



PERIMETRIX SAFESPACE™

UMFASSENDE SCHUTZ FÜR
VERTRAULICHKEIT UND
INTEGRITÄT IHRER DATEN

KEEPING SECRETS SAFE





INHALTSVERZEICHNIS

1. EINFÜHRUNG	3
2. VERALTETE ANSÄTZE ZUR DATENINTEGRITÄT	4
2.1. GRÜNDE FÜR DAS VERSAGEN	5
2.2. UNAUSGEREIFTE TECHNOLOGIEN DER VERGANGENHEIT	5
3. PERIMETRIX SAFESPACE™ – EINE EINFÜHRUNG	7
3.1. SECRET DOCUMENTS LIFECYCLE™	7
3.2. PERIMETRIX SAFESPACE™	8
3.3. PERIMETRIX SAFESTORE™	9
3.4. PERIMETRIX SAFEUSE™	11
3.5. PERIMETRIX SAFEEDGE™	14
3.6. VERÖFFENTLICHUNG GEHEIMER DOKUMENTE	15
3.7. PRODUKTIONSKAPAZITÄT UND SKALIERBARKEIT	15
3.8. FAZIT	16
4. ÜBER PERIMETRIX	17

Durch die Implementierung von Perimetrix SafeSpace™ kann jede Organisation, unabhängig von ihrer Größe, ein einfaches, verlässliches und komfortables Schutzsystem gegen Gefahren durch Insider realisieren.

Jedes Unternehmen muss seine Betriebsgeheimnisse schützen: vertrauliche Informationen, geistiges Eigentum und personenbezogene Daten der Mitarbeiter und Kunden. Diese vitalen Daten müssen jedoch nicht nur gegenüber der Außenwelt geschützt werden, sondern auch gegenüber internen Gefahren.

Jeder Manager sieht ein, dass ein Verlust von Betriebsgeheimnissen die Wettbewerbsfähigkeit einschränkt, Beziehungen mit Kunden, Partnern und Investoren belastet und unerwünschte Aufmerksamkeit seitens der Behörden auf sich zieht.

Trotzdem schützen sich viele Unternehmen und staatliche Organisationen immer noch nicht gegen Datenlecks. Das Problem liegt in der mangelnden Effizienz der Lösungen am Markt, die entweder nur gegen zufällige Datenlecks schützen oder so kompliziert und bürokratisch sind, dass sie die Geschäftsprozesse zum Erliegen bringen.

Zudem bieten die verfügbaren Produkte keine umfassende Lösung für das Problem der Datenlecks. Stattdessen konzentrieren sie sich auf einen einzelnen Aspekt, zum Beispiel die Blockade der Ports einer Workstation oder die Filterung ausgehenden Netzwerkverkehrs. Alles andere bleibt dem Unternehmen überlassen, wie zum Beispiel der Umgang mit gestohlenen oder verlorenen Laptops und mobilen Geräten, die vertrauliche Informationen enthalten, oder der Schutz vor Datenmissbrauch über Drucker.

Unternehmen scheuen die Investition in Schutzsysteme gegen Datenlecks, da sie auf eine umfassende Lösung angewiesen sind. Alles was z.Zt. angeboten wird, ist aber nur Fassade und soll die Probleme überspielen, vom Preis ganz zu schweigen. Diese dubiosen und oft schnell überholten Technologien sind oft mit großen Investitionen verbunden.

Die Verantwortlichen in den Unternehmen wissen nur zu gut, dass die aufgezählten Probleme aus der mangelnden Reife der Schutztechnologie gegen Datenlecks resultieren. Topmanager warten daher auf eine effektive, umfassende Lösung.

Dieses Dokument betrachtet genau so eine Lösung: Perimetrix SafeSpace™ unterliegt nicht mehr den Beschränkungen der heutigen Technologien. Den Kern dieser Technologie stellt der einmalige Secret Documents Lifecycle™ dar. Mit seiner Hilfe konnten die Entwickler alle Prinzipien der sicheren Handhabung vertraulicher Dokumente umsetzen, die sich mit Dokumenten in Papierform seit Jahrzehnten in Unternehmen bewährt haben.

