



Sicherheit im Unternehmen über den Perimeter hinaus





Inhaltsverzeichnis

WARUM SIE DIESE INFORMATIONSBROSCHÜRE LESEN SOLLTEN	3
DEPERIMETERISIERUNG: NOTWENDIGKEIT UND RISIKEN FÜR DAS UNTERNEHMEN	4
SICHERHEIT IST NUR SO STARK WIE IHRE SCHWÄCHSTE VERBINDUNG	5
HERAUSFORDERUNGEN BEI DER DATENSICHERUNG IN EINEM DEPERIMETERISIERTEN NETZWERK	5
DIE SECUWARE-LÖSUNG	6
C4K	6
DEVICE MANAGEMENT	7
VORTEILE VON SECUWARE	7
360° RUNDUM-DATENSCHUTZ	7
EINFACHE ANWENDUNG UND VERWALTUNG	8
ENDNUTZERTRANSPARENZ	8
GERINGE AUSWIRKUNG AUF DIE SYSTEMLEISTUNG	8
HOHER ROI DURCH GERINGE VERWALTUNGSKOSTEN	8
ZUSAMMENFASSUNG	9
ÜBER SECUWARE	9



Warum Sie diese Informationsbroschüre lesen sollten

Deperimeterisierung ist einer der neuesten Schlagwörter im Bereich Sicherheit. Was ist Deperimeterisierung? Grundsätzlich handelt es sich bei diesem Begriff um die Beeinträchtigung des Perimeters in einem Unternehmensnetzwerk, die erste Linie der strategischen Verteidigung, durch die allgemeine Einführung von Laptops, mobilen Speichergeräten, etc. in Unternehmen. Der Perimeter ist nicht verschwunden, hat sich jedoch zu einer zunehmend chaotischen und dynamischen Einheit entwickelt, dessen Grenzen sich heute nur noch sehr schwer definieren lassen.

Vor einigen Jahren hat Sun Microsystems den Slogan „*The network is the computer*“ [Der Computer ist das Netzwerk] geprägt. Heute wäre es wohl angebrachter zu sagen „*The network is everything*“ [Das Netzwerk ist Alles]. Laptops, USB-Sticks, CD's und DVD's, iPod's sowie zahlreiche weitere Geräte können über das Gateway zum Unternehmensnetzwerk und den darin befindlichen Daten gelangen. In einer heute zunehmend hektischen und weitschweifigen Geschäftswelt ist es notwendig, einen solchen Zugang zum Netzwerk zu ermöglichen – was jedoch auch Kopfschmerzen bereitet, da die Mehrheit von Sicherheitseinrichtungen und -anwendungen den Informationstechnologien keine Kontrolle über Geräte, die verbunden werden können, gewährt – und welche Daten zu und von diesen Geräten übertragen werden.

Diese Informationsbroschüre befasst sich mit den Risiken in Verbindung mit der Deperimeterisierung und erklärt, wie die Lösungen von Secuware eingesetzt werden können, um solche Risiken abzuschwächen ohne dabei die Leistungsfähigkeit des Nutzers zu beeinträchtigen.



Deperimeterisierung: Notwendigkeit und Risiken für das Unternehmen

Deperimeterisierung stellt eine Notwendigkeit für Unternehmen dar. Um wettbewerbsfähig zu bleiben und den Bedürfnissen von zunehmend über den Globus verstreuten und mobilen Arbeitskräften gerecht zu werden, müssen Unternehmen ihre Mitarbeiter durch Zugang zu den Unternehmensdaten von überall auf der Welt unterstützen. Das hat zur Folge, dass sich Daten nicht mehr nur auf stationären Desktops oder Servern, die durch eine Unternehmens-Firewall geschützt sind, befinden. Vielmehr werden die Daten über mehrere mobile Computer und Speichergeräte verteilt, über die viele IT-Abteilungen nur sehr begrenzt Kontrolle haben. Das führt zu schwerwiegenden Risiken für das Unternehmen, wie durch folgende Fälle veranschaulicht wird:

- Eine Festplatte der UK Driving Standards Agency, auf der sich Informationen über 3 Mio. Personen befanden, ging durch einen Auftraggeber verloren.¹
- CD's mit unverschlüsselten, personenbezogenen Daten von etwa 25 Mio. Empfängern von staatlicher Unterstützung im Vereinigten Königreich gingen auf dem Postweg verloren. Die CD's haben auf dem Schwarzmarkt einen geschätzten Wert von 3 Mrd. US-Dollar.²
- Ein Chemiker versuchte an geschützte Informationen in einem Wert von mehr als 400 Mio. US-Dollar von seinem Arbeitgeber, DuPont, zu gelangen, indem er Daten auf den Laptop eines Konkurrenten übertragen hat.³
- Ein Laptop mit persönlichen Daten von 800.000 Personen wurde aus den Geschäftsstellen eines Händlers gestohlen, der Stellenbewerbungen im Auftrag von Gap Inc. verwaltete. Daraufhin bot Gap Inc. jedem Betroffenen die Zahlung der Kosten für die Kreditüberwachung für 12 Monate an.⁴

Sicherheitslücken dieser Art sind nicht ungewöhnlich. Einer 2007 vom Computer Security Institute (CSI) durchgeführten Studie zufolge standen bereits etwa 50 % der Unternehmen mit einem potentiellen Datenverlust infolge eines Verlusts oder Diebstahls von Laptops, mobilen Speichergeräten oder anderen Medien gegenüber.⁵ Die von der Verbrauchergruppe Privacy Rights Clearinghouse gesammelten Statistiken zeigen weiterhin deutlich das Ausmaß dieses Problems: Seit Januar 1995 waren mehr als 200 Mrd. Auszeichnungen mit personenbezogenen Daten aufgrund von Sicherheitslücken in Amerika gefährdet.⁶

Auch Bedrohungen innerhalb eines Unternehmens stellen reale und ernsthafte Risiken dar. Die CSI-Studie führt an, dass mehr als 50 % der US-amerikanischen Unternehmen mindestens einen finanziellen Verlust aufgrund von Aktivitäten durch Mitarbeiter innerhalb eines Unternehmens verzeichneten. Auch in der 2007 vom US-Geheimdienst, CERT und Microsoft durchgeführten E-Crime Watch Studie berichteten 34 % der Unternehmen davon, dass Aktivitäten durch interne Mitarbeiter einen größeren Schaden verursacht haben, als Bedrohungen von außen. Die E-Crime Studie fand ebenso heraus, dass in 36 % der Fälle von Computerkriminalität USB-Sticks sowie andere mobile Speichermedien zum Einsatz kamen, die dazu verwendet wurden, Kundendaten, geistiges Eigentum sowie sonstige geschützte und sensible Informationen zu kopieren.

Datenverlust stellt nicht das einzige Risiko in Verbindung mit mobilen Rechen- und Speichergeräten dar. Solche Geräte dienen potentiell auch als Vektor für Malware. Das ist natürlich nichts Neues. Vom Elk Cloner Virus⁸ bis hin zum oft publizierten Rootkit⁹ Speichermedien werden seit langem dazu verwendet, den schädlichen Code zu verbreiten. Bis vor kurzem war es noch recht einfach für IT-Abteilungen, gegen dieses Problem anzukämpfen: Die Mehrheit der Mitarbeiter sah keinen Bedarf darin, mobile Medien zu nutzen und so könnten CD-Laufwerke und andere Plug&Play Geräte einfach untauglich gemacht werden. In vielen Unternehmen stellt dies jedoch keine Option mehr dar, da mobile Mitarbeiter auf ebenso mobile Daten zugreifen müssen.

