IT-Sicherheitsaspekte im Münchner Wissenschaftsnetz (MWN)

Victor Apostolescu
E-Mail: apo@lrz.de Tel.: 089 /289-28739

Gliederung

Aktuelle Sicherheitslage im MWN

- Das MWN
- derzeitige Policy
- Bericht zur aktuellen Lage

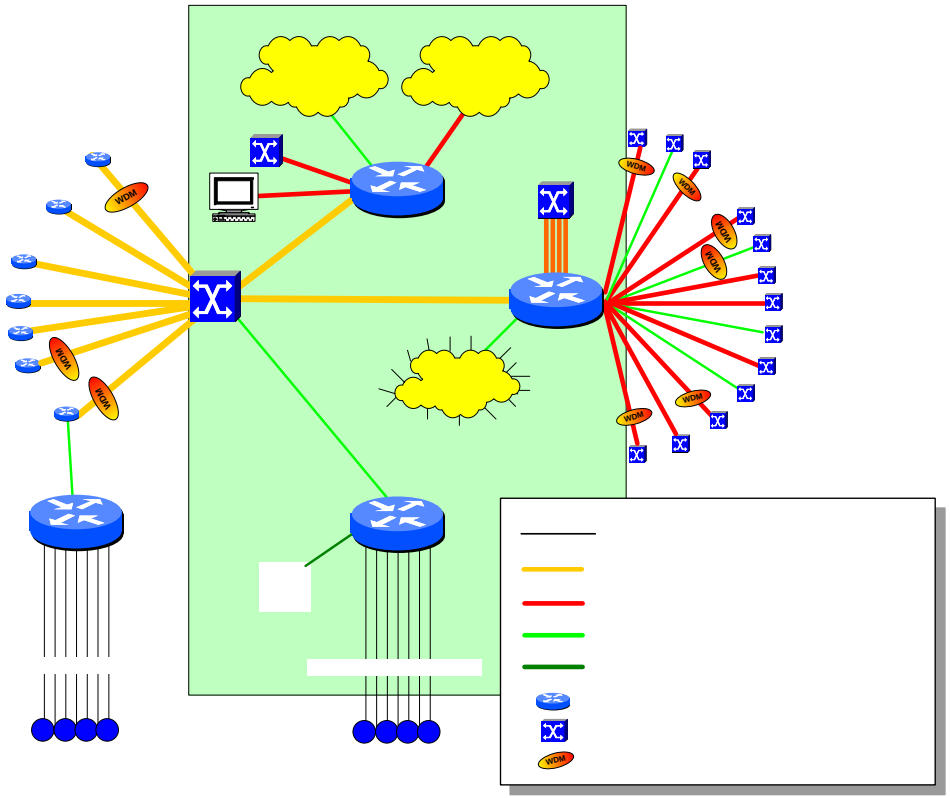
Wo sind die Fronten (Bedrohungsanalyse und "Angebote" des LRZ)

- Systemsicherheit (Updates, mobile Clients, ...)
- Anwendungssicherheit (Spam, Würmer und sonstige Schädlinge)
- Netzsicherheit (insb. bei konvergenten Netzen)

Wohin müssen und sollten wir kommen (Das Ziel)

- Managementwerkzeuge zur Überprüfung des "Zustandes" von Rechnern
- Managementwerkzeuge für eine verteilte "Netzsicherheit („virtuelle Firewalls)
- Validierung des Sicherheitsstatus (IDS / IPS-System)
- Sicherheitsrichtlinien (für Netze und Systeme)

Das MWN
- einige Fakten



In München ist alles etwas „größer“

- ❑ Mehr als 5 Hochschulen
- ❑ Etwa 30 Institutionen
- ❑ Mehr als 700 Institute
- ❑ Mehr als 60 Areale
- ❑ Mehr als 220 Gebäudekomplexe
- ❑ Ca. 100.000 Nutzer (potentiell)
- ❑ Mehr als 50.000 Rechner
- ❑ Mehr als 30 Studentenwohnheime
- ❑ Mehr als 400 „Router-Interfaces“
- ❑ 10 GBit/s Ethernet-Backbone
- ❑ 1 GBit/s G-WiN-Anschluss
- ⇨ **Aber auch nur beschränkte Personalkapazität vorhanden**