Durch die Implementierung von Perimetrix SafeSpace™ kann jede Organisation, unabhängig von ihrer Größe, ein einfaches, verlässliches und komfortables Schutzsystem gegen Insidergefahren einrichten und so die Vertraulichkeit und Integrität geheimer Dokumente ein für alle Mal schützen.

2. VERALTETE ANSÄTZE ZUR DATENINTEGRITÄT

Gartner zeigt auf, dass die Produkte am Markt keinen zuverlässigen Schutz bieten.

Warum hat die Mehrheit der am Markt vorhandenen Lösungen bisher keinen Erfolg gehabt? Gartner – eines der führenden IT-Beratungsunternehmen weltweit – gibt die Antwort: in seiner letzten Studie, genannt „Hype Cycle for Information Security 2007“, haben die Analysten klar festgestellt, dass die Technologien gegen Datenlecks erst in nächster Zeit die Marktreife erreichen. Nach Gartner wird dies in den nächsten zwei bis fünf Jahren stattfinden; im Moment bietet die Implementierung dieser Lösungen nur „beschränkte“ Vorteile für Unternehmen.

Obwohl Schutztechnologien gegen Datenlecks üblicherweise als effiziente Methode angesehen werden, um geistiges Eigentum zu schützen, zeigt Gartner, dass sich die Technologie in der Praxis noch weit besser eignet, um fehlerhafte Geschäftsprozesse zu identifizieren, jedoch nur zufällige Datenlecks findet. Auch wenn die Mehrheit der Zwischenfälle durch ungewollte Datenlecks, Datenänderungen und Vernichtungen von Daten geschieht, hat die Technologie bisher wenig gegen einen mutwilligen Angriff eines Insiders zu bieten.

Gartner zeigt, dass die Produkte am Markt keinen zuverlässigen Schutz bieten. Zusätzlich erreicht ihre Effizienz gerade 80%; sogar die so genannten „Full-Spectrum“-Lösungen tragen ihren Namen also nicht zu Recht.

Datenlecks treten auf, wenn vertrauliche Informationen die Unternehmensgrenzen verlassen.

2.1. GRÜNDE FÜR DAS SCHEITERN

Das Hauptproblem der heutigen Lösungen ist der gewählte Ansatz, mit dem sie ihre Aufgabe angehen. Obwohl die Entwickler absolut richtig erkennen, dass Datenlecks auftreten, wenn vertrauliche Informationen die Unternehmensgrenzen verlassen, so nehmen sie fälschlicherweise an, dass sich ihre Aufgabe in den Kanälen erschöpft, über die Daten das Unternehmen verlassen können: E-Mail, Internet, Mobilgeräte und Drucker.

Als Ergebnis bleiben viele Aspekte des Problems ungelöst. Beispielsweise kann ein Mitarbeiter nicht daran gehindert werden, Daten auf seinen Laptop zu kopieren und dann einen Diebstahl vorzutäuschen. Zudem arbeitet der Datenschutz auf Workstations normalerweise nach dem schwarz-weiß-Prinzip, das heißt der Zugriff wird erlaubt oder verboten; die Vertraulichkeitsstufe eines Dokuments wird nicht in Betracht gezogen, wenn dieses beispielsweise auf einen USB-Stick kopiert wird. So kann sich ein Angestellter, der Zugriff auf geheime Daten hat, diese Freigabe zu kriminellen Zwecken missbrauchen und sich und die Daten der Kontrolle entziehen.

Im Vergleich zur niedrigen Effizienz der marktüblichen Produkte sind die oben genannten Probleme jedoch nachrangig.

2.2. UNAUSGEREIFTE TECHNOLOGIEN DER VERGANGENHEIT

Die niedrige Effizienz der genutzten Technologien lässt sich primär mit der mangelnden Reife erklären. Obwohl die Methoden zur Identifizierung vertraulicher Daten bereits zwei Evolutionsstufen hinter sich haben, bieten sie entweder nur eine Effizienz von 80% oder sind so schwerfällig, dass sie die Geschäftsprozesse behindern.

