Verwendung von Festplattenvollverschlüsselung im geschäftlichen und privaten Umfeld

Christoph Sibinger Tilo Müller

Lehrstuhl für Informatik 1
Friedrich-Alexander-Universität Erlangen-Nürnberg
Martensstr. 3, 91054 Erlangen

christoph.m.sibinger@informatik.stud.uni-erlangen.de, tilo.mueller@informatik.uni-erlangen.de

Abstract: Festplattenvollverschlüsselung (engl. *Full Disk Encryption (FDE)*) stellt eine benutzerfreundliche und sichere Methode zum Schutz sensitiver Daten gegen physische Angriffe dar. Während es für den US-amerikanischen Markt in den letzten Jahren eine Reihe von Studien zur Verwendung von FDE gegeben hat, betrachtet die vorliegende Arbeit den deutschen Markt. Neben der Verwendung von FDE auf Laptops werden Smartphones in Betracht gezogen, und zusätzlich zum geschäftlichen Einsatz die private Nutzung untersucht. Zu diesem Zweck wurden Internet-gestützte Umfragebögen erstellt, in der die Teilnehmer zur eingesetzten Verschlüsselungstechnik und den jeweiligen Gründen befragt wurden, sowie Hintergrundwissen getestet wurde. Im Rahmen der Studie nahmen 1.034 Privatpersonen teil und 37 Unternehmen, wobei die Hälfte der befragten Unternehmen mindestens 1.000 Mitarbeiter beschäftigt und ein Drittel mindestens 10.000 Mitarbeiter.

1 Einleitung

Durch das Bundesdatenschutzgesetz (BDSG) schreibt der Gesetzgeber seit 1990 allen "Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen" vor, "technische und organisatorische Maßnahmen zu treffen (...) um die Ausführung der Vorschriften dieses Gesetzes (...) zu gewährleisten". Diese Vorschrift gilt "wenn der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht" (§9 BDSG). Durch eine zunehmend große Auswahl von Softwareprodukten zur Festplattenverschlüsselung, und der Verbreitung von Halbleiterlaufwerken (engl. *Solid-State Drives (SSDs)*) mit integrierter Hardware-Verschlüsselung, steht der oben genannte Aufwand heute i. d. R. in einem angemessenen Verhältnis zur Schutzbedürftigkeit der Daten. Neben diesen vom Gesetzgeber als schützenswert angesehenen Daten, gibt es in der Geschäftswelt schützenswerte Firmengeheimnisse, und auch einige Privatanwender haben ein Interesse daran ihre Daten abzusichern. In all diesen Szenarien bietet Festplattenverschlüsselung, egal ob hardware- oder softwarebasiert, einen relativ günstigen aber hohen Schutz gegen Datenlecks durch physischen Verlust oder Diebstahl von Datenträgern.

1.1 Motivation und Ziele

In welchem Umfang wird die Technologie der Festplattenverschlüsselung heute tatsächlich von Unternehmen eingesetzt? Nach welchen Gesichtspunkten werden die eingesetzten Lösungen ausgewählt? Sind sich Firmen und Privatpersonen auch der Schwachpunkte der von ihnen eingesetzten Lösung bewusst?

Während es für den Einsatz von Verschlüsselungstechnologien in amerikanischen Unternehmen bereits eine Reihe von Studien gibt (vgl. Kapitel 1.2), wird in der vorliegenden Arbeit erstmals der deutsche Markt betrachtet sowie Privatanwender hinzugezogen. Ziel dieser Arbeit ist die Erstellung und Auswertung eines Fragenkatalogs zum Einsatz von Festplattenvollverschlüsselungen bei in Deutschland angesiedelten Unternehmen und Anwendern.

1.2 Verwandte Arbeiten

Die im Jahr 2012 veröffentlichte Studie "US Full Disk Encryption 2011 Survey" [SEC12] der Firma SECUDE betrachtet 209 amerikanische Firmen. Die Studie kommt zu dem Ergebnis, dass in den USA 58% aller teilnehmenden Firmen im Jahr 2011 Festplattenverschlüsselungen einsetzte. Darüberhinaus gaben 25% an die Nutzung von Festplattenverschlüsselung zukünftig einführen oder ausbauen zu wollen. Allerdings gaben 25% der Betriebe an, dass – obwohl sie bisher keine Verschlüsselung einsetzen – auch in naher Zukunft keine Verschlüsselung eingeführt werden soll. Die Studie zeigt außerdem, dass ca. die Hälfte aller Firmen neben objektiven Anschaffungskriterien (wie bspw. dem Preis-/Leistungsverhältnis) viel Wert auf das Firmenimage des Partners legen. Wenig überraschend sind die Wünsche der Unternehmen hinsichtlich Benutzerfreundlichkeit und Performance: eine einfache, transparente Nutzung, die auch für unerfahrene Nutzer ohne Schulung möglich ist, und eine Systemleistung, die die tägliche Arbeit nicht beeinflusst, wird von mehr als drei Vierteln der Befragten als wichtig angesehen.

Die Studie "2010 Annual Study: US Enterprise Encryption Trends" [Pon10] des Ponemon Instituts wurde über ca. 1.000 Teilnehmer erhoben und ist der letzte Teil einer Serie von bis dahin jährlich durchgeführten Umfragen zu Verschlüsselungsstrategien amerikanischer Unternehmen. 59% der befragen Unternehmen setzten im Jahr 2010 eine Festplattenvollverschlüsselung ein. Trotzdem beklagten in diesem Zeitraum zwei Drittel der Unternehmen mehrere Vorfälle eines Datenlecks; lediglich 12% gaben an, nie ein derartiges Vorkommen gehabt zu haben. Außerdem zeigt die Studie, dass Unternehmen Verschlüsselung inzwischen weniger zur freiwilligen Abwehr von Datenlecks betreiben, als vielmehr zur Erfüllung von Datenschutzrichtlinien durch den Gesetzgeber.

1.3 Übersicht der Ergebnisse

Wie sich im Rahmen unserer Studie herausgestellt hat, ist Verschlüsselung im geschäftlichen Umfeld in Deutschland weit verbreitet. 85% aller befragten Unternehmen gaben an ihre

Festplatten zu verschlüsseln, so dass FDE durchaus als Standard bei deutschen Unternehmen gesehen werden kann. Hardwarebasierte Verschlüsselung wird noch verhältnismäßig selten eingesetzt (20%), während der Großteil der Firmen per Software verschlüsseln, in erster Linie mit Microsoft BitLocker. Die Verschlüsselung von Mitarbeiter-Smartphones ist etwas weniger verbreitet (68%), was allerdings auch darauf zurückzuführen ist, dass einige Firmen die Speicherung sensitiver Daten auf diesen Geräten nicht erlauben. Die wichtigsten Kriterien deutscher Firmen für den Erwerb einer Verschlüsselungslösung sind die Usability (62%), die Performance (51%), eine einfache Inbetriebnahme (51%), der Preis (46%) und das Image des Herstellers (41%).

