Sicherheit von Speichernetzen

Probleme und Lösungen

Wilhelm Dolle
HiSolutions AG

und

Dr. Christoph Wegener
wecon.it-consulting

München, 13. März 2008

Frühjahrs Fach2008 Gespräch

Zur Person: Wilhelm Dolle

- Wilhelm Dolle
- HiSolutions AG: Senior Security Consultant
- CISSP, CISA, CISM
- ISO 27001 und IT-Grundschutzauditor des BSI
- ITIL-Service-Manager
- Fachautor/-lektor/-gutachter
- Verschiedene Lehraufträge an Hochschulen und Berufsakademien
- E-Mail: wilhelm.dolle@dolle.net Web: www.dolle.net

Frühjahrs Fach2008 Gespräch

Zur Person: Christoph Wegener

- Christoph Wegener

- Horst Görtz Institut für IT-Sicherheit (HGI)
- Gründer der **wecon.it**-consulting
- Gründungsmitglied der Arbeitsgruppe Identitätsschutz im Internet (a-i3)

- Auditor und Sachverständiger
- CISA, CISM, CBP
- Fachautor/-lektor/-gutachter
- Verschiedene Lehrtätigkeiten

- E-Mail: wegener@wecon.net Web: www.wecon.net

Frühjahrs Fach2008 Gespräch

Was werden wir heute vorstellen?

- Motivation und Hintergrund
- Allgemeine Einführung
  - Speichernetzen und BSI-Grundschutz
  - Risikofaktor "Management"
- Fibre Channel Protocol (FC)
  - Sicherheit durch Zoning?
- Gefährdungen in IP-basierten Speicherprotokollen
  - Generelle Gefährdungen
  - RFC 3723 als Lösung
- Zusammenfassung und Ausblick

Sicherheit von Daten(netzen)?

news 18.06.2005 11:44

<< Vorige | Nächste >>

40 Millionen Kreditkarten-Daten gestohlen

vorlesen

Durch eine Sicherheitslücke beim US-amerikanischen Dienstleister CardSystems Solutions, der Transaktionen zwischen Händlern und Kreditkarten-Unternehmen durchführt, haben sich Betrüger Zugang zu 40 Millionen Kundendaten verschafft, teilte MasterCard International am gestrigen Freitag mit. Davon betroffen seien Besitzer diverser Kreditkarten, darunter 13,9 Millionen MasterCard-Kunden. "Das hier hört sich nach dem Guinness Buch der Weltrekorde an", kommentierte Aktivist Richard Smith, der eine Website zum Thema Sicherheit betreibt.

Frühjahrs Fach2008 Gespräch

Sicherheit von Daten(netzen)?

news 18.06.2005 11:44

40 Millionen Kreditkarten-

vorlesen

Durch eine Sicherheitslücke beim US-amerika
Solutions, der Transaktionen zwischen Händle
durchführt, haben sich Betrüger Zugang zu 40
teilte MasterCard International am gestrigen F
Besitzer diverser Kreditkarten, darunter 13,9
"Das hier hört sich nach dem Guinness Buch d
Aktivist Richard Smith, der eine Website zum

ZDNet Security

Security - Sicherheit > News

USA: Daten von fast 185.000 Patienten gestohlen

Von Dawn Kawamoto und Joachim Kaufmann
CNET News.com
11. April 2005, 08:59 Uhr

FEEDBACK Ihre Meinung zum Thema

Informationen waren auf Desktop-Rechnern gespeichert, die am 28. März entwendet wurden

Der Gesundheitsdienstleister San Jose Medical Group warnt nahezu 185.000 derzeitige und ehemalige Patienten vor einem möglichen Missbrauch ihrer persönlichen Daten, darunter medizinische und finanzielle Informationen. Die Daten waren auf zwei Desktop-Rechnern abgelegt, die in den Morgenstunden des 28. März von Einbrechern entwendet wurden.

In Anbetracht der Zahl möglicher Betroffener handelt es sich bei dem Fall um eines der größten je bekannt gewordenen Datenlecks in den Vereinigten Staaten. Mike Patel, Vice President of Information Technology, sagte, dass bislang keine Hinweise auf den Missbrauch der Daten vorlägen. Das Material sei von der Medical Group von gesicherten Servern auf zwei neue Dell-Rechner kopiert worden, die von Einbrechern entwendet wurden. Das Material sei teilweise verschlüsselt gewesen.

