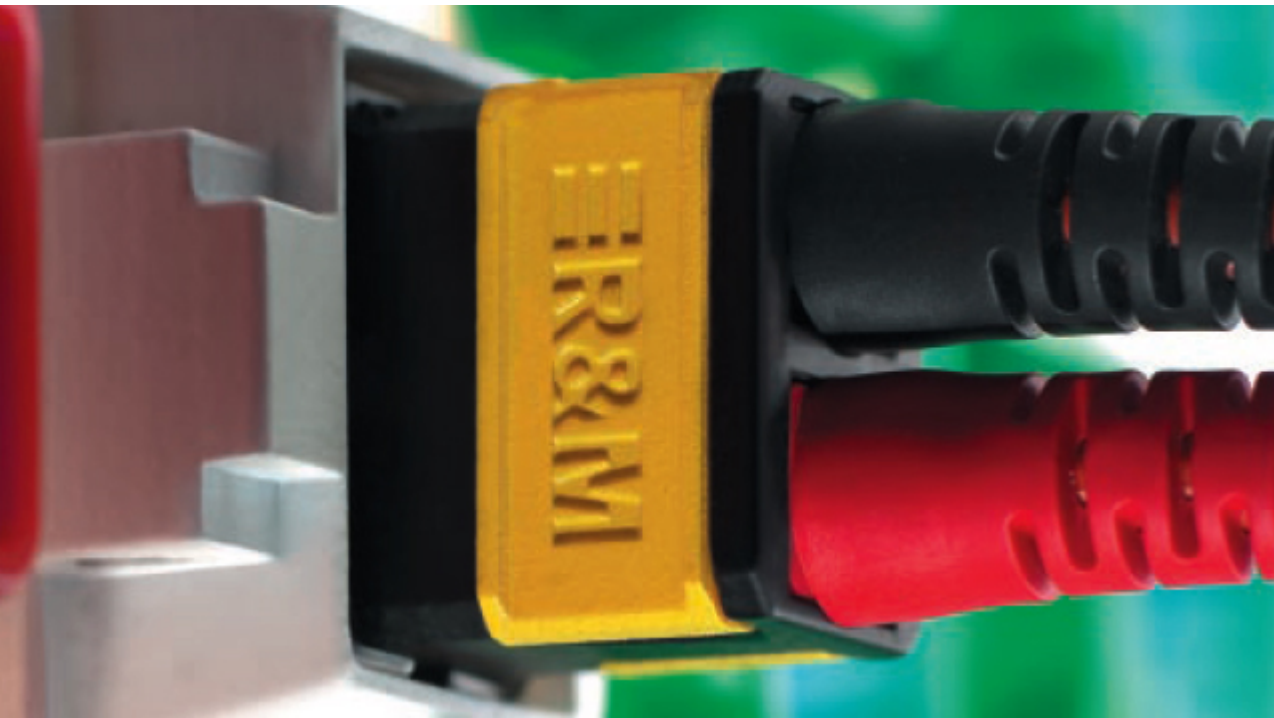


White Paper



Sicherheitslücken im LAN?

Die Angst vor dem grossen Blackout trübt den Blick
für die vielen kleinen Risiken



Convincing cabling solutions

Inhalt

Sicherheitslücken im LAN?

Die Angst vor dem grossen Blackout
trübt den Blick für die vielen kleinen Risiken

1. GROSSER BLACKOUT ODER VIELE KLEINE VERLUSTE?	3
2. WIE LANGE KANN IHR UNTERNEHMEN EINEN NETZAUSFALL ÜBERLEBEN?	4
3. NETZSICHERHEIT –EINE FRAGE DER PRIORISIERUNG?	4
4. HAUPTFEHLERQUELLEN AUSSCHLIESSEN	5
5. FLEXIBILITÄT UND SICHERHEIT – KONTRÄRE FORDERUNGEN	7
6. SCHON BEI DER PLANUNG DIE WEICHEN STELLEN	7

© Copyright 2004 Reichle & De-Massari AG (R&M). Alle Rechte vorbehalten.

Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch Reichle & De Massari AG nicht gestattet. In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden. Die Erstellung dieses Dokuments erfolgte mit grösstmöglicher Sorgfalt und enthält den zum Zeitpunkt der Erstellung aktuellen technischen Stand. Technische Änderungen vorbehalten.

Sicherheitslücken im LAN?

Viren, Würmer und Trojaner machen Schlagzeilen. Die Schäden für grössere Unternehmen werden oft mit Hunderten von Millionen Dollar beziffert. Dass jedoch die meisten Netzwerkstörungen auf unspektakuläre Verbindungsfehler zurückgehen, machen sich nicht alle Verantwortlichen klar. Denn dabei geht es um Geld, das nicht dammbbruchartig verschwindet, sondern nebenbei versickert.

Verbindungsfehler entstehen durch technische Unzulänglichkeiten, menschlichen Irrtum oder mutwillige Manipulation. Gegen alle drei Ursachen kann man sich wirksam schützen – mit der richtigen Technik.

Geschäftsfeld:	Enterprise Cabling
Anwendung:	Local Area Networks (LAN), Anschlusstechnik
Format:	White Paper
Topic:	Sicherheit in lokalen Netzen durch Massnahmen gegen unbeabsichtigte oder unberechtigte Manipulation der Anschlüsse
Ziel:	Information über die häufigsten Ursachen von Netzwerkstörungen, ihre Auswirkungen und ihre Vermeidung
Audience:	IT-Manager, Planer und Installateure, IT-Consultants
Autoren:	Thomas Bürgler
Erschienen:	Juli 2004

1. Grosser Blackout oder viele kleine Verluste?

„Disaster Recovery Planning“ war nach dem 11. September 2001 das Schlagwort, unter dem IT-Verantwortliche vor allem in den USA ihre Netze auf Sicherheit prüften, um im Fall der Fälle die „Business Continuity“ zu garantieren. Die Stromausfälle vom 14. August 2003 im Norden der USA und Ende September 2003 in Italien hatten ungleich grössere Auswirkungen auf die Firmennetze, doch vergleichbare Aktivitäten blieben aus – vielleicht weil kein terroristischer Hintergrund bestand.

In Europa hat auch der 11. September keine umgreifende Steigerung der Sicherheitsanstrengungen ausgelöst. Nach einer Umfrage der Computerwoche vom 20. November 2001 reagierten nur 9 % der Unternehmen stark, 66 % dagegen gar nicht mit zusätzlichen Sicherheitsvorkehrungen auf die Vorgänge. Und inzwischen wird wieder weltweit an der Sicherheit gespart. Diesen Trend konnte Ernst & Young in seiner Umfrage zur IT-Sicherheit in Unternehmen vom August 2003 ausmachen.

Dabei nimmt die Zahl der Sicherheitsverstösse deutlich zu. Doch auch das veranlasst nur etwa jedes dritte Unternehmen zu erhöhten Sicherheitsvorkehrungen – laut der zurzeit laufenden Information Week-Studie IT-Security 2004.

Nun muss man unterscheiden zwischen dem Katastrophenfall und den vielen kleinen Ausfällen und Störungen im Alltag. Viren, Würmer und Trojaner machen regelmässig Schlagzeilen. Gezielte Angriffe von aussen sind meist Einzelfälle und werden nur bekannt, wenn sie ein gewisses Ausmass an Schaden verursachen. Dass die meisten Netzausfälle auf Hardware- und Verkabelungsfehler zurückgehen, bleibt weitgehend unbeachtet, weil unspektakulär. Dennoch weisen renommierte Studien gerade auf dieses Problem hin.

2. Wie lange kann Ihr Unternehmen einen Netzausfall überleben?

Für 46 % der Unternehmen bedeutet ein einstündiger Netzausfall einen Schaden von bis zu 50.000 US-Dollar, für 8 % einen Verlust von über einer Million. Dabei fürchten 4 % der Unternehmen schon bei einem einstündigen Netzausfall um ihren Bestand, nach 72 Stunden sind auch die letzten 40 % der Unternehmen gefährdet. Das ergab eine Umfrage von Contingency Planning Research im Frühjahr 2001, auf die 163 Unternehmen antworteten.

