



SECRET DOCUMENTS LIFECYCLE™

SCHUTZTECHNOLOGIE DER
NÄCHSTEN GENERATION FÜR
BETRIEBSGEHEIMNISSE

KEEPING SECRETS SAFE





INHALTSVERZEICHNIS

1. EINFÜHRUNG	3
2. ANSÄTZE ZUM DATENSCHUTZ	4
2.1. ERSTE GENERATION: PROBABILISTISCHE FILTERMETHODEN	5
2.2. ZWEITE GENERATION: DETERMINISTISCHE FILTERMETHODEN	7
2.3. FAZIT	9
3. DAS KONZEPT DES SECRET DOCUMENTS LIFECYCLE™	10
3.1. DAS KONZEPT DES SECRET DOCUMENTS LIFECYCLE™	11
3.2. SCHUTZ AN ALLEN PUNKTEN IM LEBENSZYKLUS	13
3.3. DATENSCHUTZ AUSSERHALB DES BÜROS	16
3.4. UMFASSENDE REVISION AN JEDER STELLE DES LEBENSZYKLUS	17
3.5. INTEGRITÄTSREVISION FÜR VERTRAULICHE DOKUMENTE	18
3.6. FAZIT	19
4. ÜBER PERIMETRIX	20

1. EINFÜHRUNG

Dem Ponemon Institute nach kostet ein Datenleck ungefähr 4,7 Mio. US-Dollar.

Betriebsgeheimnisse stellen jene Informationen in einem Unternehmen dar, die vertraulich bleiben müssen. Dazu zählen personenbezogene Daten von Mitarbeitern und Kunden, vertrauliche Details über Partner, das geistige Eigentum des Unternehmens, Businesspläne und Strategien – alles sehr wertvolle Daten für ein Unternehmen, die auf keinen Fall nach außen gelangen dürfen. Wenn diese Betriebsgeheimnisse in die Hände von Wettbewerbern, Kriminellen oder Journalisten fallen oder an die Öffentlichkeit gelangen, ergeben sich schmerzhaftige Konsequenzen für das Management sowie die Beziehung zu Kunden, Investoren, Mitarbeitern und Geschäftspartnern.

Aber Datenlecks geschehen ständig und einige der bekanntesten Unternehmen der Welt sind durch sie in die Schlagzeilen gekommen, darunter angesehene Consulting-Firmen, große Industrieproduzenten und vertrauenswürdige Banken. Solche Vorfälle führen zu Imageschäden, Wettbewerbsnachteilen und einer sinkenden Attraktivität für Investoren, sowie unerwünschter Aufmerksamkeit seitens der Behörden, die eine Nichterfüllung gesetzlicher Anforderungen in diesen Fällen besonders verfolgen.

Nach Erkenntnissen von Gartner kosten Datenlecks ein Vielfaches dessen, was die Implementierung geeigneter Vorsorgemaßnahmen kosten würde.¹ Die Ersparnisse bewegen sich im Bereich von 500%. Inzwischen bedeutet dem Ponemon Institute nach ein einziges Datenleck durchschnittlich einen Schaden von 4,7 Mio. US-Dollar.²

Der Markt bietet eine ganze Palette von Technologien, die auf dem einen oder anderen Weg Datenlecks vorbeugen und damit Betriebsgeheimnisse schützen. Dieses Dokument beleuchtet die heutigen Ansätze – mit ihren Stärken und Schwächen – und beschäftigt sich danach mit dem Secret Documents Lifecycle™ (kurz SDL), der Schutztechnologie der nächsten Generation für Betriebsgeheimnisse von Perimetrix.

¹ Quelle: Avivah Litan, Vice President und Distinguished Analyst bei Gartner

² Quelle: 2006 Ponemon Data Breach Study

2. ANSÄTZE ZUM DATENSCHUTZ

Heutige Technologien zur Identifizierung von Betriebsgeheimnissen in Datenströmen haben sich in zwei Stufen entwickelt.

Vom Begriff her tritt ein Datenleck auf, sobald Betriebsgeheimnisse die informationstechnischen Grenzen des Unternehmens verlassen. Ein Beispiel: Ein Mitarbeiter druckt Finanzdaten aus und nimmt diese in seinem Aktenkoffer aus dem Büro mit. Natürlich hätte der Insider statt des Druckers eine ganze Reihe anderer Kanäle nutzen können, um die Daten zu entwenden. Aus diesem Grund wurden Abwehrsysteme entwickelt, die sich auf die Überwachung der Kanäle konzentrierten, auf denen Informationen das Unternehmen verlassen konnten.

Diese Kanäle lassen sich in vier Hauptgruppen unterteilen:

- E-Mail
- Internet
- Drucker
- Tragbare bzw. mobile Geräte

Der Gedanke hinter einem großen Teil der Schutztechnologien für Betriebsgeheimnisse gründet sich auf der Überprüfung ausgehender Dokumente, wenn diese die Unternehmensgrenzen über einen der oben genannten Wege verlassen.

Daher war es die Aufgabe der Entwickler, einen Weg zur Unterscheidung von geheimen und nicht geheimen Dokumenten zu finden und diesen zusätzlich so weit wie möglich zu automatisieren und damit möglichst wenig manuelle Eingriffe zu erfordern.

Heutige Technologien zur Identifizierung von Betriebsgeheimnissen in Datenströmen haben sich in zwei Evolutionsstufen entwickelt. Im ersten Schritt konzentrierten sich die Entwickler der Schutzsysteme auf probabilistische Methoden, die linguistische Analysen oder digitale Fingerabdrücke nutzen. Im zweiten Schritt entwickelten die Anbieter dieser Systeme deterministische Methoden, die auf der Markierung von vertraulichen Dokumenten mit einem einmaligen Sicherheitslabel beruhen.

Wir werden beide Ansätze noch näher betrachten, können jedoch jetzt schon sagen, dass die Effektivität der probabilistischen und der deterministischen Ansätze zu wünschen übrig lässt. Nach Gartner³ stellen beide höchst unzuverlässige Technologien dar, die ein Angestellter einfach umgehen kann, der willentlich vertrauliche Daten zu entwenden versucht. Dabei erreichen diese Systeme nur eine Effizienz von 80%. In anderen Worten: Diese Ansätze sind nur gegen zufällige Datenlecks wirksam, die durch Fehlbedienungen entstehen, und selbst dann nicht mit völliger Zuverlässigkeit.

