secunet

Sicherheit von SAN-Systemen

Christina Helbig
Seniorberater

>> **Agenda**

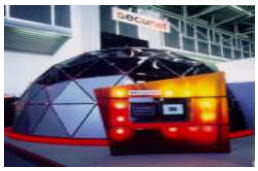
secunet

- Kurzinformation secunet
- Bedrohungen
- Kontroverse bzgl. SAN-Security
- Angriffe im Detail
- Sicheres SAN: Funktionen
- Sicheres SAN: Einordnung
- Sicheres SAN: Kosten

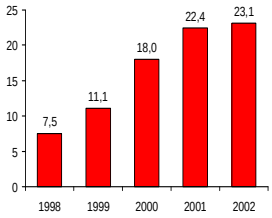
>> Kurzinformation secunet

secunet

- Gegründet im Dezember 1996
- Wurzeln im RWTÜV
- IPO: Nov 9, 1999
- 220 Mitarbeiter
- Shareholders:
  - RWTÜV
  - Giesecke & Devrient
- 7 Niederlassungen in D
- Niederlassungen in der Schweiz und Tschechien
- Fokus auf Informations- und IT-Sicherheit
- Liefern Systemlösungen vom Konzept über Entwicklung zum Rollout und Schulung
- Über 400 Kunden
- Starke Referenzen im öffentlichen Bereich (SINA)



turnover in Mio. €



>> 3

>> Agenda

secunet

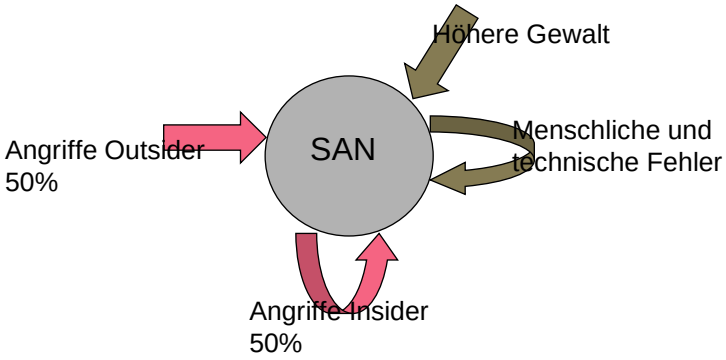
- Kurzinformation secunet
- Bedrohungen
- Kontroverse bzgl. SAN-Security
- Angriffe im Detail
- Sicheres SAN: Architektur
- Sicheres SAN: Einordnung
- Sicheres SAN: Kosten

>> 4

>> Bedrohungen

secunet

Sicherheit: Wirksamkeit des Schutzes vor Bedrohungen



>> 5

>> Bedrohungen

secunet

- ANSI, T11.3: 17 Bedrohungen (Angriffe) gegen FC SAN [1]
- IETF, IPS Working Group: 8 Bedrohungen (Angriffe) im Draft “Securing block storage protocols” [2]
- SNIA, Security Working Group: SAN threat model (Angriffe) [3]
- SSIF: Endnutzer besorgt über Konfigurationsfehler und Mißbrauch von Managementfunktionen [3]

>> 6

>> Bedrohungen

secunet

Wichtigste Bedrohungen:

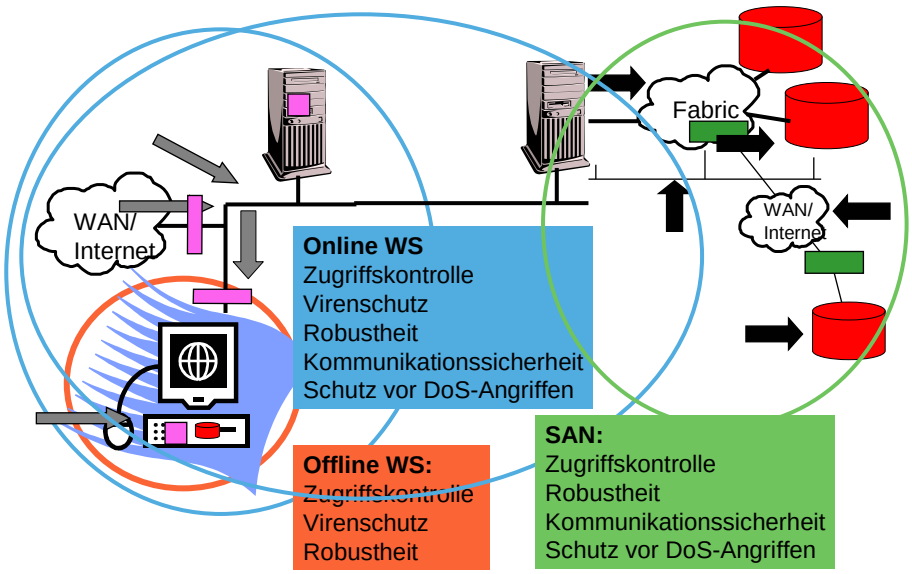
1. Managementfehler mit Datenverlust
2. Angriffe über IP-Link im SAN
3. Angriffe mit Managementapplikationen
4. Angriffe mit unauthorisierten Switch oder HBA