Im Gegensatz zu Unternehmen liegt der Anteil der untersuchten Privatanwender, die Festplattenverschlüsselung einsetzen, mit ca. 25% deutlich niedriger. Zudem ist unsere Umfrage bei Privatanwendern nicht repräsentativ für die deutsche Allgemeinheit, sondern umfasst vor allem Studenten und Angestellte der Technischen und der Wirtschaftswissenschaftlichen Fakultät der Universität Erlangen-Nürnberg. Es ist davon auszugehen, dass der Anteil der Privatanwender, die Festplattenverschlüsselung einsetzen, gemessen an der gesamtdeutschen Bevölkerung weniger als 25% beträgt. Der Grund ist eine signifikante Korrelation zwischen dem Einsatz von Verschlüsselung und PC-Kenntnissen, die wir feststellen konnten (Cramers $V = 0,398$, $p < 0,001$). Interessanterweise wird von den befragten Teilnehmern die Sicherheit hardwarebasierter Verschlüsselung im Schnitt schwächer bewertet als die Sicherheit softwarebasierter Methoden. Die Verschlüsselung von Smartphones ist relativ weit verbreitetet und war bei immerhin 42% der untersuchten Teilnehmer aktiviert.

2 Technischer Hintergrund

Im Folgenden wird kurz auf die verschiedenen Ausprägungen von Festplattenverschlüsselung (Kapitel 2.1) eingegangen, sowie auf deren Sicherheit (Kapitel 2.2). Insbesondere werden Schwachstellen aufgezeigt und einige, in der Praxis relevante Angriffe auf Verschlüsselungssysteme dargestellt.

2.1 Arten der Festplattenverschlüsselung

Eine *Festplattenverschlüsselung*, oder *Festplattenvollverschlüsselung* (engl. *Full Disk Encryption (FDE)*), zeichnet sich gegenüber der Verschlüsselung einzelner Dateien und Verzeichnisse dadurch aus, dass ganze Partitionen einer Platte verschlüsselt werden. Für den Anwender, wie auch die Anwendersoftware, ist die Verschlüsselung damit transparent, denn es wird unterhalb der Dateisystemebene verschlüsselt. Dies kann technisch entweder im Betriebssystemkern erfolgen, in diesem Fall sprechen wir von *softwarebasierter* Verschlüsselung, oder durch die Festplatte selbst, in dem Fall sprechen wir von *hardwarebasierter* Verschlüsselung.

2.1.1 Softwarebasierte Verschlüsselung

Bei softwarebasiertem FDE werden alle Daten durch den Betriebssystemkern verschlüsselt bevor sie auf die Festplatte geschrieben werden, bzw. entschlüsselt nachdem sie gelesen wurden. Für den Ver- und Entschlüsselungsschritt wird jeweils der Hauptprozessor und -speicher beansprucht. Da von derart gesicherten Medien nicht gestartet werden kann, existiert zusätzlich ein unverschlüsselter Bootloader, der vor dem Starten des eigentlichen Systems den Benutzer authentifiziert und das notwendige Passwort abfragt. Zu den bekanntesten softwarebasierten Verfahren zählen Microsoft BitLocker und die Open-Source Lösung TrueCrypt. Unter Apple MacOS findet darüberhinaus FileVault Verwendung, und unter Linux meist dm-crypt. Android-basierte Smartphones verfügen seit Version 4.0 ebenfalls über eine Option die Benutzer-Partition zu verschlüsseln (jedoch nicht die System-Partition), und iPhones verfügen ebenfalls über eine Verschlüsselung.

Solche softwarebasierten Verfahren haben zwei Nachteile: einerseits sinkt durch die Belastung des Hauptprozessors die Performance des Gesamtsystems, und andererseits eröffnet die Nutzung des Hauptspeichers Angriffsmöglichkeiten wie Cold-Boot (vgl. Kapitel 2.2). Dennoch haben unsere Untersuchungen gezeigt, dass softwarebasiertes FDE, vor allem BitLocker und TrueCrypt, heute sehr beliebt sind. Dies kann historisch erklärt werden, denn softwarebasierte Methoden existieren seit etwa 10 Jahren, und damit wesentlich länger als hardwarebasierte Methoden. Außerdem sind softwarebasierte Methoden flexibler, unabhängig von bestimmten Hardware-Herstellern, und teilweise kostenlos.

2.1.2 Hardwarebasierte Verschlüsselung

Seit etwa 4 Jahren finden sogenannte *selbstverschlüsselnde Festplatten* (engl. *Self Encrypting Drives (SEDs)*) zunehmend Verbreitung. Diese führen die Ver- bzw. Entschlüsselung transparent für das Betriebssystem in Hardware durch und basieren i.d.R. auf modernen *Solid-State Drives (SSDs)*, da diese einen komplexen Disk-Controller aufweisen der relativ einfach um die Funktion einer Verschlüsselung ergänzt werden kann. Beispiele für SEDs sind die Fujitsu DX8090, Seagate Cheetah, Intel 320 oder 520 und Samsung 830.

Im Unterschied zu softwarebasierter Verschlüsselung können SEDs stets alle Daten einer Festplatte verschlüsseln. Ein unverschlüsselter Bootloader ist nicht nötig, weil das BIOS die Aufgabe der Passwortabfrage übernimmt und die Festplatte entsperrt. Nach der Entsperrung verschlüsseln sich SEDs dann autonom und verhalten sich nach außen wie unverschlüsselte Platten. Die Performance des Hauptsystems wird daher nicht beeinflusst und prinzipiell werden alle Betriebssysteme unterstützt, auch wenn sie selbst keine Verschlüsselungsoption bieten. Nachteilig sind unter Umständen höhere Anschaffungskosten und der vergleichsweise geringe Speicherplatz auf SSDs zu nennen.

2.2 Sicherheit von Festplattenverschlüsselung

Wie unsere Untersuchungen zeigen, genießt softwarebasiertes FDE in Deutschland sowohl eine höhere Verbreitung als auch ein größeres Vertrauen unter den Anwendern. Das dieses Vertrauen nicht in jedem Fall gerechtfertigt ist, wollen wir kurz anhand einer Reihe von bekannten Schwachstellen zeigen.

