Data Loss Prevention

René Pfeiffer

web.luchs.at

25. April 2012

Inhaltsübersicht - Wovon reden wir?

- Informationssicherheit - Sicherheit von Informationen
- Wo leben Daten?
- Wie bewegen sich Daten?
- Was ist *Data Loss Prevention*?
- Wir reden **nicht** über defekte Datenträger!
- Was sollte man wissen?
- mögliche Implementationen
- *keine* Empfehlungen ☺

Inhaltsübersicht - Wovon reden wir?

- Informationssicherheit - Sicherheit von Informationen
- Wo leben Daten?
- Wie bewegen sich Daten?
- Was ist *Data Loss Prevention*?
- Wir reden **nicht** über defekte Datenträger!
- Was sollte man wissen?
- mögliche Implementationen
- *keine* Empfehlungen ☺

Informationssicherheit

- *Information* ist alles, was sich speichern / drucken / aufschreiben / merken läßt.
- *Sicherheit* ist ein Kompromiß zwischen Gruppen mit verschiedenen Agenden.
- *Informationssicherheit*
  - ist nicht wohldefiniert,
  - ist eine komplexe/periodische Tätigkeit, kein Zustand, kein Objekt, keine Ware.

Informationssicherheit

- *Information* ist alles, was sich speichern / drucken / aufschreiben / merken läßt.
- *Sicherheit* ist ein Kompromiß zwischen Gruppen mit verschiedenen Agenden.
- *Informationssicherheit*
  - ist nicht wohldefiniert,
  - ist eine komplexe/periodische Tätigkeit, kein Zustand, kein Objekt, keine Ware.

Informationssicherheit

- *Information* ist alles, was sich speichern / drucken / aufschreiben / merken läßt.
- *Sicherheit* ist ein Kompromiß zwischen Gruppen mit verschiedenen Agenden.
- *Informationssicherheit*
  - ist nicht wohldefiniert,
  - ist eine komplexe/periodische Tätigkeit, kein Zustand, kein Objekt, keine Ware.

Informationssicherheit

- *Information* ist alles, was sich speichern / drucken / aufschreiben / merken läßt.
- *Sicherheit* ist ein Kompromiß zwischen Gruppen mit verschiedenen Agenden.
- *Informationssicherheit*
  - ist nicht wohldefiniert,
  - ist eine komplexe/periodische Tätigkeit, kein Zustand, kein Objekt, keine Ware.

Informationssicherheit

- *Information* ist alles, was sich speichern / drucken / aufschreiben / merken läßt.
- *Sicherheit* ist ein Kompromiß zwischen Gruppen mit verschiedenen Agenden.
- *Informationssicherheit*
  - ist nicht wohldefiniert,
  - ist eine komplexe/periodische Tätigkeit, kein Zustand, kein Objekt, keine Ware.

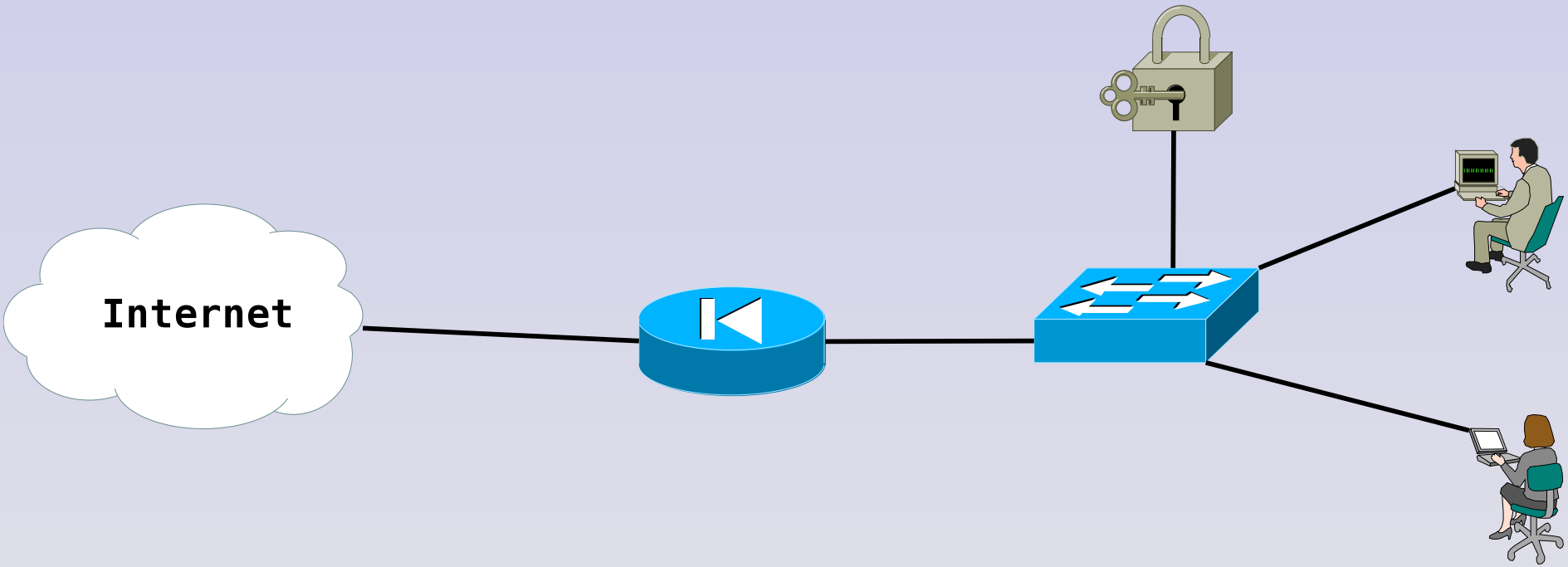
Informationssicherheit

- *Information* ist alles, was sich speichern / drucken / aufschreiben / merken läßt.
- *Sicherheit* ist ein Kompromiß zwischen Gruppen mit verschiedenen Agenden.
- *Informationssicherheit*
  - ist nicht wohldefiniert,
  - ist eine komplexe/periodische Tätigkeit, kein Zustand, kein Objekt, keine Ware.

