Technische Universität Dresden

Institut für Systemarchitektur

Lehrstuhl für Datenschutz und Datensicherheit

 &

Fraunhofer – Center für Nanoelektronische Technologien (CNT)

Analyse und Vergleich professioneller Software zur Festplattenverschlüsselung anhand von Verschlüsselungsmethoden und Handhabbarkeit zur Absicherung tragbarer Computer

Diplomarbeit

Verfasser:

Francheska Ilcheva Angelova

Matr.Nr. 3104626

vorgelegt bei:

Verantwortlicher Hochschullehrer: Dr.-Ing. Stefan Köpsell

Betreuer:	Dr.-Ing.	Stefan Köpsell
	Dipl.-Ing.	Boris Vasilev (Fraunhofer CNT)
	Dipl.-Inf. (BA)	Felix Richter (Fraunhofer CNT)

Eigenständigkeitserklärung

Hiermit erkläre ich, die vorliegende Diplomarbeit zum Thema *„Analyse und Vergleich professioneller Software zur Festplattenverschlüsselung anhand von Verschlüsselungsmethoden und Handhabbarkeit zur Absicherung tragbarer Computer“* selbstständig und unter ausschließlicher Verwendung der angegebenen Literaturquellen und Hilfsmittel erstellt zu haben.

Dresden, 30.09.2011

Unterschrift:

Danksagung

Diese Zeilen möchte ich dazu nutzen, den Menschen zu danken, die direkt oder indirekt am Gelingen dieser Arbeit beteiligt waren.

Herrn **Prof. Dr. Andreas Pfitzmann** möchte ich posthum dafür danken, dass er mich für seine Fachdisziplin begeistert und in meinem Studium und Werdegang vielseitig unterstützt hat.

Meinen Betreuern **Dr.-Ing. Stefan Köpsell**, **Dipl.-Ing. Boris Vasilev** und **Dipl.-Inf. (BA) Felix Richter**, danke ich für die hilfreichen Anregungen und die kompetente Unterstützung, für Ihre Zeit, Ihr Verständnis und nicht zuletzt für die Möglichkeit, diese Arbeit am Lehrstuhl Datenschutz und Datensicherheit der Technischen Universität Dresden und im Fraunhofer CNT verfassen zu dürfen.

Beim **Fraunhofer CNT** möchte ich mich ganz besonders für die freundliche Arbeitsatmosphäre und die zur Verfügung gestellten technischen und organisatorischen Mittel bedanken.

Meinem guten Freund **Ralf Udtke** verdanke ich die grammatische Korrektheit der vorliegenden wissenschaftlichen Arbeit.

Allen meinen Freunden und Familienangehörigen, die mich moralisch unterstützt und sich um mein Wohlergehen gekümmert haben, bin ich ebenso zu großem Dank verpflichtet.

Vielen Dank!

Inhaltsverzeichnis:

1 Motivation

Praktisch alle Unternehmen und öffentlichen Einrichtungen erhalten, verwenden, speichern und verwalten sensible personenbezogene Daten über Kunden, Mitarbeiter, Patienten, Studenten, Schüler oder andere Einzelpersonen. Dazu kommen auch interne Informationen über Geschäftsvorgänge, Know-how, Erfindungen oder laufende Projekte. Der Verlust solcher Daten kann zu enormen finanziellen Einbußen, Imageschäden, sowie ethischen und rechtlichen Folgen führen, die wiederum fatale Auswirkung auf die Existenz des Unternehmens haben können. Somit stellen gespeicherte Informationen eines der wertvollsten Unternehmensgüter dar und müssen gegen unbefugte Zugriffe entsprechend abgesichert werden.

Viele Firmen nehmen die Gefahr vor Datenverlust oder Datenklau nicht ernst genug. Parallel dazu werden die Kapazität der Speichermedien (Festplatten, SD-Karten, USB-Sticks, DVDs usw.) immer größer, die Größe der Geräte immer kleiner und die Kosten niedriger. Somit ist es für die Unternehmen oft „billiger", zusätzlich Speicher zu kaufen als die bereits gespeicherten Daten abzusichern, zu verwalten oder veraltete bzw. bereits irrelevante Informationen zu archivieren bzw. zu löschen (endgültig zu vernichten). Zusätzlich dazu werden in der modernen Gesellschaft praktisch alle Dokumente digital erfasst und irgendwo mindestens ein Mal gespeichert.

Ob Datenklau, Veröffentlichung oder Missbrauch der sensiblen Daten – die Kosten für alle betroffenen Parteien sind am Ende oft viel höher als die Kosten für mögliche präventive technische Schutzmaßnahmen (wie eine komplette oder partielle Festplattenverschlüsselung). Dazu werden kurz zwei aktuelle markante Beispiele aufgeführt, um das Ausmaß dieses Problems zu verdeutlichen:

1. Beispiel: Verlust sensibler Daten in Großbritannien: Die auf 2 CDs gespeicherten Daten aller britischen Familien mit Kindern unter 16 Jahren[1] wurden im Oktober 2007 per Kurier verschickt und sind auf dem Sendeweg spurlos verschwunden. Auf den CDs befand sich eine Kopie der gesamten Dateneinträge, die für die Kindergeldzahlung benötigt werden – Namen, Adressen, Geburtsdaten, Kontoinformationen usw. Der

[1] Es waren insgesamt 25 Millionen Personen und 7,25 Millionen Familien durch den Vorfall betroffen.

Vorfall hat zu einem großen Imageverlust der britischen Steuerbehörde und der Regierung im eigenen Land gesorgt. Auch international ist Großbritannien dadurch in Kritik geraten. Der geschätzte Wert der Daten auf dem Schwarzmarkt beträgt 1, 5 Milliarden Pfund Sterling (nach [BBC11a] und [BBC11b]).

2. Beispiel: BP-Datenverlust:

Auf einer routinemäßigen Geschäftsreise verliert ein BP-Angestellter seinen dienstlichen Laptop und somit die persönlichen Daten von 13.000 Geschädigten der Ölpest im Golf von Mexiko (siehe [tdt11]). Neben Namen, Adressen, Geburtsdaten und Telefonnummern waren auch die in den USA so wichtigen Sozialversicherungsnummern (SSN) in dem verlorenen Datenbestand enthalten. Die Daten lagen laut BP-Sprecher unverschlüsselt auf der Festplatte und waren somit völlig ungeschützt gegen potenzielle Angreifer (siehe Abschnitt 5.2).

Immer mehr Mitarbeiter agieren mit vertraulichen Daten unterwegs. Dabei gewinnt das Erreichen eines gewissen Schutzniveaus der sensiblen Unternehmensdaten auf mobilen Clients (z.B. Laptops, Netbooks oder PDAs) und Wechselmedien (z.B. USB - Sticks) an Bedeutung und erweist sich gleichzeitig als eine der größten Schwachstellen in der IT-Infrastruktur des modernen Unternehmens. Sie sind für Verlust oder Diebstahl besonders anfällig. Das Problem wird durch ihre Handhabung und immer kleiner werdende Größe verstärkt. Diese Tendenz wird auch durch die Statistiken aus dem Microsoft Security Intelligence Report bestätigt (siehe [Mic10]). Bei Datenverlust (vor allem in Unternehmen) führen gestohlene und verlorene Geräte die Statistiken an. Abbildung 1 zeigt den Prozentsatz[2] der unterschiedlichen Sicherheitsverletzungen, die in dem Zeitraum von 3. Quartal 2009 bis 4. Quartal 2010 erfasst wurden.

[2] Die Summe der gemeldeten Sicherheitsverletzungen ist ungleich 100, weil es möglich ist, dass kein Vorfalltyp bzw. mehrere Vorfalltypen ausgewählt werden.

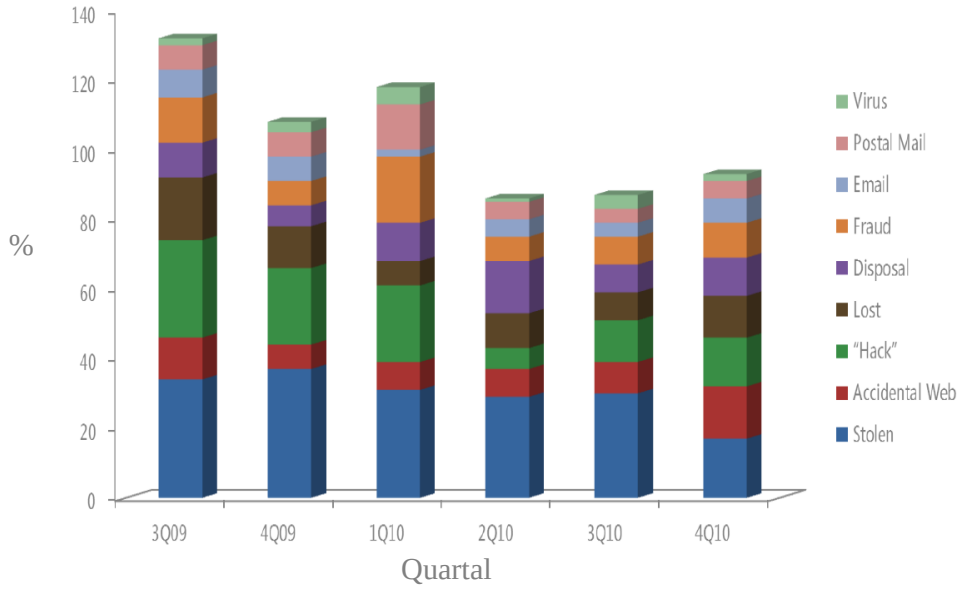


Abbildung 1. Sicherheitsverletzung nach Vorfalltyp, 3. Quartal 2009 bis 4. Quartal 2010 [Mic10]

Laut [CJK07] wurden Laptops zuerst aufgrund ihres eigentlichen Marktwertes als lukratives Diebesgut angesehen. In letzter Zeit konzentrieren sich Diebe jedoch nicht nur aufgrund des Wiederverkaufswertes der Hardware auf tragbare Systeme, sondern auch wegen der darauf enthaltenen vertraulichen, persönlichen und geschäftlichen Daten. Demnach kann ein Laptop-Diebstahl (bzw. Wechselmedien-Diebstahl) schwerwiegende Folgen für die Geschäfte eines Unternehmens haben:

- Kosten zur Kundenbenachrichtigung
- Schädigung des Images des Unternehmens
- Schäden an der Marke des Unternehmens
- Kundenverluste
- Umsatzverluste und geringere Gewinne
- Bußgelder
- Kostspielige Prozesse
- Erhöhtes Kundendienst- und Helpdesk-Aufkommen

- Niedrigerer Unternehmenswert
- Erschwerter Gewinn neuer Kunden
- Vertrauensverlust der Investoren
- Weitere straf- und zivilrechtliche Folgen bei Nichteinhaltung der gesetzlichen Rechtsvorschriften

Um die Wahrscheinlichkeit an Datenabfluss durch den Verlust oder Diebstahl mobiler Geräten so gering wie möglich zu halten, wird eine Sicherheitslösung benötigt, die es ermöglicht, dass Unbefugte keinen Zugriff auf gespeicherten Daten oder den Rest der IT-Infrastruktur bekommen. Andererseits soll das System möglichst zentralisiert und einfach zu verwalten sein.

Dazu gibt es eine Reihe vorhandener Produkte, die die bereits genannten Ziele durch Festplattenverschlüsselung zu erreichen versprechen. Dabei bestehen zwischen den einzelnen IT-Lösungen diverse Unterschiede bezüglich Benutzbarkeit, Sicherheit, Plattformunabhängigkeit, Wartbarkeit usw. Ziel der vorliegenden Arbeit ist es eine repräsentative Menge solcher Produkte auszuwählen, zu vergleichen und entsprechend zu bewerten. Dabei werden sie in der IT-Infrastruktur von Fraunhofer CNT getestet, um ein möglichst praxisnahes Untersuchungsszenario zu simulieren.

2 Einleitung

In der vorliegenden wissenschaftlichen Arbeit wird zuerst auf die theoretischen und die aufgabenspezifischen Rahmenbedingungen der durchgeführten Untersuchungen eingegangen. Es wird der Begriff der Festplattenverschlüsselung erläutert und die unterschiedlichen Verschlüsselungsmethoden vorgestellt (siehe Abschnitt 3). Anschließend werden die aufgabenspezifischen Auswahlkriterien und Rahmenbedingungen aufgezählt (siehe Abschnitt 4.1), die zum Festlegen der zu untersuchenden Softwareprodukte führten (siehe Abschnitt 4.2). Die konkreten Bedrohungen und zutreffenden Angriffsszenarien, die die IT-Infrastruktur des Fraunhofer CNT im Sinne des Aufgabenbereichs der vorliegenden Arbeit betreffen sowie ihre theoretische Grundlage werden im Abschnitt 5 im Detail betrachtet. Weiterhin wird im Kapitel 6 auf die Vergleichskriterien für die Produktauswahl, die technische Beschreibung der Testumgebung sowie die Methodik zum Testen von Benutzer- bzw. Administratorfreundlichkeit eingegangen. Der theoretische Teil wird mit der detaillierten Beschreibung des eingesetzten Verschlüsselungsalgorithmus (AES-256) abgerundet (siehe Abschnitt 7).

Als Nächstes werden die vier ausgewählten Verschlüsselungslösungen, ihre Funktionalität, ihre Integration in die Testumgebung und die Ergebnisse der damit verbundenen Tests betrachtet (siehe Abschnitte 8 bis 11). Kapitel 12 befasst sich mit der Untersuchung der Leistungsveränderungen des Testsystems durch die Festplattenverschlüsselung mit den gewählten Produkten. Dabei wird auf wichtige Merkmale, wie Ressourcenbelegung, Lese-, Schreib- und Kopierzugriffsgeschwindigkeit sowie Energieverbrauch eingegangen.

Kapitel 13.1 stellt eine Bewertung der Softwareprodukte bezüglich der ermittelten Ergebnisse dar. Weiterhin wird in Abschnitt 13.2 auf den Prozess der unternehmensinternen Implementierung eingegangen. Abschließend werden eine kurze Zusammenfassung und ein Ausblick auf offene relevante Forschungsfragen herausgearbeitet (Abschnitt 13.3).

3 Festplattenverschlüsselung – Begriffserklärung

Unter dem Begriff Festplattenverschlüsselung wird das Verschlüsseln der gesamten Festplatte beziehungsweise einzelner Partitionen verstanden, um sensible Daten vor unbefugtem Zugriff zu schützen (vgl. [wik11b]). Festplattenverschlüsselung wird oft als Full Disk Encryption (FDE) in der Fachliteratur bezeichnet und wird als Abkürzung in der vorliegenden Arbeit benutzt.

Grundsätzlich wird nach [CH09] bei der Festplattenverschlüsselung zwischen zwei Aufgaben unterschieden:

- Die eigentliche Ver- und Entschlüsselung kann sowohl durch die Software als auch die Hardware realisiert werden (siehe Punkt 3.1.1).
- Für eine erweiterte Benutzerauthentifizierung (jenseits eines simplen BIOS-Passworts) ist immer eine zusätzliche Software erforderlich (z.B. Mehrbenutzerbetrieb – Zugang zu einem bestimmten Rechner für unterschiedliche Benutzer mit jeweils eigenen Passwörtern).

Im Firmenumfeld besteht dazu oft noch die zusätzliche Anforderung, dass die unterschiedlichen Benutzerkonten über mehrere Systeme synchronisieren werden sollen, was sich durch den Einsatz einer zentralen Verwaltungslösung realisieren lässt.

3.1.1 Verschlüsselungsmethoden

Softwarebasierte Verschlüsselung: Wie man aus [wik11c] und [CH09] entnehmen kann, bleibt bei der softwarebasierten Festplattenverschlüsselung entweder ein Teil der Festplatte (z.B. der Master Boot Record) unverschlüsselt, weil dort die Verschlüsselungssoftware und das verwendete Schlüsselmaterial abgelegt sind, oder es wird ein zusätzlicher Datenträger genutzt (siehe Abbildung 2), von dem die Verschlüsselungssoftware bzw. das Schlüsselmaterial geladen werden. Das Schlüsselmaterial ist üblicherweise selbst mit einem Benutzerschlüssel (Passwort)

verschlüsselt, so dass ein Benutzer seinen Schlüssel ändern kann, ohne dass sämtliche Daten entschlüsselt und wieder neu verschlüsselt werden müssen. Dabei muss nur das Schlüsselmaterial entschlüsselt und mit dem neuen Benutzerschlüssel verschlüsselt werden. In einer bestehenden IT-Unternehmensinfrastruktur haben die Mitarbeiter in der Regel individuelle Passwörter, die den Zugriff auf die Firmenressourcen gewähren. Die Verschlüsselung des Schlüsselmaterials durch das Mitarbeiterlogin ermöglicht somit die transparente, im Hintergrund laufende Ver- und Entschlüsselung der Daten.

Hardwarebasierte Verschlüsselung: bei einer hardwarebasierten FDE kümmert sich die Festplatten-Hardware selbst um die Authentifizierung sowie um Ver- und Entschlüsselung der Daten. Dabei wird die Ver- bzw. Entschlüsselung der Daten transparent bei Lese- bzw. Schreibzugriffen durch die Festplatten-Firmware als Teil der Festplatten-Hardware realisiert [wik11c]. Nach [CH09] ist hierzu grundsätzlich keine zusätzliche Software nötig. Dabei werden die benötigten Schlüssel in einem speziellen Chip oder einer Festplatte verwaltet, die sie nie verlassen (siehe Abbildung 2). Die Verschlüsselungsoperationen sind direkt in der Hardware implementiert, wodurch der Prozessor entlastet wird (nach [wik11c]).

Beide Verschlüsselungsmethoden haben ihre Vor- und Nachteile bezüglich ihres Einsatzbereichs. Nach [Auf09] zeigt die Hardware-Verschlüsselung eine bessere Leistung und höhere Interoperabilität auf Kosten der Erweiterbarkeit, Administration und Recovery-Mechanismen. Darüber hinaus ist eine unternehmensweit einheitliche Ausstattung mit Verschlüsselungs-Hardware kaum möglich. Die Technologie selbst ist für Wechseldatenträger noch nicht reif genug (weist beträchtliche Sicherheitslücken auf [Sch10]) und mit höheren Kosten verbunden. Dadurch erweist sich die Hardware-Verschlüsselung als ungeeignet für den Unternehmenseinsatz.

Reine Softwarelösungen dagegen zeichnen sich weitestgehend als kompatibler zu vorhandenen Systemen ab. Sie unterstützen eine breite Palette verschiedener Benutzerauthentifizierungsverfahren (z.B. USB-Tokens, Smartcards, Fingerprintsensoren). Weiterhin bieten die meisten kommerziellen Software-Verschlüsselungsprodukte eine zentrale Verwaltung und Passwort- bzw. Datenwiederherstellungs-Mechanismen. Somit werden im weiteren Verlauf der

vorliegenden wissenschaftlichen Arbeit reine Softwarelösung untersucht und verglichen, die in der bereits vorhandenen IT-Infrastruktur des Fraunhofer CNT integriert werden könnten.

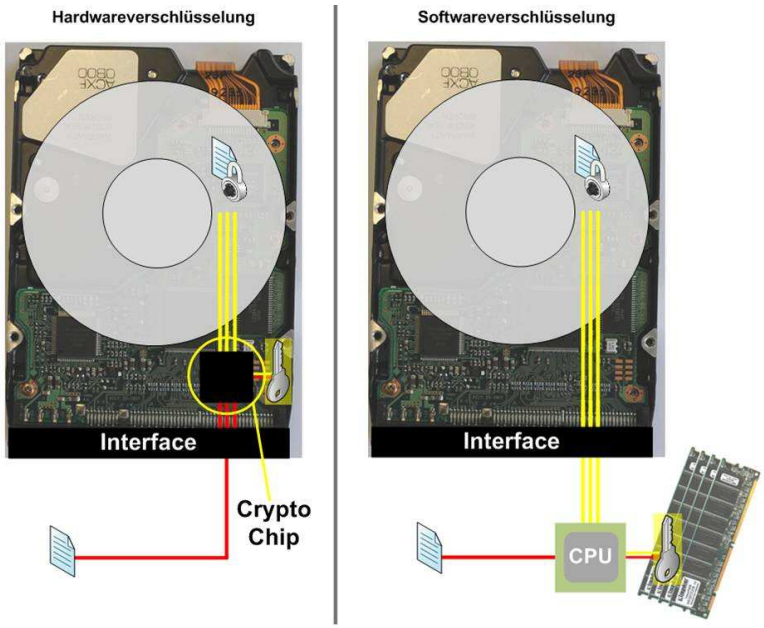


Abbildung 2. Verschlüsselungsmethoden [CH09]

4 Auswahlkriterien und Festlegen der zu untersuchenden softwarebasierten Lösungen zur Festplattenverschlüsselung

In diesem Kapitel werden die Rahmenbedingungen und Auswahlkriterien vorgestellt, die durch die konkrete IT-Infrastruktur des Fraunhofer-CNT und der beiden Interessensgruppen (Technische Universität Dresden und Fraunhofer-CNT[3]) entstanden sind. Anschließend werden die vier ausgewählten Full Disk Encryption-Lösungen kurz präsentiert.

4.1 Rahmenbedingungen und Auswahlkriterien

Um die Auswahl der zu untersuchenden softwarebasierten Lösungen zur Festplattenverschlüsselung zu treffen, sind zwei wichtige Aspekte im Vorfeld zu beachten. Erstens – welche Rahmenbedingungen entstehen durch die Anforderungen und die technischen Besonderheiten bezüglich der IT-Infrastruktur des Fraunhofer CNT und der Technischen Universität Dresden. Zweitens – welche weiteren Auswahlkriterien spielen eine Rolle für die Beschränkung der breiten Palette an vorhandenen FDE-Produkten für die Zwecke der vorliegenden Diplomarbeit.

Folgende Rahmenbedingungen bzw. Aspekte wurden bei der Auswahl der geeigneten Festplattenverschlüsselungsprodukte berücksichtigt:

- Die bereits existierende IT-Infrastruktur der FhG-CNT basiert auf dem von Microsoft angebotenen Betriebssystem – Windows XP Professional Service Pack 3, wobei ein Umstieg auf Windows 7 geplant ist. Somit wären FDE-Lösungen, die rein für andere Betriebssysteme konzipiert sind, ausgeschlossen. Weiterhin werden nur die Funktionen der Produkte unter Windows untersucht. Es wird jedoch darauf hingewiesen, dass in heterogenen

[3] Übersichtshalber werden in der vorliegenden Diplomarbeit die Abkürzungen TU-Dresden für Technischen Universität Dresden und FhG-CNT für Fraunhofer-CNT benutzt.

Unternehmensinfrastrukturen die Plattformunabhängigkeit der FDE-Lösung durchaus eine wichtige, zu berücksichtigende Anforderung darstellt.

- Ein weiterer wichtiger Aspekt besteht darin, welche Lizenzen von Softwareprodukten bereits vorhanden sind, die zur Festplattenverschlüsselung verwendet oder um die Festplattenverschlüsselungsfunktionalität erweitert werden können.

- Weiterhin wurde bereits durch die an der FhG-CNT geplante Umstellung von Windows XP auf Windows 7 die dafür benötigte Software erworben. Somit steht auch die von Microsoft angebotene, softwarebasierte FDE-Lösung – BitLocker zur Verfügung.

- Es muss berücksichtigt werden, welche Produkte sowohl für das FhG-CNT als auch für TU-Dresden von Interesse sind. Es muss Balance zwischen den beiden Interessensgruppen gefunden werden (siehe Abschnitt 4.2).

- Beschränkung der geeigneten FDE-Produkte auf eine realistische Anzahl, die im Rahmen der vorliegenden wissenschaftlichen Arbeit untersucht werden kann (siehe Abschnitt 4.2).

- Open Source vs. kommerzielle Lösungen für Festplattenverschlüsselung – Als Teil der Aufgabenstellung wird noch die Bedingung gestellt, dass kostenlose Open Source Lösungen und kommerzielle Produkte gegenüber gestellt werden sollen. In diesem Zusammenhang soll mindestens ein Produkt der jeweiligen Klasse im Rahmen der vorliegenden Diplomarbeit getestet werden (siehe Abschnitt 4.2).

- Ein „must-have“-Kriterium bei der Auswahl der zu untersuchenden FDE-Lösungen ist die Marktbeständigkeit der Softwareanbieter. Dabei muss gewährleistet werden, dass der Anbieter einen guten Namen auf dem Gebiet der Datensicherung hat und sich relativ stabil in den letzten Jahren auf dem Markt behauptet. Zum einen wird dadurch die Wartung der angebotenen Produkte

gesichert. Zum anderen liegt die Vermutung nahe, dass die Produkte solcher Anbieter eine höhere Sicherheitsstufe bieten.

- Unternehmensgröße – Es wird nach einer FDE-Lösung für das Fraunhofer-CNT und somit nach passenden Softwareprodukten für Unternehmen mit circa 50 Angestellten gesucht. Diese Bedingung spielt nur eine Rolle, wenn unterschiedliche Produkte für unterschiedliche Unternehmensgrößen angeboten werden.

4.2 Festlegen der zu untersuchenden softwarebasierten FDE-Lösungen

Bei der Auswahl der zu untersuchenden Softwarelösungen zur Festplattenverschlüsselung haben sich einige Schwierigkeiten ergeben. Viele der Anbieter und der Produkte sind entweder nicht mehr vorhanden, von anderen Unternehmen übernommen und unter neuen Namen geführt oder mit anderen Produkten verschmolzen. Dadurch ergibt sich ein sehr unübersichtliches Bild, was die für die Zwecke dieser Arbeit benötigten FDE-Lösungen betrifft.

Unter Berücksichtigung der in Abschnitt 4.1 beschriebenen Rahmenbedingungen wurden folgende 4 Produkte festgelegt, die im Rahmen der Diplomarbeit untersucht werden sollen:

- ***TrueCrypt*** ist als einzige nicht kommerzielle FDE-Software im Sinne der vorliegenden wissenschaftlichen Arbeit ausgewählt worden. Das Programm bietet eine breite Palette an Verschlüsselungsmechanismen und Funktionen an. Damit können unter anderem auch ganze Partitionen und Wechselmedien verschlüsselt werden. Wichtige Aspekte bei der Auswahl waren der sehr gute Ruf des Produkts unter den kostenlosen FDE-Lösungen, die ständige Weiterentwicklung, Verbesserung und Funktionalitätserweiterung von TrueCrypt seit bereits 7 Jahre (Version 1.0 wurde im Februar 2004 veröffentlicht) und die Tatsache, dass TrueCrypt ein Open Source Produkt ist (siehe Abschnitt 8). Bei kostenlosen Softwareprodukten ist es besonders wichtig,

dass sie Open Source (Softwareprodukte mit öffentlich zugänglichem Quelltext) sind. Somit besteht keine Anbieterabhängigkeit und der Quellcode kann auf eventuelle Schwachstellen jederzeit überprüft werden. Außerdem ist die Gefahr sehr gering, dass ein Masterkey vorhanden ist.

- ***PGP Whole Disk Encryption (PGP WDE)***: Eine kommerzielle FDE-Lösung, die für die Zwecke der vorliegenden wissenschaftlichen Arbeit ausgewählt wurde, ist die vor kurzem von Symantec übernommene „PGP Whole Disk Encryption“. Diese Festplattenverschlüsselungssoftware überzeugt mit einer langen und erfolgreichen Geschichte und ist durch hohe Sicherheit und geschickte Implementierung der Verschlüsselungsalgorithmen bekannt. Von PGP WDE wird eine zentrale Verwaltung bereitgestellt, die sich durch eine umfassende Funktionalität und Integrationsmöglichkeiten in bereits vorhandene IT-Infrastrukturen auszeichnet (für weitere Details siehe Abschnitt 9).

- ***SafeGuard Enterprise (SGN)*** ist das Produkt von Sophos zum Thema Festplattenverschlüsselung, das nach der Übernahme von Utimaco entstanden ist. Diese FDE-Lösung ist aktuell in der Version 5.60.0.192 und bietet neben den Verschlüsselungsfunktionalitäten eine zentrale Verwaltung und zahlreiche Erweiterungen, wie Nutzung bestehender Smartcard- und PKI- Strukturen, Verwendung bestehender Active Directory-Daten usw. (siehe Beschreibung des Produkts, Abschnitt 10). Die Auswahl dieser softwarebasierten Festplattenverschlüsselungssoftware wurde unter Beachtung der Rahmenbedingungen getroffen (siehe Abschnitt 4.1).

- ***McAfee Endpoint Encryption 6.1 (EE)*** ist das Produkt des Sicherheitsunternehmens McAfee, das etablierte Verschlüsselungsalgorithmen (z.B. AES-256 und RC5) benutzt und einen breiten Anwendungsfeld bietet, der Desktop-PCs, Laptops, Netzwerkdateien und -ordner, Wechseldatenträger und USB-Speichergeräte umfasst. Die zentrale Management-Konsole ePolicy Orchestrator (ePO)-Plattform übernimmt die Überwachung, Wartung und Berichterstattung. Die Software von McAfee wurde ausgewählt, da sie die Randbedingungen erfüllt. Somit könnte man bei diesem Produkt Vorteile auf

zwei Gebieten erwarten. Einerseits könnten Zeit- und Kostenaufwand durch Verlängerung bzw. Aktualisierung bereits vorhandener Lizenzen minimiert werden. Andererseits ist in dem neuen Produkt (McAfee EE) das Know-how von SafeBoot integriert worden, was sich für die Administration als vorteilhaft ergeben könnte (z.B. bekannte Verwaltungsvorgänge). Weitere Details und Besonderheiten des Produkts werden in Abschnitt 11 betrachtet.

In der engeren Auswahl für die Untersuchung war der Windows 7 BitLocker. Dabei handelt es sich um den Nachfolger von Windows Vista Bitlocker, der die von Microsoft erarbeitete FDE-Lösung für Enterprise- und Ultimate-Kunden darstellt. Bitlocker bietet eine Verschlüsselung von Datenpartitionen, USB-Medien (durch die für Windows 7 konzipierte Erweiterung für Wechselspeichergeräten – BitLocker To Go) oder auch des Systemlaufwerks an und erfüllt die gestellten Rahmenbedingungen. Es wurde jedoch im Verlauf der Vorbereitungsphase aus der Untersuchung ausgeschlossen. Ein Auszug der Gründe für diese Entscheidung wird im Folgenden beschrieben:

- BitLocker unterstützt nur einen Benutzer pro Gerät, wobei es immer den Maschinenschlüssel benötigt (in Form eines TPM-Chips, eines Files auf einem USB-Stick oder als ein konstantes 48-stelliges Kennwort, das durch seine Länge praktisch in einem Unternehmen nicht einsetzbar ist). Des Weiteren gibt es keine Funktionen wie verschiedene Benutzer-IDs, wechselbare PINs, Challenge/Response Mechanismen oder Passwortsynchronisation mit Windows Konten in BitLocker.

- Der für die Bitlocker-Authentifizierung benötigte TPM-Chip wird zwar bereits in viele Rechner eingebaut, aber es sind immer noch wenige Laptops damit ausgestattet. Speziell bei den im Fraunhofer CNT vorhandenen mobilen Rechnern ist der TPM-Chip nicht vorhanden.

- Microsoft bot zurzeit der Untersuchungen der vorliegenden wissenschaftlichen Arbeit keine zentrale Verwaltung für das Windows 7 BitLocker an und war somit für den Unternehmenseinsatz eher ungeeignet. Am 1. August 2011 hat Microsoft den *„Microsoft BitLocker Administration and Monitoring“*

veröffentlicht (siehe [Bea01]), wobei das Produkt zusätzlich erworben werden muss und mit zusätzlichen Kosten verbunden ist.

- Das Produkt konnte nicht gleichberechtigt mit den anderen FDE-Lösungen untersucht werden, da die zur Verfügung stehende Testumgebung auf Windows XP basiert und somit wäre ein Vergleich schwer bzw. überhaupt nicht realisierbar.

5 Bedrohungen und Schutzziele (Angreifermodell)

In diesem Kapitel wird auf die Fragen eingegangen: Was ist zu schützen? Vor wem ist zu schützen? Dabei werden als Erstes die theoretischen Ansätze betrachtet. Anschließend werden die konkreten Bedrohungen und Angriffsszenarien vorgestellt, die die IT-Infrastruktur des Fraunhofer CNT im Sinne des Aufgabenbereichs der vorliegenden Arbeit betreffen.

Die Bestimmung der spezifischen Angreifermodelle erlaubt es eine gezielte und präzisere Analyse der ausgewählten Softwareprodukte durchzuführen.

5.1 Begriffserklärung

In diesem Abschnitt wird die klassische Einteilung der Bedrohungen und korrespondierenden Schutzziele für Systeme der Informationstechnik vorgestellt. Anschließend wird auf den Begriff Angreifermodell eingegangen.

Zunächst muss geklärt werden, was unter dem Begriff „unbefugt“ zu verstehen ist. Die genaue Beschreibung wird beispielsweise durch internationale Konventionen, Verfassung, Gesetze, Betriebsvereinbarungen oder berufsständische Ethik festgelegt. „Unbefugtes“ Handeln wird mit einer Strafe bedroht, falls es überhaupt entdeckt wird (nach [Pfi10], S12). Um Unbefugtes möglichst zu erschweren bzw. zu verhindern, sollen Organisationsstrukturen entsprechend gewählt werden. Für ein Unternehmen bedeutet jedoch „unbefugt“, alles was das Unternehmen selbst als unbefugtes Handeln definiert. Damit ist eine Vorgehensweise gemeint, die die intern festgelegten Richtlinien verletzt bzw. von denen abweicht. Also wird „unbefugtes Handeln“ als die Kombination von internen Organisationsrichtlinien und der Gesetzeslage definiert.

Organisatorische Maßnahmen, wie Ge- und Verbote bieten in der Regel keine genügende Sicherheit gegen unbefugtes Handeln. Ein Verbot ist nur dann wirkungsvoll, wenn seine Einhaltung mit angemessenem Aufwand überprüft und durch

Strafverfolgung gesichert und der ursprüngliche Zustand durch Schadensersatz wiederhergestellt werden kann. Beides ist bei IT-Systemen leider nicht gegeben.

Datendiebstahl im Allgemeinen und speziell das direkte Abhören von Leitungen oder Kopieren von Daten aus Rechnern, ist kaum feststellbar (siehe Abschnitt 5.2), da sich an den Originaldaten nichts verändert. Genauso feststellbar ist das Installieren Trojanischer Pferde oder die unerlaubte Weiterverarbeitung von Daten, die man legal (oder auch illegal) erhalten hat.

Der ursprüngliche Zustand kann vor allem durch Löschen aller entstandenen Daten[4] wiederhergestellt werden. Es kann aber nie sichergestellt werden, dass nicht weitere Kopien existieren, die teilweise nicht vernichtet werden können bzw. dürfen (z.B. Daten, die im Gedächtnis von Menschen festgesetzt werden).

Demzufolge werden zusätzliche, wirkungsvollere Maßnahmen benötigt, wobei die vorbeugenden, technischen Schutzmaßnahmen die einzigen bekannten in diesem Zusammenhang sind.

Bedrohungen (Was ist zu schützen?): Die klassische Dreiteilung der Schutzziele für Systeme der IT wird aus ([Pfi10], S.7) entnommen und lautet:

- *Vertraulichkeit* – Informationen werden nur Berechtigten bekannt.
- *Integrität* – Informationen sind richtig, vollständig und aktuell[5] oder aber dies ist erkennbar nicht der Fall.
- *Verfügbarkeit* – Informationen sind dort und dann zugänglich, wo und wann sie von Berechtigten gebraucht werden.

Dabei werden unter „Information“ Daten, aber auch Programme und Hardwarestrukturen verstanden.

Damit „Berechtigten“ einen Sinn hat, muss zumindest außerhalb des betrachteten IT-Systems geklärt sein, wer, wann und wozu berechtigt ist.

[4] Modifikationen, die durch unbefugtes Handeln entstanden sind.
[5] „Richtig, vollständig und aktuell“ bezieht sich nur auf das Innere eines betrachteten Systems, da das Zutreffen von dessen Bild von seiner Umwelt nicht innerhalb des betrachteten Systems entscheidbar ist.

Durch technische Schutzmaßnahmen (Kryptographie) können die Schutzziele Vertraulichkeit und Integrität erreicht werden. Zur Verfügbarkeit trägt Kryptographie nicht oder allenfalls indirekt bei.

Angreifermodell: ein Angreifermodell definiert nach ([US07], S. 489) die Stärke eines Angreifers gegen den ein bestimmter Schutzmechanismus (z.B. ein bestimmtes Verschlüsselungsverfahren) noch sicher ist.

Dabei sind folgende Aspekte zu berücksichtigen:

1. Angreifer ist **aktiv** oder **passiv**:
   - Was kann der Angreifer **maximal** passiv **beobachten**?

     In diesem Fall wird analysiert, ob sich der Angreifer außerhalb seines Berechtigungsbereiches bewegt, indem er beispielsweise Leitungen oder Funkstrecken abhört, lokal Daten anders auswertet oder länger speichert als er darf. In diesem Fall spricht man von einem beobachtenden Angriff.

   - Was kann der Angreifer **maximal** aktiv kontrollieren (steuern, verhindern) bzw. **verändern**?
2. Mächtigkeit des Angreifers
   - Wie viel Rechenkapazität besitzt der Angreifer?
   - Wie viele finanzielle Mittel besitzt der Angreifer?
   - Wie viel Zeit besitzt der Angreifer?
   - Welche Verbreitung[6] hat der Angreifer?

Potenzielle Angreifer können Außenstehende, Teilnehmer (Benutzer des Systems), Betreiber, Hersteller, Entwickler und Wartungstechniker[7] sein, wobei sie natürlich miteinander kooperieren können. Es kann auch nach Angreifern unterschieden werden,

[6] Welche Leitungen, Kanäle, Stationen können von dem Angreifer beherrscht werden?
[7] Es sind auch weitere Angreifer möglich, wie Produzenten bzw. Entwerfer der Entwurfs- und Produktionshilfsmittel ([Pfi10], S. 8).

die sich innerhalb und außerhalb des beobachteten IT-Systems befinden. Die Feststellung, dass eine Instanz angreifen kann, bedeutet nicht, dass sie auch tatsächlich angreift.

Dennoch gilt, dass Schutz vor einem allmächtigen Angreifer natürlich nicht möglich ist ([Pfi10], S. 13). Deswegen sind alle folgenden Maßnahmen nur Annäherung an den perfekten Schutz der Teilnehmer vor jedem möglichen Angreifer.

Abbildung 3 gibt eine Übersicht über möglichen Schutzmechanismen gegen bestimmte Angreifergruppen. Es werden die möglichen Angreifer und die gewünschten Schutzziele veranschaulicht. Dabei ist ein Open-Source Softwareprodukt ein gutes Beispiel für die Absicherung der Benutzer gegen Entwerfer und Produzenten des Systems. Mehrere unabhängige Entwerfer arbeiten mit untereinander verständliche Zwischensprachen und Zwischenergebnisse, die mit unabhängigen (öffentlichen) Werkzeugen analysiert werden. Das Produkt wird durch unabhängige Experten immer wieder auf Schwachstellen untersucht.

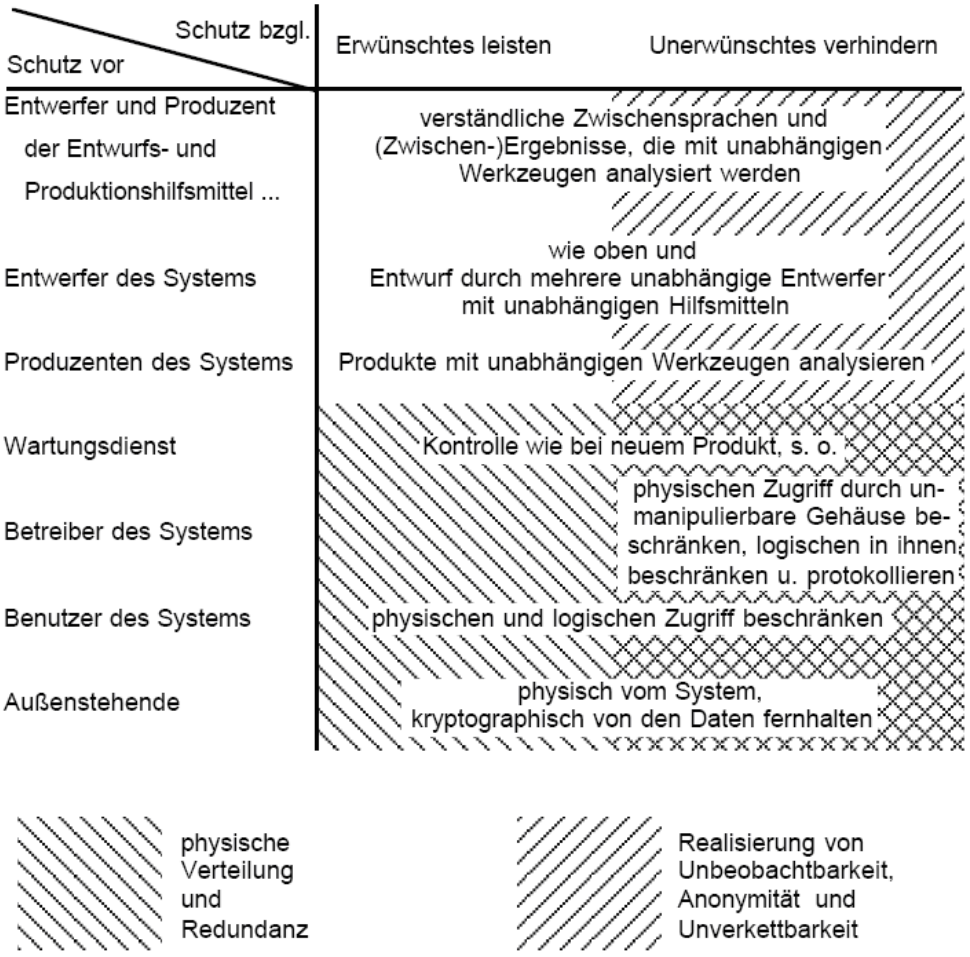


Abbildung 3. Welche Schutzmaßnahmen schützen gegen welche Angreifer ([Pfi10], S. 13)

Die resultierenden Schutzziele und Schutzmechanismen lassen sich nach ([Pfi10], S. 146) grob in folgende zwei Kategorien einteilen:

Erwünschtes leisten, d.h. das System soll bestimmte Aktionen ausführen: Ein Teilnehmer kann dann geschädigt werden, wenn ein von ihm angeforderter Dienst verhindert, verzögert oder verändert wird oder über seinen Account bzw. auf seine Kosten eine Kommunikationsbeziehung ohne sein Wissen oder seine Billigung aufgebaut wird. Eine Schädigung kann ebenfalls eintreten, wenn er in einem Streitfall den Versandt oder den Empfang einer bestimmten Nachricht nicht nachweisen kann.

Dieses sind – mit anderen Worten formuliert – bereits unter „Integrität und Verfügbarkeit“ aufgeführte Schutzziele.

Damit dieser Schaden tatsächlich entsteht, sind verändernde Angriffe nötig. Diese können prinzipiell im IT-System erkannt werden. Oder anders gesagt: Ob das Erwünschte geleistet wurde, ist auch im Nachhinein überprüfbar.

Unerwünschtes verhindern, d.h. unerwünschte Aktionen des Systems sollen verhindert werden: Ein Teilnehmer kann auch dadurch Schaden erleiden, wenn ein Außenstehender seine Kommunikation ausspäht. Dieses bezieht sich hierbei nicht nur auf das Erfassen der Inhalte sondern auch der jeweiligen Umstände (Partner, Zeitpunkt, Ort) der Kommunikation. Eine Formulierung erfolgte bereits unter dem Schutzziel „Vertraulichkeit“.

Damit ein möglicher Schaden tatsächlich entsteht, sind nur beobachtende Angriffe nötig. Diese können im IT-System prinzipiell nicht erkannt werden. Die Einhaltung des Schutzzieles „Vertraulichkeit“ ist hier also im Nachhinein nicht überprüfbar und vorbeugende Maßnahmen sind daher unumgänglich.

5.2 Relevante Angriffsszenarien

In diesem Abschnitt werden die Angriffsszenarien betrachtet, die für die Ziele der vorliegenden Arbeit als relevant eingestuft wurden. Daraus wird abschließend ein konkretes Angreifermodell gebildet. Die in der vorliegenden Arbeit untersuchten Schutzmaßnahmen (FDE-Lösungen) müssen das konkrete System (mobile Rechner und Wechselmedien) gegen die maximale Stärke des beschriebenen Angreifers absichern.

Das zugrunde liegende System ist bereits bei dem schwächsten Angreifer nicht mehr geschützt.

Angreifer besitzt keine zusätzlichen Informationen:

1. Bei Verlust bzw. Diebstahl von externen Speichermedien (wie z.B. USB-Sticks, externe Festplatten, digitale Speicherkarten u.Ä.) liegen die Daten ungeschützt vor und sind ohne Hindernisse für alle Unberechtigten zugreifbar. Auch Daten

die bereits aus den genannten Speichermedien gelöscht, aber nicht überschrieben wurden, können ohne viel Aufwand rekonstruiert werden[8]. Somit werden die klassischen Sicherheitsziele Verfügbarkeit und Vertraulichkeit verletzt.

2. Bei Verlust oder Diebstahl von Laptops oder ähnlichen Geräten, die über eine demontierbare Festplatte verfügen und durch einen Benutzerpasswort gesichert sind, kann der Angreifer diese entfernen und an eine beliebiges Gerät anschließen. Die Daten liegen ungeschützt auf der Festplatte und werden somit ohne weiteren Aufwand für Unbefugte zugreifbar (Verletzung der Verfügbarkeit und Vertraulichkeit).

3. Eine Verletzung der Integrität ist durch unbemerktes Entwenden der unverschlüsselten Festplatte (hier besteht kein Unterschied, ob es sich dabei um ein externes Speichermedium oder um eine eingebaute Festplatte handelt), Verändern der Daten (Löschen, Hinzufügen, Modifizieren des Datenbestandes) und wieder unbemerktes Zurückbringen (bzw. Einbauen) der Festplatte möglich.

4. Nachdem sich der Benutzer an seinem Laptop authentifiziert hat, gelingt es dem Angreifer unbemerkt auf ein eigenes externes Speichermedium Daten zu kopieren.

5. Nachdem sich der Benutzer an seinem Laptop authentifiziert hat, gelingt es dem Angreifer unbemerkt Daten zu modifizieren[9].

6. Der Angreifer hat freie Sicht auf den Bildschirm und kann vertrauliche Daten auslesen bzw. ansehen. In diesem Fall kann durch technische Maßnahmen kein Schutz gewährleistet werden und er wird weiterhin in der vorliegenden Arbeit nicht betrachtet.

Es ist denkbar, dass auch weitere Angriffsszenarien für das beschriebene System konstruiert werden können und durchaus möglich sind. Die Wahrscheinlichkeit des

[8] Dafür ist eine Datenrekonstruktionssoftware nötig. Online sind jedoch genügend Open Source Anwendungen, die leicht und ohne großes zusätzliches Wissen bereits gelöschte Daten wiederherstellen.
[9] Die Angriffsszenarien 4 und 5 können dabei auch in einer kombinierten Form auftreten.

Auftretens solcher Angriffe wird jedoch als minimal eingestuft und in der vorliegenden wissenschaftlichen Arbeit nicht weiter betrachtet.

