Storage Security

IT- Sicherheit von innen nach außen

Klaus Kupfer
Technical Manager Central Europe
kkupfer@decru.com

DECRU
SECURING NETWORKED STORAGE™

Agenda

- Warum Speichersicherheit
- Bedrohungen für Speichernetzwerke
- Decru Lösung
  - NAS
  - SAN & Tape
  - Datenbanken
  - DCS
- Lifetime Key Management
- Zusammenfassung
- Über Decru

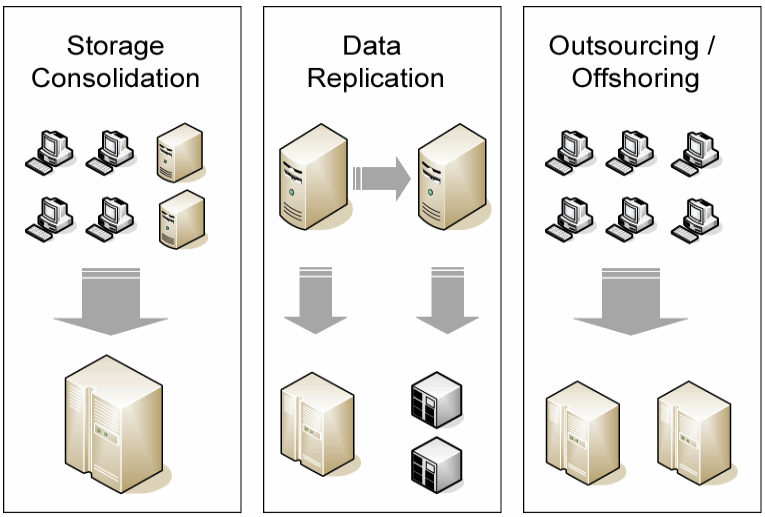
DECRU
SECURING NETWORKED STORAGE™

Wachsende Anforderung für Speichersicherheit

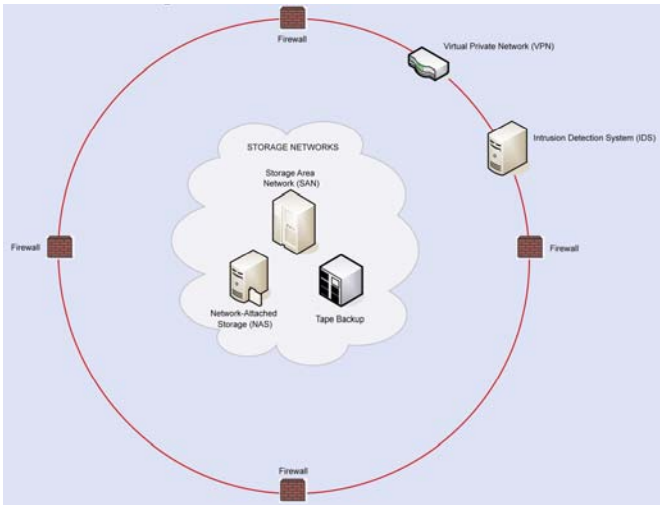
- Unternehmen speichern Terabytes von sensiblen Daten in Speichernetzwerken
- Information Lifecycle Management
- Disaster Recovery
- Replikation
- Heutige Sicherheitsmodelle fokussieren rein auf die Perimeterabsicherung
  - Daten innerhalb des Unternehmens werden nicht betrachtet
- Data in transit vs. data at rest

DECRU
SECURING NETWORKED STORAGE™

Gängige IT Strategien vergrößern das Risiko

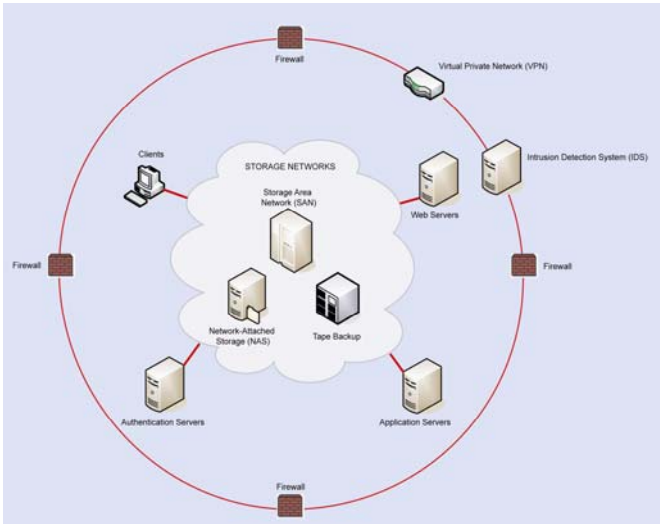


Der traditionelle Security Ansatz: Schutz des Storage Netzwerks vor externen/ Angriffen



DECRU
SECURING NETWORKED STORAGE™

50-80% aller Attacken haben ihren Ursprung innerhalb der Firewall Quelle: IDC and KPMG



•67% aller Unternehmen meldeten interne Sicherheitsverletzungen innerhalb der letzten 12 Monate
•Durchschnittlicher Schaden jeder Verletzung war $2.7 million