Cold-Boot Angriffe Cold-Boot Angriffe greifen die Schlüsselverwaltung im Hauptspeicher an und richten sich somit gegen softwarebasierte Verschlüsselung. Entgegen der Annahme vieler Menschen, verflüchtigen sich Inhalte des Hauptspeichers nicht sofort nach dem Ausschalten eines Rechners, sondern bleiben mehrere Sekunden ohne Strom erhalten. Im Jahr 2008 konnten Halderman et al. [HSH+08] erstmals zeigen, dass sich dieser Effekt für praktische Angriffe gegen Festplattenverschlüsselungen ausnutzen lässt. Unter der Voraussetzung, dass ein Zielsystem eingeschaltet ist (oder sich im Bereitsschaftszustand befindet), entnimmt der Angreifer die Speicherriegel, baut diese in einen Analyserechner ein und durchsucht sie nach dem Festplattenschlüssel. Auf diese Weise konnten BitLocker und TrueCrypt erfolgreich angegriffen werden. 2013 zeigten Müller und Spreitzenbarth [MS13] darüberhinaus, dass ähnliche Angriffe auch gegen die Verschlüsselung von Android eingesetzt werden können.

Evil-Maid Angriffe Dieser Angriff, welcher im Wesentlichen das Benutzerpasswort erspäht, richtet sich ebenfalls gegen softwarebasierte Festplattenverschlüsselung. 2009 beschrieb Rutkowska [Rut09] folgendes, namensgebende Angriffsszenario gegen TrueCrypt: Ein Hotelgast lässt seinen ausgeschalteten Laptop unbeaufsichtigt zurück, so dass ein "böses Zimmermädchen" unbemerkt Zugriff auf diesen erlangen kann. Für das Zimmermädchen ist es nun möglich den unverschlüsselten Teil des Bootloaders mit einem Keylogger zu infizieren. Sobald der Hotelgast zurückkehrt und sich anmeldet, wird das Benutzerpasswort auf der Festplatte geloggt. Mit einem zweiten Zugriff kann das Zimmermädchen dieses auslesen und somit die Festplattenverschlüsselung umgehen. 2013 zeigten Götzfried und Müller [GM13], dass der Angriff prinzipiell auch gegen Android funktioniert.

Direct-Memory-Access Angriffe DMA Angriffe richten sich gegen software- und hardwarebasierte Verschlüsselung gleichermaßen. 2005 haben Dornseif et al. [DBK05] erstmals gezeigt, dass sich DMA-fähige Schnittstellen wie FireWire ausnutzen lassen um eingeschaltete Rechner zu entsperren. Der Grund ist, dass per DMA angeschlossene Geräte vollen Lese- und Schreibzugriff auf den Hauptspeicher eines Systems haben. Durch Schreibzugriff auf den Systemspeicher lässt sich eine Bildschirmsperre nun ohne weiteres aushebeln, obwohl das Passwort unbekannt ist. Ähnlich zu Cold-Boot Angriffen muss das Zielsystem dabei eingeschaltet sein (oder sich im Bereitschaftszustand befinden). Obwohl Gegenmaßen seit Jahren existieren, sind alle Windows-Versionen bis einschließlich Version 8 von dieser Schwachstelle betroffen.

Hot-Plug Angriffe 2012 stellten Müller, Latzo und Freiling [MLF13] erstmals einen Angriff vor, der sich ausdrücklich gegen hardwarebasierte Verschlüsselung richtet; softwarebasierte Verschlüsselung ist nicht betroffen. Grundlage dieses Angriffs ist, dass die Strom- und Datenkabel von SEDs getrennt geführt werden, SEDs aber nur gesperrt werden sobald das Stromkabel getrennt wird. Das Datenkabel kann von einem Zielrechner abgeklemmt und an einen Analyse-Rechner angeschlossen werden, ohne dass SEDs dabei gesperrt werden. Wenn der Zielrechner eingeschaltet ist (oder sich im Bereitschaftszustand befindet), erlangt ein Angriffer dadurch vollen Zugriff auf die Daten und umgeht somit die Verschlüsselung.

Zusammenfassend ist zu sagen, dass Festplattenverschlüsselung, gleich welcher Art, wesentlich sicherer ist wenn ein System vollständig heruntergefahren ist. Unternehmen sollten ihre Mitarbeiter dazu anhalten Systeme niemals eingeschaltet (oder im Bereitsschaftszustand befindlich) unbeaufsichtigt zu lassen, sondern stets herunterzufahren.

3 Studie zur Verwendung von Festplattenvollverschlüsselung

Im Folgenden präsentieren wir die Umfrageergebnisse unserer Studie zur Verwendung von FDE. Die Kernfragen unserer Studie zum privaten Umfeld (Kapitel 3.1) und der zum geschäftlichen Umfeld (Kapitel 3.2) sind sich ähnlich. Beide Fragebögen unterscheiden sich im Wesentlichen dadurch, dass sich der private Fragebogen auf einzelne Laptops bzw. Smartphones bezieht, während im professionellen Bereich nach dem Gesamtbestand eines Unternehmens gefragt war.

3.1 Festplattenverschlüsselung im privaten Umfeld

Der Großteil der privaten Antworten ging über eine Onlineumfrage ein, während einzelne analoge Antworten nachträglich in das System eingepflogen wurden. Am Ende gab es 1379 Datensätze von denen, nach Aussortierung unvollständiger und widersprüchlicher Antworten, 1034 ausgewertet wurden. Um Abbrüche und Antworten nach dem Zufallsprinzip zu vermeiden, waren die Teilnehmer nicht gezwungen alle Fragen zu beantworten. Um möglichst viele Privatanwender zu erreichen, wurde die Studie neben Facebook über verschiedene Mailinglisten der Universität Erlangen-Nürnberg angekündigt. Durch die Zielgruppe der Mailinglisten ist die Umfrage nicht repräsentativ für die Allgemeinheit, sondern umfasst vor allem Studenten und Angestellte der Technischen und der Wirtschaftswissenschaftlichen Fakultät. Dies erklärt den hohen Anteil junger und männlicher Probanden (vgl. Tabelle 1). Die PC-Kenntnisse der Teilnehmer (vgl. Tabelle 2) liegen womöglich deutlich über dem Bevölkerungsdurchschnitt.