Unter Berücksichtigung der möglichen Angriffsszenarien wird das folgende theoretische Angreifermodell gebildet:

- Angreifer hatte keinen physischen Zugriff auf die zu schützenden Speichermedien vor der Verschlüsselung oder im laufenden Betrieb und konnte keine Hardware- bzw. Softwaremanipulationen (z.B. Trojaner installieren) durchführen.
- Angreifer agiert komplexitätsbeschränkt und besitzt ungenügend intellektuelle und finanzielle Mittel, um das verschlüsselte System zu brechen.
- Die zur Verschlüsselung eingesetzten Algorithmen sollen die Daten für mindestens 10 Jahre schützen können. Somit wird angenommen, dass ein potenzieller Angreifer in diesem Zeitraum unter keinen Umständen die Algorithmen brechen kann.
- Der Angreifer ist nicht in der Lage sich die Zugangsdaten zur verschlüsselten Speichermedium bzw. System zu verschaffen (z.B. durch Erpressung).
- Angreifer ist ein auf Bezug auf die Unternehmensstruktur außenstehende Person bzw. Organisation.

Bemerkung:

Die Einsetzung einer FDE-Lösung für die tragbaren Computer bzw. externen Speichermedien ist auf jeden Fall eine für Unternehmen unverzichtbare Schutzmaßnahme. Sie deckt jedoch nicht alle möglichen Angriffsbereiche auf einem (tragbaren) System und die darauf gespeicherten Daten ab und schützt nur gegen Gerätediebstahl oder Verlust und gegen die oben beschriebene Angreiferstärke.

6 Vergleichskriterien

Der wichtigste Aspekt vor der Untersuchung und dem Vergleich der ausgewählten Softwarelösungen zur Festplattenverschlüsselung ist das Festlegen der Vergleichskriterien, die auch gleichzeitig die zu untersuchenden Merkmale darstellen. Es wurde folgende Liste an Kriterien erarbeitet:

1. Sicherheitskriterien – inwieweit werden die klassischen Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) durch das Produkt eingehalten? Bestehen bereits bekannten Schwachstellen, die zu einem Angriff im Sinne des im Abschnitt 5.2 beschriebenen Angreifermodells relevant sind? Konnten weitere Schwachstellen entdeckt werden?

2. Technologie

   - Verschlüsselungsalgorithmen und deren Sicherheitsgrad (siehe Abschnitt 7) Welche Verschlüsselungsalgorithmen werden von den ausgewählten Produkten umgesetzt und welche Merkmale zeichnen sie aus?

   - Verschlüsselungstyp (Pre-Boot oder Post-Boot-Verschlüsselung)

   - Verschlüsselungsart (Festplatte, Partition, Ordner) – Welche Funktionalitäten umfassen die ausgewählten Produkte?

   - Authentifizierungsmethode (Passwort oder Apparatur) – Wird zusätzliche Hardware für die Authentifizierung benötigt und wenn ja, welche Konsequenzen entstehen daraus?

   - Notfallmaßnahmen bei Datenverlust (Datenwiederherstellung) – Welche Strategien bieten die Softwarelösungen zur Festplattenverschlüsselung im Falle eines Datenverlusts?

3. Hardware

- Typen von Authentifizierungsgeräten und –marken (Karte, Schlüsselanhänger) – falls zusätzliche Hardware für die Authentifizierung gebraucht wird oder benutzt werden kann.
- Verschlüsselungsmodule

4. Integration in die vorhandene IT-Umgebung
   - Berechtigungen, die zur Anwendung nötig sind (Verwaltungsrechte, Zugriffsrechte, Rechtevergabe)
   - Integration in die existierende Certification Authority (CA)
   - Softwarepaketierung- und Verteilung
   - Verwaltungsfunktionalitäten
5. Wirtschaftlichkeit
   - Preis- Leistungsverhältnis, Wartung, Unterstützung durch den Anbieter
   - Plattformunabhängigkeit – Für die Auswahl der 4 softwarebasierten Lösungen zur Festplattenverschlüsselung war es wichtig, dass sie Windows XP unterstützen (siehe Abschnitt 4.1). Trotzdem ist es von Interesse, ob die Produkte auch weitere Plattformen unterstützen und ob das eventuell mit Leistungseinbußen verbunden ist.
6. Handhabung
   - Benutzerfreundlichkeit – Wie intuitiv ist die Nutzung der jeweiligen Software? Kommt auch ein unerfahrener Nutzer damit zurecht? Mit welchen zusätzlichen Störfaktoren bzw. welchem Aufwand ist die Verschlüsselung verbunden – wie viel merkt der Endnutzer dabei?
   - Unternehmensfreundlichkeit – Administration/Management

1. Passwort: Hinterlegen, Verwalten, Wiederherstellen. Welche Strategien sind in den FDE-Lösungen eingebaut (sowie Funktionsweise und Effizienz)?

2. Back-up – Konzepte und Funktionsweise – Dabei werden die Back-up Strategien verglichen, die von den Produkten angeboten werden, ohne die bereits bestehende Infrastruktur von FhG-CNT zu berücksichtigen, in der bereits eine sehr gute Lösung implementiert ist.

6.1 Wichtige Bemerkungen

6.1.1 Technische Ressourcen zum Testen der Produkte

Für die Tests der vier FDE-Softwareprodukte wurden vier identische Rechner zur Verfügung gestellt, die als Clients dienen und mit der jeweiligen Software verschlüsselt werden sollen. Sie haben folgende Charakteristiken:

- *Rechner:* HP Compaq dc7700 Small Form Factor Base Unit; Intel Core 2 CPU 6300 @ 1,86 GHz 1,86 GHz; 1 GB RAM; DVD RW;

- *Test-Festplatte:* Western Digital Caviar 80GB Festplatte; Model Nummer: WD800JD-60LSA5; Firmware: 10.01E03; Standard-Version: ATA/ATAPI-7; Puffergröße: 8192KB; Unterstützte UDMA-Modi: 0 1 2 3 4 5; UDMA-Mode 5 aktiviert;

- *Test-Betriebssystem:* Microsoft Windows XP Professional, Version 2002 Service Pack 3 – Installiert mit allen aktuellen Updates;

- *Netzwerk-Infrastruktur:* Der Rechner hat Zugriff auf den NetApp Filer (Netzwerk Speichersystem);

Für die Verwaltungssoftware der FDE-Lösungen von Symantec (PGP), Sophos und McAfee sind 2 virtuelle Server mit folgenden Charakteristiken eingerichtet worden:

Server für die Verwaltung der FDE-Lösungen von Sophos und McAfee:

Betriebssystem: Windows Server 2008 R2 Datacenter Service Pack 1 (64-Bit), Prozessor: Intel Xeon CPU E5620 @ 2,40 GHz 2,40 GHz (2 Prozessoren); 4 GB RAM; Festplatte: 70 GB;

Server für die Verwaltung der FDE-Lösungen von PGP:

Betriebssystem: Anderes[10] 2.6x Linux-System (32-Bit); Prozessor: 2 vCPU, Intel Xeon @ 3 GHz; EVC-Modus: Intel Xeon 32nm Core i7; 4 GB RAM; Festplatte: 54 GB;

6.1.2 Der Cognitive Walkthrough – Methode zum Messen von Benutzer- bzw. Administratorfreundlichkeit

Um eine möglichst akkurate Bewertung für die Benutzer- bzw. Administratorfreundlichkeit der untersuchten Softwareprodukte erstellen zu können, wird die Methode des Cognitive Walkthrough zu Grunde gelegt. Sie wird zum Testen der Benutzbarkeit eines Systems bei der erstmaligen Nutzung und ohne formales Training verwendet [Ram11]. Dabei ist der Cognitive Walkthrough eine Methode zur formalen (analytischen) Evaluation und basiert auf der Theorie zum explorativen Lernen, die aus der Kognitionswissenschaft stammt. Der Ablauf der Methode wird nach [wik11a] folgendermaßen gegliedert:

1. Definieren der Eingangsdaten

    - Benutzercharakteristiken: Definieren der Benutzergruppe des Produkts – welches Wissen und welche Erfahrungen müssen die Zielpersonen minimal besitzen.

    - Beispielaufgaben: Welche Aufgaben sollen von den Benutzern erledigt werden (z.B. das Verschlüsseln eines USB-Sticks).

    - Handlungssequenzen: Es wird der ideale Weg festgelegt, der zum erfolgreichen Lösen bzw. Erledigen der Aufgabe führt.

[10] Linux-basiertes eigenes Betriebssystem von dem PGP Universal Server.

2. Untersuchung der Handlungssequenz:

   In dieser Phase werden die Einzelschritte des korrekten Lösungswegs untersucht, wobei für jede Benutzereingabe sowohl die benötigten Voraussetzungen, als auch die daraus resultierenden Folgen durchzudenken sind. Dabei wird auf folgenden Fragen eingegangen:

   - Wird der Benutzer versuchen, den richtigen Effekt zu erzielen?
   - Wird der Benutzer erkennen, dass die korrekte Aktion zur Verfügung steht?
   - Wird der Benutzer eine Verbindung zwischen der korrekten Aktion und dem gewünschten Effekt herstellen?
   - Wenn die korrekte Aktion ausgeführt worden ist: Wird der Benutzer den Fortschritt erkennen, also Feedback erhalten?

3. Protokollierung kritischer Informationen

   - Welche Informationen (in Form von Kenntnissen und Erfahrungen der Benutzer) werden zum erfolgreichen Erledigen der verschiedenen Handlungsschritte benötigt?
   - Daten über Aktionen , die wahrscheinlich zu Fehlbedingungen und damit zu Problemen beim Nutzer führen.

4. Revision des Interfaces

   Erarbeiten von Verbesserungsvorschlägen anhand der durch das Verfahren des Cognitive Walkthrough ermittelten Ergebnisse.

Die Methode der Cognitive Walkthrough wird entsprechend der Ziele der vorliegenden wissenschaftlichen Arbeit angepasst. Die daraus entstandenen Bewertungen der untersuchten Produkte bezüglich ihrer Benutzer- und Administratorfreundlichkeit werden in den dazu korrespondierenden Kapiteln präsentiert, wobei nicht auf die einzelnen Schritten explizit eingegangen wird. Dies wird unter anderem durch den

intuitiven Ablauf und die subjektive Natur des Verfahrens ermöglicht. Das konkrete Ablaufschema und die dazugehörigen Spezifikationen werden wie folgt definiert:

1. Definieren der Eingangsdaten
    - Benutzercharakteristiken: Die Produkte werden unter dem Gesichtspunkt von zwei unterschiedlichen Zielgruppen untersucht, die folgende minimale Anforderungen erfüllen:

      Benutzer: Erfahrung mit Windows XP oder höher. Allgemeines Wissen über den Installationsvorgang von einfachen Computeranwendungen (Walkthrough-Installationen).

      Administrator: Vertieftes Wissen in der IT-Infrastruktur des FhG-CNT, sowie ihrer Verwaltung (z.B. Struktur der Active Directory, Verwalten von Benutzern, Rechtevergabe bzw. Beschränkung der Rechte, Installationen von neuen Softwareprodukten, sowie ihr Verbreiten durch das interne Netzwerk usw.).

    - Aufgaben :

      Benutzer: Reibungslose Authentifikation; Transparente Verschlüsselung der Computerfestplatte; Verschlüsselung eines externen Mediums (externe Festplatte, USB-Stick) ; Selfrecovery im Falle eines vergessenen Passwortes usw.

      Administrator: Installation der Verwaltungssoftware der entsprechenden Produkte; Erstellung von Richtlinien; Verteilung der Software an die Clients; Passwort Recovery usw.

      Bemerkung: Die Liste der Aufgaben dient zur Veranschaulichung der Methodik zum Bewerten der Benutzer- bzw. der Administratorfreundlichkeit und beinhaltet nicht alle getesteten Aufgaben. Der volle Umfang der getesteten Aufgaben wird in den korrespondierenden Kapiteln vorgestellt

- Handlungssequenzen: Bei der Untersuchung werden die Softwareprodukte zum ersten Mal getestet. Somit wird das erfolgreiche Lösen bzw. Erledigen der Aufgabe/n angestrebt. Ein idealer Weg kann nicht festgelegt werden.

2. & 3. Untersuchung der Handlungssequenz & Protokollierung kritischer Informationen

Bemerkungen:

Schritt 2 und 3 werden kombiniert durchgeführt, um eine entsprechende Beurteilung bilden zu können, ob ein bestimmter Vorgang benutzerfreundlich bzw. administratorfreundlich gestaltet ist oder eventuelle Mängel aufweist. Die daraus entstehenden Ergebnisse werden, wie bereits erwähnt, in den jeweiligen produktspezifischen Abschnitten präsentiert.

Schritt 4 fällt aus, da die untersuchten FDE-Lösungen anhand ihrer Merkmale und Funktionalitäten verglichen werden und nicht in der Entwicklungsphase stehen. Somit werden keine Verbesserungsvorschläge benötigt.

7 Verschlüsselung – Verfahren, Struktur und kryptografische Stärke

Die Qualität einer FDE-Lösung hängt von dem Aufbau und der kryptografischen Stärke des in dem Produkt implementierten Verschlüsselungsverfahrens ab, wobei die ausgewählten Software-Produkte in Einzelfällen mehrere unterschiedliche Algorithmen zur Verfügung stellen. Beispielsweise bietet TrueCrypt neben dem Advanced Encryption Standard (AES) auch die Verschlüsselungsalgorithmen Twofish und Serpent. Man hat die Möglichkeit zwischen diesen drei Algorithmen auszuwählen oder sogar Kaskaden dieser drei Algorithmen zu bilden. Andere FDE-Lösungen, wie zum Beispiel die Softwareprodukte zur Endpointverschlüsselung von McAfee, Sophos oder PGP bieten dagegen nur den AES, wobei man meistens die Möglichkeit hat, zwischen unterschiedlichen Modi und Schlüssellängen auszuwählen (siehe nachfolgend die Spezifikationen der einzelnen Produkten). Somit dient der AES-Algorithmus als „quasi-Standard“ bei der Festplattenverschlüsselung und wird in diesem Abschnitt im Detail vorgestellt und weiterhin als Vergleichskernpunkt bezüglich des Verschlüsselungsaufbaus der zu untersuchenden FDE-Lösungen genutzt.

7.1 Advanced Encryption Standard (AES)

Nachdem der Data Encryption Standard (DES) durch Brute-Force-Angriffe (Durchprobieren aller möglichen Schlüssel) gebrochen wurde und aufgrund seiner geringen Schlüssellänge und der stark angestiegenen Rechenleistung als zu schwach eingestuft worden war, hat die US Regierung im Jahr 1997 einen Wettbewerb für einen neuen Standard gestartet, nämlich den Advanced Encryption Standard (AES). Drei Jahre später wurde eine leichte Modifikation des Rijndael als Standard ausgewählt.

Rijndael [11] ist eine symmetrische Blockchiffre. Somit werden Daten mit ein- und demselben Schlüssel blockweise ver- und entschlüsselt. Dabei haben Blöcke eine variable Größe von 128, 192 oder 256 Bits. Unabhängig davon kann eine

[11] Rijndael ist der ursprüngliche Name des AES Standards. Beide Bezeichnungen werden im Kontext der vorliegenden Arbeit als Äquivalent genutzt.

Schlüssellänge von 128, 192 oder 256 Bits festgelegt werden. Davon wird entsprechend die Bezeichnung der drei AES-Varianten AES-128, 192 bzw. 256 abgeleitet. Bereits der kürzeste Schlüssel von 128 Bit macht einen Brute-Force-Angriff 2^{72} mal aufwendiger als bei DES ($2^{128\text{ Bit Schlüssel bei AES-56 Bit Schlüssel bei DES}} = 2^{72}$). Nach dem Mooreschen Gesetz verdoppelt sich die Anzahl der Transistoren pro Chipfläche aller 18 Monate und somit verdoppelt sich auch die Geschwindigkeit der Computerprozessoren bei gleichbleibendem Preis in diesem Zeitraum (vgl. [Wil04]). Danach ist in 100 Jahren das Durchprobieren aller 128 Bit-Schlüssel bei AES ungefähr so zeitaufwändig wie beim DES heute. Werden gegen Rijndael keine effektiveren Angriffsmöglichkeiten gefunden, so dürfte er mit Schlüsseln $\geq$ 192 Bit für die nächsten 100 Jahre sicher genug sein.

7.1.1 Beschreibung des Algorithmus[12]

Die Blocklänge für alle AES-Kandidaten wurde auf 128 Bit vorgeschrieben, wobei der Rijndael-Algorithmus auch die Blocklängen 192 und 256 Bit unterstützt. Die vorliegende Arbeit wird auf die Betrachtung einer Blocklänge von 128 Bit beschränkt, da dies der relevanten Größe für die getesteten Softwareprodukte entspricht. Beim AES richten sich die standardmäßig verwendeten Rundenzahlen nach der Schlüssellänge. Wird ein 128-Bit-Schlüssel eingesetzt, so durchläuft der Klartext 10 Runden des AES. Bei Einsatz eines 192-Bit-Schlüssels werden 12 Runden durchlaufen und bei einer Schlüssellänge von 256 Bit werden 14 Runden durchlaufen.

Der Textblock wird beim AES als 4x*Nb*-Matrix betrachtet, wobei *Nb* für die Blocklänge in Bit dividiert durch 32 steht. Bei einer Blocklänge von 128 Bit ist *Nb* demnach 4 und es handelt sich um eine 4x4-Matrix. Die Einträge dieser Matrix, die im Folgenden als *T* bezeichnet wird, besitzen eine Länge von 1 Byte.

Zu Beginn des Algorithmus werden alle Einträge der Matrix *T* mit jeweils einem Byte eines Teilschlüssels XOR-verknüpft. Anschließend beginnen die einzelnen Runden, die nach folgendem Schema bearbeitet werden.

[12] Die Beschreibung des AES-Algorithmus richtet sich nach [Wil04], [Rep11] und [aes01].

Zunächst wird die Matrix *T* einer Substitution, die als „ByteSub“ bezeichnet wird, unterzogen. Jedes Byte der Matrix ist dabei Input für eine *S*-Box, deren Output wiederum ein Byte ist. Die *S*-Box ist die Komposition aus zwei Transformationen. Zuerst wird die multiplikative Inverse über das Galoisfeld GF(2^8) gebildet. Anschließend wird eine affine Transformation über GF(2) nach folgender Definition durchgeführt:

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} * \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Die Substitution wird im folgenden Bild veranschaulicht:

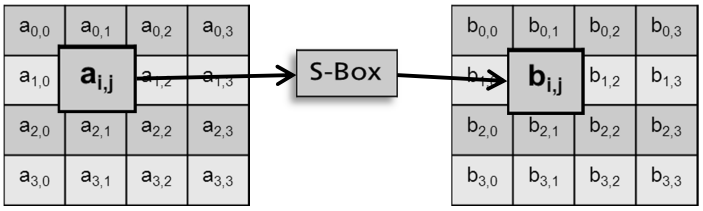


Abbildung 4. ByteSub (nach [Rep11])

Anschließend wird auf dem Textblock *T* eine Zeilenrotation durchgeführt, die als „ShiftRow“ bezeichnet wird. Die Art der Rotation ist hierbei von der Größe der Matrix bzw. von der Blocklänge abhängig. Im betrachteten Fall (die Blocklänge ist dabei 128 Bit => T ist eine 4x4-Matrix) rotiert die erste Zeile um 0, die zweite um 1, die dritte um 2 und die vierte Zeile um 3 Positionen nach links (siehe Abbildung 5).

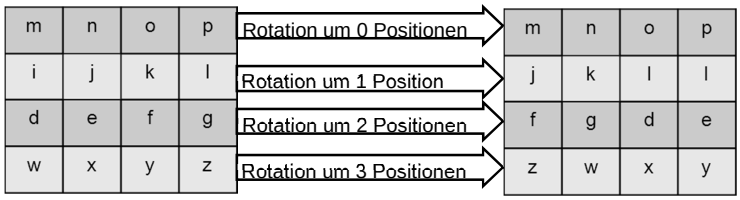


Abbildung 5. Darstellung der „ShiftRow“ Transformation (nach [Rep11])

Als Nächstes werden die Einträge der Matrix *T* als Polynome über GF(2^8) betrachtet. Jede Spalte der Matrix *T* wird in der Funktion „*MixColumn*“ mit einem fest definierten Polynom *c(x)* modulo $(x^4 + 1)$ multipliziert. Dies kann auf Grund des Moduls als Matrixmultiplikation geschrieben werden.

Das Polynom *c(x)* ist gegeben durch:

$c(x) = ´03´ \cdot x^3 + ´01´ \cdot x^2 + ´01´ \cdot x + ´02´$

Die Koeffizienten entsprechen hierbei der hexadezimalen Schreibweise von Polynomen modulo $(x^4 + 1)$. Daraus ergibt sich die Matrix *C*:

$$C = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

Die einzelnen Spalten der Matrix *T* werden also mit der Matrix *C* multipliziert, wobei die Addition der Einträge einer XOR-Verknüpfung entspricht und die Multiplikation der Einträge modulo $(x^4 + 1)$ durchgeführt werden muss (siehe Abbildung 6).

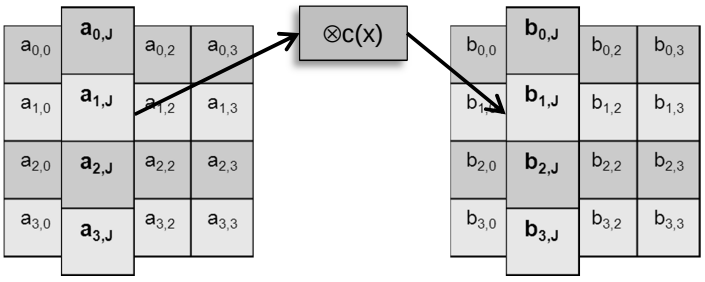


Abbildung 6. Darstellung der „MixColumn“ Transformation (nach [Rep11])

Abschließend werden alle Einträge der Matrix *T* mit den Einträgen einer rundenabhängigen Teilschlüsselmatrix XOR-verknüpft. Dabei hat die Teilschlüsselmatrix die gleiche Größe, wie die Textmatrix *T*. Weitere Details zur Berechnung des Rundenschlüssels, des Aufbaus der rundenabhängigen Teilschlüsselmatrix, des Ablaufs der „*AddRoundKey*“ - Transformation oder generell zu dem Algorithmus können aus der offiziellen Veröffentlichung des AES durch NIST (National Institute of Standards and Technology) entnommen werden (vgl. [aes01]).

In der letzten Runde des Algorithmus wird die Funktion „*MixColumn*“ nicht durchgeführt.

Zur Entschlüsselung wird der gesamte Algorithmus rückwärts durchlaufen und auch die Teilschlüssel werden umgekehrt zugeordnet. Die XOR-Verknüpfung ist selbstinvers, somit muss keine gesonderte Funktion eingesetzt werden.

Für die Funktion „MixColumn“ muss eine inverse Operation definiert werden. Die Einträge der Matrix *T* werden wiederum mit einer Matrix, der inversen Matrix zu *C* multipliziert (im Folgenden als D bezeichnet).

Die Matrix *D* ist gegeben durch:

$$D = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$$

D repräsentiert das Polynom *d(x)*, das sich aus der folgenden Bedingung ergibt:

$c(x) \otimes d(x) = ´01´$.

Die inverse Funktion von „*ShiftRow*“ entspricht einer Rotation nach rechts um die entsprechende Anzahl an Positionen für die jeweilige Zeile der Matrix *T*.

Zur Invertierung der Funktion „*ByteSub*“ müssen die inversen S-Boxen gebildet werden. Dazu muss zunächst die Inverse der affinen Transformation über GF(2) und anschließend auch die multiplikative Inverse über $GF(2^8)$ gebildet werden.

Zu Beginn des Algorithmus und in jeder Runde wird eine Teilschlüsselmatrix *K* der Größe 4x*Nb* benötigt. Jeder Teilschlüsseleintrag ist 4 Byte oder 32 Bit lang. Mit der Rundenzahl *Nr* ergibt sich so eine Gesamtlänge des Teilschlüssels von $4 \cdot Nb \times (Nr + 1)$ Byte. Für den Fall, dass die Blocklänge und die Schlüssellänge 128 Bit betragen und 10 Runden des Algorithmus durchlaufen werden, ergibt sich also der benötigte Gesamtschlüssel von 176 Byte oder 1408 Bit.

Die Länge *Nk* des geheimen Schlüssels wird in Byte geteilt durch vier angegeben. Bei einer Schlüssellänge von 128 Bit ist *Nk* = 4. Die ersten Teilschlüssel werden durch Kopieren des geheimen Schlüssels gesetzt. Ist der geheime Schlüssel ausgeschöpft, werden die weiteren Teilschlüssel aus einer XOR-Verknüpfung des vorangegangenen Teilschlüssels und des Teilschlüssels, der *Nk* Positionen zurück liegt, gesetzt. Ist die Nummer *i* des zu erzeugenden Teilschlüssels ein Vielfaches von *Nk*, so wird der vorangegangene Teilschlüssel vor der XOR-Verknüpfung einer Rotation und einer Substitution mit den oben definierten Funktionen unterzogen. Außerdem wird der Teilschlüssel mit einer Rundenkonstanten XOR-verknüpft, die dem Polynom x^{j-1}, mit $j = i \div Nk$, entspricht. Zudem wird bei Schlüssellängen über 192 Bit der vorangegangene Teilschlüssel einer Substitution unterzogen, falls für die Nummer *i* des zu erzeugenden Teilschlüssels gilt, dass *(i – 4)* ein Vielfaches von *Nk* ist.

Die so erzeugten Teilschlüssel werden in den einzelnen Runden nacheinander genutzt. Hierbei bestimmt die Blocklänge, wie viele der 32-Bit-Teilschlüssel benötigt werden.

7.1.2 Betriebsmodi des AES-Algorithmus

Die unterschiedlichen Betriebsarten bei den Blockchiffren (AES inbegriffen) verschlüsseln Klartexte, die länger als die Blocklänge des jeweiligen Chiffrierverfahrens sind. Wie bereits erwähnt, verschlüsselt AES nur Blöcke von jeweils 128 Bit, obwohl der ursprüngliche Algorithmus auch größere Blöcke unterstützt. Neben den klassischen Betriebsmodi für Blockchiffren (wie Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB) oder Message Authentication Codes (MAC)) werden auch einige neue Vorschläge für weitere Betriebsarten unter den Gesichtspunkten Sicherheit, Fehlertoleranz, Synchronisationseigenschaften und Implementierbarkeit diskutiert und teilweise bereits standardisiert (wie z.B. XST-AES (XEX - based Tweaked CodeBook mode (TCB) with CipherText Stealing (CTS)), was in der aktuellen Version von TrueCrypt umgesetzt ist). Die neuen Betriebsmodi bieten zusätzlichen Integritätsschutz oder setzen AES als Schlüsselstromgenerator ein [Sta08].

7.1.3 AES – kryptographische Stärke und Kryptoanalyse

Wie man aus [Wil04] entnehmen kann, könnte bei nur 6 Runden unter Verwendung von $6*2^{32}$ ausgewählten Klartextblöcken mittels 2^{44} komplexer Operationen (d. h. ca. 17 Billionen) der Schlüssel berechnet werden. Das bedeutet, dass etwa 400 GB vom Angreifer vorgegebener Klartext verschlüsselt und analysiert werden muss. Wenn eine komplexe Operation eine Mikrosekunde dauert, werden dazu rund 200 Tage benötigt, um den Schlüssel zu ermitteln.

Bei 7 Runden sind fast 2^{128} ausgewählte Klartexte (entsprechend ca. $5*10^{39}$ Byte) und ein Rechenaufwand von 2^{120} notwendig. D.h. dass bei 1 Nanosekunde pro Operation $4*10^{19}$ Jahre (40 Trillionen) benötigt werden, um den Schlüssel herauszufinden.

Es ist zu betonen, welcher große Unterschied im Sicherheitsniveau durch das Hinzufügen einer 7. Runde erreicht wird. Rijndael führt jedoch mindestens 10 Runden durch (bei Block- und Schlüssellänge von 128 Bit) (siehe Spezifikation des Standards durch NIST [aes01]).

Trotzdem ist zu beachten, dass bei allen praktischen kryptografischen Verfahren die Sicherheit nicht bewiesen werden kann. Es kann höchstens untersucht werden, ob es gegen alle bisher bekannten Angriffsmethoden resistent ist.

Bereits bei dem Entwurf, wurde der Algorithmus gegen alle bekannten Attacken getestet, so dass ein Angriff mit allen herkömmlichen Verfahren nicht effizienter sein sollte als ein Brute-Force-Angriff. Bei AES ergibt sich einen Schlüsselraum von 3,4 x 10^{38}; 6,2 x 10^{57} bzw. 1,1 x 10^{77} Schlüssel je nach Schlüssellänge – 128, 192 bzw. 256Bit. Gäbe es eine Maschine, die den ganzen DES-Schlüsselraum in einer Sekunde durchsucht, dann würde es bei Rijndael ungefähr 149 000 Milliarden Jahre[13] dauern (vgl. [Wil04]). AES erwies sich als resistent gegen alle möglichen Angriffe. Implementierungen von Rijndael können im Vergleich zu den anderen Kandidaten mit dem geringsten Aufwand gegen Angriffe geschützt werden, die auf Messungen von Änderungen der Stromaufnahme beruhen (sog. Power Analysis-Attacken).

Fergusion, Schroeppel und Whiting stellen den Rijndael-Algorithmus in [NF01] als geschlossene Formel dar, die aus 2^{50} Termen besteht, d.h. etwa einer Billiarde Summanden. Obwohl kein anderes als sicher geltendes Verschlüsselungsverfahren in solch einer einfachen Form dargestellt werden konnte, existiert bis heute noch kein sinnvoller Angriff auf AES.

Ein Qualitätssprung war jedoch die Arbeit der Mathematiker Courtois und Pieprzyk, die ganze Klassen von Chiffrierungen mittels sehr großer Systeme quadratischer Gleichungen beschrieben (z.B. 128-Bit-AES als System von 8000 Gleichungen mit 1600 Variablen [Wil04]). Der Rechenaufwand wird stark durch die so genannte XSL-Methode reduziert. Dabei wird ausgenutzt, dass die Gleichungssysteme mehr Gleichungen als Unbekannte enthalten, die meisten Koeffizienten Null sind und dass sie eine besonders reguläre Struktur besitzen. Somit scheint nach [Wil04] einen Angriff auf AES mit 2^{100} Rechenoperationen als möglich.

Aktuell wurde ein erfolgreicher, aber immer noch impraktikabler Angriff auf den Algorithmus veröffentlicht (siehe [aes11]), der die Schlüssellänge effektiv um 2

[13] Zum Vergleich existiert unser Universum seit weniger als 20 Milliarden Jahren!

Bitstellen verkürzt (von 128Bit auf 126Bit bzw. von 256 Bit auf 254Bit). Mithilfe von einem Cluster bestehend aus 1 Billion Rechnern, die jeweils 1 Billion Schlüssel pro Sekunde durchprobieren, würde er bei einem 128 Bit langem Schlüssel etwa 10 Millionen Jahre rechnen. Mit dem um 2 Bits verkürzten Schlüssel konnte die Dauer bei denselben Bedingungen auf knapp 3 Millionen Jahre reduziert werden.

Trotzdem gilt AES weiterhin als sicher! Es gibt immer noch keine bekannten Angriffe, die den Algorithmus erfolgreich in einer realistischen Zeit brechen können bzw. gebrochen haben. Die beschriebenen Attacken sind eher theoretischer Natur und konnten bislang praktisch nicht umgesetzt werden. Es muss jedoch der aktuelle Sicherheitsstand des Algorithmus weiterhin verfolgt werden, um eventuelle neuentdeckte Sicherheitslücken zu berücksichtigen und sie möglichst schnell und effektiv zu beheben.

7.1.4 Bewertung und Ausblick

Rijndael gehörte zu den Kandidaten des AES-Wettbewerbs, die laut [Sta08] die schnellsten Implementierungen erlauben. Weiterhin zeichnet sich der Algorithmus insbesondere durch eine gleichmäßig gute Leistung über alle betrachteten Plattformen (z.B. 32-Bit Prozessoren, 8-Bit Mikrocontroller, die derzeit weitverbreitet in Chipkarten eingesetzt werden) und gute Implementierbarkeit in die Hardware aus. Rijndael bietet die schnellste Erzeugung von Rundenschlüsseln im Vergleich zu allen anderen Kandidaten.

Weitere Vorteile des Algorithmus werden bezüglich des Speicherbedarfs ersichtlich. Rijndael benötigt sehr geringe Ressourcen an RAM- und ROM-Speicher und ist damit hervorragend für den Einsatz in Umgebungen mit beschränkten Ressourcen geeignet (siehe [Sta08]).

Der Rijndael-Algorithmus wurde in einem offenen und sehr transparenten Prozess zum Standard ausgewählt. Dabei konnten auch unabhängige Sicherheitsexperten die kryptografischen Stärken des Verfahrens testen und sich von der Robustheit des Algorithmus gegen alle bekannten Angriffe überzeugen. Trotz den in den letzten Jahren

entdeckten theoretischen Schwächen des AES-Standards sind bis heute noch keine praktisch umsetzbaren Angriffe dagegen bekannt.

AES hat in den vergangenen Jahren sehr viel an Akzeptanz gewonnen und wird in vielen Soft- und Hardwareprodukten, wie z.B. PGP, TrueCrypt, SSH, IBM zSeries 990, Microsoft .NET, IBM WebSphere J2EE, Intel & AMD Prozessoren der neuen Generation (z.B. i7-980X Extreme Edition von Intel) mit integrierter Verschlüsselungsbeschleunigung in Form der *AES New Instructions* (AES-NI) eingesetzt.

8 TrueCrypt 7.0a

In diesem Abschnitt wird das kostenlose Open Source Programm TrueCrypt behandelt. Neben einem ausführlichen Überblick über die Funktionen, Möglichkeiten und Grenzen des Produkts, wird TrueCrypt systematisch nach den festgelegten Vergleichskriterien und unter Beachtung der vorgestellten Randbedingungen untersucht. Abschließend werden die Ergebnisse zusammengefasst und für die Zwecke der vorliegenden Arbeit ausgewertet.

Die Beschreibung des Aufbaus des Produkts und seiner Einzelteile wurde aus der TrueCrypt-Dokumentation entnommen und entsprechend bearbeitet (siehe [tru11]).

8.1 Übersicht – Funktionsumfang

Die im September 2010 veröffentlichte Neuversion (v. 7.0a) des TrueCrypt bietet eine breite Palette an Funktionalitäten, die zum sicheren Verschlüsseln von einzelnen Daten, Verzeichnissen, ganzen Partitionen (auch der Systempartition) und externer Speichermedien (z.B. USB-Sticks, externe Festplatten o.Ä.) dienen. Die wichtigsten implementierten Merkmale des Produkts sind:

- Das Erstellen und Verwalten von verschlüsselten Daten-Containern, die sich wie reale Datenträger verhalten, sobald sie in TrueCrypt eingebunden werden.
- Das Verschlüsseln und Verwalten von ganzen Partitionen oder externen Datenträgern, wie USB-Sticks und externen Festplatten.
- Das Verschlüsseln und Verwalten von Systempartitionen mit installiertem Windows (zurzeit unterstützt TrueCrypt eine Systemverschlüsselung nur bei diesem Betriebssystem). Weiterhin werden auch Systeme unterstützt, die mehr als ein installiertes Betriebssystem haben.
- Die Verschlüsselung wird von TrueCrypt „on-the-fly“ realisiert. „On-the-fly“-Verschlüsselung bedeutet dabei, dass die Daten genau in dem Moment

automatisch verschlüsselt bzw. entschlüsselt werden, in dem sie geladen bzw. gespeichert werden.

- Daten können durch Prozessorparallelisierung (Mehrkernprozessor) und Pipelining genauso schnell gelesen bzw. geschrieben werden, wie bei einem unverschlüsselten Laufwerk.

- Die AES-Verschlüsselung kann hardwarebedingt auf modernen Prozessoren beschleunigt werden durch den so genannten AES instruction set (AES-NI).

- Verschlüsselung von Solid State Drives wird unterstützt.

- TrueCrypt bietet die einzigartige Möglichkeit ein verstecktes Laufwerk bzw. ein verstecktes Betriebssystem zu erstellen, deren Existenz nicht nachweisbar sein sollte (vorausgesetzt, dass gewisse Richtlinien eingehalten werden).

- TrueCrypt bietet die Verschlüsselungsalgorithmen AES, Twofish und Serpent, sowie verschiedene Konkatenationen der einzelnen Algorithmen zur Auswahl. Die kombinierte Nutzung der Algorithmen gewährleistet zwar eine höhere Sicherheit (um an die Daten zu kommen, muss der Angreifer alle an der Verschlüsselung beteiligten Algorithmen brechen), ist aber mit großen Geschwindigkeitsverlusten bei der Ver- bzw. Entschlüsselung der Daten verbunden. Die Entscheidung, welcher Algorithmus zu nehmen ist, wird durch die in TrueCrypt integrierte Benchmark unterstützt. Dabei werden für eine bestimmte Dateigröße die Geschwindigkeiten bei der Ver- bzw. Entschlüsselung für die unterschiedlichen Verschlüsselungsmöglichkeiten ermittelt. Abbildung 7 zeigt die Benchmark am Beispiel von 5 MB Datengröße. Dabei ist deutlich zu sehen, dass eine Ver- bzw. Entschlüsselung mit AES mehr als dreifach schneller ist als die Kaskade AES-Twofish-Serpent.

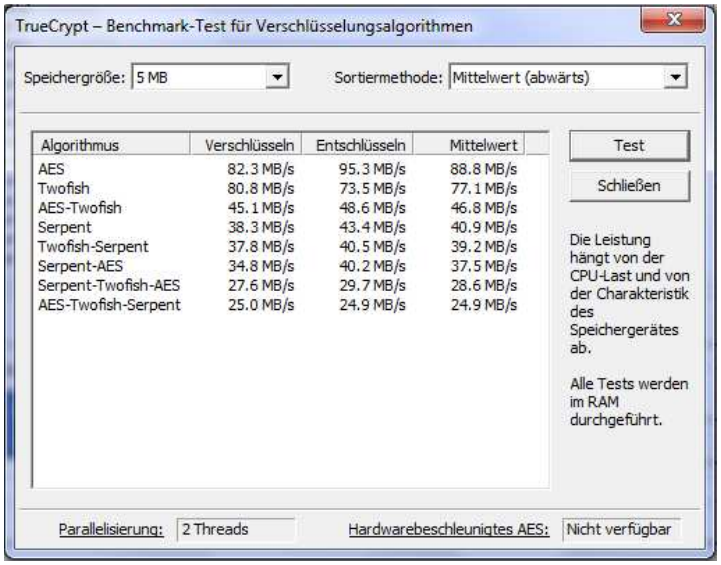


Abbildung 7. TrueCrypt-Test für Verschlüsselungsalgorithmen

- Zusätzliche Sicherheit wird durch die in TrueCrypt eingebetteten Hash-Algorithmen erreicht, die als Mischfunktionen genutzt werden. Diese sind RIPEMD-160, SHA-512 und Whirlpool. Bei einer vollständigen Festplattenverschlüsselung (inklusive der Systempartition) steht dem Benutzer nur RIPEMD-160 zur Verfügung.

Für den weiteren Verlauf sind hauptsächlich die Funktionalitäten von Interesse, die mit der gesamten Festplattenverschlüsselung[14] (inklusive Systempartition) oder mit dem Verschlüsseln und Verwalten von Wechselmedien verbunden sind. Das Betrachten und Testen aller in dem Programm integrierten Features würde sowohl den zeitlichen Rahmen der vorliegenden Arbeit sprengen, als auch die Aufgabenspezifikation verfehlen. Für weitere Details bezüglich der nicht behandelten Themenbereiche wird auf die offizielle Seite und die Dokumentation von TrueCrypt verwiesen (siehe [tru11]).

8.2 Installation

TrueCrypt kann direkt auf dem Rechner installiert werden oder im stand-alone-Modus aus einem Ordner oder von einem beliebigen Wechselmedium aus im so genannten

[14] Im weiteren Verlauf der Arbeit auch als Systemverschlüsselung bezeichnet.

„portable mode“ ausgeführt werden , falls keine Systemverschlüsselung beabsichtigt wird. Für die Untersuchungen, die in diesem Abschnitt durchgeführt werden, wurde True Crypt auf einem der Test-Computer installiert. Abbildung 8 zeigt das Optionsmenü beim Start der Installation.

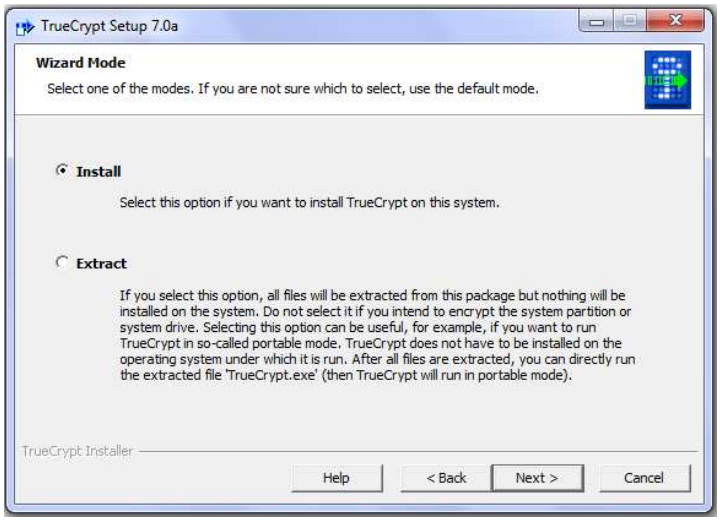


Abbildung 8. True Crypt 7.0a : Installationsvorgang

Die Installation verläuft standardmäßig, benötigt sehr wenig Speicherplatz (Installationspaket ist gerade mal 3,32 MB groß und die installierte Software beansprucht ca. 8 MB auf der Festplatte) und ist mit kaum spürbarem Zeitaufwand (im Sekundenbereich) verbunden. Der Installationsvorgang erfolgt nur in Englischer Sprache. Sobald das Produkt installiert ist, können Sprachpakete von Drittanbietern heruntergeladen werden (unter Settings → Language → Download Language Pack). Dabei ist das deutsche Sprachpaket eines der wenigen, die eine vollständige Übersetzung des GUI der aktuellen TrueCrypt-Version anbieten. TrueCrypt leitet direkt zur Seite mit den Sprachpaketen weiter. Das gewünschte Sprachpaket muss nur dem Ordner hinzugefügt werden, wo TrueCrypt installiert ist und kann sofort eingesetzt werden. Die Übersetzung gilt jedoch nicht für den Bootloader (Pre-Boot-Authentifikationsbildschirmanzeige), der nur auf Englisch angezeigt werden kann.

8.3 Systemverschlüsselung

Im Folgenden wird die Vorgehensweise vorgestellt, die zu einer Systemverschlüsselung der dafür vorgesehenen Testumgebung mittels TrueCrypt führt (im Anhang A: befinden sich die zu den Systemverschlüsselungsschritten korrespondierenden Screenshots von TrueCrypt).

Die Systemverschlüsselung erfolgt mittels eines Assistenten, der den gesamten Vorgang sehr vereinfacht. Als erstes wurde das gesamte Laufwerk als Ziel der Verschlüsselung angegeben. Die Software bietet im weiteren Einstellungsverlauf unter Anderem auch Option zur Verschlüsselung der Host-Umgebung an, die, bedingt durch die Testumgebung, nicht eingesetzt wurde.

Weiterhin wurde der AES-256 als Verschlüsselungsalgorithmus ausgewählt, der als Vergleichskriterium der untersuchten FDE-Lösungen (siehe Abschnitt 7) dient. Er ermöglicht eine einfache Implementierung, die eine schnelle Verschlüsselung bzw. Entschlüsselung zur Folge hat.

Im nächsten Schritt wurde das Kennwort für die Pre-Boot-Authentifikation festgelegt. Dabei ist prinzipiell eine Mindestlänge von 8 Zeichen zu beachten, da kürzere Passwörter sehr anfällig für Brute-Force Angriffe sind – je länger und zufälliger das Passwort ist, desto höher ist das Sicherheitsniveau. Für die Testverschlüsselung wurde das Kennwort „GasMDC_12“ ausgewählt. TrueCrypt gab eine Warnung aus, dass das Kennwort zu kurz und damit unsicher sei. Die Meldung wurde jedoch ignoriert, da die Kennwortstärke für die durchgeführten Untersuchungen ausreichte. Wichtig dabei ist, dass diese Zeichenkombination auf dem Testrechner noch nicht genutzt wurde!

Dadurch, dass keine „echten“ Zufallsgeneratoren existieren, werden im nächsten Schritt Zufallsdaten durch Mausbewegungen gesammelt, um den Zufallsfaktor zu erhöhen. Somit wurden die benötigten Schlüssel endgültig erzeugt und dem Benutzer angezeigt (falls gewünscht).

Eine in dem Produkt eingebaute Sicherheitsmaßnahme vor dem Start der tatsächlichen Systemverschlüsselung ist das Erstellen einer Rettungsdatenträger-CD (zur

Systemwiederherstellung – siehe Abschnitt 8.3.1.2), die bei dem Einstellungsverlauf lokal gespeichert und auf einer CD gebrannt wurde. Anschließend musste die CD vom Verschlüsselungsassistenten verifiziert werden.

TrueCrypt führte einen Pre-Test durch, damit sichergestellt wird, dass alle Optionen richtig ausgewählt sind und die Systemverschlüsselung ohne Hindernisse durchgeführt werden kann. Dabei wurde der Rechner neu gestartet und vor dem Boot-Vorgang (Pre-Boot-Authentifikation) das festgelegte Kennwort verlangt. Es wurde absichtlich eine Anmeldung mit einem falschen Kennwort versucht, die zu einer Fehlermeldung führte. Mit der Eingabe des richtigen Passworts startete der Boot-Vorgang standardmäßig.

Bemerkung: Die Windows Authentifikation und die Pre-Boot-Authentifikation von TrueCrypt können nicht verbunden werden – also muss man sich zusätzlich mit dem Firmenlogin anmelden (nach dem Betriebssystemstart).

Nach der erfolgreichen Anmeldung wurde der Pre-Test von TrueCrypt als erfolgreich gemeldet und die Verschlüsselung des Systems gestartet.

Der Verschlüsselungsvorgang kann auch unterbrochen und später wieder fortgesetzt werden. Man kann theoretisch auch während der Verschlüsselung ganz normal an dem Rechner arbeiten, wobei Geschwindigkeitseinbußen durch die CPU-Auslastung möglich sind. Um die Dauer der Verschlüsselung realistisch messen zu können, wurde der Rechner während des Prozesses jedoch nicht anderweitig genutzt. Für die gesamte Festplatte (80 GB) hat TrueCrypt ca. 60 Minuten benötigt. Nach dem erfolgreichen Verschlüsseln des Systems wurde eine Bestätigungsmeldung angezeigt und damit ist der Prozess abgeschlossen.

8.3.1 Weitere Testergebnisse auf dem mit TrueCrypt verschlüsselten System

8.3.1.1 Datenspuren auf der verschlüsselten Festplatte

In diesem Abschnitt wird ein Test präsentiert, der die verschlüsselte Festplatte nach konkreten sensiblen Daten durchsucht. Durch fehlende technischen Voraussetzungen,

konnte der Test nicht im Rahmen der vorliegenden Arbeit durchgeführt werden und wird nach [tce11] beschrieben.

Nach dem Herunterfahren von einem mit TrueCrypt verschlüsselten Rechner wird die Festplatte ausgebaut und von ihr mit Hilfe des forensischen Werkzeugs EnCase 4.22a ein forensisches Abbild erstellt.

Nach der Untersuchung des ersten Sektors der Festplatte (die ersten 512 Bytes) wurde ein abweichender Bootvorgang festgestellt. In den ersten 521 Bytes konnte eindeutig der TrueCrypt Boot-Loader erkannt werden[15]. Der Rest der Festplatte wird als eine Sammlung von „nicht zugewiesenen Clustern“ („Unallocated Cluster“) von dem EnCase-Programm diagnostiziert. Das bedeutet, dass die verschlüsselten Dateien nicht als solche erkannt werden. Mit anderen Worten wird ein Angreifer die Festplatte als leer oder als mit zufälligen Daten gefüllt erkennen.