Quelle: FBI/Computer Security Institute

DECRU
SECURING NETWORKED STORAGE™

Storage in Gefahr

Konsolidierung & Replikation gefährden Terabyte

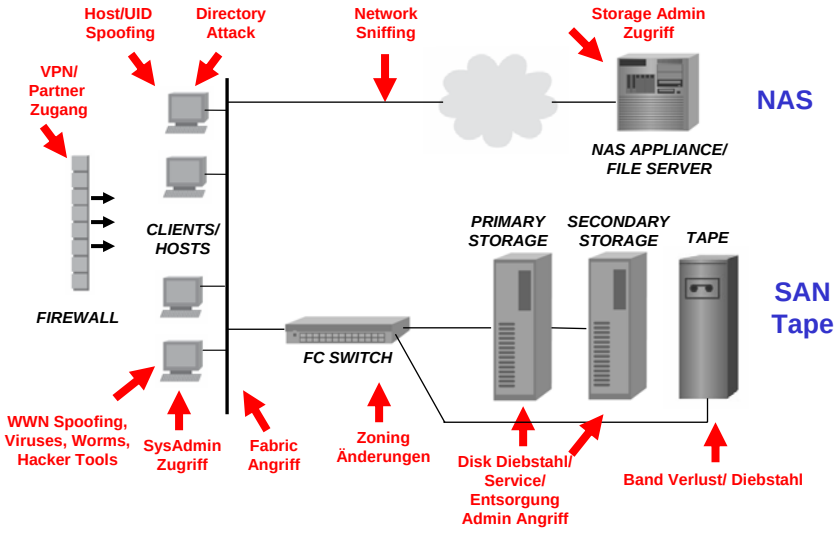
- Feb 2003 – Visa, Amex, Mastercard
  - Hacker hackt 8 Millionen Kreditkarten Konten
- Jan 2004 – MTC
  - Kundendatenbank von Russlands größtem Mobilfunk Anbieter gestohlen
- Feb, Mai 2004 – Microsoft and Cisco
  - Source Code gestohlen
- 2004 – Yahoo
  - Daten von 4,5 Mil. Kunden gestohlen
  - Folgekosten $22 Mil. für Kundenentschädigung
  - Geschätzte $338 Mil. um verlorene Kunden zurückzugewinnen ($75/Kunde)
- Juli 2004 – Los Alamos Nuclear Lab
  - Zwei Festplatten aus dem Labor werden vermisst. Aus diesem Grund muss die ganze Anlage abgeschaltet werden.
- Sept 2004 – Klage auf $50 Mil.
  - Helpdesk Angestellter stahl zehntausende Kundendaten von Kreditdatenbank

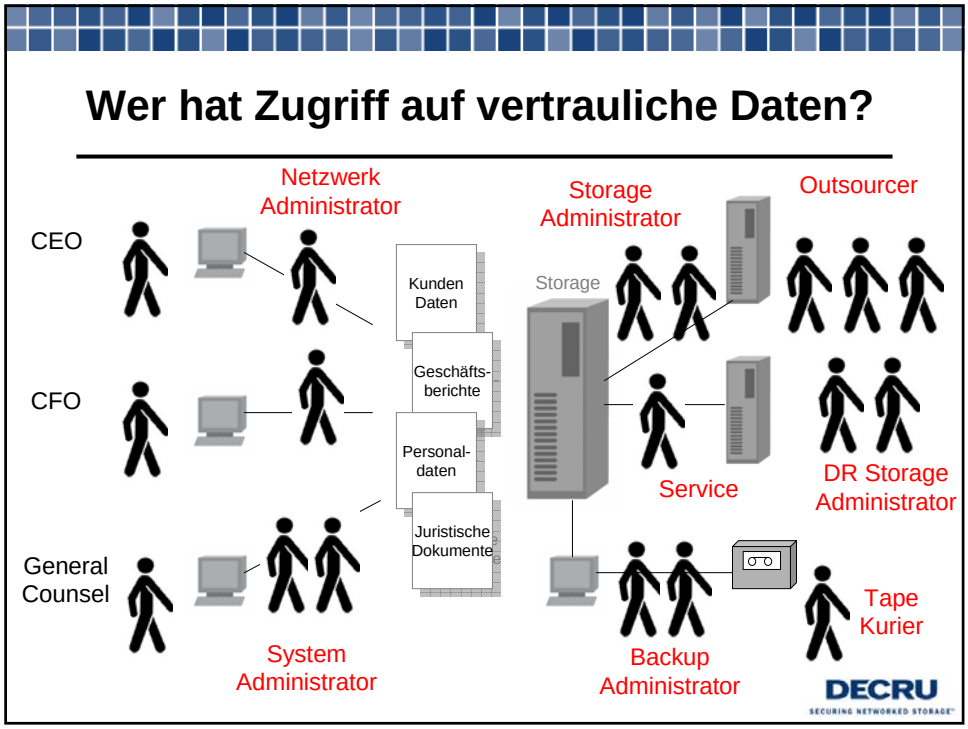
Februar, 2005
Bank of America "verlegt" Bänder mit Kontodaten ihrer Kunden u.a. US-Senatoren