MEISTGELESENE ARTIKEL

- Windows XP-Boot-CD mit integriertem SP2
- Schutz vor dem Crash: Top-Tools sichern wichtige Daten
- Hacker-Psychologie: Die neuen Tricks der Cyberkriminellen
- Arcor sperrt Porno-Sites
- Sicher wie beim Geheimdienst: Festplatten fachgerecht löschen

SECURITY BLOG

- Sicherheitslücke in Media Player Classic
- Microsoft: "Office Open XML bietet mehr Sicherheit"
- Microsoft startet Hacker-Blog
- RFID-Schlappe in Prag: Chips zu unsicher
- Die Geschichte eines rumänischen Ebay-Betrügers
- Vorsicht vor vvindowsupdate.com
- 28 Prozent der installierten Standardsoftware sind unsicher
- Mac-Wurm-Autor erhält Todesdrohungen
- Web Crash 2007: Alle Online-Daten verloren
- Windows Vista Service Pack 1: Beta im Anmarsch

alle Blog-Einträge...

Sicherheit von Daten(netzen)?

news 18.06.2005 11:44

40 computer security.de
Das Online-Magazin für Computersicherheit

Login | Registrieren

Suchen

MAGAZIN | TESTBERICHTE | BLOG | SICHERHEITSLÜCKEN | VERANSTALTUNGEN | RSS-FEEDS | KONTAKT

Schon wieder persönliche Daten gestohlen

08. August 2007

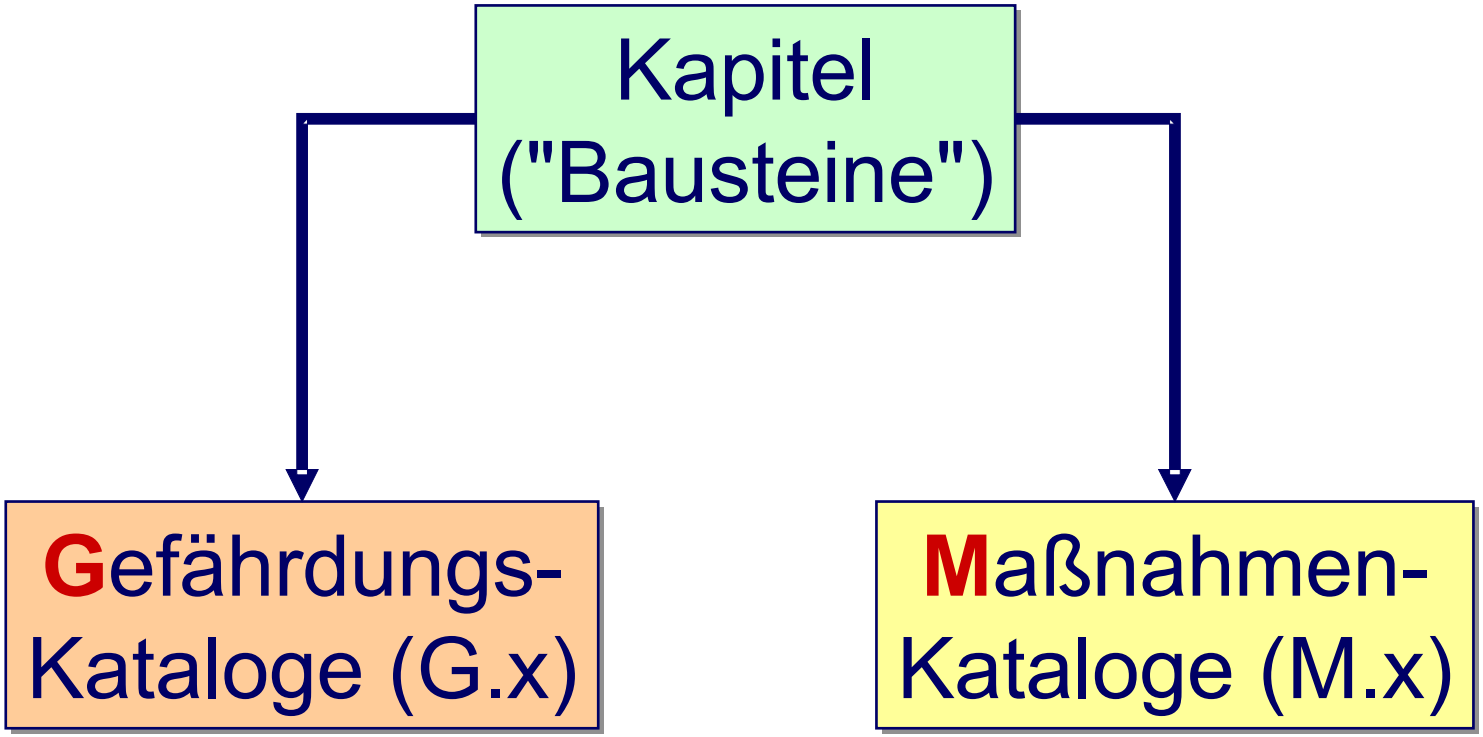
Erst kürzlich stellten wir im Zusammenhang mit anonymisiertem Suchen Überlegungen zu der Sicherheit von persönlichen Daten an, die bei Firmen gespeichert sind. Und schon wieder erreichen uns Berichte über den Diebstahl von persönlichen Daten. Wie „The Register" berichtet, wurden bei einem Einbruch bei „First Response Finance" Datenträger gestohlen, die Kundendaten enthielten. „First Response Finance" warnt daher die englischen Kunden auf verdächtige Kontobewegungen zu achten.
Auch Verisign, bekannter Internet Hoster und Aussteller von Zertifikaten, ist Opfer eines Diebstahls geworden. Laut Computerworld bestätigt Verisign, dass ein Laptop, der Daten über Angestellte enthalten hat, entwendet wurde. Der Angestellte, dem der Laptop abhanden gekommen ist, hat wohl die Vorgaben bezüglich Laptops mit sicherheitsrelevantem Inhalt missachtet und hat mittlerweile den Dienst quittiert.