Weiterhin wurde das Abbild der physischen Festplatte nach bestimmten Inhalten durchsucht, die verschlüsselt auf der Festplatte vorhanden sind. Es wurde konkret nach dem Inhalt einer Text-Datei – „This_is_test_data“, sowie kleinere Teile davon, wie „This_is“ gesucht. Weiterhin wurde auf Übereinstimmungen mit dem Kennwort für die Pre-Boot-Authentifikation (in diesem Fall „ThreeBY16“) geprüft. Keine der angegebenen Zeichenketten konnte auf der Festplatte wiedererkannt werden.

8.3.1.2 Wiederherstellung verschlüsselter Daten

Für die Zwecke der vorliegenden Arbeit ist das Wiederherstellen von verschlüsselten Daten bei einer Systemlaufwerkverschlüsselung mit der Rettungsdatenträger-CD von besonderem Interesse. Andere Back-up- Vorgänge sind entweder vom Nutzer selbst oder vom Administrator (falls es sich um eine Unternehmensumgebung handelt) zu verwalten und werden hier nicht weiter behandelt.

Der Rettungsdatenträger wird bei der Vorbereitung der Verschlüsselung der System-Partition bzw. des Laufwerks erstellt (siehe Abschnitt 8.3) und soll das System vor kritischen Fehlern schützen, wie zum Beispiel:

[15] Diese Tatsache wird auch in der Dokumentation von TrueCrypt angegeben.

- Ausfall des TrueCrypt-Boot-Loaders beim Systemstart;
- Beschädigung des Master-Key oder anderer kritischen Daten ;
- Windows ist beschädigt und kann nicht gestartet werden;

Der Rettungsdatenträger-CD kann als TrueCrypt-Boot-Loader genutzt werden und ist nur in Zusammenhang mit dem Passwort verwendbar, das bei der Erstellung der Rettungs-CD für die Pre-Boot-Authentifikation festgelegt wurde. Falls man das Kennwort geändert hat oder die Rettungs-CD beschädigt wird bzw. verloren geht, kann jederzeit eine neue CD erstellt werden.

Das Erstellen und Anwenden der Rettungsdatenträger-CD für den Boot-Vorgang wurde durchgeführt und ist auf dem Testrechner reibungslos und nach den vom Anbieter gemachten Angaben verlaufen.

8.3.1.3 Administration von TrueCrypt

TrueCrypt bietet keine zentrale Verwaltung an und somit fehlen viele Funktionen, die für den Unternehmenseinsatz von essentieller Bedeutung sind, wie zum Beispiel Passwortwiederherstellung, Verwaltung und Überwachung der verschlüsselten Rechner, Einbindung der bestehenden Active Directory des Unternehmens, Nutzung von Smart Cards für die Pre-Boot-Authentifikation oder als zusätzliche Sicherung des Passworts uvm.

Trotzdem kann TrueCrypt für die Verschlüsselung einer geringeren Anzahl[16] von mobilen Endgeräten (Laptops) so angepasst werden, dass es für ein kleines Unternehmen bzw. eine kleine Einrichtung eine ausreichende FDE-Lösung bietet. Dabei kann höchstens folgendes Niveau an Administrierbarkeit erreicht werden:

Der Administrator installiert TrueCrypt auf den zu verschlüsselnden Rechnern. Die gesamten Laufwerke der ausgewählten Geräte werden vom Administrator mittels TrueCrypt einzeln verschlüsselt. Es werden Rettungsdatenträger-CDs von allen PCs erstellt und zusammen mit den jeweiligen Passwörtern sicher aufbewahrt.

[16] Eine Anzahl von bis zu 10 Geräten wird als realistisch empfunden.

Der Endnutzer kann bei der ersten Nutzung des mobilen Endgerätes das Passwort für die Pre-Boot-Authentifikation ändern, jedoch nur unter Aufsicht des Administrators (für Passwortänderung werden Administratorrechte verlangt). Danach kann der Administrator mit der ersten Rettungsdatenträger-CD und dem ersten Passwort immer auf den Rechner zugreifen, falls der Benutzer sein Passwort verliert bzw. vergisst. Der Endnutzer kann Daten auf dem verschlüsselten System lesen, speichern und verändern. Er hat aber keine Rechte das verschlüsselte Laufwerk zu entschlüsseln bzw. zu formatieren, das Passwort zu verändern oder TrueCrypt zu deinstallieren (Für weitere Einschränkungen der Nutzer ohne Administratorrechte wird auf der Dokumentation des Produkts verwiesen [tru11]).

Dieses Modell birgt jedoch diverse Gefahren, wie zum Bespiel die Tatsache, dass der Administrator jederzeit Zugriff auf den verschlüsselten Rechner und somit auf den gesamten Inhalt besitzt.

8.3.1.4 Ressourcenbelegung

Es wurden mehrere Messungen zum Ermitteln der CPU- und RAM- Belastung, sowie der Kopier-, Schreib-, Lesezugriffsgeschwindigkeit bzw. –zugriffszeit für verschiedene Dateigrößen auf dem mit TrueCrypt verschlüsselten Testrechner durchgeführt. Ziel der Messungen war, diese Größen bei den mit den unterschiedlichen FDE-Lösungen verschlüsselten Rechnern sowie einem unverschlüsselten Testsystem zu vergleichen. Details über die durchgeführten Messungen, die Ergebnisse und ihre Auswertung werden in Abschnitt 12 betrachtet.

8.3.1.5 System-Partition/ Laufwerk dauerhaft entschlüsseln

Dieser Test hat das Ziel, den Vorgang der vollständigen Entschlüsselung des Systems zu prüfen.

Nachdem die Entschlüsselung (unter System → „System-Partition/ Laufwerk dauerhaft entschlüsseln“) durchgeführt wurde, wurde das System neu gestartet und auf den Normalzustand ohne Pre-Boot-Authentifikation zurückgestellt. Der Zeitaufwand für die Entschlüsselung ist mit dem für die Verschlüsselung vergleichbar. Der Prozess verläuft

im Hintergrund, automatisch und unkompliziert. Dabei kann der Nutzer während des Entschlüsselungsvorgangs weiter an dem Rechner arbeiten, wobei Verzögerungen[17] bei Anwendungen mit großer CPU-Belastung zu erwarten sind.

8.4 Verschlüsselung von Wechselmedien

In diesem Abschnitt wird die Verschlüsselung von Wechselmedien (wie USB-Sticks und externen Festplatten) mittels TrueCrypt vorgestellt und untersucht.

Im Folgenden wird die Vorgehensweise betrachtet, die zur vollständigen Verschlüsselung eines USB-Sticks mit 2 GB Speicherplatz führte (die Vorgehensweise bei einer externen Festplatte oder einer lokalen Nicht-Systempartition ist identisch).

Es wurde das zu verschlüsselnde Speichermedium mittels des TrueCrypt-Assistenten ausgewählt. Weiterhin wurde die Formatierung des USB-Sticks durchgeführt, wobei zu beachten ist, dass nur das NTFS-Dateisystem unterstützt wird. Eine „in-place"-Verschlüsselung ist erst ab Windows Vista vorhanden und konnte somit nicht untersucht werden.

Im weiteren Verlauf der Verschlüsselungseinrichtung wurden Verschlüsselungs- und Hashalgorithmus festgelegt: AES-256 und RIPEMD-160.

Im nächsten Schritt wurde das Kennwort für den Wechseldatenträger festgelegt. Dabei ist eine Mindestlänge von 8 Zeichen zu beachten, da kürzere Passwörter sehr anfällig für Brute-Force Angriffe sind – je länger und zufälliger das Passwort ist, desto höher ist das Sicherheitsniveau. Für die Testverschlüsselung wurde das Kennwort „Gud_FDE31" ausgewählt. TrueCrypt gab eine Warnung aus, dass das Kennwort zu kurz und damit unsicher sei. Die Meldung wurde jedoch ignoriert, da die Kennwortstärke für die durchgeführten Untersuchungen ausreichte. Wichtig dabei ist, dass diese Zeichenkombination auf dem Testrechner noch nicht genutzt wurde!

Anschließend wurden Zufallsdaten gesammelt (analog zu der Systemverschlüsselung siehe Abschnitt 8.3) und den Formatierungs- und Verschlüsselungsvorgang gestartet.

[17] Die Verzögerung der Arbeitsprozesse während der Ver- bzw. Entschlüsselung des Systems wurde nicht getestet, damit der Zeitaufwand für die beiden Vorgänge nicht beeinflusst wird.

Nach erfolgreichem Verschlüsseln des USB-Sticks wurde eine Warnung von TrueCrypt angezeigt, dass sich der Laufwerkbuchstabe, mit dem das Laufwerk vom Betriebssystem identifiziert wird, von dem Laufwerkbuchstaben unterscheidet, der zum Anbinden des Laufwerks über TrueCrypt genutzt wird.

Der USB-Stick wurde von dem Computer entfernt, erneut angeschlossen und bekam wieder „Laufwerk G:“ vom System zugeordnet. Beim Versuch, den USB-Stick (G:) über den Windows Explorer zu öffnen, erscheint folgende Meldung:

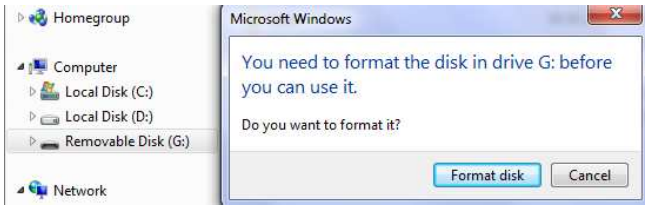


Abbildung 9. TrueCrypt Datenträger wird von Windows als nicht formatiert erkannt

Wenn man hier auf „Format disk“ drückt, wird das Speichermedium formatiert und somit die Verschlüsselung von TrueCrypt aufgehoben.

Der verschlüsselte USB-Stick wird dann von TrueCrypt eingebunden und dabei das festgelegte Passwort verlangt. TrueCrypt ordnet dem verschlüsselten Laufwerk einen anderen Laufwerkbuchstaben zu – in diesem Fall „M:“. Im Windows Explorer wird „M:“ als lokales Laufwerk hinzugefügt. Die Struktur sieht folgendermaßen aus:

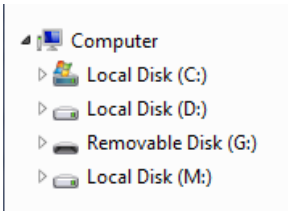


Abbildung 10. Laufwerkstruktur nach dem Einbinden von Laufwerk G: mittels TrueCrypt

Ein Zugriff auf den Wechseldatenträger über „G:“ ist weiterhin nicht möglich. Auf die entschlüsselten Daten wird über das lokale Volume „M:“ zugegriffen.

Bemerkung: Beim Versuch, ein nicht mit TrueCrypt verschlüsseltes Laufwerk an TrueCrypt einzubinden oder ein falsches Passwort beim Einbinden einzugeben, kann ein potenzieller Angreifer keine Informationen gewinnen. TrueCrypt zeigt in beiden Fällen eine Fehlermeldung, dass das Volume *entweder* kein TrueCrypt Volume ist *oder* das Passwort falsch ist.

8.4.1 Datenspuren auf verschlüsselten Wechseldatenträgern

Es wurde eine Text-Datei auf dem verschlüsselten Wechseldatenträger mit dem Namen „Test.txt“ und dem Inhalt – „Das ist eine Testdatei“ erstellt. Anschließend wurde der USB-Stick von dem Rechner entfernt und neu eingesteckt. Bevor das Laufwerk durch TrueCrypt eingebunden wurde, wurde der Inhalt des Datenträgers (auf Laufwerk „G:“) mit Hilfe des Programms WinHex[18] 16.1 nach der Textdatei, sowie nach Zeichenketten, die den Namen der Datei, den Inhalt oder Teile davon (wie z.B. „Das ist“) durchsucht. Alle Tests hatten keine Treffer zur Folge. Weiterhin wurde das verschlüsselte Speichermedium nach Hinweise für die Benutzung von TrueCrypt untersucht und es konnten ebenfalls keine Informationen darüber gefunden werden.

Als Nächstes wurde der USB-Stick durch TrueCrypt eingebunden und die Test mit WinHex wiederholt (auf Laufwerk „M:“). In diesem Fall konnte, wie erwartet, die Datei und ihr Inhalt anhand der angegebenen Zeichenketten gefunden werden.

Der USB-Stick wurde danach von TrueCrypt getrennt und von Windows formatiert. Die Tests wurden erneut wiederholt und führten zu negativen Ergebnissen – es konnten keine Datenspuren und keine Hinweise für die Benutzung von TrueCrypt nachgewiesen werden.

8.4.2 Portable mode

Es ist in bestimmten Situationen unbequem bzw. nicht möglich, TrueCrypt auf einem verfügbaren, anderen Rechner zu installieren, um die Daten eines verschlüsselten Wechselmediums zu verwalten. Dazu bietet TrueCrypt den so genannten „portable

[18] Seite des Produkts: http://www.x-ways.net/winhex/index-d.html

mode“ an. In diesem Modus muss die Anwendungssoftware nicht installiert werden. Es gibt zwei Möglichkeiten, TrueCrypt in diesem Modus zu starten:

- Nach dem Entpacken des TrueCrypt-Ordners kann direkt die ausführbare Datei TrueCrypt.exe gestartet werden. Es wird das gleiche GUI und der volle Funktionsumfang des Produkts angeboten. Diese Option wurde in Rahmen der vorliegenden Arbeit getestet und funktioniert intuitiv und einwandfrei.

- Es kann eine Traveler Disk erstellt werden, um das Programm von dort auszuführen („Extras“ →“Traveler Disk Installation“). Es können dabei weitere Konfigurationen vorgenommen werden. Diese Option wurde nicht getestet, weil sie über den thematischen Rahmen der vorliegenden Arbeit hinausgeht. Weitere Details darüber können aus [tru11] entnommen werden.

8.4.3 Entschlüsselung von Wechselmedien bzw. Nicht-Systempartitionen

TrueCrypt bietet keine Möglichkeit den verschlüsselten Wechseldatenträger bzw. Nicht-Systempartitionen „in-place“ zu entschlüsseln. Die einzige Möglichkeit besteht darin, die Daten auf einen nicht verschlüsselten Speicherbereich bzw. -medium zu kopieren (und somit zu entschlüsseln) und die zu entschlüsselnden Speichermedien zu formatieren.

8.5 Zusammenfassung

Der getestete Funktionsumfang von TrueCrypt hat die Angaben des Anbieters bestätigt. Es konnten keine zusätzlichen Sicherheitsmängel gefunden werden. Das Produkt bietet zusätzlich eine ausführliche Dokumentation (siehe [tru11]), eine starke Community[19] und wird ständig von unabhängigen Wissenschaftlern nach Sicherheitslücken untersucht.

[19] Es können viele zusätzliche Materialien (Tutorials, Videos usw.) gefunden werden, die von Privatpersonen zur Verfügung gestellt werden und sich mit den verschiedenen Themengebieten, Optionen und Vorgängen des Programms beschäftigen.

Die Installation und die Nutzung von TrueCrypt sind direkt und unkompliziert. Die grafische Oberfläche ist schlicht und übersichtlich gehalten. Die Funktionen des Programms sind leicht zu finden. Durch den „portable mode“ können verschlüsselte Datenträger auf jedem Rechner[20] genutzt werden.

Weitere Vorteile des Produkts sind, dass es keine großen technischen Voraussetzungen erfordert und wenig Speicherplatz benötigt. Es beansprucht zwar mehr CPU-Ressourcen für Schreib-/ Lesezugriffe als ein vergleichbares unverschlüsseltes System (siehe Abschnitt 12.3), dafür ist es aber fast genauso schnell. Im Normalbetrieb wird die Arbeit der Nutzer durch die Verschlüsselung des Systempartition bzw. Wechseldatenträgers nicht bzw. kaum spürbar eingeschränkt. Zusätzlich ist das Produkt kostenlos und Open Source.

Nachteilig ist jedoch das Fehlen einer Zentralverwaltung und einer zuverlässigen technischen Unterstützung für den Einsatz in einer Unternehmensumgebung. Des Weiteren bietet TrueCrypt keine Funktionen wie Verwaltung verschiedener Benutzer-IDs, Kennwortwiederherstellungsstrategien oder Passwortsynchronisation mit Windows Konten.

Zusammenfassend ist TrueCrypt für den privaten Gebrauch empfehlenswert. Mit einem starken Passwort kann der Endnutzer seine Daten sicher aufbewahren und modifizieren. Für einen Unternehmenseinsatz ist das Produkt eher ungeeignet und nur durch einige Sicherheits- und Nutzungseinschränkungen für eine geringe Anzahl von Rechnern anwendbar (siehe Abschnitt 8.3.1.3).

[20] Vorausgesetzt, dass der Benutzer Administratorrechte auf dem jeweiligen Rechner besitzt.

9 PGP Whole Disk Encryption (PGP WDE)

In diesem Abschnitt wird die kommerzielle FDE-Lösung PGP WDE des Sicherheitsunternehmens Symantec betrachtet. Neben einem ausführlichen Überblick über die Funktionen, Möglichkeiten und Grenzen des Produkts, wird es systematisch nach den festgelegten Vergleichskriterien und unter Beachtung der vorgestellten Randbedingungen untersucht. Abschließend werden einige Bemerkungen zum Produkt gemacht und die ermittelten Ergebnisse zusammengefasst.

PGP Whole Disk Encryption wird als Teil des Softwarepakets *PGP Desktop* eingebaut, das neben der vollständigen Festplattenverschlüsselung auch Softwareeinheiten, wie *PGP NetShare* und *PGP Desktop E-Mail* beinhaltet, die für einen umfassenderen und mehrschichtigen Schutz sorgen. Je nach vorhandener Lizenz wird der Zugang zu einem bestimmten Teil der Funktionen von PGP Desktop ermöglicht. Für die Zwecke der vorliegenden Arbeit wird die Untersuchung auf den Funktionsumfang der PGP WDE beschränkt.

Um die PGP WDE - Funktionalität für den Unternehmenseinsatz zu implementieren und die zentrale Verwaltung und Richtliniendurchsetzung zu ermöglichen wird der PGP Universal Server und die dazugehörige Administrationssoftware eingerichtet.

9.1 Übersicht – Funktionsumfang

9.1.1 PGP Universal Server

Die Beschreibung des Aufbaus des Produkts und seiner Einzelteile orientieren sich an dem PGP Universal Server-Datenblatt [pgp11c].

PGP Universal Server in der aktuellen Version 3.1.2 umfasst unter anderem[21] folgende Funktionalitäten:

[21] PGP Universal Server ist ein mächtiges Werkzeug zum Verwalten von mehreren Anwendungen. Aus diesem Grund werden hier nur die wichtigsten und für die zum Thema der vorliegenden Diplomarbeit relevanten Funktionen betrachtet. Für weitere Details wird auf die Dokumentation des Produkts verwiesen (siehe [pgp11d]).

- Eine einzige zentralisierte webbasierte Verwaltungskonsole mehrerer Symantec-Verschlüsselungsanwendungen für alle Clients (siehe Abbildung 11). Dabei können Verschlüsselungsanwendungen jederzeit hinzugefügt bzw. entfernt werden.

Abbildung 11. Zentrale Verwaltung von Verschlüsselungsrichtlinien für mehrere Anwendungen [pgp11c]

- Zentralisierte Richtlinienkonfiguration zur automatisierten Durchsetzung von Benutzer-, Kennwort- und Computerrichtlinien. Z.B. Durchsetzung einer Richtlinie zur automatisierten Verschlüsselung der Client-Festplatte und alle angeschlossenen Wechseldatenträger bei der nächsten Anmeldung des Benutzers oder zum Erstellen eines verschlüsselten Datencontainers mit einer bestimmten Größe auf der Festplatte.

- Berichterstellung und Protokollierung zur Gewährleistung der Richtlinieneinhaltung – z.B. Computerverschlüsselungsstatus, Information über fehlgeschlagene Anmeldungen u. A.

- Erstellen und Verwalten von Administratoren mit unterschiedlichen Verantwortungsbereichen. Mindestens einen SuperUser (Administrator mit vollständiger Rechtezuweisung) muss dafür vorhanden sein.

- PGP Portable – Erstellen von verschlüsselten mobilen passwortgeschützten Ordnern bis einer maximalen Größe von 128 GB, die plattformübergreifend und ohne installierten Software zugreifbar sind.

- Erstellen, Verteilen und Speichern von Verschlüsselungsschlüsseln.

- Automatische Benutzerregistrierung – automatisiertes Verfahren zum Erstellen von Benutzerkonten, zur Verwaltung von Verschlüsselungsschlüssel und zur Richtlinienzuweisung.
- Wiederherstellungsstrategien für Passwörter und verschlüsselte Daten im Unternehmen.
- Integration in das vorhandene Unternehmensverzeichnis.
- Festlegen der Funktionen, die die Benutzer am Client-PC sehen bzw. ausführen können.
- PGP Remote Disable and Destroy mit Intel Auto Theft Technology – Geräte können als gestohlen bzw. verloren von dem Administrator gemeldet und somit gesperrt werden. Diese Option ist mit Soft- und Hardwarevoraussetzungen verbunden, die von der Testumgebung nicht erfüllt sind und wird nicht weiter berücksichtigt.

9.1.2 PGP Whole Disk Encryption

Der Aufbau des Produkts und seine Einzelteile wurden nach den Informationen aus der PGP WDE - Datenblatt beschrieben (siehe [pgp11b]). Die untersuchte PGP WDE ist Teil des Softwarepakets PGP Desktop Enterprise Complete Edition 10.1.2 und umfasst folgende Eigenschaften:

- Verschlüsselung und Verwaltung von dem gesamten System (zurzeit werden Windows, Linux und Mac OS unterstützt), von einzelnen Laufwerken und von externen Speichermedien (z.B. USB-Sticks und externe Festplatten).
- Erstellung von virtuellen verschlüsselten Laufwerken, die mit eigenen Laufwerkbuchstaben initialisiert werden.
- Erstellung von verschlüsselten Zip-Archiven mit der möglichen Konfiguration, dass sie auch unter Systemen (zurzeit wird diese Option nur unter Windows-

Systemen unterstützt) geöffnet werden, auf denen PGP WDE oder PGP Desktop nicht installiert sind.

- Dateien und Ordner vollständig zerstören bzw. freien Speicherplatz auf Laufwerken sicher löschen, so dass sogar mit Datenwiederherstellungssoftware keine Informationen wiederhergestellt werden können.
- Berichte zur Gewährleistung der Richtlinieneinhaltung: Computerverschlüsselungsstatus, Warnhinweise zu fehlgeschlagenen Anmeldung und die Geräteverwaltung.
- Mehrere Pre-Boot-Authentifizierungsoptionen für Windowsbenutzer: Pre-Boot-Smartcard, TPM- und „Single-Sign-On"-Unterstützung.
- Verwaltung von Benutzerschlüsseln.
- Diverse Strategien zur Passwort- und Computerwiederherstellung (werden in Abschnitt 9.3.3 ins Detail betrachtet).
- Als Verschlüsselungsalgorithmus wird nur der Quasistandard AES mit 128-Bit (steht nur in PGP Universal Server zur Auswahl) bzw. 256-Bit Verschlüsselung angeboten. Dabei basiert die Verschlüsselung auf *PGP Hybrid Cryptographic Optimizer*, der laut Anbieter die Leistung des verschlüsselten Systems bis zu 40 % verbessert im Vergleich zur älteren Versionen des Softwareprodukts, schnellere Festplattenzugriffe ermöglicht.
- Unterstützung der AES-NI-Technologie von Intel.
- Verschlüsselung von SSD-Festplatten wird unterstützt.

Für die vorliegende Diplomarbeit sind hauptsächlich die Funktionalitäten von Interesse, die mit der gesamten Systemverschlüsselung oder mit dem Verschlüsseln und Verwalten von Wechselmedien verbunden sind. Das Betrachten und Testen alle weiteren in der Software integrierten Features würde sowohl den zeitlichen Rahmen der vorliegenden Arbeit sprengen, als auch die Aufgabenspezifikation verfehlen. Für

weitere Details bezüglich der nicht behandelten Themenbereiche wird auf die offizielle Seite und die Dokumentation[22] von Symantec verwiesen.

9.2 Installation und Konfigurieren der Verschlüsselung

In diesem Abschnitt werden der Installations- und der Konfigurationsvorgang beim Einrichten der untersuchten Software beschrieben. Dabei werden die Einstellungen und Funktionen von der Server- und Clientseite betrachtet und nicht als PGP Universal Server- und PGP Desktop- bzw. PGP WDE-Funktionalität bezeichnet, weil die für die zentrale Verwaltung benötigten Funktionalitäten der Verschlüsselungssoftware in der Administratorsoftware eingebaut sind.

Das von Symantec für die vorliegende Untersuchung zur Verfügung gestellte Softwarepaket entspricht den aktuellsten und funktionsunbeschränkten Versionen der benötigten Komponenten. Dazu wurde eine detaillierte Schritt-für-Schritt Installationseinleitung bereitgestellt (siehe [pgp]).

9.2.1 Einrichten der PGP Universal Server und die Verwaltungskonsole (Serverseite)

9.2.1.1 PGP Universal Server Installation und Grundeinstellungen

Die Installation und das Einrichten der PGP Universal Server wurde auf einer von Fraunhofer CNT zur Verfügung gestellten virtuellen Maschine und unter Berücksichtigung der Softwaresystemvoraussetzungen (siehe [pgp11a]) durchgeführt. Die zugewiesenen Hardwareressourcen und die Systembeschreibung des eingerichteten PGP Servers können unter Abschnitt 6.1.1 eingesehen werden.

Das webbasierte Installationssetup erfolgte intuitiv und unkompliziert nach der vorhandenen Einleitung und wurde ohne große Schwierigkeiten durchgeführt. Für das Errichten der virtuellen Maschine und die Installation der Server waren ungefähr 1,5

[22] Siehe http://www.symantec.com/business/support/index?page=products

Stunden nötig. Dabei wurden unter anderem das PGP eigene Betriebssystem installiert, Datum und lokale Zeit eingerichtet, Netzwerk eingestellt, der Benutzer mit den vollen Administratorrechten erstellt, sowie verwalteter Domain-Name und Active Directory-Name (Verzeichnisdienst) angegeben, um die Software in der bestehenden Unternehmensinfrastruktur einzubauen. Zum Abschluss der Installation wurde eine Zusammenfassung der gemachten Grundeinstellungen angezeigt.

Sowohl für den Installationsvorgang als auch für den eingerichteten Server und die grafische Oberfläche steht eine Vielzahl an unterstützten Sprachen und Tastaturen zur Verfügung (siehe [pgp11a]).

9.2.1.2 Verwaltungskonsole – Überblick und Integration des Unternehmensverzeichnisdienstes

In diesem Abschnitt wird einen Überblick über das Universal Server Betriebssystem und die unterschiedlichen Navigationsmöglichkeiten in dem HTTPS-basierten GUI für seine Verwaltung betrachtet. Es werden weiterhin die Schritte präsentiert, die zur Integration der Unternehmensverzeichnisdienst (Active Directory) durchgeführt wurden.

Der PGP Universal Server ist über die Browser-Schnittstelle von jedem Rechner zugreifbar, der an dem internen Netzwerk angeschlossen ist. Für den Aufruf muss der vollständige Name des Serverdomains (fully qualified domain name) auf dem Port 9000 angegeben werden. In dem konkreten Fall wird der Server durch die absolute Adresse https://cntsx042.cnt.fraunhofer.de:9000/ (CNTSX042 ist der konfigurierte Name der eingerichteten virtuellen Maschine) aufgerufen.

Nach erfolgreicher Anmeldung als Administrator wird ein Standardbegrüßungs-bildschirm angezeigt, der auf Produktinformationen, -dokumentation und weitere Hilfsmittel verweist.

Als Nächstes wird der Systemübersichtsbildschirm angezeigt (siehe Abbildung 12), der einen Überblick über das verwaltete System (z.B. Anzahl Benutzer, verwaltete Benutzergruppen, Richtlinien, Geräten) verschafft. Am oberen Rand des Bildschirms

sind verschiedene Registerkarten zu sehen, die zum Konfigurieren und Verwalten von Richtlinien, Benutzer, Mail, Organisation, Dienstleistungen und Systemeinstellungen dienen, die jeweils weitere Optionen in Form von untergeordnete Registerkarten besitzen. Weiterhin steht kontextsensitive Hilfe zu jeder Registerkarte bzw. Option zur Verfügung (- Symbol). Die Navigation in der Verwaltungskonsole ist intuitiv, schlicht und übersichtlich organisiert.

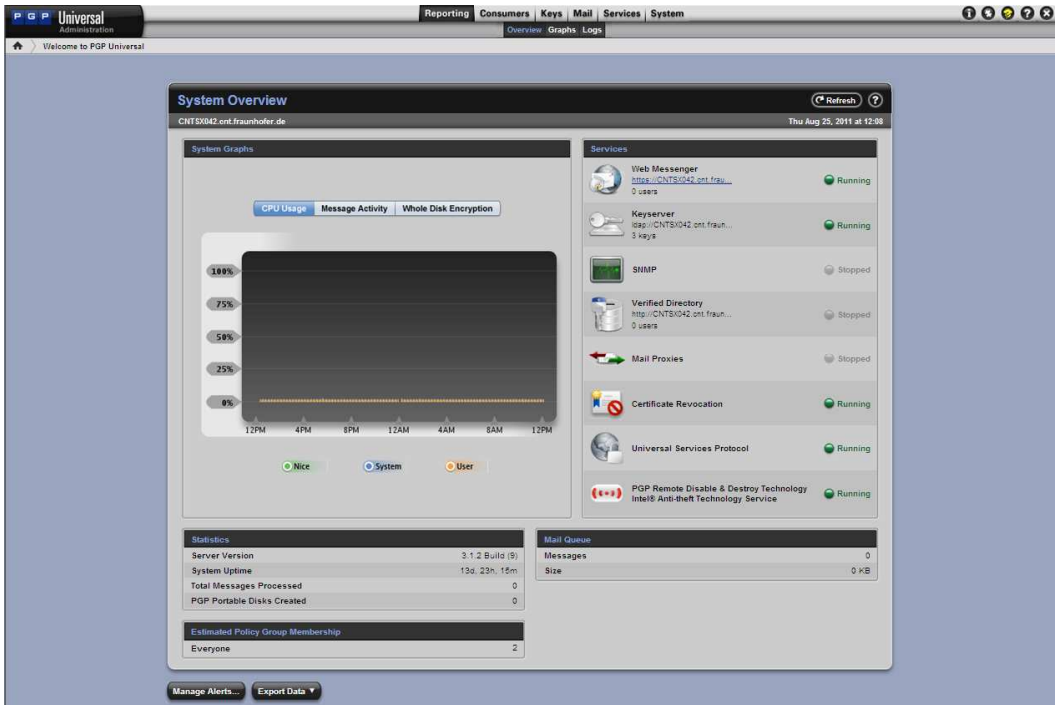


Abbildung 12. PGP Universal: Systemübersicht

Für die Zwecke der vorliegenden wissenschaftlichen Arbeit sind jedoch nur die Registerkarte Benutzer („Consumers“) und die unterliegenden Einstellungs-möglichkeiten von Bedeutung.

Die Integration der Unternehmensverzeichnisdienst von Fraunhofer CNT erfolgte genau nach der bereits genannten Schritt-für-Schritt-Einleitung (siehe [pgp]). Unter „Consumers“ → „Directory Synchronization“, kann man die synchronisierten Verzeichnisdienste sehen, bearbeiten, löschen bzw. Neue hinzufügen (siehe Abbildung 13).

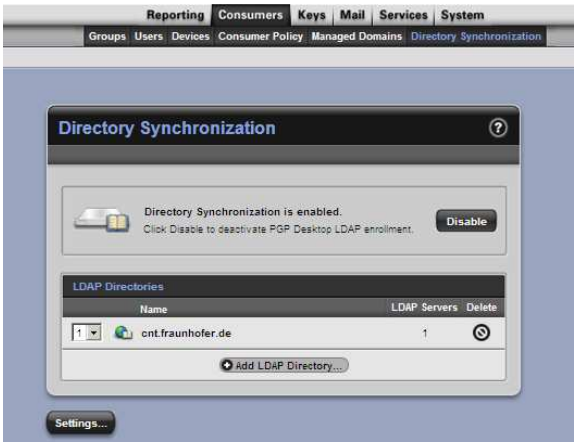


Abbildung 13. PGP Universal: Directory Synchronization

Wichtig ist, dass man unter „Consumers“ → „Directory Synchronization“ → „Settings“ die Option „enroll clients using directory authentication“ auswählt (siehe Abbildung 14). Dadurch werden Benutzer beim Anmelden an einem von dem PGP Universal Server verwalteten Client-Geräten automatisch zu den von PGP Universal Server verwalteten Benutzern hinzugefügt.

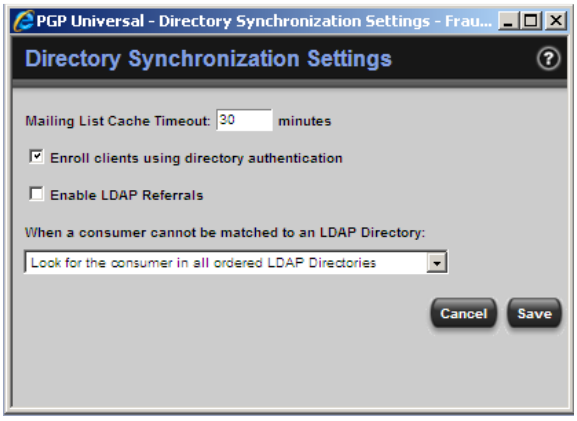


Abbildung 14. PGP Universal: Directory Synchronization Settings

9.2.1.3 Verwaltungskonsole – Arbeiten mit Benutzerrichtlinien und Verschlüsselungseinstellungen

Um die Festplattenverschlüsselung der gewünschten Geräte zentral und möglichst transparent für den Benutzer durchzuführen, werden zuerst die Benutzerrichtlinien konfiguriert und dann der Clientinstallationspaket erstellt. Die umgekehrte

Vorgehensweise ist auch möglich, ist jedoch für die Ziele der vorliegenden Arbeit irrelevant.

Unter „Consumers“ → „Consumer Policy“→ „Default“ werden die möglichen Konfigurationsoptionen für die Benutzerrichtlinie der Standardbenutzergruppe („Everyone“) angezeigt (siehe Abbildung 15).

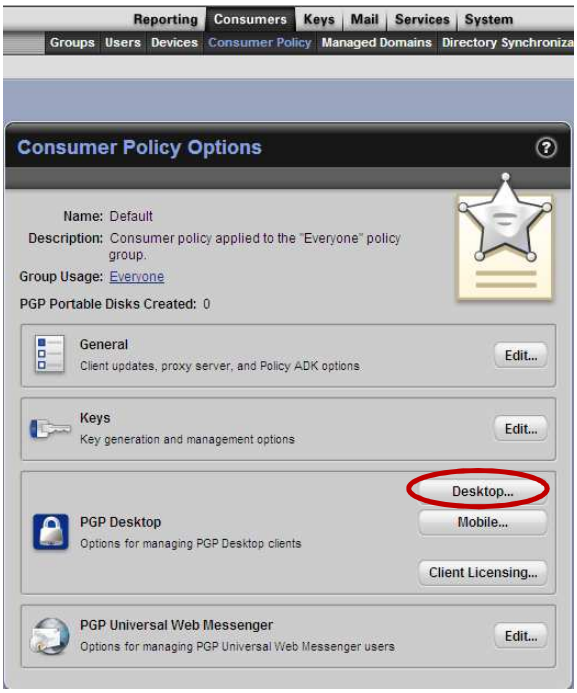


Abbildung 15. Konfiguration der Benutzerrichtlinie für die Standardbenutzergruppe

Für das Einrichten der Festplattenverschlüsselung sind nur die Einstellungsoptionen unter *PGP Desktop* von Bedeutung (Rotmarkierung auf der Abbildung 15). Weiterhin werden nur die Einstellungen unter den Registrierkarten „General“ und „Disk Encryption“ betrachtet. Sie sind dafür zuständig, welche Operationen von den Endnutzern durchgeführt werden können, wie z.B. das Entschlüsseln der Festplatte oder Veränderung an der zentral verteilten Benutzerrichtlinie. Für den durchgeführten Test der FDE-Lösung von Symantec wurde die Starteinstellungskombination auf Abbildung 16 und Abbildung 17 ausgewählt. Im Folgenden werden die wichtigsten Optionen kurz eingegangen.

Durch das Aktivieren des Feldes „Enable Silent Enrollment“ unter den Generalsettings (siehe Abbildung 16) wird die erstellte Richtlinie benutzertransparent (im Hintergrund) durchgesetzt bzw. aktualisiert.

Unter „Disk Encryption“ werden als Erstes die Benutzerrechte bezüglich interne und externe Speichermedien festgelegt. Diese sind selbsterklärend und werden nicht weiter betrachtet. Für die vorliegende Untersuchung wurden die vollständigen Rechte vergeben.

Des Weiteren wird die Authentifizierungsmethode für die Pre-Boot- Authentifikation ausgewählt. PGP WDE bietet die so genannte „Single-Sign-On“-Authentifikation (Aktivierung durch „Force“ bzw. „Allow“ in dem ersten Fallmenü). Dabei werden der Authentifikationsprozess der Verschlüsselungssoftware und die standardmäßige Authentifizierung unter Windows synchronisiert. Sobald die vollständige Festplattenverschlüsselung durchgeführt wurde, braucht sich der Endnutzer nur ein einziges Mal beim Systemstart mit seinen Anmeldedaten authentifizieren. Änderungen an den Anmeldedaten in der Active Directory werden von dem PGP Server automatisch aktualisiert und berücksichtigt.

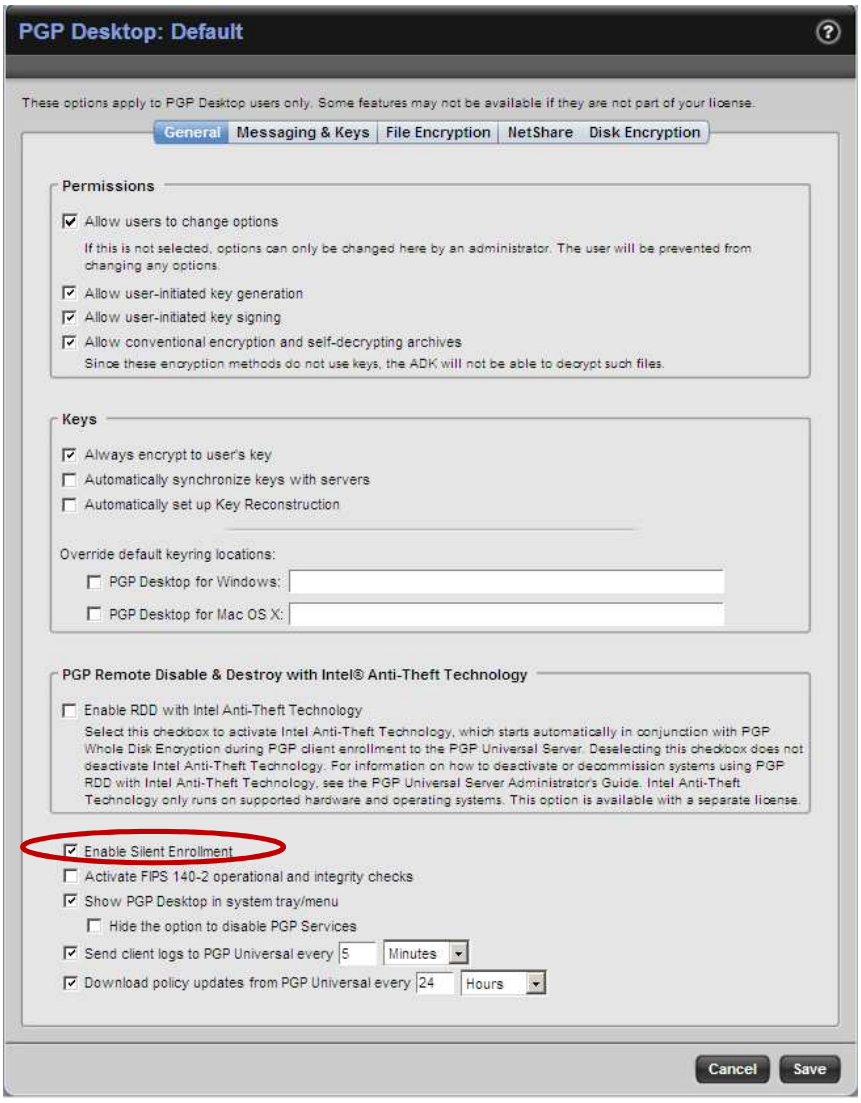


Abbildung 16. PGP Desktop Konfigurationsoptionen

Für die vorliegende Untersuchung wurde eine Richtlinie erstellt, die nach der Installation des Clientgeräts die gesamte Festplatte automatisch und benutzertransparent verschlüsselt. Für die Pre-Boot-Authentifizierung wird „Single-Sign-On“ erzwingt und den Benutzerkennwort unter Windows verlangt (Smartcard-Authentifikation wird in Abschnitt 9.3.2 betrachtet, TPM-Authentifikation ist für die vorliegende Arbeit irrelevant). Es wurden zusätzlich die maximale CPU-Auslastung und Sicherheit gegen Stromausfall durch die Richtlinie erzwungen.

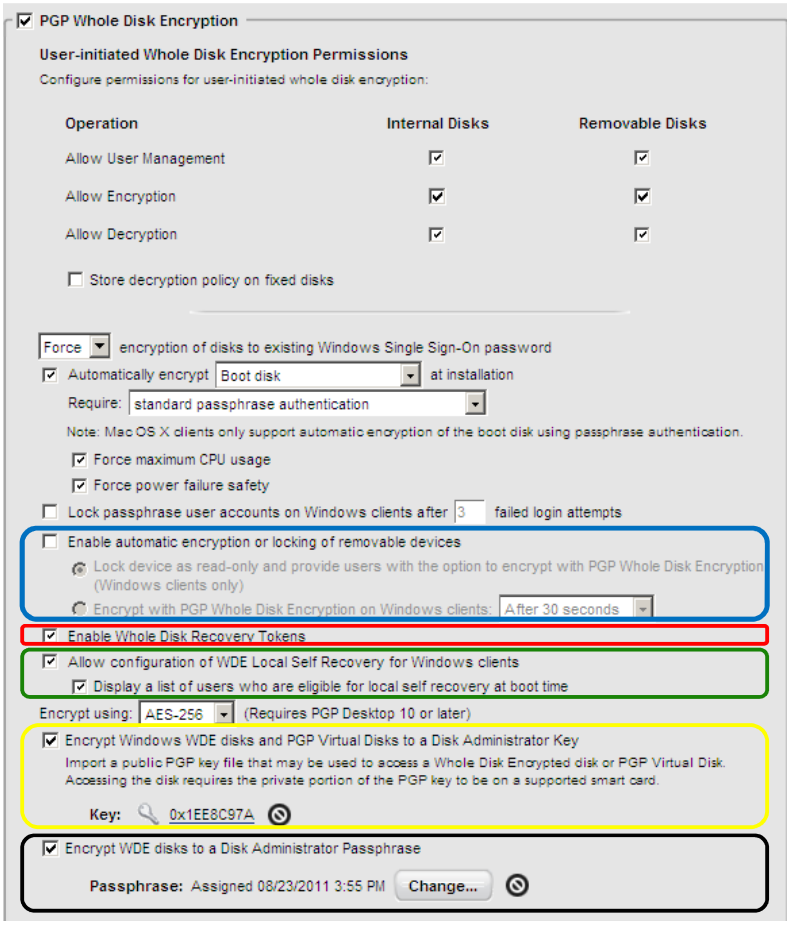


Abbildung 17. Konfigurationsoptionen für die Festplattenverschlüsselung

In der Richtlinie können auch unterschiedliche Optionen zum Umgehen mit externen Speichermedien an den Clientgeräten festgelegt werden (siehe Abschnitt 9.3.1).

Weiterhin können System- bzw. Benutzerkennwortwiederherstellungsoptionen ausgewählt und eingerichtet werden, die im Abschnitt 9.3.3 ins Detail eingegangen werden.

Änderungen der Standardrichtlinie werden auf den Clientgeräten automatisch ein Mal am Tag, beim Neustart oder durch manuelles Anfordern durchgesetzt.

9.2.1.4 Erstellung der PGP-Clientinstallationspaket

Nach dem Festlegen der Startkonfiguration der Standardrichtlinie wurde der Clientinstallationspaket erstellt. Durch Drücken der „Download Client“ - Taste unter „Consumers“ → „Groups“ (siehe Rotmarkierung auf der Abbildung 18) wird man auf das Installationskonfigurationsmenü weitergeleitet (siehe Abbildung 19).

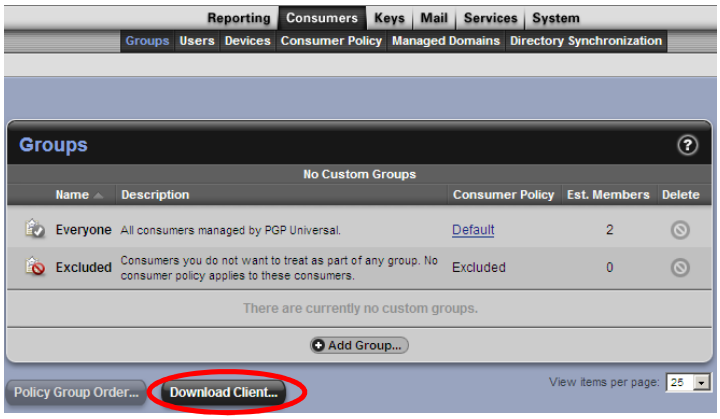


Abbildung 18. Erstellung des Clientinstallationspakets

Es wurden die zutreffende Version des Clients, sowie das Operationsplattform und die gewünschte GUI-Sprache ausgewählt. Zu beachten ist, dass die „Auto-detect Policy Group“ ausgewählt ist, damit die erstellte Richtlinie automatisch erkannt und durchgesetzt werden kann (siehe Rotmarkierung auf der Abbildung 19).

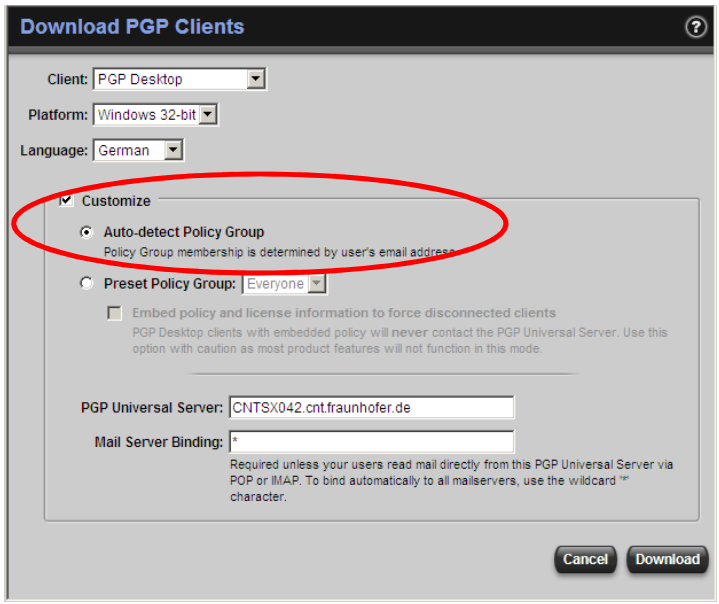


Abbildung 19. Konfiguration des Clientinstallationspakets

Somit wird ein für Windows standardmäßigen MSI-Installationspaket für die Clientseite erzeugt, der durch bereits existierende Unternehmensstrukturen an den Clientgeräten verteilt werden kann (z.B. NetInstall Installer). Für die vorliegende Untersuchung wurde der Clientinstallation jedoch manuell durchgeführt.