Die erste Generation dieser Technologie nutzte probabilistische Analysen in verschiedenen Ausprägungen. Das umfasste integrierte linguistische Analysen und Signaturanalysen (digitale Fingerabdrücke). Die in der Gartner-Studie genannten 80%ige Effizienz ist das bestmögliche Ergebnis für die obigen Technologien, bei der Aufgabe, ausgehenden Verkehr zu filtern und dabei vertrauliche von nicht vertraulichen Dokumenten zu unterscheiden. Sogar bei Verwendung von Schlüsselwörtern in ihrem Kontext in Verbindung mit einer kundenspezifischen Inhaltsdatenbank ist die Effizienz probabilistischer Analysen generell kleiner als 80%.

Werden zur Erkennung vertraulicher Dokumente digitale Markierungen oder Labels an Stelle linguistischer Analysen eingesetzt, ergibt sich kein großer Unterschied, da diese Labels einfach umgangen werden können. Ein böswilliger Insider kann dabei immer noch Steganographie oder eine einfache Verschlüsselung nutzen, um die Erkennung der Daten als vertraulich zu umgehen. Schon ein anderer Zeichensatz oder der Austausch von Buchstaben durch Ziffern erfüllt diesen Zweck.

Die zweite Generation dieser Technologien nutzte deterministische Methoden, die vertrauliche Dokumente über eine besondere Markierung erkannten. Sie erlaubte einen 100%igen Schutz geheimer Daten, die in der Klassifizierungsphase als solche erkannt wurden. Trotzdem taucht auch hier eine ganze Reihe von Fragen auf. Was beispielsweise soll mit neuen Dokumenten geschehen, die von Anwendern nach der Implementierung des Systems erstellt werden? Hier zeigt sich die hauptsächliche Schwäche: das System ist nicht fähig, neue Daten in einem laufenden Prozess zu klassifizieren.

Desweiteren sind solche Lösungen oft schwierig einzusetzen und ergeben ein hochgradig unflexibles System für den Anwender. Seine Nutzung führt zu steigender Bürokratie, die zu Interessenkonflikten zwischen der Sicherheitsabteilung und anderen Abteilungen führt.¹

¹ Weitere Informationen über die Entwicklung von Schutztechnologien gegen Datenlecks finden Sie in „Secret Documents Lifecycle™: Schutztechnologie der nächsten Generation für Betriebsgeheimnisse“

3. PERIMETRIX SAFESPACE™ – EINE EINFÜHRUNG

Perimetrix nutzt zum Schutz der Daten einen Weg, mit dem seit Jahrzehnten Staatsgeheimnisse geschützt werden.

Anstatt sich auf die verschiedenen Kanäle zu konzentrieren und die Fehler der letzten Generationen zu wiederholen, nutzte Perimetrix zum Schutz der Daten einen Weg, den auch Organisationen seit Jahrzehnten nutzen, die mit dem Schutz von Staatsgeheimnissen beauftragt sind. Heraus kam eine neue Generation von Technologien, die geheime Dokumente während ihres gesamten Lebenszyklus schützen – Secret Documents Lifecycle™, kurz SDL.

3.1. SECRET DOCUMENTS LIFECYCLE™

Das zentrale Konzept hinter SDL ist die Schaffung eines geschützten Raumes, in dem die Anwender mit geheimen Dokumenten unter der Überwachung eines Schutzsystems arbeiten können. In jeder Firma 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.

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 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.



Die betrachtete Arbeitsweise mit vertraulichen Dokumenten in einer Firma mit hohem Sicherheitsbewusstsein ist mit vielen internen Verfahren und einem hohen Maß an Bürokratie verbunden. Der Transfer des formalen Arbeitszyklus mit geheimen Dokumenten auf die elektronische Datenverarbeitung erlaubt uns, diese negativen Aspekte auszuschließen. Das Schutzsystem pflegt hierbei selbst die Kontendatei, beobachtet alle Veränderungen an Dokumenten und hält Kopien verschiedener Dateiversionen in einem Archiv vor.

Die SDL-Technologie ist nicht nur in der Lage, die Nutzung vertraulicher Dokumente zu kontrollieren, sie deckt auch alle anderen Teile des Lebenszyklus eines Dokuments ab: Die Erstellung, Speicherung, Archivierung und Vernichtung von Dokumenten wie auch weniger übliche Aktionen wie die Senkung der Vertraulichkeitsstufe von Dokumenten und der Umzug von Dokumenten in eine andere Aufbewahrungsstätte.