Dell-Rechner kopiert worden, die von Einbrechern entwendet wurden. Das Material sei teilweise verschlüsselt gewesen.

Was ist IT-Sicherheit?

- Summe, der vier allgemeinen Sicherheitsziele
  - **Vertraulichkeit**
    - Alle Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden können.
    - Dies gilt sowohl beim Zugriff auf gespeicherte Daten, wie auch während der Datenübertragung.
  - **Integrität**
    - Daten dürfen nicht unbemerkt verändert werden können.
    - Alle Änderungen müssen jederzeit nachvollziehbar sein.
  - **Verfügbarkeit**
    - Zugriff auf Daten muss jederzeit (=innerhalb eines vereinbarten Zeitrahmens) gewährleistet sein.
  - **Verbindlichkeit**
    - Kombination von Authentizität und Nichtabstreitbarkeit.
    - Bei der Übertragung von Informationen bedeutet dies, dass die Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann. Urheber von Datenänderungen müssen erkennbar sein und dürfen die Veränderungen nicht abstreiten können.
- *Gilt insbesondere für Speichermedien, z.B. SANs!!!*

Aufbau der IT-Grundschutzkataloge des BSI



Frühjahrs Fach2008 Gespräch

Anforderungen des BSI an den sicheren Betrieb von Speichernetzen (I)

- Baustein B 3.303 "Speichersysteme und Speichernetze"
- NAS (Network Attached Storage)
  - Typisch: *Ethernet-Netzwerk* mit *dateibasierten Protokollen* wie
    - NFS (Network File System Protokoll) oder
    - CIFS (Common Internet File System)
- SAN (Storage Area Network)
  - *Blockbasierte Protokolle* (meist SCSI)
    - darunter meist *FC (Fibre Channel)*
    - seltener *TCP/IP (als Internet(i)SCSI)*
  - Typisch: Nutzung eines dedizierten Netzes zwischen Speichersystemen und Servern
  - Bestandteile
    - Plattensystem(e)
    - Aktive Elemente (SAN-Switches)
    - Weitere Speichersysteme (z. B. Bandlaufwerken) und angeschlossene Server

Frühjahrs Fach2008 Gespräch

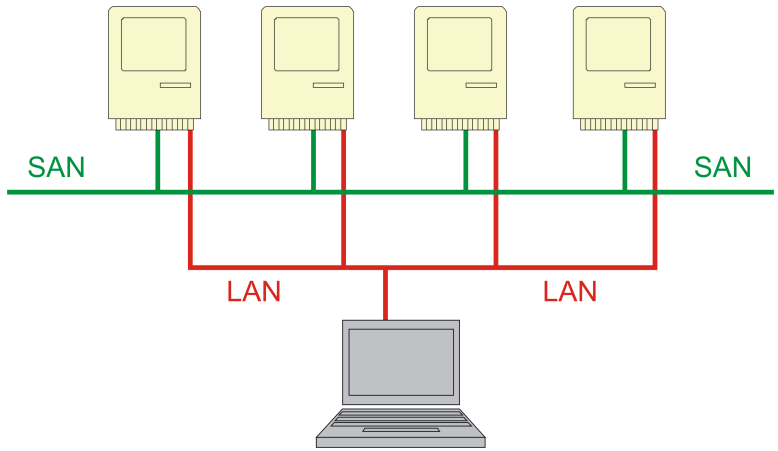
Anforderungen des BSI an den sicheren Betrieb von Speichernetzen (II)