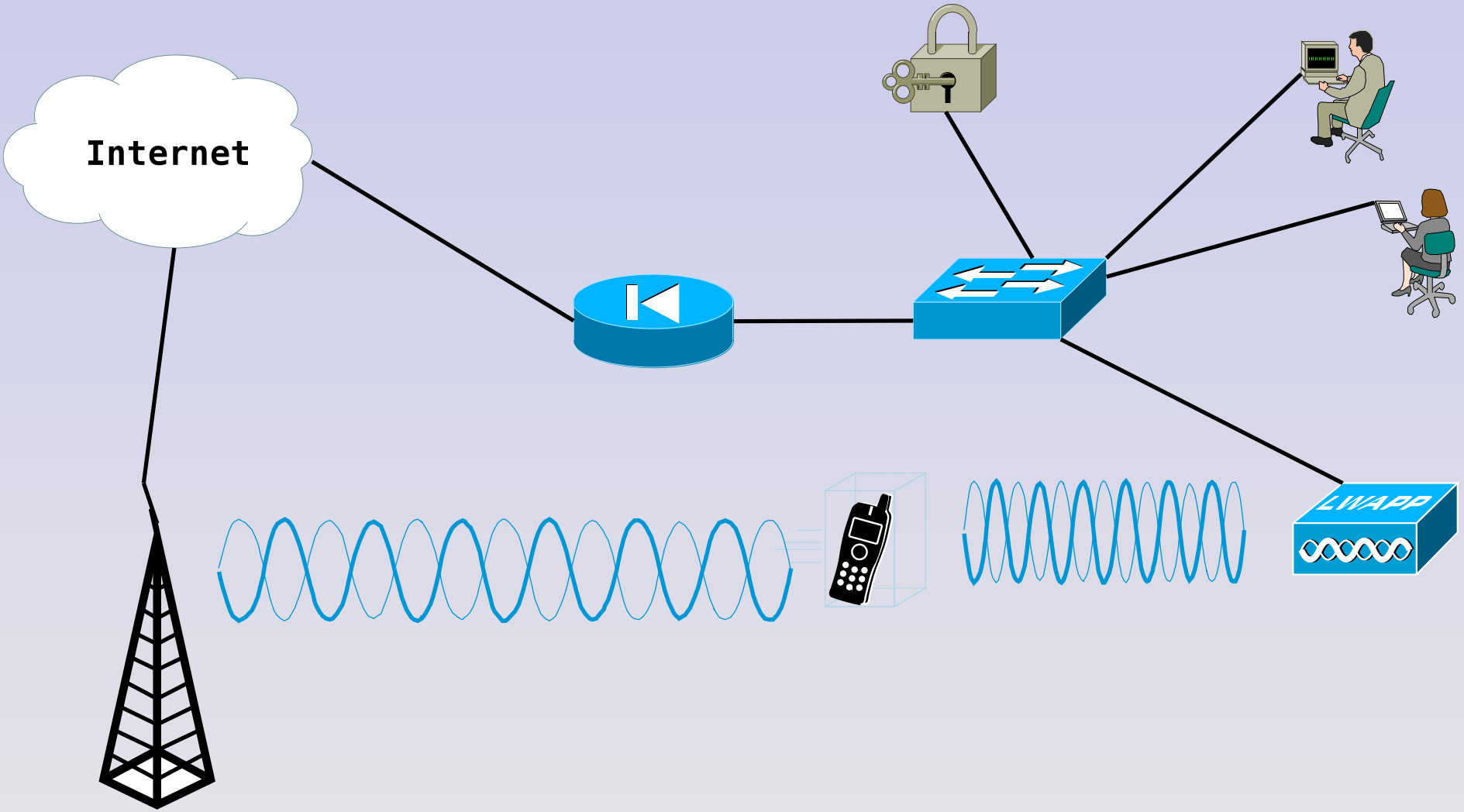
Informationssicherheit

- *Information* ist alles, was sich speichern / drucken / aufschreiben / merken läßt.
- *Sicherheit* ist ein Kompromiß zwischen Gruppen mit verschiedenen Agenden.
- *Informationssicherheit*
  - ist nicht wohldefiniert,
  - ist eine komplexe/periodische Tätigkeit, kein Zustand, kein Objekt, keine Ware.

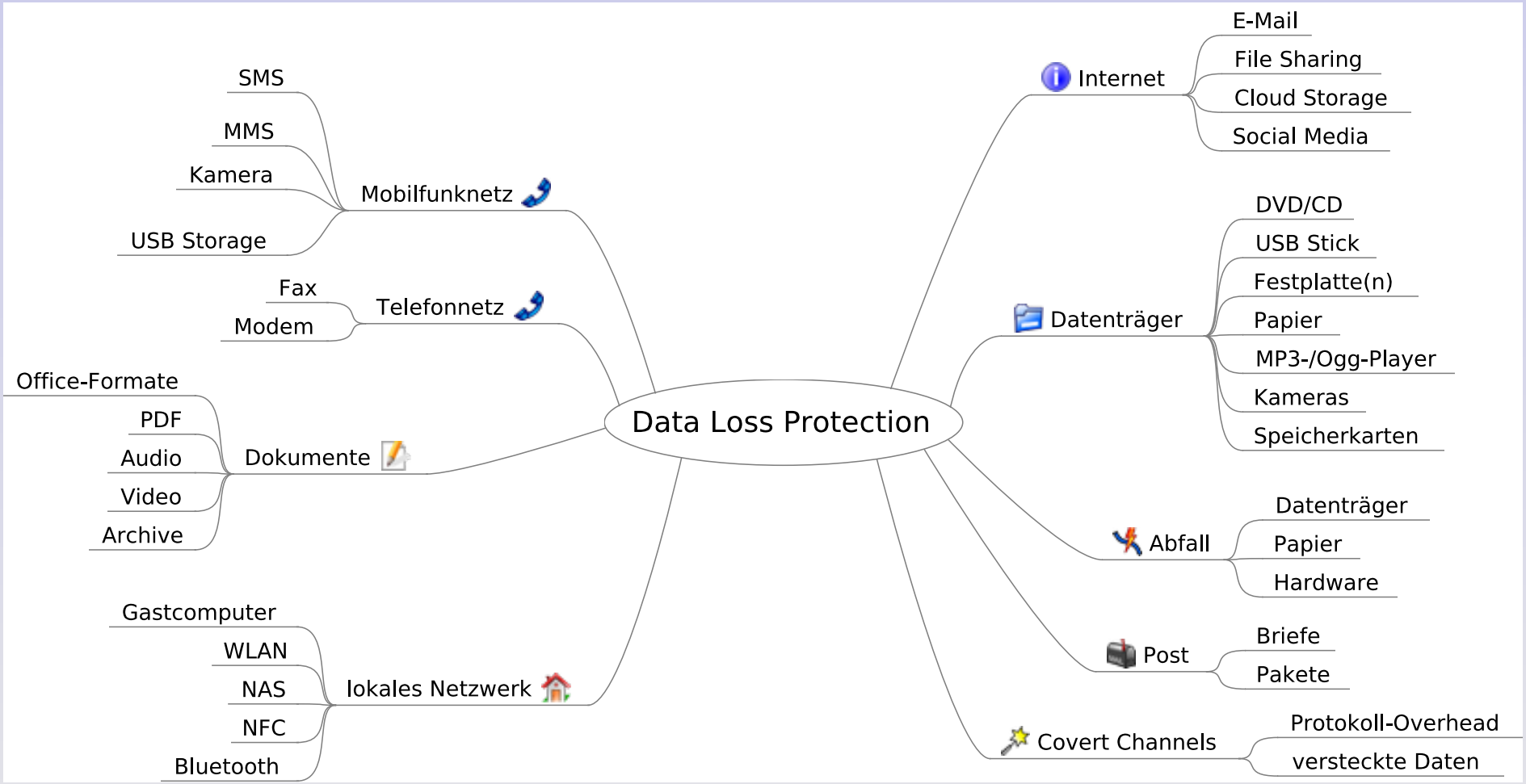
Daten in freier Wildbahn (1)