Darüber hinaus erhöhen mobile Rechen- und Speichergeräte die Anforderungen hinsichtlich der Erfüllung des Sarbanes-Oxley-Gesetzes (SarbOx), des HIPAA-Gesetzes [Gesetz zur Vereinheitlichung des elektronischen Datenverkehrs im Gesundheitswesen sowie der Datensicherheit], dem Gramm-Leach-Bliley-Gesetz sowie weiteren Entscheidungen, die Vorschriften in Bezug auf den Datenschutz festlegen. Kriminelle oder zivile Sanktionen sind jedoch nicht die einzigen nachteiligen Folgen eines Datenverlusts. Maßnahmen zur Behebung können sich als sehr kostspielig herausstellen und auch die negative Presse ist im Hinblick auf die Schädigung des Rufes und vielleicht sogar bis hin zum endgültigen Sterben eines Unternehmens nicht von unwesentlicher Bedeutung.



Sicherheit ist nur so stark wie ihre schwächste Verbindung

Früher galt der Perimeter als wichtigster Punkt der Verteidigung: Einfach verriegeln und sowohl Netzwerk als auch Daten des Unternehmens sind sicher. Obwohl der Schutz des Perimeters - auch in einer weniger ausgeprägten Form - auch weiterhin eine wichtige und integrierte Komponente einer beliebigen Sicherheitsstrategie ist, bieten Intrusion Detection Systeme (System zur Erkennung von Angriffen auf einen Computer oder ein Netzwerk) und Firewalls keinen ausreichenden für die mobile Welt von heute.

Sicherheit ist nur so stark, wie ihre schwächste Verbindung, und der Wert eines „gehärteten“ Perimeters erhält einen erheblichen Knacks, wenn weitere ungesicherte Verbindungen zum Netzwerk bestehen. Das mit der Verwendung von mobilen Geräten verbundene Risiko wurde nun weitgehend erkannt. Teilnehmer an der Konferenz InfoSecurity 2007 gaben mobile Geräte als wichtigstes Sicherheitsmanko an.¹⁰ Obwohl sich das Bewusstsein jedoch zunehmend erweitert, kann die Suche nach einer machbaren Lösung zu einem schwer fassbaren Problem werden.

Herausforderungen bei der Datensicherung in einem deperimeterisierten Netzwerk

Die Sicherheit in einer deperimeterisierten Umgebung stellt zunehmend einen komplexer und anspruchsvoller werdenden Faktor dar.

- Wie können Sicherheitspolitiken in zeitweise mit dem Netzwerk verbundenen mobilen Geräten - ob Laptop oder ein mobiles Speichermedium – durchgesetzt werden?
- Wie können Daten auf diesen Geräten – oder Geräten, auf die zu einem späteren Zeitpunkt Daten übertragen werden - gesichert werden?
- Wie kann einem vorsätzlichen oder unbeabsichtigten Datenabfluss über mobile Geräte vorgebeugt werden?
- Wie können die zuvor genannten Punkte erreicht werden, ohne die Anwendbarkeit der Geräte oder die Leistungsfähigkeit beim Endnutzer zu beeinträchtigen?

Traditionelle Sicherheitslösungen verfügen einfach nicht über eine deperimeterisierte Infrastruktur. Firewalls und Intrusion Detection Systeme können Daten in einem Speichernetzwerk (SAN) oder NAS (Network Attached Storage) schützen, nicht jedoch unstrukturierte Daten, die unter mehreren mobilen Geräten ausgetauscht werden. Produkte zur Verschlüsselung bringen auch nicht mehr den gewünschten Effekt, auch wenn sie zusätzlich für Sicherheit sorgen. Auch wenn ein Verschlüsselungs-Produkt vorhanden ist, haben Benutzer immer noch die Wahl, ob sie diese Versicherung außer Acht lassen und unverschlüsselte Daten auf einen Laptop oder USB-Stick übertragen möchten. Dies hat zur Folge, das Unternehmen auch weiterhin dem Risiko sowohl von vorsätzlichem Datendiebstahl als auch dem nachlässigen Datenverlust ausgesetzt sind.