- Relevante Gefährdungen unter anderem:
  - Manipulation der Konfiguration
  - Abhören bzw. Manipulation von Daten
  - Fehlerhafte Zuordnung von Ressourcen
- Relevante Maßnahmen unter anderem:
  - M 2.353
    "Erstellung einer Sicherheitsrichtlinie für SAN-Systeme"
  - M 2.357
    "Aufbau eines Administrationsnetzes für Speichersysteme"
  - M 4.274
    "Sichere Grundkonfiguration von Speichersystemen"
  - M 4.275
    "Sicherer Betrieb eines Speichersystems"
  - M 5.130
    "Absicherung des SANs durch Segmentierung"

Einige Risikofaktoren

- Generell: "Der Schutz von Speichersystemen stellt die letzte Verteidigungslinie der IT-Systeme einer Institution dar"

- Management von Speichernetzen
  - Das Management eines Speichernetzes ist ein wichtiger, aber oft vernachlässigter Faktor.
  - Generell *alle Speichersysteme* in ein *separates Netz* stellen (in Analogie zu Fibre Channel).



- Virtualisierung
  - Neue Probleme, denn viele Standardmaßnahmen greifen nicht mehr

Frühjahrs Fach2008 Gespräch

Sicherheit beim "Management"

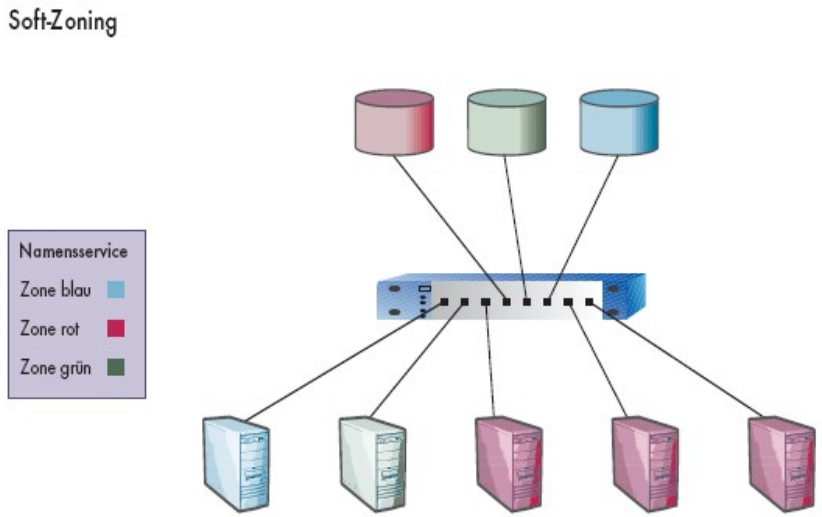
- "Goldene Regeln" für die Administration von aktiven (Speicher-)Komponenten (z.B. FC-Switches)
  - Default Passwörter durch eigene starke Passwörter ersetzen
  - Unsichere Telnet-, HTTP-Frontends oder proprietäre Management-Software durch sichere, verschlüsselte Varianten (SSH, HTTPS, wahlweise auch VPN) ersetzen
  - Deaktivieren von nicht benötigten Diensten
    - Portscan ratsam, da teilweise unvollständige Dokumentation!
  - Eigenes Managementsegment im Netz oder zumindest Einschränkung auf bestimmte IP-Adressen oder Netzwerksegmente nutzen
  - Nutzung von privaten IP-Adressen im Management-LAN

Fibre Channel
Schutz durch Zoning

- Fibre Channel bringt bereits eine eigene Netzinfrastruktur mit
- Zoning: Eigener Mechanismus zur Segmentierung
  - Separieren von Elementen wie
    - Speichersystemen,
    - Switches und
    - Servern im Speichernetz.
  - Endgeräte, die sich im FC-SAN gegenseitig sehen sollen, können zusammengefasst werden
  - Zonen dürfen sich auch überlappen
- Arten des Zoning
  - Soft-Zoning
  - Hard-Zoning