So schafft die SDL-Technologie einen geschützten Raum, in dem Dokumente gespeichert, genutzt, bewegt und schließlich vernichtet werden können. Das ist ein Schlüsselement der umfassenden Perimetrix SafeSpace™-Lösung.

3.2. PERIMETRIX SAFESPACE™

Perimetrix SafeSpace™ umfasst drei Schlüsselkomponenten, die alle auch als Einzelprodukt eingesetzt werden können (siehe Abbildung 1):

- **Perimetrix SafeStore™** ist ein System zur anfänglichen Klassifizierung von Dokumenten, das mehrere Vertraulichkeitsstufen einschließt und geheime Dokumente dann im SafeHouse™ speichert, einem verteilten Speicher. Dieses Produkt stellt die Sicherheit der Daten bei der Aufbewahrung sicher.
- **Perimetrix SafeUse™** ist ein System zur Kontrolle der Nutzung von klassifizierten Dokumenten durch autorisierte Angestellte. Dieses Produkt stellt die Sicherheit der Daten bei der Nutzung, die automatische Klassifizierung neuer Dokumente, die Integritätsrevision geheimer Dokumente und die retrospektive Analyse sicher, letztere mit Hilfe von ShadowCore™, dem zentralen Archiv.
- **Perimetrix SafeEdge™** ist ein System zur Echtzeitkontrolle für alle Dokumente, die das Unternehmensnetzwerk verlassen (SMTP, HTTP, Drucker, IM, FTP und P2P). Es klassifiziert zudem automatisch eingehende Dokumente. Dieses Produkt stellt die Sicherheit der Daten während der Übertragung sicher.

Obwohl jedes dieser drei Perimetrix-Produkte als Insellösung implementiert werden kann, sind die synergetischen Vorteile überwältigend, die aus der Nutzung aller drei Produkte zusammen entstehen: Ein Unternehmen kann ein zuverlässiges System gegen Datenlecks erstellen, das Datensicherheit in allen drei Stadien sicherstellt: Speicherung, Nutzung und Übertragung der Daten. Die Möglichkeit einer Integritätsrevision rundet das Paket ab.



3.3. PERIMETRIX SAFESTORE™

Selbstverständlich existiert schon bei der Erstellung eines Schutzsystems für Vertraulichkeit und Integrität eine große Anzahl an Dokumenten in einer Organisation. Daher ist der erste Schritt bei der Implementierung des Systems die Klassifizierung und Kategorisierung aller dieser Informationen. Dieser Prozess ist deutlich einfacher als bei den Produkten der Vorgängergenerationen, da die integrierte Perimetrix ReadyCompliance™-Technologie die Kategorisierung auch großer Datenmengen innerhalb weniger Stunden erlaubt.

Ist die Vertraulichkeitsstufe eines Dokuments festgelegt, weist ihm Perimetrix SafeStore™ ein Geheimhaltungs- und Zugriffslevel zu. Das dazu verwendete Label wird so in das Dokument eingefügt, dass es dem Nutzer gegenüber unsichtbar bleibt und weder verändert noch gelöscht werden kann.