Daten in freier Wildbahn (2)



Datenwege


Data Loss Protection
Internet
E-Mail
File Sharing
Cloud Storage
Social Media
Datenträger
DVD/CD
USB Stick
Festplatte(n)
Papier
MP3-/Ogg-Player
Kameras
Speicherkarten
Abfall
Datenträger
Papier
Hardware
Post
Briefe
Pakete
Covert Channels
Protokoll-Overhead
versteckte Daten
Mobilfunknetz
SMS
MMS
Kamera
USB Storage
Telefonnetz
Fax
Modem
Dokumente
Office-Formate
PDF
Audio
Video
Archive
lokales Netzwerk
Gastcomputer
WLAN
NAS
NFC
Bluetooth

Preisfrage: Was ist das?

Was ist Data Loss Protection?

- Data Loss Protection (oder Prevention) - DLP -
  - verringert das Risiko für „verlorene“ Informationen,
  - entdeckt Zugriffe Datenlecks und
  - verbietet bzw. regelt Zugriffe auf Daten.

  Theoretisch.
- DLP besteht aus einer Reihe von Maßnahmen
- DLP muß Daten kennen
  - `aptitude install data-loss-prevention` geht nicht
  - Daten müssen klassifiziert sein

Was ist Data Loss Protection?

- Data Loss Protection (oder Prevention) - DLP -
  - verringert das Risiko für „verlorene“ Informationen,
  - entdeckt Zugriffe Datenlecks und
  - verbietet bzw. regelt Zugriffe auf Daten.

  Theoretisch.
- DLP besteht aus einer Reihe von Maßnahmen
- DLP muß Daten kennen
  - `aptitude install data-loss-prevention` geht nicht
  - Daten müssen klassifiziert sein

Was ist Data Loss Protection?

- Data Loss Protection (oder Prevention) - DLP -
  - verringert das Risiko für „verlorene“ Informationen,
  - entdeckt Zugriffe Datenlecks und
  - verbietet bzw. regelt Zugriffe auf Daten.

  Theoretisch.
- DLP besteht aus einer Reihe von Maßnahmen
- DLP muß Daten kennen
  - `aptitude install data-loss-prevention` geht nicht
  - Daten müssen klassifiziert sein

Was ist Data Loss Protection?

- Data Loss Protection (oder Prevention) - DLP -
  - verringert das Risiko für „verlorene“ Informationen,
  - entdeckt Zugriffe Datenlecks und
  - verbietet bzw. regelt Zugriffe auf Daten.

  Theoretisch.
- DLP besteht aus einer Reihe von Maßnahmen
- DLP muß Daten kennen
  - `aptitude install data-loss-prevention` geht nicht
  - Daten müssen klassifiziert sein

Was ist Data Loss Protection?

- Data Loss Protection (oder Prevention) - DLP -
  - verringert das Risiko für „verlorene“ Informationen,
  - entdeckt Zugriffe Datenlecks und
  - verbietet bzw. regelt Zugriffe auf Daten.

  Theoretisch.
- DLP besteht aus einer Reihe von Maßnahmen
- DLP muß Daten kennen
  - `aptitude install data-loss-prevention` geht nicht
  - Daten müssen klassifiziert sein

Wo leben Daten?

- Data at Rest (DaR)
  - gespeicherte Daten
  - archivierte Daten
  - ausgedruckte Daten
- Data in Motion (DiM)
  - Daten auf dem Weg von *A* nach *B*
  - Netzwerktransmissionen
  - bewegte Datenträger
- Data in Use (DiU)
  - Daten am Endpunkt (Start oder Ziel)
  - Arbeitsstation, Endgerät, Server

Wo leben Daten?

- Data at Rest (DaR)
  - gespeicherte Daten
  - archivierte Daten
  - ausgedruckte Daten
- Data in Motion (DiM)
  - Daten auf dem Weg von *A* nach *B*
  - Netzwerktransmissionen
  - bewegte Datenträger
- Data in Use (DiU)
  - Daten am Endpunkt (Start oder Ziel)
  - Arbeitsstation, Endgerät, Server

Wo leben Daten?

- Data at Rest (DaR)
  - gespeicherte Daten
  - archivierte Daten
  - ausgedruckte Daten
- Data in Motion (DiM)
  - Daten auf dem Weg von *A* nach *B*
  - Netzwerktransmissionen
  - bewegte Datenträger
- Data in Use (DiU)
  - Daten am Endpunkt (Start oder Ziel)
  - Arbeitsstation, Endgerät, Server

Wo leben Daten?

- Data at Rest (DaR)
  - gespeicherte Daten
  - archivierte Daten
  - ausgedruckte Daten
- Data in Motion (DiM)
  - Daten auf dem Weg von *A* nach *B*
  - Netzwerktransmissionen
  - bewegte Datenträger
- Data in Use (DiU)
  - Daten am Endpunkt (Start oder Ziel)
  - Arbeitsstation, Endgerät, Server

Wo leben Daten?