Aktuelle Sicherheitspolicy im MWN - Netzseitige Schutzmaßnahmen

- **Policy: „Alles ist erlaubt, was nicht explizit verboten ist“**
- **proaktiv**
  - Paket-Filter am G-WiN Zugang (Sperren „bekannter“ Ports)
  - beschränktes Angebot an Firewall-Funktionalität auf LRZ-Router
  - logische Gruppierung der Netzinfrastruktur (VLANs)
  - Nutzung privater Adressen
  - Authentifizierungspflicht (VPN für mobile Nutzer)
  - Schulung von Nutzern und Netzverantwortlichen
- **reaktiv (Monitoring am G-WiN-Zugang)**
  - „Accounting“ („Spitze des Eisbergs“)
    - Identifikation von „Großverbrauchern“
    - Port-Scan-Aktivitäten („halbautomatisch“)
    - Direkte Mail-Verbindungen ins Internet (Spam-Versand, „halbautomatisch“)
  - Intrusion Detection System (IDS) mit automatischer Sperre
    - FTP-Server auf „Nicht-Standard-Ports“

Aktuelle Sicherheitspolicy im MWN - Systemseitige Schutzmaßnahmen

- **Rezentralisierung der Serverlandschaft, Dienste konzentrieren (ggf. ins LRZ auslagern)**
  - Mailserver mit automatischer Virenerkennung und Spam-Markierung
  - WWW-Server, Name-Server, DHCP-Server, ...
- **Zentrale Betreuung von Servern und Arbeitsplätzen in Instituten**
  - Konzentration auf Fakultätsebene erfolgreich
  - Zentral im LRZ geringer Erfolg, da Anforderungen zu heterogen (betreuungsintensiv)
- **Betrieb eines zentralen Software-Update-Servers (Microsoft „SUS-Servers“)**
- **Campus-Lizenzen für „nützliche Helfer“**
  - Landeslizenz für Viren-Scanner, Betrieb eines Remote-Update-Servers (Sophos Anti-Virus)
  - Personal Firewalls (Standard bei Windows-XP, Rest in der Untersuchung)
- **Ausbildung der Nutzer und Systemadministratoren**

Aktuelle Sicherheitspolicy im MWN - Allgemeine Aktivitäten

- **Bewusstseinsbildung der Nutzer („Steter Tropfen höhlt den Stein")**
  - Veranstaltungen in Verbindung mit den Instituten
  - Sensibilisierung durch aktuelle Vorfälle (u.a. SQL-Slammer, W32.Blaster, ...)

  http://www.lrz.de/services/security/motivation/

- **Kurse, Beratung, Ausbildung, Infos**
  - Einführungskurse zu Sicherheits-Thematiken auch vor Ort

  http://www.lrz.de/services/security/lrz-dienste/

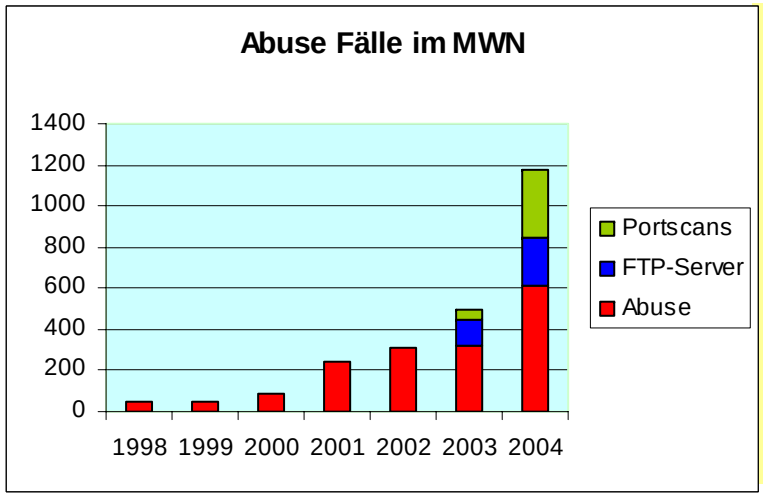
- **MWN-CERT („Computer Emergency Response Team“)**
  - Werkzeuge teilweise im Vorfeld implementiert
  - Personal fehlt (noch)
  - noch ein Traum, bei anderen bereits Realität (RUS-Stuttgart, Bayern CERT, CERT-BW, …)