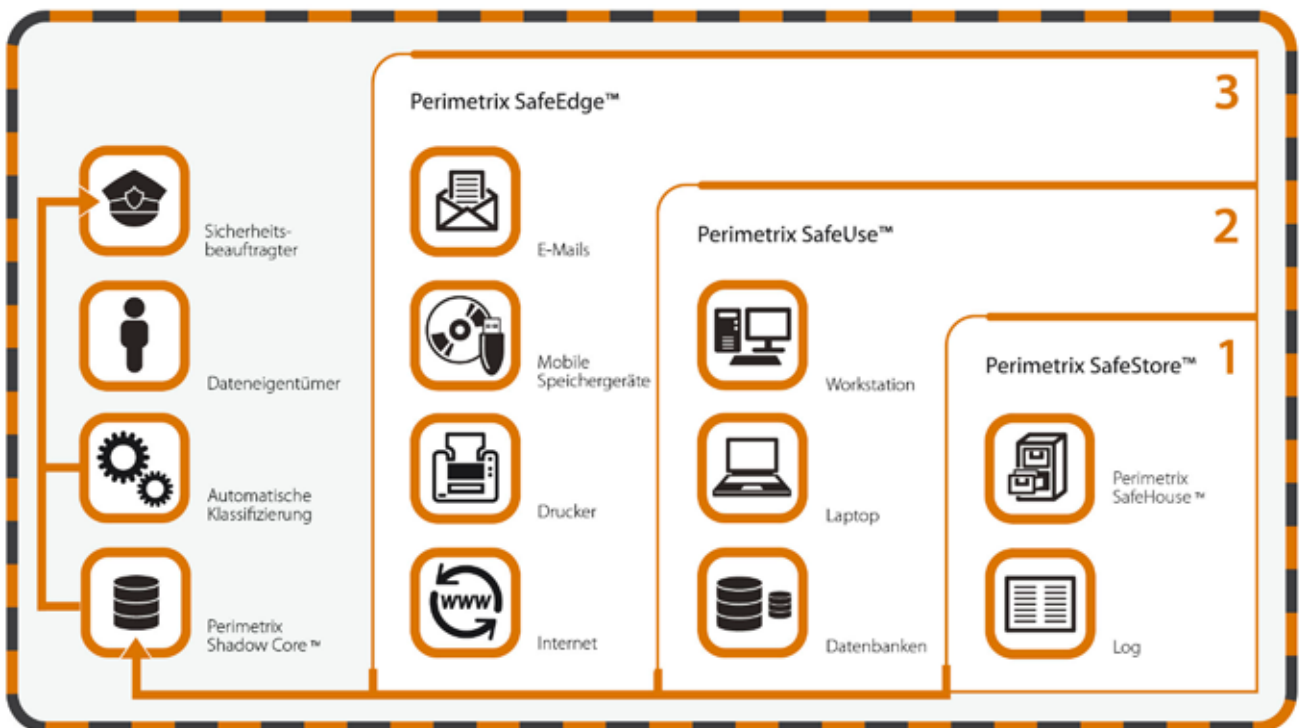


Abbildung 1. Perimetrix SafeSpace™

Dieses Label enthält Informationen zum Eigentümer und der Klasse des Dokuments. Dank der verschiedenen Vertraulichkeitsstufen kann die Klasse selbst verschiedene Aspekte haben. Beispielsweise könnte eine Klasse folgendes umfassen:

- Die Kategorie der Informationen im Dokument (Finanzdaten, personenbezogene Daten, geistiges Eigentum, usw.)
- Verbindung zu einer spezifischen Abteilung (Finanzabteilung, Marketing, Produktion, usw.)
- Vertraulichkeitsstufe (Intern, Geheim, Top Secret, usw.)

Wenn Perimetrix SafeStore™ alle klassifizierten Dokumente mit dem Label versehen hat, werden diese an einen speziellen Speicher übersendet, wo sie in verschlüsselter Form gespeichert werden: Perimetrix SafeHouse™.

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 erfolgt.

Diese Art der Speicherung macht zudem keinen Unterschied zwischen Textdokumenten, Tabellen, Grafiken, Multimediadateien 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.

Perimetrix SafeStore™ bietet außerdem Schutz für geheime Dokumente auf Laptops und mobilen Geräten. Wenn ein Angestellter ein solches Gerät verliert, bleiben die vertraulichen Dokumente verschlüsselt und können von keinem Unbefugten genutzt werden.

3.4. PERIMETRIX SAFEUSE™

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 Mitarbeiter im Rahmen ihrer Aufgaben nicht nur bestehende klassifizierte Dokumente, sondern erstellen auch neue. Alle damit verbundenen Operationen werden von Perimetrix SafeUse™ überwacht.

Die Arbeit mit klassifizierten, markierten Dokumenten wird von den Richtlinien kontrolliert, für die sich das Unternehmen entschieden hat. Das heißt, dass Angestellte mit Informationen, für die sie nicht die entsprechende Sicherheitsfreigabe haben, keine Operationen vornehmen dürfen. Beispielsweise kann die Richtlinie allen Mitarbeitern das Kopieren von Top-Secret-Dokumenten, auch teilweise, verbieten, mit Ausnahme einer kleinen Nutzergruppe. In diesem Fall können Angestellte ohne diese spezielle Sicherheitsfreigabe Top-Secret-Dokumente weder drucken, auf USB-Sticks kopieren oder diese per E-Mail oder Internet versenden. Sie können noch nicht einmal einen beliebigen Teil dieses Textes zwischenspeichern. Wird eine unerlaubte Operation dennoch versucht, so wird der Sicherheitsbeauftragte angemessen benachrichtigt.

