bei personenbezogener Gesundheitsdaten aufgrund des HIPAA. Auch die Nutzung des Smartphones als Kreditkartenterminal ist für Unternehmen keine Zukunftsmusik mehr. Darüber hinaus zeigen Studien, dass mittlerweile 80 % der Ärzte in den USA Smartphones und medizinische Anwendungen in ihrem Praxisalltag nutzen.[10]

Die Obama-Administration hat im Februar 2012 in den Vereinigten Staaten die Consumer Privacy Bill of Rights verabschiedet, die ein dynamisches Modell zur Förderung voranschreitender Innovationen bei gleichzeitiger Wahrung eines strengen Datenschutzes unterstützt und Auflagen zum Löschen von Daten enthält. Da es in den USA bisher kein umfassendes Gesetz zum Schutz personenbezogener Daten und zum Schutz der Privatsphäre gibt, haben 46 Bundesstaaten Rechtsvorschriften erlassen, die eine Meldepflicht bei Datenschutzverletzungen in Bezug auf personenbezogene Informationen enthalten. Trotz Unterschiede innerhalb der Gesetze der einzelnen Bundesstaaten, sieht die Mehrzahl zivil- und strafrechtliche Sanktionen bei Verstößen vor.

Inzwischen wurde auch in Europa eine Änderung der Bestimmungen der seit 1995 bestehenden Datenschutzrichtlinie der EU vorgeschlagen. Ein Entwurf dieser Änderungen wird derzeit von allen Mitgliedstaaten der EU überprüft. Die Verabschiedung der neuen Datenschutz-Verordnung, die auch Bestimmungen zum Löschen von Online-Daten und zur Nutzung auditierbarer Verfahren für datenverarbeitende Unternehmen vorsieht, ist geplant. Darin wird auch der Einsatz von zertifizierten Tools und Verfahren befürwortet. Bei Verstößen gegen diese neuen Bestimmungen drohen Geldstrafen zwischen 250.000 Euro und bis zu 0,5 % des jährlichen Gesamtumsatzes bei kleineren Vergehen und zwischen 1 Million Euro und bis zu 2 % des Umsatzes bei schwerwiegenderen Verstößen.

> *Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) hat ausdrücklich darauf hingewiesen, dass eine unsachgemäße Ausmusterung von Smartphones infolge einer unvollständigen Datenlöschung eines der größten Risiken der Informationssicherheit darstellt.*

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) hat ausdrücklich hervorgehoben, dass eine unsachgemäße Ausmusterung von Smartphones infolge einer unvollständigen Datenlöschung eines der größten Informationssicherheitsrisiken darstellt. Dennoch wird bei diesen Geräten – anders als bei gebrauchten Festplatten – meist nicht auf professionelle Löschprozesse zurückgegriffen, die heute zur Verfügung stehen.[11] Besonders besorgniserregend ist dies vor dem Hintergrund, dass Analysteneinschätzungen zufolge heute über 100 Millionen Mobiltelefone wiederverwendet werden.[12]

Datensicherheit durch geprüfte Technologie

Angesichts des erheblichen Risikos bei Datenmissbrauch benötigen Unternehmen eine ausfallsichere Methode, um alle Informationen von internen und externen Speichern mobiler Geräte zu löschen, bevor diese wiederverwendet, eingelagert oder vernichtet bzw. recycelt werden. Eine solche Methode geht über das einfache Zerstören der SIM-Karte hinaus und löscht alle Daten auf internen Speichern und externen Speicherkarten, die nicht so leicht zugänglich sind. Die physische Vernichtung von mobilen Geräten allein reicht nicht aus. Zum einen ist es selbst bei zerstörten Datenträgern möglich, Informationen auszulesen, zum anderen ist ein solcher Ansatz weder nachhaltig noch umweltfreundlich.

Viele Nutzer gehen davon aus, dass durch ein Zurücksetzen des Smartphones auf den Fabrikzustand alle Daten auf dem internen Speicher gelöscht werden. Tatsächlich sind die Daten in den meisten Fällen jedoch noch vorhanden. Zwar mag ein Laie Schwierigkeiten haben, die Daten wiederherzustellen, für einen erfahrenen Hacker oder Computerforensiker stellt dies jedoch kein Problem dar.

Ein manipulationssicheres und revisionssichereres Lösch-Reporting ist für die Erfüllung behördlicher und rechtlicher Vorgaben unverzichtbar. Ohne einen solchen Datenlöschbericht haben Unternehmen keine Gewissheit, dass ihre Daten wirklich gelöscht wurden.