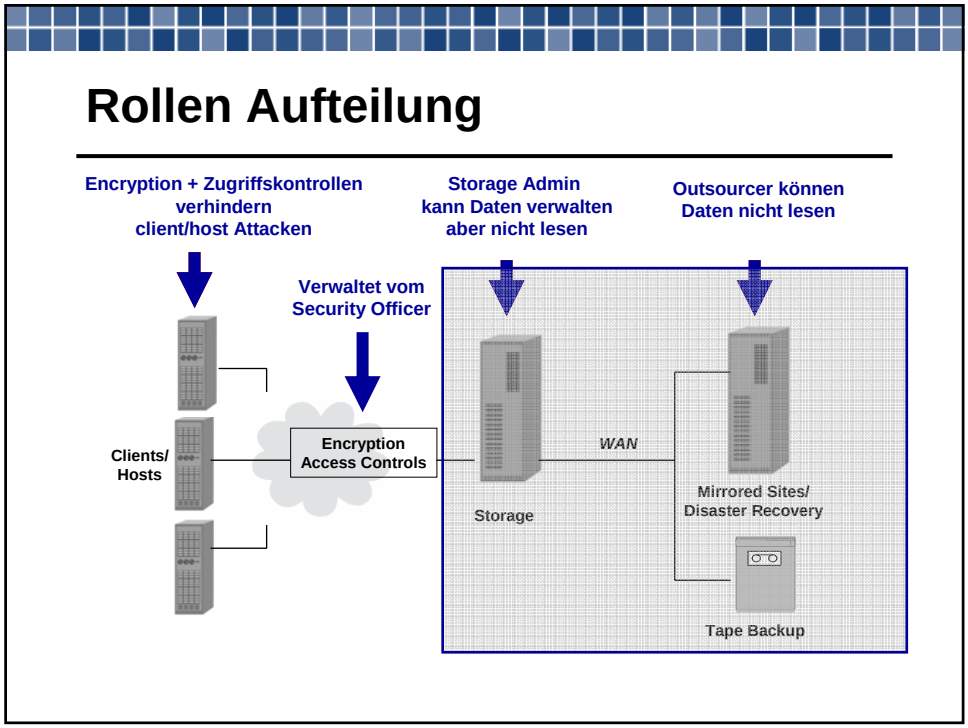
DECRU
SECURING NETWORKED STORAGE

Bedrohungen für Datenspeicher

Traditionelle Perimeterabsicherung bietet wenig Schutz für die gespeicherten Daten




Wer hat Zugriff auf vertrauliche Daten?
Netzwerk Administrator
Storage Administrator
Outsourcer
CEO
CFO
General Counsel
Kunden Daten
Geschäfts-berichte
Personal-daten
Juristische Dokumente
Storage
Service
DR Storage Administrator
Tape Kurier
System Administrator
Backup Administrator
DECRU


Rollen Aufteilung
Encryption + Zugriffskontrollen verhindern client/host Attacken
Storage Admin kann Daten verwalten aber nicht lesen
Outsourcer können Daten nicht lesen
Verwaltet vom Security Officer
Clients/ Hosts
Encryption Access Controls
WAN
Storage
Mirrored Sites/ Disaster Recovery
Tape Backup

Decru Lösung

DECRU
SECURING NETWORKED STORAGE™

Decru DataFort™

Storage Security Appliances

- **Zentrale Funktionalitäten der Decru Lösung:**
  - **Authentifizierung**
  - **Datenabsicherung (Verschlüsselung)**
  - **Auditing**
- **Einheitliche Sicherheitsplattform für alle Speicher Umgebungen**
- **Schützt vertrauliche Daten vor internen und externen Bedrohungen**
- **Rollen Separierung**
  - Separiert den Datennutzer vom Datenadministrator
- **Erhöht Nutzung vorhandener Infrastruktur**
- **Macht die Daten sicher, nicht die Infrastruktur**
- **Hilft bei der Einhaltung gesetzlicher und sonstiger Regelungen**
  - Versicherung, dass Bedienerfehler, nicht authorisierter Adminstrator Zugriff oder böswillige Attacken die Sicherheit der Daten nicht beeinträchtigt
- **Kompatibilitätstest mit allen führenden Storage, Switch und OS Plattformen**
  - Transparente Integration in bestehende Umgebungen

InfoWorld
Rating: Deploy
Top 10 lab score: 8.4/10
Security: 10/10

eWEEK
THE ENTERPRISE NEWSWEEKLY
Top 10 Products of 2004

DECRU
SECURING NETWORKED STORAGE™

Decru DataFort™

Einheitliche Plattform für Storage Security

	E-Series (NAS, DAS)	FC-Series (SAN, Tape)	T-Series (Tape)
Crypto HW	SEP	SEP	SEP
FIPS 140-2 L3	Yes	Yes	Yes
Encryption	AES-256	AES-256	AES-256
Key Mgmt	LKM	LKM	LKM
Administration	Web, CLI	Web, CLI	Web, CLI
Chassis	1U, 2U	1U, 2U	1U, 2U
Interconnect	GigE	2Gb FC	2Gb FC
Auth/ACL	DCS, IPsec, SSL, Kerberos	DCS, DHA, Port Locking	DCS, DHA, Port Locking

