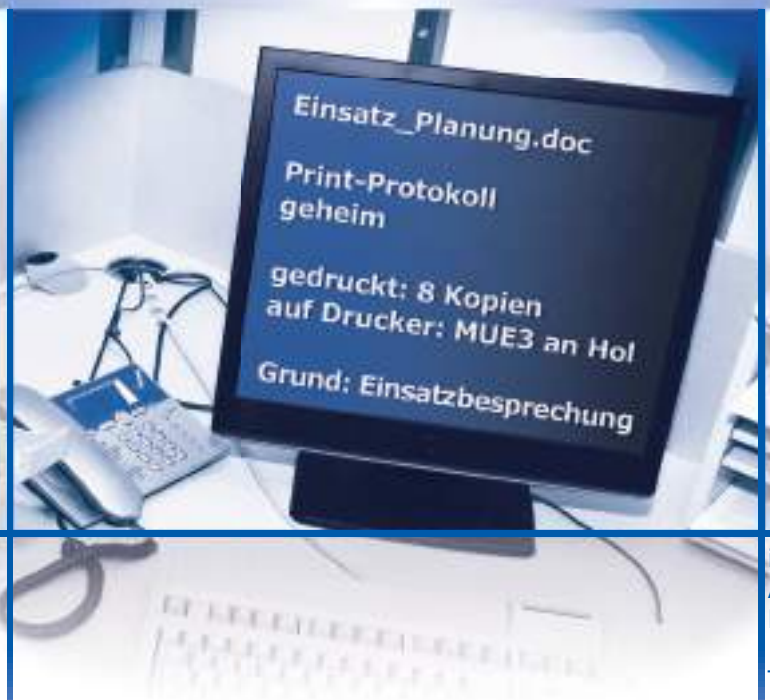
PrintWatch

Data Leakage Prevention - Kontrolle, Beweissicherung und Überblick auch über gedruckte Dokumente



itWatch

itWatch GmbH
Aschauer Str. 30
D-81549 München

Tel.: +49 (0)89 62 03 01 00
Fax: +49 (0) 89 62 03 01 069

info@itWatch.de
www.itWatch.de

PrintWatch

Data Leakage Prevention – Kontrolle, Beweissicherung und Überblick auch über gedruckte Dokumente.

PrintWatch ermöglicht es Ihnen, die in Ihrem Unternehmen gespeicherten Informationen auf dem Weg zum Drucker nach Ihren Wünschen zu kontrollieren, bevor sie das Papier als langfristigen, nicht mehr kontrollierbaren "Datenspeicher" erreichen. Damit schließt **PrintWatch** eine der letzten Lücken, durch die sensible firmeneigene Informationen aus dem Unternehmen abfließen können:

PrintWatch

- erkennt Druckaufträge für sensible Dokumente, unterscheidet diese von Druckaufträgen für unkritische Dokumente und leistet dadurch einen fortgeschrittenen Beitrag zu Ihrer Data Loss Prevention Strategie (DLP).
- kann den Ausdruck entsprechend der zentral definierten Sicherheitsrichtlinie für bestimmte Dokumente, Benutzer oder Gruppen verbieten oder erlauben.
- Der Inhalt des Ausdrucks selbst wird in Echtzeit in ein zukunftssicheres, standardisiertes Zwischenformat gebracht. Das Zwischenformat wird bei Bedarf verschlüsselt in eine revisionssichere Langzeitarchivierung überführt.
  - Gleiche Ausdrucke werden automatisch erkannt und deshalb nicht erneut übertragen oder noch einmal zentral gespeichert.
  - Selbst kleinste Veränderungen an der Ausgangsdatei werden erkannt und führen zu einer erneuten Hinterlegung.
  - Durch das standardisierte Zwischenformat ist sichergestellt, dass keine Abhängigkeiten von Druckertreiber, Drucker oder anderen Infrastrukturkomponenten besteht und die Information exakt und ohne Abweichung jederzeit auf jeder anderen Infrastruktur wieder hergestellt werden kann.
- Über die Report-Engine der **itWatch Security Suite** können Sie jederzeit recherchieren wann, wo, von wem, aus welchen Gründen, wie viele Ausdrucke eines bestimmten Dokuments gemacht wurden. Durch die Exportkontrolle der anderen Module der **itWatch Security Suite** haben Sie einen vollständigen Überblick.

Gefährdungslage:

- Ausdrucke können, wenn Sie nicht geeignet kenntlich gemacht sind, in andere Papiere oder Unterlagen integriert werden, so dass es für die Sicherheitskontrolle am Ausgang kaum möglich ist die Kritikalität einzuschätzen.
- Drucker mit Sicherheitsfunktionen sind als Standarddrucker zu teuer – besonders sensible Informationen dürfen nicht auf jedem Standarddrucker ausgedruckt werden.
- Ein Datenschutzvorfall führt ohne fundierte Beweislage zu einem Generalverdacht für alle Personen mit Leserecht und bringt dadurch unnötigen Unfrieden in die Organisation.

Herausforderungen:

- Ein Kontrollgremium darf zwar sensible Information sehen, aber nicht drucken.
- Mit Bordmitteln des Betriebssystems können zwar Drucker zugeordnet, gesperrt und frei gegeben werden, aber es ist nicht möglich die Sensibilität des Dokumentes als Entscheidungskriterium zu verwenden.
- Generelle Druckverbote behindern den Arbeitsfluss.
- Erst die Kombination der Informationen: wer, was, warum, in welcher Stückzahl, auf welchem Drucker ausgedruckt hat, bringt die geeignete Granularität für sicherheitskritische Informationen.

PrintWatch von itWatch ist die optimale Lösung für KMU und große Unternehmen

Mit **PrintWatch** bestimmen Sie selbst, welche Dokumente durch welchen Benutzer auf welchem Drucker gedruckt werden dürfen und welche Zusatzinformationen archiviert und auf den Ausdruck eingebunden werden. Dadurch wissen Sie immer, wer, wann, warum, welches Dokument, mit welchem Inhalt, in welcher Stückzahl, über welchen Drucker ausgegeben hat. Denn die Lösung protokolliert diese Daten für jeden Ausdruck und legt sie zudem revisionssicher ab. Auflagen der Langzeitarchivierung werden dadurch gleich nebenbei mit erfüllt.

PrintWatch überwacht alle Druckvorgänge und protokolliert nur diejenigen, die durch Dateiart und Kennungen im Header als kritisch eingestuft sind, oder vom Anwender in Echtzeit als kritisch eingestuft werden.

Auf diese Weise ist sichergestellt, dass alle Informationen zu einem sicherheitskritischen Druckauftrag – lokale Drucker und Netzwerkdrucker - immer vorhanden sind, über einfache Reports recherchiert werden können und kein Anwender modifizierend darauf zugreifen kann.

FSPW-170928