Ein Verfahren diese Daten sicher zu Entfernen ist der Einsatz einer Software, die alle Gerätespeicher vollständig überschreibt. Einige Herstelleranwendungen nutzen zwar ähnliche Verfahren, diese lassen jedoch einen wichtigen Aspekt vermissen: einen überprüfbaren Bericht mit Seriennummern und anderen Hardwareangaben, der nachweislich belegt, dass die Daten komplett entfernt wurden. Eine solche Funktion ist zur Einhaltung gesetzlicher Vorschriften, dem Auschluß menschlicher Fehler und zur gefahrlosen Weiterveräußerung oder Weiterbenutzung der Geräte

unerlässlich. Darüber hinaus sind solche Anwendungen in der Regel nur mit dem Betriebssystem des jeweiligen Geräts kompatibel und müssen aufwendig manuell ausgeführt werden.

PROFESSIONELLE DATENLÖSCHUNG

Eine anerkannte und geprüfte Datenlöschlösung basiert auf einer Überschreib-Software, die neben technischen Vorteilen zahlreiche Vorteile bei der Sicherheit und Produktivität besitzt. Damit können nicht nur alle Daten von einem mobilen Gerät sicher entfernt, sondern auch ein detaillierter Prüfbericht als Nachweis für eine erfolgreiche Datenlöschung erstellt werden. Ein manipulationssicheres und nachvollziehbares Lösch-Reporting ist für die Erfüllung behördlicher und rechtlicher Vorgaben unverzichtbar. Ohne ein solches Reporting haben Unternehmen keine Gewissheit, dass ihre Daten wirklich sicher gelöscht sind. Ausführliche Löschberichte enthalten wichtige Informationen für Audit-, Wiederverkaufs- und Sicherheitszwecke: Zustand der Hardware, Seriennummern und Typenbezeichnungen, Softwareinformationen zur Lizenzübertragung und von wem die Löschung wann durchgeführt wurde.

Aufgrund einer breiten Funktionalität bietet die Datenlöschung zahlreiche weitere Vorteile. Eine moderne Datenlöschtechnologie arbeitet unter anderem mit internationalen Datenlöschstandards wie HMG Infosec und DoD 5220.22-M. Die Einhaltung dieser Standards im Rahmen der Datenlöschung ist von Behörden und bei einigen Branchen längst vorgeschrieben. Allerdings wurden bisher noch keine gemeinsamen Löschstandards für alle Smartphones definiert. Das National Institute of Standards and Technology (NIST) arbeitet gerade an der Aktualisierung seiner Richtlinien zum Löschen von mobilen Geräten und SSD-Festplatten. Gleichzeitig arbeitet das Device Renewal Forum (DRF) an der Entwicklung eines einheitlichen Verfahrens zur Prüfung und Zertifizierung von wiederaufbereiteten Smartphones, Feature Phones, USB-Modems und anderen drahtlosen Geräten, um zu gewährleisten, dass diese einheitlich hohen Qualitäts- und Leistungsstandards entsprechen. Blancco arbeitet gemeinsam mit den anderen DRF-Mitgliedern an den Richtlinien für ein sicheres Datenlöschverfahren, welches den Datenschutz und das sichere Löschen von Informationen bei wiederaufbereiteten Mobilgeräten gewährleistet.

Automatisierte Löschprozesse dauern nur wenige Minuten. Dadurch ist es einem einzelnen Nutzer möglich, mehrere Hundert Smartphones pro Tag zu löschen, was die Software zu einer Lösung mit hoher Wirtschaftlichkeit macht.

Auch Unternehmen und Remarketing-/Recyclingfirmen sollten auf ein professionelles Datenlöschtool setzen, dessen Sicherheit und Effektivität bei der Datenlöschung von einer unabhängigen, international anerkannten Prüfstelle bestätigt wurde. Durch ein solches Zertifikat erhalten Unternehmen, Remarketingfirmen und Recyclingspezialisten, die ein solches Löschverfahren nutzen, absolute Gewissheit, dass alle Daten von den betreffenden mobilen Geräten entfernt wurden.