³ Quelle: HypeCycle for Information Security, 2007

Die Filtereffektivität linguistischer Technologien beträgt nur 80%.

2.1. ERSTE GENERATION: PROBABILISTISCHE FILTERMETHODEN

Probabilistische Methoden zur Filterung von ausgehenden Datenströmen bedeuten linguistische Technologien oder die Nutzung digitaler Fingerabdrücke von geheimen Dokumenten.

Linguistische Analysemethoden durchsuchen ausgehende Dokumente nach zuvor festgelegten Schlüsselphrasen und analysieren dann den Zusammenhang. Dazu lernt der Filter anhand von Dokumenten, die bereits als „vertraulich“ gekennzeichnet sind, welche Dokumente zurückgehalten werden müssen.

Die Implementierung eines Systems, das auf linguistischer Analyse beruht, erfordert die Erstellung einer Datenbank für den Inhaltsfilter, in die Signaturdokumente für vertrauliche Informationen des jeweiligen Unternehmens eingespielt werden. Jede Signatur repräsentiert eine Vorlage oder einen digitalen Fingerabdruck eines vertraulichen Dokumentes. Diese basieren auf den Schlüsselwörtern und dem Kontext des jeweiligen Dokumentes.

Die Analyse des ausgehenden Datenverkehrs nutzt diese Datenbank: Die Engine scannt jedes Dokument, findet entsprechende Schlüsselwörter und analysiert dann den Text mit Hilfe der linguistischen Signaturdatenbank der digitalen Fingerabdrücke.

Die Analyse ergibt dann ein gewisses Rating, beispielsweise von 1 bis 10. Je höher das Rating, um so höher ist die Wahrscheinlichkeit, dass der linguistische Filter auf ein vertrauliches Dokument gestoßen ist. Aus diesem Grund werden diese Datenschutztechnologien probabilistisch genannt.

Tabelle 1 zeigt uns die drei größten Probleme dieses Ansatzes: Zunächst bietet diese Technologie nur eine geringe Effizienz. Auch mit der oben genannten Datenbank beträgt die Effizienz linguistischer Filtertechnologien nur 80%. Das bedeutet, dass 20% der Betriebsgeheimnisse nicht vor dem Verlassen des Unternehmensnetzwerkes geschützt sind. Dabei zeigen reale Fälle, dass der Verlust von 20% der Betriebsgeheimnisse in 60% der Fälle zum Bankrott führt. Es sollte zudem nicht vergessen werden, dass sogar die beste linguistische Analyse mit einfacher Steganographie und Verschlüsselung umgangen werden kann.

Ein weiteres Problem ist der mit 20% sehr hohe Anteil an falschen Alarmen bei dieser Filtermethode. Es erklärt sich von selbst, dass bei starkem Traffic ein großer Anteil an falschen Alarmen die Arbeit der Sicherheitsspezialisten unnötig erschwert. Bei einer Anzahl von 100.000 E-Mails am Tag, die über das Gateway geleitet werden, würde das 20.000 E-Mails täglich bedeuten, die von Hand geprüft werden müssen. Dabei ist diese Zahl noch sehr konservativ gewählt, verglichen mit Millionen von E-Mails, die von einigen Unternehmen täglich verschickt und empfangen werden.

Wir möchten besonders betonen, dass die 80%ige Effizienz nur dann erreicht wird, wenn zuvor eine speziell auf die Eigenschaften des Unternehmens abgestimmte Filterdatenbank erzeugt wurde – was bedeutet, alle Informationen des Unternehmens zu klassifizieren. Die Anbieter von Datenschutzsystemen unterlassen diesen notwendigen Schritt oft und liefern die Anwendung nur mit einer Standarddatenbank aus. In diesem Fall kann das Produkt schnell und einfach eingesetzt werden – innerhalb weniger Tage – leidet aber unter einer nochmals reduzierten Effizienz im Bereich von 60%.

Tabelle 1: Die Hauptprobleme der linguistischen Filtermethoden

Problem	Beschreibung
Niedrige Effektivität, sogar im Best-Case-Szenario	Das Best-Case-Szenario tritt ein, wenn eine Datenbank für Inhaltsfilter vor der Implementierung erstellt wird, die auf die Bedürfnisse des jeweiligen Unternehmens abgestimmt ist. Jedoch erreicht der Filter auch in diesem Fall nur ca. 80% Effizienz, was im Umkehrschluss bedeutet, dass 20% der Betriebsgeheimnisse ungehindert das Firmennetzwerk verlassen können, neben 20% falschen Alarmen, die die Tätigkeit der Sicherheitsspezialisten extrem schwer machen.
Kein Schutz an der Workstation	Linguistische Filtermethoden können leicht auf der Gateway-Ebene implementiert werden, um den Netzwerkverkehr zu überwachen. Allerdings treten Datenlecks auch auf der Ebene von Workstations auf: Ports, externe Geräte, mobile Geräte und Wireless-Netzwerke; all dies sind potenzielle Datenlecks. Es ist aber sehr schwierig, eine Echtzeitanalyse von Daten, die beispielsweise über den USB-Port kopiert werden, über einen separaten Server mit Inhaltsfilter zu realisieren. Deshalb ziehen es Entwickler vor, die Workstations nicht direkt zu schützen, sondern empfehlen administrative oder technische Protokolle, um alle offenen Ports zu schließen.
Verwundbarkeit gegenüber Insidern	Das Konzept, nur die vier Arten von Kommunikationskanälen zu überwachen, hat beträchtliche Nachteile: Beispielsweise gibt es keinen Schutz gegen den Verlust eines Laptops mit wichtigen Betriebsgeheimnissen – wie schon häufig geschehen ist. Daher lösen Schutzsysteme mit linguistischen Technologien das Problem nur teilweise und überlassen dem Kunden die Aufgabe, einen vollständigen Datenschutz sicher zu stellen.

