



DLP

Data Loss / Leakage Prevention

An der Generalversammlung der



vom Donnerstag 23. September 2010 in Zürich bei Google

Erich Vogt, SignPool Group AG



Medienbruchfreie Abläufe elektronische Prozesse - Gesetzeskonform



Elektronische Formulare



Digitale Unterschrift



Dokumenten Management System



make IT happen

Vorstellung Erich Vogt



Informatiker seit 25 Jahren, Informatik-Lehrmeister und Prüfungsexperte

- CS (SKA) Einstieg 1984 / Prime Computer / Unternehmer
- PDF, ePaper, eForms seit PDF 1.0 (1993)
- CISSP
- ...

Mitglied eCH, Verein zur Schaffung und Förderung von eGovernment Standards in der Schweiz

- Fachgruppe Technologie (SAGA.ch)
- Leitung Fachgruppe eForms (elektronische Formulare)
- Review Fachgruppe Digitale Signatur (DigSig)

Mitglied ISSS (Information Security Society Switzerland)

- Mitarbeit SIG-SIX (Secure Information Exchange)



Der Begriff und seine Bedeutungen



Data Loss Prevention (DLP) ist ein einprägsamer Marketingbegriff aus dem Bereich der Informationssicherheit. Auch **Data Leak / Leakage Prevention** genannt, ist DLP aus der „Extrusion Prevention“ Technik hervorgegangen. Klassisch gesehen gehört DLP zu den Schutzmaßnahmen, die direkt den Schutz der Vertraulichkeit von Daten unterstützt und je nach Ausprägung direkt oder indirekt die Integrität und Zuordenbarkeit.

Data Loss (Prevention)

ist der Schutz gegen den unerwünschten Abfluss von Daten, der Schaden verursacht und auch bemerkt wird.

Data Leak/Leakage (Prevention)

Steht für einen Schutz gegen ein vermutetes, aber nicht messbares und manchmal auch im Einzelfall gar nicht feststellbares Weitergeben von Informationen an unerwünschte Empfänger.



DLP aus Sicht ICT und physisch



- **Netzwerk**
- **Operating System**
- **Firewall**
- **IDP**
- **Applikationen, Datenbanken**

- **Gebäude-, Umweltsicherheit**
- **Zutrittskontrolle, -sicherheit**
- **Sichtschutz**
- **Einbruchschutz**

Betroffene Elemente

- **Whiteboards**
- **Flipcharts**
- **physische Dokumente**



DLP mit Fokus Dokumente (Dateien)



- **Geschäftsberichte**
- **Marketing-Papiere**
- **Technische Dokumentation**
- **Präsentationen**
- **Kalkulationen**
- **Fotos**
- **Social Networks**
- **Konstruktionszeichnungen**
- **GL / VR Papiere - Mails**



Bedrohung, (Warum, Wodurch)



Unachtsamkeit, Verlieren

- Neugier

Mutwillig, Diebstahl

- Industriespionage
- Erpressung
- Politische Vorteile

Wichtig, eine seriöse, umfassende Analyse!

z.B. nach dem orthogonalem Bedrohungsmodell der ISSS =>





Wo gehen Daten "Verloren"?



MFP

- Konfiguration
- Authentifizierung zum Abruf, Druck vertraulicher Dokumente
- Bei der Wartung, Entsorgung
- Speicher
- Festplatte