9.2.2 Installation der PGP-Client, Systemverschlüsselung und Benutzerregistrierung (Clientseite)

Die Installation der Clientseite erfolgte einfach, verständlich und nach der bereits erwähnten Einleitung (siehe [pgp]). Die installierte Software hat ca. 44 MB auf der Festplatte in Anspruch genommen. Nach dem erfolgreichen Installationsvorgang musste das System standardmäßig neugestartet werden. Sobald das System neugeladen wurde, wurde man automatisch aufgefordert sich gegenüber den PGP Universal mit den Windows-Benutzerdaten anzumelden.

Die angegebenen Informationen müssen mit den hinterlegten Benutzerkontodaten in dem Verzeichnisdienst des Unternehmens übereinstimmen, um die Authentifizierung für die Festplattenverschlüsselung erfolgreich einzustellen. Beim Versuch anderer Anmeldeinformationen einzugeben, wurde eine Fehlermeldung angezeigt und man

wurde erneut zur Authentifikation aufgefordert. Sobald die korrekten Daten eingetragen wurden, wurde der Benutzer automatisch bei PGP Universal angemeldet [23], die eingestellte Richtlinie wurde durchgesetzt und die Systemverschlüsselung des Clientgeräts fing automatisch an.

Der Verschlüsselungsvorgang sollte in keiner Weise die Arbeit an dem Rechner behindern, es ist jedoch mit Geschwindigkeitseinbüßen zu rechnen (durch die CPU-Auslastung). Um den Dauer der Verschlüsselung realistisch messen zu können, wurde der Rechner während des Prozesses nicht genutzt. Der gesamte Vorgang dauerte insgesamt 82 Minuten und wurde mit einer Meldung zur erfolgreichen Systemverschlüsselung abgeschlossen.

9.3 Weitere getestete Funktionen und Möglichkeiten des Produkts im Kontext der vorliegenden Arbeit

9.3.1 Verschlüsselung von Wechselmedien

Die FDE-Lösung von Symantec bietet mehrere Möglichkeiten für den Umgang mit Wechseldatenträger. Es können einerseits zentral verwaltete Richtlinien durchgesetzt werden, die den Benutzern weniger Handlungsraum überlassen (siehe Abschnitt 9.3.1.1) und/ oder es kann auf der Clientseite die Verschlüsselung manuell durchgeführt werden, wobei man die bereits darauf gespeicherten Daten (falls vorhanden) „in place“ verschlüsseln kann (siehe Abschnitt 9.3.1.2).

9.3.1.1 Richtlinien für Wechseldatenträger

Es können durch die zentrale Verwaltungseinheit folgende drei Richtlinien festgelegt werden:

- Entscheidung für den Umgang mit Wechselspeichermedien wird den Endnutzern überlassen (siehe Abschnitt 9.3.1.2). Dafür werden die unter Abbildung 17 blaumarkierten Felder frei gelassen.

[23] Der Anmeldevorgang dauerte wenige Sekunden.

- Alle unverschlüsselten angeschlossenen Wechselmedien werden automatisch schreibgeschützt (siehe Abbildung 20) und den Endnutzern wird die Entscheidung überlassen, ob die externen Datenträger verschlüsselt werden (siehe Abschnitt 9.3.1.2).

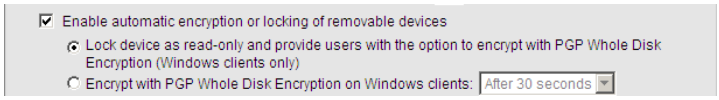


Abbildung 20. Richtlinie zum Schreibsperre ungesicherter Wechseldatenträger

Sobald ein unverschlüsselter Wechseldatenträger an dem Clientgerät angeschlossen wird, bekommt der Endnutzer folgende Meldung:

Abbildung 21. Schreibsperre ungesicherter Wechseldatenträger

- Sobald ein Wechseldatenträger an einem Clientgerät angeschlossen wird, wird er automatisch sofort bzw. nach einem bestimmten Timeout „in-place“ verschlüsselt (siehe Abbildung 22).

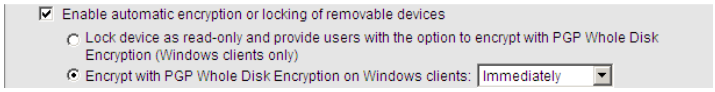


Abbildung 22. Richtlinie zur automatischen Verschlüsselung angeschlossener Wechseldatenträger

9.3.1.2 Wechseldatenträgerverschlüsselung durch den Endnutzer

Falls von der Richtlinie nicht anders vorgeschrieben, kann der Endnutzer die angeschlossenen mobilen Speichermedien manuell verschlüsseln. Dabei wird über die PGP Desktop-Konsole ein Benutzer für das Wechselmedium erstellt bzw. ein existierender Benutzer ausgewählt (Login und Kennwort für die Authentifikation) und der Datenträger „in-place“ verschlüsselt (siehe Abbildung 23). Die Daten auf den in dieser Weise verschlüsselten Speichermedien sind nur von Rechnern mit einer kompatiblen PGP Client Software und mit den korrekten Authentifikationsdaten zugreifbar.

Diese Verschlüsselungsmöglichkeit steht jedoch nicht zur Verfügung, falls die Wiederherstellungsoption - *Whole Disk Recovery Token* (WDRT) durch die Richtlinie festgelegt ist (siehe Rotmarkierung auf Abbildung 17) und keine Verbindung zum PGP Universal Server besteht. Die Datenwiederherstellungsstrategien des Produkts werden in Abschnitt 9.3.3 detaillierter behandelt.

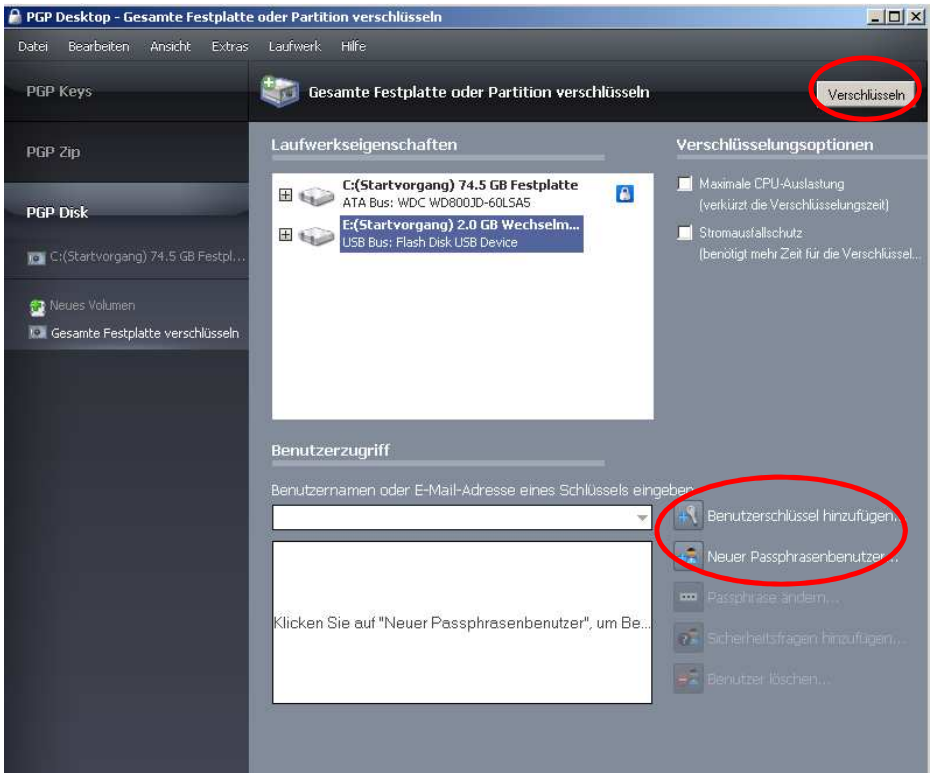


Abbildung 23. Verschlüsselung der Wechseldatenträger von den Endnutzern

9.3.1.3 Datenspuren auf verschlüsselten Wechseldatenträger

Es wurde eine Text-Datei auf dem verschlüsselten Wechseldatenträger erstellt mit dem Name „Test.txt“ und dem Inhalt – „Das ist eine Testdatei“. Anschließend wurde der USB-Stick von dem Rechner entfernt und neu eingesteckt. Vor der für die Benutzung der Daten erforderlichen Authentifikation wurde der Inhalt des Datenträgers mit Hilfe des Programms WinHex 16.1 nach der Textdatei, sowie nach Zeichenketten, die der Name der Datei, der Inhalt oder Teile davon (wie z.B. „Das ist“) durchsucht. Alle Tests hatten keine Treffer zur Folge. Weiterhin wurde das verschlüsselte Speichermedium nach Hinweise für die Benutzung von PGP WDE untersucht und es konnten ebenfalls keine Informationen darüber gefunden werden.

Nach der erfolgreichen Anmeldung wurden die Tests mit WinHex wiederholt. In diesem Fall konnte, wie erwartet, die Datei und deren Inhalte anhand der angegebenen Zeichenketten gefunden werden (wie erwartet).

Der USB-Stick wurde schließlich von Windows formatiert. Die Tests wurden erneut wiederholt und führten zu negativen Ergebnisse – also konnten keine Datenspuren und keine Hinweise für die Benutzung von PGP WDE nachgewiesen werden.

9.3.2 Authentifikationsmöglichkeiten

Es wurde, wie bereits beschrieben, eine Richtlinie durchgesetzt, die das Kennwort der Benutzer (unternehmensintern) für die Pre-Boot-Authentifikation verlangt. Dabei funktioniert der „Single-Sign-On“ - Anmeldevorgang einwandfrei und so wie der Benutzer es erwartet. Weiterhin ist es möglich, Smartcard- bzw. TPM-Authentifikation einzuschalten (nur unter Windows).

Die TPM-Authentifikation konnte in der konkreten Untersuchung nicht getestet werden, weil die technischen Voraussetzungen in der Testumgebung nicht vorhanden sind.

Die FDE-Lösung von Symantec unterstützt eine Reihe von Smartcard-Lesegeräten (siehe [pgp11b]), die sowohl für die Authentifikation, als auch für weitere zusätzliche Funktionen der Software (z.B. E-Mail Signaturen u.Ä.) genutzt werden können. In der Testumgebung wurden die dazu nötigen Einstellungen ohne große Schwierigkeiten vorgenommen. Sowohl das Lesegerät, als auch die Karte und die darauf gespeicherten Zertifikate und Schlüsselpaare wurden von der Clientsoftware erkannt. Es konnten zusätzliche Schlüsselpaare und Zertifikate auf der Karte gespeichert werden bzw. bereits vorhandene Informationen exportiert werden. Der Versuch, die Karte für die Pre-Boot-Authentifikation zu benutzen schlug jedoch fehl. Das Lesegerät wirkt zwar funktionsbereit, liest die Karte aber nicht. Für diesen Sachverhalt gibt es folgende mögliche Erklärungen:

- Veraltete Treiber des Kartenlesegeräts;
- Existierende unternehmensinterne Synchronisationsprobleme, falls keine Internetverbindung vorhanden ist. Dadurch, dass die Karte noch vor dem Start des Betriebssystems gelesen werden soll, könnte dies die Ursache für die fehlende Erkennung sein.

Es wird jedoch angenommen, dass das Problem bei einem möglichen Unternehmenseinsatz der FDE-Lösung von Symantec durchaus beseitigt werden kann, um den vollen Funktionsumfang des Produkts zu benutzen.

9.3.3 Passwortwiederherstellungsstrategien

Das Produkt bietet mehrere Möglichkeiten für die Wiederherstellung vergessener bzw. gesperrter Passwörter (siehe Abschnitt 9.3.3.1 und Abschnitt 9.3.3.2). Zusätzlich können Administratorzugriffe auf verschlüsselten Systemen erlaubt werden, um bestimmte Wiederherstellungsszenarien zu ermöglichen (siehe Abschnitt 9.3.3.3).

9.3.3.1 Wiederherstellungsfragen - Clientseite

Solange die durchgesetzte Richtlinie die lokale Wiederherstellung erlaubt (siehe Grünmarkierung auf der Abbildung 17), kann der Endnutzer eine lokale Wiederherstellung mit Frage-Antwort-Authentifizierung festlegen (siehe Abbildung 24). Der Vorgang ist intuitiv und wird durch einen Einstellungsassistenten unterstützt. Der Benutzer wird aufgefordert 5 Sicherheitsfragen zu erstellen und endsprechend zu beantworten. Die Fragen kann man aus einer Liste von vorbereiteten Standardfragen auswählen bzw. selbst entwerfen. Falls der Benutzer sein Passwort vergisst, hat er im Pre-Boot-Menü die Option die Sicherheitsfragen zu beantworten. Dabei wird das System bei 3 von 5 richtig beantworte Fragen gestartet. Die Wiederherstellung durch die Sicherheitsfragen funktioniert einwandfrei und erwartungsgemäß.

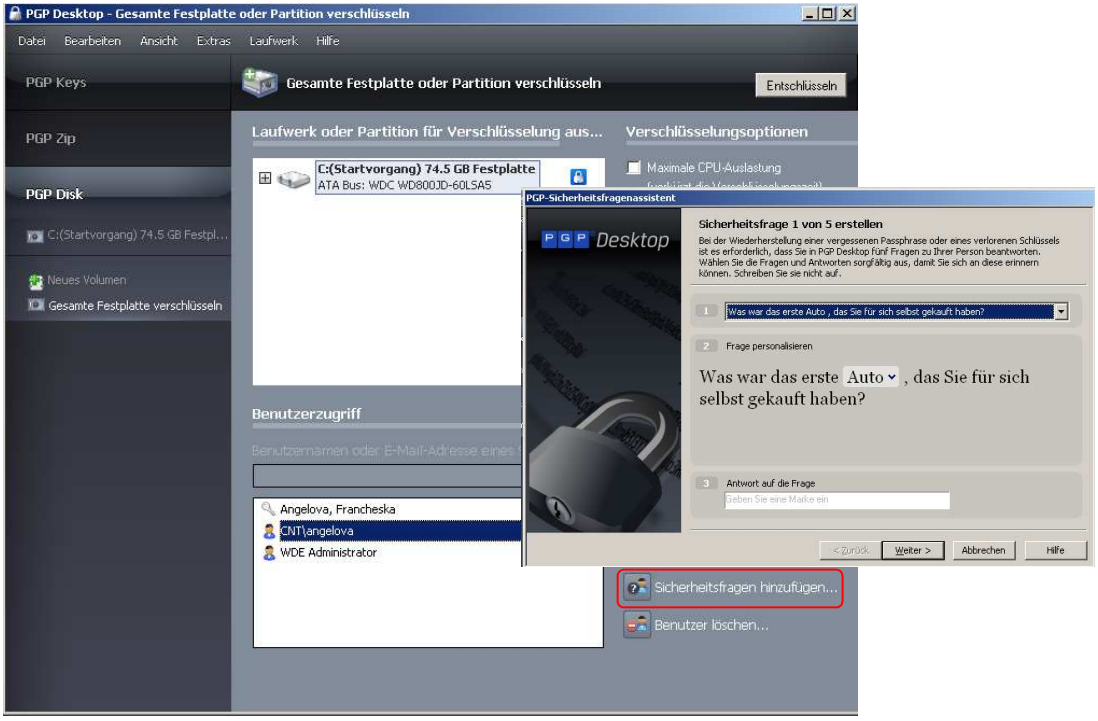


Abbildung 24. PGP Desktop: Erstellen von Sicherheitsfragen

9.3.3.2 Whole Disk Recovery Token (WDRT) - Serverseite

Eine weitere Möglichkeit zur Wiederherstellung von Benutzerpasswörtern bzw. von verschlüsselten Datenträgern bietet die WDRT-Funktion an, falls sie durch die Richtlinie aktiviert ist (siehe Rotmarkierung in der Abbildung 17). Dabei wird ein zusätzliches Token für jedes verschlüsselte Laufwerk pro registriertem Laufwerknutzer erstellt. Bei Bedarf kann dieses Token den Benutzern mitgeteilt werden bzw. vom Administrator selbst zur Authentifikation an den entsprechenden verschlüsselten Datenträgern genutzt werden (z.B. Wiederherstellung von verschlüsselten Datenträgern ehemaliger Mitarbeiter). Es wird als Passphrase in dem Pre-Boot-Authentifikationsfenster angegeben. Die Wiederherstellung durch den WDRT funktioniert einwandfrei und so wie erwartet.

Der WDRT kann folgendermaßen aufgerufen werden - unter „Consumers“ → „Users“ wird der Benutzer des verschlüsselten Ziellaufwerks ausgewählt. Im „Konto“ des Benutzers stehen unter anderem alle verschlüsselten Speichermedien zu denen dieser

Zugriff hat. Durch Drücken des Lupe-Zeichens neben dem Ziellaufwerk geling man zu dem gewünschten WDRT (siehe Abbildung 25).

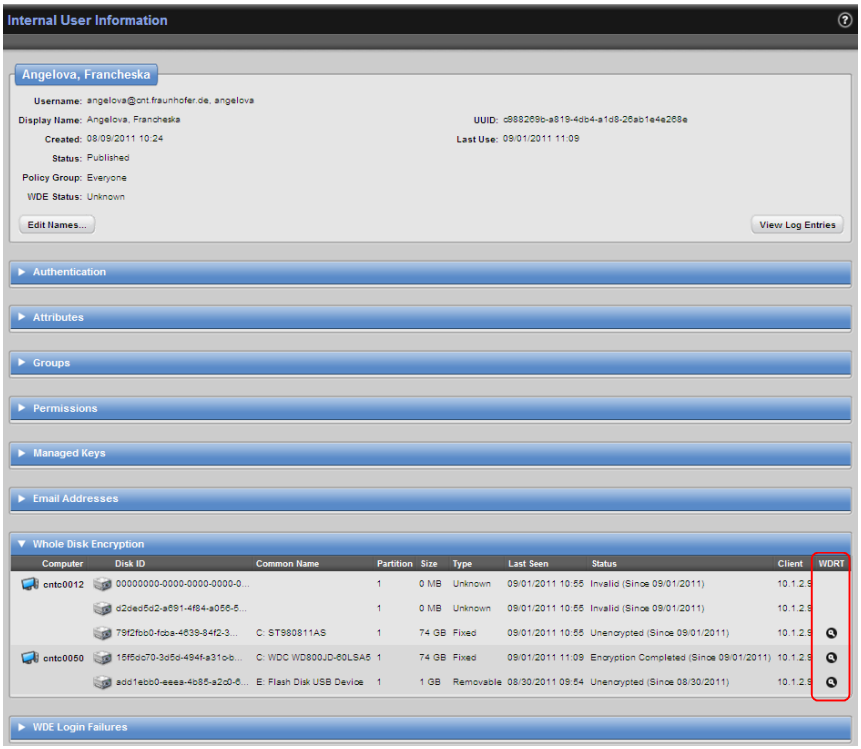


Abbildung 25. PGP Universal Server: Whole Disk Recovery Token (WDRT)

9.3.3.3 Administratorzugriff auf verschlüsselte Datenträger

Weiterhin besteht die Möglichkeit für jedes verschlüsseltes Speichermedium einen zusätzlichen Administratorschlüssel für die Smartcardauthentifikation (siehe Gelbmarkierung in der Abbildung 17) bzw. ein Administratorkennwort für die Passwortauthentifikation (siehe Schwarzmarkierung in der Abbildung 17) zu erstellen. Somit kann der Administrator ohne Benutzererlaubnis auf die verschlüsselten Daten zugreifen. Dadurch können z.B. Daten ehemaliger Mitarbeiter bei Bedarf wiederhergestellt werden, neue Benutzer für bereits verschlüsselte Laufwerke angemeldet werden. Die Smartcardauthentifikation konnte nicht getestet werden (siehe Abschnitt 9.3.2). Die Administratoranmeldung durch eine zusätzliche Passphrase funktionierte einwandfrei und erwartungsgemäß.

Hier ist jedoch die Frage zu klären, wie mächtig der Administrator sein darf und wie groß das Sicherheitsrisiko für ein Unternehmen durch einen „allmächtigen“ Administrator ist!

9.3.4 Ressourcenbelegung

Es wurden mehrere Messungen zum Ermitteln der CPU- und RAM- Belastung sowie der Kopier-, Schreib-, Lesezugriffsgeschwindigkeit bzw. –zugriffszeit für verschiedene Dateigrößen auf dem mit PGP WDE verschlüsselten Testrechner durchgeführt. Ziel der Messungen war diese Größen bei den mit den unterschiedlichen FDE-Lösungen verschlüsselten Rechnern sowie einem unverschlüsselten Testsystem zu vergleichen. Details über die durchgeführten Messungen, die Ergebnisse und ihre Auswertung werden in Abschnitt 12 betrachtet.

9.3.5 System-Partition/ Laufwerk bzw. externe Wechselmedien dauerhaft entschlüsseln

Die Entschlüsselung der Systempartition bzw. anderer eingebauter oder externer Laufwerke erfolgt lokal auf der Clientseite und verläuft intuitiv, unkompliziert und gleichartig. Nach dem Auswählen des zu entschlüsselnden Speichermediums und dem Drücken der „Entschlüsseln“-Taste wird der Benutzer zur Authentisierung aufgefordert. Bei erfolgreicher Authentifizierung startet der Entschlüsselungsprozess automatisch. Der Zeitaufwand für die Entschlüsselung der getesteten Speichermedien war mit dem für die Verschlüsselung vergleichbar. Der Prozess verläuft im Hintergrund und erlaubt den Nutzern während des Entschlüsselungsvorgangs weiter an dem Rechner zu arbeiten, wobei mit kleinen Verzögerungen[24] bei Anwendungen mit großer CPU-Belastung zu rechnen ist.

[24] Die Verzögerung der Arbeitsprozesse während der Ver- bzw. Entschlüsselung des Systems wurde nicht getestet, damit der Zeitaufwand für die beiden Vorgänge nicht beeinflusst wird.

9.4 Anmerkungen und Zusammenfassung

Das von Symantec angebotene Produkt bietet eine professionelle FDE-Lösung, die speziell für Unternehmensstrukturen konzipiert ist. Es erlaubt eine umfangreiche Verwaltung der verschlüsselten Speichermedien und kann an unterschiedliche Unternehmensgrößen angepasst werden (leichte Skalierbarkeit der Software). Das Produkt konnte ohne große Schwierigkeiten in der Testumgebung implementiert werden und bietet eine einfache und verständliche Navigation, sowohl auf der Verwaltungsseite (Serverseite) als auch auf der Endbenutzerseite (Clientseite). Weiterhin ist ein umfangreiches Angebot an Produktdokumentation sowohl für Administratoren, als auch für Benutzer vorhanden.

Zum Schluss sind noch einige Anmerkungen zum Produkt wichtig:

- Während der Testphase der Software wurde die Erfahrung gemacht, dass bei Problemen mit dem Einrichten bzw. der Funktionalität der Software eine kompetente und schnelle Unterstützung durch den Produktanbieter gewährleistet wird, wobei eine Lösung des Problems angestrebt wird.

- Der Administrator agiert als eine Art „Super User“ und besitzt die Möglichkeit, Zugriffsrechte für alle verwalteten verschlüsselten Speichermedien zu erlangen. Der Endbenutzer hat keine Informationen darüber, welche Zugriffsrechte der Administrator auf seinem Rechner besitzt.

- Bei kommerziellen Verschlüsselungsprodukten besteht immer die Gefahr, dass ein Masterkey vorhanden ist. PGP WDE hat allein in den letzten 10 Jahren dreimal den Besitzer gewechselt – es ist nicht überprüfbar, welche Gefahren in dem Sourcecode möglicherweise versteckt sind.

10 SafeGuard Enterprise (SGN)

In diesem Abschnitt wird die kommerzielle FDE-Lösung SafeGuard Enterprise von Sophos analysiert. Neben einem ausführlichen Überblick über die Funktionen, Möglichkeiten und Grenzen des Produkts, wird sie systematisch nach den festgelegten Vergleichskriterien und unter Beachtung der vorgestellten Randbedingungen untersucht. Abschließend werden einige Bemerkungen zum Produkt gemacht und die ermittelten Ergebnisse zusammengefasst.

Das Produkt ist ähnlich wie die FDE-Lösung von Symantec aufgebaut (siehe Abschnitt 9). Es besteht aus einer Management-Konsole (Verwaltungseinheit) und einer verwalteten Clientsoftware. Die Management-Konsole wurde im konkreten Untersuchungsfall auf dem dafür eingerichteten Server installiert und wird als Serverseite bezeichnet. Auf der Clientseite wird ein speziell dafür erzeugtes Paket installiert (je nach Richtlinienkonfiguration), das auf der *SafeGuard Easy (SGE)* basiert. SGE ist der Produktname für die SafeGuard Enterprise Standalone-Lösung (Vergleichbar mit PGP Desktop) und wird weiterhin als Clientseite betrachtet. Dabei wird jedoch die FDE-Lösung von Sophos (Serverseite, Clientseite, sowie dazugehörigen Konfigurationsteile, wie Datenbank und Webserver) als ein einziges komplettes Produkt vermarktet und entsprechend in der vorliegenden Arbeit als gesamtes Paket betrachtet. Eine Besonderheit des SGN ist, dass es speziell für Windows OS konzipiert ist (siehe [sgn11a]).

10.1 Übersicht-Funktionsumfang

Die Beschreibung des Aufbaus und der Einzelteile des Produktes orientieren sich an der offiziellen Seite von SafeGuard Enterprise (siehe [sgn11a]).

SGN in der aktuellen Version 5.60.0.192 besitzt eine modulare Struktur (siehe Abbildung 26).

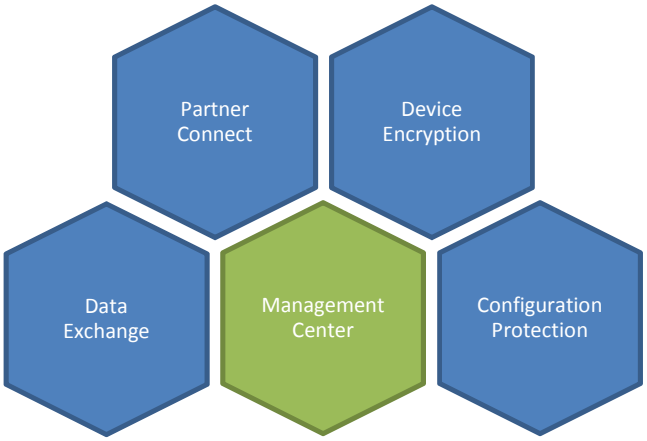


Abbildung 26. Funktionsmodule von SafeGuard Enterprise

Management Center:

- Stellt die zentrale Verwaltungseinheit, die die einzelnen Module einbaut und ihre Funktionen administriert. Es können jederzeit Funktionsmodule hinzugefügt werden.
- Erstellen, Verteilen und Speichern von Verschlüsselungsschlüsseln.
- Zentralisierte Erstellung und Verwaltung von Richtlinien zur automatisierten Durchsetzung von Benutzer-, Kennwort- und Computerrichtlinien, z.B. Durchsetzung einer Richtlinie zur automatisierten Verschlüsselung der Client-Festplatte und aller angeschlossenen Wechseldatenträger bei der nächsten Anmeldung des Benutzers.
- Zentraler Zugriff auf Protokoll- und Bericht-Status sowie Lizenzierungsinformationen.
- Automatische Benutzerregistrierung – automatisiertes Verfahren zum Erstellen von Benutzerkonten, zur Verwaltung von Verschlüsselungsschlüsseln und zur Richtlinienzuweisung.

- Integration in das vorhandene Unternehmensverzeichnis.
- Festlegen der Funktionen, die die Benutzer am Client-PC ausführen können.
- Erstellen und Verwalten von Administratoren mit unterschiedlichen administrativen Tätigkeitsfeldern. Mindestens ein Hauptsicherheitsbeauftragter (Administratorrolle bei SGN, die vollständige Verwaltungsrechte hat) muss dafür vorhanden sein.

Device Encryption:

- Verschlüsselung und Verwaltung des gesamten Systems.
- Wiederherstellungsstrategien von Passwörtern und verschlüsselten Daten im Unternehmen.
- Mehrere Pre-Boot-Authentifizierungsoptionen (In SafeGuard wird die Pre-Boot-Authentifikation als Power-on Authentication (POA) bezeichnet): Passwort, Smartcard, Token, Fingerabdrucksensoren (nur bei bestimmten PC-Modellen).
- „Single-Sign-On“-Unterstützung.
- Berichte zur Gewährleistung der Richtlinieneinhaltung: Computerverschlüsselungsstatus, Warnhinweise zu fehlgeschlagenen Anmeldungen und die Geräteverwaltung.
- Als Verschlüsselungsalgorithmus wird nur der Quasi-Standard AES angeboten mit 128-Bit bzw. 256-Bit Verschlüsselung.
- Durch verteilten Zugriff auf Mehrkernprozessoren werden laut Anbieter die Verschlüsselungsraten um bis zu 30 % im Vergleich zu älteren Versionen des Softwareproduktes verbessert.
- Verschlüsselung von SSD-Festplatten wird unterstützt.
- Unterstützung von selbst-verschlüsselnden Festplatten, die auf dem *OPAL Storage Specification (OPAL-SSC)*- Standard basieren.

Data Exchange:

- Verschlüsselung von externen Speichermedien, wie z.B. USB-Sticks, Festlatten u.A.
- Schlüsselring-Funktion zum Datenaustausch innerhalb von Projekt-Teams.
- Verwendung verschlüsselter Datenmedien auf Rechnern ohne SGN-Installation mittels einer portablen Komponente (ähnlich zu *PGP Portable*).

Configuration Protection:

- Erkennung verbundener Geräte und Einschränkung ihres Einsatzes je nach Gerätetyp, Modell oder bestimmter Seriennummer.
- Komplette Sperrung sämtlicher Speichermedien.

Partner Connect:

- Zentrale Lösung zur Datenschutzverwaltung in gemischten IT-Umgebungen.
- Verwaltung von Drittanbieter-Produkten zum Endpoint-Schutz (z.B. BitLocker auf Windows Vista und Windows 7).

SafeGuard Enterprise erlaubt durch sein modulares Konzept das Anbinden von unterschiedlichen Sicherheitslösungen, die mit ihrer Funktionalität teilweise über den Rahmen der vorliegenden Arbeit hinausgehen. Aus diesem Grund werden weiterhin nur die wichtigsten und für das Thema der vorliegenden Diplomarbeit relevanten Funktionen betrachtet. Für weitere Details wird auf die Dokumentation des Produkts verwiesen (siehe [sgn11b]).

10.2 Installation und Konfiguration der Server-Client Kommunikation

Die Installation und das Einrichten der SafeGuard Enterprise Umgebung wurde auf einem von Fraunhofer CNT zur Verfügung gestellten virtuellen Server (siehe

Abschnitt 6.1.1) und unter Berücksichtigung der Softwaresystemvoraussetzungen (siehe [sgn11a]) durchgeführt.

Für das Einrichten der SafeGuard Umgebung wird von Sophos ein automatisierter Installations-Assistent zur Verfügung gestellt, der in das Installationspaket integriert ist. Der Assistent führt nicht nur die Einstellung des Softwareproduktes selbst, sondern auch der benötigten Komponenten, wie Server (Microsoft Internet Information Server [IIS]) und der Datenbank (Microsoft SQL Express), durch. Dabei wird die Installation in drei Schritte unterteilt – Servervorbereitung, Aufsetzen der SafeGuard Enterprise Umgebung und Installieren eines Clients (siehe Abbildung 27).

Abbildung 27. SafeGuard Enterprise Installation Advisor

10.2.1 Servervorbereitung

Die für das Einrichten der FDE-Lösung von Sophos benötigten Schritte wurden mit Hilfe des Installations-Assistenten durchgeführt (siehe Abbildung 28). Die benötigten Softwarekomponenten wurden benutzertransparent, unkompliziert und automatisch von der Advisor-Konsole installiert und konfiguriert. Es wurde lediglich eine Ausführungsbestätigung, Lizenzbestätigung bzw. Login-Eingabe (für die Datenbankinitialisierung) vom Benutzer verlangt. Der Vorgang ist jedoch verständlich und intuitiv und konnte reibungslos und erfolgreich abgeschlossen werden.

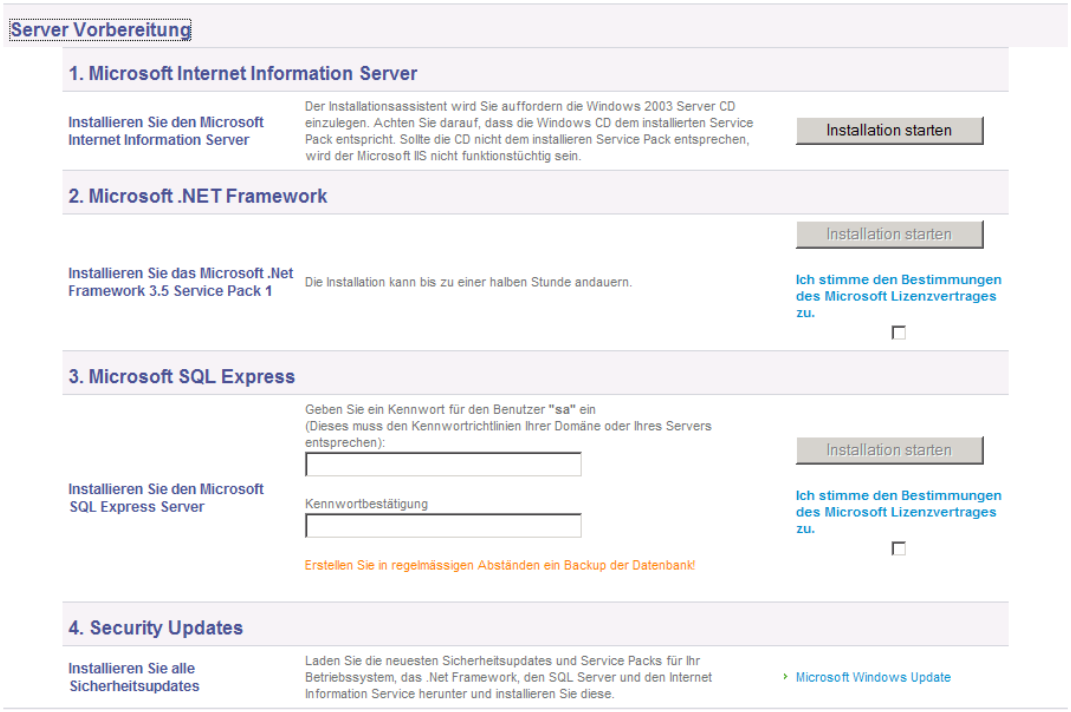


Abbildung 28. Server Vorbereitung mittels des Installations-Assistenten

10.2.2 Aufsetzen der SafeGuard Enterprise Umgebung

Im zweiten Teil des Installationsvorgangs werden der Safeguard Enteprise Server und die Management-Konsole installiert und eingerichtet. Dabei gibt es viele Schritte, die außerhalb des Advisors durchzuführen sind. Es werden zusätzliche Installationspakete erstellt und installiert. Der Vorgang wird durch mehrere zusätzliche Installationsassistenten unterstützt. Ein weiteres Hilfsmittel sind die Videos, die den Installations- und Konfigurationsvorgang veranschaulichen (siehe Rotmarkierung auf der Abbildung 29).

Bei der konkreten Installation in der Testumgebung hat das Einrichten der vielen Kleininstallationen und der zusätzlichen Konfigurationen viel Zeit in Anspruch genommen. Dazu ist noch zu bemerken, dass Operationen, die von den anderen getesteten kommerziellen FDE-Lösungen automatisch durchgeführt werden (wie Erstellen und Verteilen von Unternehmens- bzw. Benutzerzertifikate), bei SafeGuard manuell realisiert werden müssen. Wichtige Aspekte, wie das Anbinden des

Unternehmensverzeichnisdienstes, werden nicht von dem Assistenten erwähnt bzw. eingeleitet. Die Integration der vorhandenen Active Directory muss sowohl in der Datenbank als auch in der Management-Konsole durchgeführt werden. Nach der LDAP-Synchronisation können nur vollständige Organisationseinheiten in die Management-Konsole importiert werden und die Software erlaubt die Zuweisung erstellter Richtlinien nur auf diese gesamten Organisationseinheiten. Es ist nicht möglich einzelne Rechner, Gruppen oder Benutzer auszuwählen. Deswegen musste für den Testrechner eine neue Organisationseinheit angelegt werden, um mögliche Beeinflussung anderer Clientrechner der Unternehmensinfrastruktur zu verhindern.

Die Zwischenschritte für die LDAP-Synchronisation sowie das Importieren des Unternehmensverzeichnisses können aus der Installationsanleitung entnommen werden (siehe [sgn11d]).

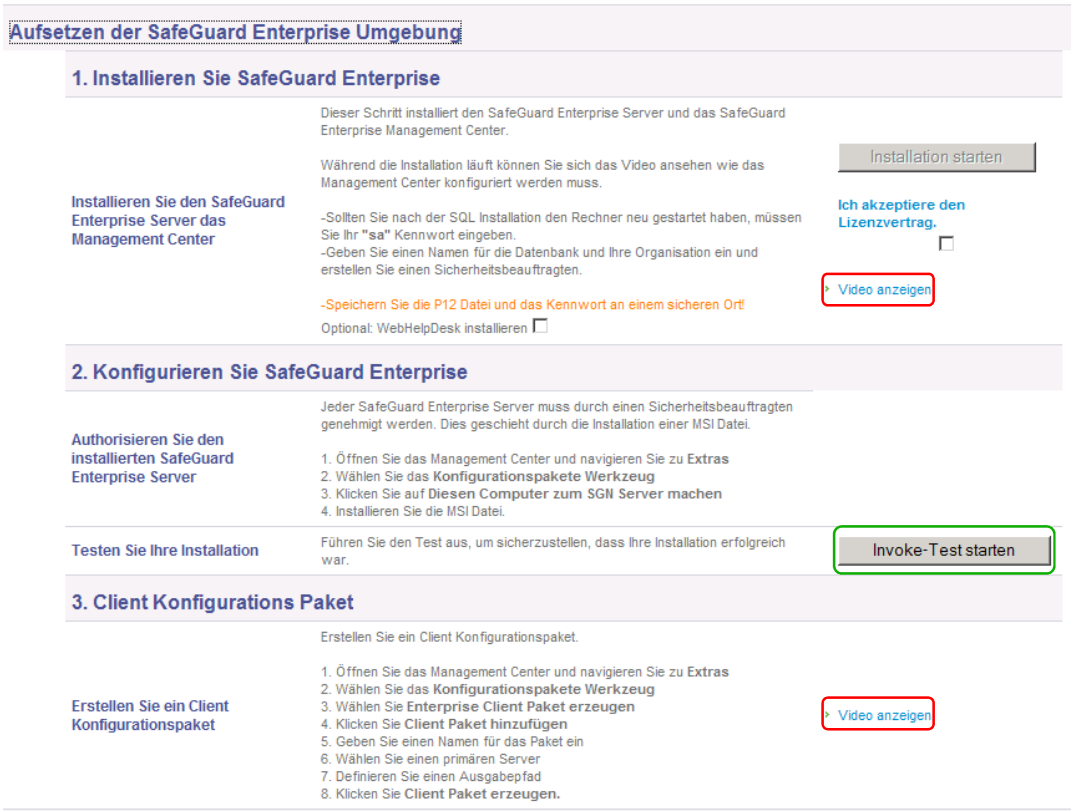


Abbildung 29. Aufsetzen der SafeGuard Enterprise Umgebung

Der Vorgang wurde scheinbar korrekt bis zu dem Punkt ausgeführt, an dem die eingerichtete Installation getestet werden sollte und der Test aber fehlschlug (siehe

Grünmarkierung auf der Abbildung 29). Es konnte schnell und unkompliziert Kontakt mit einem Ansprechpartner von Sophos für die Problembehebung telefonisch hergestellt werden. Das Problem konnte auf den Microsoft IIS eingegrenzt werden, wobei festgestellt wurde, dass die Verbindung über Port 80 (die Standardeinstellung) für Client-Server-Kommunikation überhaupt nicht hergestellt werden konnte und dadurch weitere Installationsschritte beeinflusst wurden. Manuell wurde der Port auf 82 geändert. Wie bereits erklärt, wurden beim Installationsvorgang kleine Konfigurationspakete erstellt, die ebenfalls auf dem System installiert werden und somit hat sich die nicht funktionierende Verbindungseinstellung weiterhin fortgesetzt. Für das Beheben des Problems mussten einige der Installationen erneut durchgeführt werden. Bestimmte Einstellungen, die den Kommunikations-Port betreffen, mussten mühsam und zeitaufwändig lokalisiert und manuell geändert werden. Abbildung 30 zeigt die konfigurierte Management Konsole.

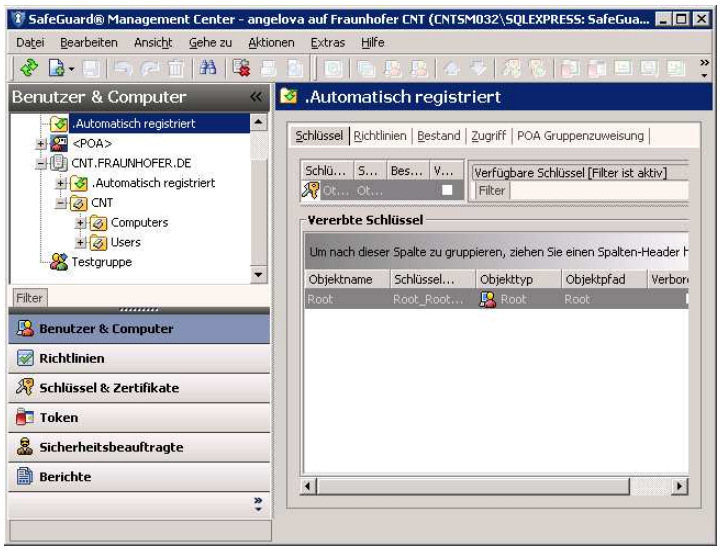


Abbildung 30. SGN: Management-Konsole

Die Erstellung bzw. Verwaltung von Zertifikaten wird mit einer zusätzlichen Konsole realisiert (siehe Abbildung 31).

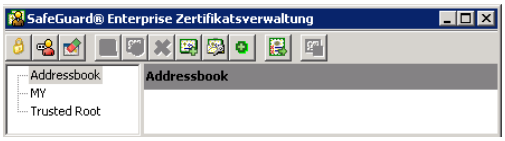


Abbildung 31. SGN: Zertifikatverwaltung

Nachdem der Test der Installation erfolgreich abgeschlossen wurde, sollte das Clientkonfigurationspaket nach den in Abbildung 29 aufgelisteten Schritten durchgeführt werden. Durch die Veränderung der Standardeinstellung mussten jedoch die bereits erstellten Installationspakete entsprechend angepasst und neu erzeugt werden, was wieder nur mit der Unterstützung des Sophos-Ansprechpartners gelang. Es wurde ein für Windows standardmäßiges MSI-Installationspaket für die Clientseite erzeugt, das über bereits existierende Unternehmensstrukturen an die Clientgeräte verteilt werden kann (z.B. NetInstall-Installer). Für die vorliegende Untersuchung wurde die Clientinstallation jedoch manuell durchgeführt.

Ein bestimmter Grund für die Kommunikationsstörung über Port 80 konnte nicht festgestellt werden.

10.2.3 Installieren eines Clients

Die Einrichtung der zu verwaltenden Clientgeräte wird nach dem in Abbildung 32 beschriebenen Schema durchgeführt. Es wurden manuell die benötigten MSI-Pakete installiert. Die gesamte Installation hat nur 7,50 MB auf der Festplatte in Anspruch genommen.

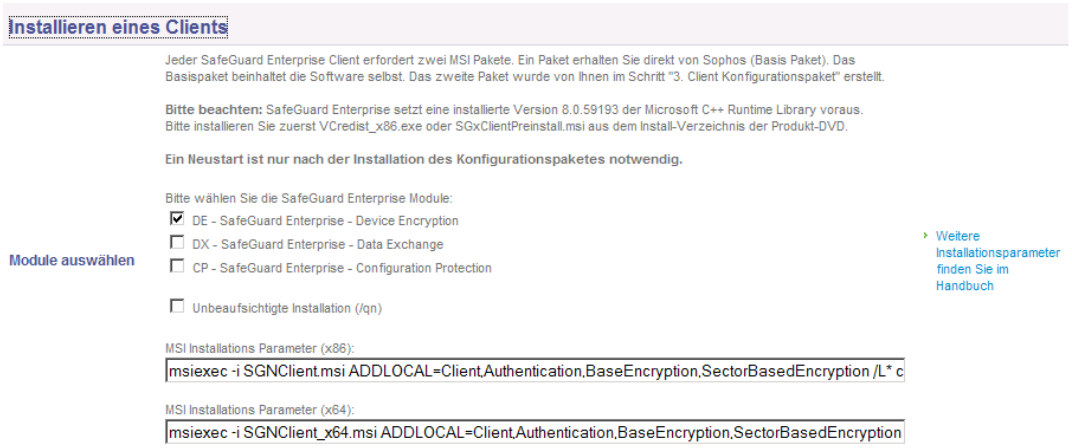


Abbildung 32. Installieren eines Clients

Nach der erfolgreichen Installation der Clientkonfigurationspakete wurde das System neu gestartet und folgende Ereignisse wurden beobachtet:

- Der Windows Startbildschirm wurde angezeigt.
- Bildschirmanzeige wechselte zu einer Ausschrift von Sophos (in diesem Moment wurde laut [sgn11d] der SGN-Kernel geschrieben) und einige Sekunden später startete das System automatisch neu, ohne dass Windows geladen wurde.
- Bei dem zweiten Neustart wurde kurz der Pre-Boot-Authentifikationsbildschirm von SGN gezeigt, da aber noch keine Systemverschlüsselung vorliegt, wurde man automatisch zur normalen Windows-Authentifikation weitergeleitet.
- Nach erfolgreichem Anmelden am Testrechner erschien das SGN-Symbol unten rechts in der Taskleiste.
- Abschließend wurde die Meldung angezeigt, dass die Benutzersynchronisation erfolgreich abgeschlossen ist – dies wurde durch die eingerichtete Kommunikation zwischen Server und Client ermöglicht.

Damit wurde das Einrichten von SafeGuard Enterprise abgeschlossen. In den nächsten Kapiteln wird die Funktionalität des Softwareprodukts im Kontext der vorliegenden Arbeit betrachtet.

10.3 Systemverschlüsselung

Ähnlich zu den anderen kommerziellen FDE-Lösungen werden auch in der SGN durch die zentrale Management-Konsole Richtlinien für die Verschlüsselung der Clientgeräte erstellt, den gewünschten Gruppen von Clientgeräten zugewiesen und durchgesetzt. Der Unterschied besteht jedoch in der Organisation der Richtlinien.

Bei SGN gibt es insgesamt 9 Richtlinientypen (siehe Rotmarkierung in der Abbildung 33).