DECRU
SECURING NETWORKED STORAGE™

DataFort Features

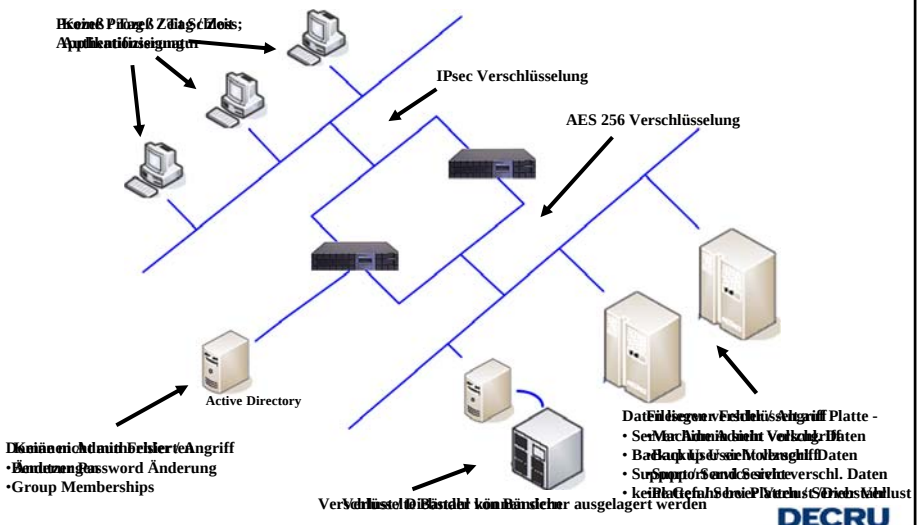
- **Starke AES-256 Verschlüsselung:**
  - Robust, volle FC bzw. GbE Geschwindigkeit, Verschlüsselung in Hardware. Einheitliche Infrastruktur für NAS, SAN iSCSI und Tape
- **Mandantenfähigkeit**:
  - Cryptainer™ Einheiten erlauben die sichere Konsolidierung von Daten verschiedener Gruppen auf eine gemeinsame Infrastruktur und verhindern den unauthorisierten Zugriff des Administrators
- **Authentifizierung und ACL's:**
  - DataFort bietet vielfältige Optionen für eine strenge Authentifizierung und granulare ACL's. Die Lösung integriert sich problemlos in existierende Verzeichnisdienste
- **CryptoShred™:**
  - Alle lokalen und replizierten Kopien von Daten können auf einen Schlag gelöscht werden, indem einfach die Keys gelöscht werden.
- **Skalierbarkeit und Verfügbarkeit:**
  - DataFort Cluster skalieren bis zu 32 Knoten und unterstützen Hochverfügbarkeits- und disastertolerante Konfigurationen
- **Lifetime Key Management™ System:**
  - automatisiertes, zentralisiertes Key Management für Archivierung und Disaster Recovery
- **Kryptographisch signierte Log Dateien:**
  - Überwachen und dokumentieren Datenzugriff und Administrationsänderungen
- **Zertifizierung:**
  - FIPS 140-2 Level 3, Common Criteria EAL 4+