Wie bereits erwähnt, nutzen Angestellte nicht nur bereits klassifizierte Dokumente, sondern erstellen auch neue. Bei der Erstellung neuer Dokumente, die Inhalte aus bereits bestehenden Dokumenten nutzen, werden diese durch die Vertraulichkeitslabels der Elterndokumente „infiziert“. Alle neuen Dokumente werden somit automatisch klassifiziert (mit Ausnahme derjenigen, die von null angefangen werden).

Perimetrix SafeUse™ muss nicht raten, ob ein Dokument geheim ist oder ob es das Unternehmensnetzwerk verlassen darf. Die Lösung weiß immer schon im Voraus genau, welche Vertraulichkeitsstufe zu einem Dokument gehört und erhält so 100% Effizienz und Zuverlässigkeit.

Natürlich bietet Perimetrix SafeUse™ auch auf mobilen Computern außerhalb des Unternehmensnetzwerks die gleiche Effektivität. Wie bereits erwähnt, schützt Perimetrix SafeStore™ vertrauliche Dokumente vor unbefugtem Zugriff, auch im Fall eines Diebstahls oder Verlustes. Perimetrix SafeUse™ erhöht diesen Schutz noch mal um eine Stufe, indem es die Operationen eines Anwenders bei der Arbeit mit klassifizierten Dokumenten mit Hilfe mehrerer Richtlinien überwacht – auch außerhalb des Büros.

Die wichtigsten Zugriffsstufen sind:

- **Eingeschränkte Nutzung.** In diesem Fall kann der Mitarbeiter 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.²
- **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.

Wir haben bereits das zentrale Archiv Perimetrix ShadowCore™ erwähnt, eine Schlüsselkomponente von Perimetrix SafeUse™ die das Problem der Integritätsrevision für geheime Dokumente effektiv löst.

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 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.

² Siehe „Umfassende Revision“ für weitere Details



Wichtig ist dabei das in Perimetrix SafeUse™ 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 pro-aktiv zu begegnen und die Versuche von Mitarbeitern, Daten zu entwenden, schon im Voraus zu vereiteln.

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, dass es immer möglich ist, den zu einer Veränderung gehörenden Anwender zu identifizieren und wichtige Dokumente in ihrem Originalzustand wieder herzustellen, sogar wenn diese vernichtet wurden.

Perimetrix SafeUse™ und ShadowCore™ adressieren diese Aufgaben, die Integritätsrevision und den 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 Dokumentes wieder hergestellt wird.

Das Fundament von Perimetrix SafeEdge™ bilden die drei probabilistischen Schutzmethoden: digitale Fingerabdrücke, linguistische Analyse und Signaturanalyse.

3.5. PERIMETRIX SAFEEDGE™

Perimetrix SafeUse™ bietet nahezu 100%igen Schutz für klassifizierte Dokumente. Wenn ein Anwender ein neues Dokument erstellt, ohne ein bestehendes Dokument oder eine bestehende Vorlage zu nutzen, wird das neue Dokument nicht automatisch klassifiziert.

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. Anders gesagt kann also nur ein sehr kleiner Anteil der neu erstellten Dokumente in einem Unternehmen nicht durch die automatische Klassifizierung erfasst werden. Dennoch müssen diese Dokumente geschützt werden – das ist die Aufgabe von Perimetrix SafeEdge™

Das Fundament von Perimetrix SafeEdge™ sind die drei probabilistischen Schutzmethoden: digitale Fingerabdrücke, linguistische Analyse und Signaturanalyse. Wir haben zuvor den Wirkungsgrad dieser Methoden mit 80% angegeben. Hier aber trifft dieser Prozentsatz nur auf den Anteil unklassifizierter Dokumente zu, der sich um 0,5% der Gesamtmenge bewegt.