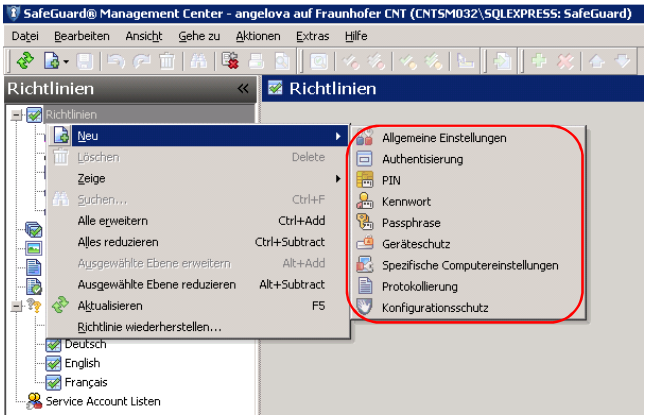


Abbildung 33. SGN Management Konsole – Richtlinienerstellung

Für die gewünschte Einstellungskonstellation werden entsprechende Objekte der jeweiligen Richtlinientypen erstellt, angepasst und der gewünschten Clientgruppe zugewiesen. Dabei werden für unterschiedliche Verwaltungsziele unterschiedliche Kombinationen von Richtlinienobjekten benötigt. In diesem Abschnitt wird die Zusammenstellung von Richtlinien und Optionen betrachtet, die zu der gewünschten Systemverschlüsselung des Testgeräts geführt haben. Für weitere Details bezüglich der Richtlinientypen wird auf die Produktdokumentation verwiesen (siehe [sgn11c]).

Für die Systemverschlüsselung (ohne Recovery- und Kennwort-Einstellungen) wurden 2 der Richtlinien eingestellt und dem Testclient zugewiesen – „Authentisierung“ und „Geräteschutz“, die im Folgenden detailliert betrachtet werden.

Um die wesentlichen Punkte nicht mit unnötigen Details zu überfrachten, wird nur auf die wichtigsten Konfigurationen eingegangen. Alle weitere Einstellungsmöglichkeiten und ihre Bedeutung können aus der Dokumentation entnommen werden (siehe [sgn11c]).

- Richtlinie zur Authentisierung:

  Es wird ein neues Objekt, der Authentisierungsrichtlinientyp, erzeugt. Abbildung 34 zeigt das erstellte Objekt und die möglichen konfigurierbaren Felder. Die rot markierten Optionen sind die für die Verschlüsselung relevanten Konfigurationseinstellungen. Es wird festgelegt, ob der Nutzer von der internen Festplatte aus das System booten darf und welche Authentifikationsmöglichkeiten für die POA genutzt werden können (kombiniert oder einzeln, siehe Abschnitt 10.4.2).

  Alle weiteren Konfigurationseinstellungen sind selbsterklärend und von keiner bzw. geringer Relevanz für die durchgeführte Untersuchung und werden nicht weiter betrachtet.

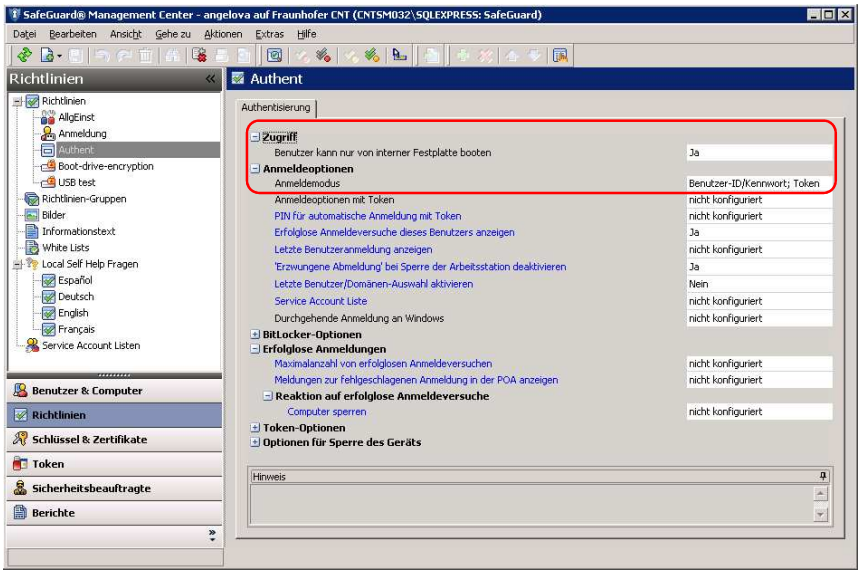


Abbildung 34. Richtlinienobjekt zur Konfiguration der Authentifizierung

- Richtlinie zum Geräteschutz:

  Es wird ein neues Objekt, der Geräteschutzrichtlinientyp, erzeugt. Dabei wird dieser Richtlinientyp, je nach zu verschlüsselndem Speichermedium, weiter unterteilt (siehe Abbildung 35). Für die Systemverschlüsselung wurde die Option „Boot-Laufwerke“ unter „Lokale Datenträger“ → „Massenspeicher“ ausgewählt.

  Bemerkung: Der Testclient hat nur ein Laufwerk, das gleichzeitig das Boot-Laufwerk ist. Somit reicht die Geräteschutzrichtlinie zur Verschlüsselung des Boot-Laufwerks für die Verschlüsselung der gesamten Festplatte. Hat jedoch die Festplatte weitere Partitionen, müssen diese durch eine zusätzliche Richtlinie vom Typ „Andere Volumes“ unter „Lokale Datenträger“ → „Massenspeicher“ verschlüsselt werden, um eine *Full Disk Encryption* zu erreichen!

Abbildung 35. SGN: Geräteschutzrichtlinie je nach Speichermedium erstellen

Abbildung 36 zeigt das erstellte Richtlinienobjekt und die möglichen konfigurierbaren Felder, wobei die relevanten Optionen rot markiert sind. Als Verschlüsselungsalgorithmus steht nur AES mit einer Schlüssellänge von 128 bzw. 256 Bit zur Verfügung. Es wurde AES mit 256 Bit festgelegt (einheitliche Einstellung bei allen untersuchten FDE-Lösungen). Weiterhin wurde die Verschlüsselung der Festplatte durch der Richtlinie erzwungen (durch „alle Medien akzeptieren und verschlüsseln“).

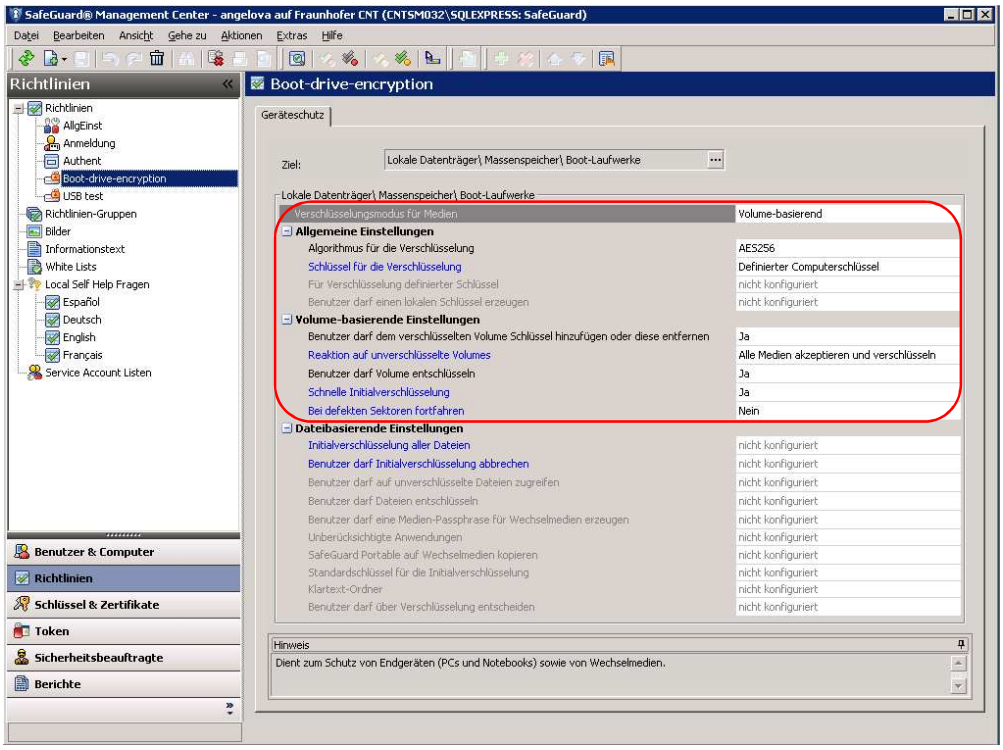


Abbildung 36. SGN Richtlinienkonfiguration zur Systemverschlüsselung

Die Richtlinien können jeder Zeit bearbeitet werden, die Durchsetzung bzw. der Datenabgleich zwischen Client und Server für die regelmäßige Aktualisierung der Richtlinien kann ebenfalls durch eine Richtlinie eingestellt werden (Richtlinientyp „Allgemeine Einstellungen“) oder auf der Client- bzw. Serverseite manuell durchgeführt werden.

Sobald die Richtlinien eingerichtet sind, wurden sie dem Clientgerät zugewiesen. Dazu wurde unter „Benutzer & Computer“ die Organisationseinheit aus dem Unternehmensverzeichnis ausgewählt, die den Testclient beinhaltet (siehe Abbildung 37). Unter der Registrierkarte „Richtlinien“ können die erstellten Richtlinien durch „Drag & Drop“ (siehe Rotmarkierung in der Abbildung 37) hinzugefügt werden.

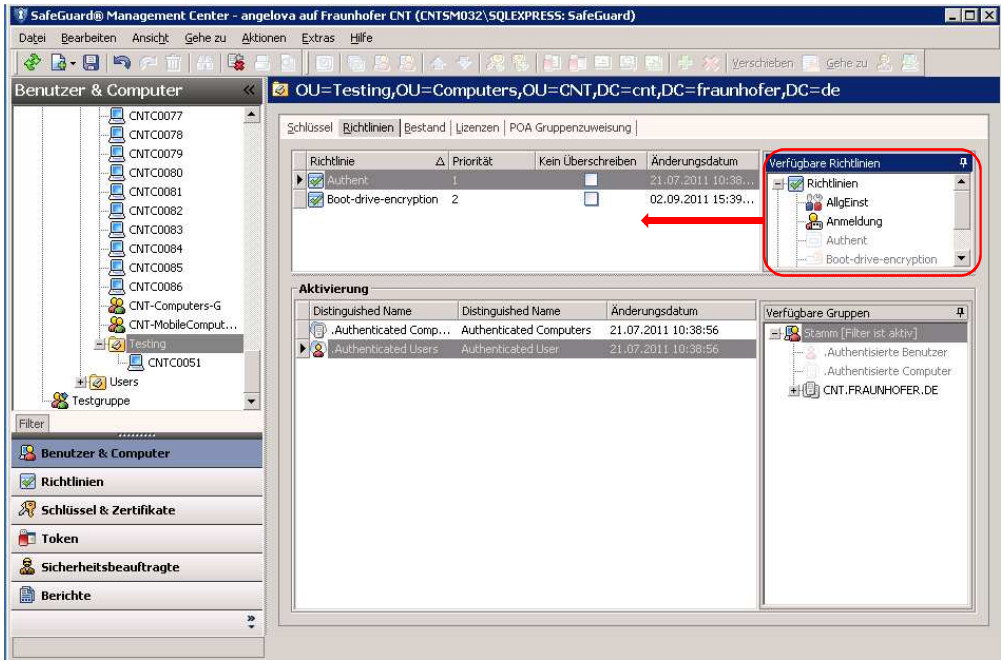


Abbildung 37. SGN Verwaltung: Richtlinienzuweisung

Durch Zuweisung der gewünschten Richtlinien in der Verwaltungseinheit fing auf der Clientseite nach Anmeldung der eingerichteten Benutzer automatisch die Verschlüsselung des Systems an. Es wurde eine Statusanzeige mit dem Verschlüsselungsfortschritt angezeigt.

Der Verschlüsselungsvorgang sollte in keiner Weise die Arbeit an dem Rechner behindern, es ist jedoch mit Geschwindigkeitseinbußen zu rechnen (durch die CPU-Auslastung). Um die Dauer der Verschlüsselung realistisch messen zu können, wurde der Rechner während des Prozesses nicht anderweitig genutzt. Der gesamte Vorgang dauerte insgesamt 48 Minuten und wurde mit einer Meldung zur erfolgreichen Systemverschlüsselung abgeschlossen.

10.4 Weitere getestete Funktionen und Möglichkeiten des Produkts

10.4.1 Verschlüsselung von Wechselmedien

SGN bietet 4 Optionen für den Umgang mit unverschlüsselten Wechselmedien mittels Richtlinienanpassung. Dabei kann die Verschlüsselung von externen Speichermedien nur durch die Verwaltungskonsole eingeleitet werden. Der Endbenutzer darf höchsten Wechselmedien entschlüsseln, falls sie bereits durch SafeGuard verschlüsselt sind (siehe Abschnitt 10.4.5).

Es wird zuerst eine Richtlinie für externe Speichermedien erstellt. Dafür wird die Option „Wechselmedien“ unter „Lokale Datenträger“ → „Massenspeicher“ ausgewählt (siehe Abbildung 35). Die Datenträger werden anforderungsgemäß Volume-basierend mit AES-256 verschlüsselt. Folgende Konfigurationsmöglichkeiten (siehe Rotmarkierung in der Abbildung 38) stehen bezüglich der Reaktion des Clientgeräts auf unverschlüsselte externe Laufwerke zur Verfügung:

- *Nicht konfiguriert:* Endbenutzer kann wie gewohnt auf unverschlüsselten Laufwerken lesen und schreiben, ohne die Daten durch Verschlüsselung jeglicher Art zu schützen.
- *Abweisend:* Externe Laufwerke werden nicht verschlüsselt und sind mit Lese- und Schreibsperre versehen.
- *Nur leere Medien akzeptieren und verschlüsseln:* Leere Speichermedien werden automatisch und benutzertransparent verschlüsselt. Alle weiteren Speichermedien werden mit Lese- und Schreibsperre versehen.
- *Alle Medien akzeptieren und verschlüsseln:* Alle externen Speichermedien werden beim Anschließen an das Clientgerät automatisch und benutzertransparent verschlüsselt.

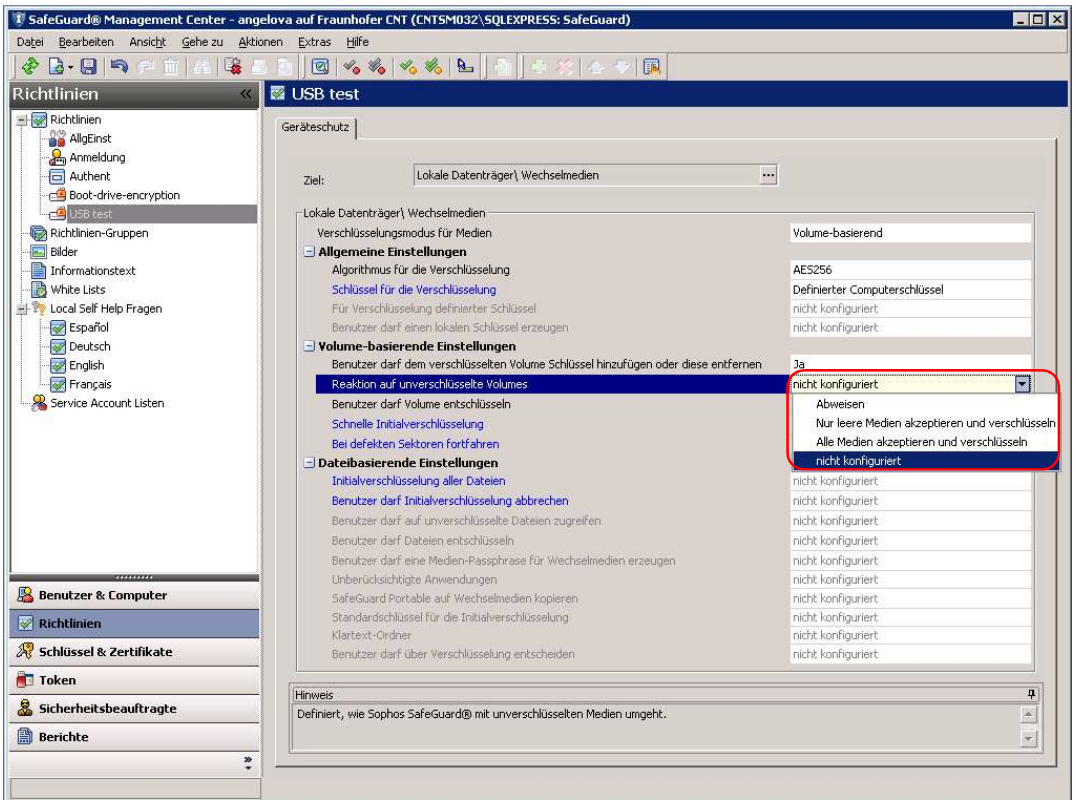


Abbildung 38. SGN Richtlinienkonfiguration zur Verschlüsselung von Wechselmedien

Alle beschriebenen Optionen wurden mit einem 2 GB großen USB-Stick getestet und funktionieren einwandfrei und wie vom Anbieter angegeben. Beim Abbruch des Verschlüsselungsvorgangs ist mit einem möglichen Datenverlust zu rechnen, falls auf dem Speichermedium Daten vorhanden sind. Bei der Untersuchung wurden Abbrüche des Vorgangs absichtlich simuliert und keine Datenverluste festgestellt. Nach Wiederanschließen des externen Laufwerks wurde der Verschlüsselungsvorgang fortgesetzt. Während des Verschlüsselungsvorgangs wurde eine spürbare Verlangsamung bei der Nutzung des Systems festgestellt. Nach erfolgreicher Verschlüsselung ist keine Authentifikation für die Nutzung der Daten nötig, solange die SGN-Software auf dem Client installiert und entsprechend eingestellt ist. Das verschlüsselte Speichermedium wurde von anderen Rechnern als unformatierter Wechseldatenträger erkannt.

Weiterhin bietet die Management-Konsole von SGN für den Umgang mit Wechselmedien die Richtlinie „Konfigurationsschutz“, die unter anderem die Kommunikation über USB-Ports sowie weitere Schnittstellen des Clientgeräts sperren bzw. einschränken kann (diese Optionen liegen jedoch außerhalb des Zieles der vorliegenden Arbeit und werden nicht weiter betrachtet).

10.4.1.1 Datenspuren auf verschlüsselten Wechseldatenträgern

Es wurde eine Text-Datei auf dem verschlüsselten Wechseldatenträger mit dem Namen „Test.txt“ und dem Inhalt – „Das ist eine Testdatei“ erstellt. Anschließend wurde der USB-Stick vom Rechner entfernt und auf einem Rechner ohne installierte SGN eingesteckt. Der Inhalt des Datenträgers wurde mit Hilfe des Programmes WinHex 16.1 nach der Textdatei, sowie nach Zeichenketten, die den Namen der Datei, deren Inhalt oder Teilen davon (wie z.B. „Das ist“) durchsucht. Alle Tests hatten keine Treffer zur Folge. Weiterhin wurde das verschlüsselte Speichermedium nach Hinweisen für die Benutzung von SGN untersucht und es konnten ebenfalls keine Informationen darüber gefunden werden.

Der Wechseldatenträger wurde erneut an dem SGN-Client angesteckt und die Tests mit WinHex wurden wiederholt. In diesem Fall konnte, wie erwartet, die Datei und deren Inhalte anhand der angegebenen Zeichenketten gefunden werden.

Der USB-Stick wurde einschließlich von Windows formatiert. Die Tests wurden erneut wiederholt und führten zu negativen Ergebnisse – es konnten keine Datenspuren und keine Hinweise für die Benutzung von SGN nachgewiesen werden.

10.4.2 Pre-Boot-Authentifikation

Falls die Smartcard-Authentifikation erlaubt werden sollte, müssen die entsprechenden Einstellungen in der „Authentisierung“ Richtlinie eingerichtet werden. Es können auch weitere Konfigurationen zur feineren Verwaltung von Smartcard-Benutzern durchgeführt werden. Da, wie bereits erklärt, der Einsatz von Smartcards für die Pre-Boot-Authentifikation aufgrund der Testumgebung nicht funktioniert (siehe Abschnitt 9.3.2), wird diese Option nicht weiter betrachtet. Sie sollte jedoch bei erfüllten

technischen Voraussetzungen als zusätzliche oder als einzige Authentifikationsoption in die Unternehmensstruktur integriert und verwendet werden können.

Sobald der Unternehmensverzeichnisdienst in die Management-Konsole integriert ist und die benötigten Zertifikate verteilt sind, steht für die Pre-Boot-Authentifikation der Single-Sign-On mittels der existierenden Windows-Konten der Benutzer zur Verfügung. Für die Aktivierung muss in der Richtlinie „Authentisierung“ als Anmeldeoption – „Benutzer ID/ Kennwort“ ausgewählt werden (siehe Rotmarkierung in der Abbildung 34). Zusätzlich könnte man eine Richtlinie für die Anforderungen an ein zu vergebendes Kennwort erstellen und durchsetzten, falls keine bereits existierenden Unternehmensrichtlinien dazu vorhanden sind[25] (siehe Abbildung 39).

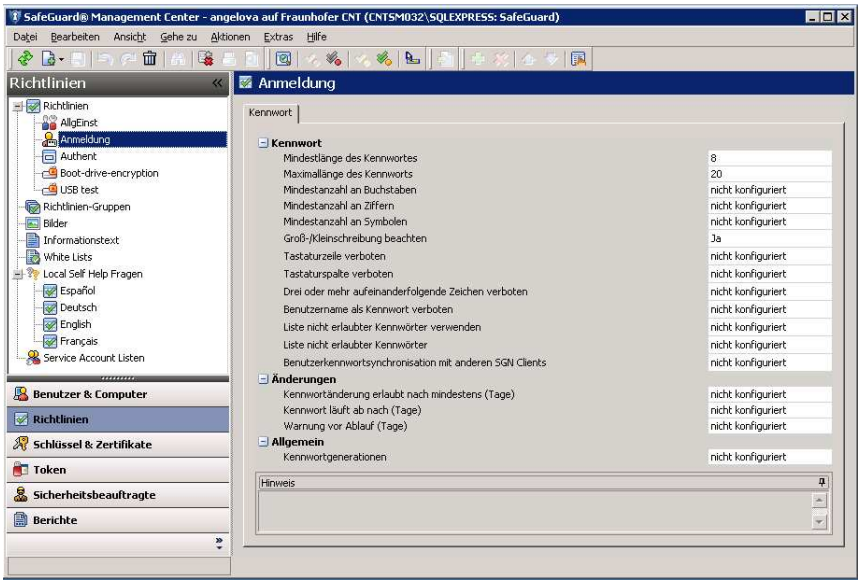


Abbildung 39. SGN Richtlinienkonfiguration für optionale Kennworteinstellungen

10.4.3 Passwortwiederherstellungsstrategien

In diesem Abschnitt werden die von SGN angebotenen Passwortwiederherstellungs-strategien betrachtet. Dabei handelt es sich um die Verfahren „Local Self Help“ (siehe Abschnitt 10.4.3.1) und „Challenge/ Response“ (siehe Abschnitt 10.4.3.2).

[25] In der Testumgebung sind Richtlinien zu Kennwortanforderungen bereits vorhanden.

Damit überhaupt eine Passwort-Recovery durchgeführt werden kann, muss sie zuerst durch die zentrale Verwaltungseinheit zugelassen werden. Beide Verfahren können durch die Instanz des Richtlinientyps „Allgemeine Einstellungen“ aktiviert werden (siehe Abbildung 40).

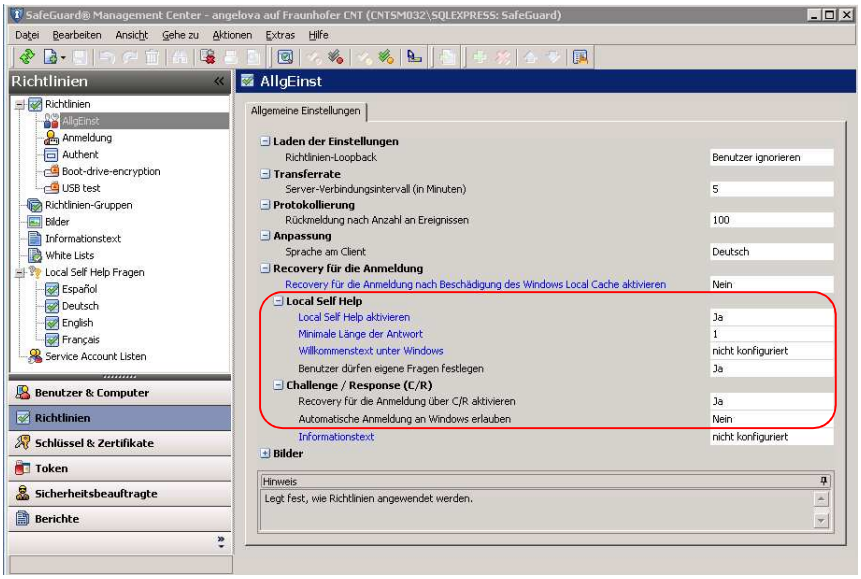


Abbildung 40. Richtlinienobjekt zur Konfiguration der allgemeinen Einstellungen

Für weitere Details bezüglich des genauen Anmeldevorgangs mittels „Local Self Help“ und „Challenge/ Response“ wird auf [sgn11e] verwiesen.

10.4.3.1 Local Self Help

Der Vorgang ist intuitiv und wird durch einen Einstellungsassistenten (siehe Abbildung 41) unterstützt. Der Benutzer wird aufgefordert 10 Sicherheitsfragen zu erstellen und entsprechend zu beantworten. Die Fragen kann man aus einer Liste von vorbereiteten Standardfragen auswählen bzw. selbst entwerfen. Falls der Benutzer sein Passwort vergisst, hat er in der Pre-Boot-Authentifikationsanzeige die Option, die Sicherheitsfragen zu beantworten (unter „Recovery“ → „Local Self Help“). Nach der erfolgreichen Beantwortung der Fragen kann sich der Benutzer sein Passwort für 5 Sekunden anzeigen lassen und wird danach automatisch an dem verschlüsselten Gerät angemeldet. Die Wiederherstellung durch die Sicherheitsfragen wurde ebenfalls getestet und funktionierte einwandfrei und erwartungsgemäß.

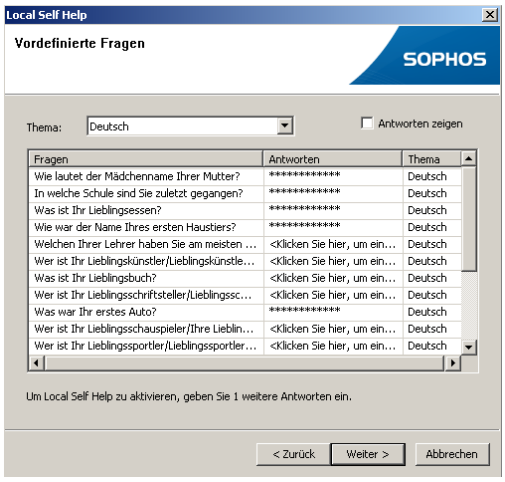


Abbildung 41. SGN: Local Self Help

10.4.3.2Challenge/Response

Die zweite Passwortwiederherstellungsmöglichkeit ist die so genannte Challenge/Response – Passwortwiederherstellungsstrategie. Dafür wählt der Benutzer bei dem Pre-Boot-Authentifikationsverfahren „Recovery“ → „Challenge/ Response“ aus und bekommt einen 30-stelligen Challenge-Code angezeigt, der innerhalb von 30 Minuten dem Administrator mitgeteilt werden soll. Der Administrator öffnet in der Management-Konsole den Recovery-Assistenten unter „Extras“ → „Recovery“ und wählt Gerät und Benutzer für die Wiederherstellung aus. Danach wird er aufgefordert den Challenge-Code des Benutzers anzugeben. Falls der Code auf Client- und Managementseite übereinstimmt, wird ein Response-Code vom Recovery-Assistenten generiert. Dieser Kode muss innerhalb von 30 Minuten dem Benutzer mitgeteilt werden. Sobald der Benutzer den Response-Code angibt, wird er automatisch an dem Rechner angemeldet.

Der gesamte Vorgang wurde getestet und ist einwandfrei und nach den Angaben des Anbieters verlaufen. Die Assistenten auf der Client- und Managerseite sind sehr schlicht und verständlich aufgebaut und erlauben eine intuitive Durchführung des Wiederherstellungsprozesses.

10.4.4 Ressourcenbelegung

Es wurden mehrere Messungen zum Ermitteln der CPU- und RAM- Belastung sowie der Kopier-, Schreib-, Lesezugriffsgeschwindigkeit bzw. –zugriffszeit für verschiedene Dateigrößen auf dem mit SGN verschlüsselten Testrechner durchgeführt. Ziel der Messungen war, diese Größen bei den mit den unterschiedlichen FDE-Lösungen verschlüsselten Rechnern sowie einem unverschlüsselten Testsystem zu vergleichen. Details über die durchgeführten Messungen, die Ergebnisse und ihre Auswertung werden in Abschnitt 12 betrachtet.

10.4.5 System-Partition/ Laufwerk bzw. externe Wechselmedien dauerhaft entschlüsseln

Für die Entschlüsselung von System-Partition, anderen Laufwerken bzw. Wechselmedien wird die gleiche Vorgehensweise genutzt. Die Entschlüsselung erfolgt nur lokal und wird vom Benutzer gestartet, insofern das durch die zentral verwalteten Richtlinien erlaubt ist. Dafür muss entweder eine neue Instanz, der Geräteschutz-Richtlinientyp, erstellt und dem Client zugewiesen werden oder die bereits existierenden entsprechend angepasst werden. Folgende Einstellungen müssen gemacht werden (siehe Rotmarkierung in der Abbildung 36):

- Verschlüsselungsmodus für Medien muss auf „keine Verschlüsselung“ gesetzt werden.
- Die Option „Benutzer darf Volume entschlüsseln“ muss auf „Ja“ gesetzt werden.

Nur beide Einstellungen in Kombination erlauben die Entschlüsselung der entsprechenden Speichermedien durch den Benutzer!

Die Entschlüsselung wird gestartet indem unter dem Windows Explorer das zu entschlüsselnde Speichermedium mit der rechten Maustaste ausgewählt wird. Dann kann unter „Verschlüsselung“ → „Entschlüsseln“ ausgewählt werden, womit der Entschlüsselungsvorgang gestartet wird (siehe Abbildung 42). Der Vorgang kann nicht ohne Weiteres vom Benutzer abgebrochen oder rückgängig gemacht werden.

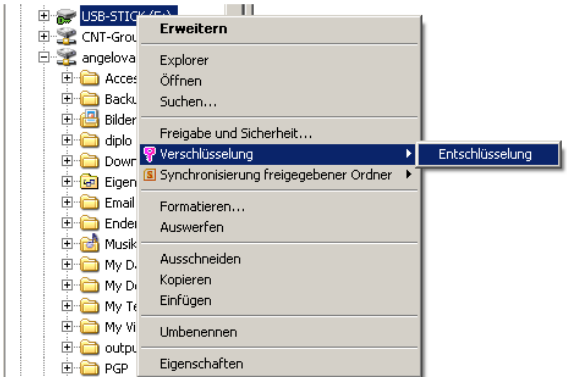


Abbildung 42. SGN: Entschlüsseln von Speichermedien

Der Zeitaufwand für die Entschlüsselung des getesteten Systems war mit dem für die Verschlüsselung vergleichbar. Der Prozess verläuft im Hintergrund und erlaubt den Nutzern während des Entschlüsselungsvorgangs weiter an dem Rechner zu arbeiten, wobei mit Verzögerungen[26] bei Anwendungen mit großer CPU-Belastung zu rechnen ist.

10.5 Anmerkungen und Zusammenfassung

Das von Sophos angebotene Produkt bietet eine professionelle FDE-Lösung für den Unternehmenseinsatz. Durch die modulare Struktur der Software kann das Funktionalitätsspektrum des Produkts ohne großen Aufwand erweitert werden. Es wird eine umfangreiche und komplexe Verwaltungseinheit für die Unternehmensstruktur angeboten. Durch unterschiedliche Richtlinientypen und ihre Einstellungen, kann eine feingranulare und exakte Steuerung der Clientgeräte und Endnutzereinstellungen erreicht werden. Weiterhin ist ein umfangreiches Angebot an Produktdokumentationen in Form von Dokumenten, Videotutorials und Webinars (Online-Seminare) sowohl für Administratoren als auch für Benutzer vorhanden.

Folgende Bemerkungen bezüglich des Umgangs mit dem Produkt und der durchgeführten Untersuchungen sind noch wichtig:

- Während der Testphase der Software wurde die Erfahrung gemacht, dass bei Problemen mit dem Einrichten bzw. der Funktionalität der Software eine

[26] Die Verzögerung der Arbeitsprozesse während der Ver- bzw. Entschlüsselung des Systems wurde nicht getestet, damit der Zeitaufwand für die beiden Vorgänge nicht beeinflusst wird.

kompetente und schnelle Unterstützung durch den Produktanbieter gewährleistet wird.

- Die Benutzeroberfläche der Management-Konsole ist durch viele Details unnötig überlastet und führt zur Unübersichtlichkeit. Die gesamte Navigation des GUI wurde als verwirrend und an bestimmten Stellen sogar als irreführend empfunden. Eine kontextsensitive Hilfe zur Unterstützung der Navigation ist nicht vorhanden.

- Die granulare Struktur der Richtlinien ermöglicht zwar eine feinere Steuerung der Endgeräte, führt jedoch wieder zu Navigationsproblemen und zur zeitaufwändigen Suche nach bestimmten Einstellungen.

- Die Verwaltung von Benutzern und Geräten wurde bei der Ersteinstellung als sehr umständlich und zeitaufwändig bewertet.

- Bei kommerziellen Verschlüsselungsprodukten besteht immer die Gefahr, dass einen Masterkey vorhanden ist. Es ist nicht überprüfbar, welche Hintertüren in dem Sourcecode möglicherweise eingebaut sind.

11 McAfee Endpoint Encryption (EE)

In diesem Abschnitt wird die kommerzielle FDE-Lösung Endpoint Encryption des Sicherheitsunternehmens McAfee betrachtet. Neben einem ausführlichen Überblick über die Funktionen, Möglichkeiten und Grenzen des Produkts, wird es systematisch nach den festgelegten Vergleichskriterien und unter Beachtung der vorgestellten Randbedingungen untersucht. Abschließend werden einige Bemerkungen zum Produkt gemacht und die ermittelten Ergebnisse zusammengefasst.

Die Organisationsstruktur der von McAfee angebotenen FDE-Lösung für den Unternehmenseinsatz weist eine verschachtelte modulare Struktur auf. Es werden ähnlich zum Produkt von Symantec getrennte Softwareprodukte für die Clientseite (*EE - Endpoint Encryption*) und die zentrale Verwaltungseinheit (*ePO – ePolicy Orchestrator*) angeboten, die einzeln vermarktet und erworben werden sollen. Auf der Serverseite wurde in der konkreten Untersuchung die Verwaltungseinheit eingerichtet (ähnlich zu SGN). Weiterhin besteht *Endpoint Encryption* (Clientseite) aus vielen kleineren Softwarepaketen, wobei die benötigte Zusammenstellung individuell je nach Bedarf des Kunden erstellt bzw. angewendet wird. Für die vorliegende Untersuchung wurde folgende Produktkonstellation eingerichtet und getestet:

McAfee ePolicy Orchestrator (ePO) – stellt die zentrale Management-Konsole dar.

Endpoint Encryption (EE):

- *Endpoint Encryption for PC (EEPC)* – Verschlüsselungssoftware für Windowsbenutzer, die auch als Standalone-Lösung für einzelne Geräte genutzt werden kann.
- *McAfee Endpoint Encryption for Files and Folders (EEFF)* – enthält unter anderem das Feature *McAfee Endpoint Encryption for Removable Media (EERM)*, das für die Verschlüsselung von Wechseldatenträgern eingesetzt wird.

11.1 Übersicht – Funktionsumfang

11.1.1 ePolicy Orchestrator (ePO)

Die Beschreibung des Produktaufbaus und seiner Einzelteile orientiert sich an dem ePO – Datenblatt (siehe [mc111]).

ePO in der aktuellen Version 4.6 umfasst unter anderem[27] folgende Funktionalitäten:

- ePO stellt die Kernkomponente der McAfee Sicherheitsmanagement-Plattform dar. Es ermöglicht die zentrale Verwaltung von Endgeräten, Netzwerken, Daten und Compliance-Lösungen durch eine einzige zentralisierte, webbasierte Verwaltungskonsole. Dabei können weitere Sicherheitsanwendungen jederzeit hinzugefügt bzw. entfernt werden.
- Automatisierte zentrale Richtlinienkonfiguration und –ausbringung, z.B. Durchsetzung einer Richtlinie zur automatisierten Verschlüsselung der Client-Festplatte bei der nächsten Anmeldung des Benutzers.
- Wiederherstellungsstrategien von Passwörtern und verschlüsselten Daten im Unternehmen.
- Integration in den vorhandenen Unternehmensverzeichnisdienst.
- Festlegen der Funktionen, die die Benutzer am Client-PC sehen bzw. ausführen können.
- Ausführliche Berichterstattung und Protokollierung von Systemereignissen, vom Verschlüsselungsstatus der Clients, von fehlgeschlagenen Benutzeranmeldungen uvm.

[27] *McAfee ePO* ist ein mächtiges Werkzeug zum Verwalten von mehreren Sicherheitsanwendungen. Aus diesem Grund werden hier nur die wichtigsten und für die zum Thema der vorliegenden Diplomarbeit relevanten Funktionen betrachtet. Für weitere Details wird auf die Dokumentation des Produkts verwiesen (siehe [mc511]).

- Anpassbare Vorlagen (über Laufzeitparameter für unterschiedliche Benutzergruppen) zur Definition von Berichterstellungen.
- Erstellen und Verwalten von Administratoren mit unterschiedlichen Verantwortungsbereichen.
- *Rogue System Detection* zur Erkennung unbekannter Systeme, die ans Netzwerk angeschlossen werden.

11.1.2 Endpoint Encryption

Der Aufbau des Produktes und seiner Einzelteile wurde entsprechend den Informationen aus dem EE - Datenblatt beschrieben (siehe [mc211]). Es werden die Komponenten und ihre Funktionalität vorgestellt, die für die durchgeführte Untersuchungsreihe und die genutzte Testumgebung relevant sind.

Endpoint Encryption for PC (EEPC):

EEPC ist die Hauptkomponente von EE und ist speziell für Windows-Benutzer konzipiert. Das untersuchte Softwarepaket hat die aktuelle Version 6.1.0 und umfasst folgende Eigenschaften:

- Verschlüsselung und Verwaltung des gesamten Systems.
- Berichte zur Gewährleistung der Richtlinieneinhaltung: Computer-verschlüsselungsstatus, Warnhinweise zur fehlgeschlagenen Anmeldungen u.A.
- Mehrere Pre-Boot-Authentifizierungsoptionen (einzeln oder in Kombination anwendbar) : Pre-Boot-Smartcard, TPM- und „Single-Sign-On“-Unterstützung.
- Die EEPC stellt die Verschlüsselungskomponente dar, wobei die Verschlüsselung nur mittels AES-256 durchgeführt werden kann.
- EEPC unterstützt Prozessoren mit eingebautem AES-NI. Dadurch kann der Ver- bzw. Entschlüsselungsvorgang beschleunigt werden (hardwarebedingt).

- Die Architektur des Produkts erlaubt die Unterstützung von selbstverschlüsselnden Festplatten.
- Wiederherstellungsstrategien von Passwörtern und verschlüsselten Daten im Unternehmen.
- Verschlüsselung von SSD-Festplatten wird unterstützt.

Endpoint Encryption for Files and Folders (EEFF):

Das untersuchte Softwarepaket hat die aktuelle Version 4.0 und umfasst folgende Eigenschaften:

- verhindert den unbefugten Datenzugriff auf PCs, Laptops, Netzwerk-Servern und Wechselmedien.
- Schlüsselverwaltung für den gesicherten Datenaustausch zwischen Benutzern des Systems.
- Automatische Verschlüsselung von Dateien und Ordnern bei der Freigabe oder beim Verschieben innerhalb des Unternehmens.
- Erstellung von verschlüsselten selbstextrahierenden Daten, die auch unter Systemen geöffnet werden, auf denen keine EEFF-Installation vorhanden ist.
- Stellt die Produkterweiterung *McAfee Endpoint Encryption for Removable Media* (EERM) zur Verfügung. Dieses Feature ist für den Umgang mit Wechseldatenträgern zuständig.

Bemerkung: Von der recht umfangreichen Funktionalität des EEFF-Modules wird nur das für die vorliegende Arbeit relevante EERM-Feature weiter im Detail betrachtet.

11.2 Installation und Konfiguration der Server-Client Kommunikation

11.2.1 Installation und Einrichten der Serverseite

11.2.1.1 Installation der Serverseite

Die Installation und das Einrichten des ePO wurde auf einem von Fraunhofer CNT zur Verfügung gestellten, virtuellen Server (siehe Abschnitt 6.1.1) und unter Berücksichtigung der Softwaresystemvoraussetzungen (siehe [mc311]) durchgeführt.

Die Installation der Verwaltungseinheit[28] ist sehr schlicht und einfach gestaltet und verlief entsprechend der Installationsanleitung des Anbieters (siehe [mc411]). Der Vorgang wird komplett durch einen Installations-Assistenten begleitet, der die wichtigen Einstellungsaufgaben systematisch abarbeitet. Dabei wurden in der konkreten Testumgebung unter anderem die Datenbank eingerichtet (Instanz von Microsoft SQL Express – wie bei SGN) und ein globaler Administrator für ePO erstellt.

11.2.1.2 Einrichten der Serverseite und der Client-Server Kommunikation

Auf ePO kann genau wie auf die Verwaltungseinheit von Symantec über die Browser-Schnittstelle von jedem Rechner aus zugegriffen werden, der an das interne Netzwerk angeschlossen ist. Für den Aufruf muss der vollständige Servername auf dem Port 8443 angegeben werden. In dem konkreten Fall wird der Server durch die absolute Adresse https://cntsm032.cnt.fraunhofer.de:8443/ (CNTSM032 ist der konfigurierte Name des eingerichteten virtuellen Servers) aufgerufen. Dabei kann die Verwaltungskonsole auf Deutsch oder Englisch mit der entsprechenden Übersetzung des GUI gestartet werden.

McAfee bietet eine „Geführte Konfiguration“ des Servers an, die zu jedem Zeitpunkt durchgeführt bzw. fortgesetzt werden kann. Sie stellt eine Schritt-für-Schritt Anleitung, wie man die wichtigsten Aufgaben und Einstellungen für die Client-Server-Kommunikation einrichtet, dar. Mit Hilfe dieses Tools wurden unter anderem die

[28] Es handelt sich dabei um die Standardinstallation. ePO bietet auch weitere Installationsmöglichkeiten, die für die vorliegende Arbeit irrelevant sind.

entsprechenden Module für die verwalteten Client- und Wechselmedienverschlüsselungen in ePo integriert (EEPC & EEFF), die LDAP Synchronisation durchgeführt und die Unternehmensverzeichnisdienststruktur übernommen. Zusätzlich zu der geführten Konfiguration wurden für die korrekte Einrichtung folgende weitere Hilfsmittel benutzt: die kontextsensitive Hilfe, die in ePO integriert ist und unter dem  -Symbol zur Verfügung steht, sowie die *Quick Start Guides* (siehe [mc611] und [mc711]) und die Installationsanleitungen für die Einrichtung von EEPC- und EEFF-Softwarepaketen.

Zusammenfassend war die Einrichtung des Servers und der Client-Server Kommunikation zwar komplex, lies sich aber durch die genannten Hilfsmittel sehr organisiert durchführen. Folgende Besonderheiten sind dabei nennenswert:

- Die LDAP Synchronisation wird beim ePO anders als bei den anderen betrachteten kommerziellen Management-Konsolen organisiert. Es wird dabei ein neuer registrierter LDAP-Server erzeugt, dem die konkreten Unternehmensdaten zugewiesen werden. Das Prinzip und die Funktionalität dahinter sind jedoch dieselben.

- Der Unternehmensverzeichnisdienst wird wie bei den anderen betrachteten kommerziellen Produkten in die Verwaltungseinheit integriert. Richtlinien können jedoch einzelnen Benutzern, einzelnen Geräten oder ganzen Organisationseinheiten zugewiesen werden.

  Bemerkung: Zum Vergleich – bei PGP WDE wurden die verwalteten Benutzer und Endgeräte automatisch bei der Erstnutzung am Server registriert und bei SGN konnte man Richtlinien nur an Organisationseinheiten zuweisen.

- Im Gegensatz zu den PGP WDE und SGN wurde bei dem Produkt von McAfee auf der Serverseite kein Clientinstallationspaket erstellt (entspricht der Produktarchitektur) sondern die entsprechenden Modulpakete integriert. Für die Clientseite gibt es standardisierte MSI-Installationspakete, die durch ePO (mittels „Client Tasks“) oder durch bereits existierende Unternehmensstrukturen an die Clientgeräte verteilt werden können (z.B. NetInstall-Installer). Für die

vorliegende Untersuchung wurde die Clientinstallation jedoch manuell durchgeführt.

- Sobald das gesamte System eingerichtet ist, bietet ePO eine anpassbare Systemübersicht, genau wie bei PGP WDE – es werden die verwalteten Systeme angezeigt, ihr Verschlüsselungsstatus, unterschiedliche Protokolle und Statistiken uvm. Abbildung 43 zeigt die Verschlüsselungsübersicht der verwalteten Testumgebung nach erfolgreicher Systemverschlüsselung.

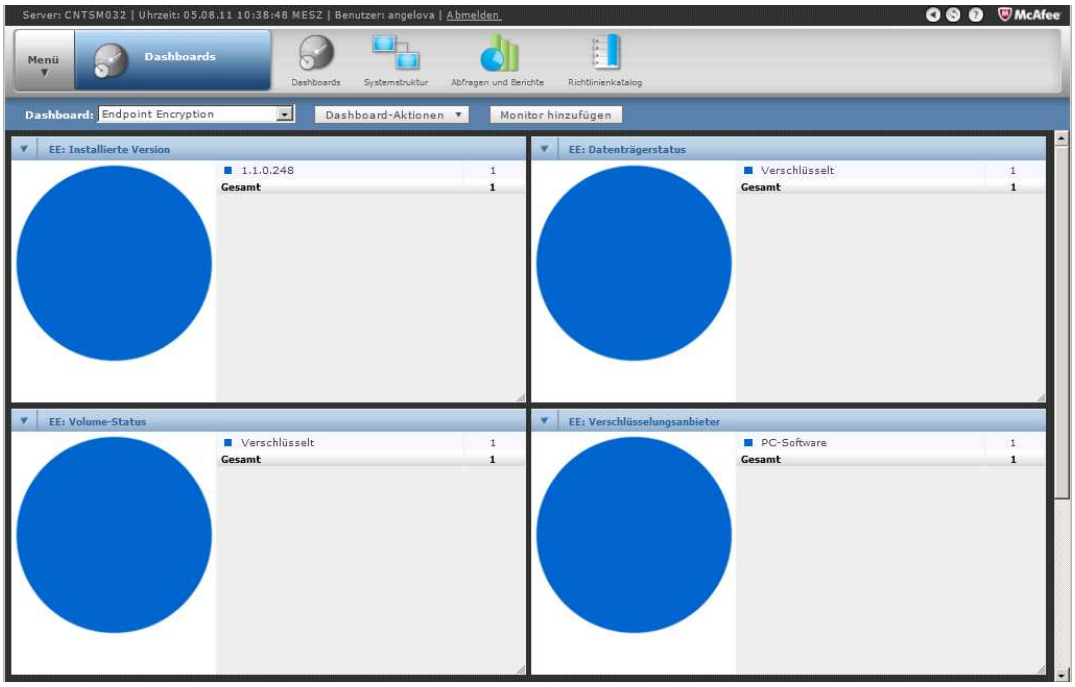


Abbildung 43. ePO 4.6 - Übersicht des verwalteten Systems

11.2.2 Installation und Einrichten der Clientseite

Auf der Clientseite wurden die Installationspakete für den Kommunikationsagent (Endpoint Encryption Agent – für die Server-Client Kommunikation) und für die System- und Wechseldatenträgerverschlüsselung installiert (EEPC- und EEFF-Clientseite). Die gesamte Installation hat 66,4 MB auf der Festplatte in Anspruch genommen. Der Rechner wurde neu gestartet, um den Installationsvorgang zu vollenden. Nach dem Neustart erschien das -Taskleistensymbol von McAfee, das

unter anderem, eine EE-Statusabfrage ermöglicht (siehe Abbildung 50). Weiterhin ist das EEFF-Clientverwaltungsmenü aufrufbar (siehe Abbildung 44).