Ein weiteres Problem der linguistischen Filterung ist die mangelnde Anwendbarkeit auf Datenverkehr außerhalb des Netzwerkes. Während E-Mails relativ leicht zu analysieren und kontrollieren sind, ist das Kopieren von Dateien auf externe Geräte ungleich schwerer zu überwachen.

Alle Versuche, Datenschutzsysteme mit linguistischer Analyse auf lokale Kopieroperationen auf externe Geräte auszuweiten, sind fehlgeschlagen. Dazu müssten alle ausgehenden Dateien zu einem eigenen Server geroutet werden und dann auf Workstationebene die entsprechenden Maßnahmen eingeleitet werden, je nach Antwort des Datenschutzservers.

Ein solcher Ansatz lässt sich nur mit Mühe als „integriert“ bezeichnen, da er zu erhöhter Rechenlast auf den Workstations und unnötigem Netzwerkverkehr führt sowie nur eine geringe Effektivität bietet. Daher bieten Entwickler, die linguistische Analysen nutzen, entweder gar keinen Schutz auf der Workstationebene an oder empfehlen, alle offenen Ports durch administrative oder technische Mittel zu schließen.

Die letzte große Schwäche dieser Technologie ist, dass es für Insider Myriaden von Wegen gibt, sie zu umgehen. Ein Beispiel dafür ist die altbekannte Methode des Datendiebstahls mit Hilfe eines Laptops.

Ein Angestellter kann seinen Laptop verlieren oder ein Dieb kann einen Laptop stehlen, auf dem er geheime Daten vermutet. Keines dieser Szenarien passt zu dem üblichen Modell der vier Kanäle. Das bedeutet, dass die Anbieter von linguistischen Filtersystemen nur eine Teillösung liefern, da sie nicht dem Bedürfnis der Kunden nach umfassendem Schutz entspricht.

2.2. ZWEITE GENERATION: DETERMINISTISCHE FILTERMETHODEN

Deterministische Technologien erfordern, dass alle vertraulichen Dateien gesondert als solche markiert werden. Bei einigen Lösungen bedeutet das einen Zusatz zum Dateinamen. In diesem Fall beginnt beispielsweise der Dateiname immer mit der Vertraulichkeitsklasse bzw. dem geforderten Sicherheitslevel. Daraus ergeben sich Unternehmensrichtlinien zur Dateinamengebung. Dies stellt offensichtlich weder ein bequemes, noch transparentes Verfahren dar und erschwert die Arbeit der Mitarbeiter unnötig.

Dabei gibt es deutlich elegantere Methoden der Arbeit mit vertraulichen Dokumenten, die nicht das primitive Einfügen eines Labels in den Dateinamen erfordern. Beispielsweise kann ein solches Label auch in der Datei in einer ihrer Attribute untergebracht werden.

In diesem Fall muss der Filter, wenn die Datei das Unternehmen über Netzwerkkanäle wie E-Mail verlässt, nicht die gesamte Datei analysieren, sondern nur das Label lesen und die entsprechende Sicherheitsrichtlinie anwenden. In anderen Worten: da das Label dem System bekannt ist, kann es zuverlässig entscheiden, ob eine Datei geheim ist oder nicht. Daher hat diese zweite Generation von Schutzsystemen ihren Namen: deterministisch.

Die Implementierung eines solchen Systems erfordert die komplette Klassifizierung aller elektronischen Dokumente in einem Unternehmen und die Markierung aller geheimen Dateien. In diesem Fall ist Effizienz des Schutzes für markierte Dateien 100%.

Allerdings gibt es dabei eine ganze Reihe anderer Probleme. Besonders ist nicht klar, wie neue Dokumente behandelt werden, von denen in jeder Organisation täglich Dutzende erstellt werden. Es ist beispielsweise nicht möglich, einen Insider daran zu hindern, Teile eines geheimen Dokumentes in ein neues Dokument zu kopieren und diese neue Datei zu entwenden.

Tabelle 2: Die Hauptprobleme der deterministischen Filtermethoden

Problem	Beschreibung
Mangel an Flexibilität	Der Mangel an Flexibilität ist schon in Namen und Konzept dieser Technologie verankert. Das System trifft nur die Entscheidungen, die bereits im Voraus erwartet und definiert wurden. Deshalb ist der Zugriff auf Dokumente im Unternehmensnetzwerk merklich erschwert, Bürokratie nimmt zu und ein Spannungsfeld zwischen Geschäfts- und Sicherheitsinteressen entsteht.
Umfassender Schutz unmöglich	Auch hier gibt es keine Vorsorge gegen Datenverluste durch verloren gegangene Laptops und ähnliche Fälle. Obwohl ein Agent-Programm des Sicherheitssystems die Sicherheitsrichtlinien auch außerhalb des Büros durchsetzen kann, kann es den physischen Verlust eines mobilen Computers und den folgenden uneingeschränkten Zugriff durch unbefugte Personen nicht verhindern. Daher lösen deterministische Methoden das Problem nicht vollständig, sondern adressieren nur einen kleinen Teil.

Das führt zu einer Art von Systemschutz, der auf dem Level der Workstation ansetzt und die Funktion der Zwischenablage einfach unterbindet, wenn das Dokument als „geheim“ markiert ist (siehe Tabelle 2). Zudem hat diese Technologie ein großes Problem mit der Flexibilität, was in einer Kettenreaktion zu einer schlechteren Verfügbarkeit des Dokumentes, einer Verringerung der Produktivität und mehr Bürokratie führt. In einem Unternehmen mit 50 bis 100 Mitarbeitern kann es noch leicht möglich sein, die Arbeit auf diese Art und Weise zu überwachen, aber in einem großen Unternehmen mit verteilten Netzwerken, Subunternehmen oder einfach mit 500 und mehr Mitarbeitern überwiegt der Nachteil der mangelnden Flexibilität den Sicherheitsgewinn.

Zudem kann die Implementierung einer solchen Lösung interne Konflikte verstärken, wenn innerhalb eines Unternehmens die Anforderungen des Geschäftsbetriebes mit Sicherheitsbedenken zusammenstoßen. Laufen die Interessen von Managern denen der Sicherheitsbeauftragten entgegen, so schadet dies dem Unternehmen im Ganzen.