HÖHERE PRODUKTIVITÄT DURCH AUTOMATISIERTE PROZESSE

Ein weiteres wichtiger Vorteil einer professionellen Datenlöschsoftware ist die Möglichkeit für Nutzer, den gleichen Löschprozess für mehrere mobile Geräte zu automatisieren und beispielsweise von einem herkömmlichen Desktop auszuführen. Die Einrichtung eines automatisierten Löschprozesses selbst dauert nur wenige Minuten. Dadurch ist es einem einzelnen Nutzer möglich, mehrere Hundert Smartphones pro Tag zu löschen, was die Software zu einer hocheffizienten Lösung macht. Dank automatischer Übermittlung von Löschberichten an eine zentrale Konsole profitieren Unternehmen und Wiedervermarktungsfirmen von einer deutlichen Produktivitätssteigerung.

Neben der Leistungsfähigkeit überzeugt eine moderne Löschsoftware, dass Daten bei allen gängigen Smartphone- und Tablet-Plattformen richtig erkannt und sicher gelöscht werden. Möglich ist dies durch die direkte Kommunikation mit den verschiedenen Betriebssystemen. Unterstützt werden sollten auch die gängigen Betriebssysteme: iOS, Nokia Symbian, Android, Windows Mobile und BlackBerry. Diese Plattform-Flexibilität gewinnt angesichts der Vielzahl unterschiedlicher mobiler Geräte, die auf dem Markt erhältlich sind, zunehmend an Bedeutung, da für jeden Gerätetyp ein etwas anderer Löschprozess erforderlich ist.

Anforderungen zum Löschen bei unterschiedlichen Plattformen	
Apple iOS	iPhones, iPods und iPads sind verschlüsselt. Es muss deshalb der Verschlüsselungs-Schlüssel sicher und nachweislich überschrieben werden, damit Nutzerdaten nicht wiederhergestellt werden können.
Android	Bei Android Geräten ist ein Überschreiben der Nutzerdatenbereiche notwendig. Das Zurücksetzen auf den Fabrikzustand und/oder Formatieren bietet keine ausreichende Sicherheit; denn diese Daten können problemlos wiederhergestellt werden.
BlackBerry	Bei BlackBerrys müssen die IT-Policies und Anwendungen von Drittanbietern gelöscht sowie die Nutzerdatenbereiche überschrieben werden.
Nokia Symbian	Bei Nokia Symbian Geräten ist ein Überschreiben der Nutzerdatenbereiche erforderlich. Ein Zurücksetzen auf den Fabrikzustand ist unzureichend.
Windows Mobile	Bei Windows Mobile Geräten ist ein Überschreiben der Nutzerdatenbereiche erforderlich. Ein Zurücksetzen auf den Fabrikzustand ist unzureichend.

Umsetzung einer Datenlöschrichtlinie

Die sichere Verwaltung moderner mobiler Geräte am Arbeitsplatz erfordert, dass Unternehmen für eine Reihe von Sicherheitsrisiken gewappnet sind. Experten raten zum Schutz sensibler und geheimer Geschäftsinformationen zur Entwicklung einer klaren Sicherheitsstrategie in Form einer Richtlinie für mobile Geräte.[13] Da die Nutzung privater Endgeräte für geschäftliche Zwecke in vielen Unternehmen mittlerweile gestattet oder begrüßt wird, muss eine solche Richtlinie komplexe Szenarien berücksichtigen.[14]

EIN DATENLÖSCHKONZEPT IMPLEMENTIEREN

Ebenso wichtig wie die Wahl der richtigen Technologie zum Löschen von Daten von mobilen Geräten ist die Einbindung dieser Technologie in eine klare Richtlinie zur Nutzung mobiler Geräte durch Mitarbeiter. Falls es sich bei einem mobilen Gerät um Firmeneigentum handelt, sollten hierfür in Bezug auf die Datenlöschung die gleichen Richtlinien wie für firmeneigene Laptops oder andere Computergeräte gelten.

Sollte ein Unternehmen beispielsweise beabsichtigen, ein Smartphone oder ein Tablet zu verkaufen, zu spenden oder einem anderen Nutzer zur Verfügung zu stellen, empfiehlt die International Association of IT Asset Managers (IAITAM) in ihren "Best Practices" den Einsatz eine professionelle Datenlöschlösung, um sicherzustellen, dass alle Daten wirklich entfernt wurden, bevor das Gerät die Geschäftsräume verlässt.[15] Dazu müssen die IT-Mitarbeiter eines Unternehmens lediglich die Löschsoftware starten. Als Alternative bietet sich für Unternehmen auch die Möglichkeit, ein Verwertungsunternehmen zu beauftragen, das eine anerkannte Datenlöschung vor Ort durchführt oder einen sicheren Transport gewährleistet, um die mobilen Geräte mit einem professionellen Verfahren in den eigenen Räumen zu löschen. Die IT-Mitarbeiter oder Asset Manager können anschließend den eindeutigen Löschbericht mit den vorhandenen Asset Daten abgleichen mit dem sich nachweisen lässt, dass alle Daten gelöscht wurden.