Weitere Statistiken zeigen: Am empfindlichsten reagieren das Börsengeschäft und der Zahlungsverkehr mit Kreditkarten auf Netzwerkstörungen und Datenverlust. Es folgen Energieversorgung, Telekommunikation, Transport und Verkehr sowie grosse Fertigungsbetriebe.

Einem schlüssigen IT-Sicherheitskonzept geht deshalb eine Risikoanalyse voraus. Dabei spielen Grössen wie die mögliche Schadenshöhe, die Eintrittshäufigkeit und der Wert der bedrohten Objekte eine Rolle. Dann die Natur der Angriffe oder Störungen: Viren, unberechtigte Zugriffe, Denial-of-Service-Attacken, Manipulationen. Schliesslich die möglichen Angreifer selbst: Computerhacker, Terroristen, autorisierte oder nicht autorisierte Mitarbeiter, ehemalige Mitarbeiter, Wettbewerber. So werden sich die Verantwortlichen klar, wo das „Herz“ des Unternehmens schlägt, wo die Schlagadern verlaufen und wie sie zu schützen sind.

Modellrechnung

Wirtschaftlicher Schaden durch Leitungs- und Verbindungsfehler

1 Stunde Netzausfall in sensiblen Bereichen von Unternehmen verursacht durchschnittlich einen Verlust von 90.000 US-Dollar (Contingency Planning Research).

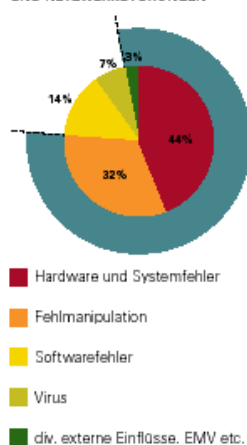
72 % aller Systeme in sensiblen Bereichen fallen 9 Stunden pro Jahr aus (The Standish Group).

59 % der Netzwerkprobleme sind direkt auf die physikalische Infrastruktur und die Verbindungen zurückzuführen (The Gartner Group).

Damit beträgt der Schaden durch Leitungs- und Verbindungsfehler $0,72 \times 90.000 \text{ Dollar/Stunde} \times 9 \text{ Stunden/Jahr} \times 59 \% = 344.088 \text{ Dollar/Jahr}$.

3. Netzsicherheit – eine Frage der Priorisierung?

URSACHEN VON DATENVERLUST UND NETZWERKSTÖRUNGEN¹⁾



Hauptursachen für Datenverlust.

Quelle: CPR

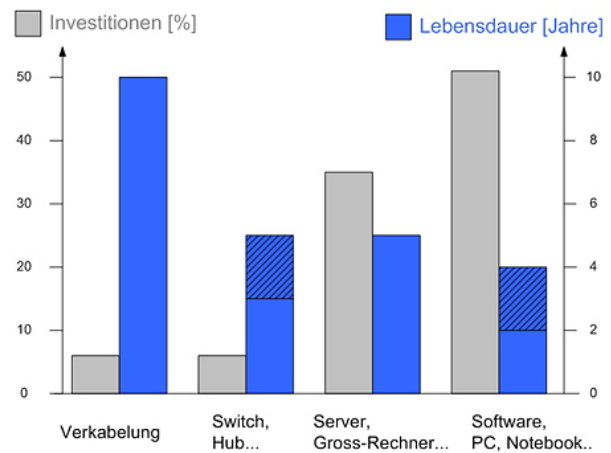
Die Studie von Contingency Planning Research zeigt, dass nur 7 % der Datenverluste durch Viren verursacht werden, aber 44 % auf Hardwarefehler und 32 % auf menschliche Irrtümer zurückzuführen sind. Die beiden zuletzt genannten Bereiche lassen sich mehr oder weniger dem Layer 1 zuordnen (petrol-farbige Schale in der Grafik links).