Zuletzt ist anzumerken, dass deterministische Methoden zum Datenschutz ebenfalls wirkungslos gegen den Diebstahl von externen Geräten und Laptops sind. Sogar wenn der Anwender das Agent-Programm des Sicherheitssystems auf seinem Laptop installiert hat, hilft dies nicht gegen den physischen Verlust oder Diebstahl des Computers. In anderen Worten: diese Technologie adressiert nur einen Teil des gesamten Problems und überlässt den Rest dem Unternehmen.

Wir können zusammenfassend sagen, dass die Nutzung deterministischer Systeme ebenso veraltet ist wie linguistische Filterverfahren.

Die Antwort auf die Nachfrage nach umfassender Sicherheit für Betriebsgeheimnisse ist die Entwicklung einer neuen Technologie der dritten Generation: Secret Documents Lifecycle™, entwickelt von Perimetrix.

2.3. FAZIT

Die beiden angesprochenen Generationen von Datenschutztechnologien sind heute veraltet. Sie erreichen kein akzeptables Niveau an Effektivität, Transparenz und Verfügbarkeit. Zusätzlich bietet kein Ansatz eine umfassende Lösung. Jedes Unternehmen fordert aber den Schutz aller Betriebsgeheimnisse vor Datenlecks, egal wo und wie diese auftreten können. Daher bringt eine Investition in eine der beiden obigen Ansätze höchstens eine Teillösung, und zwar mit starken Einschränkungen.

Die Antwort auf die Nachfrage nach umfassender Sicherheit für Betriebsgeheimnisse ist die Entwicklung einer neuen Technologie der dritten Generation: Secret Documents Lifecycle™, entwickelt von Perimetrix. Seine größten Vorteile sind: nahezu 100% Effizienz beim Schutz klassifizierter vertraulicher Informationen, ein hoher Grad an Transparenz und Verfügbarkeit und das Ganze in einer einzigen, umfassenden Lösung.

3. DAS KONZEPT DES SECRET DOCUMENTS LIFECYCLE™

Die fünf Prozesse der Informationssicherheit: Classification, Control, Monitoring, Notification, Audit (Klassifizierung, Kontrolle, Überwachung, Benachrichtigung und Revision)

Secret Documents Lifecycle™ (SDL) schützt die Integrität vertraulicher Daten von Anfang bis Ende - das heißt, von dem Moment, in dem das Dokument erstellt wird, bis zu dem, wenn es endgültig gelöscht ist. Den Kern dieses Konzeptes stellen die fünf Prozesse der Informationssicherheit dar: Classification, Control, Monitoring, Notification, Audit

1. Classification. Der erste Schritt für ein Schutzsystem gegen Datenlecks erfordert die Klassifizierung und Kategorisierung von Informationen. Das bedeutet, dass man identifizieren muss, was genau geschützt werden muss. Angemessene Zugriffsebenen werden sofort auf bestehende klassifizierte Dokumente angewendet; für neu erstellte und eingehende Dokumente wird ein Verfahren zur Behandlung erstellt und optimiert.

2. Control. Der zweite Schritt zielt auf den Schutz von geheimen Dokumenten während der Speicherung und der Zuweisung von Zugriffsrechten auf Basis der Klassen und Zugriffsebenen ab, die im ersten Schritt erstellt wurden. Das Ergebnis ist ein vielschichtiges Modell zum Schutz vertraulicher Daten. Ferner schließt der Schutz von Daten während der Speicherung die Nutzung von Verschlüsselung ein. Das bedeutet, dass Betriebsgeheimnisse auch dann gegen unbefugten Zugriff und Datenlecks geschützt sind, wenn ein Computer oder ein mobiles Gerät verloren geht oder gestohlen wird. Zusätzlich wird an diesem Punkt der nötigen Dokumentation in Zusammenhang mit der Zugriffsrichtlinie für Anwender Rechnung getragen.

3. Monitoring. Der dritte Schritt umfasst den Schutz vertraulicher Dokumente, die von Angestellten auf ihren Computern genutzt werden. Hier wird die Prozessüberwachung für vertrauliche Dokumente durch eine Kombination von probabilistischen und deterministischen Methoden realisiert. Dabei weiß das Schutzsystem zu jeder Zeit, was wann von wem mit einer jeden vertraulichen Datei getan hat.

4. Notification. Der vierte Schritt ist der Echtzeitschutz gegen willentliche Übertretungen der Sicherheitsrichtlinien und die Benachrichtigung der Sicherheitsbeauftragten über alle Vorfälle, so dass diese schnell reagieren können.

5. Audit. Der fünfte und abschließende Schritt bei der Erstellung eines Schutzsystems ist die Archivierung aller Daten, die im Unternehmensnetzwerk zirkulieren, sowie die Aufzeichnung aller Handlungen, die von den Anwendern an diesen Daten vorgenommen werden. Dank diesem Archiv, können Organisationen leicht Revisionen vornehmen, retrospektive Analysen durchführen und Vorfälle untersuchen. Ein solches Archiv erfüllt zudem gesetzliche Auflagen wie zum Beispiel SOX (Sarbanes-Oxley Act) und die Basel II-Vereinbarung.

Um den ganzen Wert der SDL-Technologie zu verstehen, möchten wir nun einen Blick auf den Lebenszyklus eines typischen vertraulichen Dokuments werfen.



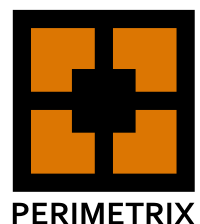
3.1. DAS KONZEPT DES SECRET DOCUMENTS LIFECYCLE™

Perimetrix hat einen neuen Ansatz beim Design des SDL gewählt, aber nicht versucht, das Rad neu zu erfinden. Statt dessen haben sich unsere Entwickler damit beschäftigt, wie vertrauliche Dokumente vor dem elektronischen Zeitalter in Hochsicherheitsumgebungen behandelt wurden.