Sicherheit
– ein ernstzunehmendes Thema

Erster „bewusster“
Sicherheitsvorfall am 1. April 1995

Abuse-Fälle im MWN

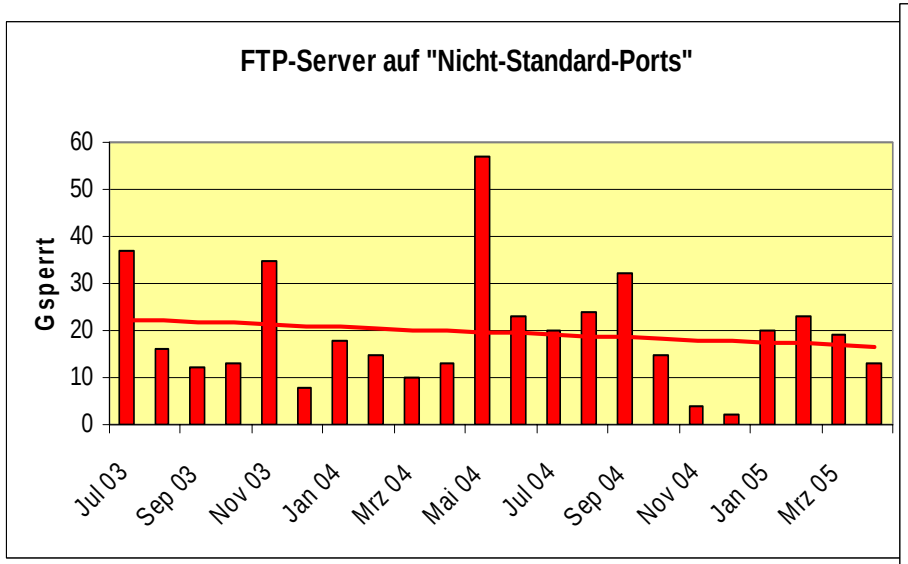
- **Arten von Abuse-Fällen :**
  - gehackte oder mit Würmern (seltener Viren) infizierte Rechner
  - (Un)berechtigte (Spam-)Beschwerden
  - Copyright-Verletzungen (externe Hinweise)
  - Hinweise und Anfragen von MWN-Benutzern
  - Fehlverhalten von MWN-Benutzern (absichtlich und unabsichtlich)
- **Zahl der bearbeiteten Vorgänge**

