GO OUT IT-SECURITY HOSTING

klubschule MIGROS

insinova

interway net intelligence

SKYBOW

IT - Security Forum #4

Warum und wie Daten verschlüsselt werden – am Beispiel von Max P.

Jens Albrecht

Dipl. El. Ing. FH

CEO **insinova ag**

jens.albrecht@insinova.ch

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

insinova

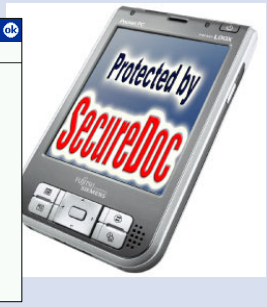
interway net intelligence

SKYBOW

IT - Security Forum #4

7:30 Termin auf PDA checken

- Max P. macht sich auf zu einem Kundentermin. Er überprüft die Adresse und die Zeit auf seinem PDA – denn sicher ist sicher.
- Sein PDA ist passwortgeschützt und die Dateien sind verschlüsselt inkl. SD-Card.
- Die beste Sicherheit vor seinen kleinen Kindern – und vor weiteren Gefahren.



GO OUT IT-SECURITY HOSTING

klubschule MIGROS

inOnova

interway net intelligence

SKYBOW

IT - Security Forum #4

9:00 Besprechung beim Kunden

- Max P. startet sein Notebook und bespricht das aktuelle Konzept mit dem Kunden.
- Ohne Pre-Boot-Authentifikation startet das Notebook nicht. Zur Authentifikation benutzt er mIDentity und die PIN, mit dem er sich auch an der Windows Domäne und Citrix anmelden kann.

3

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

inOnova

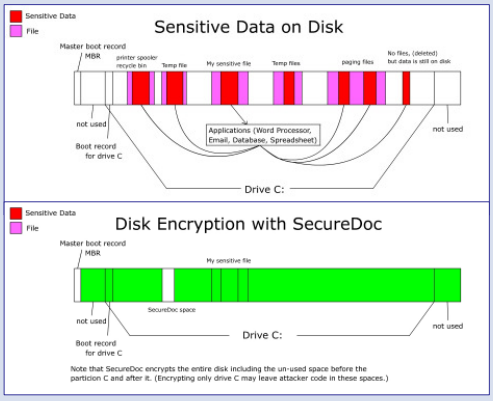
interway net intelligence

SKYBOW

IT - Security Forum #4

9:00 Besprechung beim Kunden

- Max P. muss sich um die Verschlüsselung seiner Daten **nicht kümmern**, denn die gesamte Festplatte ist jederzeit verschlüsselt. Ebenfalls sein 4 GB Memory Stick.
- Davon merkt er nichts, **SecureDoc** arbeitet transparent.



SecureDoc

4

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

inOnova

interway net intelligence

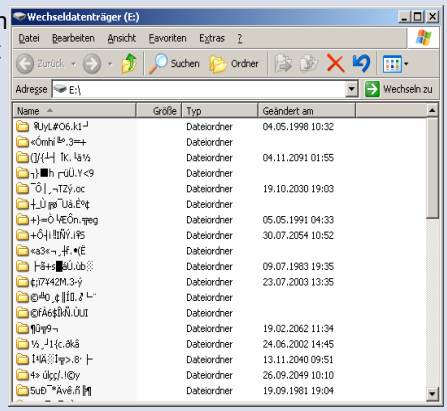
SKYBOW

IT - Security Forum #4

11:30 Lunch mit CFO

SecureDoc

- Max P. trifft sich zum Lunch mit dem CFO seines Kunden. Aktuelle Pläne zur Übernahme eines Konkurrenten werden besprochen.
- Das überarbeitete Konzept wird dem CFO auf dem Notebook präsentiert und zur Übergabe auf seinen Memory Stick kopiert.
- Essen war gut, Konzept auch…
- **Uppps…**der CFO hat seinen Memory Stick im Restaurant liegen lassen.
- Glücklicherweise kann der **neugierige Kellner** mit den Daten nichts anfangen.
- Denn der Stick ist ja verschlüsselt ☺.



5

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

inOnova

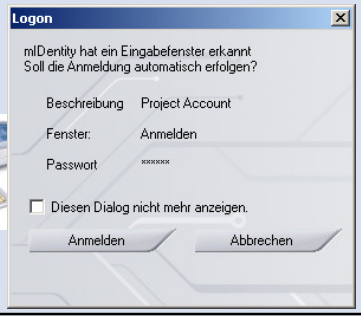
interway net intelligence

SKYBOW

IT - Security Forum #4

14:00 Ankunft im Büro

- Max P. benutzt mIDentity auch für den Gebäudezutritt und die Zeiterfassung (LEGIC).
- Danach startet er sein Notebook und meldet sich mit mIDentity und seiner **PIN** an der Windows Domäne an.
- Für seine weitere Arbeit benötigt Max P. einige Preis- und Liefer-Informationen vom Web-Portal eines Distributors.
- Glücklicherweise muss er sich die verlangten Passwörter **weder merken noch aufschreiben**: Sie sind alle sicher auf dem mIDentity hinterlegt. mIDentity meldet Max P. sogar automatisch an den Applikationen an!