- Data at Rest (DaR)
  - gespeicherte Daten
  - archivierte Daten
  - ausgedruckte Daten
- Data in Motion (DiM)
  - Daten auf dem Weg von *A* nach *B*
  - Netzwerktransmissionen
  - bewegte Datenträger
- Data in Use (DiU)
  - Daten am Endpunkt (Start oder Ziel)
  - Arbeitsstation, Endgerät, Server

Wege zu DLP

- Daten administrativ klassifizieren
  - intern (vertraulich, geheim, ...)
  - öffentlich
- Daten digital identifizieren
  - Checksummen (MD5, SHA1, ...)
  - Metadaten
- Datenbereiche abtrennen
  - Schleusen einbauen (Proxies)
  - *alle* Datentransmissionen überprüfen
  - *alle* verschlüsselten Datentransmissionen überprüfen
- DaR & DiU sichern
  - Verschlüsseln
  - Zugriff an Applikationen und Betriebssystem sichern

Wege zu DLP

- Daten administrativ klassifizieren
  - intern (vertraulich, geheim, . . .)
  - öffentlich
- Daten digital identifizieren
  - Checksummen (MD5, SHA1, . . .)
  - Metadaten
- Datenbereiche abtrennen
  - Schleusen einbauen (Proxies)
  - *alle* Datentransmissionen überprüfen
  - *alle* verschlüsselten Datentransmissionen überprüfen
- DaR & DiU sichern
  - Verschlüsseln
  - Zugriff an Applikationen und Betriebssystem sichern

Wege zu DLP

- Daten administrativ klassifizieren
  - intern (vertraulich, geheim, . . .)
  - öffentlich
- Daten digital identifizieren
  - Checksummen (MD5, SHA1, . . .)
  - Metadaten
- Datenbereiche abtrennen
  - Schleusen einbauen (Proxies)
  - *alle* Datentransmissionen überprüfen
  - *alle* verschlüsselten Datentransmissionen überprüfen
- DaR & DiU sichern
  - Verschlüsseln
  - Zugriff an Applikationen und Betriebssystem sichern

Wege zu DLP

- Daten administrativ klassifizieren
  - intern (vertraulich, geheim, . . .)
  - öffentlich
- Daten digital identifizieren
  - Checksummen (MD5, SHA1, . . .)
  - Metadaten
- Datenbereiche abtrennen
  - Schleusen einbauen (Proxies)
  - *alle* Datentransmissionen überprüfen
  - *alle* verschlüsselten Datentransmissionen überprüfen
- DaR & DiU sichern
  - Verschlüsseln
  - Zugriff an Applikationen und Betriebssystem sichern

Wege zu DLP

- Daten administrativ klassifizieren
  - intern (vertraulich, geheim, . . .)
  - öffentlich
- Daten digital identifizieren
  - Checksummen (MD5, SHA1, . . .)
  - Metadaten
- Datenbereiche abtrennen
  - Schleusen einbauen (Proxies)
  - *alle* Datentransmissionen überprüfen
  - *alle* verschlüsselten Datentransmissionen überprüfen
- DaR & DiU sichern
  - Verschlüsseln
  - Zugriff an Applikationen und Betriebssystem sichern

Das Problem mit dem Identifizieren

- `sha224sum Marines-in-Fallujah.jpg`
  `97ddd1eb977e1713bbeeaab74a159b018929ed4931ca70ae224604a6`
  `Marines-in-Fallujah.jpg`
- `cp -a Marines-in-Fallujah.jpg Marines-in-Fallujah1.jpg`
- `jhead -purejpg Marines-in-Fallujah1.jpg`
- `sha224sum Marines-in-Fallujah1.jpg`
  `307b890f07f906aa414d62a3011e151ca9532a5487d83ac379ab99ac`
  `Marines-in-Fallujah1.jpg`
- `convert -quality 89 Marines-in-Fallujah.jpg`
  `Marines-in-Fallujah2.jpg`
- `sha224sum Marines-in-Fallujah2.jpg`
  `4010a1260ebe72697cbfa37ed9c42b1a81f06ae4d0a37d98b6e7f39b`
  `Marines-in-Fallujah2.jpg`

Das Problem mit dem Identifizieren

- `sha224sum Marines-in-Fallujah.jpg`
  `97ddd1eb977e1713bbeeaab74a159b018929ed4931ca70ae224604a6`
  `Marines-in-Fallujah.jpg`
- `cp -a Marines-in-Fallujah.jpg Marines-in-Fallujah1.jpg`
- `jhead -purejpg Marines-in-Fallujah1.jpg`
- `sha224sum Marines-in-Fallujah1.jpg`
  `307b890f07f906aa414d62a3011e151ca9532a5487d83ac379ab99ac`
  `Marines-in-Fallujah1.jpg`
- `convert -quality 89 Marines-in-Fallujah.jpg`
  `Marines-in-Fallujah2.jpg`
- `sha224sum Marines-in-Fallujah2.jpg`
  `4010a1260ebe72697cbfa37ed9c42b1a81f06ae4d0a37d98b6e7f39b`
  `Marines-in-Fallujah2.jpg`

Das Problem mit der Kontamination

- Daten hinterlassen lesbare Spuren
  - beschriebene Datenträger
  - „Reste“ im Arbeitsspeicher
- Daten kontaminieren Umgebung
  - ☣ & ☢ sind gute Analogien
  - Datenträger immer reinigen oder vernichten
- Daten werden transportiert
  - ☣ Ansteckung, Epidemie
  - ☢ „Fallout“, Leck im Kühlsystem
  - Umgebung wird verunreinigt

Das Problem mit der Kontamination

- Daten hinterlassen lesbare Spuren
  - beschriebene Datenträger
  - „Reste“ im Arbeitsspeicher
- Daten kontaminieren Umgebung
  - ☣ & ☢ sind gute Analogien
  - Datenträger immer reinigen oder vernichten
- Daten werden transportiert
  - ☣ Ansteckung, Epidemie
  - ☢ „Fallout“, Leck im Kühlsystem
  - Umgebung wird verunreinigt

Das Problem mit der Kontamination

- Daten hinterlassen lesbare Spuren
  - beschriebene Datenträger
  - „Reste“ im Arbeitsspeicher
- Daten kontaminieren Umgebung
  - ☣ & ☢ sind gute Analogien
  - Datenträger immer reinigen oder vernichten
- Daten werden transportiert
  - ☣ Ansteckung, Epidemie
  - ☢ „Fallout“, Leck im Kühlsystem
  - Umgebung wird verunreinigt