90% der Befragten gaben an einen Laptop zu besitzen. Den Markt teilen sich dabei die Hersteller wie folgt auf: Acer (15%), Lenovo (14%), Apple (12%) und Dell (11%), Asus, HP und Samsung (je unter 10%) und schließlich sonstige Hersteller (je unter 5%). Der große Vorteil eines Laptops – seine Mobilität – wird von fast allen Befragten genutzt; lediglich

männlich	69%
weiblich	28%
keine Angabe	3%
18-24	64%
25-34	32%
sonstiges Alter	4%

Tabelle 1: Geschlechts- und Alterstruktur.

sehr gut (1)	22%
gut (2)	28%
durchschnittlich (3)	30%
schlecht (4)	8%
sehr schlecht (5)	2%
Durchschnitt	2,29

Tabelle 2: PC-Kenntnisse der Teilnehmer.

8% gaben an ihren Laptop nur zu Hause zu benutzen. Die Verlustquote bei privaten Laptops liegt bei 4%. Smartphones sind nicht so verbreitet wie Laptops; nur 2/3 der Befragten gaben an ein Smartphone zu besitzen. Die Marktanteile sind dabei konzentrierter als bei Laptops: Samsung (37%), Apple (20%) und HTC (16%) teilen sich über 70% des Marktes. Sony und Nokia folgen mit 7% respektive 5%. Die höhere Verlustrate von 9% bei Smartphones erstaunt nicht.

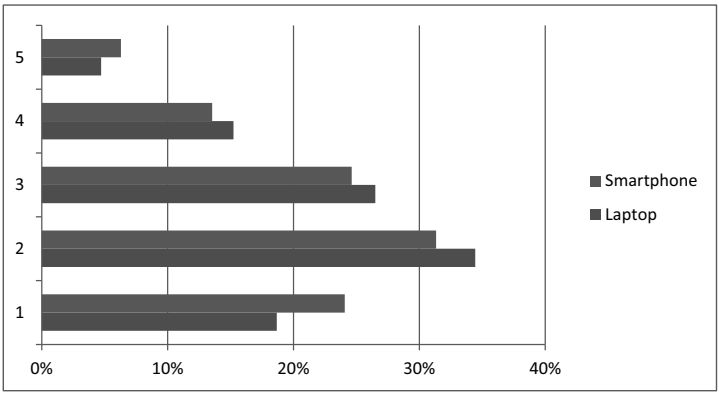

Abbildung 1: Potentieller Schaden durch Datendiebstahl (von 1: kein Schaden bis 5: hoher Schaden).

Die Höhe des potentiellen Schadens, den ein Diebstahl der gespeicherten Daten auf einem Laptop bzw. Smartphone für einen Probanden zur Folge hat, zeigt Abbildung 1. Dabei handelt es sich um den subjektiven Eindruck eines Teilnehmers auf einer Skala von 1 (kein Schaden) bis 5 (hoher Schaden). Der durchschnittliche Schaden wird mit 2,53 (Laptops) und 2,47 (Smartphones) für beide Geräteklassen ähnlich angegeben.

3.1.1 Eingesetzte Verschlüsselung

Abbildung 2 verdeutlicht, dass die Mehrheit der privaten Nutzer keine Verschlüsselung auf Laptops einsetzt (über 70%). Wenn verschlüsselt wird, so wird i.d.R. auf softwarebasierte Verschlüsselung zurückgegriffen (19%). Der Markt der softwarebasierten Verschlüsselung wird dabei von TrueCrypt dominiert (63%), gefolgt von dm-crypt für Linux (16%), FileVault für MacOS (7%) und BitLocker für Windows (4%). Selbstverschlüsselnde Festplatten (SEDs) nutzen nur etwa 4% der Befragten, wobei ein Großteil dabei interessanterweise

angibt zusätzlich softwarebasierte Verschlüsselung zu nutzen. Technisch ist dies zwar möglich, bedeutet in der Praxis aber kaum einen Sicherheitsgewinn.

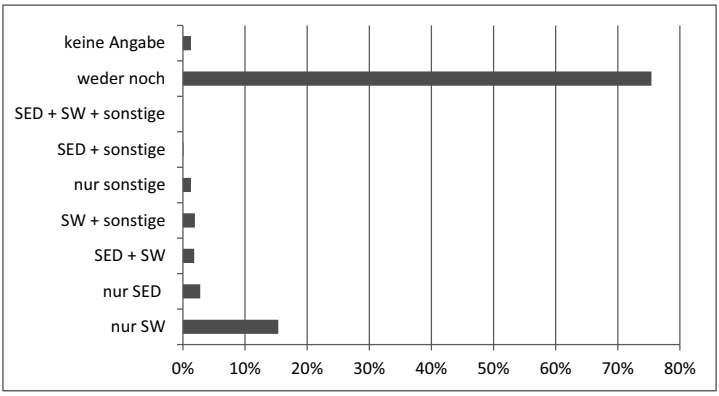

Abbildung 2: Verwendete Verschlüsselungsprodukte für Laptops bei Privatpersonen.

Im Smartphonebereich ist die Verschlüsselungsquote deutlich höher als bei Laptops, obwohl das Schadenspotential der Daten als vergleichbar angegeben wird. 42% der Befragten haben ihr Smartphone verschlüsselt. Eine Erklärung dafür ist, dass viele Smartphones heute eine einfach zu aktivierende Verschlüsselung bieten (Android) oder gar ab Werk verschlüsselt sind (iPhone), was bei vielen Laptops nicht der Fall ist. So ist BitLocker bspw. nur in den Enterprise-Versionen von Microsoft Windows verfügbar.

Eine Korrelationsanalyse zwischen PC-Kenntnissen und dem Einsatz von Verschlüsselung auf Laptops ergibt einen mittleren Zusammenhang (Cramers $V = 0,398$, $p < 0,001$). Dies ist insofern nicht überraschend, als dass davon auszugehen ist, dass es vor allem erfahrene Nutzer sind, die ihre Systeme mit Funktionen schützen, die nicht standardmäßig installiert bzw. aktiviert sind. Eine ähnliche Korrelationsanalyse für den Einsatz von Verschlüsselung auf Smartphones ergibt einen geringeren Zusammenhang (Cramers $V = 0,118$, $p < 0,1$).

Codestellen	numerisch	alphanumerisch	keine Angabe	Summe
4	201	11	0	212
5	29	2	1	32
6	28	4	0	32
7	7	2	0	9
8	22	19	0	41
9	10	5	0	15
10	3	8	0	11
11	0	2	2	4
12	5	26	2	33
mehr	0	3	0	3

Tabelle 3: Art und Länge von Code-Sperren bei privaten Smartphones.