Zur Gewährleistung eines umfassenden und kostengünstigen Schutzes wichtiger Daten benötigen Unternehmen eine Lösung, die sich nahtlos in den bestehenden Security und Policy Framework einfügt und den Zugang zu solchen Daten verhindert, die automatisch eine Politik auf einem Gerät ausführt, das sich mit dem Netzwerk verbindet, und die Daten auch nach der Übertragung außerhalb der Grenzen des Unternehmensnetzwerks schützt.



Die Secuware-Lösung

Die integrierte Lösung von Secuware wurde von Grund auf dazu entwickelt, umfassenden Schutz für Unternehmensdaten zu bieten, ohne dabei die Leistungsfähigkeit des Systems oder des Endnutzers zu beeinträchtigen. Basierend auf dem Konzept des geschlossenen Informationskreislaufs, d.h. nur bestimmte Benutzer oder Gruppen verwenden dieselbe Verschlüsselung und sind in der Lage, auf exakt dieselben Daten zuzugreifen. Die Lösung besteht derzeit aus einer zentralen Management-Konsole, die als Directory-Snap-In realisiert wird und als Front-End zu zwei einfach übertragbaren Client-Modulen dient:

C4K

C4K wird dazu verwendet, Sicherheitspolitiken in Bezug auf die Pre-Boot-Authentication (Authentifizierung vor dem Startvorgang) sowie die physikalische und logische Entschlüsselung, die eine Kombination aus Computer- und Benutzerprofilen verwenden, zu erstellen und zu verstärken. C4K Computerprofile führen die Entschlüsselung der ganzen Disk sowie die Pre-Boot-Authentication aus und legen die zulässigen Authentifizierungsmechanismen fest (USB-Token, Smartcards, etc.). Benutzerprofile schützen vor einem internen Datenabfluss sowie unbefugten Zugriff auf Informationen und können für individuelle Benutzer, Benutzergruppen, eine Domain oder eine beliebige Kombination festgelegt werden. Auch in Verbindung mit dem **Device Management** (siehe unten) sind diese Profile im Hinblick auf die Zugriffsbeschränkung zu Daten, Anwendungen und Geräte anwendbar. Jede Benutzergruppe, der ein Benutzerprofil zugewiesen wurde, wird sich im selben geschlossenen Informationskreislauf befinden.

Administratoren können so viele oder so wenig Sicherheitsprofile erstellen, wie sie es für angemessen erachten. Einige Unternehmen benötigen womöglich nur wenige Benutzerprofile, wobei jedes dieser Profile einer größeren Geschäftseinheit im Unternehmen zugewiesen ist. Andere Unternehmen hingegen wünschen eine feinere Untergliederung und weisen kleinen Funktionsgruppen oder auch einzelnen Personen ein einmaliges Benutzerprofil zu. Ein Kunde von Secuware hat nur drei Profile erstellen lassen, unter denen er seine 10.000 Mitarbeiter erfasst – ein Profil für die oberste Führungsebene, ein Profil für die mittlere Führungsebene und ein Profil für Mitarbeiter, die nicht in der Führungsebene sind - während andere Unternehmen mehrere Profile erstellt haben, um auf diese Weise eine granulare Steuerung zu ermöglichen.

Mit C4K können Unternehmen hochgranulare Sicherheitspolitiken schaffen, die den Schutz ihrer Daten durch eine Vielzahl von Mechanismen gewährleisten: -

- Pre-Boot-Authentication zur Sicherstellung, dass lediglich Benutzer mit Zugriffsberechtigung ein System starten und die Daten ansehen können.
- Völlige Verschlüsselung von lokalen Festplatten zur Sicherstellung, dass die Daten für Personen ohne Zugriffsberechtigung nicht lesbar sind.
- Logische Verschlüsselung von Dateien und Ordnern im Netzwerk zur Sicherstellung, dass nur berechtigte Benutzer oder Benutzergruppen Zugriff darauf haben.
- Völlige Verschlüsselung von CD's, USB-Speichergeräten und anderen mobilen Medien zur Sicherstellung, dass diese Daten nur von berechtigten Benutzern, die mit Computern arbeiten, auf denen die Secuware-Lösung installiert ist, gelesen werden können.