6

15:15 Daten sichern

- Max P. hat nun das vertrauliche Übernahmekonzept fertig gestellt und speichert die Dateien auf seinem Home-Verzeichnis auf dem Firmen-Server ab.
- **Komisches Gefühl?** Nein, denn er verwendet die Container-Verschlüsselung. Nur er kann mit mIDentity und dem richtigen PIN den Container öffnen.
- Die **Administratoren** sehen lediglich eine grosse Datei, die sie ganz normal sichern können.

15:30 Dokumente signieren

- Max P. hat zwischenzeitlich einige Dokumente empfangen, die er digital signieren und weiterleiten muss.
- Dazu verwendet er mIDentity und signiert mit seinem **Signatur-Zertifikat** die erhaltenen PDF-Dokumente, speichert diese und mailt sie so weiter.

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

inetnova

interway net intelligence

SKYBOW

IT - Security Forum #4

15:50-19:10 Arbeit ausser Hause

- Max P. fährt zu seinem Vertriebspartner, um gemeinsam am neusten Verkaufskonzept zu arbeiten. Die benötigten Dateien befinden sich im sicheren Container auf dem mIDentity.
- Max P. kann **von fremden Computern** nach der PIN-Eingabe auf seinen Container auf den mIDentity zugreifen, weil **keine Software** für die Container-Funktion auf den PCs installiert werden muss.
- 19:10: Das Verkaufskonzept ist beinahe fertig. Max P. zieht seinen mIDentity vom PC ab und fährt nach Hause. Es befinden sich keine Kopien der Dateien auf dem PC beim Vertriebspartners.

9

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

inetnova

interway net intelligence

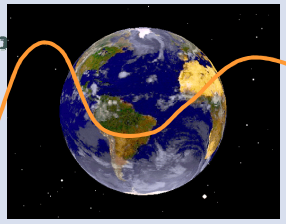
SKYBOW

IT - Security Forum #4

21:45 Arbeit zu Hause

- Die Kinder sind im Bett und Max‘s Frau sieht Fern.
- Max P. kann es nicht lassen und bearbeitet einige Bilder der neuen Produkte an seinem Heim-PC, weil er dort einen 20“-CAD-Monitor hat. **Raten Sie mal:** Wo liegen die Bilder der neuen Produkte?
- Max P. fällt ein, dass er morgen den ganzen Tag ausser Haus ist und die Marketing-Abteilung die Bilder braucht.
- Max P. startet den **installationslosen** Firefox-Browser als SSL-VPN Client von seinem mIDentity. Er benutzt das **Client-Zertifikat** (ebenfalls auf dem mIDentity) für die sichere Verbindung und überträgt die bearbeiteten Bilder in das Marketing-Verzeichnis.

Firefox rediscover the web



10

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

insinova

interway net intelligence

SKYBOW

IT - Security Forum #4

Zusammenfassung

- **SecureDoc Disk Encryption:**
  - für Notebooks, PCs, PDAs.
  - Transparent für die Benutzer.
  - Einfachster Roll-Out und Verwaltung.
  - Viele Token werden unterstützt.

- **KOBIL mIDentity:**
  - Anmelden an der Windows Domäne und an Citrix
  - **Sicherer Daten-Safe auf mIDentity, lokaler Festplatte, Netzwerk.**
  - **Single Sign-On Funktion mit mobilem Passwort-Safe.**
  - Signieren und Verschlüsseln von Dokumenten und E-Mails.
  - SSL-VPN Authentifikation mit Zertifikat.

  = funktioniert ohne Software-Installation am Client

11

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

insinova

interway net intelligence

SKYBOW

IT - Security Forum #4

insinova - Ihr Partner für Sicherheit

- **Ausgezeichnetes Know-how:**
  Von der Leitlinie, über Konzepte, bis hin zur Implementierung.

- **Starke Partnerschaften:**
  WinMagic, KOBIL, neupart, SafeNet, Totemo

- **Tolle Referenzen:**
  AWD: SecureDoc Festplattenverschlüsselung
  BIT: Festplattenverschlüsselung mit Smart Cards
  BKW FMB Energie: Einmalpasswort-System zur Authentifikation
  Cendres & Métaux: Einmalpasswort-System zur Authentifikation
  DSB Kanton Zürich: Festplattenverschlüsselung
  Kanton Aargau: Festplattenverschlüsselung mit Smart Cards
  Kanton Genf: Festplattenverschlüsselung mit Token
  Rothschild Bank: Einmalpasswort-System zur Authentifikation
  SUVA: PKI mit Smart Cards für 2'500 Benutzer auf 22 Agenturen
  SUVA: Festplattenverschlüsselung für 865 Benutzer

12