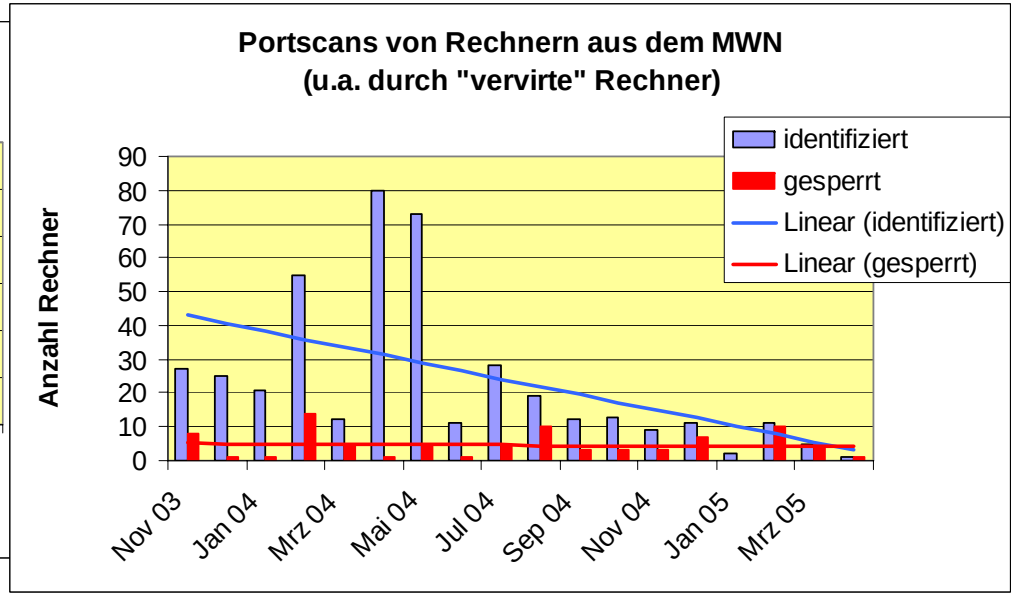


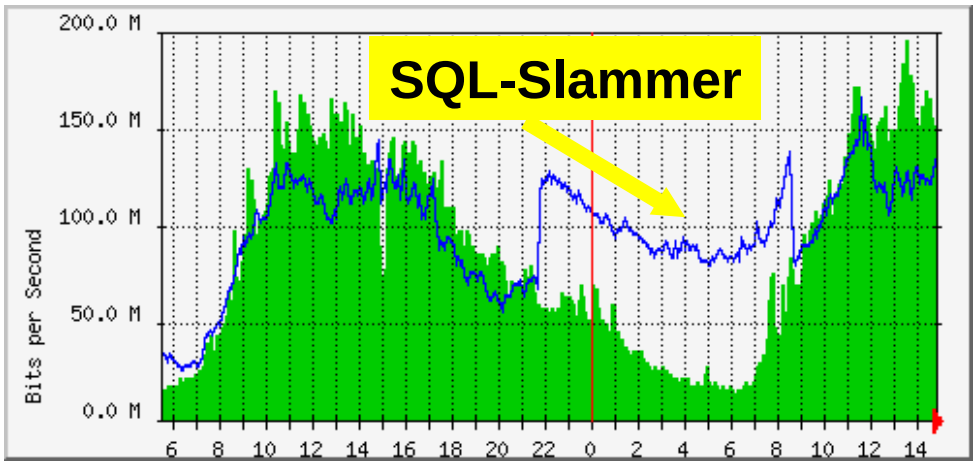
2004

27 Copyright-Verletzungen
74 Spam-Versand (externe Info)
38 Spam-Versand (autom. erkannt)
108 Spam-Beschwerden (unber.)
155 Wurm-Infektionen
231 FTP-Server (autom. erkannt)
331 Portscans (autom. erkannt)

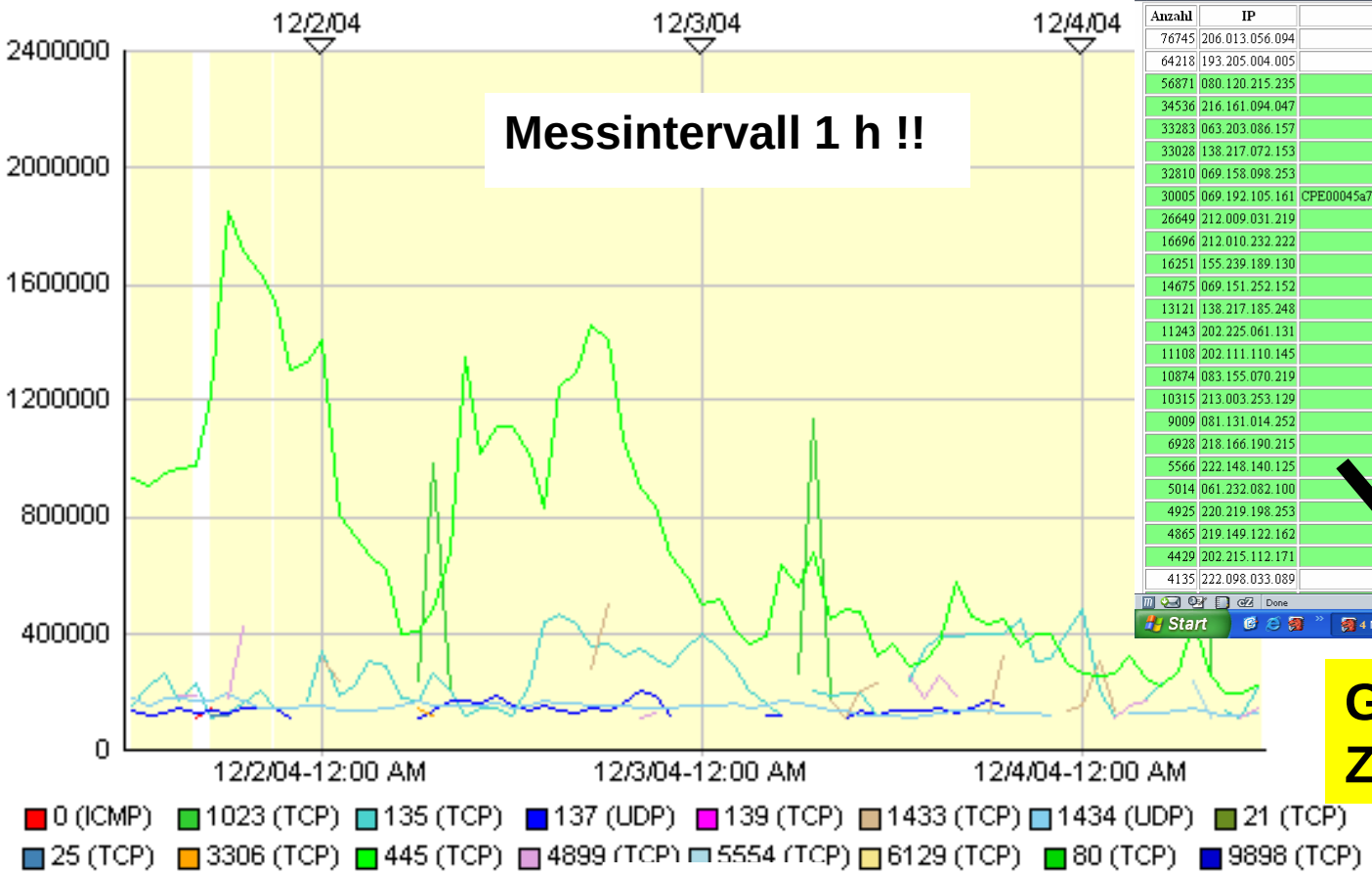
Statistiken („das reale Leben“)
- FTP-Server und Portscans ausgehend