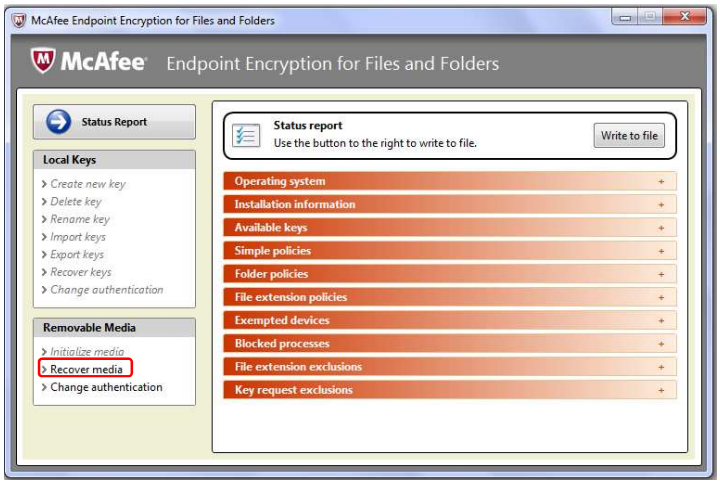


Abbildung 44. McAfee EEFF 4.0 Clientverwaltungsmenü

Damit wurde das Einrichten der McAfee FDE-Lösung abgeschlossen. In den nächsten Kapiteln wird die Funktionalität des Softwareprodukts im Kontext der vorliegenden Arbeit betrachtet.

Bemerkung: McAfee EE war das erste untersuchte Produkt der kommerziellen FDE-Lösungen. Die gesamte Installation und Einrichtung verlief reibungslos und entsprechend den Anbieterangaben. Nichtsdestotrotz war sie mit einem großen Zeitaufwand verbunden. Gründe dafür waren unter anderem die ersten praktischen Erfahrungen mit der konkreten IT-Unternehmensinfrastruktur und der Integration einer komplexen Software (Einrichten von Server-Client-Kommunikation, Arbeiten mit Richtlinien u.Ä.).

11.3 Systemverschlüsselung

Die Systemverschlüsselung wird von der FDE-Lösung von McAfee, genau wie bei den anderen betrachteten kommerziellen Produkten, mittels Richtlinien realisiert. Für die Einrichtung der Verschlüsselung bietet EEPC zwei Richtlinien, die entsprechend eingestellt werden sollten – „Produkteinstellungen“ und „Benutzerbasierte Richtlinie“ (siehe Abbildung 45).

Abbildung 45. McAfee EEPC: Richtlinien

Produkteinstellungen:

Die Richtlinie ist sehr einfach und übersichtlich in Registrierkarten strukturiert. Abbildung 46 und Abbildung 47 zeigen die wichtigsten Optionsfelder bei der Einstellung der Richtlinie (alle anderen Registrierkarten sind im Anhang B: McAfee EEPC: Richtlinien abgebildet).

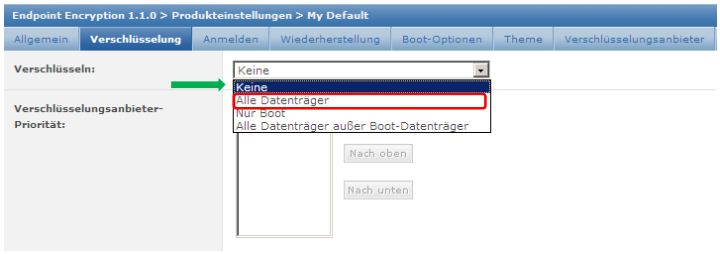


Abbildung 46. McAfee EEPC: Produkteinstellungen → Verschlüsselung

Für die konkrete Testumgebung wurden alle Datenträger verschlüsselt (siehe Rotmarkierung in der Abbildung 47) und Single-Sign-On mit dem vorhandenen Windows-Benutzerkonto aktiviert (siehe Rotmarkierung in der Abbildung 47).

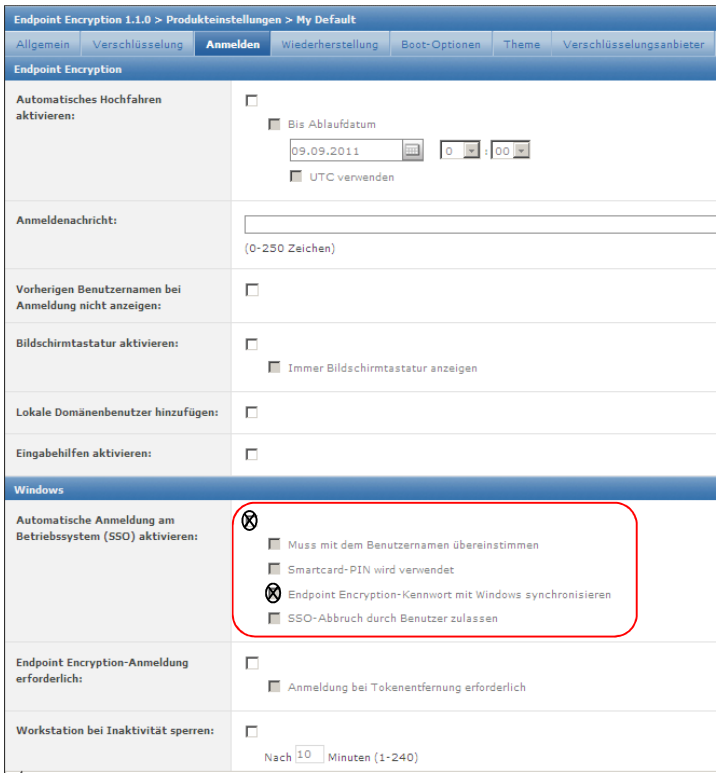


Abbildung 47. McAfee EEPC: Produkteinstellungen → Anmelden

Benutzerbasierte Richtlinie:

Die Einstellungen der Benutzerrichtlinie stellen die wichtigsten Optionen zur Benutzerverwaltung der verschlüsselten Endgeräte dar. Der vollständige Funktionsumfang dieser Richtlinie ist im Anhang B: McAfee EEPC: Richtlinien vorhanden. Abbildung 48 zeigt die wichtigste Einstellung für die durchgeführte Systemverschlüsselung, nämlich die Pre-Boot-Authentifikationsmethode. Es wird, wie bei den anderen zwei kommerziellen FDE-Lösungen, die Password-Identifikation ausgewählt. Eine Einstellung der Authentifikation mittels Smartcards (als einzige oder zusätzliche Authentifikationsmethode) ist in ePO vorhanden, aber in der Testumgebung nicht anwendbar (siehe Abschnitt 9.3.2) und wird somit nicht weiter betrachtet.

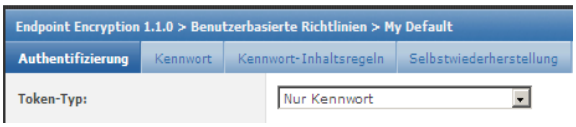


Abbildung 48. McAfee EEPC: Benutzerbasierte Richtlinie → „Benutzerbasierte Richtlinie“

Bevor die Richtlinien dem Clientgerät zugewiesen wurden, wurde ein Benutzer[29] dem zu verschlüsselnden Systems hinzugefügt (unter „Aktionen“ (siehe Rotmarkierung in der Abbildung 49) → „EE Nutzer hinzufügen“ → Benutzer aus Unternehmensverzeichnisdienst auswählen). Als Nächstes wurden die Richtlinien dem Client zugewiesen (siehe Gelbmarkierung in der Abbildung 49). Der Benutzer übernimmt automatisch (nach den Standardeinstellungen) die benutzerdefinierte Richtlinie vom System.

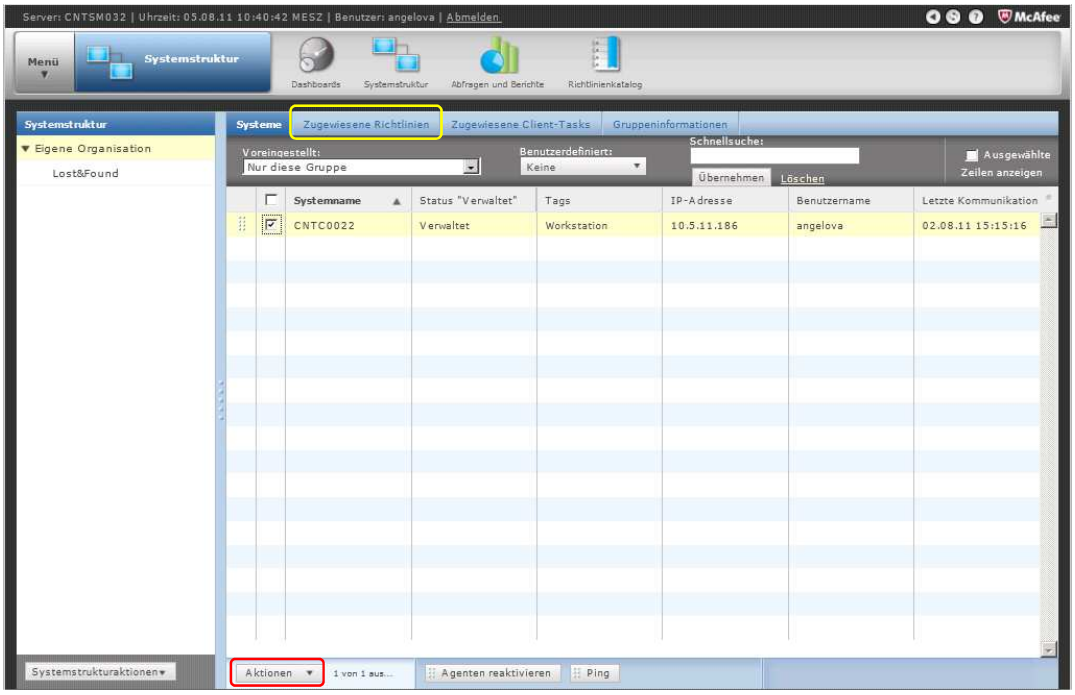


Abbildung 49. Verwaltetes Clientgerät mit zugewiesenem Benutzer

Durch die Zuweisung der gewünschten Richtlinien in der Verwaltungseinheit fing auf der Clientseite nach Anmeldung der eingerichteten Benutzer automatisch die Verschlüsselung des Systems an.

[29] Es können auch mehrere Benutzer oder Gruppen von Benutzern einem verschlüsselten System hinzugefügt werden.

Der Verschlüsselungsvorgang sollte in keiner Weise die Arbeit an dem Rechner behindern, es ist jedoch mit Geschwindigkeitseinbußen zu rechnen (durch die CPU-Auslastung). Um die Dauer der Verschlüsselung realistisch messen zu können, wurde der Rechner während des Prozesses nicht anderweitig genutzt. Der gesamte Vorgang dauerte insgesamt 73 Minuten und wurde mit einer Meldung zur erfolgreichen Systemverschlüsselung abgeschlossen. Dabei wurde die Statusanzeige auf der Clientseite als „aktiv“ geändert (siehe Abbildung 50).

Abbildung 50. McAfee Statusanzeige auf der Clientseite

11.4 Weitere getestete Funktionen und Möglichkeiten des Produkts

11.4.1 Verschlüsselung von Wechselmedien

Die Verschlüsselung von Wechselmedien wird vom EEFF-Softwaremodul realisiert, das über eigene Richtlinien verfügt. Für die Zwecke der vorliegenden Arbeit sind die Richtlinien – „Allgemein“ (siehe Abbildung 51) und „Wechseldatenträger“ relevant (siehe Abbildung 52).

Allgemein:

Verwaltet die Verschlüsselungsrechte, die den Endbenutzern für die lokale Benutzung am Clientgerät zugewiesen werden.

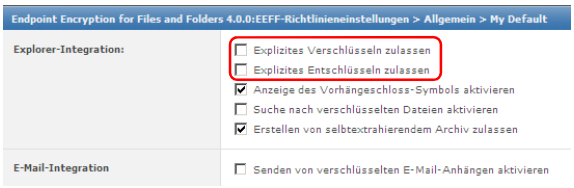


Abbildung 51. McAfee EEFF: Allgemeine Richtlinie

Wechseldatenträger:

Mittels dieser Richtlinie werden die Wechselmedienverschlüsselungsoptionen festgelegt. Um die Verschlüsselung zentral durch den Administrator durchzuführen wird die Option „EERM verwenden“ ausgewählt (siehe Grünmarkierung in der Abbildung 52). Somit werden an dem Client angeschlossene externe Speichermedien automatisch verschlüsselt.

Falls der Endnutzer die benötigten Rechte besitzt (siehe Abbildung 51) und die Option „Explizites Verschlüsseln zulassen“ festgelegt wird, darf er manuell über die Client-Konsole (siehe Abbildung 44) die Verschlüsselung von Wechseldatenträgern durchführen.

In der konkreten Untersuchung wurde ein 2 GB großer USB-Stick zentral verschlüsselt. Der Vorgang ist genau nach dem beschriebenen Szenario abgelaufen und wurde reibungslos und mit dem gewünschten Ergebnis durchgeführt.

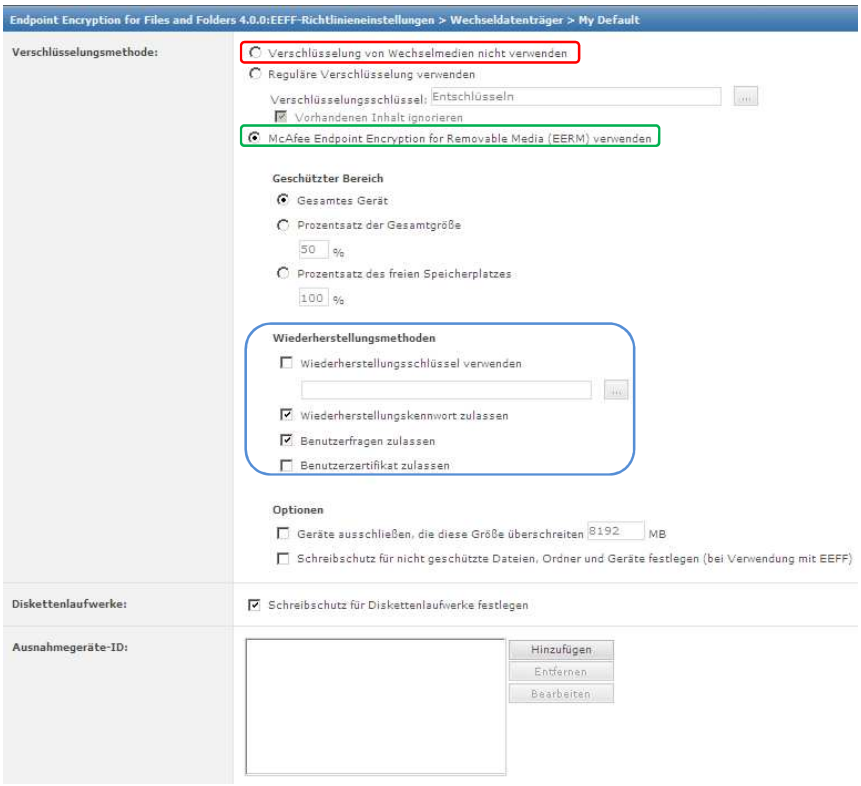


Abbildung 52. McAfee EEFF: Richtlinie Wechseldatenträger

11.4.1.1 Datenspuren auf verschlüsselten Wechseldatenträgern

Es wurde eine Text-Datei auf dem verschlüsselten Wechseldatenträger mit dem Namen „Test.txt“ und dem Inhalt – „Das ist eine Testdatei“ erstellt. Anschließend wurde der USB-Stick von dem Rechner entfernt und auf einem Rechner ohne installierten EEFF eingesteckt. Der Inhalt des Datenträgers wurde mit Hilfe des Programms WinHex 16.1 nach der Textdatei, sowie nach Zeichenketten, die den Namen der Datei, den Inhalt oder Teile davon (wie z.B. „Das ist“) enthalten, durchsucht. Alle Tests hatten keine Treffer zur Folge. Weiterhin wurde das verschlüsselte Speichermedium nach Hinweisen für die Benutzung von EE untersucht und es konnten ebenfalls keine Informationen darüber gefunden werden.

Der Wechseldatenträger wurde erneut an den EEFF-Client angeschlossen und die Tests mit WinHex wurden wiederholt. In diesem Fall konnte, wie erwartet, die Datei und deren Inhalt anhand der angegebenen Zeichenketten gefunden werden.

Der USB-Stick wurde anschließend unter Windows formatiert. Die Tests wurden erneut wiederholt und führten zu negativen Ergebnissen – es konnten keine Datenspuren und keine Hinweise auf die Benutzung von EEFF nachgewiesen werden.

11.4.1.2 Wiederherstellungsstrategien für externe Wechseldatenträger

Insgesamt werden vier Strategien zur Datenwiederherstellung auf Wechseldatenträgern von EEFF angeboten. Damit sie den Benutzern zur Verfügung stehen, müssen sie vom Administrator in der Richtlinie freigeschaltet/ aktiviert werden (siehe Blaumarkierung in der Abbildung 52).

Die Wiederherstellungsmöglichkeiten können auf der Clientseite über die EEFF-Konsole aufgerufen werden (siehe Rotmarkierung in der Abbildung 44).

Wiederherstellungsschlüssel: Es wird ein regulärer Schlüssel oder persönlicher Benutzerschlüssel festgelegt, der zum Wiederherstellen der verschlüsselten Wechselspeichermedien verwendet werden kann. *Bemerkung:* Diese Option ist mit weiteren Richtlinieneinstellungen von EEFF verbunden und wurde nicht getestet.

Wiederherstellungskennwort: Den Endnutzern wird die Angabe eines Kennworts während der Initialisierungsphase des zu verschlüsselnden Wechselmediums ermöglicht, das zu Wiederherstellung der Daten genutzt werden kann. Diese Option wurde getestet und funktioniert reibungslos entsprechend den Anbieterangaben.

Benutzerfragen zulassen: Die Endbenutzer werden dazu berechtigt fünf Wiederherstellungsfragen während der Initialisierungsphase des zu verschlüsselnden Wechselmediums festzulegen. Die Benutzer müssen dann mindestens vier Fragen richtig beantworten, um das Gerät wiederherzustellen. Diese Option wurde getestet und funktioniert reibungslos entsprechend den Anbieterangaben.

Benutzerzertifikat: Den Endnutzern wird das Anhängen eines Windows-Zertifikats während der Initialisierungsphase des zu verschlüsselnden Wechselmediums ermöglicht, der zu Wiederherstellung der Daten genutzt werden kann. Diese Option wurde getestet und funktioniert reibungslos entsprechend den Anbieterangaben.

11.4.1.3 Externe Wechselmedien dauerhaft entschlüsseln

Die Entschlüsselung von Wechselmedien erfolgt lokal und nur falls der Endnutzer dazu von der zentral verwalteten Richtlinie zugelassen ist (siehe Rotmarkierung in der Abbildung 51) und zusätzlich dazu in der EERM-Richtlinie die Option „Verschlüsselung von Wechselmedien nicht verwenden“ ausgewählt ist (siehe Rotmarkierung in der Abbildung 52). Um den Vorgang zu starten, muss der Benutzer die benötigten Authentifizierungsdaten eingeben (in dem konkreten Untersuchungsfall wurden die Daten durch ein Kennwort geschützt). Der Vorgang ist intuitiv und unkompliziert.

Der beschriebene Entschlüsselungsmechanismus wurde im Rahmen der Untersuchung durchgeführt und funktioniert einwandfrei und entsprechend den Angaben des Anbieters.

11.4.2 Daten- bzw. Passwortwiederherstellungsstrategien

Die FDE-Lösung von McAfee bietet für die Daten- bzw. Passwortwiederherstellung dieselben Verfahren wie SGN – Wiederherstellungsfragen (Festlegen von Fragen und Antworten zur Datenwiederherstellung) und das Challenge/ Response - Verfahren (Interaktion zwischen Endnutzer und Administrator).

Um die Verfahren überhaupt nutzen zu können, sollen sie durch die entsprechenden Richtlinien zugelassen werden.

11.4.2.1 Wiederherstellungsfragen

Die lokale Selbstwiederherstellung wird über die benutzerbasierte Richtlinie von EEPC für die Endnutzer des Systems freigeschaltet (siehe „Benutzerbasierte Richtlinie“ → „Selbstwiederherstellung“ im Anhang B: McAfee EEPC: Richtlinien). Dabei kann noch eingestellt werden, wie viele Wiederherstellungsfragen der Benutzer beantworten muss und wie viele davon er beim Wiederherstellungsvorgang richtig beantworten soll. Nachdem die Richtlinie durchgesetzt wird, wird der Benutzer bei der nächsten Pre-

Boot-Authentifikation aufgefordert, die Fragen und die entsprechenden Antworten für die Selbstwiederherstellung festzulegen.

Falls der Benutzer sein Passwort vergisst, hat er im Pre-Boot-Menü die Möglichkeit, die Sicherheitsfragen nach den entsprechenden Richtlinieneinstellungen zu beantworten (unter „Options“ → „Recovery“ → „Self Recovery“). Der gesamte Vorgang wurde getestet und ist einwandfrei und entsprechend den Angaben des Anbieters verlaufen.

11.4.2.2 Challenge/ Response

Die zweite Passwortwiederherstellungsmöglichkeit ist eine Challenge/ Response – Passwortwiederherstellungsstrategie. Sie wird über die Produkteinstellungen der EEPC-Richtlinie ermöglicht (siehe „Produkteinstellungen“ → „Wiederherstellung“ im Anhang B: McAfee EEPC: Richtlinien).

Dafür wählt der Benutzer beim Pre-Boot-Authentifikationsverfahren „Options“ → „Recovery“ → „Administrator Recovery“ aus und bekommt einen Challenge-Code angezeigt, der dem Administrator mitgeteilt werden muss. Der Administrator öffnet in der Management-Konsole den Datenwiederherstellungsbildschirm (unter „Menü“ → „Datenschutz“) und gibt den Challenge-Code des Benutzers ein. Falls der Code auf Client- und Managementseite übereinstimmt wählt der Administrator die Wiederherstellungsoptionen für das betroffene Endgerät und/ oder den betroffenen Endnutzer und bekommt, je nach eingerichteter Wiederherstellungsschlüsselgröße, einen Responsecode. Dieser Code muss dem Benutzer mitgeteilt werden. Sobald der Benutzer den Response-Code eingibt, wird er automatisch an dem Rechner angemeldet.

Der gesamte Vorgang wurde getestet und ist einwandfrei und entsprechend den Angaben des Anbieters verlaufen. Die Assistenten auf der Client- und Managerseite sind sehr einfach und verständlich aufgebaut und erlauben eine intuitive Durchführung des Wiederherstellungsprozesses.

11.4.3 Ressourcenbelegung

Es wurden mehrere Messungen zum Ermitteln der CPU- und RAM- Belastung, sowie der Kopier-, Schreib-, Lesezugriffsgeschwindigkeit bzw. –zugriffszeit für verschiedene Dateigrößen auf dem mit EEPC verschlüsselten Testrechner durchgeführt. Ziel der Messungen war, diese Größen bei den mit den unterschiedlichen FDE-Lösungen verschlüsselten Rechnern sowie einem unverschlüsselten Testsystem zu vergleichen. Details über die durchgeführten Messungen, die Ergebnisse und ihre Auswertung werden in Abschnitt 12 betrachtet.

11.4.4 System-Partition/ Laufwerk dauerhaft entschlüsseln

Der Entschlüsselungsvorgang des Systems wird von EEPC zentral abgewickelt und kann lokal vom Benutzer nicht durchgeführt werden. Dafür wird in der Produktrichtlinie die Verschlüsselung auf „keine“ gesetzt (siehe Grünmarkierung in der Abbildung 46) und die Richtlinienzuweisung aktualisiert. Danach fängt die Entschlüsselung auf der Clientseite automatisch an und wird benutzertransparent durchgeführt.

Der Zeitaufwand für die Entschlüsselung des getesteten Systems war mit dem für die Verschlüsselung vergleichbar. Der Prozess verläuft im Hintergrund und erlaubt den Nutzern während des Entschlüsselungsvorgangs weiter an dem Rechner zu arbeiten, wobei mit Verzögerungen[30] bei Anwendungen mit großer CPU-Belastung zu rechnen ist.

11.5 Anmerkungen und Zusammenfassung

McAfee bietet eine professionelle FDE-Lösung als Teil der Palette von Softwareprodukten zu Sicherung von IT-Infrastrukturen für den Unternehmenseinsatz an. Die zentrale Management-Konsole (ePO) erlaubt das Anbinden von unterschiedlichen Softwarepaketen und stellt ein sehr komplexes und mächtiges Verwaltungswerkzeug dar. Die Steuerung der Endgeräte und der Endnutzer wird genau wie bei den anderen untersuchten kommerziellen FDE-Lösungen durch Richtlinien realisiert, die produktspezifisch organisiert sind. Weiterhin ist ein umfangreiches Angebot an Produktdokumentationen vorhanden.

[30] Die Verzögerung der Arbeitsprozesse während der Ver- bzw. Entschlüsselung des Systems wurde nicht getestet, damit der Zeitaufwand für die beiden Vorgänge nicht beeinflusst wird.

Folgende Bemerkungen bezüglich des Umgangs mit dem Produkt und der durchgeführten Untersuchungen sind noch wichtig:

- In der Vorbereitungsphase war es schwer zu entschieden, welche Softwarepakete bzw. –produkte für die gewünschte Konfiguration gebraucht werden, was unter anderem durch die verschachtelte Struktur von EE und die Vielfalt von Produktangeboten und Zusammenstellungen von McAfee hervorgerufen wurde.

- Die Einrichtungsphase bei diesem Produkt hat mehr Zeit als bei den anderen zwei kommerziellen Lösungen in Anspruch genommen. Dafür konnte es aber komplett ohne externe Hilfe eingerichtet werden.

- Die Benutzeroberfläche der Verwaltungseinheit ist sehr übersichtlich gehalten. Durch die umfangreiche Funktionalität der Konsole wird die Navigation und die Einrichtung der gewünschten Einstellungen erschwert und ist nicht intuitiv. Die Arbeit wird zwar durch die vorhandene kontextsensitive Hilfe erleichtert, musste aber bei komplexeren Aufgaben durch weitere Hilfsmittel (Dokumentation, Videos etc.) ergänzt werden.

- Die Verwaltung von Benutzern und Geräten ist sehr fein und flexibel gesteuert. Es kann mit einzelnen Instanzen oder gesamten Organisationsstrukturen des Unternehmensverzeichnisdienstes gearbeitet werden.

- Bei kommerziellen Verschlüsselungsprodukten besteht immer die Gefahr, dass einen Masterkey vorhanden ist. Es ist nicht überprüfbar, welche Hintertüren in dem Sourcecode möglicherweise eingebaut sind.

12 Leistungstests und Ergebnisse

Für die Zwecke der vorliegenden Arbeit war von besonderem Interesse, welchen Einfluss die Endgeräteverschlüsselung mit den betrachteten FDE-Lösungen auf die konkrete Testumgebung hat und in welchem Ausmaß. Es wurden mehrere Messungen bezüglich unterschiedlicher Parameter, wie CPU- und RAM- Belastung, sowie Kopier-, Schreib-, Lesezugriffsgeschwindigkeit bzw. –zugriffszeit durchgeführt.

In diesem Kapitel wird weiterhin auf die Vorbereitung, die Bedingungen und die benötigten Tools für die Durchführung der Messungen eingegangen (siehe Abschnitt 12.1). Danach wird der Testverlauf betrachtet (siehe Abschnitt 12.2). Anschließend werden die Ergebnisse vorgestellt, ausgewertet (siehe Abschnitt 12.3) und am Ende werden einige Schlussfolgerungen gezogen (siehe Abschnitt 12.4).

12.1 Beschreibung der Untersuchung

Es wird im Folgenden das entwickelte Untersuchungsszenario vorgestellt, um die Leistung der betrachteten verschlüsselten Systeme miteinander zu vergleichen und sie zusätzlich einem unverschlüsselten System gegenüberzustellen. Im Anschluss werden die für die Messungen gebrauchten Tools beschrieben.

12.1.1 Untersuchungsszenario

Es werden Dateien mit unterschiedlichen Größen lokal auf den Testrechnern kopiert. Dabei wird der Kopiervorgang in 2 unterschiedlichen Modi durchgeführt.

Messung in Modus 1: Byte-by-Byte – Kopieren:

Es werden lokal auf der Festplatte Dateien mit unterschiedlicher Größe abgelegt. Sie werden in einen anderen lokalen Ordner kopiert. Dabei werden die Dateien Byte-by-Byte kopiert, d.h. dass die Dateien byteweise in den RAM eingelesen und auf den Zielspeicherplatz geschrieben werden. Ziel der Untersuchung ist, die CPU-Auslastung und die Kopiervorganggeschwindigkeit zu messen.

Messung in Modus 2: Kopieren als Gesamtdatei:

Es werden lokal auf der Festplatte Dateien mit unterschiedlicher Größe abgelegt. Sie werden in einen anderen lokalen Ordner kopiert. Dabei werden die Dateien als Ganzes kopiert, d.h., dass sie komplett im RAM abgelegt werden (entspricht dem Lesevorgang) und dann wieder als Ganzes auf den Zielspeicherplatz geschrieben werden (entspricht dem Schreibvorgang). Somit können der Lese- und Schreibvorgang beim Kopieren getrennt betrachtet werden und die Zeiten bzw. Geschwindigkeiten für den Lese-, Schreib- und Kopiervorgang gemessen werden.

12.1.2 Vorbereitung der Untersuchung und genutzte Tools

Als Erstes mussten die Dateigrößen für die Untersuchung festgelegt werden. Für den Kopiervorgang im Modus 1 wurden Dateien von 1 MB bis 2 GB bezüglich der Potenzen von 2 generiert. Für die Messungen im Modus 2 wurden unter Berücksichtigung der RAM-Größe der Testgeräte Dateien von 1 MB bis 512 MB bezüglich der Potenzen von 2 generiert (siehe Abschnitt 6.1.1).

Folgende Tools wurden für die Durchführung der Untersuchungen benötigt:

Dummy File Creator, Version 1.2 [dum11]:

Ein kleines Freeware-Programm zum Erstellen von Dateien mit willkürlichem Inhalt. Es ist wichtig, dass die Dateien mit zufälligen und voneinander unabhängigen Inhalten gefüllt sind, damit die Messungen nicht durch gepufferte Daten beeinflusst werden.

Benchmark FB3:

Um die genannten Messungen durchzuführen wurde im Rahmen der vorliegenden Arbeit eine eigene Benchmark entwickelt und auf bereits vorhandene Werkzeuge, wie zum Beispiel die IOzone-Benchmark[31], verzichtet. Es wurden in der Vorbereitungsphase mehrere solcher Tools in Betracht gezogen. Sie bieten jedoch im Regelfall einen CPU-Leistungstest an, wobei automatisch unterschiedliche Dateigrößen auf unterschiedlichen Parameter, wie Lese- und Schreibzugriffsgeschwindigkeit, geprüft

[31] Siehe www.iozone.org

werden. Auch bei feineren Einstellungen der benötigten Testrahmenbedingungen konnte nicht genau die CPU-Leistung während eines bestimmten Prozesses (z.B. Lesen einer Testdatei) mittels Perfmon aufgenommen werden. IOzone generiert beispielsweise die Testdateien selbst und damit ist nicht genau bekannt, welche zusätzliche Hintergrundbelastung der CPU bzw. des Arbeitsspeichers dadurch entsteht. Aus diesen Gründen hat sich die Notwendigkeit ergeben, eine kleine Benchmark zu entwerfen, deren beschränkte Funktionalität genau den Anforderungen der beabsichtigten Messungen und dem anschließenden Leistungsvergleich der unterschiedlich verschlüsselten Systeme entspricht. Zusätzlich wird dadurch eine bessere Transparenz der durchgeführten Messungen geschaffen.

FB3 stellt die im Rahmen der vorliegenden Arbeit entworfene und in ANSI-C geschriebene Benchmark dar (der Quellcode steht im Anhang C: FB3 - Quellcode). Es gibt 2 eingebaute Funktionen, die den Modi aus dem Untersuchungsszenario entsprechen (siehe Abschnitt 12.1.1). Für die Messung müssen der Untersuchungsmodus und die vollständigen Pfade des Speicherorts und des Zielspeicherorts der zu kopierenden Datei angegeben werden (siehe Abbildung 53). Die Benchmark ermittelt in Modus 1 die benötigte Zeit (in Millisekunden) und die Geschwindigkeit (in KB pro Sekunde) für den Byte-by-Byte – Kopiervorgang der jeweiligen Datei. In Modus 2 (Kopieren als Gesamtdatei) werden die benötigte Zeit (in Millisekunden) und die Geschwindigkeit (in KB pro Sekunde) für den Lese-, Schreib- bzw. Kopiervorgangs der jeweiligen Datei ermittelt.

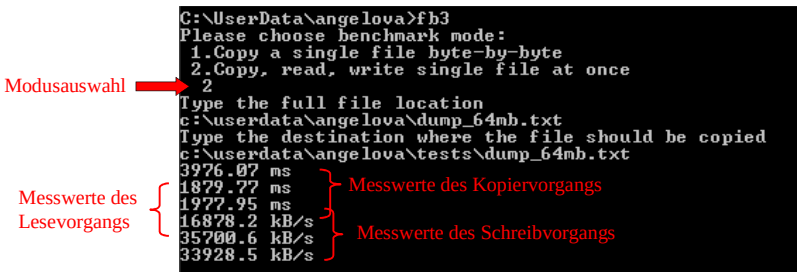


Abbildung 53. FB3: Kopiervorgang in Modus 2 am Beispiel von einer 64 MB großen Datei

Windows Performance-Monitor (Perfmon):

Perfmon bietet die Möglichkeit unterschiedliche Parameter des Systems in Echtzeit aufzunehmen und zu protokollieren. Für die vorliegende Untersuchung wurde ein neues Leistungsindikatorenprotokoll auf jedem Testrechner erstellt, der die gesamte CPU-Auslastung (Leistungsindikator „% Processor Time“[32]) und der verfügbare RAM (Leistungsindikator „Available KBytes“) im Sekundentakt verfolgt und die ermittelten Werte in einer .tsv-Datei (tabulatorgetrennte Inhalte in einer Textdatei) speichert.

Während der Messungen dürfen keine weiteren Aufgaben durch den Nutzer an den Testrechnern durchgeführt werden.

12.2 Durchführung der Messung

Die Messungen wurden entsprechend der Beschreibung in Abschnitt 12.1.2 durchgeführt. Die Schritte 1 bis 9 stellen den gesamten Untersuchungsvorgang bei den verschlüsselten Testgeräten dar.

1. Verschlüsselung des Testsystems mit der jeweiligen FDE-Lösung.
2. Anlegen der Ordner mit den Testdateien auf der lokalen Festplatte.
3. Erstellen des Leistungsindikatorenprotokolls entsprechend der Beschreibung im Abschnitt 12.1.2 in Perfmon.
4. Ausschalten des Testrechners für 2 Stunden, um einen definierten Ausgangszustand für die nachfolgenden Tests zu schaffen.
5. Nach dem Neustart: Es werden 30 Minuten Wartezeit eingelegt, damit alle Hintergrundprozesse, die zum Systemstart gehören, abgeschlossen werden. Anschließend werden Perfmon und FB3 gestartet.
6. Durchführen der FB3-Messungen im Modus 1. Dabei werden die Messungen für alle Testdateien in aufsteigender Reihenfolge bezüglich ihrer Größe (von 1 MB

[32] Es wird als Instanz „Total“ ausgewählt. Somit wird die gesamte CPU-Auslastung für alle Prozessorkerne des Prozessors aufgenommen.

bis 2 GB) mit Ablegen einer Protokollaufnahme durch Perfmon für jede Datei durchgeführt.

7. Ausschalten des Testrechners für 2 Stunden, um einen definierten Ausgangszustand für die nachfolgenden Tests zu schaffen.

8. Nach dem Neustart: Es werden 30 Minuten Wartezeit eingelegt, damit alle Hintergrundprozesse, die zum Systemstart gehören, abgeschlossen werden. Anschließend werden Perfmon und FB3 gestartet.

9. Durchführen der FB3-Messungen im Modus 2. Dabei werden die Messungen für alle Testdateien in aufsteigender Reihenfolge bezüglich ihrer Größe (von 1 MB bis 512 MB) mit Ablegen einer Protokollaufnahme durch Perfmon für jede Datei durchgeführt.

Die Messungen wurden zusätzlich auf einem unverschlüsselten System durchgeführt. Dies wurde auf einem der Testrechner realisiert, indem die Messungen gleich nach dem Einrichten des Systems und vor der Verschlüsselung mit einer der betrachteten FDE-Lösungen durchgeführt wurden. Für das unverschlüsselte Testgerät sind bei der Durchführung der Messungen die Schritte 2 bis 9 relevant.

12.3 Ergebnisse und Erkenntnisse (Auswertung)

In diesem Abschnitt werden die wichtigsten Ergebnisse und Erkenntnisse der durchgeführten Messungen vorgestellt.

12.3.1 Byte-by-Byte – Kopieren (Modus 1)

Die Messungen im Modus 1 der Benchmark (Byte-by-Byte Kopieren) wurden nach dem beschriebenen Schema durchgeführt und werden in diesem Abschnitt im Detail betrachtet.

Abbildung 54 zeigt die aufgenommene benötigte Zeit für den Kopiervorgang der unterschiedlichen Dateigrößen bei den unterschiedlichen Testclients. Bei den kleineren Dateien (bis 256 MB) verhalten sich die Systeme sehr ähnlich. Ein für den Benutzer

bedeutender Unterschied konnte nicht festgestellt werden. Hier muss auch beachtet werden, dass bei kleineren Dateien die möglichen Hintergrundprozesse, die durch die Testumgebung bedingt sind, einen spürbaren Einfluss auf die Ergebnisse haben können. Somit können aus den Ergebnissen der kleineren Dateien keine aussagekräftigen Schlüsse gezogen werden.

Die obere Grenze der Testdateigröße wurde, wie bereits erwähnt, auf 2 GB festgelegt. Beim Modus 1 spielt jedoch die Größe der Dateien im Vergleich zum Modus 2 keine Rolle bezüglich der Arbeitsspeicherbelastung, da den Kopiervorgang byteweise erfolgt. Ein weiterer Grund ist, dass für den alltäglichen Gebrauch im Fraunhofer CNT verhältnismäßig selten größere Dateien benutzt werden. Weiterhin wird anhand der ermittelten Ergebnisse angenommen, dass die für den Kopiervorgang benötigte Zeit linear mit der Dateigröße ab 256 MB wächst.

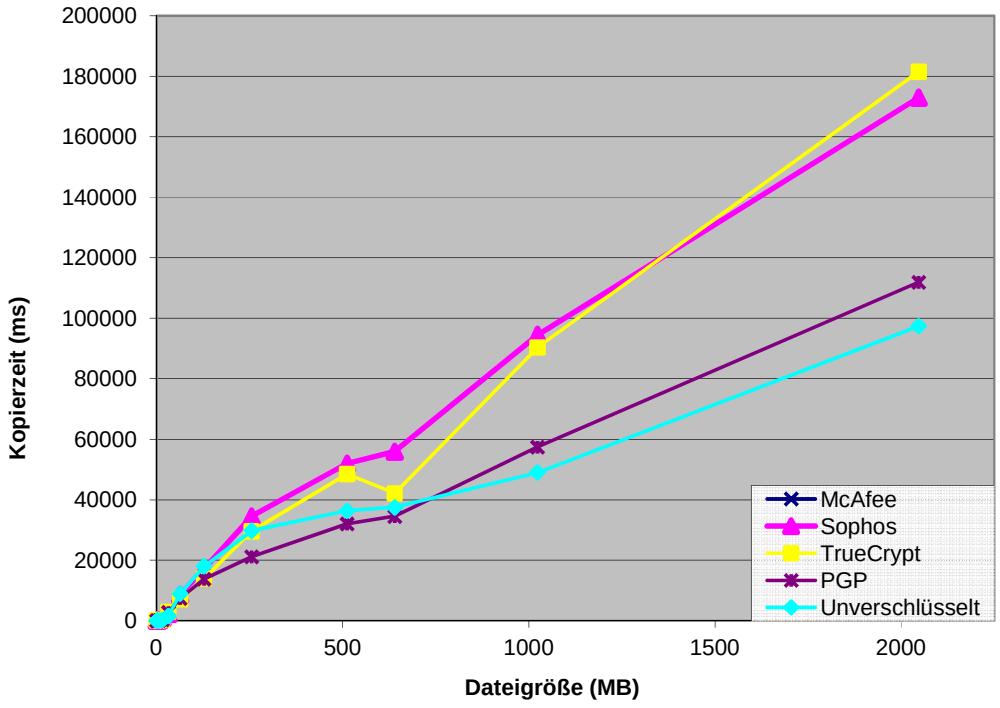


Abbildung 54. Byte-by-Byte-Kopieren

Für Dateien größer als 256 MB können in Abbildung 54 folgende Tendenzen beobachtet werden:

- Die Verschlüsselung durch PGP erlaubt ein vergleichbar schnelles Lesen und Schreiben von Daten, wie bei einem unverschlüsselten Laufwerk. Immerhin wurde bei der 2 GB großen Datei ein Unterschied von ca. 10 Sekunden festgestellt.

- Bei dem mit TrueCrypt verschlüsselten System erhöht sich die Kopierzeit sprunghaft für Dateigrößen über 512 MB. Trotz der von TrueCrypt eingebauten Prozessorparallelisierung (siehe Abschnitt 8.1) sind die Messwerte spürbar langsamer als bei dem unverschlüsselten System - die Abweichung beträgt bei den 2 GB bereits um die 40 Sekunden.

- Ähnlich zu dem TrueCrypt-Client ist auch bei dem SGN-Client (Sophos) eine sprunghafte Erhöhung des Zeitaufwandes bei den höheren Dateigrößen festgestellt worden. Der Unterschied zwischen dem Sophos-Client und dem unverschlüsselten Gerät bei der 2 GB großen Datei liegt bereits bei ca. 84 Sekunden.

- Bei dem McAfee-Client wurden die größten Zeitunterschiede gegenüber dem unverschlüsselten System für den Kopiervorgang der Testdateien über 128 MB ermittelt. Mit erhöhender Dateigröße wird der Zeitaufwand für den Kopiervorgang bei McAfee- und Sophos-Client vergleichbar (siehe Abbildung 54).

Der Arbeitsspeicher wird durch die byteweise durchgeführten Kopiervorgänge kaum belastet. Dieser Testmodus ist aber besonders gut für die Untersuchung der CPU-Auslastung bei den betrachteten Systemen. In Abbildung 55 ist die grafische Darstellung der durch Perfmon aufgenommenen Prozessorauslastungsdaten bei der Durchführung des Kopiervorgangs der 2 GB großen Testdatei[33] dargestellt.

[33] Es wurde die größte Testdatei für die Visualisierung gewählt, weil dabei eventuelle Hintergrundprozesse kaum einen Einfluss auf die Ergebnisse haben und die Zeitspanne am größten ist. Somit können aussagekräftigere Schlüsse aus der Messung gezogen werden.

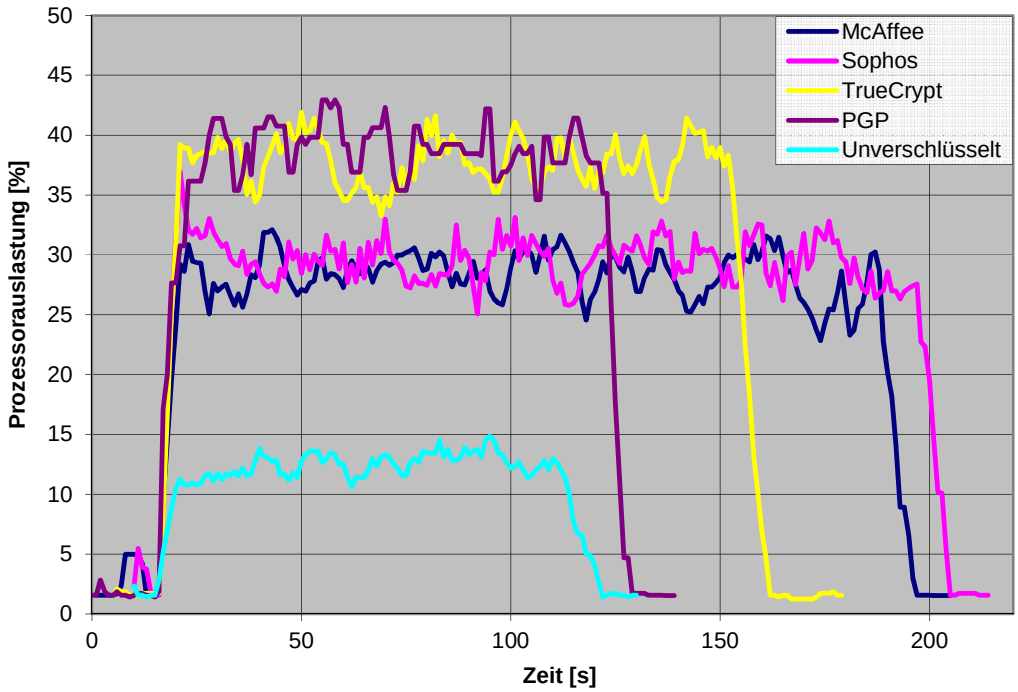


Abbildung 55. Byte-by-Byte – Kopieren: CPU-Auslastung[34] bei 2 GB Datei

Aus der Abbildung wird ersichtlich, dass durch die Verschlüsselung der Clientgeräte, die CPU durch gewöhnliche Lese- Schreibvorgänge viel mehr belastet wird. Dabei verhalten sich die FDE-Lösungen paarweise sehr ähnlich bezüglich der CPU-Auslastung. Die Testgeräte, die mit PGP bzw. TrueCrypt verschlüsselt wurden, belasten den Prozessor bei der Durchführung des konkreten Kopiervorgangs bis zu vier Mal mehr als der gleiche Vorgang bei dem unverschlüsselten System. Bei den Sophos- und McAfee-Clients ist die durch das byteweise Kopieren resultierende CPU-Belastung zwar niedriger als bei dem PGP- und dem TrueCrypt-Client (ca. das Dreifache der Belastung des unverschlüsselten Systems), dafür werden die Ressourcen aber länger beansprucht.

Aus diesen Beobachtungen resultieren folgenden Problemstellungen:

- Die höhere CPU-Belastung bedeutet auch ein höher Energieverbrauch. Es ist interessant in welcher Relation diesbezüglich die verschlüsselten Testgeräte

[34] Die CPU wird vor und nach dem Kopiervorgang mit ca. 1,5 % belastet (siehe Abbildung 55). Dieser Wert stellt den Ruhezustandswert des Prozessors bei laufenden Perfmon dar.

untereinander und gegenüber dem unverschlüsselten System stehen. Der Energieverbrauch der Geräte ist auch deswegen wichtig, weil die FDE-Lösungen hauptsächlich auf Laptops angewendet werden sollen. Somit stellt der Energieverbrauch einen wichtigen Leistungsparameter dar und wird des Weiteren in Abschnitt 12.3.3 betrachtet.