Erstellung von Dokumenten. Der Lebenszyklus eines vertraulichen Dokumentes beginnt mit der Erstellung eines neuen Dokumentes. Ein Angestellter, der ein solches Dokument erstellen will, stellt einen formalen Antrag und der Prozess der Bewilligung und Bestätigung beginnt. Das Ergebnis dieses Vorgehens ist die Erstellung eines leeren Dokumentes, dem ein gewisser Sicherheitslevel und eine Inventurnummer zugewiesen wurden. In anderen Worten: bevor in einem Dokument irgendeine Information erscheint, bekommt es einen Sicherheitslevel (über den die Zugriffsrechte auf das Dokument geregelt werden) und eine Inventurnummer (die den physischen Aufenthaltsort des Dokumentes angibt) zugewiesen. Erst dann wird Inhalt hinzugefügt und das Dokument wird in die Prozesse oder zur Speicherung gegeben.

Dokumentennutzung. Ort und Art der Dokumentennutzung werden strikt kontrolliert. In jedem Unternehmen mit hohem Sicherheitsbewusstsein gibt es eine spezielle Abteilung, an die sich eine Person wendet, die Zugriff auf ein geheimes Dokument haben möchte. Zu Beginn trägt sich diese Person in ein Register ein, in dem sie die eigene Identität und den Grund für den gewünschten Zugriff auf das Dokument angibt. Dann sucht ein anderer Angestellter - der Verwalter des Archivs für geheime Dokumente, der Bibliothekar - das Dokument anhand dessen Inventurnummer heraus und übergibt es dem Antragsteller. Natürlich kann der Zugriff auf geheime Dokumente in vielen verschiedenen Arten erfolgen, ebenso, wie es verschiedene Arten von Sicherheitsrichtlinien gibt: Zugriff für normale Tätigkeiten, einmaliger Zugriff, Zugriff in Abhängigkeit von der Sicherheitsstufe, zeitbeschränkter Zugriff usw.

Nach dem Erhalt des Dokumentes, darf der Angestellte sich nicht entfernen. Er darf mit den geheimen Dokumenten nur in einem bestimmten Bereich arbeiten. Das bedeutet, dass der Angestellte einen Leseraum im direkten Anschluss an die Abteilung für geheime Dokumente nutzen muss, in dem er das Dokument lesen darf. Während dieses Prozesses ist jegliche Arbeit mit dem Dokument streng kontrolliert. Der Mitarbeiter darf das erhaltene Dokument nicht verändern, weder vom Inhalt her, noch ist eine Zerstörung oder Kopie des Inhaltes oder von Teilen dessen erlaubt. Hat er eine spezielle Freigabe, so darf der Mitarbeiter das Dokument auch ändern, in diesem Fall wird jedoch in einem separaten Journal über alle Änderungen Buch geführt, einschließlich der genauen Beschreibung der Änderungen, der Zeit und des jeweiligen Autors. Das bedeutet, dass bei einer Untersuchung die Identifizierung jedes Beteiligten möglich ist, der gegen Sicherheitsrichtlinien verstoßen hat.



Wird ein solcher Ansatz genutzt, so ist gleichzeitig eine verlässliche Revision der Integrität vertraulicher Dokumente, aber auch der Schutz der Vertraulichkeit gegenüber allen Eventualitäten unautorisierten Zugriffes sichergestellt. Darf sich beispielsweise ein Mitarbeiter mit einem geheimen Dokument nur innerhalb eines bestimmten Bereiches bewegen und dieses geheime Dokument geht verloren oder wird gestohlen, so ist der Raum, in dem das Dokument genutzt und gelagert wird unter voller Kontrolle und die Sicherheit bleibt gewährleistet.

Dokumentenvernichtung. Am Ende des Lebenszyklus muss jedes vertrauliche Dokument vernichtet, archiviert oder anders gelagert werden. Hier ist es - genauso wie bei der Erstellung des Dokumentes - nötig, einen Antrag zur Vernichtung, Archivierung oder Übergabe des Dokumentes (z.B. an eine externe Agentur) zu stellen. Im letzten Szenario wird nicht nur das Dokument selbst übergeben, sondern auch die Verantwortung für dessen Integrität und Vertraulichkeit. Ist ein solcher Antrag genehmigt, so beginnt der Prozess der Vernichtung bzw. der Übergabe an eine andere Lager-einrichtung. Oder das Dokument wird archiviert. Wir sollten das übliche Verfahren zur Behandlung von Dokumenten im Hinterkopf behalten: alle Handlungen müssen im passenden Journal wiedergegeben werden. Dazu ein Beispiel: entsprechend dem angewendeten Verfahren, wer welches Dokument wann vernichtet hat. Damit ist es immer möglich, vergangene Handlungen und die Geschichte eines Dokumentes nach zu verfolgen und Missetäter zu identifizieren.



Abbildung 1. Der Lebenszyklus eines vertraulichen Dokumentes

2 Siehe „Umfassende Revision“ für weitere Details



Wir sollten beachten, dass der Lebenszyklus mit der Senkung oder Erhöhung der Geheimhaltungsstufe enden kann. In diesem Fall wird ein neues Dokument mit einem strengeren oder weniger strengen Satz an Regeln zur Zugriffssteuerung und Nutzung erstellt.

Der betrachtete Lebenszyklus eines geheimen Dokumentes in einer Hochsicherheitsorganisation ist mit vielen internen Verfahren und einem hohen Maß an Bürokratie verbunden. Das führt zur Verlangsamung des ganzen Prozesses bis zu dem Punkt, an dem die Ideen zu Verfügbarkeit und Transparenz redundant werden. Zur gleichen Zeit erlaubt uns der Transfer des formalen Arbeitszyklus mit geheimen Dokumenten auf die elektronische Datenverarbeitung die negativen Aspekte auszuschließen. Beispielsweise können alle Journale automatisch ausgefüllt und Anträge sofort beantwortet werden.

3.2. SCHUTZ AN ALLEN PUNKTEN IM LEBENSZYKLUS

Der Sinn der SDL-Technologie ist der Schutz geheimer und vertraulicher Dokumente während deren kompletten Lebenszyklus. Es ist offensichtlich, dass zu dem Zeitpunkt, an dem ein Datenschutzsystem eingeführt wird, bereits eine große Anzahl an Dokumenten existiert. Daher ist der erste Schritt wie bereits beschrieben die Klassifizierung und Kategorisierung aller Informationen.