C4K ermöglicht Unternehmen, ihre Daten unabhängig vom Speicherort und -medium zu schützen. Verschlüsselte Daten bleiben verschlüsselt, wenn sie auf ein mobiles Gerät kopiert werden und sind lediglich lesbar, nachdem sie auf einem Computer zurück übertragen wurden, auf dem C4K installiert ist - und, auch dann, nur durch einen Benutzer, der über eine Zugriffsberechtigung verfügt. Durch die Beschränkung des Zugriffs nur für berechtigte Benutzer ermöglicht C4K Unternehmen, sowohl das Risiko von vorsätzlichem als auch unbeabsichtigten Datenabfluss zu verringern.



Device Management

Das Device Management ermöglicht Sicherheitsadministratoren die Erstellung einer White List für zugelassene USB- und FireWire-Geräte basierend auf der Hersteller- bzw. Seriennummer des jeweiligen Gerätes sowie die Zuweisung eines jeden zu einer oder mehr Benutzern oder Computern. Benutzer oder Computer mit Sicherheitsprofilen, denen kein Gerät zugewiesen wurde, können nicht auf ein Gerät zugreifen, wohingegen Benutzer oder Computer unter einem Sicherheitsprofil, denen ein/mehrere Geräte zugewiesen wurden, fähig sind, lediglich auf dieses/diese Gerät(e) zuzugreifen.

Auf diese Weise können Unternehmen festlegen, welche Benutzer Zugriff auf mobile Geräte Zugriff haben und auf welche Geräte diese Benutzer Zugriff haben. Durch eine begrenzte Anwendung für zugelassene Benutzer und Geräte kann die Wahrscheinlichkeit eines Datenabflusses sowie die Anzahl der Channels, über die Malware in das Netzwerk gelangen kann, verringert werden.

Secuware sorgt dafür, dass durch die Durchsetzung der Aufteilung von Aufgaben unter dem Sicherheitsadministrator und dem Systemadministrator das beste Verfahren angewandt wird: Nur der Sicherheitsadministrator kann Politiken erstellen oder ändern und nur der Systemadministrator kann Politiken Benutzern und Computern zuweisen. Dadurch verringert sich das Fehlerrisiko und die Sicherheit wird verstärkt, indem sichergestellt wird, dass ein Administrator nur die Aufgaben in seinem/ihrer Zuständigkeitsbereich durchführen kann.

Diese zwei Module verbunden mit der Management-Konsole sorgen dafür, dass lediglich *autorisierte Benutzer*, die *autorisierte Geräte* verwenden, Zugriff auf *autorisierte Daten* haben und in der Tat einen mobilen Schutz für die mobilen Daten von heute gewährleistet. Die Einführung weiterer Module ist während 2008 geplant.

Vorteile von Secuware

360° Rundum-Datenschutz

C4K bietet Unternehmen die Möglichkeit, auszuwählen, welche Daten verschlüsselt werden sollen und welche Benutzer oder Benutzergruppen Zugriff auf diese Daten haben können. Daten, die entschlüsselt wurden, werden wieder automatisch verschlüsselt, wenn sie auf ein mobiles Gerät kopiert werden und sind nur für berechtigte Benutzer auf berechtigten Geräten, auf denen die Secuware-Software installiert ist, zugänglich. Durch die Einschränkung der Zugriffsberechtigung auf Daten und der Sicherstellung, dass diese nicht unverschlüsselt aus dem Netzwerk herausgeleitet werden können, eliminiert C4K alle mit einem Verlust oder Diebstahl von Geräten verbundene Risiken, verringert die Möglichkeit eines Datenabflusses oder Diebstahls von geistigem Eigentum und widersteht Bedrohungen sowohl von Innen als auch von Außen.