Das Problem mit der Kontamination

- Daten hinterlassen lesbare Spuren
  - beschriebene Datenträger
  - „Reste“ im Arbeitsspeicher
- Daten kontaminieren Umgebung
  - ☣ & ☢ sind gute Analogien
  - Datenträger immer reinigen oder vernichten
- Daten werden transportiert
  - ☣ Ansteckung, Epidemie
  - ☢ „Fallout“, Leck im Kühlsystem
  - Umgebung wird verunreinigt

DLP Implementationen

- Erfassen der digitalen Resourcen
- Komponenten in der Infrastruktur
  - DLP Content Inspection
  - Firewalls
  - Partitionierung
  - Proxies
  - physische Trennung
- Komponenten an Endpunkten
  - DLP Agents
  - Betriebssystemrichtlinien

DLP Implementationen

- Erfassen der digitalen Resourcen
- Komponenten in der Infrastruktur
  - DLP Content Inspection
  - Firewalls
  - Partitionierung
  - Proxies
  - physische Trennung
- Komponenten an Endpunkten
  - DLP Agents
  - Betriebssystemrichtlinien

DLP Implementationen

- Erfassen der digitalen Resourcen
- Komponenten in der Infrastruktur
  - DLP Content Inspection
  - Firewalls
  - Partitionierung
  - Proxies
  - physische Trennung
- Komponenten an Endpunkten
  - DLP Agents
  - Betriebssystemrichtlinien

DLP Implementationen

- Erfassen der digitalen Resourcen
- Komponenten in der Infrastruktur
  - DLP Content Inspection
  - Firewalls
  - Partitionierung
  - Proxies
  - physische Trennung
- Komponenten an Endpunkten
  - DLP Agents
  - Betriebssystemrichtlinien

Erfassen der digitalen Resourcen

- zu schützende Daten komplett erfassen
  - jeden Datenträger, jedes Bit!
  - jeden Ort!
  - jedes Gerät!
- Definieren & Erfassen der Datenformate
  - DLP mit Formatinformationen versorgen
  - DLP mit Signaturen versorgen
- Prozeß zur Aktualisierung implementieren
  - schützenswerte Daten verändern sich
  - Geräte, Orte & Konten wechseln

Ohne diese Schritte macht DLP keinen Sinn!

Erfassen der digitalen Resourcen

- zu schützende Daten komplett erfassen
  - jeden Datenträger, jedes Bit!
  - jeden Ort!
  - jedes Gerät!
- Definieren & Erfassen der Datenformate
  - DLP mit Formatinformationen versorgen
  - DLP mit Signaturen versorgen
- Prozeß zur Aktualisierung implementieren
  - schützenswerte Daten verändern sich
  - Geräte, Orte & Konten wechseln

Ohne diese Schritte macht DLP keinen Sinn!

Erfassen der digitalen Resourcen

- zu schützende Daten komplett erfassen
  - jeden Datenträger, jedes Bit!
  - jeden Ort!
  - jedes Gerät!
- Definieren & Erfassen der Datenformate
  - DLP mit Formatinformationen versorgen
  - DLP mit Signaturen versorgen
- Prozeß zur Aktualisierung implementieren
  - schützenswerte Daten verändern sich
  - Geräte, Orte & Konten wechseln

Ohne diese Schritte macht DLP keinen Sinn!

Erfassen der digitalen Resourcen

- zu schützende Daten komplett erfassen
  - jeden Datenträger, jedes Bit!
  - jeden Ort!
  - jedes Gerät!
- Definieren & Erfassen der Datenformate
  - DLP mit Formatinformationen versorgen
  - DLP mit Signaturen versorgen
- Prozeß zur Aktualisierung implementieren
  - schützenswerte Daten verändern sich
  - Geräte, Orte & Konten wechseln

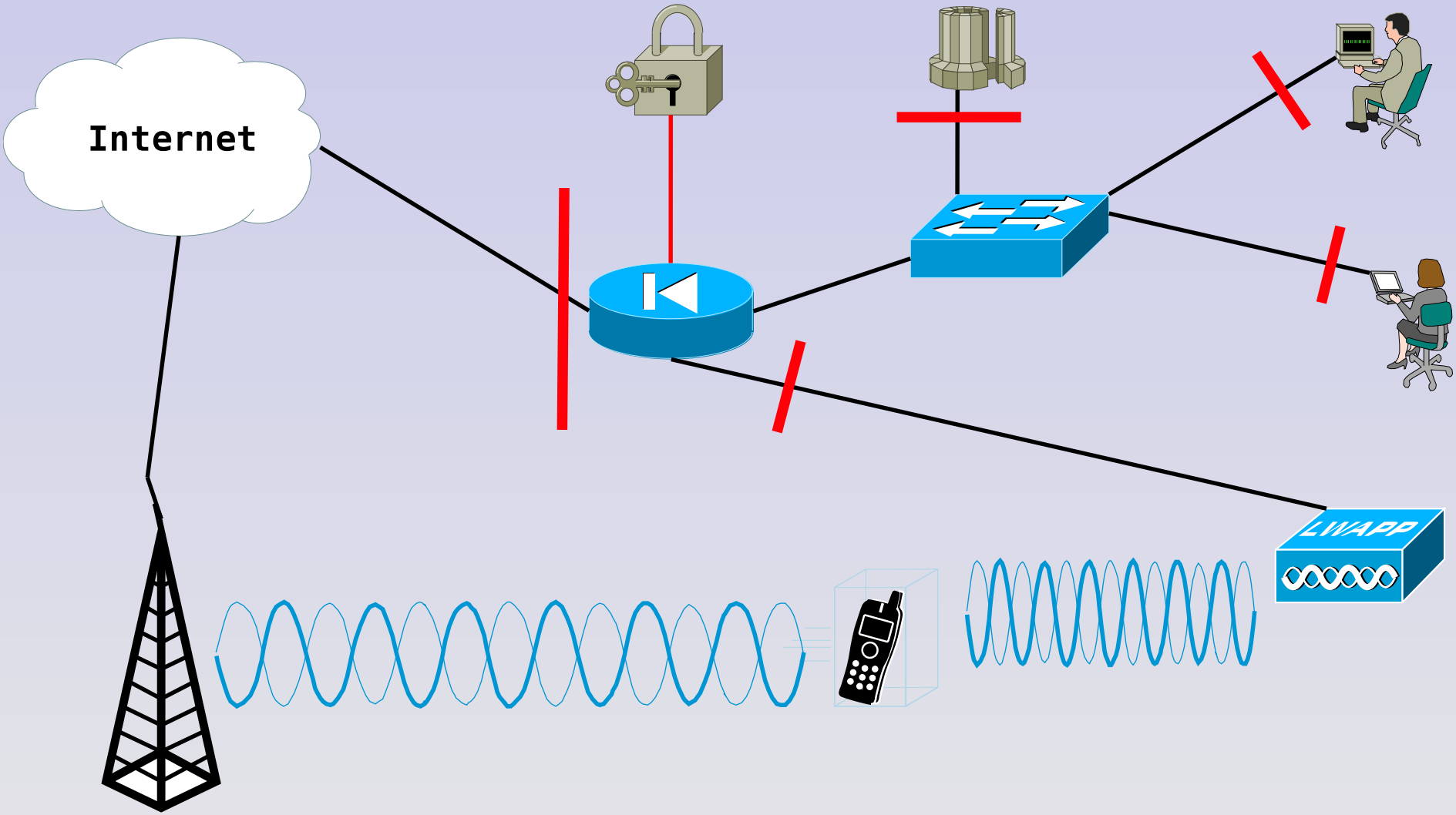
Ohne diese Schritte macht DLP keinen Sinn!