BERÜCKSICHTIGUNG PRIVATER ENDGERÄTE IN DER SICHERHEITSRICHTLINIE

Heutzutage werden immer mehr private Endgeräte für geschäftliche Zwecke genutzt, und dieser Trend wird sich voraussichtlich in den kommenden Jahren fortsetzen. Gartner schätzt, dass bis 2014 90 % aller Unternehmen die Nutzung von Geschäftsanwendungen auf privaten Geräten unterstützen werden. Damit zeichnet sich ein komplexes Szenario für den Schutz sensibler Geschäftsinformationen ab.[16]

> *Experten raten zum Schutz sensibler und geheimer Geschäftsinformationen die Umsetzung einer klaren Sicherheitsstrategie in Form einer Richtlinie für mobile Geräte.*

Viele Unternehmen haben erkannt, dass ihre Mitarbeiter zufriedener und produktiver sind, wenn sie mobile Geräte nach ihren persönlichen Präferenzen auswählen und einsetzen können. Dadurch sind die Verwaltungs- und Supportkosten für das Unternehmen schnell amortisiert. Allerdings bergen diese Modelle auch ein Sicherheitsrisiko, insbesondere dann, wenn es an vernünftigen Sicherheitsstrategien fehlt. Besonders groß ist das Sicherheitsrisiko, wenn solche Geräte den Besitzer wechseln.

Eine Sicherheitsrichtlinie für mobile Geräte bedarf daher expliziter Bestimmungen zur Nutzung privater mobiler Endgeräte für geschäftliche Zwecke. Wichtiger Aspekt einer solchen Sicherheitsrichtlinie ist die Registrierung der Seriennummer des Geräts durch die IT-Abteilung, die dann die Möglichkeit hat, die Zugriffe auf Unternehmensdaten von dem Gerät zu überwachen.

Ferner erfordert eine solche Richtlinie eine schriftliche Erklärung der Mitarbeiter, in der versichert wird, dass sie das Gerät vor der Entsorgung oder vor einem Upgrade auf ein neues Modell,

wie dies bei Mobilfunkverträgen üblich ist, der Firma zur Datenlöschung aushändigen. Die Datenlöschung erfolgt erst, nachdem alle sensiblen Geschäftsinformationen von dem Gerät heruntergeladen und gesichert wurden.

Auch wenn Unternehmen in der Regel keinen Support für private mobile Geräte anbieten, sollten sie ein Mindestmaß an Sicherheitsmaßnahmen definieren, indem sie ihren Mitarbeitern ein Tool zum Löschen von Daten zur Verfügung stellen, falls die Datenlöschung nicht von der IT-Abteilung selbst durchgeführt wird. Gemäß der Richtlinie für die Nutzung mobiler Geräte haftet der Mitarbeiter und das Unternehmen als Eigentümer der Daten für die Offenlegung von Unternehmensinformationen, die auf dem Smartphone oder Tablet gespeicherten sind, bis die IT- oder Helpdesk-Mitarbeiter den Löschbericht erhalten haben, unabhängig davon, ob der Bericht von dem Mitarbeiter oder einem IT-Techniker stammt.

Sollten Mitarbeiter Bedenken bezüglich der Löschung ihres Smartphones oder Tablets oder anderer Sicherheitsmaßnahmen haben, können Unternehmen Anreize schaffen, die eine aktive Unterstützung der Richtlinie fördern. Forrester empfiehlt Unternehmen zum Beispiel, einen Teil der monatlichen Mobilfunkrechnung zu übernehmen, je nachdem, in welchem Umfang das Gerät für geschäftliche Zwecke genutzt wird.[13]

Fazit: Eine nachprüfbare Datenlöschung erhöht die Sicherheit mobiler Geräte

IT Asset Manager von Unternehmen müssen im Rahmen einer soliden Sicherheitsrichtlinie für mobile Geräte nachvollziehen können, welche Nutzer mit welchen Geräten auf Unternehmensdaten zugreifen, unabhängig davon, ob der Zugriff über firmeneigene oder private Geräte erfolgt. Ein wichtiger Aspekt einer solchen Richtlinie ist die revisionssichere Löschung von Smartphones und Tablets, bevor diese entsorgt, wiederverwendet oder weiterverkauft werden. Dabei handelt es sich um eine wichtige Sicherheitsmaßnahme, um Datenmissbrauch, Geldstrafen und andere negative Folgen für das Unternehmen zu vermeiden.