C4K löst den Endbenutzer durch die automatische Durchsetzung der Politik von seiner Zustimmung ab. Von einem Unternehmen bestimmte Daten sind stets zu verschlüsseln, werden stets verschlüsselt – unabhängig vom Speicherort und -medium.

Das **Device Management** beugt einem Datenabfluss vor, indem es Unternehmen ermöglicht, festzulegen, welche USB- oder FireWire-Geräte verwendet werden können und welche Benutzer oder Benutzergruppen Zugriff auf diese Geräte haben. Unternehmen haben auch die Wahl, den Zugriff auf mobile Geräte für bestimmte Benutzergruppen zu sperren oder lediglich Geräte mit einer geringen Speicherkapazität in eine White List aufzunehmen, um die zu übertragende Datenmenge einzugrenzen. Daneben trägt die Beschränkung der Zugriffsberechtigung für Geräte auf zugelassene Benutzer und Geräte dazu bei, das Risiko von in das Netzwerk eindringender Malware zu verringern.



Einfache Anwendung und Verwaltung

Die Lösungen von Secuware lassen sich nahtlos in das Microsoft Active Directory (AD) und weitere LDAP-basierte Directory-Dienste integrieren und machen die Anwendung und Verwaltung somit zu einem Kinderspiel. Benutzerprofile und Computerprofile werden im Active Directory als Schema gespeichert und können, sobald sie erstellt wurden, einfach und schnell auf alle bestehenden Benutzer und Computer angewendet werden. Ähnlich werden Änderungen der Profile automatisch angenommen, wenn sich der Benutzer das nächste Mal einloggt oder beim nächsten Group Policy Update. Wird einer Gruppe ein neuer Benutzer zugewiesen, werden das Benutzer- und Computerprofil für diese Gruppe automatisch auf diesen Benutzer angewandt.

Die Interoperabilität mit AD und anderen Directory-Diensten führt ebenfalls dazu, dass Secuware hoch skalierbar ist. Unabhängig davon, wie groß ein Unternehmen werden kann und wie granular die Sicherheitspolitiken auch sein müssen, die Lösung bleibt immer einfach zu handhaben.

Zusätzlich dazu ermöglicht Secuware Unternehmen durch den wirksamen Einsatz der bestehenden Infrastruktur die effiziente Nutzung von Know-how. Administratoren, die bereits mit LDAP-basierten Directory-Diensten vertraut sind, werden die Einfachheit in der Anwendung kennen lernen.

Secuware kann mittels eines Verteilermechanismus für Standardsoftware, wie z. B. SMS, schnell in Betrieb genommen werden und erfordert weder eine geeignete Datenbank, noch einen Datenbankserver.

Endbenutzertransparenz

Secuware ist für den Endbenutzer vollkommen transparent. Die Pre-Boot-Authentication ist in den Windows-Login-Vorgang eingebettet – die Benutzer geben lediglich Standard-User-ID's sowie Passwörter, Smartcards oder USB-Tokens ein – und die Ver-/Entschlüsselung läuft automatisch und unsichtbar im Hintergrund ab. Secuware beeinträchtigt dabei weder die Zusammenarbeit eines Benutzers mit anderen Benutzern, noch ihre Möglichkeit, mobile Rechen- und Speichergeräte zu verwenden.

Die Endbenutzer werden Secuware nur dann wahrnehmen, wenn sie versuchen, auf einen Ordner oder eine Datei zuzugreifen, für die sie keine Zugriffsberechtigung haben, oder aber auf ein Gerät zuzugreifen oder versuchen, darauf zuzugreifen.