Wurde festgestellt, wie vertraulich ein bestimmtes Dokument zu behandeln ist, findet folgender Prozess statt: Jedes Dokument wird entsprechend seiner Vertraulichkeits- bzw. Zugriffsklasse markiert. Das wird durch eine speziell entwickelte Technologie erreicht, die ein Label auf eine für den Benutzer weder sichtbare noch manipulierbare Art und Weise in das Dokument einfügt. Das Label enthält neben den Arbeitsinformationen Details über die Dokumentenklasse und Zugriffsrechte sowie Informationen über den Eigentümer des Dokuments. Hierbei wird das bereits genannte mehrschichtige Vertraulichkeitsmodell genutzt.

Schutz der Daten bei der Speicherung. Der nächste Schritt ist die Unterbringung aller klassifizierten Dokumente im Perimetrix SafeHouse™-Speicher, wo sie in verschlüsselter Form aufbewahrt werden. Dieser Speicher kann als zentrales Depot oder als verteilter Speicher realisiert sein. Wird die zweite Möglichkeit gewählt, so werden die Dokumente wie zuvor auf den Workstations der Anwender gespeichert, allerdings in verschlüsselter Form und mit den eingebetteten Labels. Das Ergebnis ist eine schützende Speichereinrichtung, die geheime Dokumente zuverlässig vor Datenlecks und ungewollter Verbreitung schützt, sogar wenn ein Laptop verloren geht oder auf andere Weise unbefugter Zugriff besteht. Zudem macht diese Art der Speicherung keinen Unterschied zwischen Textdokumenten, Tabellen, Grafiken, Multimedialedateien und sogar Datenbanken.

Im Falle einer Datenbank wird die Datenbank nicht selbst im SafeHouse-Speicher gespeichert. Stattdessen arbeiten die Anwender mit dem sicheren Speicher und die Daten von der Datenbank laufen durch diesen, bevor sie die Anwender erreichen.

Schutz von genutzten Daten. Wenn alle Dokumente klassifiziert und im sicheren Speicher untergebracht wurden, beginnt der Arbeitsprozess. Hierbei werden alle Handlungen mit und an vertraulichen Dokumenten von Perimetrix SafeUse™ kontrolliert. Allerdings nutzen die Angestellten im Rahmen ihrer Aufgaben nicht nur bestehende klassifizierte Dokumente, sondern erstellen auch neue. Sie erwarten sicher, dass sich nun all die Probleme der deterministischen Methode auftun, die wir bereits zuvor identifiziert haben, aber unsere Entwickler haben eine elegante Lösung für diese Probleme gefunden: Bei der Erstellung neuer Dokumente, die Inhalte aus bereits bestehenden Dokumenten nutzen, werden diese durch die Vertraulichkeitslabels der Elterndokumente „infiziert“. Daher werden alle neuen Dokumente automatisch klassifiziert (mit Ausnahme derjenigen, die von null angefangen werden).

Von Perimetrix durchgeführte Untersuchungen haben ergeben, dass nur die wenigsten Dokumente wirklich von null auf ohne jeglichen Inhalt aus anderen Dokumenten erstellt werden. Als Daumenregel kann gesagt werden, dass der Anteil dieser Dokumente nur selten 0,5% aller erstellten Dokumente übersteigt. Nur bei besonderen Umständen, beispielsweise bei Künstlern oder Designern, steigt dieser Anteil auf bis zu 3%. Anders gesagt kann also nur ein sehr kleiner Anteil der neu erstellten Dokumente in einem Unternehmen nicht durch die automatische Klassifizierung erfasst werden. Der Schutz vertraulicher und markierter Dokumente gegenüber Diebstahl geht nahe an 100% Effizienz – was ein Merkmal deterministischer Methoden ist. Das System weiß einfach, dass ein Dokument vertraulich ist und gibt es nicht frei, wenn der Angestellte nicht die entsprechende Freigabe besitzt.

Gleichzeitig bringt uns ein Versuch, ein nicht klassifiziertes Dokument zu stehlen (eines, das vom Autor von null auf erstellt wurde und nur dessen eigenen Inhalt enthält), zu Perimetrix SafeEdge™, das drei probabilistische Schutzmethoden nutzt: Digitale Fingerabdrücke, linguistische Analyse und Signaturanalyse. In diesem Fall steigt die Schutzeffizienz deutlich gegenüber den o.g. Zahlen für diese Methoden, da die Anzahl der unklassifizierten Dateien an sich unter 0,5% der Gesamtmenge liegt. Daher liegt der Anteil falscher Alarme oder nicht erkannter geheimer Dokumente nach der Wahrscheinlichkeitstheorie bei $0,005 * 0,8 = 0,004$. Die Effektivität dieser Technologie beträgt also 99,6%, was mehr als ausreichend für eine Gefahrenabschätzung und Bedrohungsanalyse ist. Bei diesen Zahlen ist das Problem der falschen Alarme so gut wie nicht mehr existent.

Gleichzeitig wird auch der Schutz unklassifizierter Dokumente erreicht, sogar wenn diese das Unternehmensnetzwerk nicht über ein Gateway verlassen (E-Mail, Internet, Drucker usw.), sondern über einen Port einer Workstation; beispielsweise, wenn Dateien auf einen USB-Stick kopiert werden. In diesem Fall, wird die Datei trotzdem zur Echtzeitklassifizierung zum Filterserver geschickt. Die dadurch zusätzlich erzeugte Last für die Workstation und das Unternehmensnetzwerk ist minimal, da die Anzahl dieser Dateien sehr klein ist.

Natürlich können unklassifizierte Dokumente auch nur auf der Workstation des Anwenders aufbewahrt werden, wenn die Anwender nicht versuchen, diese Dateien über das Netzwerk zu verschicken, wodurch sie automatisch klassifiziert würden. Das SDL-System führt jedoch für diesen Fall eine regelmäßige Inventur der Dokumente durch, wenn das Netzwerk nur schwach genutzt wird, beispielsweise nachts oder an Wochenenden. Dabei werden alle neuen Dokumente automatisch klassifiziert und im sicheren Speicher untergebracht.



Abbildung 2. SDL-Technologie schützt Daten während der Speicherung, der Nutzung und der Übertragung (Data at Rest, Data in Use und Data in Motion).