Bei Diskussionen über die Sicherheit von Verschlüsselung wird immer wieder angeführt, dass diese nur so sicher ist wie das gewählte Passwort. Aus diesem Grund wurde in unserer

Umfrage nach der Länge und Art der Code-Sperren bei Smartphones gefragt. Inbesondere bei Smartphones ist man aus Gründen der Benutzerfreundlichkeit dazu verleitet kurze PINs bzw. Passwörter zu wählen. Tabelle 3 zeigt, dass die Codestärke der meisten Nutzer in der Tat relativ schwach ist. Eine Häufung der Passwortlänge von 4 ist dadurch zu erklären, dass dies bei vielen Geräten die Mindestlänge darstellt. Geht man davon aus, dass sichere Passwörter mindestens 8 alphanumerische Zeichen haben, so benutzen nur 9% der Anwender ein sicheres Passwort.

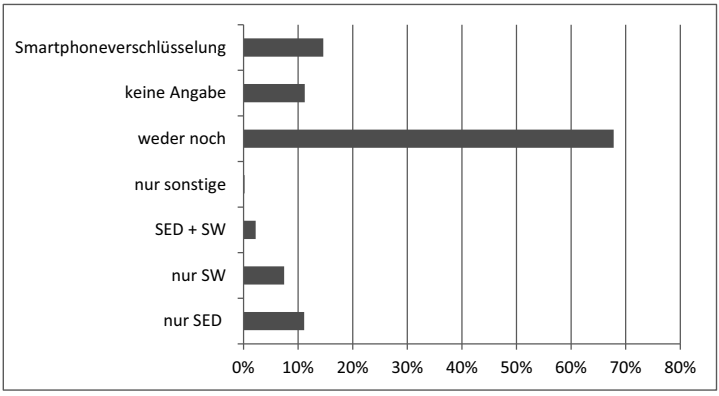

Abbildung 3: Geplanter Einsatz von Verschlüsselung im privaten Umfeld.

Außerdem wurde gefragt, inwieweit die Teilnehmer planen zukünftig Verschlüsselungsprodukte einzusetzen. Weitere 19% der Befragten gaben an, in Zukunft ihre Daten auf dem Laptop verschlüsseln zu wollen. Der Anteil von SEDs gemessen am Gesamtaufkommen von Verschlüsselungslösungen wird dabei steigen (vgl. Abbildung 3).

3.1.2 Entscheidungsgründe und Einschätzungen

In einer Freitextantwort konnten die Teilnehmer ihre Gründe für bzw. gegen den Einsatz von Verschlüsselungsprodukten angeben, wovon 462 Teilnehmer (45%) Gebrauch machten. Die Ergebnisse dazu zeigt Tabelle 4. Hauptgrund für die Verschlüsselung ist erwartungsgemäß die Verbesserung der Datensicherheit, während andere Gründe nur vereinzelt genannt wurden. Die Argumente gegen die Verschlüsselung sind vielfältiger. Der Verzicht auf Verschlüsselung bei Abwesenheit schützenswerter Daten ist nachvollziehbar. Zudem ist Unwissenheit häufig genannt und die Tatsache, dass sich viele Nutzer vor dem Aufwand einer Neuinstallation scheuen.

Schließlich wurden die Teilnehmer gebeten die Sicherheit von hardware- und softwarebasierter Verschlüsselung einzuschätzen (Abbildung 4) bzw. anzugeben wo sie Vor- und Nachteile dieser Technologien sehen (Abbildung 5). Dabei nehmen wir aufgrund der hohen Anzahl derjenigen an, die keine Angaben gemacht haben, dass viele Befragte zu wenig technisches Verständnis von Festplattenverschlüsselung hatten, um diese Fragen sinnvoll zu beantworten.

Gründe gegen Verschlüsselung		Gründe für Verschlüsselung	
keine Notwendigkeit	175	Datensicherheit	105
Unwissenheit	87	einfache Installation	11
hoher Aufwand	68	Interesse	4
kein Diebstahlrisiko	41	Paranoia	3
kein Interesse	28	günstiger Preis	3
Performanceeinbußen	21	externe Vorgaben	1
Angst vor Datenverlust	21	SED mitgeliefert	1
kein Vertrauen in die Sicherheit	8	gute Performance	1
keine (gute) OS Unterstützung	5		

Tabelle 4: Gründe für bzw. gegen den Einsatz von Verschlüsselung im privaten Umfeld.

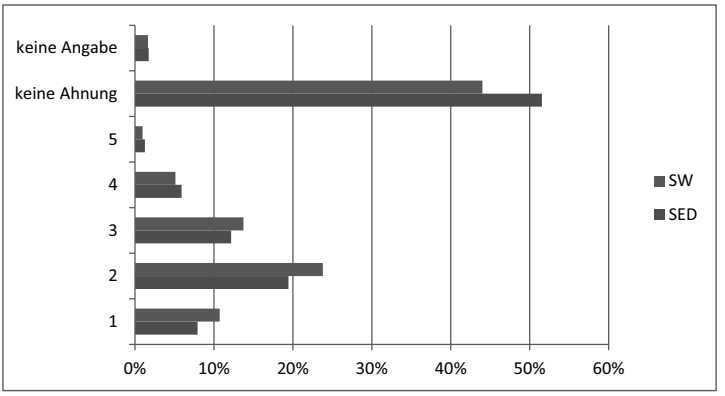

Abbildung 4: Einschätzung der Sicherheit (von 1: sehr gut bis 5: sehr schlecht).

Die Sicherheit von SEDs wird von den Teilnehmern im Schnitt schwächer bewertet als die softwarebasierter Methoden (SEDs: 2,42 vs SW: 2,30). Aufgrund verfügbarer Open-Source Lösungen ist es wenig überraschend, dass beim Preis ebenfalls die Vorteile bei softwarebasierter Verschlüsselung genannt werden. Weitere Eigenschaften ergaben leichte Vorteile zugunsten von SEDs, inbesondere die Usability, Performance und Installation.

Als letztes wurden die Teilnehmer gefragt, ob sie die in Kapitel 2.2 beschriebenen Angriffe kennen. Der bekannteste Angriff war der DMA bzw. FireWire Angriff mit 23%, gefolgt von Cold-Boot und Hot-Plug mit je 15%, und schließlich dem Evil-Maid Angriff mit 7%.