Handy's

- Trojaner
- Chipmodifikation

Mobile Devices

Memory Sticks

eMail

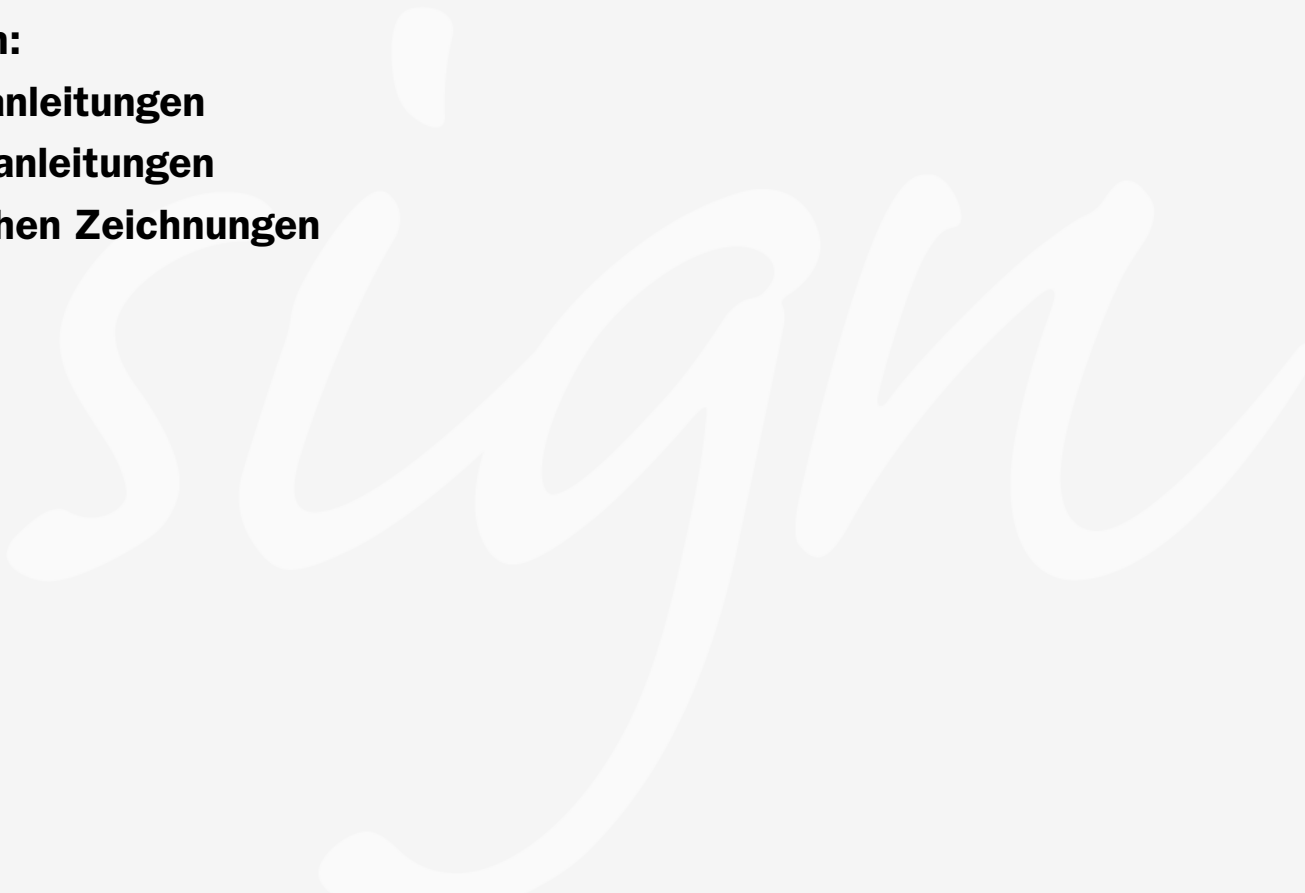


Datenmodifikation



Abändern von:

- **Betriebsanleitungen**
- **Montageanleitungen**
- **Technischen Zeichnungen**



make IT happen

(DL) Prevention 1



DRM/IRM (Digital/Information Rights Management)

- Klassifizierung der Dokumente (Information)
- aktuelle/Live Dokumente (Dateien)
- Archivierte Dokumente (Dateien)

ILM

- Aufbewahrungsfristen
- gezielte vernichtung von Daten (Dokumenten)

IAM Schwergewicht Identiy

- Zertifikatshandling
 - *Persönlich*
 - *Unternehmen*
 - *Ersatzzertifikate*
- Temporär
- Permanent
- HR
 - *Muss zwingend eingebunden sein*
 - *Eintritts und vor allem Austrittsdatum*
 - *Funktionswechsel*



(DL) Prevention 2



Physical- / ICT-Security

- Firewalls (klassisch)
- Application (Firewalls)
- IDP (Intrusion Detection and Prevention)
- Loganalyse
- Application Security
- Device Management
- USB-devices
- Mobile-Devices
- CD, DVD, MO, Tape
- Device-, Datenträgerentsorgung



Umsetzungsprobleme



- **Awareness**
- **User**
- **Managment**
- **Budget**
- **Technologie**

sign



Weitere Informationen



- www.melani.admin.ch
- www.im.nrw.de/wirtschaftsspionage
- alle Security Software Hersteller
- div. Security Newsletter und Newsguppen





Medienbruchfreie Abläufe

elektronische Prozesse – gesetzeskonform und sicher



Innovative und Zukunftsorientierte Betriebe sind **heute** dazu in der Lage!



Lassen Sie es uns tun!

erich.vogt@signpool.com