Geringe Auswirkung auf die Systemleistung

Die Ver- und Entschlüsselung von Daten kann zu einem hohen Overhead sowie verlangsamten Vorgängen führen. Um dies zu vermeiden, nutzt Secuware effiziente, symmetrische Ziffernblockalgorithmen, die die beeinträchtigende Wirkung auf die Leistung sowie die Ver- und Entschlüsselung auf ein Overhead-Minimum von 0,15 % reduziert.

Hoher ROI durch geringe Verwaltungskosten

Durch die Interoperabilität und holistische Annäherung von Secuware in Kombination mit der Einzelkonsole, zentralen Verwaltung, entsteht eine Lösung, die weitaus einfach zu handhaben ist, als jede Sammlung von plattformspezifischen bzw. gerätespezifischen Produkten. Daher ist möglich, einen weitaus höheren ROI zu erzielen als mit Produkten, die nur eine Teillösung für das Problem im Bereich der Datensicherheit bereitstellen.



Zusammenfassung

Die Lösung von Secuware wurde von Grund auf dazu entwickelt, eine kostengünstige Lösung für Probleme in Verbindung mit der Datensicherung in heutigen deperimetrisierten Umgebungen bereitzustellen. Die Module **C4K** und **Device Management** ermöglichen Unternehmen, starke, datenbasierte Sicherheitspolitiken einzusetzen und diese über die Grenzen des Unternehmensnetzwerks hinaus auszuweiten. Auf diese Weise werden Daten transparent in Echtzeit geschützt, unabhängig vom Speicherort und -medium.

Einfach gesagt: Secuware bringt Ordnung in das Chaos der Netzwerk-Perimeter von heute.

Über Secuware

Secuware ist ein führender Anbieter von sicheren IT-Infrastrukturlösungen für Unternehmen. Die Flaggschiff-Produkte von Secuware schützen sensible Informationen, die sich auf Desktops, Laptops und anderen Geräten befinden, während es gleichzeitig unerlaubte Zugriffe auf lokale und Netzwerkressourcen abwehrt. Das Unternehmen wurde 1998 gegründet und konzentriert sich auf die Entwicklung von proaktiven Sicherheitssteuerungen für Verteidigungsministerien in Europa. Zu den Geschäftstätigkeiten und Kunden von Secuware gehören heute auch Regierungen und Handelsgewerbe auf unterschiedlichen Kontinenten, einschließlich Wal-Mart, Telefonica, Warner Brothers und BBVA. Weitere Informationen über Secuware und Lösungen finden Sie unter www.secuware.com.

Hauptgeschäftsstelle Deutschland

Eifelstraße 9
53119 Bonn
Telefon: 0228 962979-0
Fax: 0228 962979-29

Hauptgeschäftsstelle Europa

Plaza Ruíz Picasso, s/n
Torre Picasso, Planta 14
28020 Madrid
Spanien



Referenzen

¹Millions of L-driver details lost

http://news.bbc.co.uk/1/hi/uk_politics/7147715.stm

²Discs 'worth £1.5bn' to criminals

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

³Massive Insider Breach At DuPont

<http://www.informationweek.com/news/showArticle.jhtml?articleID=197006474>

⁴Gap Inc. Security Assistance

<http://www.gapsecurityassistance.com>

⁵CSI Computer Crime and Security Survey

<http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf>

⁶A Chronology of Data Breaches (Privacy Rights Clearinghouse)

<http://www.privacyrights.org/ar/ChronDataBreaches.htm>

⁷2007 E-Crime Watch Survey

www.cert.org/archive/pdf/ecrimesummary07.pdf

⁸Elk Cloner Virus (Wikipedia)

http://en.wikipedia.org/wiki/Elk_Cloner

⁹Extended Copy Protection (Wikipedia)

http://en.wikipedia.org/wiki/Sony_rootkit

¹⁰Security's Top Five Priorities

http://www.darkreading.com/document.asp?doc_id=123294