3.2 Festplattenverschlüsselung im geschäftlichen Umfeld

Von 59 geschäftlichen Datensätzen, die ebenfalls meist online eingegangen sind, wurden am Ende 37 vollständige und widerspruchsfreie Datensätze ausgewertet. Die Kontaktaufnahme zu potentiellen Teilnehmern erfolgte auf drei verschiedene Wege: durch persönliche Kontakte, durch das Kompetenzforum Cyber-Sicherheit Deutschland und durch offizielle

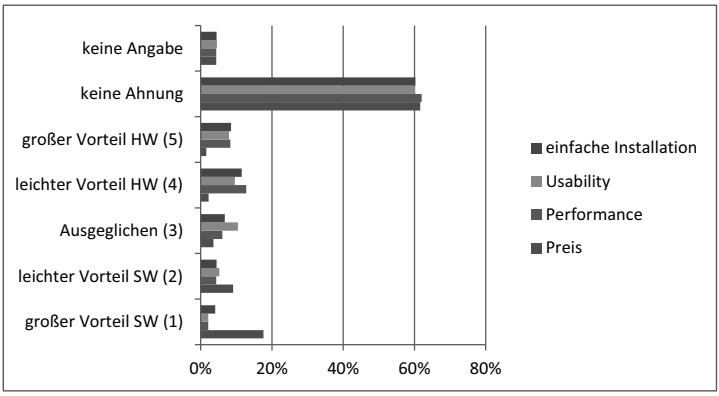

Abbildung 5: Vergleich von hardware- (HW) und softwarebasierter (SW) Verschlüsselung.

Kontaktadressen der Firmen. Neben Unternehmen wurde auch Ämter, Ministerien, Polizeibehörden, Forschungseinrichtungen und andere öffentliche und halböffentliche Institutionen angeschrieben.

Lehre und Wissenschaft	4
Behörde	2
Finanzdienstleister	2
Industrie und Einzelhandel	6
Dienstleister	6
Gesundheits- und Pharmaindustrie	3
Technologie- und Softwareunternehmen	3
Telekommunikationsunternehmen	3
Konsumgüter und Transportwesen	2
sonstige	6

Tabelle 5: Branchen der teilnehmenden Unternehmen.

keine Angabe	5	8
1-5	0	0
6-20	4	6
21-100	8	9
101-500	6	1
501-1000	1	4
1001-5000	5	5
5001-10000	5	2
10001+	3	2

Tabelle 6: Im Umlauf befindliche Laptops (li.) und Smartphones (re.).

Innerhalb der Stichprobe von 37 Unternehmen konnte ein breites Spektrum an Branchen abgedeckt werden (vgl. Tabelle 5). Außerdem war es möglich relativ viele Konzerne mit großen Mitarbeiterzahlen und einer entsprechend großen Anzahl firmeneigener Laptops und Smartphones für die Teilnahme zu gewinnen. Fast die Hälfte der befragten Unternehmen hat mindestens 1.000 Beschäftigte, 2/3 davon mindestens 10.000. 34 Firmen geben dabei Laptops zur täglichen Arbeit an ihre Mitarbeiter aus.

Im geschäftlichen Bereich sind die meistgenutzten Laptophersteller Dell und Lenovo (je über 40%) sowie HP (24%), gefolgt von Apple (11%) und Fujitsu (16%). Die Verlustquote für Laptops wird mit maximal 4% angegeben, ist mit durchschnittlich 0,7% aber sehr gering und steht damit im Gegensatz zu den uns bekannten amerikanischen Studien [Pon10, SEC12]. Möglicherweise liegt die Dunkelziffer hier um einiges höher; ein Teilnehmer gab an, dass es im Konzern keine Meldepflicht für verlorene Laptops gäbe.

Smartphones sind in Unternehmen ähnlich verbreitet wie Laptops (vgl. Tabelle 6). 33

der befragten Betriebe geben Smartphones an ihre Mitarbeiter aus. Die meistgenutzten Hersteller (Mehrfachnennung möglich) sind dabei Apple und Research in Motion (je knapp 60%), Samsung (33%), HTC (24%), Nokia (12%) und Sony (3%). Die Verlustquote ist mit 1,1% im Schnitt etwas höher als bei Laptops, und entspricht etwa 25 verlorenen Smartphones pro Firma und Jahr.

3.2.1 Datensensitivität

Inwieweit eine Verschlüsselung Sinn macht, hängt maßgeblich von der Sensitivität der Daten ab. Deshalb wurde gefragt auf wievielen Laptops bzw. Smartphones vertrauliche Daten gespeichert werden (vgl. Abbildung 6). Interessant ist dabei die unterschiedliche Verteilung für Smartphones und Laptops: während die Verteilung für Laptops grob einer Normalverteilung entspricht, werden sensitive Daten auf Smartphones entweder möglichst vermieden oder vergleichsweise häufig gespeichert. Dabei unterliegen die Daten sowohl auf Laptops als auch auf Smartphones häufig Gesetzen wie dem BDSG. 71% aller Unternehmen gaben an, BDSG Daten auf Laptops zu speichern, und 59% aller Unternehmen gaben an, dies ebenfalls auf Smartphones zu tun. Dementsprechend hoch ist der potentielle Schaden, den ein Diebstahl der gespeicherten Daten verursachen kann. Mehr als ein Drittel erwarten im Ernstfall hohen bzw. sehr hohen Schaden durch Datendiebstahl.

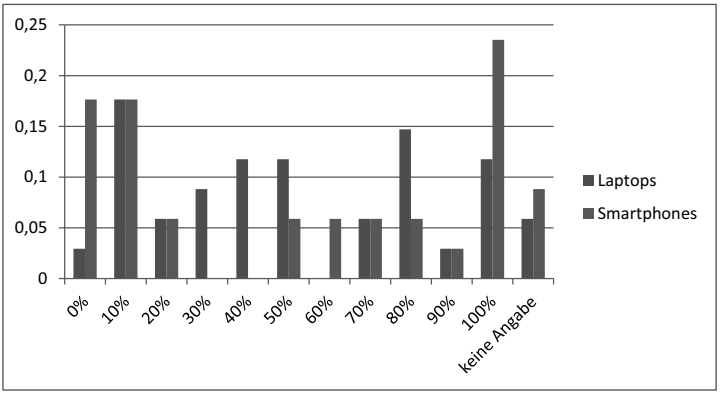

Abbildung 6: Hardware mit vertraulichen Daten im geschäftlichen Umfeld. Die Y-Achse beschreibt den Anteil der Firmen die auf dem durch X angegeben Anteil ihrer Hardware kritische Daten speichert.