Erfassen der digitalen Resourcen

- zu schützende Daten komplett erfassen
  - jeden Datenträger, jedes Bit!
  - jeden Ort!
  - jedes Gerät!
- Definieren & Erfassen der Datenformate
  - DLP mit Formatinformationen versorgen
  - DLP mit Signaturen versorgen
- Prozeß zur Aktualisierung implementieren
  - schützenswerte Daten verändern sich
  - Geräte, Orte & Konten wechseln

Ohne diese Schritte macht DLP keinen Sinn!

Umbau des Netzwerkes mit DLP



Umbau des Netzwerkes mit DLP (2)

- Fluß aller Daten durch DLP Komponenten garantieren
  - Inspizieren aller transmittierten Daten
  - Lernphase / DLP Modus
- Absichern aller Betriebssysteme
  - Betriebssystemhärtung teil von DLP
  - Ausnutzen aller Betriebssystemmittel
- Installieren der DLP Agents
  - Schlagwort „endpoint protection“
  - Daten werden am Client „bewacht“

Umbau des Netzwerkes mit DLP (2)

- Fluß aller Daten durch DLP Komponenten garantieren
  - Inspizieren aller transmittierten Daten
  - Lernphase / DLP Modus
- Absichern aller Betriebssysteme
  - Betriebssystemhärtung teil von DLP
  - Ausnutzen aller Betriebssystemmittel
- Installieren der DLP Agents
  - Schlagwort „endpoint protection“
  - Daten werden am Client „bewacht“

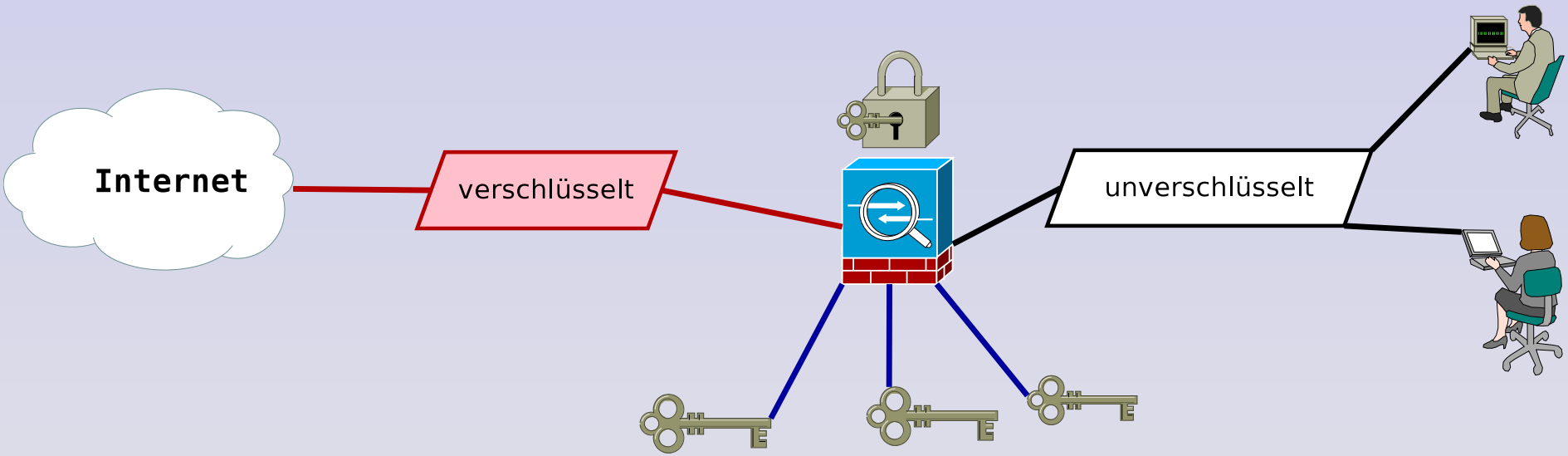
Umbau des Netzwerkes mit DLP (2)

- Fluß aller Daten durch DLP Komponenten garantieren
  - Inspizieren aller transmittierten Daten
  - Lernphase / DLP Modus
- Absichern aller Betriebssysteme
  - Betriebssystemhärtung teil von DLP
  - Ausnutzen aller Betriebssystemmittel
- Installieren der DLP Agents
  - Schlagwort „endpoint protection“
  - Daten werden am Client „bewacht“

Umbau des Netzwerkes mit DLP (2)

- Fluß aller Daten durch DLP Komponenten garantieren
  - Inspizieren aller transmittierten Daten
  - Lernphase / DLP Modus
- Absichern aller Betriebssysteme
  - Betriebssystemhärtung teil von DLP
  - Ausnutzen aller Betriebssystemmittel
- Installieren der DLP Agents
  - Schlagwort „endpoint protection“
  - Daten werden am Client „bewacht“

Umgang mit Verschlüsselung



Umgang mit Verschlüsselung (2)

- DLP Inspektion muß Daten sehen
- Verschlüsselung macht Inspektion unmöglich
- Lösung: Verschlüsselung endet/beginnt am Perimeter
  - Vertrauensverhältnisse überwacht DLP Gateway
  - Schlüssel / SSL CAs müssen hinterlegt werden
- Verwaltungsaufwand für DLP Überprüfung
  - Vertrauensverhältnisse müssen konfiguriert werden
  - Clients können Identitäten nicht überprüfen