➢ Gegen Vertraulichkeit, Integrität, Verfügbarkeit der Daten

>> 7

>> Bedrohungen

secunet



>> 8

>> Bedrohungen

secunet

Grundlegender Unterschied zwischen DAS und SAN:

- DAS:
  - Vertrauen in den “Besitzer” der Daten (Server, OS) und in das Transportmedium (SCSI)
- SAN:
  - Daten müssen vor dem “Besitzer” (Server, OS) und dem “Transportmedium” (HBA, Switch) geschützt werden

>> 9

>> Agenda

secunet

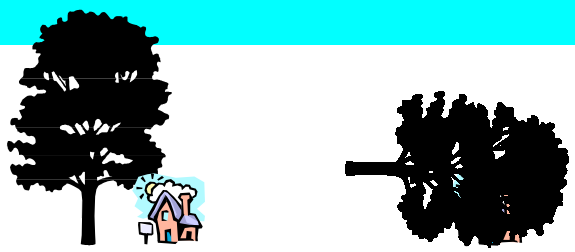
- Kurzinformation secunet
- Bedrohungen
- Kontroverse bzgl. SAN-Security
- Angriffe im Detail
- Sicheres SAN: Funktionen
- Sicheres SAN: Einordnung
- Sicheres SAN: Kosten

>> 10

>> Kontroverse bzgl. SAN-Security

secunet

Das SAN ist sicher – unsicher ist die Umgebung (Zugangs-LAN, Managementnetzwerk)!



- Strenge Sichtweise: SAN-Security unter Einschluss des Zugangs-LANs und des Managementnetzwerks
- Semi-strenge Sichtweise: SAN-Security unter Einschluss des Managementnetzwerks aber ohne Zugangs-LAN

>> 11

>> Kontroverse bzgl. SAN-Security

secunet

Von Insidern geht keine Gefahr aus oder man kann nichts gegen sie tun!

50% Insider  *50% Outsider*

- SAN ist z. Z. vollständig ungeschützt vor Insidern
- Bsp. für Datendiebstahl zum Vergleich (kein SAN):
  - USA, 01/03, TriWest Healthcare Alliance (military contractor): Theft of hard drives with half-million health-care records [5]
  - Canada, 01/03, ISM Canada (SSP): Theft of a hard disk with 180,000 insurance records and government information [6]
- Empfehlung: Verteilung der Administrationsaufgaben (Server, SAN, LAN, SAN-Security) auf mehrere Personen

>> 12

>> Kontroverse bzgl. SAN-Security

secunet

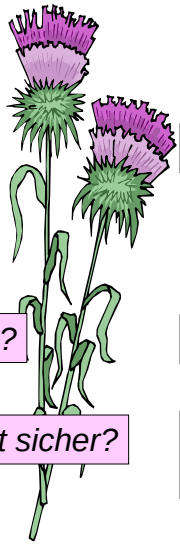
Nutzer

Zu kompliziert!

Zu teuer!

Keine Standards?

Ist das SAN nicht sicher?



Storage-Anbieter

Stört unsere Lösung!

Wir verdienen daran nichts!

Nicht interoperabel!

Keine schlafende Hunde wecken!