DECRU
SECURING NETWORKED STORAGE™

Decru E-Series

DECRU
SECURING NETWORKED STORAGE™

NAS Infrastruktur - Lösung

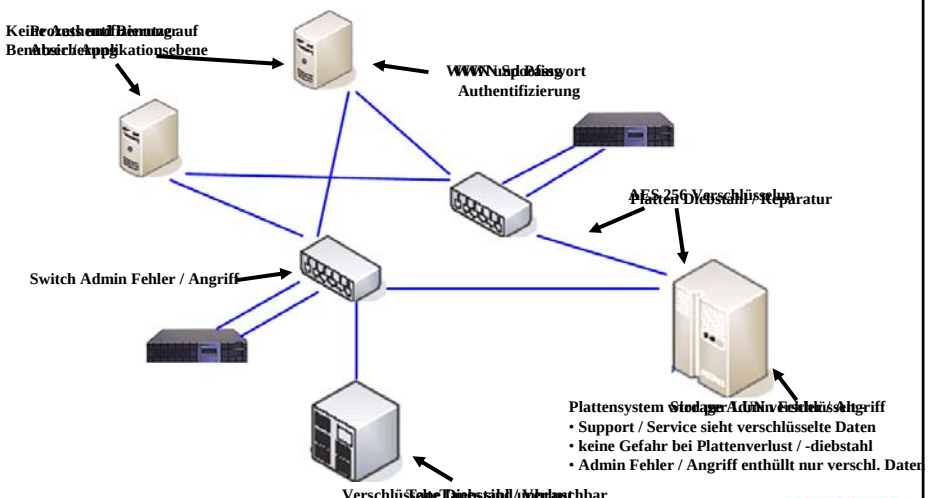


DECRU
SECURING NETWORKED STORAGE™

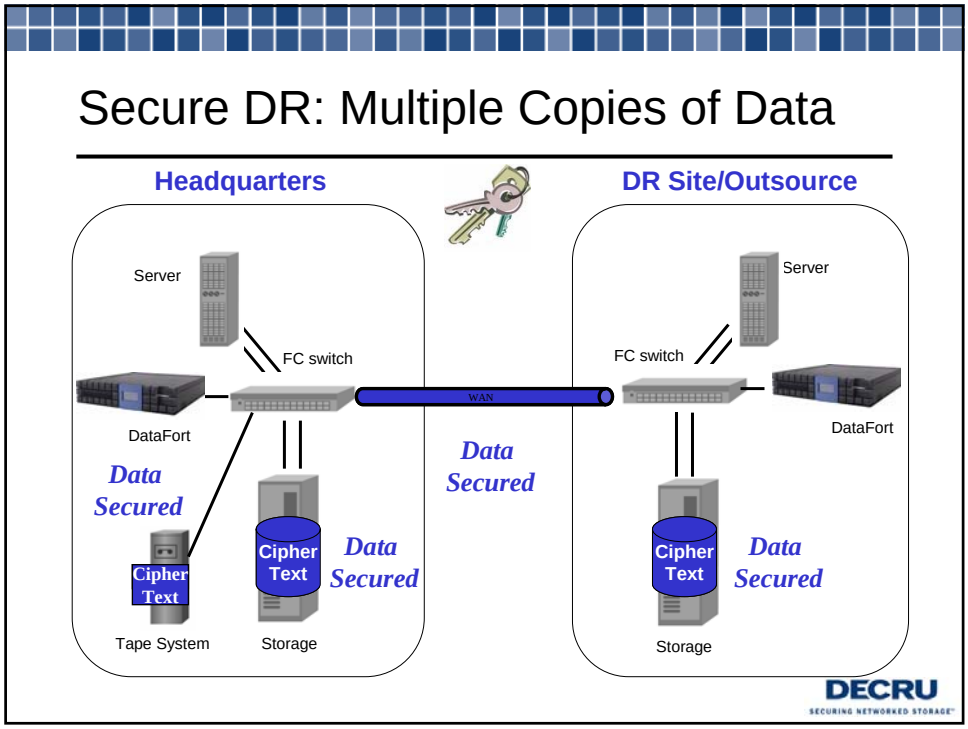
Decru FC/ T-Series

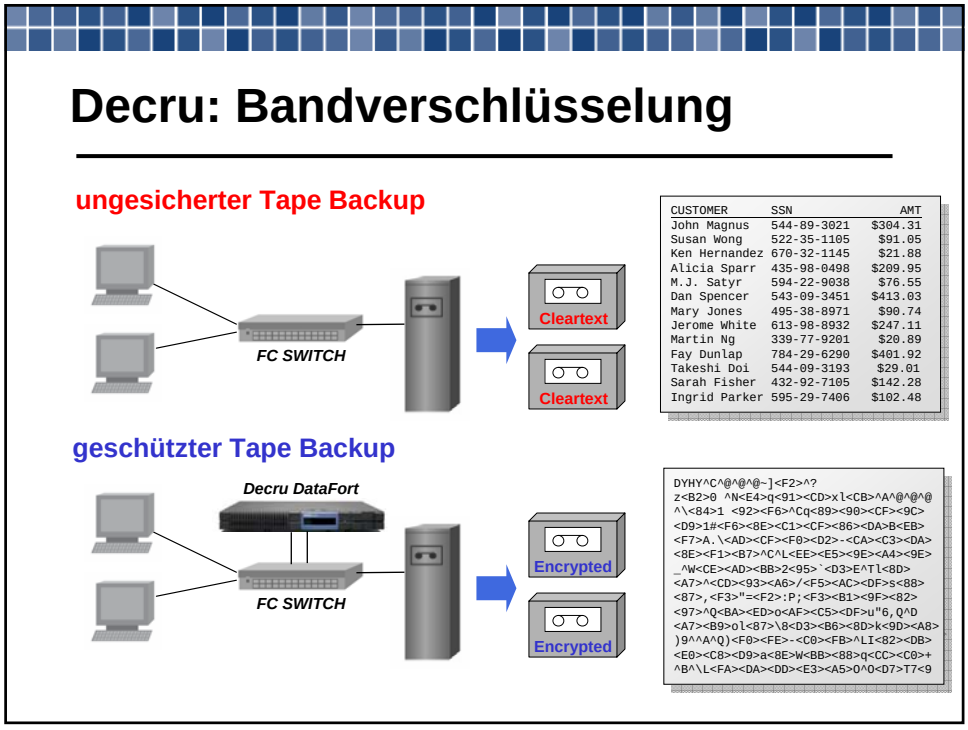
DECRU
SECURING NETWORKED STORAGE™

SAN Infrastruktur – Lösung



DECRU
SECURING NETWORKED STORAGE™


Secure DR: Multiple Copies of Data
Headquarters
DR Site/Outsource
Server
FC switch
DataFort
WAN
Data Secured
Cipher Text
Tape System
Storage
Server
FC switch
DataFort
Cipher Text
Storage
DECRU
SECURING NETWORKED STORAGE


Decru: Bandverschlüsselung
ungesicherter Tape Backup
FC SWITCH
Cleartext
Cleartext
CUSTOMER SSN AMT
John Magnus 544-89-3021 $304.31
Susan Wong 522-35-1105 $91.05
Ken Hernandez 670-32-1145 $21.88
Alicia Sparr 435-98-0498 $209.95
M.J. Satyr 594-22-9038 $76.55
Dan Spencer 543-09-3451 $413.03
Mary Jones 495-38-8971 $90.74
Jerome White 613-98-8932 $247.11
Martin Ng 339-77-9201 $20.89
Fay Dunlap 784-29-6290 $401.92
Takeshi Doi 544-09-3193 $29.01
Sarah Fisher 432-92-7105 $142.28
Ingrid Parker 595-29-7406 $102.48
geschützter Tape Backup
Decru DataFort
FC SWITCH
Encrypted
Encrypted