Die meisten alltäglichen Netzwerkstörungen und Datenverluste entstehen also durch kleinere Funktionsfehler und menschliche Unzulänglichkeiten. Sie sind nicht bestandsbedrohend und treffen die Unternehmen trotzdem empfindlich, beispielsweise wenn Teile der Produktion kurzzeitig stillstehen, weil ein neuer PC als Terminal falsch verbunden wurde und das Netz „lahm legt“, oder wenn die Auftragsabwicklung nicht buchen kann, weil der Server durch ein falsch angeschlossenes Endgerät irritiert ist. Selbst wenn nur der LAN-Anschlussstecker beim Putzen vom Besen mitgenommen und nachher falsch eingesteckt wurde, verrinnt wertvolle Arbeitszeit, bis der Irrtum erkannt und korrigiert ist.

Nicht gerechnet sind die Zeiten, die verstreichen, „weil das Netz mal wieder langsam ist“. Schlechte Kabel, unsichere Kontakte, Fehlanpassungen führen zu Sendewiederholungen in der Übertragung und bremsen die Datenrate ganz erheblich. Sie führen nicht zum Stillstand, sondern zur Ineffizienz. Das technische Problem bekommt ein wirtschaftliches Ausmass.

Damit ist klar: Der Super-GAU, der ein Unternehmen schlagartig stilllegt, ist eher unwahrscheinlich. Die meisten Unternehmen leiden unter den vielen kleinen Sicherheits-Lecks und die sind im physikalischen Netzwerk zu finden.

Dass gerade hier gespart wird, ist deshalb unverständlich. Denn laut dem IT-Analysten Datapro verursacht die Verkabelung nur rund 5 % der IT-Kosten. Etwas über die Hälfte der Investitionen steckt in Software und Hardware, die Server und Grossrechner kommen zusätzlich auf einen Anteil von 35 %, die Aktivgeräte wie Switch und Hub auf 7 %. Betrachtet man nun die Lebensdauer der einzelnen IT-Segmente, so wird klar dass der Verkabelung mit einer Lebensdauer von ca. 10 Jahren eine viel höhere Beachtung geschenkt werden muss! Das Fundament jeder IT-Infrastruktur ist die Verkabelung und auf der wird nachher das ganze IT-Netzwerk aufgebaut. So wird auch beim Bau eines Hauses zuerst ein solides Mauerwerk erstellt!



Verhältnis von Investitionskosten zu Lebensdauer bei verschiedenen IT-Segmenten. Die fundamentale Bedeutung der Verkabelung wird dabei oft falsch eingeschätzt.

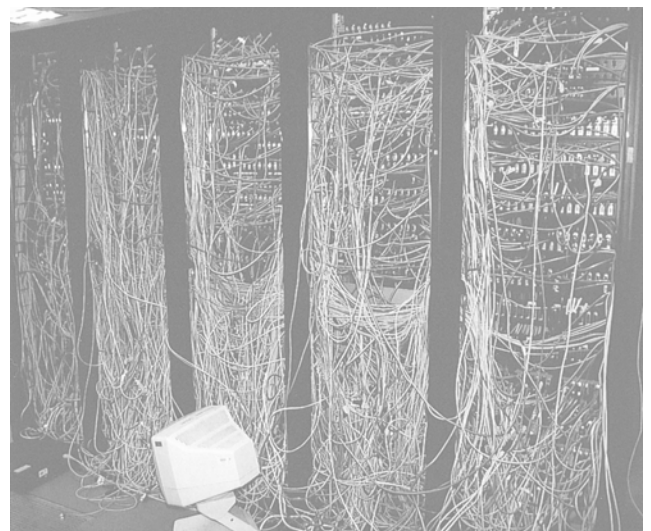
Quelle: Datapro / Grafik: R&M

4. Hauptfehlerquellen ausschliessen

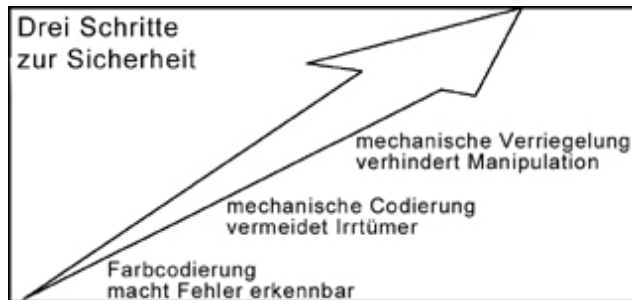
Ursachen für schlechte oder falsche Verbindungen haben meist drei Gründe: technische Unzulänglichkeiten, menschlichen Irrtum oder mutwillige Manipulation.