>> 13

>> Kontroverse bzgl. SAN-Security

secunet

18% der Nutzer verzichten auf ein SAN aus Sicherheitsbedenken [4]:

„Security is a key source of anxiety when it comes to SANs. According to the 2002 InfoWorld Networked Storage Survey, 18 percent of the readers polled have not deployed a SAN due to security concerns. And 56 percent of the respondents who have implemented a SAN or are planning to are concerned about its security“

>> 14

>> Agenda

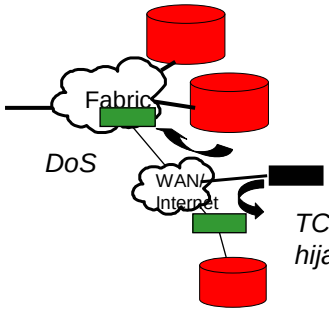
secunet

- Kurzinformation secunet
- Bedrohungen
- Kontroverse bzgl. SAN-Security
- Angriffe im Detail
- Sicheres SAN: Funktionen
- Sicheres SAN: Einordnung
- Sicheres SAN: Kosten

>> Angriffe im Detail

secunet

Angriffe über IP-Link des SANs:



1. Data sniffing
2. DoS
3. TCP/IP-connection hijacking

Experten für Internet-Sicherheit schätzen Angriffe über IP-Links folgendermaßen ein [4]:
“Attackers are expected to be able to exert almost total control over the communication between any two end systems. Specifically, that attacker will be able to remove packets, inject bogus packets, copy all traffic, repeat previously legal packets etc.”

>> Angriffe im Detail

secunet

Angriffe mit Managementapplikationen, insbesondere über WAN:

Gebräuchliche Passwörter für Router und Switches (FC inklusive) (http://www.phenoelit.de/dpl/dpl.html (default password list):
password
admin
root
Abcd1234
…

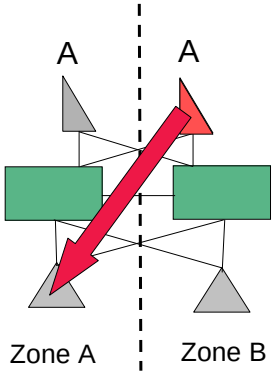
Security= 20% Technologie + 80% Umsetzung (Best practices)!!!!!!!

>> Angriffe im Detail

secunet

Angriff mit unautorisiertem HBA:

Ändern des WWN eines HBA (spoofing) mit Managementfunktionen des HBA (Ergebnis: Unautorisierter N_Port verbindet sich mit der Fabric)

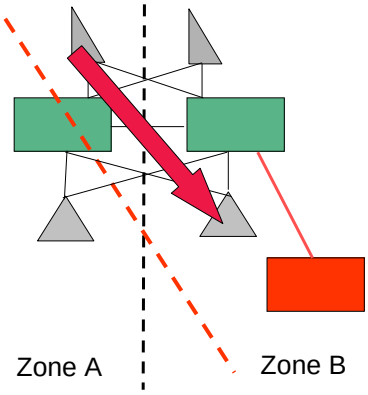


>> Angriffe im Detail

secunet

Angriff mit unautorisiertem Switch:

Unautorisierter Switch ändert Zoning-Informationen und ermöglicht unautorisierten Zugriff auf Daten (kann jederzeit entfernt werden)



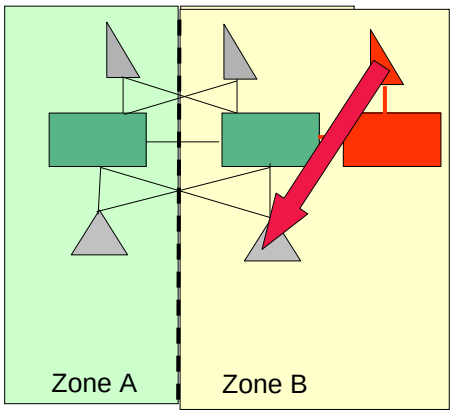
>> 19

>> Angriffe im Detail

secunet

Angriff mit unautorisiertem Switch und Server:

Unautorisierter Switch mit unautorisiertem Server ändert Zoning-Informationen und ermöglicht unautorisiertem Server Zugriff auf Daten (Switch und Server können jederzeit entfernt werden)



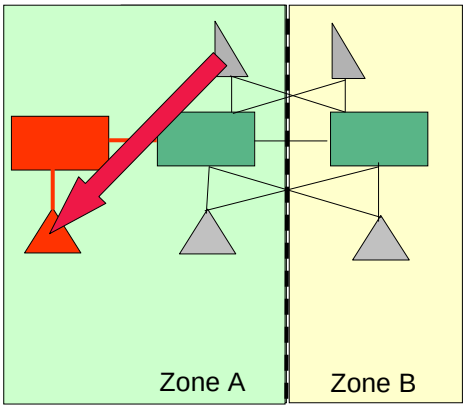
>> 20

>> Angriffe im Detail

secunet

Angriff mit unautorisiertem Switch und Speichergerät:

Unautorisierter Switch mit unautorisiertem Speichergerät ändert Zoning-Informationen und ermöglicht unautorisiertes Speichern von Daten in Kooperation mit einem Server (Switch und Speicher können jederzeit entfernt werden)



>> 21

>> Agenda

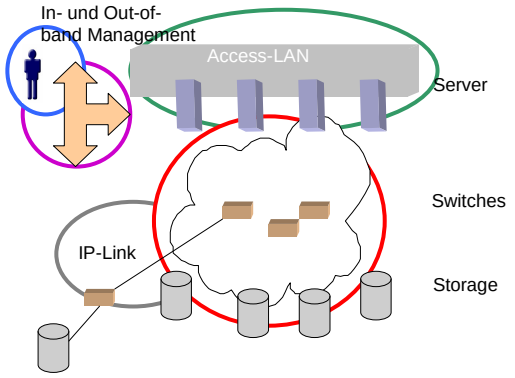
secunet

- Kurzinformation secunet
- Bedrohungen
- Kontroverse bzgl. SAN-Security
- Angriffe im Detail
- Sicheres SAN: Funktionen
- Sicheres SAN: Einordnung
- Sicheres SAN: Kosten

>> 22

>> Sicheres SAN: Architektur

secunet



Bereiche für Sicherheitsfunktionen:

- **SAN (IP-Link)**
- **Management**
- **User**
- **Access-LAN**

>> Sicheres SAN: Architektur

secunet

Gegenwärtige Sicherheitsfunktionen (< Gb):

- Zugangs-LAN
  - Härtung der Server
  - Intrusion Detection
  - Firewall
  - Virenschutz
  - Authentifikation, Autorisation der Nutzer
- SAN
  - Zoning (WWN, Portnummer, Hardzoning, Softzoning)
  - Portbinding (ACL)
  - LUN-Masking
  - IPSec-Hardware im IP-Link
- Management
  - Authentifikation der Managementapplikation gegenüber dem zu managenden Gerät (SSH, SNMPv3, SSL…)

>> Sicheres SAN: Architektur

secunet

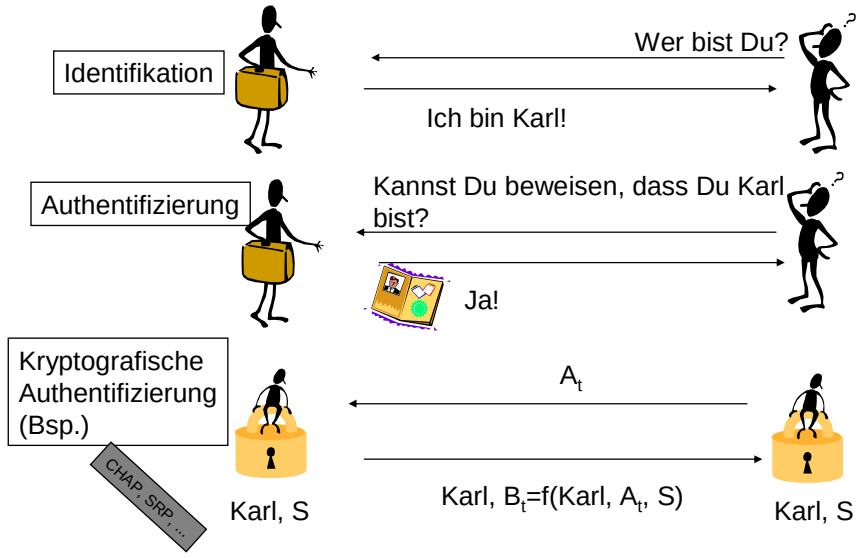
Gegenwärtige Sicherheitsfunktionen (< Gb):

- User
  - Authentifikation des Administrators (Passwort)
- Sicherheitsmanagement
  - Risk assessment toolkit (SSIF)
  - Best practice (SSIF)
  - Storage security audit (SSIF)

>> 25

>> Sicheres SAN: Architektur Authentifizierung

secunet



>> 26

>> Sicheres SAN: Architektur

secunet

Aufkommende Sicherheitsfunktionen (> Gb):