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. Perimetrix SafeStore™ kann jedoch so eingestellt werden, dass es eine regelmäßige Inventur der Dokumente durchführt, wenn das Netzwerk nur schwach genutzt wird, beispielsweise nachts oder an Wochenenden. Dabei werden alle neuen Dokumente automatisch klassifiziert und im sicheren SafeHouse™ Speicher untergebracht.



Perimetrix SafeEdge™ schützt also Daten bei der Übertragung. Sobald ein geheimes Dokument das Unternehmensnetzwerk verlässt und beispielsweise an einen Partner gesendet wird, wird das Dokument automatisch entsprechend der Richtlinien und vollkommen transparent verschlüsselt.

3.6. VERÖFFENTLICHUNG VERTRAULICHER DOKUMENTE

Egal ob mit einer Insellösung oder der umfassenden Perimetrix SafeSpace™ Lösung kann es vorkommen, dass ein Unternehmen ein geheimes Dokument in eine ungeschützte Umgebung transferieren möchte. Um das zu erleichtern, gibt es ein Verfahren, um die Vertraulichkeitsstufe eines Dokuments zu senken.

Selbstverständlich könnte ein Mitarbeiter beim Kopieren von geheimen Daten eine Datei zur öffentlichen Nutzung oder zum Versand außerhalb der Organisation erstellen. In diesem Fall, kann der Angestellte das Verfahren zur Senkung der Vertraulichkeitsstufe anstoßen. Das erfordert die Teilnahme eines oder sogar zwei weiterer Kollegen, je nach verwendeter Sicherheitsrichtlinie. Bei diesen Personen kann es sich beispielsweise um einen Sicherheitsbeauftragten, den direkten Vorgesetzten oder eine Person mit unbeschränktem Zugriff handeln.

Für Anwender, die regelmäßig öffentliche Dokumente erstellen, gibt es Vorlagen, die die sofortige Erstellung öffentlicher Dokumente erlauben. Der Anwender kann jedoch während dieses Prozesses nicht mit vertraulichen Informationen aus anderen Dokumenten arbeiten – eine logische Folge.

Der hohe Durchsatz von Perimetrix SafeSpace™ wird durch ein einzigartiges Loadbalancing-System ermöglicht.

3.7. PRODUKTIONSKAPAZITÄT UND SKALIERBARKEIT

Perimetrix SafeSpace™ wurde zum Schutz geheimer Dokumente in großen Unternehmen geschaffen – mit bis zu 500 und mehr Workstations. Die Hauptanforderungen solcher Kunden sind hoher Durchsatz und einfache Skalierbarkeit.

Der hohe Durchsatz von Perimetrix SafeSpace™ wird durch ein einzigartiges Loadbalancing-System ermöglicht, das den schnellsten Weg für die Bearbeitung jeder Anfrage findet und ungleichmäßige Belastungen im Prozess ausgleicht.

Hohe Skalierbarkeit ergibt sich aus der Cluster-Struktur der Lösung, die ein einfaches Hinzufügen neuer Elemente erlaubt. Praktisch alle Elemente von Perimetrix SafeSpace™ können geclustert werden. Daher können auch Engpässe schnell durch ein Cluster erweitert werden. Durch das Hinzufügen eines neuen Knotens löst der Cluster das Durchsatzproblem.

Die Komponenten von Perimetrix SafeSpace™ sind völlig plattformunabhängig und arbeiten unter Windows, Linux und Unix.



3.8. FAZIT

Im Gegensatz zu den üblichen und veralteten Ansätzen die deterministische und probabilistische Methoden nutzen, bietet die SDL-Technologie einen extrem hohen Sicherheitslevel (über 99%) und schützt Ihre Daten bei der Speicherung, der Nutzung und der Übertragung (Data at Rest, Data in Use und Data in Motion).

Der Hauptvorteil des SDL-Konzeptes ist die Tatsache, dass dieser Ansatz die aktuellen Herausforderungen vollständig und umfassend löst. Auch wenn ein Mitarbeiter 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.

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.



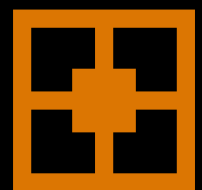
Perimetrix Systems GmbH

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



PERIMETRIX