Data in Motion. Wir möchten noch einmal daran erinnern, dass alle geheimen Dokumente in verschlüsselter Form gespeichert werden. Wenn also jemand ein solches Dokument verschickt, wird es in verschlüsselter Form verschickt, was bedeutet, dass die Daten auch während der Übertragung geschützt sind (siehe Abb. 2). Zudem kann die Verschlüsselung vollautomatisch und transparent erfolgen, wenn ein geheimes Dokument das Unternehmensnetzwerk verlässt und beispielsweise an einen Partner gesendet wird.

Zum Abschluss dieses Themas möchten wir hervorheben, dass die SDL-Technologie besondere Aktionen, wie die Senkung einer Vertraulichkeitsstufe, erlaubt. Natürlich ist es denkbar, dass ein Angestellter ein nicht-vertrauliches Dokument mit Inhalten aus einem geheimen Dokument erstellen möchte, das eine spätere Bearbeitung oder einen Versand auch außerhalb des Unternehmens erlaubt. In diesem Fall, könnte der Angestellte die Senkung des Sicherheitslevels einleiten, was die Teilnahme von einem oder zwei anderen Kollegen erfordert, je nach aktiver Sicherheitsrichtlinie; beispielsweise der Sicherheitsbeauftragte und der direkte Vorgesetzte oder eine Person mit unbeschränkten Zugriffsrechten. Für Nutzer, die regelmäßig öffentliche Dokumente erstellen, gibt es Dokumentenvorlagen, die die Erstellung nicht-vertraulicher Dateien erlauben. Trotzdem können die Angestellten während des Prozesses logischerweise nicht mit vertraulichen Informationen aus anderen Dokumenten arbeiten.

Der Secret Documents Lifecycle™ erleichtert die Arbeit der Anwender außerhalb des Unternehmensnetzwerkes.

3.3. DATENSCHUTZ AUSSERHALB DES BÜROS

Wie zuvor bereits genannt, schließt der Schutz der Daten während der Speicherung die Nutzung von Verschlüsselung ein, was bedeutet, dass die Dokumente auf Laptops genauso gut geschützt sind wie im Unternehmensnetzwerk. Wenn allerdings außerhalb mit vertraulichen Informationen gearbeitet wird – beispielsweise auf einer Geschäftsreise – wird es schwierig, Nutzer entsprechend zu authentifizieren und einen effektiven Schutz der genutzten Dokumente zu gewährleisten.

Die SDL-Technologie erleichtert die Arbeit des Anwenders auch außerhalb des Unternehmensnetzwerkes. Dazu werden mehrere Sicherheitsrichtlinien angewendet, die die Zugriffsstufe für klassifizierte Dokumente festlegen.

Die wichtigsten Zugriffsstufen sind:

- **Eingeschränkte Nutzung.** In diesem Fall kann der Angestellte auf der Geschäftsreise mit Hilfe eines persönlichen Schlüssels Zugriff auf die entsprechenden Dokumente erhalten; beispielsweise durch sichere Authentifizierung oder über ein Passwort. Bei dieser Zugriffsstufe gibt es keine Kontrolle über die Nutzung des Dokumentes durch den Anwender.



- **Secret.** Diese Zugriffsstufe nutzt Authentifizierung und weitergehende Überwachung für geheime Dokumente im gleichen Umfang wie innerhalb des Unternehmensnetzwerkes. Gleichzeitig werden Operationen am Dokument zur Revision und Integritätskontrolle aufgezeichnet. Wird der mobile Computer wieder mit dem Unternehmensnetzwerk verbunden, werden alle Journale und Revisionsdatenbanken ins zentrale Archiv übertragen.⁴
- **Top Secret.** Um Zugriff auf Dokumente dieser Zugriffsstufe zu erhalten ist es nötig, eine Authentifizierung zu durchlaufen und eine VPN-Verbindung mit dem Unternehmensnetzwerk aufzubauen. Nur dann ist es möglich, mit einem Top-Secret-Dokument zu arbeiten. Selbstverständlich werden alle Operationen am Dokument überwacht und für eine spätere Revision aufgezeichnet. Darüber hinaus werden Benachrichtigungen über Richtlinienverletzungen in Echtzeit weiter gegeben. So kann ein Sicherheitsbeauftragter wenn nötig einem Anwender außerhalb des Unternehmensnetzwerkes den Zugriff auf das Top-Secret-Dokument entziehen, wenn es nötig wird.

Auf diese Art und Weise adressiert die SDL-Technologie umfassend alle Ansprüche an Schutz und Revision für vertrauliche Dokumente und deren Integrität, auch über die Beschränkungen des Unternehmensnetzwerkes hinaus. Gleichzeitig wird die Arbeit von Angestellten außerhalb des Unternehmensnetzwerkes vollkommen transparent gehalten.

3.4. UMFASSENDE REVISION AN JEDER STELLE DES LEBENSZYKLUS

Die Revision der Vertraulichkeit und Integrität geheimer Dokumente an allen Stellen des Lebenszyklus ist ein wichtiger Teil der SDL-Technologie im Rahmen der Sicherung gegen Datenlecks.

Das SDL-Konzept schließt die Implementierung einer zentralen Perimetrix ShadowCore-Datenbank ein, in der alle Ereignisse (wer wann was mit dem Dokument getan hat) sowie die Dokumente selbst gespeichert werden. Letzteres trifft auf Dokumente innerhalb und außerhalb des Unternehmensnetzwerkes zu. Auf diesem Weg wird eine leistungsfähige Basis für eine Integritätskontrolle, rückblickende Analyse und die Aufklärung von Vorfällen gegeben.

Mit Hilfe dieser Datenbank können Sicherheitsbeauftragte Statistiken erstellen und analysieren sowie Grafiken und Berichte erstellen. Auf der Basis dieser Informationen ist es möglich, die Nutzung der Informationsressourcen eines Unternehmens auf Effektivität hin zu untersuchen und Datenströme zu balancieren und zu optimieren sowie die internen Kommunikationsprozesse zu verbessern.

