

**Datensicherheit
für sensible und
vertrauliche
Informationen**



**Das Plus an Effizienz und
Unternehmenssicherheit
für mittlere und große
Unternehmen**

**iC Compas
Sicherheit für Unternehmensdaten**

**Schützen Sie vertrauliche Daten vor böartig oder
unbeabsichtigt hervorgerufenen
Informationslücken.**



Information Leakage Prevention – Data Loss Prevention

Ob Managementdaten, Kundeninformationen oder Details aus Ihrer Produktentwicklung:
In jedem Unternehmen existieren Informationen, die nicht für alle Augen bestimmt sind. Einige möchten Sie zum definierten Zeitpunkt veröffentlichen oder im Rahmen von Arbeitsprozessen nach außen geben. Andere Daten dürfen Ihr Unternehmen nicht verlassen. Unachtsamkeit in der Hektik des Tagesgeschäfts oder absichtliche bzw. kriminelle Datenzugriffe von Unbefugten können den nötigen Schutz sensibler Daten durchkreuzen.

Die Bekämpfung der unerlaubten Weitergabe derartiger Unternehmensdaten ist aufgrund der Komplexität heutiger IT-Infrastrukturen und der vermehrten Nutzung von E-Mail, Instant Messaging und sonstiger Kanäle eine höchst komplexe Aufgabe.

Zusätzlich sind die Art und Qualität der Bedrohungen – im Gegensatz z.B. zu Viren oder Würmern – von Unternehmen zu Unternehmen sehr verschieden. Um daher die notwendigen Gegenmaßnahmen aufbauen zu können, ist es im Vorfeld notwendig, auf 3 Fragen eine geeignete Antwort zu finden:

- Welche Arten von Daten sind nicht für die Öffentlichkeit bestimmt oder gelten als vertraulich und müssen daher gegen eine unerlaubte Weitergabe geschützt werden (Kunden- und Mitarbeiterdaten, vertrauliche Unternehmensdaten, usw.)?
- Auf welche Art und Weise tritt die Verletzung der Vertraulichkeit auf? Welche Geschäftsprozesse sind betroffen und welche Schnittstellen müssen geschützt werden?
- Welche Benutzergruppen dürfen mit welchen Daten welche Tätigkeit durchführen?

Durch die Überwachung der zwei potentiellen Problembereiche „Netzwerk“ und „Arbeitsplatz“ können all diejenigen Schnittpunkte überwacht werden, bei denen Datenbewegungen zu einem Problem führen können.



Notwendigkeit durch gesetzliche Richtlinien

Datenschutzrichtlinien jedweder Art bestimmen immer mehr die Richtlinien, welche von der Unternehmensführung beachtet werden muss, um sowohl den gesetzlichen Bestimmungen zu genügen als auch – je nach Gesetzeslage – zu vermeiden, sich persönlich strafbar zu machen. Neben den generellen Datenschutzrichtlinien für persönlich identifizierbare Daten (von der EU 1995 verabschiedet) mit all den länderspezifischen Umsetzungen sind die bekannten Richtlinien wie Basel II, Sarbanes-Oxley (SOX) und HIPPA nur ein kleiner Ausschnitt aus den existierenden Regularien.



Welche Daten können kontrolliert werden

Um sicherzustellen, dass auch alle relevanten Daten eines Unternehmens abgesichert werden können, ist natürlich zu gewährleisten, dass diese Daten auch von einem zentralen ILP-System verstanden werden können. Folgende Arten von Erkennung sind zwingende Bestandteile im Rahmen einer derartigen Lösung:

- Schlüsselwörter und ausgewählte Begriffe
- Auf Regeln basierende Texte / Zeichenketten (z.B. „Ist das eine gültige Visa-Kreditkartennummer?“)
- Auf Linguistik basierende Erkennung von Texten (z.B. „Kann dieses Dokument ein Lebenslauf sein?“)
- Auf Basis von vorliegenden Datenbanken wird die Verwendung von Inhalten bestimmter Datenbankfelder erkannt
- Auf Basis von vorliegenden Dokumenten wird die Verwendung dieser Dokumente (bzw. auch nur die Verwendung von Ausschnitten) erkannt



Welche Datenwege müssen überprüft werden

Neben den Arten der Daten müssen natürlich auch alle relevanten Wege der Informationsflüsse überwacht werden:

- E-Mail (SMTP / Exchange)
- HTTP, FTP – in bestimmten Fällen auch HTTPS
- Instant Messenger
- USB-Geräte / externe Festplatten
- Drucken (zentral und lokal)
- Copy & Paste / Printscreen

