Bestands- en schijfencryptie

Een onderzoek naar de toepasbaarheid binnen SURFnet bv.

Amsterdam, juli 2005

Marya Steenman en Thijs van den Berg

SURFnet Hoogwaardig internet voor hoger onderwijs en onderzoek

Opdracht

- Onderzoek naar verschillende manieren van bestands– en schijfencryptie voor desktops/laptops

Code voor Informatie Beveiliging

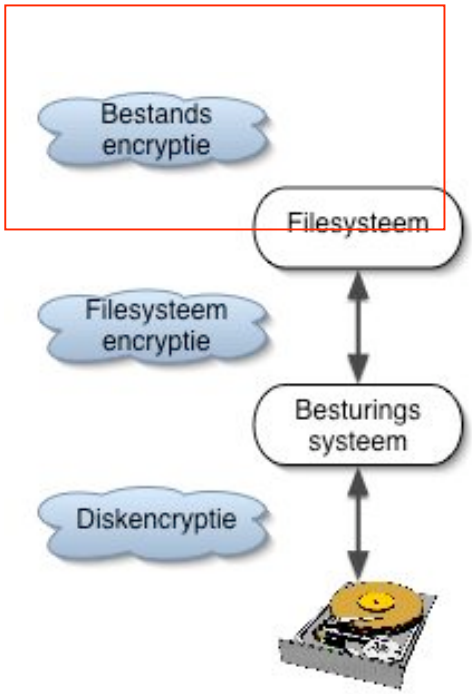
- Discussie wetgeving

Methoden

- Bestandsencryptie
- Filesysteemencryptie
- Schijfencryptie

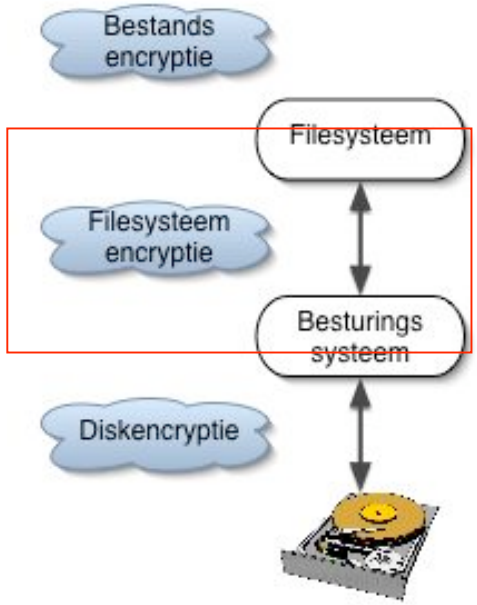
Bestandsencryptie

- Software
- Losse bestanden
- Containers
- Gebruiker zelf verantwoordelijk



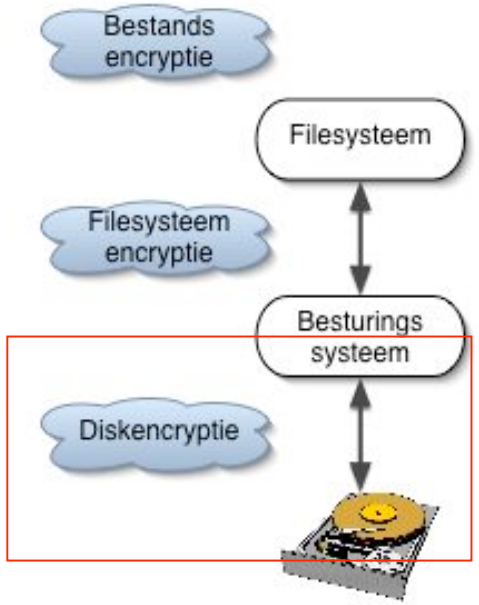
Filesysteemencryptie

- Geen standaard filesysteem met encryptie
- Gebruiker deels zelf verantwoordelijk
- Bij elk OS anders
- Encryptie/decr. transparant



Schijfencryptie

- Gebruiker heeft geen verantwoordelijkheid
- Encryptie/decr. transparant
- Read/write
- Alle data geëncrypt
- Software/hardware
- Pre-boot



Risico's

- Sleutels en wachtwoorden
  - Verloren gaan
  - Te kort wachtwoord
- Verantwoordelijkheid
- Tijdelijke bestanden

Aandachtspunten

- Schaalbaarheid
- Performance
- Backup
- Schijfbeheer
- Fileserver

Bedrijfsanalyse

- Gebruikersgroepen
  - Hoog aantal technische gebruikers
  - Bekend met encryptie
- Vertrouwelijke gegevens
  - Personeelsgegevens
  - Wachtwoorden
  - Aanbestedingen
  - SURFnet-CERT incidenten
- Platformen
  - Desktop/laptop met Windows XP Pro.

Productselectie

Op basis van:

- Ondersteuning Windows XP Pro.
- Verschillende manieren van encryptie
- Mix commercieel en open-source
- Zeker mate van volwassenheid/ bekendheid
- Hedendaagse encryptiestandaarden

Productselectie

Veel verschillende producten beschikbaar.

Geselecteerde producten:

- AxCrypt
- TrueCrypt
- PGP Desktop
- Encrypted File System
- CompuSec
- DriveCrypt Plus Pack

Onderzoek

- Performance
- Gebruiksgemak
- Recovery
- Veiligheid
- Praktische aspecten

Resultaten(1)

- Performance
  - Performanceverlies minimaal
  - Bij bestandsencryptie is encryptieduur van bestanden groter dan 10 MB storend
- Gebruiksgemak
  - In het algemeen goed
  - Bestandsencryptie veel gebruikers interactie
- Recovery
  - Bij EFS en schijfencryptie over nagedacht

Resultaten(2)

- Veiligheid
  - Containers risicovol
  - Meerdere gebruikers
- Praktische aspecten
  - Hibernation
  - Backup

Conclusie

- Veel verschillende soorten producten geschikt voor verschillende situaties
- Schijfencryptie biedt twee grote voordelen tov de andere methoden:
  - Alle data wordt geëncrypt
  - Geen gebruikersinteractie/ Transparantie

Aanbeveling

- Schijfencryptie
  - CompuSec (www.ce-infosys.com)
- Als aanvulling bestandsencryptie
  - AxCrypt (axcrypt.sourceforge.net)

Vragen