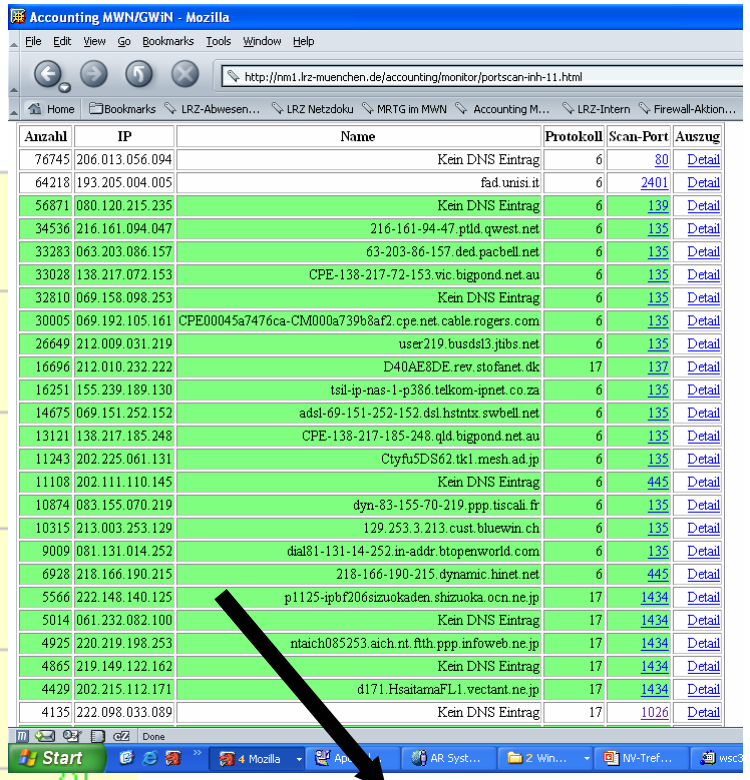






Statistik
- Portscans eingehend





Grün: am G-WiN-Zugang geblockt!!

Statistiken
- Mailversand : Spamerkennung

Die Fronten
- netzseitige Sicherheit

- **„Fehlen“ einer globalen Sicherheitspolicy für das MWN**
- **Firewall-Lösungen für einzelne Institute**
  - (Einfacher) Paketfilter am G-WiN-Übergang ist nicht ausreichend
    - Portsperren, Anti-Spoofing, Einschränkung der Dienstnutzung
  - Firewall am Backbone-Router zum Institut
    - LRZ-Warenkorb deckt derzeit nur 5-10% der Nutzerwünsche ab
  - Eigene Firewall für Institut bzw. Institution
    - **LRZ:** Administration und Konfiguration der Netzkomponenten, Beratung des Instituts bzgl. Policies und Hardware
    - **Institut:** Betreuung und Betrieb der Firewall

Problematisch wegen

- ⇨ **Kontinuität der Betreuung,**
- ⇨ **Teilweise unzureichendes Know-how und**
- ⇨ **zukünftiger Konvergenz der Netze (Daten u. Sprache)**

Die Fronten
- system- und anwendungsseitige Sicherheit

- **Schwächen in Betriebs- und Anwendungssystemen erfordern permanente Updates**
  - ⇨ Permanente Schulung und Automatisieren wichtiger Vorgänge
- **Fehlendes Know-how und Kontinuität der Systemadministratoren**
  - ⇨ Permanente Schulung und Zentralisierung des Supports
- **Mangelhaftes Sicherheitsbewusstsein und Ohnmacht der Endnutzer**
  - ⇨ Permanente Schulung