Fibre Channel – Soft-Zoning (I)

- Basiert auf World Wide Node Names (WWNN) oder World Wide Port Names (WWPN) der betreffenden Endgeräte
  - Beschränkt damit auf die Auskunft des Nameservers (SNS oder DNS) der Zone, der stets eine aktuelle Liste der verfügbaren Endgeräte verwaltet.
- Bei der Anmeldung in der Zone gibt der Nameserver die Liste der Endgeräte zurück, mit denen das anfragende System mindestens eine gemeinsame Zone hat.
- Vorteil: Zonen bleiben beim Neu- oder Umverkabeln der Geräte ebenso wie bei deren Umzug auf andere Switch-Ports erhalten.



Fibre Channel – Soft-Zoning (II)

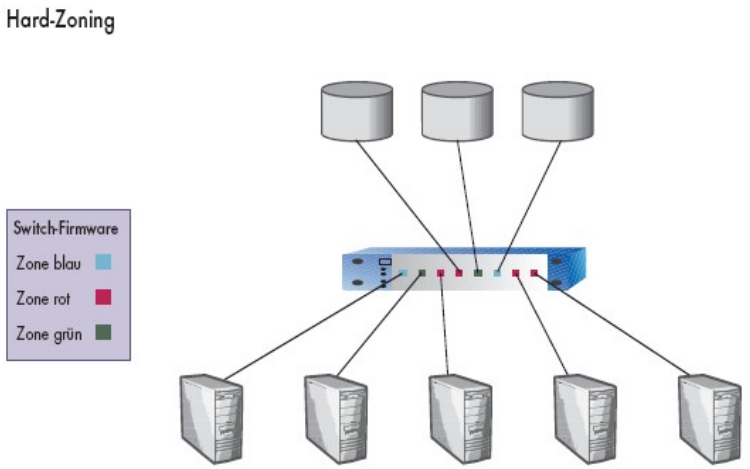
- Für den Schutz von sensiblen Daten nur bedingt geeignet, da die bloße Kenntnis der Adresse ausreicht, um mit dem gewünschten System trotzdem zu kommunizieren.
- Keinerlei Schutz gegen WWxN-Manipulationen (zum Beispiel Spoofing!)
- Manche Betriebssysteme unterlaufen das Zoning, indem sie eine Liste der Namen von Geräten verwalten, mit denen sie jemals eine gemeinsame Zone hatten. Dadurch bei Änderungen der Zonen oft noch Zugriffe auf Endgeräte möglich, die aktuell nicht mehr in ihrer Zone liegen.

Fibre Channel – Hard-Zoning

- Hard-Zoning (oft auch Port-Zoning genannt) basiert auf den "physischen Adressen" oder Port-IDs der Switch-Ports
  - Jeder Switch unterhält dazu eine Zonenliste, die festlegt, welche Ports intern miteinander kommunizieren dürfen.

- Switches, die über eine Crossbar-Switch-Architektur verfügen, de-aktivieren alle unerlaubten Port-zu-Port-Verbindungen durch Abschalten der entsprechenden Switchports.

- Nachteil: Bei jedem "Umstöpseln" muss die Zonen-Konfiguration auf dem Switch geändert werden.



Eine Checkliste zur Sicherheit

- Management
  - Unsichere Dienste abschalten
  - Durch sichere Varianten ersetzen (wenn dies möglich ist)
  - Nicht benötigte Dienste abschalten
  - Separates Management-LAN (private IP-Adressen) einrichten
  - Bereits beim Kauf auf diese Punkte achten!
- Fibre Channel – Zoning:
  - Wenn immer möglich Hard-Zoning verwenden
  - Kombination mit *LUN-Masking* (Einschränken des LUN-Zugriffs auf bestimmte WWNs) und Einschränken von Zugriffsrechten (R/W) erhöht Sicherheit weiter
  - *Virtuelle SANs (VSANs)* geben zusätzlichen Schutz

Gefährdungen in IP-basierten Speicherprotokollen

- IP-Block-Storage-Protokolle transportieren letztendlich SCSI-Kommandos über IP
  - Anfällig für Angriffe auf das Protokoll selbst, aber auch auf die transportierten Nutzdaten, Angriffsmöglichkeiten sind vielfältig:
    - Sniffing
    - Manipulation von Paketen
    - Einfügen von Paketen
    - Übernehmen ganzer Sessions
    - DoS-Attacken
    - Vorspielen von Storage-Geräten, um Benutzerdaten abzufangen.
- Benötigt werden also Sicherheitserweiterungen, die
  - die Vertraulichkeit,
  - eine bidirektionale Authentifizierung der Geräte,
  - die Integrität der Daten und
  - einen Schutz vor Replay-Attacken

  in jedem übertragenen Paket gewährleisten.