Decru Client Security Module

DECRU
SECURING NETWORKED STORAGE™

Decru Client Security Module (DCS)

Powerful Endpoint Security for Servers and Desktops

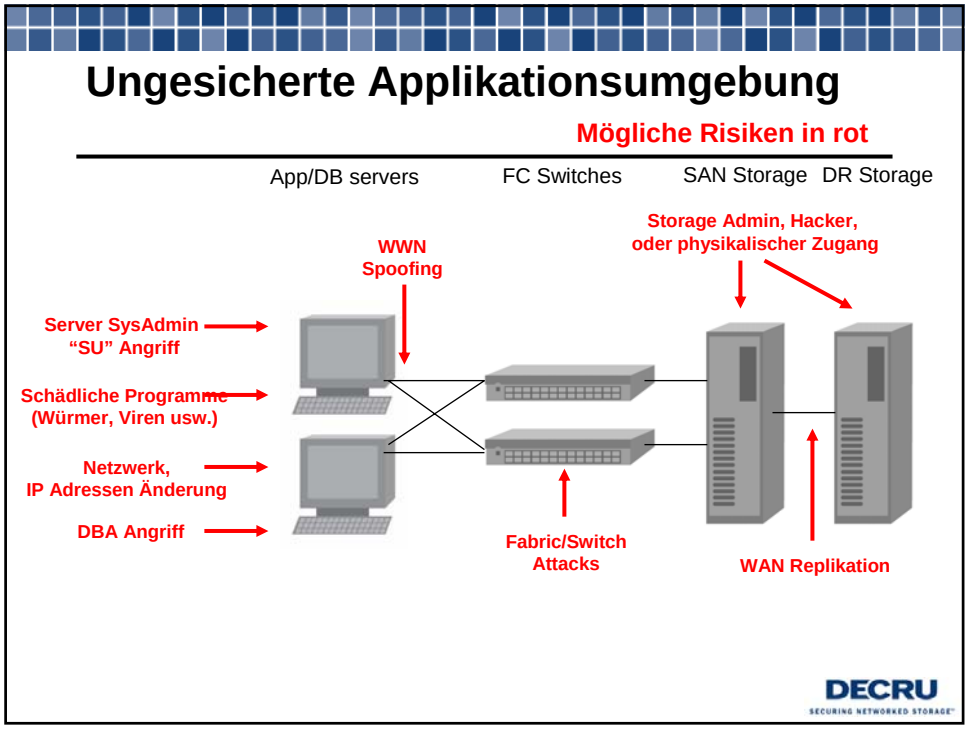
DETAILS

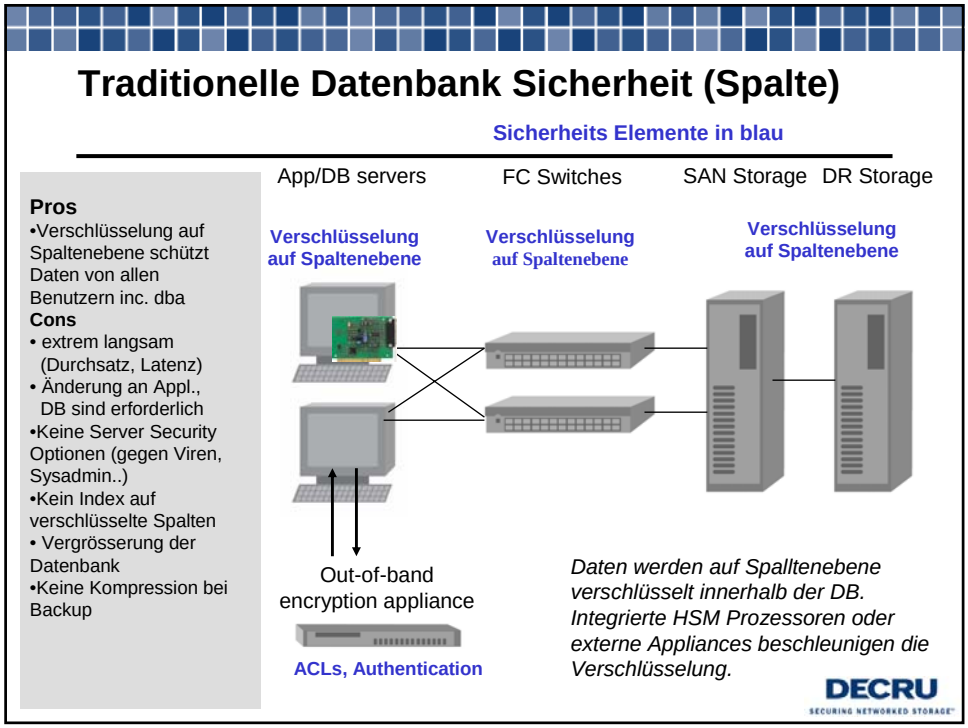
- *Unterstützt NAS, DAS, SAN, Tape, iSCSI*
- *OS support: Windows, Linux, Solaris (1H'05)*
- *Optionale Komponente- minimiert Management Kosten und Betriebsrisiko*
- *Unterstützt 2 Gbps FC, ohne jegliche Performance Beeinflussung*
- *Eng an DataFort gekoppelt; sichere HW dient als "Rettungsangker"*