- Es wird anhand der Ergebnisse vermutet, dass beim gleichzeitigen Ausführen mehrerer Prozesse bzw. komplexerer Aufgaben auf einem verschlüsselten Testrechner, die CPU-Auslastung zu weiteren Verzögerungen und Geschwindigkeitseinbußen führen wird. Diese Annahme konnte nicht methodisch im Rahmen der vorliegenden Arbeit bewiesen bzw. widerlegt werden, wird aber als selbstverständlich angenommen.

12.3.2 Kopieren als Gesamtdatei (Modus 2)

Das Kopieren als Gesamtdatei wurde simuliert, um die Lese- bzw. Schreibgeschwindigkeit der unterschiedlichen Systeme für die generierten Testdateigrößen aufnehmen zu können. Bei diesem Vorgang wird die gesamte Datei in den RAM eingelesen und erst danach auf die Festplatte geschrieben.

In diesem Abschnitt wird auf die Ergebnisse des Lese- (siehe Abschnitt 12.3.2.1), Schreib- (siehe Abschnitt 12.3.2.2) und Kopiervorgangs (siehe Abschnitt 12.3.2.3) eingegangen. Anschließend werden die RAM- und CPU-Auslastung bei diesem Test betrachtet (siehe Abschnitt 12.3.2.4).

Bemerkung: Es muss zusätzlich beachtet werden, dass bei kleineren Dateien die möglichen Hintergrundprozesse, die durch die Testumgebung bedingt sind, einen spürbaren Einfluss auf die Ergebnisse haben können. Die Testergebnisse für die Dateigrößen bis 32 MB sind mit vernachlässigbar kleinen Unterschieden in der Ausführungszeit verbunden, die vom Benutzer nicht wahrnehmbar sind. Somit werden sie als nicht aussagekräftig betrachtet.

12.3.2.1 Lesen

Abbildung 56 und Abbildung 57 zeigen die ermittelten Lesezeiten und die bei dem Lesevorgang erreichten Lesegeschwindigkeiten, die für die unterschiedlichen Dateigrößen unter den betrachteten Systemen ermittelt wurden.

In den beiden Abbildungen ist deutlich zu sehen, dass die mit PGP WDE und TrueCrypt verschlüsselten Geräte fast genauso schnell, wie das unverschlüsselte System sind. Das Produkt von Sophos zeigt ebenso gute Ergebnisse bei den Dateien bis 256 MB. Der McAfee-Client unterscheidet sich deutlich von den anderen Systemen. Er zeichnet sich zwar durch eine stabile Verhaltensweise aus (fast linear bei den Lesezeiten), die aber die meiste Zeit benötigt und somit die niedrigste Geschwindigkeit für den Lesevorgang erreicht.

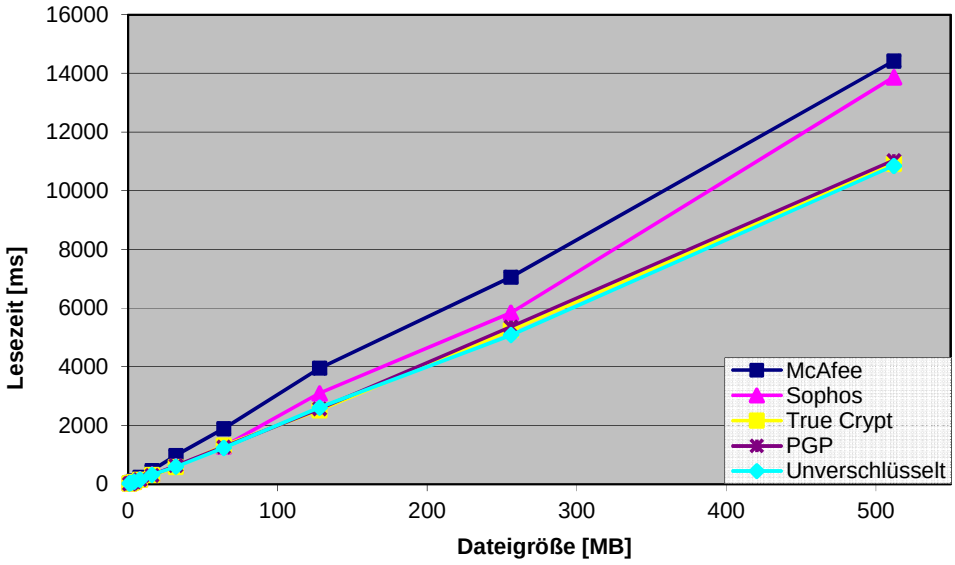


Abbildung 56. Ausführungszeit des Lesevorgangs für die unterschiedlichen Dateigrößen

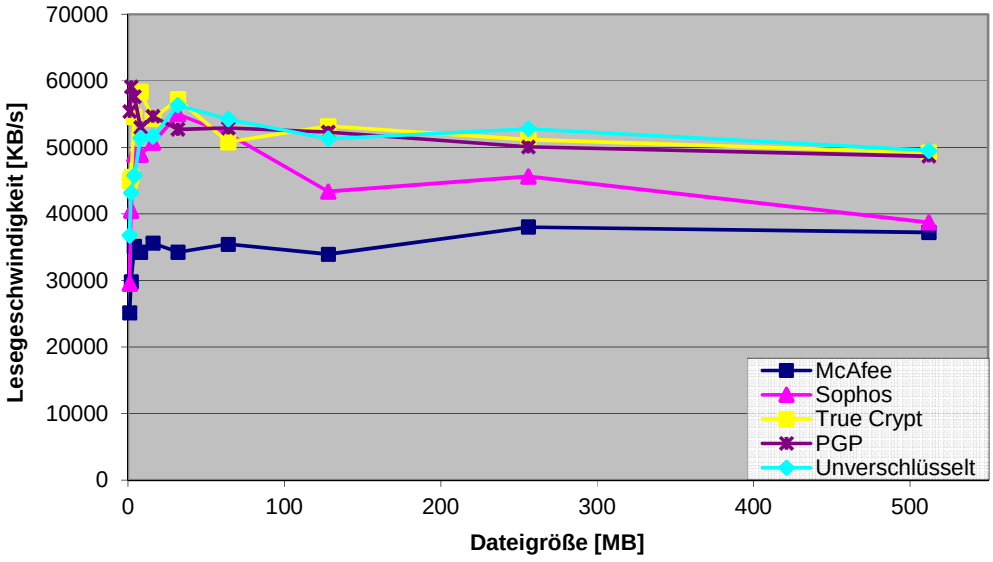


Abbildung 57. Geschwindigkeit des Lesevorgangs für die unterschiedlichen Dateigrößen

12.3.2.2 Schreiben

Abbildung 58 und Abbildung 59 zeigen die ermittelten Schreibzeiten und die bei dem Schreibvorgang erreichten Schreibgeschwindigkeiten, die für die unterschiedlichen Dateigrößen unter den betrachteten Systemen ermittelt wurden.

Bei dem Schreibvorgang bleiben die beobachteten Tendenzen bei den PGP und McAfee-Clients erhalten. Das mit PGP WDE verschlüsselte System erreicht auch bei dem Schreibvorgang Werte, die mit dem unverschlüsselten System vergleichbar sind. Der McAfee-Testclient arbeitet weiterhin am langsamsten und liegt deutlich über den Schreibvorgangszeiten der anderen FDE-Lösungen bzw. des unverschlüsselten Systems.

Überraschend sind die von dem mit dem SGN-Client (Sophos) verschlüsselten System ermittelten Ergebnisse. Er hat sich bei dem Schreibvorgang einiger Dateigrößen sogar als schneller als das unverschlüsselte System erwiesen.

TrueCrypt ist deutlich langsamer als das unverschlüsselte System, erreicht aber trotzdem gute Werte für die Durchführung des Schreibvorgangs.

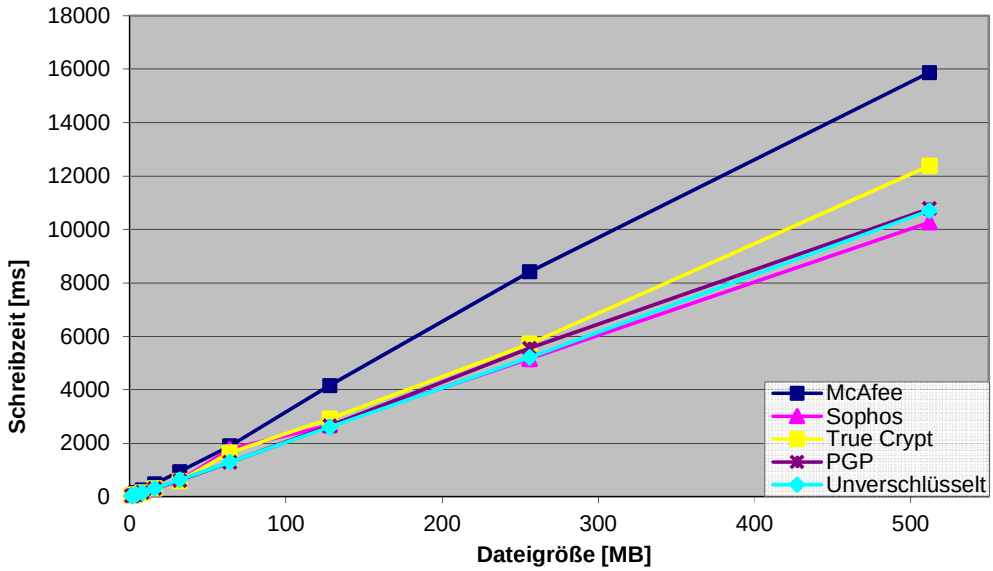


Abbildung 58. Ausführungszeit des Schreibvorgangs für die unterschiedlichen Dateigrößen

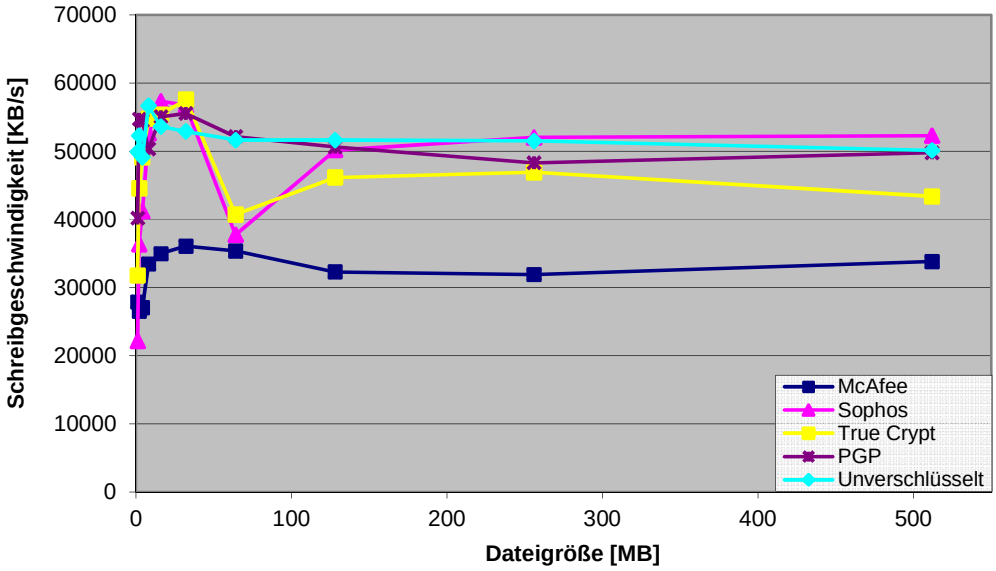


Abbildung 59. Geschwindigkeit des Schreibvorgangs für die unterschiedlichen Dateigrößen

12.3.2.3 Kopieren

Abbildung 60 und Abbildung 61 zeigen die ermittelten Kopierzeiten und die bei dem Kopiervorgang erreichten Schreibgeschwindigkeiten, die für die unterschiedlichen Dateigrößen unter den betrachteten Systemen ermittelt wurden.

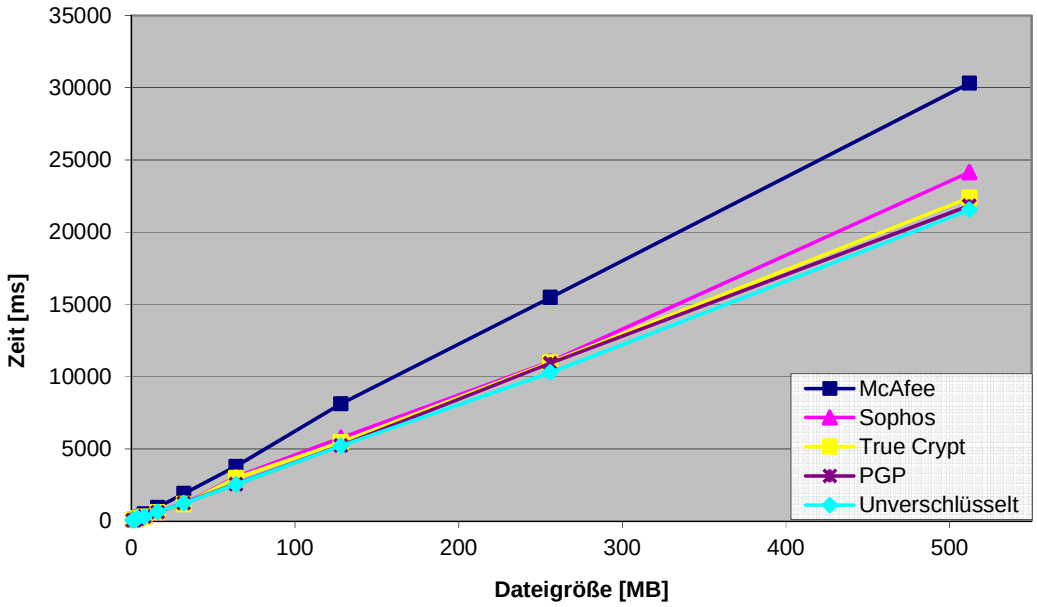


Abbildung 60. Ausführungszeit des Kopiervorgangs für die unterschiedlichen Dateigrößen

Der große Zeitaufwand für den Lese- und Schreibvorgang bei dem McAfee-Client führt logischerweise zu den höchsten Zeitwerten für den gesamten Kopiervorgang bzw. die niedrigste Kopiergeschwindigkeit.

Die Ergebnisse des PGP-Clients sind sowohl bei den Lese- und Schreibvorgängen als auch beim Kopiervorgang konstant geblieben und mit denen durch das unverschlüsselte System erreichten Werten vergleichbar. Es konnten kaum Leistungseinbüße durch die PGP-Verschlüsselung festgestellt werden.

Dadurch, dass der TrueCrypt-Client etwas schneller beim Lesevorgang und langsamer beim Schreibvorgang war und der Sophos-Client sich bei den durchgeführten Tests genau umgekehrt verhalten hat, sind die Ergebnisse für den gesamten Kopiervorgang dieser zwei FDE-Lösungen vergleichbar. Beide Produkte haben gute Ergebnisse

geliefert, die mit geringen Verzögerungen verbunden sind und kaum vom Benutzer bemerkt werden können.

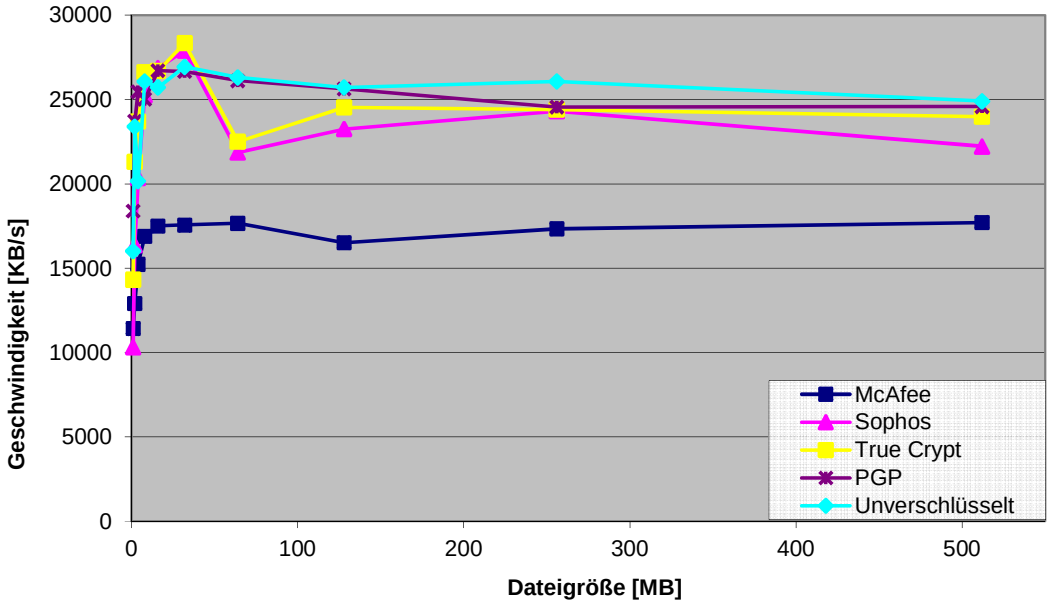


Abbildung 61. Geschwindigkeit des Kopiervorgangs für die unterschiedlichen Dateigrößen

12.3.2.4 RAM- und CPU-Belastung

Als nächstes werden die RAM-Belegung und die CPU-Belastung bei den unterschiedlichen FDE-Lösungen für den Kopiervorgang der 512 MB großen Datei[35] betrachtet.

Abbildung 62 zeigt die mittels Perfmon aufgezeichnete RAM-Belegung während des Kopiervorgangs als Gesamtdatei. Bei allen untersuchten Systemen wird der benötigte Arbeitsspeicherplatz für die Datei reserviert. Als Nächstes werden die kompletten Dateiinhalte in dem RAM eingelesen (Lesevorgang). Danach werden die Daten auf die Festplatte geschrieben (Schreibvorgang). Sobald der Prozess vollendet ist, wird der reservierte RAM-Speicherplatz wieder freigegeben.

[35] Der Kopiervorgang mit der 512 MB großen Testdatei ist mit dem größten Zeitaufwand verbunden, und somit sind die Unterschiede zwischen den einzelnen verschlüsselten Systemen besser erkennbar.

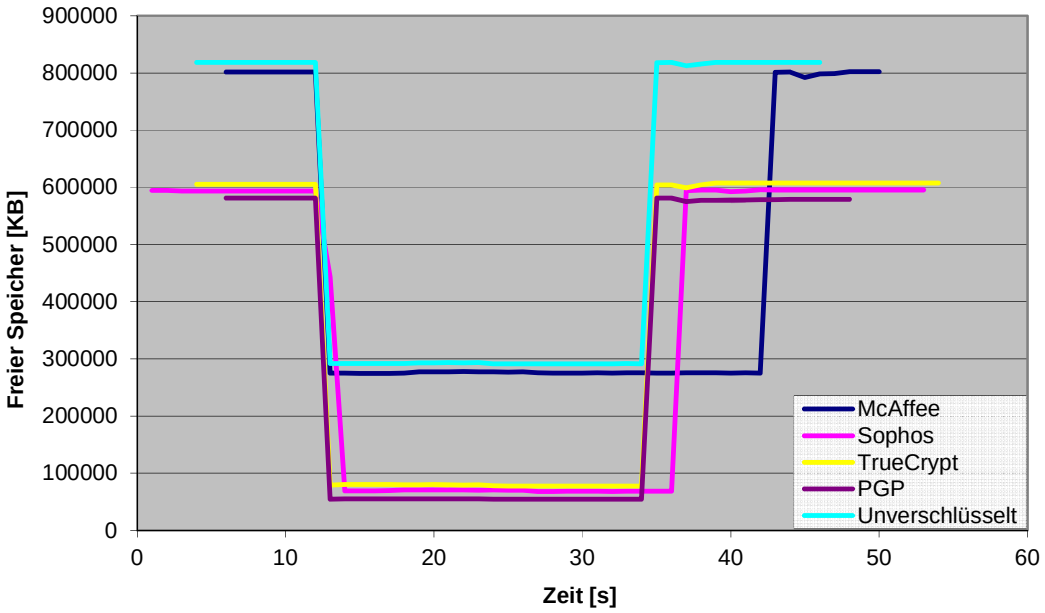


Abbildung 62. RAM-Belegung durch den Kopiervorgang bei der 512 MB großen Datei

Besonders interessant bei den ermittelten Werten ist die Tatsache, dass die unterschiedlich verschlüsselten Systeme unterschiedliche Mengen an Arbeitsspeicher für ihren Normalbetrieb (Ruhezustand) benötigen. Dabei wird bei den Testrechnern, die mit TrueCrypt, PGP WDE und SGN (Sophos) verschlüsselt sind, ca. 200 MB mehr Arbeitsspeicher als bei dem unverschlüsselten System belegt. Das entspricht ungefähr 20 % des in den Testgeräten eingebauten RAM-Speichers (die Testgeräte sind mit 1GB RAM ausgestattet – siehe Abschnitt 6.1.1), der zusätzlich belastet wird, was zur Ressourcenknappheit führen kann. Der EEPC-Client (McAfee) beansprucht hingegen fast die gleiche RAM-Kapazität wie der unverschlüsselte Client.

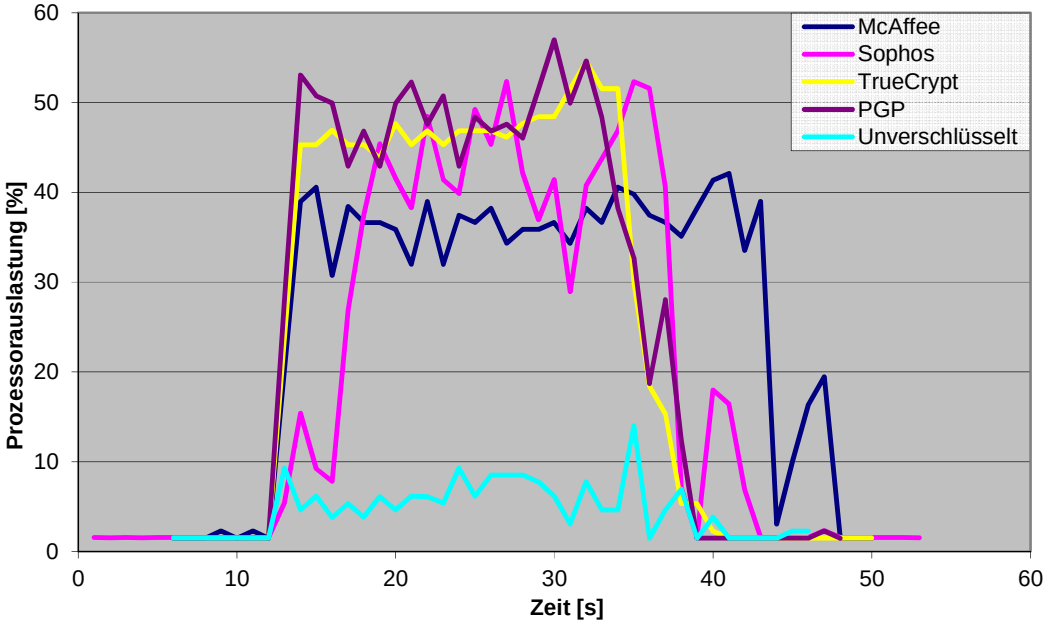


Abbildung 63. CPU-Auslastung durch den Kopiervorgang bei der 512 MB großen Datei

Abbildung 63 zeigt die Prozessorauslastung bei der Durchführung des Kopiervorgangs als Gesamtdatei. Die gewonnenen Belastungsprofile der unterschiedlichen Systeme sind sehr heterogen und es kann kein bestimmtes Muster erkannt werden. Alle verschlüsselten Clients belasten den Prozessor deutlich mehr als bei dem unverschlüsselten System. Nennenswert ist jedoch die CPU-Belastung von McAfee, da es sich deutlich von den anderen FDE-Lösungen unterscheidet. Die Prozessorauslastung ist dabei zwar niedriger, dafür wird der Prozessor für einen längeren Zeitraum beansprucht. Dadurch, dass die konkrete Implementierung nicht zur Verfügung steht, können leider die genauen Hintergründe für solche Verhaltensweisen bzw. Ressourcenbelegung nicht ermittelt werden.

Bemerkung: Der CPU wird im Normalbetrieb bei laufenden Perfmon mit ca. 1,5 % belastet. Dies ist vor und nach dem Kopiervorgang auf Abbildung 63 erkennbar.

12.3.3 Energieverbrauch

In diesem Abschnitt wird der Energieverbrauch der verschlüsselten Systeme bezüglich des unverschlüsselten Testclients für den byteweise durchgeführten Kopiervorgang (Modus 1) der 2 GB großen Datei betrachtet. Dafür werden die in [ea11] ermittelten Formeln zur Berechnung des Prozessorenergieverbrauchs bei Mehrkernprozessoren entsprechend eingesetzt:

(1) $$P_c = P_{max} * L_C$$

P_c..*Leistung eines Prozessorkerns* [W]
P_{max}..*maximale Leistung des Kerns* [W]
L_c..*mittlere Auslastung des Prozessors* [%]

(2) $$P_{CPU} = P_{idle} + \sum_{i=1}^{n} P_{C_i}$$

P_{CPU}..*Leistung des Prozessors* [W]
P_{idle}..*Leistung des Geräts in Ruhezustand* [W]
n..*Anzahl Prozessorkerne*
P_{C_i}..*Leistung des* $i-ten$ *Prozessorkerns* [W]

Dabei wird mit der ersten Formel die Leistung von jedem Prozessorkern und mit der Zweiten die gesamte CPU-Leistung ermittelt. P_{max}, P_{idle} sind Konstanten, d.h. dass sie gleiche[36] Werte bei allen Testgeräte haben, wobei P_{max} die maximale Leistung des Geräts und P_{idle} die Leistung es Geräts in Ruhezustand darstellt. L_C ist der mittlere Auslastung der CPU während des Kopiervorgangs. $P_{Unverschlüsselt}$, P_{PGP}, $P_{TrueCrypt}$, P_{Sophos}, P_{McAfee} stellen den Energieverbrauch des jeweiligen verschlüsselten Testclients für die Durchführung des Kopiervorgangs dar.

In der konkreten Untersuchung wurden Messungen in Sekundentakt gemacht. Somit wird der Energieverbrauch pro Sekunde berechnet. Die durch Perfmon aufgenommenen CPU-Belastungswerte wurden als Mittelwert von beiden vorhandenen Prozessorkernen der Testclients ermittelt. Es wird nur der Energieverbrauch während des Kopiervorgangs gesucht und dabei befindet sich der Prozessor in einem aktiven

[36] Es wurden identische Testgeräte (siehe Abschnitt 6.1.1) für die Untersuchung genutzt. Somit sind mögliche Abweichungen in der Größe dieser Werte als vernachlässigbar klein und unbedeutend betrachtet.

Zustand. Somit spielt P_{idle} keine Rolle mehr für die Berechnung und kann entfernt werden. Die Formel für die Berechnung der gesamten CPU-Leistung sieht für den bestimmten Untersuchungsfall folgendermaßen aus:

(3) $$P_{CPU} = P_{max} * L_C$$

P_{CPU}..*Leistung des Prozessors* [W]
P_{max}..*maximale Leistung des Kerns* [W]
L_C..*mittlere Auslastung des Prozessors* [%]

Für den gesamten Byte-by-Byte – Kopiervorgang wird folgende Formel ermittelt:

(4) $$P_{CPU_{Kopiervorgang}} = (P_{max} * L_C) * t_{Kopiervorgang}$$

$P_{CPU_{Kopiervorgang}}$..*Energieverbrauch eines Prozessorkerns* [$W * s$]
P_{max}..*maximale Leistung des Kerns* [W]
L_C..*mittlere Auslastung des Prozessors* [%]
$t_{Kopiervorgang}$..*Zeitdauer des Kopiervorgangs* [s]

$t_{Kopiervorgang}$ stellt die benötigte Zeit für den byteweise durchgeführten Kopiervorgang in Sekunden dar.

Aufgrund der durch Perfmon aufgenommenen CPU-Belastungswerte wurden die mittleren Auslastungen (L_C) der Testclients während des Kopiervorgangs (nur während der Prozessausführung) und die Dauer des Kopiervorgangs ermittelt (siehe Tabelle 1). Daraus ist es ersichtlich, dass die verschlüsselten Testgeräte auf jeden Fall mehr Energie für denselben Prozess verbrauchen als das unverschlüsselte System (dadurch, dass sowohl L_C, als auch die Zeitdauer des Kopiervorgangs bei dem unverschlüsselten System niedrigere Werte als alle anderen Systeme aufweisen).

Testclient	Mittlere CPU-Belastung (L_C)	Benötigte Zeit für den Kopiervorgang
Unverschlüsselt	12 %	97 s
PGP	38 %	108 s
TrueCrypt	38 %	137 s
Sophos	29 %	184 s
McAfee	28 %	172 s

Tabelle 1. Mittlere CPU-Belastung und benötigte Zeit für den Byte-by-Byte - Kopiervorgang

Durch direktes Ersetzten der Werte aus Tabelle 1 in der Formel (4) ergibt sich folgender Energieverbrauch für die einzelnen Systeme für den durchgeführten Kopiervorgang:

- $P_{Unverschlüsselt} = (P_{max} * 0,12) * 97\ s \approx 12 * P_{max}\ [W * s]$;
- $P_{PGP} = (P_{max} * 0,38) * 108\ s \approx 41 * P_{max}\ [W * s]$;
- $P_{TrueCrypt} = (P_{max} * 0,38) * 137\ s \approx 52 * P_{max}\ [W * s]$;
- $P_{Sophos} = (P_{max} * 0,29) * 184\ s \approx 53 * P_{max}\ [W * s]$;
- $P_{McAfee} = (P_{max} * 0,28) * 172\ s \approx 48 * P_{max}\ [W * s]$.

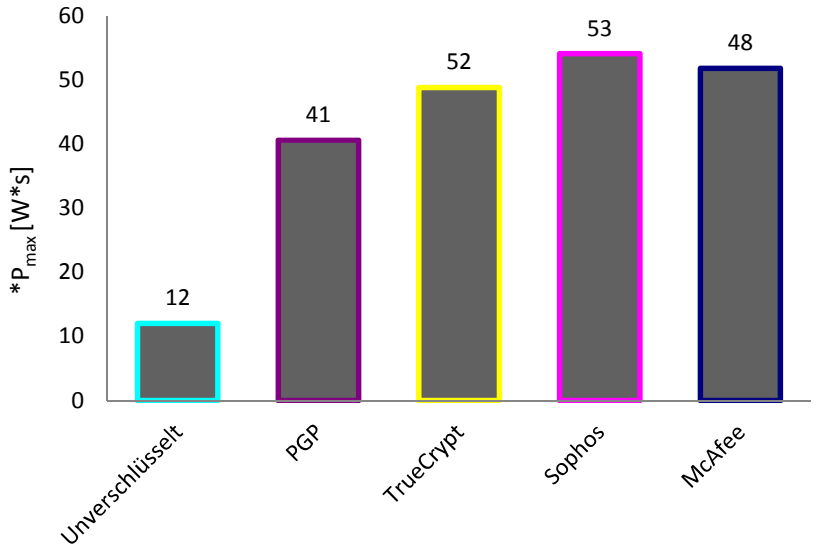


Abbildung 64. Energieverbrauch für den durchgeführten Kopiervorgang

Aus diesen Ergebnissen können folgenden Schlussfolgerungen gezogen werden:

- Der Energieverbrauch bei der Durchführung des Testkopiervorgangs ist bei dem mit PGP WDE verschlüsselten Testclient am niedrigsten gegenüber den anderen verschlüsselten Testsystemen. Immerhin verbraucht der PGP-Client dabei ca. 3,4-mal mehr Energie als das unverschlüsselte System.

- Obwohl der McAfee-Client die CPU-Ressourcen für einen längeren Zeitraum beansprucht, verbraucht er im Vergleich weniger Energie als die mit TrueCrypt und SGN (Sophos) verschlüsselten Testgeräte. Für den Kopiervorgang hat er 4-mal mehr Energie gegenüber dem unverschlüsselten System verbraucht.

- Der Energieverbrauch bei der Durchführung des Testkopiervorgangs ist bei den mit TrueCrypt und SGN (Sophos) verschlüsselten Testgeräten am höchsten gegenüber den anderen verschlüsselten Testsystemen. Sie verbrauchen jeweils 4,3 bzw. 4,5-mal mehr Energie gegenüber dem unverschlüsselten System bei diesem konkreten Kopiervorgang.

12.4 Schlussfolgerung

Obwohl alle untersuchten FDE-Lösungen den AES-Verschlüsselungsalgorithmus benutzen, führt die unterschiedliche Implementierung zu unterschiedlicher Ressourcenbelegung bzw. –ausnutzung. Die durchgeführten Untersuchungen zeigen eindeutig, dass durch die Festplattenverschlüsselung auf jeden Fall mit Leistungseinbußen zu rechnen ist.

Die ermittelten Ergebnisse zeigen, dass es zu Engpässen bei der Nutzung von mobilen Endgeräten kommen könnte. Der hohe Energieverbrauch bei der Durchführung von Schreib-, Lese- bzw. Kopierzugriffen kann beispielsweise zur Verminderung der Betriebszeit der Rechner und zu einer geringeren Lebensdauer der Batterien führen. Weiterhin haben die hohe CPU-Auslastung und RAM-Belegung längere Ausführungszeiten und somit auch eine geringere Arbeitsleistung zur Folge, falls ein bzw. mehrere komplexen Prozesse auf dem Rechner parallel ausgeführt werden (wie beispielsweise Simulationen oder Rendering von 3D - Animationen).

Alltägliche Aufgaben, wie E-Mail lesen, im Internet surfen, Texte bearbeiten, Dateien in kleineren Größenordnungen verwalten u.Ä. sind jedoch auf den Testrechnern ohne wahrnehmbare Leistungsverluste des Systems durchgeführt worden. Bei der Auswahl der geeigneten FDE-Lösung für die mobilen Geräte eines Unternehmensumfelds muss ihre Arbeitsbestimmung geklärt werden, d.h. welche Aufgaben primär auf diesen Rechner durchgeführt werden. Falls sie hauptsächlich für den Einsatz bei Dienstreisen, ohne das Durchführen komplexer Aufgaben eingesetzt werden sollen, ist die Festplattenverschlüsselung mit vertretbaren Leistungsverlusten verbunden.

13 Bewertung, Zusammenfassung und Ausblick

In diesem letzten Kapitel werden die untersuchten FDE-Lösungen anhand der im Rahmen der vorliegenden Arbeit ermittelten Ergebnisse bewertet (siehe Abschnitt 13.1). Als Nächstes wird grob auf den unternehmensinternen Prozess zur Einführung eines Festplattenverschlüsselungsprodukts eingegangen (siehe Abschnitt 13.2). Anschließend werden eine kurze Zusammenfassung der erreichten Ergebnisse und ein Ausblick auf offene relevante Forschungsfragen vorgestellt (siehe Abschnitt 13.3).

13.1 Bewertung der untersuchten FDE-Produkte

In Tabelle 2 sind die wichtigsten Anforderungskriterien bezüglich der Auswahl einer FDE-Lösung für den Einsatz am Fraunhofer CNT tabellarisch zusammengefasst. Die untersuchten Softwareprodukte zur Festplattenverschlüsselung werden dabei entsprechend den im Rahmen der vorliegenden Arbeit durchgeführten Untersuchungen bewertet. Die Tabelle ist wie folgt strukturiert:

- Die Produkte werden mit einer Skala von -1 bis 1 auf Grund der ermittelten Ergebnisse bewertet. Die Bewertungsskala ist wie folgt definiert:

    -1: Merkmal wird nicht unterstützt (siehe grün markierter Bereich in der Tabelle 2);
    Mangelhafte Leistung im Vergleich zu den anderen untersuchten FDE-Lösungen;

    0: mittelmäßige Leistung im Vergleich zu den anderen untersuchten FDE-Lösungen;

    1: Merkmal wird unterstützt (siehe grün markierter Bereich in der Tabelle 2);
    Sehr gute Leistung im Vergleich zu den anderen untersuchten FDE-Lösungen;

Bei den Anforderungskriterien im grün markierten Bereich der Tabelle 2 sind Funktionen aufgelistet, die entweder von dem jeweiligen Softwareprodukt unterstützt werden oder nicht. Somit werden sie entweder mit -1 (nicht unterstützt) oder mit 1 (unterstützt) bewertet.

- Die Spalten TrueCrypt, PGP, SGN (Sophos) und McAfee enthalten die Bewertungen der betrachteten Produkte. Dabei steht „PGP“ für die gesamte FDE-Softwarelösung von Symantec (PGP Universal Server & PGP WDE) und „McAfee“ für die gesamte untersuchte Konfiguration von McAfee (ePO, EEPC & EEFF).

- Die ausgewählten Bewertungskriterien und die durchgeführte Bewertung sind auf die Anforderungen des Fraunhofer CNT ausgerichtet. Somit wird kein Anspruch auf Vollständigkeit erhoben.

FDE-Lösung / Bewertungskriterien	TrueCrypt	PGP	SGN (Sophos)	McAfee
Unterstützung von SSD-Festplatten	1	1	1	1
Unterstützung von AES-NI-Technologie	1	1	0[37]	1
Passwortwiederherstellung	-1	1	1	1
Single-Sign-On	-1	1	1	1
Systemwiederherstellung	1	1	1	1
Zentrale Verwaltung	-1	1	1	1
Verschlüsselung von Wechselmedien	1	1	1	1
Pre-Boot-Authentifikation	1	1	1	1
Kopiergeschwindigkeit	1	1	0	-1
Lesegeschwindigkeit	1	1	-1	-1
Schreibgeschwindigkeit	0	1	1	-1
Unternehmensfreundlich	-1	1	1	1
Administratorfreundlich	-1	1	-1	0
Benutzerfreundlich (Clientseite)	1	1	1	1
Grafische Benutzeroberfläche (Serverseite)	-1	1	0	0
Energieverbrauch	-1	1	-1	0
Installationsgröße (Clientseite)	1	0	1	0
RAM-Belastung (im Ruhezustand)	-1	-1	-1	1
CPU-Auslastung (siehe Abschnitt 12.3.1)	-1	-1	0	0
Authentifikationsmethodenvielfalt	0	1	1	1
Gesamtdokumentation (inkl. Videos, Foren u.Ä.)	1	1	1	1
Service (Vorhandensein, Kompetenz, Reaktionszeit)	-1	1	1	1
Einrichtungsaufwand	1	0	-1	0
Gesamtbewertung:	1	16	10	10

Tabelle 2. Bewertung der untersuchten FDE-Lösungen.

Dabei erreicht TrueCrypt eine niedrige Gesamtbewertung. Das Produkt erfüllt zwar die Grundbedingungen für die sichere Festplattenverschlüsselung mobiler Geräte, aber es ist für den Unternehmenseinsatz im Vergleich zu den untersuchten kommerziellen FDE-

[37] Es konnte keine Information darüber gefunden werden, ob die untersuchte FDE-Lösung von Sophos die AES-NI-Technologie unterstützt oder nicht.

Lösungen durch fehlende Grundfunktionen, wie zum Beispiel die fehlende Wartung (nur Community-Unterstützung bei Problemen mit der Software vorhanden) eher nicht geeignet.

Bei den betrachteten kommerziellen Produkten erreichen die FDE-Lösungen von Sophos und McAfee die gleiche Gesambewertung. Beide Softwarepakete liefern die gewünschte Funktionalität und bieten eine professionelle und leicht skalierbare Plattform zur Verwaltung der zu verschlüsselnden mobilen Endgeräte. Dabei weisen sie aber Mängel bezüglich der Ausnutzung der Systemressourcen und der erreichten Kopiergeschwindigkeiten auf.

Die Bewertung wird von der FDE-Lösung von Symantec geführt. Das PGP-Softwarepaket hat in den meisten Vergleichskriterien gute Ergebnisse geliefert und erfüllt die gewünschte Funktionalität, wobei es eine breite Palette an Steuerungsoptionen und Rollenmöglichkeiten sowohl für Administratoren, als auch für Endnutzer bietet. Nachteilig sind jedoch die hohen CPU- und RAM-Auslastung, sowie der hohe Energieverbrauch.

Als Ergebnis der durchgeführten Bewertung und des allgemeinen Produkteindruckes während der Testphase wird die softwarebasierte FDE-Lösung von Symantec als geeignetster Kandidat ausgewählt und für den Einsatz im Fraunhofer CNT empfohlen. Im nächsten Abschnitt werden die nach dieser Studie folgenden Maßnahmen geschildert, die die endgültige Produktauswahl beeinflussen können (siehe Schritt 4 des unternehmensinternen Auswahl- und Einführungsschemas im Abschnitt 13.2).

13.2 Unternehmensinterne Implementierung

Die Auswahl und Einführung von komplexen Softwaresystemen in eine vorhandene IT-Infrastruktur eines Unternehmens, einer Einrichtung bzw. Organisation sind ein wichtiger, zeitaufwändiger und oft komplexer Prozess, besonders wenn er nicht gut vorbereitet wird. Aktuelle Softwareprodukte müssen unabhängig von der Funktionalität hohen Anforderungen an Datenschutz, Verfügbarkeit, Performance und Benutzerfreundlichkeit genügen. Andererseits sollen sie in heterogene Systemlandschaften möglichst gut integrierbar bzw. ausführbar sein.

Um den Prozess zur Auswahl und Einführung einer geeigneten Festplattenverschlüsselungssoftware für das Fraunhofer CNT möglichst zu systematisieren und zu erleichtern, wird unternehmensintern folgender Leitfaden eingesetzt:

Bereits durchgeführte Schritte:

1. Anforderungen festlegen.

   Die Fraunhofer Gesellschaft verfügt über ein eigenes IT-Sicherheitshandbuch, das die gültigen Regeln, Verantwortlichkeiten und Mindestmaßnahmen zur Sicherung der Informationstechnik für alle Fraunhofer Einrichtungen beschreibt. Durch die darin enthaltene Richtlinie für den Umgang mit mobilen Endgeräten wird die Festplattenverschlüsselung strengstens empfohlen.

2. Marktrecherche: Welche Produkte eignen sich am besten.

   Dieser Schritt wurde in der Vorbereitungsphase der vorliegenden Arbeit durchgeführt (siehe Abschnitt 4.2).

3. Evaluierungsphase: Drei bis vier Produkte in der engeren Auswahl installieren und im Praxistest prüfen.

   Dieser Schritt entspricht den in der vorliegenden wissenschaftlichen Arbeit durchgeführten Tests.

Bevorstehende Schritte:

4. Finanzierung sichern und die Lizenzen für das Produkt der Wahl erwerben: Unternehmens-politisch bedingt.

5. Installation der Managementumgebung, Einführung (Rollout) für die Clients vorbereiten.

6. Testphase mit Testrechnern.

7. Zwei bis drei Nutzer das Produkt testen lassen.

8. Einführung (Rollout) der Software.

In den ersten drei Stufen des vorgestellten Ablaufschemas werden die Argumente und Fakten gesammelt, die zur Entscheidung für ein passendes Festplattenverschlüsselungsprodukt beitragen. Der vierte Schritt ist unternehmens-politisch bedingt. Dabei werden im konkreten Fall die genauen Preise für die softwarebasierten FDE-Lösungen ermittelt, da sie im Rahmen der durchgeführten Untersuchung aus organisatorisch-rechtlichen Gründen nicht von den Produktanbietern abgefragt werden durften. Somit werden die bei der vorliegenden Arbeit gewonnen Erkenntnisse zwar in Betracht gezogen, der Auswahlprozess wird aber maßgeblich durch die Finanzierung, die Investitionssicherheit und die bei der Fraunhofer Gesellschaft vorhandenen Lizenzen beeinflusst.

In der nächsten Phase wird die ausgewählte Software auf ein bis zwei Testrechnern installiert und eingerichtet. Somit werden eventuelle Probleme beim Installations- und Einrichtungsvorgang durch den Administrator ausgeschlossen bzw. entsprechend bereinigt.

Im achten Schritt wird die Clientseite der Software von zwei bis drei Nutzern getestet. Somit können eventuelle Unklarheiten bei der Benutzung des Produkts festgestellt werden, um darauf entsprechend reagieren zu können (zum Beispiel durch gezielte Schulungen der Endnutzer).

Abschließend wird die FDE-Lösung unternehmensweit eingeführt. Die Integration der ausgewählten Software zur Festplattenverschlüsselung in die bestehende Organisationsstruktur erfolgt dabei analog zu der Einrichtung der jeweiligen Testumgebung, die in der vorliegenden Arbeit bereits beschrieben wurde (siehe Abschnitte 8-12).

13.3 Zusammenfassung und Ausblick

Die durch die Aufgabenstellung gesetzten Anforderungen für die Auswahl und die Untersuchung bzw. den Vergleich professioneller Software zur Festplattenverschlüsselung konnten erfüllt bzw. erfolgreich durchgeführt werden. Es wurden vier FDE-Lösungen bestimmt, die im Detail betrachtet wurden. Dabei wurden sie in der zur Verfügung gestellten Testumgebung installiert und in die IT-Infrastruktur

vom Fraunhofer CNT entsprechend integriert. Es wurde nicht nur ihre Funktionalität sondern zusätzlich ihr Einfluss auf die Leistung des Testsystems untersucht. Die betrachteten FDE-Lösungen weisen dabei sowohl viele Ähnlichkeiten, als auch wesentliche Unterschiede auf, die im Folgenden kurz zusammengefasst werden:

- TrueCrypt: Diese FDE-Lösung bietet eine direkte und unkomplizierte Installation und Nutzung auf der Endbenutzerseite, wobei für die Softwareeinrichtung keine besonderen technischen Voraussetzungen erforderlich sind und vernachlässigbar wenig Speicherplatz benötigt wird. Bei den Leistungsuntersuchungen tritt TrueCrypt durch einen hohen Energieverbrauch sowie hohe RAM- und CPU-Belastung hervor. Dazu konnte das Produkt mit guten Lese-, Schreib- und Kopierzugriffsgeschwindigkeiten im Vergleich zu den anderen FDE-Lösungen und dem unverschlüsselten System überzeugen. Das Produkt ist kostenlos, Open Source und für die Clientseite konzipiert. Für den Unternehmenseinsatz fehlen jedoch wichtige Funktionalitäten, wie eine zentrale Verwaltungseinheit, zuverlässige technische Unterstützung, Single-Sign-On und Passwortwiederherstellung.

- PGP: Das von Symantec angebotene Produkt bietet eine professionelle FDE-Lösung, die speziell für Unternehmensstrukturen konzipiert ist. Es kann vollständig in die Unternehmensinfrastruktur integriert werden. Das Softwarepaket bietet eine einfache und verständliche Navigation, sowohl auf der Verwaltungsseite (Serverseite) als auch auf der Endbenutzerseite (Clientseite). Es ist ein breites Angebot an Benutzer- und Administratoreinstellungen vorhanden. Das mit PGP WDE verschlüsselte System hat bei dem Leistungstest den Prozessor und den Arbeitsspeicher am meisten belastet, wies aber den niedrigsten Energieverbrauch gegenüber den anderen verschlüsselten Systemen auf. Bei den gemessenen Zugriffsgeschwindigkeitswerten bei Lese-, Schreib und Kopiervorgängen hat das Produkt ähnliche Leistungen wie das unverschlüsselte System gezeigt. Zusammenfassend hat die von Symantec angebotene FDE-Lösung die beste Gesamtbewertung erhalten und wird für den Unternehmenseinsatz am Fraunhofer CNT empfohlen.