Gegen technisches Versagen hilft bessere Technik – und dennoch hat dieses Problem eine menschliche Komponente: Das Qualitätsbewusstsein aller Verantwortlichen und Mitarbeiter.

Dem menschlichen Irrtum kann man umgekehrt mit Technik begegnen: mit einer übersichtlichen Installation und einer sauberen Dokumentation. Ein erster Schritt dorthin besteht in einer eindeutigen Kennzeichnung aller Netzwerkkomponenten, Anschlusskabel und Anschlüsse, beispielsweise durch ein Farbsystem.



Bei diesem „Kabalsalat“ sind Fehlverbindungen im lokalen Daten-netz vorprogrammiert. Fehlersuche ist praktisch unmöglich.



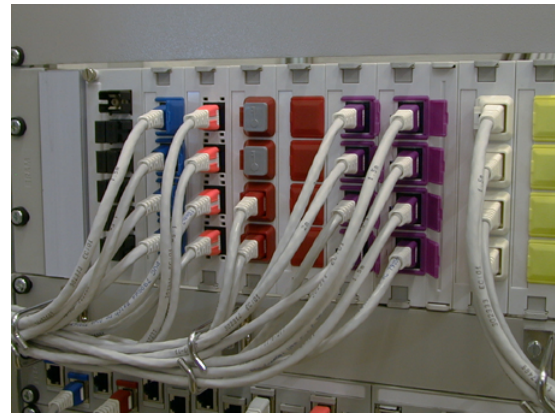
Der Weg zu grösserer Sicherheit in Netzwerken beginnt bei einfachsten Schutzmassnahmen im Bereich der Kabel und Stecker, wodurch zahlreiche teure Pannen verhindert werden können.

Ein weiterer Schritt ist, Fehlverbindungen mechanisch zu verhindern. Das ist umso wichtiger, je mehr sich die RJ45-Steckverbindung durchgesetzt hat. Scheinbar passt alles zusammen: der Telefonanschluss, die Token-Ring-Workstation, das Ethernet-PC-LAN. Denn alle benutzen RJ45. So kann es passieren, dass man bei Verwechslungen nicht nur die Funktion der Netze stört, sondern beispielsweise mit der Gleichspannung des Telefonnetzes empfindliche Datenports „verheizt“.

Hier hilft ein mechanischer Einsteckschutz mit visueller Codierung. Er macht die Anschlüsse verwechslungssicher und verhindert undefinierte Zustände im Netz.

Den besten Schutz gegen Irrtum und Manipulation bietet ein System, das unbeabsichtigtes oder vorsätzliches Trennen von Netzwerkverbindungen genauso verhindert wie unberechtigten Zugang. Intrusion Detection besteht nicht nur in einer Software, mit der man professionellen Angreifern und ambitionierten Hobby-Hackern das Handwerk legt. Viele unberechtigte Eingriffe kann man einfach mechanisch verhindern.

Das ist unumgänglich in Notrufzentralen und Krankenhäusern, wo es um menschliches Leben geht, oder bei Banken, Börsen und allen Unternehmen, deren geschäftliche Lebensader das Netz ist. Dringend zu empfehlen ist dieser Schutz in Schulen, Bibliotheken und öffentlichen Räumen, wo Missbrauch oder einfacher Spieltrieb den Netzwerkverantwortlichen auf Trab halten würden. Ebenso wichtig ist er für Konferenzräume, Arbeitsplätze mit ständig wechselndem Personal, Hotelhallen oder Kaufhäuser, die im Aussenbereich Datenanschlüsse haben, um ihre Kassen anzuschliessen. Sie müssen verhindern, dass nachts jemand auf ihre Kosten im Internet surft. Wertvoll ist dieser Schutz auch zu Hause, wo Kinderhände an den Kabeln herumspielen.



Sauberes Kabel-Management. Die Ports sind farblich gekennzeichnet, mechanisch gegen falsches Einstecken codiert und können mit einem Ein- und Aussteckschutz versehen werden, den nur autorisiertes Personal entfernen kann.