Lösungsansatz: RFC 3723 "Securing Block Storage Protocols over IP"

- Verschlüsselter Tunnel zwischen zwei Punkten durch IPsec
  - Alle IP-Block-Storage-Protokolle müssen IPsec ESP (Encapsulation Security Payload) bereitstellen
  - Unglücklich: 3DES Pflicht, AES optional
  - Unglücklich: Implementierung des *Tunnel Mode* zwingend vorgeschrieben, allerdings *Transport Mode* ebenfalls erlaubt
- Authentifizierung
  - Optional können sich die Kommunikationspartner gegenseitig per
    - Kerberos V5
    - SPKM1, SPKM2 (Simple Public-Key GSS-API Mechanism)
    - SRP (Secure Remote Password)
    - CHAP (Challenge Handshake Authentication Protocol) oder
    - Herstellereigenen Methoden authentifizieren oder
    - Einfach darauf verzichten!!! (hierzu RFC 3720 "Internet Small Computer Systems Interface (iSCSI)", Abschnitt 11.1).
  - Zwingend vorgeschrieben für iSCSI-Implementierungen nur CHAP (anfällig für Wörterbuchangriffe, daher IPsec bei Key-Längen unter 96 Bit und ein echt zufälliges, einmaliges CHAP-Secret vorgeschrieben)

Zusammenfassung

- Management von Speichernetzen
  - Segmentierung von Netzen nutzen
  - Unsichere Dienste abschalten
  - Sichere Varianten nutzen (wenn möglich)
  - Bereits bei der Kaufentscheidung beachten!
- Fibre Channel – Zoning
  - Hard-Zoning verwenden
  - Weitere Verbesserung der Sicherheit durch LUN-Masking
  - Nutzung von VSANs
- RFC 3723 – Sicherheit für Block Storage Protokolle
  - IPsec für Transport der Daten vorgeschrieben
  - Leider unglückliche, da aufgeweichte Anforderungen
  - Gesicherte Authentifizierung dennoch nur "optional"
  - Auch hier bereits beim Kauf Interoperabilität beachten!

Frühjahrs Fach2008 Gespräch

FC-SP und FC-SP2 – ein Ausblick

- Fibre Channel Security Protocol (FC-SP)
  - Draft der "ANSI-Arbeitsgruppe T11.3" in Version 1.8
  - Sichere Authentifizierung zwischen beliebigen Paaren von Switches und Endgeräten mittels
    - Direkter Identifikation oder durch
    - Nutzung eines RADIUS- oder TACACS+-Servers.
  - Authentifizierung mittels
    - CHAP,
    - Digitalen Zertifikaten (FC-AP) oder
    - Passwörtern (FC-PAP).
- Zukünftiger Standard: FC-SP2
  - Weitere Sicherheitserweiterungen
  - Berücksichtigung von Inter Fabrics Routing (FC-IFR) (zum Aufbau von weltweiten Datennetzen)
  - Arbeitspapiere der T11.3 bereits verfügbar

Literatur – eine Auswahl

- RFC 3720 "Internet Small Computer Systems Interface (iSCSI)"
  www.ietf.org/rfc/rfc3720.txt?number=3720
- RFC 3723 "Securing Block Storage Protocols over IP"
  www.ietf.org/rfc/rfc3723.txt?number=3723
- Projekte und -Standards der ANSI T11
  http://www.t11.org
- Arbeitspapiere der ANSI T11 zu FC-SP2
  http://www.t11.org/t11/stat.nsf/fcproj?OpenView&Count=70
- "Sicherheitsbereich - Schutz von Speichernetzen";
  Wilhelm Dolle, Christoph Wegener, Susanne Nolte; iX 02/2007

Danke :)

- Ihnen für Ihre Aufmerksamkeit :)
- Fragen?!?

- Wilhelm Dolle
  - E-Mail: wilhelm.dolle@dolle.net
  - Web: www.dolle.net
- Dr. Christoph Wegener
  - E-Mail: wegener@wecon.net
  - Web: www.wecon.net