⁴ Siehe „Umfassende Revision“ für weitere Details



Wichtig ist dabei das in der SDL-Technologie integrierte System der Benutzeridentifikation. Das bedeutet, dass es mit Hilfe einer zentralen Datenbank möglich ist, einer Handlung den entsprechenden Anwender zuzuordnen. Damit wird auch einer der Hauptnachteile von nicht integrierten Systemen zum Datenschutz umgangen, die aus mehreren Teilsystemen zusammengesetzt sind. Diese speichern zu Operationen über den Internetkanal nur gesichtslose IP-Adressen, die auch dynamisch sein können, E-Mail-Adressen, die sich leicht fälschen lassen, oder über externe Dienste und die dort verwendeten Benutzernamen.

Zuletzt ist es bei der Analyse der zentralen Datenbank und der Aufklärung eines Zwischenfalles möglich, eine Kette von Ereignissen zu identifizieren, die einem versuchten Datendiebstahl oder einer anderen Richtlinienübertretung voraus geht. Mit der Sammlung solcher Daten wird es möglich, Gefahren von innerhalb des Unternehmens proaktiv zu begegnen und die Versuche von Angestellten, Daten zu entwenden, schon im Voraus zu vereiteln.

Eine Integritätsrevision erfordert, dass jedes vertrauliche Dokument vor Veränderung geschützt ist.

3.5. INTEGRITÄTSREVISION FÜR VERTRAULICHE DOKUMENTE

Der Integritätsrevision für vertrauliche Dokumente wurde ein eigenes Kapitel gewidmet, da sie eine Schlüsselanforderung vieler Richtlinien, Standards und Direktiven ist. Insbesondere SOX legt besonderen Wert auf die Integrität von Finanzdokumenten – und ist damit zum de-facto Standard im Bereich der Unternehmensführung geworden. Zusätzlich stellt die Integritätsrevision für vertrauliche Dokumente den Grundstein für jeden Standard, der mit Informationssicherheit und Risikomanagement zu tun hat.

Eine Integritätsrevision erfordert, dass jedes sensible Dokument vor Veränderung (bis hin zur Vernichtung des Dokuments) geschützt ist. Das bedeutet zunächst, dass Verfahren zur internen Kontrolle eingerichtet werden müssen, die allerdings im Allgemeinen nicht verhindern, dass Anwender mit der entsprechenden Freigabe wichtige Dokumente verändern. Allerdings bedeuten solche Verfahren der internen Kontrolle immer, dass es stets möglich ist, den zu einer Veränderung gehörenden Anwender zu identifizieren und wichtige Dokumente in ihrem Originalzustand wieder herzustellen, sogar wenn diese vernichtet wurden.

Die SDL-Technologie adressiert diese Aufgaben, die Integritätsrevision und der Schutz eines Dokumentes vor Veränderung und Vernichtung, umfassend. Das im vorherigen Kapitel beschriebene zentrale Archiv enthält alle für eine Revision nötigen Details: verschiedene Versionen des Dokumentes, Aufzeichnungen mit Änderungsdaten, einschließlich des ändernden Nutzers und der Zeit. Wenn nötig kann so die Geschichte eines Dokumentes einfach dargestellt und sein kompletter Lebenszyklus offen gelegt werden, so dass der Punkt, an dem ein Angreifer das Dokument verändert hat, leicht gefunden werden kann und die Änderungen rückgängig gemacht werden können, indem einfach eine frühere Version des Dokuments wieder hergestellt wird.



3.6. FAZIT

Im Gegensatz zu den üblichen und veralteten Ansätzen die deterministische und probabilistische Methoden nutzen, bietet die SDL-Technologie ein extrem hohes Sicherheitsniveau (über 99%) und schützt Ihre Daten at Rest, in Use und in Motion). Der Hauptvorteil des SDL-Konzeptes ist die Tatsache, dass dieser Ansatz das Problem vollständig und umfassend löst. Auch wenn ein Angestellter einen Laptop mit geheimen Dokumenten verliert oder versucht, vertrauliche Informationen auf einen USB-Stick zu überspielen wird kein Datenleck auftreten. Daher löst die Implementierung des SDL-Konzeptes in einer Organisation das Problem von Datenlecks ein für alle Mal.

Um bei dem bereits betrachteten Modell der klassischen Dokumente auf Papier zu bleiben: SDL erlaubt die Erstellung eines sicheren Raumes, in dem Dokumente gespeichert, genutzt und bewegt werden können – in dem sie ausschließlich existieren. Dieser sichere Raum hat seinen eigenen Platz in der Gesamtlösung: Perimetrix SafeSpace™.⁵

⁵ Siehe „Perimetrix SafeSpace™ – verschließt Datenlecks endgültig.“

4. ÜBER PERIMETRIX

Perimetrix entwickelt Lösungen der dritten Generation zur Absicherung von Geschäftsprozessen. Im Gegensatz zu Wettbewerbern bündeln wir unsere Skills, innovativen Ideen und unsere enorme Erfahrung, um eine unternehmensweite Plattform für interne Informationssicherheit zu schaffen. Diese sichert wichtige Geschäftsprozesse und ist in die organisatorische und technologische Infrastruktur des Kunden integriert.

Unser Ziel ist es, unsere Kunden bei der Steigerung des Unternehmenswertes zu unterstützen. Das erreichen wir durch die Gewährleistung ungestörter Geschäftsprozesse, die Minimierung von Datenverlusten, die Erhöhung der Konkurrenzfähigkeit sowie den Aufbau von gewinnbringenden Beziehungen zu Investoren und Partnern, stets unter Beachtung der gesetzlichen Vorgaben.

Mit dem revolutionären Konzept Secret Documents Lifecycle™ bietet Perimetrix Schutz für vertrauliche Dokumente während sämtlicher Lebenszyklus-Phasen. Darüber hinaus ermöglicht die Lösung das Monitoren von Kommunikationskanälen und die Überprüfung elektronischer Prozesse. Die zugrunde liegende Technologie dieses Systems besteht in der Kenntnis der zu schützenden Dokumente und Komponenten sowie in der Steuerung von Zugriffsrechten und Benutzeraktionen und verhindert damit die Verletzung von Unternehmensrichtlinien.



Perimetrix Systems GmbH

Birkenstrasse 4a
85107 Baar-Ebenhausen
Deutschland

Tel.: +49 (0)8453 3399700

Fax: +49 (0)8453 3399704

info@perimetrix-systems.com

www.perimetrix-systems.com

KEEPING SECRETS SAFE

