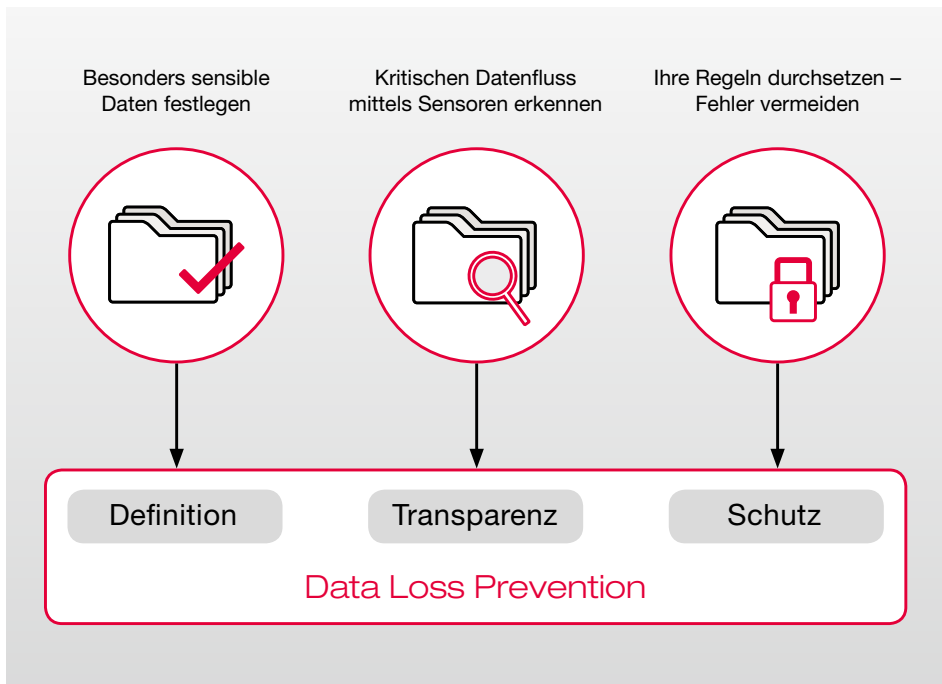


Sensible Unternehmensdaten präventiv schützen



Ihre Vorteile:

- » **Transparenz über die Verarbeitung sensibler Daten mittels Netzwerksensoren**
- » **Festlegung individueller Regeln zur Speicherung und Weitergabe sensibler Daten**
- » **Automatisierte Regelüberwachung**
- » **Präventive Sicherung vor unkontrolliertem Datenabfluss**

„80% der Informationen im Unternehmen sind ohnehin frei zugänglich. Von den verbleibenden 20% Firmeninterna sind etwa 5% die Kronjuwelen, der Wissensvorsprung eines Unternehmens“, so Herbert Kurek vom Bundesamt für Verfassungsschutz*. Jedes Unternehmen besitzt solche Kronjuwelen, beispielsweise in Form vertraulicher Personal-, Finanz- und Kundendaten oder in der Forschungs- und Entwicklungsabteilung.

Gefahren eines Verlustes sind vielfältig: Ein verlorener Laptop, eine falsch adressierte E-Mail oder versehentlich auf einem öffentlichen Netzwerk abgelegte vertrauliche Daten sind nur einige Beispiele. Moderne Data Loss Prevention-Lösungen (DLP) identifizieren, kontrollieren und schützen besonders sensible Daten von Unternehmen und Behörden.

* Treser, Tanja: Schwachstelle Mensch. In: FOCUS Magazin, Nr. 1 vom 29. Dezember 2008.

Es gilt, die für die spezifische Infrastruktur geeignetste Lösung aus einer Vielzahl an Produktangeboten auszuwählen. Um eine ganzheitliche, effektive Schutzlösung zu schaffen, müssen Unternehmensdaten, interne Datenflüsse und individuelle Regeln eng aufeinander abgestimmt werden. secunet berät und begleitet Kunden bei der Auswahl und Implementierung einer passgenauen Data Loss Prevention-Lösung in einem zweistufigen Prozess:

Phase I: Vermeidbare Risiken ausschließen

Ein ganzheitlicher Ansatz zu Data Loss Prevention beinhaltet mehr als Dateiverschlüsselung und Regelungen für USB-Anschlüsse. Aber schon einfache Sicherheitsmaßnahmen entfalten gebündelt große Wirkung: Eine Speicherverschlüsselung zum Beispiel minimiert den Schaden bei Verlust mobiler Geräte (Laptop, Smartphone, USB-Stick), da die Daten so nicht mehr frei zugänglich sind. Eine zentrale Managementlösung steuert den

Arbeitsplatz der Mitarbeiter direkt und lässt passgenau jeweils nur die Geräte, Dienste, Schnittstellen und Anwendungen zu, die der Mitarbeiter für seine jeweiligen Aufgaben benötigt. Eine solche Lösung ist schnell installiert und einfach zu bedienen, unnötige Gefahren von Datenverlust sind auf ein Minimum reduziert. Innerhalb dieser individuellen Arbeitsumgebungen können Mitarbeiter Daten eigenverantwortlich bewegen und verarbeiten.