3.2.2 Eingesetzte Verschlüsselung

Es zeigt sich, dass der Anteil von Unternehmen die Verschlüsselung einsetzen mit fast 85% im Vergleich zu Privatanwendern relativ hoch ist. Lediglich 15% aller Unternehmen setzen keine Produkte zur Festplattenverschlüsselung ein (vgl. Abbildung 7).

Wie im privaten Gebrauch, sind SEDs auch im professionellen Einsatz vergleichsweise selten anzutreffen. Da die meisten Unternehmen eine große, gewachsene IT-Struktur haben, ist ein kompletter Umstieg auf SEDs oftmals nur schwer zu realisieren. Deshalb geben

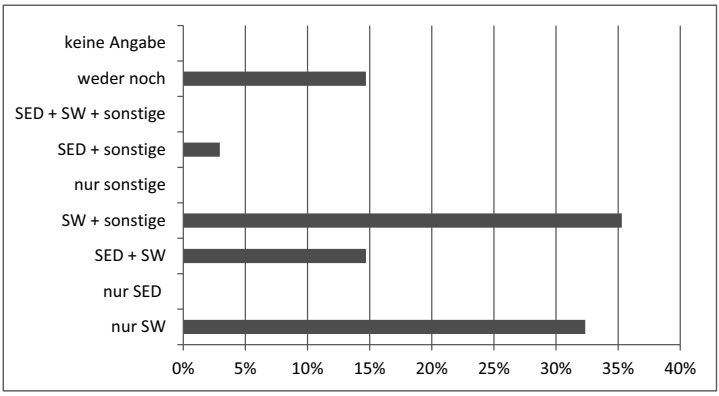

Abbildung 7: Verwendete Verschlüsselungsprodukte in Unternehmen.

alle Firmen, die bereits SEDs nutzen, zusätzlich auch an softwarebasierte Produkte zu verwenden. Dies ist aber nicht, oder nicht unbedingt, gleichbedeutend mit der Praxis beide Technologien auf ein und demselben Laptop einzusetzen. In 50% der Unternehmen die SEDs einsetzen, werden lediglich 10% der Laptops tatsächlich auf diese Weise geschützt. Zwei Firmen die bisher softwarebasierte Produkte verwenden, planen in naher Zukunft den Einsatz von SEDs. Eine Firma, die ihre Daten bisher nicht schützt, plant dagegen die Nutzung einer softwarebasierten Lösung einzuführen.

Im Softwaresegment ist Microsoft BitLocker, das nur 4% der Privatanwender einsetzen, mit Abstand das meistgenutzte Produkt. Über 50% der Firmen geben an, BitLocker im Einsatz zu haben. Darauf folgen Sophos Safeguard (18%), SECUDE Finally Secure (11%), McAfee Endpoint Encryption (11%), PGP Whole Disk Encryption (7%), Check Point PointSec (7%) und Apple FileVault (7%).

Betrachtet man wieviele Laptops innerhalb eines Unternehmens verschlüsselt werden, so geben 69% der Unternehmen an alle Laptops (100%) zu verschlüsseln. Weitere 10% der Unternehmen verschlüsseln mindestens 90% ihrer Laptops. Ein Teilnehmer gab an, dass lediglich 80% der Geräte verschlüsselt werden, obwohl die Sollquote bei 100% liege.

Im Smartphonebereich scheint die Verschlüsselung auf den ersten Blick nicht ganz so verbreitet: 68% aller Firmen aktivieren Verschlüsselungsfunktionen vor der Ausgabe von Smartphones an ihre Mitarbeiter. Hierbei ist jedoch zu berücksichtigen, dass viele Firmen keine sensitiven Daten auf Smartphones dulden. Lediglich 3% der Firmen die angaben, sensitive Daten auf Smartphones zu speichern, verschlüsseln diese nicht. Zu denken gibt aber, dass wie im privaten Bereich, die Passwortstärke auf Smartphones oft zu gering ist. Analog zu Tabelle 3 vergeben nur 19% der Unternehmen sichere Passwörter (d.h. mindestens 8 alphanumerische Zeichen).

3.2.3 Entscheidungsgründe und Einschätzungen

Von der Möglichkeit ihre Entscheidung für oder gegen den Einsatz einer Verschlüsselungsmethode zu begründen, machten 24 Teilnehmer (73%) Gebrauch. Für die Verwendung wurden hauptsächlich zwei Argumente genannt: Schutz der eigenen Daten, sowie Vorgaben durch Sicherheitsrichtlinien und gesetzliche Vorschriften (vgl. Tabelle 7).

Datensicherheit	12
Sicherheitsrichtlinien/Vorschriften	6
Standard	2
Active Directory	1
Imageschutz	1
Schutz vor Schadensersatzklagen	1

Tabelle 7: Gründe für Verschlüsselung i.A.

Administrierbarkeit/Flexibilität	14
Kosten	8
bessere Wiederherstellbarkeit	2
SED Technik unausgereift	1
mangelnde Erfahrung mit SEDs	1
Software für Nutzer verständlicher	1

Tabelle 8: Gründe für SW-basiertes FDE.

Für eine softwarebasierte Verschlüsselung sprechen aus Firmensicht vor allem zwei Dinge (vgl. Tabelle 8): die Flexibilität und bessere Administrierbarkeit, sowie finanzielle Erwägungen. Vereinzelt tauchen darüberhinaus Argumente auf, die für ein noch nicht vorhandenes Vertrauen in die Technologie der SEDs sprechen.

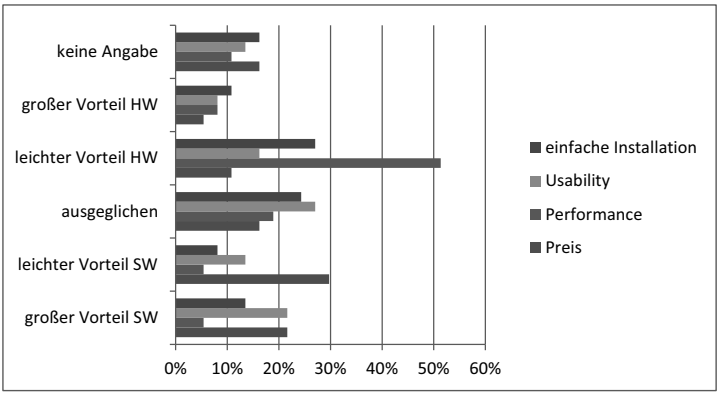

Abbildung 8: Vergleich software- und hardwarebasierter Verschlüsselung.