DCS schützt Clients and Server mit Hilfe folgender Sicherheitsfeatures:

- **Granulare Policy Durchsetzung**: Benutzer, Administrator, Applikation, Zeit,Tag, Cryptainer
- **Applikations Whitelist**: Security Administrator bestimmt freigegebene Applikationen. Alle anderen Applikationen, Viren, Würmer, DLL's und Hacker Tools sind blockiert
- **Cryptographische Authentifizierung:** Applikationen sind cryptograpisch signiert und Maschinen auf denen DCS läuft authentifizieren sich am DataFort und verhindern damit spoofing

DECRU
SECURING NETWORKED STORAGE™


Ungesicherte Applikationsumgebung
Mögliche Risiken in rot
App/DB servers
FC Switches
SAN Storage
DR Storage
WWN Spoofing
Storage Admin, Hacker, oder physikalischer Zugang
Server SysAdmin "SU" Angriff
Schädliche Programme (Würmer, Viren usw.)
Netzwerk, IP Adressen Änderung
DBA Angriff
Fabric/Switch Attacks
WAN Replikation
DECRU

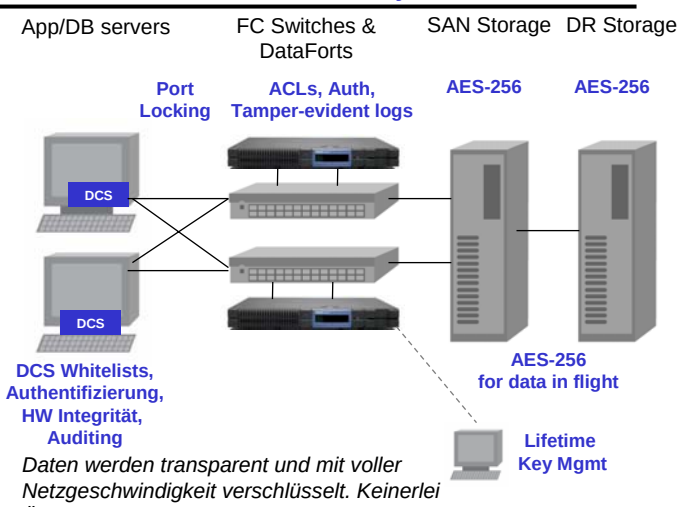

Traditionelle Datenbank Sicherheit (Spalte)
Sicherheits Elemente in blau
App/DB servers
FC Switches
SAN Storage
DR Storage
Pros
•Verschlüsselung auf Spaltenebene schützt Daten von allen Benutzern inc. dba
Cons
• extrem langsam (Durchsatz, Latenz)
• Änderung an Appl., DB sind erforderlich
•Keine Server Security Optionen (gegen Viren, Sysadmin..)
•Kein Index auf verschlüsselte Spalten
• Vergrösserung der Datenbank
•Keine Kompression bei Backup
Verschlüsselung auf Spaltenebene
Verschlüsselung auf Spaltenebene
Verschlüsselung auf Spaltenebene
Out-of-band encryption appliance
ACLs, Authentication
Daten werden auf Spalltenebene verschlüsselt innerhalb der DB. Integrierte HSM Prozessoren oder externe Appliances beschleunigen die Verschlüsselung.
DECRU

Decru Secure Application Environment

Security Elemente in blau

Pros
- Volle (2 Gbps) Performance
- Skalierbare Cluster
- Transparent für OS, Appl., DB
- Keine Appl. Änderungen
- Blockt Sysadmin
- App-level authent, ACLs, Integrität
- zentrales Key Mgmt.
- volle DB Funktionalität (indexing, calc…)
- Voller DR support

Cons
- nur DBA Audit



Daten werden transparent und mit voller Netzgeschwindigkeit verschlüsselt. Keinerlei Änderungen an der DB oder Appl. notwendig