Durch die automatisierte Erstellung ausführlicher Löschberichte, die Unterstützung zahlreicher Geräteplattformen und die Fähigkeit, mehrere Geräte gleichzeitig zu löschen, bietet eine professionelle Datenlöschsoftware eine sichere und wirtschaftliche Lösung für Unternehmen und Remarketing Firmen. Dank neuester technologischer Standards und internationaler Prüfbestätigungen bietet eine professionelle Software die sichere Gewissheit, dass alle Daten vor dem Weiterverkauf oder der Wiederverwendung des Geräts gelöscht wurden.

Quellen- und Literaturverzeichnis

[1] IDC, "IDC Benchmark Study Examines Enterprise Mobile Device Policies," 04 June 2012, http://www.idc.com/getdoc.jsp?containerId=prUS23519412

[2] Blackberry, "Employee-owned Smartphones: Seize the Opportunity," White paper

[3] *TechCrunch.com*, "Gartner: 1.2 Billion Smartphones, Tablets To Be Bought Worldwide In 2013; 821 Million This Year: 70% Of Total Device Sales," 6 November 2012, http://techcrunch.com/2012/11/06/gartner-1-2-billion-smartphones-tablets-to-be-bought-worldwide-in-2013-821-million-this-year-70-of-total-device-sales/

[4] KnowBe4 – ITIC, "KnowBe4 and ITIC Latest Study Reveal Companies Lack Security for 'BYOD'," 04 September 2012, http://www.prweb.com/releases/2012/9/prweb9858074.htm

[5] *Government Technology*, "4.2 Million Cell Phone Users Leave Sensitive Data Unprotected," 19 March 2009, http://www.govtech.com/security/42-Million-Cell-Phone.html

[6] *Businessweek*, "The Recycled Cell-Phone Trap," 3 November 2008, http://www.businessweek.com/technology/content/nov2008/tc2008113_981236.htm

[7] *PC World*, "Your Old Smartphone's Data Can Come Back to Haunt You," 10 July 2011, http://www.pcworld.com/article/235276/your_old_smartphones_data_can_come_back_to_haunt_you.html

[8] *Dark Reading*, "Old Smartphones Leave Tons Of Data For Digital Dumpster Divers," 15 December 2011, http://www.darkreading.com/mobile-security/167901113/security/news/232300628/old-smartphones-leave-tons-of-data-for-digital-dumpster-divers.html

[9] CPPGroup plc, "Second Hand Mobiles Contain Personal Data," 22 March 2011, http://www.prnewswire.com/news-releases/second-hand-mobiles-contain-personal-data-118434314.html

[10] *Healthcare Technology Online*, "Bracing For Healthcare's Mobile Explosion," 6 January 2012, http://www.healthcaretechnologyonline.com/article.mvc/Bracing-For-Healthcares-Mobile-Explosion-0001?sectionCode=Welcome&templateCode=EnhancedStandard&user=2431702&source=nl:32854\

[11] ENISA, http://www.enisa.europa.eu/act/application-security/smartphone-security-1/top-ten-risks/top-ten-smartphone-risks?searchterm=Top+Ten+Smartphone+

[12] ABI Research, "Recycled Handset Shipments to Exceed 100 Million Units in 2012, 20 December 2007, http://www.abiresearch.com/press/1015-Recycled+Handset+Shipments+to+Exceed+100+Million+Units+in+2012"

[13] *CIO*, "Managing Mobile Devices: 10 Lessons Learned, via Forrester," 22 September 2011, http://www.cio.com/article/690281/Managing_Mobile_Devices_10_Lessons_Learned_via_Forrester

[14] *Government Security News*, "The Urgent Need for Mobile Device Security Policies," 14 November 2011, http://www.gsnmagazine.com/article/24983/urgent_need_mobile_device_security_policies

[15] International Association of Information Technology Asset Managers (IAITAM)

[16] Gartner, "Gartner Reveals Top Predictions for IT Organizations and Users for 2011 and Beyond," 2010, http://www.gartner.com/it/page.jsp?id=1480514

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