iC Compas - Sicherheit für Unternehmensdaten

Produktprofil

Primäre Lösungskomponenten

Lokalisieren	Innerhalb des gesamten Netzwerks werden die Daten und Informationen lokalisiert. Auf dieser Basis können notwendige Klassifikation von relevanten Daten durchgeführt werden. Darüber hinaus ist es dadurch möglich, nun entsprechende Schutzrichtlinien festzulegen und zu implementieren. Die jeweils definierten „schützenswerten“ Datenbereiche werden automatisch überwacht und auf diese Art und Weise ist die Aktualität der Datenüberwachung immer gewährleistet.
Überwachen Analysieren	Mittels einer kompletten Echtzeitüberwachung Ihrer Informationen - wo auch immer sich diese befinden oder wie auch immer diese übertragen werden - können die relevanten Informationsflüsse kontrolliert werden. Zudem ist es möglich, das Ausdrucken der zu überwachenden Informationen im Rahmen der Überwachung ebenfalls zu berücksichtigen. Durch ein robustes Datenanalysemodul ist es möglich, auch Daten zu erkennen, die nur Teile der Originaldaten sind. Dies wird erreicht durch einen sehr fortgeschrittenen „Fingerabdruck der Daten“, d.h. eine mathematische Darstellung einer Gruppe von Zeichen, Wörtern, Sätzen oder Datenfeldern innerhalb eines Dokuments, einer Nachricht oder einer Datenbank, und identifiziert so akkurat die entsprechend sensiblen Daten zusammen mit deren Metadaten.
Schützen	Werden die analysierten Daten als „sicherheitsrelevant“ eingestuft, können diese Informationen automatisch durch vordefinierte und Richtlinien-basierte Regularien (welche Benutzer- und Inhaltsbasiert definiert werden können) protokolliert, gesperrt oder auch verschlüsselt werden. Je nach der Klassifikation des Sicherheitsvorfalles können auch direkt die entsprechenden Verantwortlichen informiert werden.
Policy Engine	Die primären Bestandteile einer solchen Lösung werden zentral gesteuert, so dass jede Änderung an den Richtlinien automatisch im gesamten Unternehmen gilt. Eine derartige Policy Engine erlaubt es, zentral Richtlinien zu definieren, die dann im Rahmen einer gesamtheitlichen Sicherheitsrichtlinie Ihre Berücksichtigung finden. Damit wird eine derartige Lösung ein weiterer wichtiger Bestandteil des umfassenden IT-Security-Konzepts. Es können zentral alle relevanten internen und externen Richtlinien und rechtlichen Vorgaben umgesetzt werden um damit auch sicherzustellen, dass interne und vertrauliche Informationen auch innerhalb der Unternehmensgrenzen verbleiben. Der Datenfluss sensibler Informationen bleibt somit wirksam geschützt.

Beispiel der ILP-Arbeitsweise

Schutz persönlicher Daten

Ein Sachbearbeiter schickt im Rahmen eines definierten Geschäftsprozesses die Daten von einem Kunden (Name, Anschrift, Kreditkartennummer) per Mail an einen externen Geschäftspartner. Dies wird vom System genehmigt. Schickt der gleiche Mitarbeiter mehrere solcher Datensätze innerhalb einer einzigen Mail an einen externen Kontakt, ist dies nicht Teil eines erlaubten Prozesses und damit wird die Mail gestoppt und der vermeintliche Datenverlust im Ansatz gestoppt.

Rechte und Pflichten von Mitarbeitern beachten

Ein gutes Beispiel für die rollenbasierte Informationssicherheit ist z.B. die Arbeit von Finanzabteilungen. Eine ILP-Strategie kann in diesem Bereich sicherstellen, dass ein Mitarbeiter vertrauliche Finanzdaten zwar an berechnete Kollegen weiterleiten kann, beim Versenden an externe Empfänger würden dieselben Daten aber geblockt oder verschlüsselt werden. Wichtig bei dieser Vorgehensweise ist besonders, dass die Mitarbeiter von der Verantwortung entlastet werden, beim Arbeiten mit derartigen Informationen alle relevanten Richtlinien präsent haben zu müssen und jeweils über deren richtige Umsetzung entscheiden zu müssen. Dies ist vor allem bei längeren Dokumenten oder E-Mails manuell nicht mehr immer möglich.

- Es wird ein Optimum an Sicherheit und Effizienz für die Firma erreicht

Treffen Sie die richtige Entscheidung



Starten Sie den Dialog und profitieren Sie von verlässlicher Beratung, kundenspezifischer Umsetzung und umfangreichen Services.

Sichern Sie die vorhandenen Werte Ihres Unternehmens konsequent ab und steigern Sie Ihren Wettbewerbsvorteil.

Lassen Sie sich von iC Compas und ihren Partnern das für Ihr Unternehmen passende Sicherheitspaket schnüren und schützen Sie Ihr Unternehmen vor den täglichen Risiken in der IT

Zuverlässiger Partner – garantierte Sicherheit

Mit wem ein Unternehmen eine Lösung zur Steigerung der Sicherheit der Unternehmensdaten einführt, sollte keine Zufallsentscheidung sein. Die Leistungsfähigkeit, die Innovationskraft und die Zuverlässigkeit haben letztendlich Auswirkungen auf den Bestand Ihrer Investition. Die iC Compas GmbH & Co KG garantiert Ihnen langfristig alle Dimensionen an Sicherheit.



iC Compas GmbH & Co KG

**Lise-Meitner-Strasse 1
85716 Unterschleißheim
Germany**

**Tel.: +49 (0) 89 / 370 603 31
Fax.:+49 (0) 89 / 316 094 11
info@ic-compas.de
www.ic-compas.de**