- SAN
  - iSCSI:
    - (IETF; IPS): Kryptografische Authentifikation zwischen Initiator und Target (Protokoll CHAP)
  - FC:
    - (T11, FC Security Protocol, FC-SP): Kryptografische Authentifikation zwischen Objekten: Switches, Switch-Ports, HBA und Switch, HBA und Storagegerät (Protokolle CHAP, FCAP (optional), FCPAP (optional))
  - Alle Protokolle:
    - (T11, IETF): Kryptografische Authentifikation bezogen auf Frame bzw. Paket; Verschlüsselung bei den Endpunkten der Kommunikation (Protokoll ESP)

>> Sicheres SAN: Architektur

secunet

Aufkommende Sicherheitsfunktionen (> Gb):

- Management
  - SNIA:
    - Kryptografische Authentifikation zwischen Managementapplikaktion und zu managendem Gerät (Protokoll: TLS als Teil von SMI-S 1.1);
      100 Produkte von 14 Firmen sind z. Z. konform zu SMS 1.0.2 mit SSL 3.0 (SNIA-CTC, Conformance Test Program)
- User
  - Kryptografische Authentifikation des Administrators (Chipkarte)
- IP-Link
  - IPSec-Hardware mit sehr geringer Verzögerung
- Storagegeräte:
  - Verschlüsselung der Daten bei der Speicherung

>> Agenda

secunet

- Kurzinformation secunet
- Bedrohungen
- Kontroverse bzgl. SAN-Security
- Angriffe im Detail
- Sicheres SAN: Funktionen
- Sicheres SAN: Einordnung
- Sicheres SAN: Kosten

>> Sicheres SAN: Einordnung

secunet

- Standardisierungs- und Lobbygruppen arbeiten (T11.3 (FC-SP wird für Mitte des Jahres erwartet), IETF, SNIA, SSIF)
- Hersteller implementieren Sicherheitsfunktionen und demonstrieren Zusammenarbeit (Brocade, McData, Cisco, Emulex, Qlogic)
- Sicheres SAN ist ein Geschäftsvorteil:
  - Es ermöglicht kontinuierliche Geschäftstätigkeit
  - Es spart Kosten durch Speicherkonsolidierung
  - Es spart Kosten durch die Nutzung intelligenter Managementapplikationen
  - Es spart Kosten durch den Einsatz von IP-Protokollen
  - Ermöglicht Geschäftstätigkeit durch die sichere Speicherung sensibler Informationen (gesetzliche Anforderungen)

>> Agenda

secunet

- Kurzinformation secunet
- Bedrohungen
- Kontroverse bzgl. SAN-Security
- Angriffe im Detail
- Sicheres SAN: Funktionen
- Sicheres SAN: Einordnung
- Sicheres SAN: Kosten

>> 31

>> Sicheres SAN: Kosten

secunet

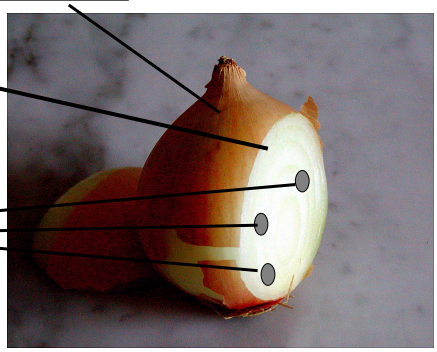
Ist SAN-Security zu teuer?

- Bestimmung der angemessenen Sicherheitsfunktionen gegen relevante Bedrohungen: 1-5% der SAN-Kosten

Kostenreduzierung mit SAN-Security

Risikoanalyse
Storage Security Policy,
Sicherheitskonzept

Sicherheitsfunktionen



>> 32

>> Sicheres SAN: Kosten

secunet

Ist SAN-Security zu teuer?

- Bestimmung der angemessenen Sicherheitsfunktionen gegen relevante Bedrohungen:
  - 1-5% der SAN-Kosten
- Sicherheitsfunktionen:
  - 5-15% der SAN-Kosten
- Management der Sicherheitsfunktionen:
  - 1-5% der Managementkosten (insbesondere für Schlüsselmanagement)

Denken Sie darüber nach, Geld zu sparen mit intelligenten und sicheren SANs!

>> 33

>> Referenzen

secunet

[1] www.t11.org
[2] www.ietf.org
[3] www.snia.org
[4]: InfoWorld, SAN Security goes IP, 2002
[5] www.informationweek.com
[6] www.thestar.com

>> 34

secunet

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?
Anmerkungen?
Jetzt oder später: helbig@secunet.de