- SGN: Safeguard Enterprise ist die kommerzielle FDE-Lösung von Sophos für den Unternehmenseinsatz, die eine umfangreiche und komplexe Verwaltungseinheit für die Unternehmensstruktur bietet. Durch unterschiedliche Richtlinientypen und ihre Einstellungen kann eine feingranulare und exakte Steuerung der Clientgeräte und der Endnutzereinstellungen erreicht werden. Bei den Leistungstests hat diese Verschlüsselungssoftware den höchsten Energieverbrauch verursacht. Der Arbeitsspeicher wird zwar ähnlich wie von PGP und TrueCrypt belastet, dafür hält sich die CPU-Auslastung, vergleichbar mit dem Verschlüsselungsprodukt von McAfee, in Grenzen. Das mit SGN verschlüsselte System zeichnet sich durch eine hohe Schreibgeschwindigkeit, aber auch niedrige Lese- und Kopiergeschwindigkeiten im Vergleich zum unverschlüsselten System aus.

- McAfee EE: McAfee bietet eine professionelle FDE-Lösung als Teil der Palette von Softwareprodukten zu Sicherung von IT-Infrastrukturen für den Unternehmenseinsatz an. Die zentrale Management-Konsole (ePO) erlaubt das Anbinden von unterschiedlichen Softwarepaketen und stellt ein sehr komplexes und mächtiges Verwaltungswerkzeug dar. Die Steuerung der Endgeräte und der Endnutzereinstellungen wird genau wie bei den anderen untersuchten kommerziellen FDE-Lösungen durch Richtlinien realisiert, die produktspezifisch organisiert sind. Bei den Leistungstests hat das mit EEPC verschlüsselte System eine äußerst geringe, zusätzliche Hauptspeicherbelastung verursacht. Die zusätzliche Prozessorauslastung ist im Vergleich zu den anderen verschlüsselten Systemen am niedrigsten und auch der Energieverbrauch hält sich in Grenzen. Bei den getesteten Lese-, Schreib- und Kopiervorgängen erreicht das Produkt jedoch nur die niedrigsten Geschwindigkeiten aller untersuchten FDE-Lösungen.

Alles in allem hat sich ergeben, dass die Arbeit auf den verschlüsselten Endgeräten mit einer höheren Ressourcenauslastung im Vergleich zum unverschlüsselten System verbunden ist.

Es muss jedoch in Betracht gezogen werden, dass trotz der gegenwärtigen Sicherheit des von den betrachteten FDE-Lösungen eingesetzten Verschlüsselungsalgorithmus

AES-256, die verschlüsselten Systeme nicht gegen Datenverlust jeglicher Art gesichert sind. Die Festplattenverschlüsselung sichert die Daten hauptsächlich für den Fall des Verlustes bzw. des Diebstahls von Laptops und externer Wechselspeichermedien. Um die Endgeräte besser zu schützen, sollten auch weitere Sicherheitsmaßnahmen eingesetzt werden.

Folgende Themengebiete stellen einen Ausblick über empfehlenswerte Wartungsarbeiten bzw. weiterführende Forschungsaufgaben dar:

- Es können weitere, feinere Messungen und tiefer gehende Analysen der betrachteten Software durchgeführt werden, um ihren gesamten Funktionalitätsumfang auszutesten und um ihre Möglichkeiten und Grenzen zu ermitteln.

- Es werden immer wieder neue Schwachstellen in den Verschlüsselungsalgorithmen (siehe z.B. Abschnitt 7.1.3) entdeckt bzw. neue Angriffsstrategien entwickelt, die die Verschlüsselungstechniken umgehen, um an den Daten heranzukommen. Deswegen ist es wichtig, dass der aktuelle Stand der in einem Unternehmen eingesetzten Sicherheitsmaßnahmen regelmäßig überprüft und bei Bedarf entsprechend angepasst wird.

- TrueCrypt bietet eine kostenfreie FDE-Lösung, die von der Funktionalität her keine Mängel gegenüber den kommerziellen Lösungen aufweist. Durch die fehlende Managementkonsole ist die Software jedoch für den Unternehmenseinsatz ungeeignet. Ein interessantes Forschungsprojekt wäre somit der Entwurf und die Implementierung einer zentralen Verwaltung für TrueCrypt.

- Bei allen untersuchten verschlüsselten Testrechnern wurde ein höherer Energieverbrauch im Vergleich zu dem unverschlüsselten System festgestellt. Für mobile Endgeräte ist jedoch Energie und Batterieausdauer ein wichtiger und oft kritischer Parameter. Ein mögliches Forschungsgebiet wäre somit die Verbesserung der Energieeffizienz von Verschlüsselungssoftware. Es kann auch

am Beispiel von TrueCrypt im Rahmen eines öffentlichen wissenschaftlichen Projekts erfasst werden.

Zum Schluss muss jedoch nochmals betont werden, dass die vorgestellten Produktfunktionalitäten einen Bruchteil der Möglichkeiten der untersuchten Softwareprodukte darstellen. Die Ergebnisse und die Auswertung bzw. Bewertung der FDE-Lösungen wurden ausschließlich an den Anforderungen und der IT-Infrastruktur des Fraunhofer CNT und der genutzten Testumgebung ausgerichtet.

Literaturverzeichnis

[aes01] Specification for the ADVANCED ENCRYPTION STANDARD (AES), 2001
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[aes11] Erster Kratzer für Kryptoalgorithmus AES, Stand: August 2011
http://www.heise.de/security/meldung/Erster-Kratzer-fuer-Kryptoalgorithmus-AES-1324532.html

[Auf09] Richard Aufreiter, 2009: Software- oder Hardwareverschlüsselung
http://www.all-about-security.de/kolumnen/thema-des-monats/artikel/9825-utimaco-safeware-software-oder-hardwareverschluesselung/

[BBC11a] BBC Online: Discs 'worth J1.5bn' to criminals, Stand: June 2011

http://news.bbc.co.uk/2/hi/uk_news/politics/7117291.stm

[BBC11b] BBC Online: UK's families put on fraud alert, Stand: June 2011
http://news.bbc.co.uk/2/hi/7103566.stm

[Bea01] Steve Beaumont, 2001: Microsoft BitLocker Administration and Monitoring (MBAM)
http://systemscentre.blogspot.com/2011/08/microsoft-bitlocker-administration-and.html

[CH09] Christian Halusa, Martin Huber, Peter Mayer, 2009: Sicherheitsaspekte bei Full Disk Encryption
http://www.all-about-security.de/kolumnen/thema-des-monats/artikel/9009-secaron-ag-grundsaetzlich-muss-bei-fde-zwischen-zwei-aufgabe/

[CJK07] Charles J. Kolodgy, Gerry Pintal, 2007: Laptops mit umfassender Festplattenverschlüsselung absichern. *IDC*

[dum11] Dummy File Creator, Version 1.2, 2011
www.mynikko.com/dummy

[ea11] Robert Basmadjian et. al, 2011: A Methodology to Predict the Power Consumption of Servers in Data Centers

[mc111] McAfee ePolicy Orchestrator - Datenblatt, 2011
http://www.mcafee.com/de/resources/data-sheets/ds-epolicy-orchestrator.pdf

[mc211] McAfee Endpoint Encryption - Datenblatt, 2011
http://www.mcafee.com/de/resources/data-sheets/ds-endpoint-encryption.pdf

[mc311] McAfee ePolicy Orchestrator, 2011
http://www.mcafee.com/de/products/epolicy-orchestrator.aspx

[mc411] McAfee ePolicy Orchestrator 4.6.0 - Installation Guide, 2011
https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/22000/PD22974/en_US/epo_460_install_guide_en-us.pdf

[mc511] McAfee ePolicy Orchestrator 4.6.0 Software - Product Guide, 2011.
https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/22000/PD22975/en_US/epo_460_product_guide_en-us.pdf

[mc611] Quick Start Guide - EEFF 4.0.0, 2011
https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/23000/PD23272/en_US/eeff_4400_quick_start_guide_en-us.pdf

[mc711] Quick Start Guide - EEPC 6.1, 2011
https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/23000/PD23084/en_US/eepc_quick_start_guide_en-us.pdf

[Mic10] Microsoft. Microsoft Security Intelligence Report, Ausgabe 10, Juli - Dezember 2010.

[NF01] Niels Ferguson, Richard Schroeppel, Doug Whiting, 2001: A simple algebraic representation of Rijndael
http://www.macfergus.com/pub/rdalgeq.pdf

[Pfi10] Andreas Pfitzmann, 2010: *Sicherheit in Rechnernetzen: Mehrseitige Sicherheit in verteilten und durch verteilte Systeme*; Skript zu den Vorlesungen „Security and Cryptography“ I+II, Fakultät Informatik an der Technischen Universität Dresden

[pgp] Universal Server 30 Day Whole Disk Evaluation Quick Start Guide

[pgp11a] PGP Universal Server, 2011
http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-pgp_universal_server_DS_21064413.en-us.pdf

[pgp11b] PGP Whole Disk Encryption, 2011
http://www.symantec.com/de/de/business/products/sysreq.jsp?pcid=pcat_info_risk_comp&pvid=wd_encryption_1

[pgp11c] PGP Universal Server from Symantec - Data Sheet, 2011
http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-pgp_universal_server_DS_21064413.en-us.pdf

[pgp11d] PGP Universal Server Administrator's Guide, 2011
http://www.symantec.com/business/support/index?page=content&id=DOC3598

[Ram11] Thomas Ramming, 2011: *Elektronische Untersuchungsanforderungen für Labor und Radiologie: Eine Usability-Studie zur Bewertung klinischer Anwendungen*, Medizinische Fakultät der Friedrich-Alexander-Universität Erlangen-Nürnberg

[Rep11] Markus Repges: Der Advanced Encryption Standard, Stand: June 2011.
http://www.repges.net/AES-Kandidaten/AES/aes.htm

[Sch10] Jürgen Schmidt, 2010: NIST-zertifizierte USB-Sticks mit Hardware-Verschlüsselung geknackt
http://www.heise.de/security/meldung/NIST-zertifizierte-USB-Sticks-mit-Hardware-Verschluesselung-geknackt-894962.html

[sgn11a] SafeGuard Enterprise, Stand: August 2011
http://www.sophos.com/de-de/products/encryption/safeguard-enterprise.aspx

[sgn11b] Sophos Support Knowledgebase, Stand: August 2011
http://de.sophos.com/support/knowledgebase/

[sgn11c] SafeGuard Enterprise - Administrator Hilfe, April 2011
http://de.sophos.com/sophos/docs/deu/manuals/sgn_56_h_deu_administrator_hilfe.pdf

[sgn11d] SafeGuard Enterprise Installation best practice, April, 2011
http://www.sophos.com/sophos/docs/eng/manuals/sgn_bpg_eng_installation_best_practice.pdf

[sgn11e] SafeGuard Device Encryption - Recovery Options, May 2011
http://www.sophos.com/sophos/docs/eng/manuals/Utimaco/KBA/108156_RecoverySGDE.pdf

[Sta08] StarShaper, Laurent Haan, 2008: Advanced Encryption Standard (AES)
http://www.codeplanet.eu/tutorials/cpp/51-advanced-encryption-standard.html#aes_introduction

[tce11] TrueCrypt Version 7.0a - Evaluation Report, 2011
http://www.justnet.org/Documents/ECT_CoE/00-TrueCrypt-report-0329.pdf

[tdt11] taz. die tageszeitung, 2011: Datenverlust on the Road
http://www.taz.de/!68282/

[tru11] TrueCrypt, Stand:June 2011:
http://www.truecrypt.org/

[US07] Uwe Schneider, Dieter Werner, 2007: *Taschenbuch der Informatik*, Fachbuchverlag Leipzig im Carl Hanser Verlag

[wik11a] Wikipedia: *Cognitive Walkthrough*, Stand: Juli 2011
http://de.wikipedia.org/wiki/Cognitive_Walkthrough

[wik11b] Wikipedia: *Festplattenverschlüsselung*, Stand: Juni 2011
http://de.wikipedia.org/wiki/Festplattenverschl%C3%BCsselung

[wik11c] Wikipedia: *Full Disk Encryption*, Stand: Juni 2011
http://de.wikipedia.org/wiki/Full_Disk_encryption

[Wil04] Christian Wilkin, 2004: Der Algorithmus des "Advanced Encryption Standard"

Abkürzungsverzeichnis

AES	Advanced Encryption Standard
AES-NI	Advanced Encryption Standard instruction set
CNT	Center für Nanoelektronische Technologien
DES	Data Encryption Standard
EEFF	Endpoint Encryption for Files and Folders
EEPC	Endpoint Encryption for PC
EERM	Endpoint Encryption for Removable Media
ePO	ePolicy Orchestrator
FDE	Full Disk Encryption
FhG	Fraunhofer Gesellschaft
GUI	Graphical User Interface
NIST	National Institute of Standards and Technology
POA	Power-on Authentication (Pre-Boot-Authetifikation von SGN)
PGP	Pretty Good Privacy
PGP WDE	PGP Whole Disk Encryption
SGE	SafeGuard Easy
SGN	SafeGuard Enterprise
TUD	Technische Universität Dresden
TU-Dresden	Technische Universität Dresden
WDRT	Whole Disk Recovery Token

ZIH	Zentrum für Informationsdienste und Hochleistungsrechner

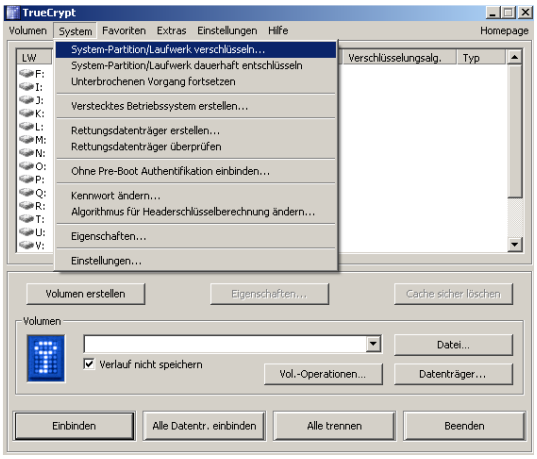
Abbildungsverzeichnis

Tabellenverzeichnis

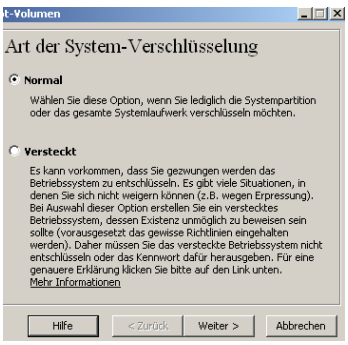
Anhang

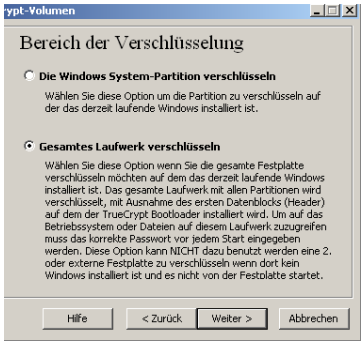
Anhang A: TrueCrypt-Systemverschlüsselungsvorgang

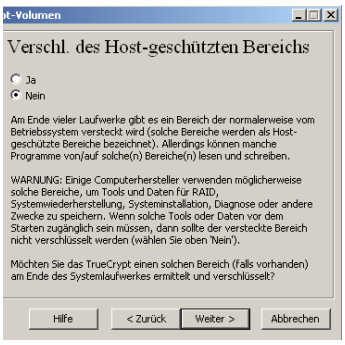
1.



2.



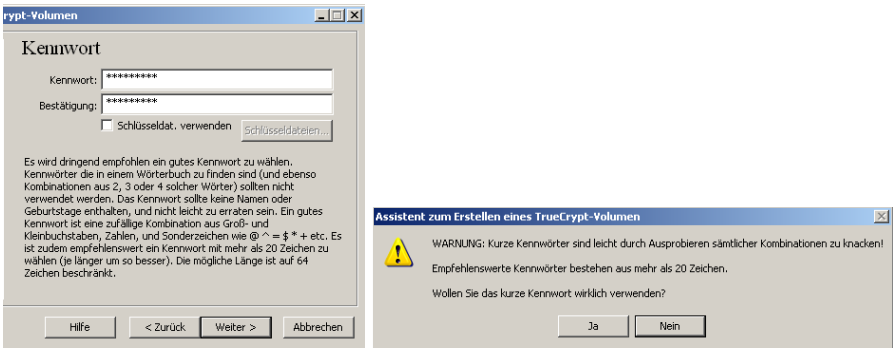




3.


Assistent zum Erstellen eines TrueCrypt-Volumen
Verschlüsselungseinstellungen
Verschlüsselungsalgorithmus
AES
Test
Ist von der FIPS genehmigter Blockchiffre (Rijndael, 1998 veröffentlicht) und wird z.B.von den U.S. Regierungbehörden und Agenturen genutzt um Dokumente mit bis zu höchster Geheimhaltung zu schützen. 256-bit Schlüssellänge, 128-bit Blockgröße, 14 Runden (AES-256). Arbeitet im XTS-Modus.
Weitere Informationen über AES
Benchmark
Hash-Algorithmus
RIPEMD-160
Infos über Hash-Algorithmen
Hilfe
< Zurück
Weiter >
Abbrechen

4.


rypt-Volumen
Kennwort
Kennwort:
Bestätigung:
Schlüsseldat. verwenden
Schlüsseldateien...
Es wird dringend empfohlen ein gutes Kennwort zu wählen. Kennwörter die in einem Wörterbuch zu finden sind (und ebenso Kombinationen aus 2, 3 oder 4 solcher Wörter) sollten nicht verwendet werden. Das Kennwort sollte keine Namen oder Geburtstage enthalten, und nicht leicht zu erraten sein. Ein gutes Kennwort ist eine zufällige Kombination aus Groß- und Kleinbuchstaben, Zahlen, und Sonderzeichen wie @ ^ = $ * + etc. Es ist zudem empfehlenswert ein Kennwort mit mehr als 20 Zeichen zu wählen (je länger um so besser). Die mögliche Länge ist auf 64 Zeichen beschränkt.
Hilfe
< Zurück
Weiter >
Abbrechen
Assistent zum Erstellen eines TrueCrypt-Volumen
WARNUNG: Kurze Kennwörter sind leicht durch Ausprobieren sämtlicher Kombinationen zu knacken!
Empfehlenswerte Kennwörter bestehen aus mehr als 20 Zeichen.
Wollen Sie das kurze Kennwort wirklich verwenden?
Ja
Nein

5.


Assistent zum Erstellen eines TrueCrypt-Volumen
Zufällige Daten sammeln
Aktueller Inhalte-Pool (teilweise)
BE 20 EE FC 49 92 CF EB 9B 49 F5 AC EF BB 0B
84 7F 3D 87 06 2E CA 2A B9 9A C2 3C 06 52 21
7F E3 F2 37 F0 7F 3C 1A 86 A8 2C F6 51 71 27
01 16 CF B4 0D 36 C3 3B A4 10 C2 51 B7 22 1E
EB 41 72 BF 6F 82 97 9C A6 1D FD D1 8A 4A BC
66 36 87 63 BE B2 61 50 50 4A 93 46 62 8C 97
28 CE B2 FA EC 19 F1 20 5B 1E 2C 94 E0 75 7A
26 60 61 18 A9 38 11 9F A2 55 C1 60 13 64 95
Pool-Inhalt anzeigen
Wichtig: Den Mauszeiger in diesem Fenster zufällig hin und her bewegen. Je länger (min. 30 Sek.) Sie die Maus bewegen, desto besser. Dies trägt zu einer verbesserten Verschlüsselung bei. Klicken Sie dann auf 'Weiter' um fortzufahren.
Hilfe
< Zurück
Weiter >
Abbrechen

6.


Assistent zum Erstellen eines TrueCrypt-Volumen
Schlüssel generieren
Die Schlüssel, Salt-Wert, und andere Daten wurden erfolgreich erstellt. Wenn Sie neue Schlüssel erstellen möchten, klicken Sie auf 'Zurück' und dann auf 'Weiter'. Andernfalls klicken Sie auf 'Weiter'.
Headerschlüssel: DA8B9376488EEA8E0158648BD0F813A6...
Hauptschlüssel: C6FEA2DD617E92638AC75CB173A3AB8B...
Generierte Schlüssel anzeigen (deren Teile)
Hilfe
< Zurück
Weiter >
Abbrechen

7.


Rettungsdatenträger
Bevor sie die Partition/das Laufwerk verschlüsseln können müssen Sie eine TrueCrypt Rettungs-CD (TRD) erstellen, die für die folgenden Fälle notwendig ist:
- Wenn der TrueCrypt Bootloader, der Hauptschlüssel oder andere kritische Daten beschädigt werden, erlaubt die TRD diese Daten wieder herzustellen (Sie benötigen trotzdem das korrekte Passwort).
- Wenn Windows beschädigt wird und nicht starten kann ermöglicht die TRD es die Partition/das Laufwerk vor dem Systemstart dauerhaft zu entschlüsseln.
- Die TRD enthält eine Sicherung des derzeitigen Inhaltes des ersten Datenblocks (Header) der Partition/des Laufwerks (welcher normalerweise einen Systemstarter oder Bootmanager enthält) und erlaubt es diesen, falls nötig, wieder herzustellen.
Das TrueCrypt Rettungs-CD Abbild (Image) wird hier erstellt:
C:\Documents and Settings\angelova\My Docume
Suchen...
Hilfe
< Zurück
Weiter >
Abbrechen
Rettungsdatenträger brennen
Das TrueCrypt Rettungs-CD Abbild (Image) wurde erfolgreich erstellt und an folgendem Ort gespeichert:
C:\Documents and Settings\angelova\My Documents\TrueCrypt Rescue Disk.iso
Jetzt müssen Sie es auf eine CD oder DVD brennen.
WICHTIG: Bitte beachten Sie, dass die Datei als ISO Imagedatei und NICHT als einzelne Datei auf die CD geschrieben werden muss. Informationen wie Sie das tun erhalten Sie in der Dokumentation Ihrer Brennsoftware. Wenn Sie keine CD/DVD Brennsoftware besitzen, welche das ISO-Abbild auf eine CD/DVD schreiben kann, klicken Sie auf den unten stehenden Link um ein freies Programm herunterzuladen.
Nachdem Sie das getan haben, klicken Sie bitte "Weiter" um die Korrektheit der Rettungs-CD zu überprüfen.
Download einer CD/DVD Brennsoftware
Hilfe
< Zurück
Weiter >
Abbrechen
Rettungsdatenträger überprüfen
Der TrueCrypt Rettungsdatenträger wurde erfolgreich überprüft. Bitte entfernen Sie diesen aus dem Laufwerk und bewahren Sie es an einen sicheren Ort auf.
Klicken Sie "Weiter" um fortzufahren.
Hilfe
< Zurück
Weiter >
Abbrechen

8.


Assistent zum Erstellen eines TrueCrypt-Volumen
Sicher Löschen
Lösch-Modus: Ohne (am schnellsten)
Bei einigen Typen von Speichermedien könnten Daten, die überschrieben wurden, mithilfe der Magnetkraftmikroskopie wiederhergestellt werden. Dies gilt auch für Daten, die in Ihrer verschlüsselten Form überschrieben wurden (was passiert, wenn TrueCrypt erstmals unverschlüsselte Partitionen oder Laufwerke verschlüsselt). Einige Studien und öffentliche Publikationen geben an, dass die Wiederherstellung von überschriebenen Daten verhindert (oder zumindest erschwert) werden kann, indem die Daten mit pseudo-zufälligen und bestimmten nicht zufälligen Daten überschrieben werden. Wenn Sie glauben, dass ein Angreifer möglicherweise solche Techniken verwenden könnte um Ihre verschlüsselten Daten wiederherzustellen, dann sollten Sie einen der Lösch-Modi wählen (vorhandene Daten gehen NICHT verloren). Das Löschen kann NICHT ausgeführt werden nachdem die Partition/ das Laufwerk verschlüsselt wurde. Dann werden alle Daten nämlich zuerst im Speicher verschlüsselt und erst dann auf den Datenträger geschrieben.
Hilfe
< Zurück
Weiter >
Abbrechen

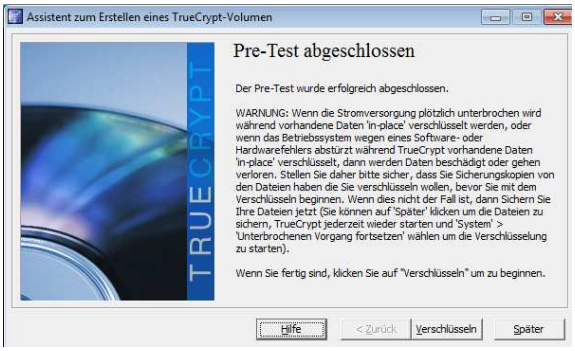
9.


Assistent zum Erstellen eines TrueCrypt-Volumen
Systemverschlüsselungs-Pre-Test
Bevor das Verschlüsseln Ihrer Systempartition oder Ihres Laufwerkes beginnen kann, muss TrueCrypt überprüfen ob alles ordnungsgemäß funktioniert.
Nach dem Sie auf "Test" klicken werden alle notwendigen Komponenten (z. B. die Pre-Boot Authentifikations-Komponente, d. h. der TrueCrypt Bootloader) installiert und Ihr Computer wird dann neu gestartet. Anschließend müssen Sie Ihr Kennwort im TrueCrypt Bootloader-Bildschirm eingeben, welcher angezeigt wird bevor Windows startet. Nachdem Windows gestartet wurde, werden Sie automatisch über das Ergebnis dieses Pre-Tests informiert.
Das folgende Laufwerk wird bearbeitet: Laufwerk #0
Wenn Sie jetzt auf Abbrechen klicken, dann wird der Pre-Test nicht ausgeführt.
TRUECRYPT
Hilfe
< Zurück
Test
Abbrechen
Assistent zum Erstellen eines TrueCrypt-Volumen
Warnung: Aufgrund von technischen Einschränkungen in der Pre-Boot Umgebung können Texte durch TrueCrypt in der Pre-Boot Umgebung (d. h. bevor Windows gestartet wird) nicht übersetzt angezeigt werden. Die Oberfläche des TrueCrypt Bootloader ist vollständig in Englisch.
Fortfahren?
Yes
No

10.

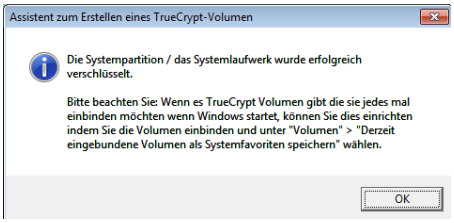

TrueCrypt Boot Loader 7.0
Keyboard Controls:
[Esc] Skip Authentication (Boot Manager)
Enter password: _

11.


Assistent zum Erstellen eines TrueCrypt-Volumen
Pre-Test abgeschlossen
Der Pre-Test wurde erfolgreich abgeschlossen.
WARNUNG: Wenn die Stromversorgung plötzlich unterbrochen wird während vorhandene Daten 'in-place' verschlüsselt werden, oder wenn das Betriebssystem wegen eines Software- oder Hardwarefehlers abstürzt während TrueCrypt vorhandene Daten 'in-place' verschlüsselt, dann werden Daten beschädigt oder gehen verloren. Stellen Sie daher bitte sicher, dass Sie Sicherungskopien von den Dateien haben die Sie verschlüsseln wollen, bevor Sie mit dem Verschlüsseln beginnen. Wenn dies nicht der Fall ist, dann Sichern Sie Ihre Dateien jetzt (Sie können auf 'Später' klicken um die Dateien zu sichern, TrueCrypt jederzeit wieder starten und 'System' > 'Unterbrochenen Vorgang fortsetzen' wählen um die Verschlüsselung zu starten).
Wenn Sie fertig sind, klicken Sie auf "Verschlüsseln" um zu beginnen.
TRUECRYPT
Hilfe
< Zurück
Verschlüsseln
Später

12.

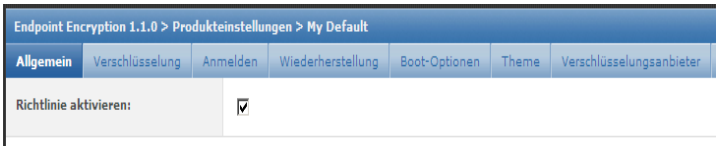

Assistent zum Erstellen eines TrueCrypt-Volumen
Verschlüsseln
Optionen
Lösch-Modus: Ohne (am schnellsten)
Pause
Fertig 1.996% Status verschlüsseln Rest 51 Minuten
Sie können jederzeit "Pause" oder "Später" klicken um den Ver- oder Entschlüsselungsprozess anzuhalten, diesen Assistenten verlassen, den Computer neu starten oder herunterfahren und den Prozess dann vom pausierten Punkt wieder aufnehmen. Um ein Verlangsamen des Computers zu verhindern wenn das System oder ein Programm auf das Systemlaufwerk zugreifen, wartet TrueCrypt automatisch bis die Daten geschrieben oder gelesen wurden (siehe Status oben) und fährt dann automatisch fort.
Mehr Informationen
Hilfe
< Zurück
Verschlüsseln
Später
TRUECRYPT

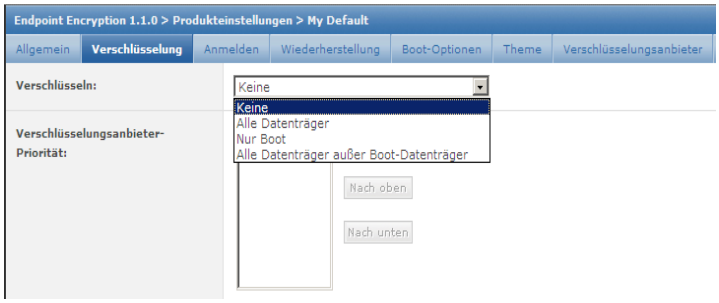

Assistent zum Erstellen eines TrueCrypt-Volumen
Die Systempartition / das Systemlaufwerk wurde erfolgreich verschlüsselt.
Bitte beachten Sie: Wenn es TrueCrypt Volumen gibt die sie jedes mal einbinden möchten wenn Windows startet, können Sie dies einrichten indem Sie die Volumen einbinden und unter "Volumen" > "Derzeit eingebundene Volumen als Systemfavoriten speichern" wählen.
OK

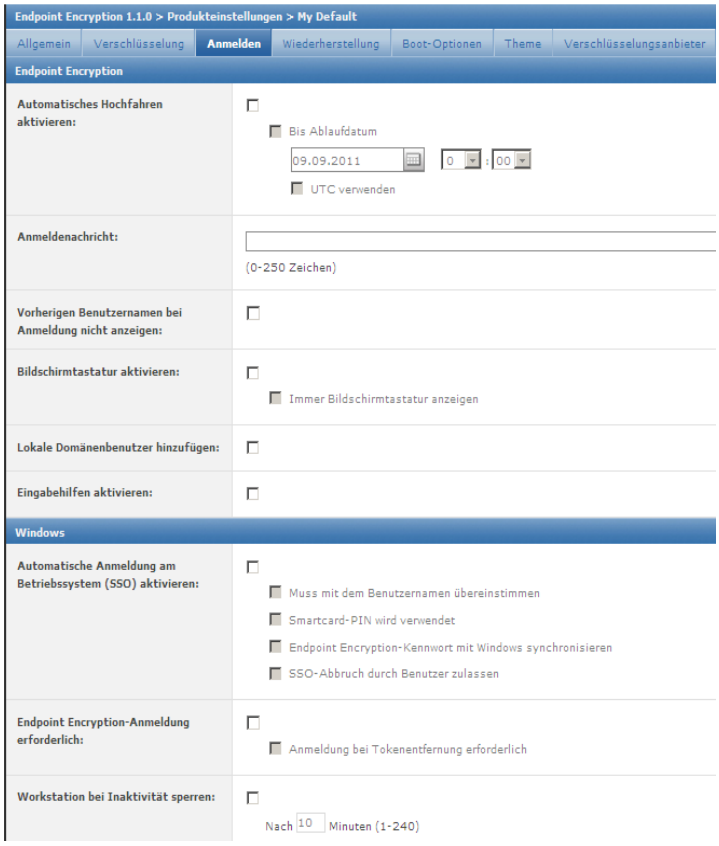

Assistent zum Erstellen eines TrueCrypt-Volumen
Verschlüsseln
Optionen
Lösch-Modus: Ohne (am schnellsten)
Weiter
Fertig 100% Status Fertig Rest
Sie können jederzeit "Pause" oder "Später" klicken um den Ver- oder Entschlüsselungsprozess anzuhalten, diesen Assistenten verlassen, den Computer neu starten oder herunterfahren und den Prozess dann vom pausierten Punkt wieder aufnehmen. Um ein Verlangsamen des Computers zu verhindern wenn das System oder ein Programm auf das Systemlaufwerk zugreifen, wartet TrueCrypt automatisch bis die Daten geschrieben oder gelesen wurden (siehe Status oben) und fährt dann automatisch fort.
Mehr Informationen
Hilfe
< Zurück
Fertig stellen
Später
TRUECRYPT

Anhang B: McAfee EEPC: Richtlinien

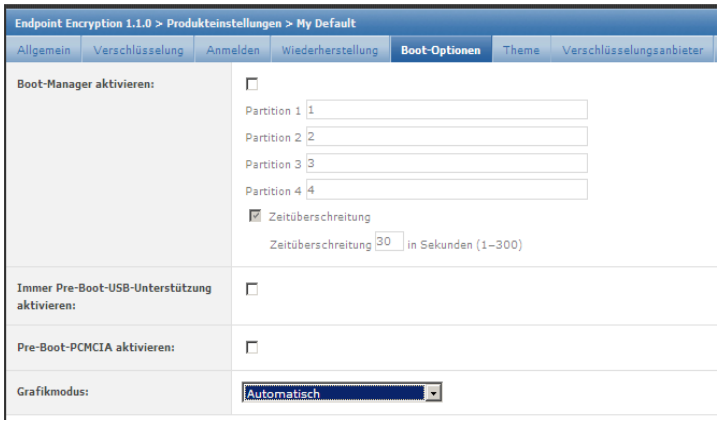
Produkteinstellungen:



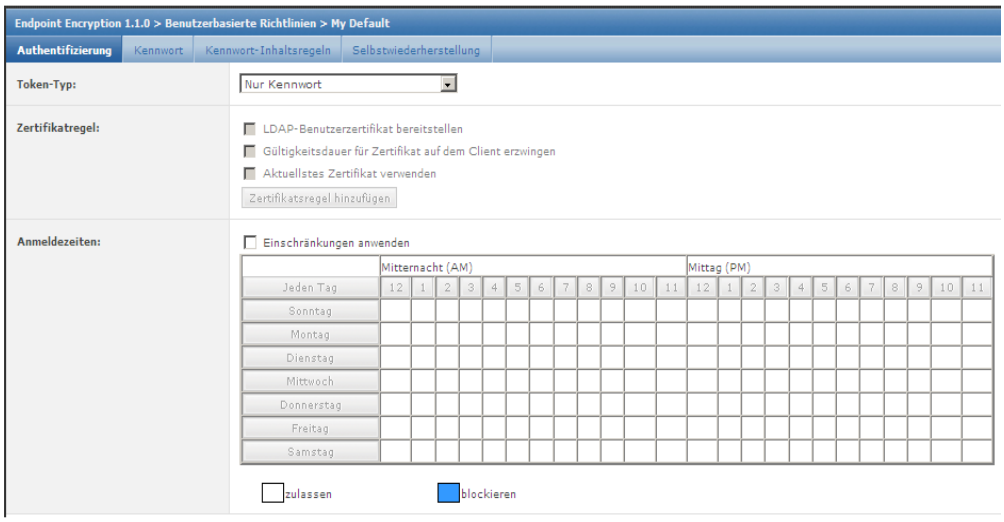


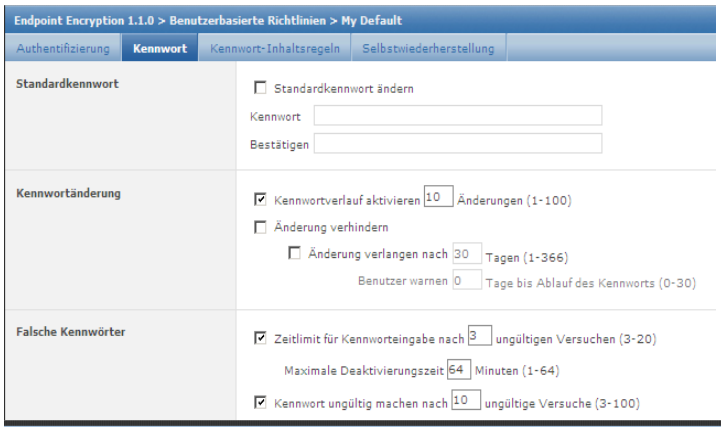


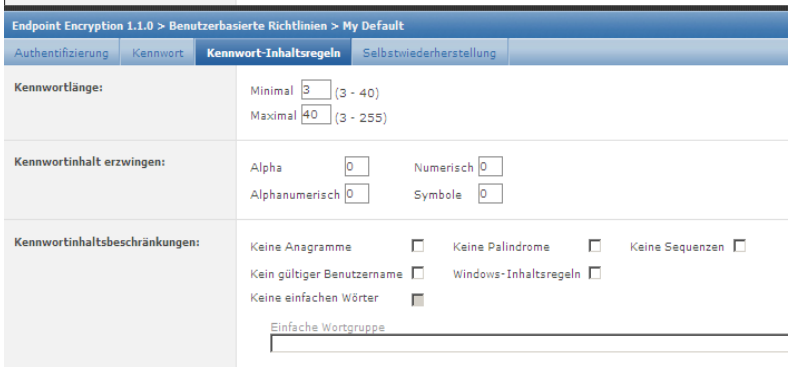

Endpoint Encryption 1.1.0 > Produkteinstellungen > My Default
Allgemein
Verschlüsselung
Anmelden
Wiederherstellung
Boot-Optionen
Theme
Verschlüsselungsanbieter
Aktiviert:
Schlüsselgröße:
Niedrig
Nachricht:
(0-250 Zeichen)

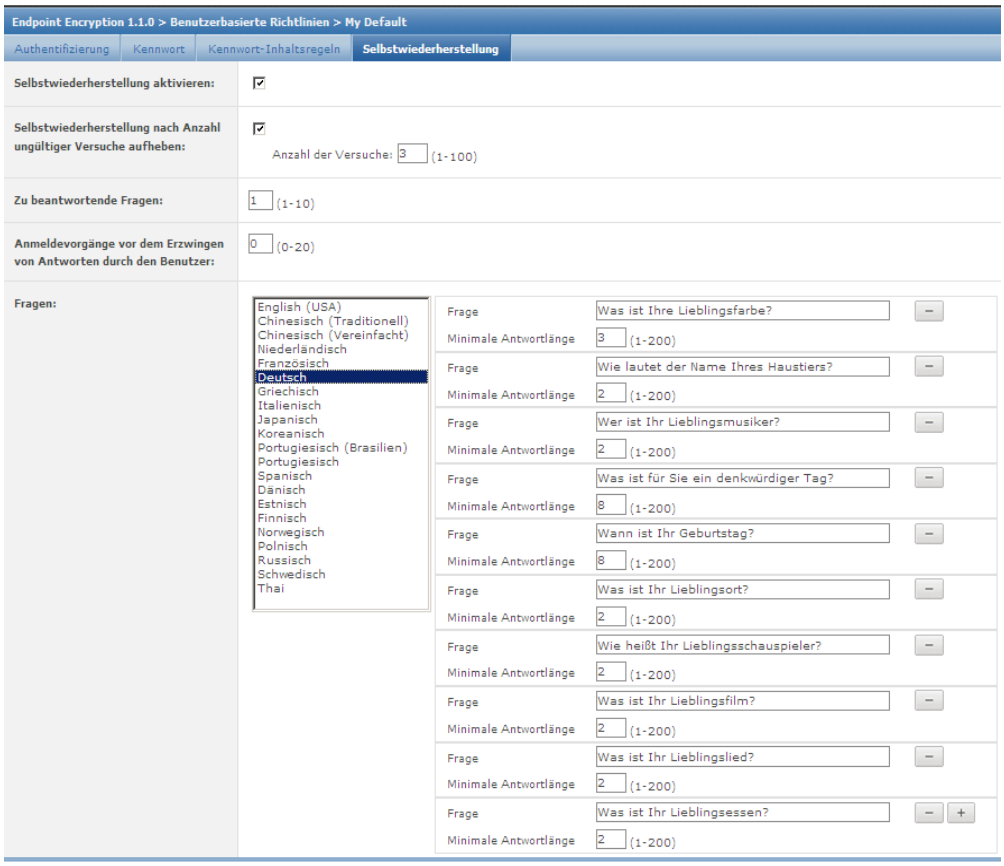

Endpoint Encryption 1.1.0 > Produkteinstellungen > My Default
Allgemein
Verschlüsselung
Anmelden
Wiederherstellung
Boot-Optionen
Theme
Verschlüsselungsanbieter
Boot-Manager aktivieren:
Partition 1 1
Partition 2 2
Partition 3 3
Partition 4 4
Zeitüberschreitung
Zeitüberschreitung 30 in Sekunden (1–300)
Immer Pre-Boot-USB-Unterstützung aktivieren:
Pre-Boot-PCMCIA aktivieren:
Grafikmodus:
Automatisch

Benutzerdefinierte Richtlinien:








Endpoint Encryption 1.1.0 > Benutzerbasierte Richtlinien > My Default
Authentifizierung
Kennwort
Kennwort-Inhaltsregeln
Selbstwiederherstellung
Selbstwiederherstellung aktivieren:
Selbstwiederherstellung nach Anzahl ungültiger Versuche aufheben:
Anzahl der Versuche: 3 (1-100)
Zu beantwortende Fragen: 1 (1-10)
Anmeldevorgänge vor dem Erzwingen von Antworten durch den Benutzer: 0 (0-20)
Fragen:
English (USA)
Chinesisch (Traditionell)
Chinesisch (Vereinfacht)
Niederländisch
Französisch
Deutsch
Griechisch
Italienisch
Japanisch
Koreanisch
Portugiesisch (Brasilien)
Portugiesisch
Spanisch
Dänisch
Estnisch
Finnisch
Norwegisch
Polnisch
Russisch
Schwedisch
Thai
Frage
Was ist Ihre Lieblingsfarbe?
Minimale Antwortlänge 3 (1-200)
Frage
Wie lautet der Name Ihres Haustiers?
Minimale Antwortlänge 2 (1-200)
Frage
Wer ist Ihr Lieblingsmusiker?
Minimale Antwortlänge 2 (1-200)
Frage
Was ist für Sie ein denkwürdiger Tag?
Minimale Antwortlänge 8 (1-200)
Frage
Wann ist Ihr Geburtstag?
Minimale Antwortlänge 8 (1-200)
Frage
Was ist Ihr Lieblingsort?
Minimale Antwortlänge 2 (1-200)
Frage
Wie heißt Ihr Lieblingsschauspieler?
Minimale Antwortlänge 2 (1-200)
Frage
Was ist Ihr Lieblingsfilm?
Minimale Antwortlänge 2 (1-200)
Frage
Was ist Ihr Lieblingslied?
Minimale Antwortlänge 2 (1-200)
Frage
Was ist Ihr Lieblingsessen?
Minimale Antwortlänge 2 (1-200)

Anhang C: FB3 - Quellcode

```
#include <iostream>
#include <windows.h> // for Windows APIs
#include <stdio.h>
#include <stdlib.h>
using namespace std;

int main()
{
LARGE_INTEGER frequency; // ticks per second
LARGE_INTEGER t1_1, t1_2, t2_1,t2_2, t3_1, t3_2; // ticks
double elapsedTime1,elapsedTime2,elapsedTime3;
char text1[50];   // saves user input for the file location
char text2[50];   // saves user input for the destination
int mode;         // saves user input for the benchmark type
long lSize;       // carries the information about the file size
//=====================================================================
   // User input

   printf("Please choose benchmark mode:\n 1.Copy a single file byte-
   by-byte\n 2.Copy, read, write single file at once\n ");
   scanf ("%d",&mode);
   printf("Type the full file location\n");
   scanf ("%s",&text1);
   printf("Type the destination where the file should be copied\n");
   scanf ("%s",&text2);
//=====================================================================
   // Copy a file byte-by-byte

   if (mode==1)
   {
   size_t len = 0 ;
   const char *alfa = text1; // handles the input for the file location
   const char *beta = text2; // handles the input for the file location
   char buffer[BUFSIZ] = { '\0' } ; // Buffer for information handling

   // get ticks per second
   QueryPerformanceFrequency(&frequency);

   // start timer
   QueryPerformanceCounter(&t1_1);
   FILE* in = fopen( alfa, "rb");    // input file
   FILE* out = fopen( beta, "wb");   //output file

   // obtain file size:
   fseek (in , 0 , SEEK_END);
   lSize = ftell (in);
   rewind (in);
   if( in == NULL || out == NULL )
       {
       perror( "An error occured while opening files!!!" ) ;
       in = out = 0 ;
       }

   // writes the file to the new destination byte by byte
   while( (len = fread(buffer, BUFSIZ, 1, in)) > 0 )
       {
       fwrite( buffer, BUFSIZ, 1, out ) ;
       }

   // stop timer
   QueryPerformanceCounter(&t1_2);
```

```
   // close output
   fclose(in) ;
   fclose(out) ;
   free(buffer);
   }
//=====================================================================
   //Copy single file at once

   if (mode==2)
   {
   char * buffer;
   size_t result;
   const char *alfa = text1;
   const char *beta = text2;

   // get ticks per second
   QueryPerformanceFrequency(&frequency);
   // start timer
   QueryPerformanceCounter(&t1_1);
   FILE* out = fopen( beta, "wb");
   FILE* in = fopen( alfa, "rb");
   if (in==NULL) {fputs ("File error",stderr); exit (1);}

   // obtain file size:
   fseek(in, 0, SEEK_END);
   lSize = ftell (in);
   rewind(in);

   // allocate memory to contain the whole file:
   buffer = (char*) malloc (sizeof(char)*lSize);
   if (buffer == NULL) {fputs ("Memory error",stderr); exit (2);}

   // start timer2
   QueryPerformanceCounter(&t2_1);

   // copy the file into the buffer:
   result = fread (buffer, 1, lSize, in);
   if (result != lSize) {fputs ("Reading error", stderr); exit (3);}

   // stop timer2
   QueryPerformanceCounter(&t2_2);
   /* the whole file is now loaded in the memory buffer. */

   // start timer3
   QueryPerformanceCounter(&t3_1);
   fwrite(buffer, 1, result, out);

   // stop timer
   QueryPerformanceCounter(&t3_2);

   // stop timer
   QueryPerformanceCounter(&t1_2);

   // terminate
   fclose(out) ;
   fclose(in);
   free(buffer);
   }
//=====================================================================
   // compute and print the elapsed time in milliseconds

   elapsedTime1   =   (t1_2.QuadPart   -   t1_1.QuadPart)   *   1000.0   /
   frequency.QuadPart;
   elapsedTime2   =   (t2_2.QuadPart   -   t2_1.QuadPart)   *   1000.0   /
   frequency.QuadPart;
```

```
   elapsedTime3   =   (t3_2.QuadPart   -   t3_1.QuadPart)   *   1000.0   /
   frequency.QuadPart;
   cout << elapsedTime1 << " ms\n"; //copy whole file at once
   cout << elapsedTime2 << " ms\n"; //read from file to memory
   cout << elapsedTime3 << " ms\n"; //write from memory to HDD
   cout << lSize/elapsedTime1 << " kB/s\n"; //copy whole file at once
                                            //speed
   cout << lSize/elapsedTime2 << " kB/s\n"; //read from file to memory
                                            //speed
   cout << lSize/elapsedTime3 << " kB/s\n"; //write from memory to HDD
                                            //speed
   return 0;
}
```