Umgang mit Verschlüsselung (2)

- DLP Inspektion muß Daten sehen
- Verschlüsselung macht Inspektion unmöglich
- Lösung: Verschlüsselung endet/beginnt am Perimeter
  - Vertrauensverhältnisse überwacht DLP Gateway
  - Schlüssel / SSL CAs müssen hinterlegt werden
- Verwaltungsaufwand für DLP Überprüfung
  - Vertrauensverhältnisse müssen konfiguriert werden
  - Clients können Identitäten nicht überprüfen

Umgang mit Verschlüsselung (2)

- DLP Inspektion muß Daten sehen
- Verschlüsselung macht Inspektion unmöglich
- Lösung: Verschlüsselung endet/beginnt am Perimeter
  - Vertrauensverhältnisse überwacht DLP Gateway
  - Schlüssel / SSL CAs müssen hinterlegt werden
- Verwaltungsaufwand für DLP Überprüfung
  - Vertrauensverhältnisse müssen konfiguriert werden
  - Clients können Identitäten nicht überprüfen

Umgang mit Verschlüsselung (2)

- DLP Inspektion muß Daten sehen
- Verschlüsselung macht Inspektion unmöglich
- Lösung: Verschlüsselung endet/beginnt am Perimeter
  - Vertrauensverhältnisse überwacht DLP Gateway
  - Schlüssel / SSL CAs müssen hinterlegt werden
- Verwaltungsaufwand für DLP Überprüfung
  - Vertrauensverhältnisse müssen konfiguriert werden
  - Clients können Identitäten nicht überprüfen

Grenzen von Data Loss Prevention

Lücken für DLP

- „frische“ Daten ohne Signatur
  - neu erstellte Datenobjekte
  - maximal durch Formatsperren zu verhindern
- Echtzeitdaten
  - VoIP Telefonie (Video oder Audio), Fax
  - Telekommunikationsüberwachung (Verbindungs-/Inhaltsdaten)
- transformierte Daten
  - „analog hole“
  - Ausdrucke einscannen / fotografieren
  - Datenformate wandeln (z.B. Text- in Bilddaten)
- Abfälle
  - ausrangierte Datenträger
  - Unterlagen, Papiermüll

Lücken für DLP

- „frische“ Daten ohne Signatur
  - neu erstellte Datenobjekte
  - maximal durch Formatsperren zu verhindern
- Echtzeitdaten
  - VoIP Telefonie (Video oder Audio), Fax
  - Telekommunikationsüberwachung (Verbindungs-/Inhaltsdaten)
- transformierte Daten
  - „analog hole“
  - Ausdrucke einscannen / fotografieren
  - Datenformate wandeln (z.B. Text- in Bilddaten)
- Abfälle
  - ausrangierte Datenträger
  - Unterlagen, Papiermüll

Lücken für DLP

- „frische“ Daten ohne Signatur
  - neu erstellte Datenobjekte
  - maximal durch Formatsperren zu verhindern
- Echtzeitdaten
  - VoIP Telefonie (Video oder Audio), Fax
  - Telekommunikationsüberwachung (Verbindungs-/Inhaltsdaten)
- transformierte Daten
  - „analog hole“
  - Ausdrucke einscannen / fotografieren
  - Datenformate wandeln (z.B. Text- in Bilddaten)
- Abfälle
  - ausrangierte Datenträger
  - Unterlagen, Papiermüll

Lücken für DLP

- „frische“ Daten ohne Signatur
  - neu erstellte Datenobjekte
  - maximal durch Formatsperren zu verhindern
- Echtzeitdaten
  - VoIP Telefonie (Video oder Audio), Fax
  - Telekommunikationsüberwachung (Verbindungs-/Inhaltsdaten)
- transformierte Daten
  - „analog hole“
  - Ausdrucke einscannen / fotografieren
  - Datenformate wandeln (z.B. Text- in Bilddaten)
- Abfälle
  - ausrangierte Datenträger
  - Unterlagen, Papiermüll

Lücken für DLP

- „frische“ Daten ohne Signatur
  - neu erstellte Datenobjekte
  - maximal durch Formatsperren zu verhindern
- Echtzeitdaten
  - VoIP Telefonie (Video oder Audio), Fax
  - Telekommunikationsüberwachung (Verbindungs-/Inhaltsdaten)
- transformierte Daten
  - „analog hole“
  - Ausdrucke einscannen / fotografieren
  - Datenformate wandeln (z.B. Text- in Bilddaten)
- Abfälle
  - ausrangierte Datenträger
  - Unterlagen, Papiermüll

Telekommunikationsüberwachung

- Telekommunikationsüberwachung / *lawful interception*
  - Schnittstellen fester Bestandteil von Mobilfunk
  - vorhanden bei >1000 E-Mail-Konten/Kunden (ISP) $\wedge$ >10000 E-Mail-Konten (Firmen) (DE)
- Schnittstellen sind potentielles Datenleck
  - große ISPs $\longleftarrow$ mitgefangen, mitgehangen
  - TKÜ legt Kopien der Daten an
  - abgefangene Daten vergrößern DaR Bereich
  - Verbindungsdaten geben Kontakte preis
- TKÜ muß nicht unbedingt aktiv sein
  - ändert nichts am Problem
  - *National Security Letters* (NSA/USA)

Telekommunikationsüberwachung

- Telekommunikationsüberwachung / *lawful interception*
  - Schnittstellen fester Bestandteil von Mobilfunk
  - vorhanden bei >1000 E-Mail-Konten/Kunden (ISP) $\wedge$ >10000 E-Mail-Konten (Firmen) (DE)
- Schnittstellen sind potentielles Datenleck
  - große ISPs $\longleftarrow$ mitgefangen, mitgehangen
  - TKÜ legt Kopien der Daten an
  - abgefangene Daten vergrößern DaR Bereich
  - Verbindungsdaten geben Kontakte preis
- TKÜ muß nicht unbedingt aktiv sein
  - ändert nichts am Problem
  - *National Security Letters* (NSA/USA)