Phase II: Transparenz schaffen – Datenfluss kontrollieren

Im Arbeitsalltag fällt es Mitarbeitern nicht immer leicht, die Sensibilität der Daten korrekt im Sinne der Unternehmensführung zu bewerten und die Tragweite ihrer Handlungen exakt einzuschätzen. Ebenso ist es für die Unternehmensführung schwierig zu kontrollieren, ob bestehende Anweisungen eingehalten werden.

Phase II schafft die notwendige Transparenz beim Umgang mit sensiblen Daten. Technische Komponenten setzen bestehende Anweisungen durch und beugen so ungewolltem Datenabfluss vor.

Sensible Daten identifizieren

Der Kunde identifiziert seine besonders schützenswerten Daten. Eine ausgereifte Data Loss Prevention-Lösung erkennt sensible Daten anhand unterschiedlicher Kriterien, die der Kunde individuell definiert:

- Datenformate, Strukturaufbau, Schlüsselworte
- Konkrete Kennzeichnungen einzelner Daten(-bereiche)
- Intelligentes Lernen anhand von Beispielen

Hierbei identifiziert eine solche technische Lösung sogar Teildaten als schützenswert, die aus einem größeren Kontext sensibler Daten extrahiert wurden.

Sensible Daten beobachten – Datenfluss regeln

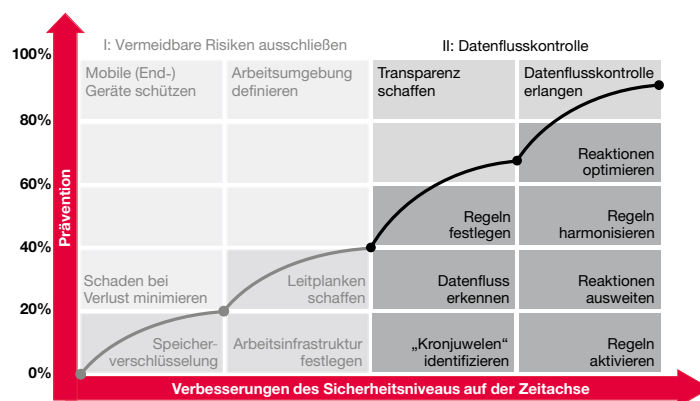
Der Kunde legt fest, wie seine sensiblen Daten übertragen, gespeichert und verarbeitet werden dürfen:

- Übertragung der Daten über Web-Mail, Webdienste etc.
- Speicherung der Daten in Verzeichnissen, Datenbanken etc.
- Datenverarbeitung an Endgeräten

Die Lösung beobachtet über spezielle Sensoren die als sensibel gekennzeichneten Daten. Der Kunde erhält so zu jeder Zeit Auskunft über den aktuellen Sicherheitsstatus dieser Daten.

Prävention optimieren

Erkennt die Lösung über die Sensoren, dass im Umgang mit den sensiblen Daten ein Regelverstoß droht, reagiert sie, noch bevor die Daten abfließen können. Diese Reaktionen sensibilisieren die Mitarbeiter fortlaufend und sind flexibel konfigurierbar: von einer Warnung vor möglichen Fehlern bis hin zur vollständigen Unterbindung des Datenflusses. Über diese Schutzfunktion kann der Kunde seine Regeln zum Umgang mit sensiblen Daten nachweislich durchsetzen. Dabei bleibt der Datenfluss innerhalb der Geschäftsprozesse erlaubt, die Produktivität ist sichergestellt, der ungewollte Datenabfluss aber wird verhindert.



Effektive Präventionslösung mit secunet

Die IT-Sicherheitsexperten von secunet verfügen über Know-how und Erfahrung in den Bereichen Datenschutz und Informationssicherheit. Die Beratung sichert eine schnelle und effektive Umsetzung des Präventionsprojekts und unterstützt bei der Auswahl

- passender und bewährter Technologie für beide Projektphasen,
- relevanter Kriterien für die effektive Erkennung sensibler Daten,
- geeigneter Sensoren passend zu den kritischen Geschäftsprozessen,
- spezifischer Regeln zum Umgang mit sensiblen Daten und
- ausgewählter Reaktionsmechanismen bei drohenden Regelverstößen.

Kunden gewährleisten somit konsequent und nachhaltig einen ganzheitlichen Schutz ihrer sensiblen Unternehmensdaten.

Weitere Informationen:
www.secunet.com/dlp



secunet Security Networks AG
 Kronprinzenstraße 30
 45128 Essen

Tel.: +49-201-5454-0
 Fax: +49-201-5454-1000
 E-Mail: info@secunet.com
www.secunet.com