- **Mobile Nutzer (z.B. Notebooks) wandern zwischen „Sicherheitszonen“**
  - Policy für das MWN gefordert
  - Überprüfung des Zustands eines Rechners (noch) nicht standardisiert
  - Separierung sehr problematisch, kaum durchsetzbar und überwachbar
  - Identifikation, Benachrichtigung einzelner Nutzer sehr schwierig

Sicherheit, ein weiter, endloser Weg ... - die nächsten Schritte (1)

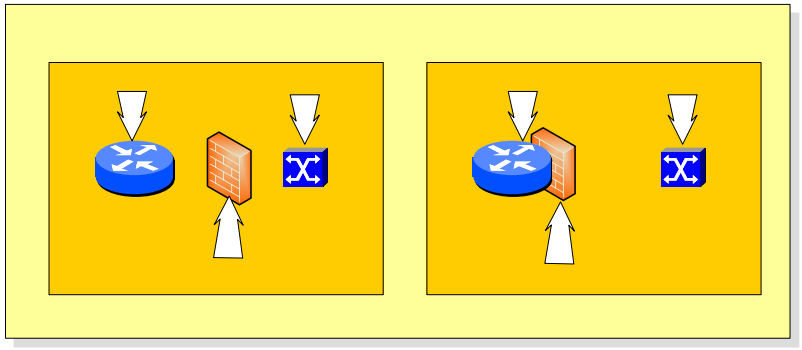
- **Generelle Authentifizierungspflicht am „Netzrand“ (802.1x)**
  - Funktionalität in den Endsystemen gegeben (90-95%)
  - Funktionalität in den Netzkomponenten (Rest)

- **Managementwerkzeuge zur Überprüfung des Zustandes eines Rechners**
  - (pro)-aktive Überprüfung von Rechnern auf Systemschwächen wie z.B. Nessus ….
  - Zugang zum Netz nur nach Überprüfung des Sicherheits-Zustands
    - Cisco Network Admission Control (NAC)
    - Microsoft Network Access Protection (NAP)
    - ...

- **(Re-)Zentralisierung von Server-Diensten (z.B. IntegraTUM)**
  - Web-Server (Schutz der Corporate Identity)
  - Mailserver, ….

Sicherheit, ein weiter, endloser Weg ... - die nächsten Schritte (2)

- **Übergang zu „virtuellen Firewalls“**
  - flexible, dezentrale Konfiguration (Template-Konzepte, Mandantenfähigkeit)
  - Zentraler Betrieb auf der Backbone-Router-Infrastruktur (HBFG 2005)



- **Intrusion Detection/Intrusion Prevention (IDS/IPS)-Aktivitäten**
  - Mehr Signaturen („as much as possible“)
  - Reaktion auf aktuelle Incident-Meldungen (CERT)
  - Zentraler Betrieb auf der Backbone-Router-Infrastruktur (HBFG 2005)

- **Schritte auf dem Weg zu einer geänderten MWN Policy : „Was nicht explizit erlaubt ist, ist verboten“**

Das Ziel:
globale Sicherheitspolicy für das MWN (1)

Probleme bei der Aufstellung einer globalen Sicherheits-Policy

- **Anzahl der Institutionen**
  - ⇨ Abstimmung, ein langer (mühsamer?) Weg durch die Instanzen
- **Freiheit der Wissenschaft („offener Ansatz“)**
  - ⇨ Das hat sich aufgrund der Ereignisse der letzten Zeit deutlich gebessert, aber ....
- **Manpower im LRZ als Dienstleister (derzeit ca. 2-3 Personen)**
  - ⇨ Daran wird sich nichts ändern
  - ⇨ Gemeinschaftsaufgabe der am MWN-beteiligten Institutionen

Rechtliche Problematik allgemein

- ⇨ Datenschutz, Personalräte, ….
- ⇨ Hier erfolgt derzeit Abstimmung mit der DFN-Rechtsstelle

Das Ziel:
globale Sicherheitspolicy für das MWN (2)

Arbeiten hierfür sind (trotzdem) im Gange

- ⇨ **Was tun andere vergleichbare Institutionen?**
- ⇨ **Konzeptarbeiten propagieren (Firewallkonzept für das MWN)**
- ⇨ **Pilothafte Lösungen im Produktionsbetrieb testen**
- ⇨ **Flankenhilfe des BSI (Bundesamt für die Sicherheit im Informationswesen)**
- ⇨ **Überzeugungsarbeit bei den Entscheidungsträgern**