Telekommunikationsüberwachung

- Telekommunikationsüberwachung / *lawful interception*
  - Schnittstellen fester Bestandteil von Mobilfunk
  - vorhanden bei >1000 E-Mail-Konten/Kunden (ISP) $\wedge$ >10000 E-Mail-Konten (Firmen) (DE)
- Schnittstellen sind potentielles Datenleck
  - große ISPs $\longleftarrow$ mitgefangen, mitgehangen
  - TKÜ legt Kopien der Daten an
  - abgefangene Daten vergrößern DaR Bereich
  - Verbindungsdaten geben Kontakte preis
- TKÜ muß nicht unbedingt aktiv sein
  - ändert nichts am Problem
  - *National Security Letters* (NSA/USA)

Telekommunikationsüberwachung

- Telekommunikationsüberwachung / *lawful interception*
  - Schnittstellen fester Bestandteil von Mobilfunk
  - vorhanden bei >1000 E-Mail-Konten/Kunden (ISP) $\wedge$ >10000 E-Mail-Konten (Firmen) (DE)
- Schnittstellen sind potentielles Datenleck
  - große ISPs $\longleftarrow$ mitgefangen, mitgehangen
  - TKÜ legt Kopien der Daten an
  - abgefangene Daten vergrößern DaR Bereich
  - Verbindungsdaten geben Kontakte preis
- TKÜ muß nicht unbedingt aktiv sein
  - ändert nichts am Problem
  - *National Security Letters* (NSA/USA)

Datenträger

- DLP sieht meist nur Netzwerk und Endgeräte
- („unlizensierte“) Datenträger können Lücke sein
  - nur DLP Agent oder
  - Betriebssystem können kontrollieren
- USB Storage Geräte sehr verbreitet
  - (Smart)phones,
  - Kameras,
  - eBook Reader, . . .
- DLP kann nur in die digitale Welt schauen
- Datenträger immer **fachgerecht** löschen/entsorgen

Datenträger

- DLP sieht meist nur Netzwerk und Endgeräte
- („unlizensierte“) Datenträger können Lücke sein
  - nur DLP Agent oder
  - Betriebssystem können kontrollieren
- USB Storage Geräte sehr verbreitet
  - (Smart)phones,
  - Kameras,
  - eBook Reader, . . .
- DLP kann nur in die digitale Welt schauen
- Datenträger immer **fachgerecht** löschen/entsorgen

Datenträger

- DLP sieht meist nur Netzwerk und Endgeräte
- („unlizensierte“) Datenträger können Lücke sein
  - nur DLP Agent oder
  - Betriebssystem können kontrollieren
- USB Storage Geräte sehr verbreitet
  - (Smart)phones,
  - Kameras,
  - eBook Reader, . . .
- DLP kann nur in die digitale Welt schauen
- Datenträger immer **fachgerecht** löschen/entsorgen

Datenträger

- DLP sieht meist nur Netzwerk und Endgeräte
- („unlizensierte“) Datenträger können Lücke sein
  - nur DLP Agent oder
  - Betriebssystem können kontrollieren
- USB Storage Geräte sehr verbreitet
  - (Smart)phones,
  - Kameras,
  - eBook Reader, . . .
- DLP kann nur in die digitale Welt schauen
- Datenträger immer **fachgerecht** löschen/entsorgen

Datenträger

- DLP sieht meist nur Netzwerk und Endgeräte
- („unlizensierte“) Datenträger können Lücke sein
  - nur DLP Agent oder
  - Betriebssystem können kontrollieren
- USB Storage Geräte sehr verbreitet
  - (Smart)phones,
  - Kameras,
  - eBook Reader, . . .
- DLP kann nur in die digitale Welt schauen
- Datenträger immer **fachgerecht** löschen/entsorgen

Datenträger

- DLP sieht meist nur Netzwerk und Endgeräte
- („unlizensierte“) Datenträger können Lücke sein
  - nur DLP Agent oder
  - Betriebssystem können kontrollieren
- USB Storage Geräte sehr verbreitet
  - (Smart)phones,
  - Kameras,
  - eBook Reader, . . .
- DLP kann nur in die digitale Welt schauen
- Datenträger immer **fachgerecht** löschen/entsorgen

Bring Your Own Device (BYOD)

- „neues“ „Konzept“ für „Büroarbeitsgeräte“
  - funktioniert für Schreibutensilien oder Kaffee
  - funktioniert nur bedingt für digitale Geräte
  - primär gedacht für Hardware-Händler
- BYOD ohne Vorgaben $\neq$ Informationssicherheit
  - DLP Agent verfügbar?
  - Schnittstellen?
  - Härtung?
- BYOD können evtl. in DLP integriert werden. . .
  But Your Operation Depends

Bring Your Own Device (BYOD)

- „neues“ „Konzept“ für „Büroarbeitsgeräte“
  - funktioniert für Schreibutensilien oder Kaffee
  - funktioniert nur bedingt für digitale Geräte
  - primär gedacht für Hardware-Händler
- BYOD ohne Vorgaben $\neq$ Informationssicherheit
  - DLP Agent verfügbar?
  - Schnittstellen?
  - Härtung?
- BYOD können evtl. in DLP integriert werden. . .
  But Your Operation Depends

Bring Your Own Device (BYOD)

- „neues“ „Konzept“ für „Büroarbeitsgeräte“
  - funktioniert für Schreibutensilien oder Kaffee
  - funktioniert nur bedingt für digitale Geräte
  - primär gedacht für Hardware-Händler
- BYOD ohne Vorgaben $\neq$ Informationssicherheit
  - DLP Agent verfügbar?
  - Schnittstellen?
  - Härtung?
- BYOD können evtl. in DLP integriert werden. . .
  But Your Operation Depends

Bring Your Own Device (BYOD)

- „neues“ „Konzept“ für „Büroarbeitsgeräte“
  - funktioniert für Schreibutensilien oder Kaffee
  - funktioniert nur bedingt für digitale Geräte
  - primär gedacht für Hardware-Händler
- BYOD ohne Vorgaben $\neq$ Informationssicherheit
  - DLP Agent verfügbar?
  - Schnittstellen?
  - Härtung?
- BYOD können evtl. in DLP integriert werden. . .
  But Your Operation Depends

DLP Implementationen

- Application Layer Gateways (Proxies)
- Antivirus-Produkte
- Data Loss Prevention Suites
- Firewalls
- MyDLP
- OpenDLP

Noch Fragen?

Über dieses Dokument

- Autor: René Pfeiffer
- Erstellt mit LaTeX und LaTeX Beamer Class
- Dokumentensammlung unter
  http://web.luchs.at/information/docs.php