Mechanisch abgesicherte Anschlussdose am Arbeitsplatz. Falsche Verbindungen können gar nicht erst entstehen und somit Zerstörungen von Netzwerkkarten im PC ausgeschlossen werden.

5. Flexibilität und Sicherheit – konträre Forderungen

Wenn ein lokales Netz einmal fix installiert ist, lässt es sich weitgehend sicher betreiben. Doch ein lokales Netz „lebt“: Endgeräte werden modernisiert, die Topologie wird erweitert, einzelne Arbeitsplätze werden verlegt oder ganze Abteilungen ziehen um. Die Erfahrung zeigt, dass ca. 40 % aller Mitarbeiter einmal jährlich von einem Umzug betroffen sind.

Das lässt sich störungsfrei nur verwirklichen, wenn zu jeder Zeit der Netzwerkstatus eindeutig ist. Das setzt ein sauberes Port-Management voraus. Die Sicherheitskomponenten müssen für das autorisierte Personal schnell zu installieren, zu ändern oder nachzurüsten sein – ohne grosse De-Installationen.

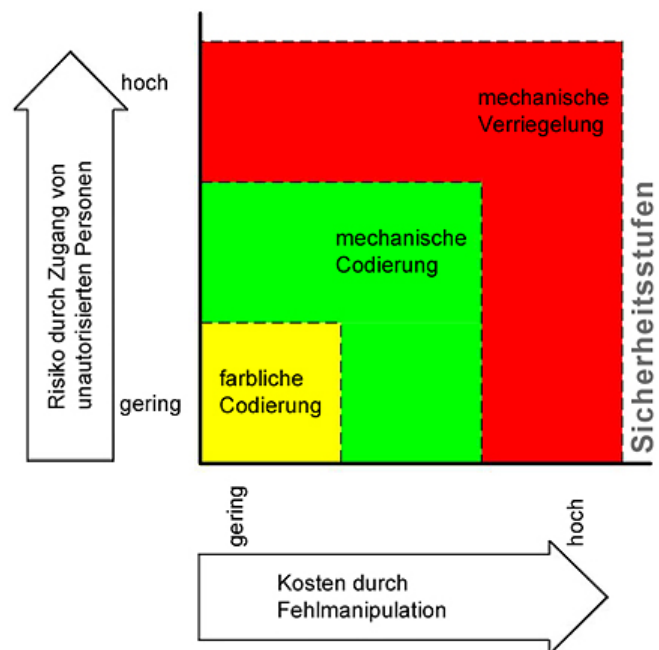
6. Schon bei der Planung die Weichen stellen

Bei der Wahl eines Verkabelungssystems für ein lokales Datennetz muss man besonders auf diese Aspekte achten, wenn man die genannten Fehlerquellen nachhaltig ausschliessen will. Auch wenn in einer ersten Ausbaustufe der Installation noch keine mechanischen Sicherheitsprodukte eingesetzt werden, sollte man sich die Möglichkeit der einfachen Nachrüstung für die Zukunft offen halten.

Nebenstehend eine Orientierungshilfe für die Planung der Sicherheit im LAN. Zwei Aspekte sind entscheidend für die Auswahl der Sicherheitsprodukte: einerseits die möglichen Kosten, die im Falle eines Netzerkausfalls entstehen können; andererseits die Möglichkeit einer Einflussnahme durch unautorisierte Personen. Je nachdem wie hoch diese Faktoren zu gewichten sind, können die Sicherheitsstufen und entsprechende Produkte bestimmt werden.

R&M hat sich mit dem Thema Sicherheitslücken im LAN intensiv auseinandergesetzt. Die daraus abgeleiteten Entwicklungen sind in ein modulares System eingeflossen, das mögliche Sicherheitslücken in einem lokalen Datennetz weitestgehend schliesst.

Mehr darüber finden Sie unter
www.rdm.com



Orientierung für die Sicherheitsplanung. Je leichter unautorisierte Personen Zugang zu Netzwerkanschlüssen haben und je riskanter Netzerkausfälle für das Unternehmen sind, umso höher sollte die Absicherung gewählt werden.
Grafik: R&M