Ebenso wie die Privatanwender, wurden auch die geschäftlichen Teilnehmer nach ihren Einschätzungen bezüglich der Sicherheit und den Vor- und Nachteilen von hardware- bzw. softwarebasierter Verschlüsselung gefragt (vgl. Abbildung 8). Die Usability und die Installation von SEDs gegenüber softwarebasierterer Verschlüsselung wird von den Befragten dabei als ausgeglichen angesehen, wohingegen der Performancevorteil deutlich bei hardwarebasierter Verschlüsselung gesehen wird und der Preisvorteil bei softwarebasierter Verschlüsselung.

Ferner wurde gefragt, nach welchen Kriterien die Betriebe neue Hardware bzw. Software erwerben. Die wichtigen und sehr wichtigen Kriterien für den Einkauf sind demnach: Usability (62%), Performance (51%), einfache Inbetriebnahme (51%), Preis (46%) und das

Image des Herstellers (41%) bzw. ob bereits eine Kooperation mit dem Hersteller besteht (35%). Der Kostenfaktor spielt für viele Firmen also nicht die wichtigste Rolle, sondern vielmehr die Usability und Performance. Knapp 2/3 der Unternehmen sind dazu bereit Geschäftsbeziehungen mit neuen Partnern einzugehen.

Abschließend wurde untersucht, ob die in Kapitel 2.2 beschriebenen Angriffe bekannt sind. Dabei ist festzustellen, dass die Angriffe durchgehend bekannter sind als im Bereich der privaten Anwender. Dies ist darauf zurückzuführen, dass die Fragebögen durch Administratoren und IT-Verantwortliche der Firmen ausgefüllt wurden; das Wissen der Mitarbeiter über solche Angriffe wird dadurch nicht wiedergespiegelt. Cold-Boot Angriffe waren demnach 65% der Firmen bekannt, FireWire bzw. DMA Angriffe 51%, Hot-Plug Angriffe 43% und Evil-Maid Angriffe 30%.

4 Fazit und Ausblick

Im geschäftlichen Umfeld ist die Verschlüsselung von Laptops weiter verbreitet als im privaten Umfeld. 85% der untersuchten Firmen gaben an Verschlüsselungstechnologien zum Schutz ihrer Daten einzusetzen, wobei nahezu alle Unternehmen auf Softwarelösungen setzen und nur vereinzelt begonnen wurde zusätzlich SEDs einzusetzen. Bevorzugt werden zur Verschlüsselung kostenpflichtige Lösungen bekannter Hersteller, wobei Microsoft BitLocker mit einem Marktanteil von 50% hervorzuheben ist. Die Smartphoneverschlüsselung erscheint gegenüber der Laptopverschlüsselung mit 68% etwas geringer, wobei aber einige Firmen keine sensitiven Daten auf Smartphones speichern.

Die Zahlen unserer Umfrage für deutsche Unternehmen decken sich in etwa mit den eingangs erwähnten amerikanischen Studien. Im Detail weichen diese zwar voneinander ab, aber gemeinsame Tendenzen sind deutlich erkennbar. Einzigst die auffallend niedrige Verlustrate von 0,7% für Laptops in deutschen Firmen, wie sie unsere Untersuchung ergeben hat, sticht hervor.

Zudem hat unsere Studie gezeigt, dass die private Verwendung von FDE mit 25% weit weniger verbreitet ist. Meist wurde der Nichteinsatz von Verschlüsselung mit einem Mangel an Notwendigkeit begründet, aber es zeigte sich auch, dass viele Teilnehmer zu wenig über Verschlüsselung wissen und den Aufwand einer Installation scheuen. Da davon auszugehen ist, dass bei der Stichprobengruppe ein gegenüber der Gesamtbevölkerung erhöhtes technisches Wissen und Interesse vorzufinden ist, nehmen wir an, dass die deutsche Allgemeinheit ihre Daten seltener verschlüsselt. Bei privaten Smartphones ist die Verschlüsselungsrate mit 42% wesentlich höher als bei Laptops. Dies liegt mutmaßlich an der leichten Verfügbarkeit von Verschlüsselungstechnologien auf modernen Smartphones, welche in diesem Punkt als Vorbild für zukünftige Laptops dienen können.

Auch Privatanwender nutzen, sofern sie denn verschlüsseln, meist ein softwarebasiertes Produkt, insbesondere die Open-Source Lösung TrueCrypt. SEDs spielen heute sowohl im geschäftlichen als auch im privaten Umfeld eher eine untergeordnete Rolle. Wie unsere Untersuchungen ergeben haben, sind die Gründe hierfür nicht ausschließlich finanzielle Aspekte, sondern es fehlt mitunter an Vertrauen in diese neue Technologie.

Literatur

[DBK05] Maximillian Dornseif, Michael Becher und Christian N. Klein. FireWire - All your memory are belong to us. In *Annual CanSecWest Applied Security Conference*, Vancouver, British Columbia, Canada, 2005. Laboratory for Dependable Distributed Systems, RWTH Aachen.

[GM13] Johannes Götzfried und Tilo Müller. Evil Maid goes after Android: How to subvert Android smartphones with keylogging. Bericht, Universität Erlangen-Nürnberg, 2013.

[HSH+08] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum und Edward W. Felten. Lest We Remember: Cold Boot Attacks on Encryptions Keys. In *17th USENIX Security Symposium*, Seiten 45–60, San Jose, CA, August 2008. Princeton University, USENIX.

[MLF13] Tilo Müller, Tobias Latzo und Felix Freiling. Self-Encrypting Disks pose Self-Decrypting Risks: How to break Hardware-based Full Disk Encryption. Bericht, Universität Erlangen-Nürnberg, Dezember 2013.

[MS13] Tilo Müller und Michael Spreitzenbarth. FROST: Forensic Recovery of Scrambled Telephones. In *11th International Conference on Applied Cryptography and Network Security (ACNS '13)*, Banff, Alberta, Canada, Juni 2013. Universität Erlangen-Nürnberg, Springer.

[Pon10] Ponemon. *2010 Annual Study: U.S. Enterprise Encryption Trends*. November 2010.

[Rut09] Joanna Rutkowska. Evil Maid goes after TrueCrypt. http://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html, Oktober 2009. The Invisible Things Lab.

[SEC12] SECUDE. *US Full Disk Encryption 2011 Survey*. Research SECUDE AG, Marz 2012.