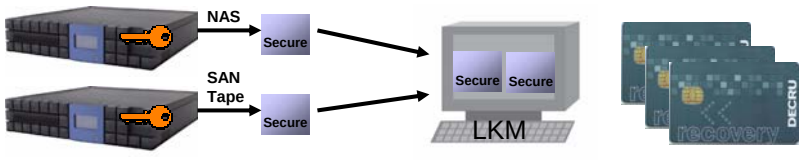
DECRU
SECURING NETWORKED STORAGE™

Decru Lifetime Key Management

DECRU
SECURING NETWORKED STORAGE™

Lifetime Key Management™

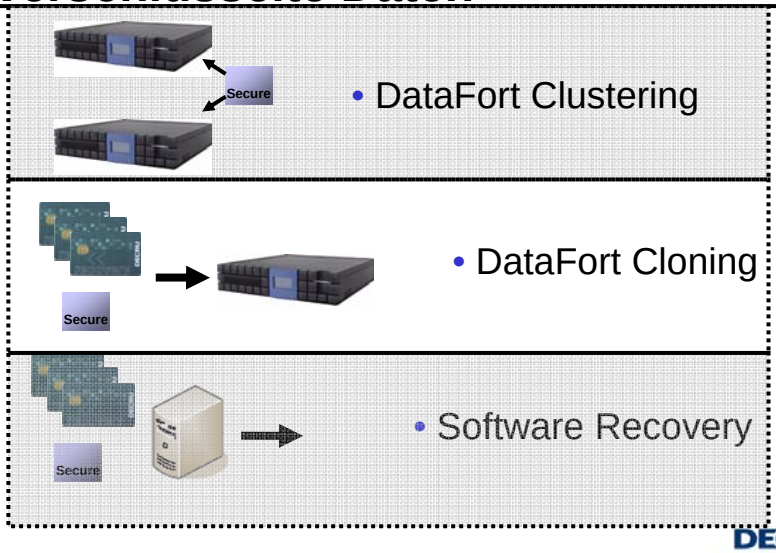
Sichere, automatisierte Key Management Infrastruktur



- DataFort verschlüsselt alle Keys, bevor sie den Storage Encryption Processor verlassen
- LKM automatisiert Backup/ Recovery und Archivierung von Verschlüsselungskeys
- LKM bietet zentrales Key Management für das gesamte Unternehmen
- Recovery Smart Cards werden für das Wiederherstellen oder Klonen eines DataForts benötigt: Quorum 2/5, 2/3 oder 3/5 Smart Cards

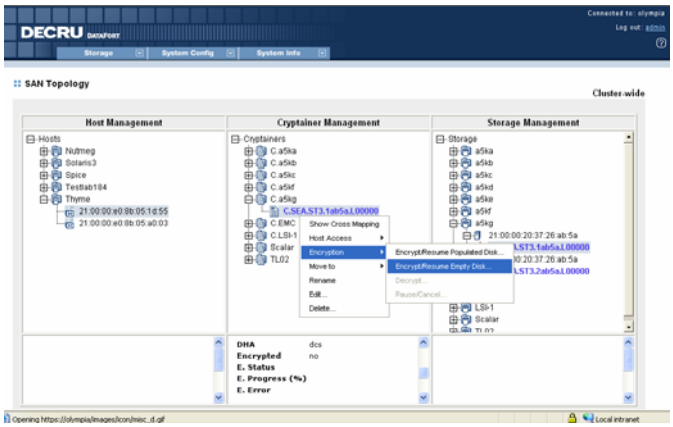
DECRU
SECURING NETWORKED STORAGE™

Hochverfügbarkeit für verschlüsselte Daten



DECRU
SECURING NETWORKED STORAGE™

DataFort: einfaches Management



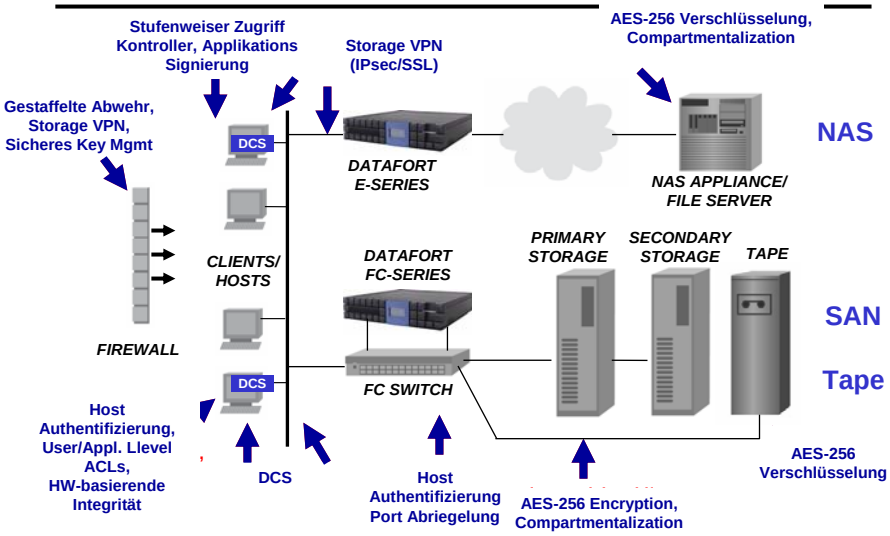
- Schnelle Installation
- Einzelnes GUI für Cluster-management
- CLI und Web-basierendes management
- Wizard hilft bei Konfiguration der Sicherheits-parameter
- Monitoring via SNMP
- Auditing, Syslog

DECRU
SECURING NETWORKED STORAGE™

Zusammenfassung

DECRU
SECURING NETWORKED STORAGE™

Bedrohung und Gegenmassnahmen



About Decru

- Gegründet 2001 mit dem Ziel das Problem der Speichersicherheit zu lösen
- HQ in Kalifornien mit Niederlassungen in London, München, Berlin und Amsterdam
- Gut finanziert von namhaften Investoren: mehr als 45 m $ Kapital
  - NEA, Benchmark, Greylock
- Geführt durch erfahrenes und erfolgreiches Management Team
- Nachgewiesene Implementationen bei:
  - Finanzdiensleistern, Regierung, Militär und kommerziellen Unternehmen -> weltweit

Nominated:
"Best Enterprise Security Product"

DECRU
SECURING NETWORKED STORAGE™


Vielen Dank
DECRU
SECURING NETWORKED STORAGE™