Dienste von Universitätskliniken für Forschungsnetze
am Beispiel des Mainzer IMBEI

Berlin, 11. Dezember 2006

Prof. Dr. Klaus Pommerening
Universität Mainz,
Institut für Medizinische Biometrie, Epidemiologie und Informatik

Was brauchen medizinische Forschungsnetze
und wie können medizinische Rechenzentren ihnen dabei helfen?

Hier: Im Hinblick auf IT-Sicherheit.

Dienste für Forschungsnetze

- Architektur eines Forschungsnetzes: Datenbanken, TTP-Dienste
- Typische Datenbanken
  - Studiendatenbank,
  - Forschungsdatenbank,
  - Bilddatenbank,
  - Register, ...
- Typische TTP-Dienste („Trusted Third Party“):
  - PID (Identitätsmanagement),
  - Pseudonymisierung,
  - Nutzerverwaltung/Directory,
  - Qualitätssicherung,
  - ...
- Realisiert als (Web-) Services
  - Techniken: http, Java, SOAP, ...

Sicherheitsanforderungen an Dienste

- Vertrauenswürdige Dienstleister und Server
  - Dienstleister: vertragliche Einbindung, Policies, SOPs
  - Server: IT-Sicherheit
- Gegenseitige starke Authentisierung
  - Nutzer zu Server
  - Dienst zu Dienst
- Verschlüsselte Kommunikation

Sicherheitsanforderungen an Server

- Sichere Aufstellung
- Serverhärtung
- Nur wirklich benötigte Dienste ansprechbar.
- Web-Server mit SSL (Authentisierung, Verschlüsselung)
- Administrator-Kennung nur für Administrator-Aufgaben.
  - Keine Anwendungsprogramme.
  - Sichern des Administrator-Passworts, keine Passwortsperre.
  - Keine Administrator-Anmeldung über das Netz (außer verschlüsselt mit SSH.)
  - Server nicht als Arbeitsplatzrechner verwenden.

Betreuung eines sicheren Servers erfordert gründliches Know-How und Sorgfalt!

Beschlagnahmeschutz

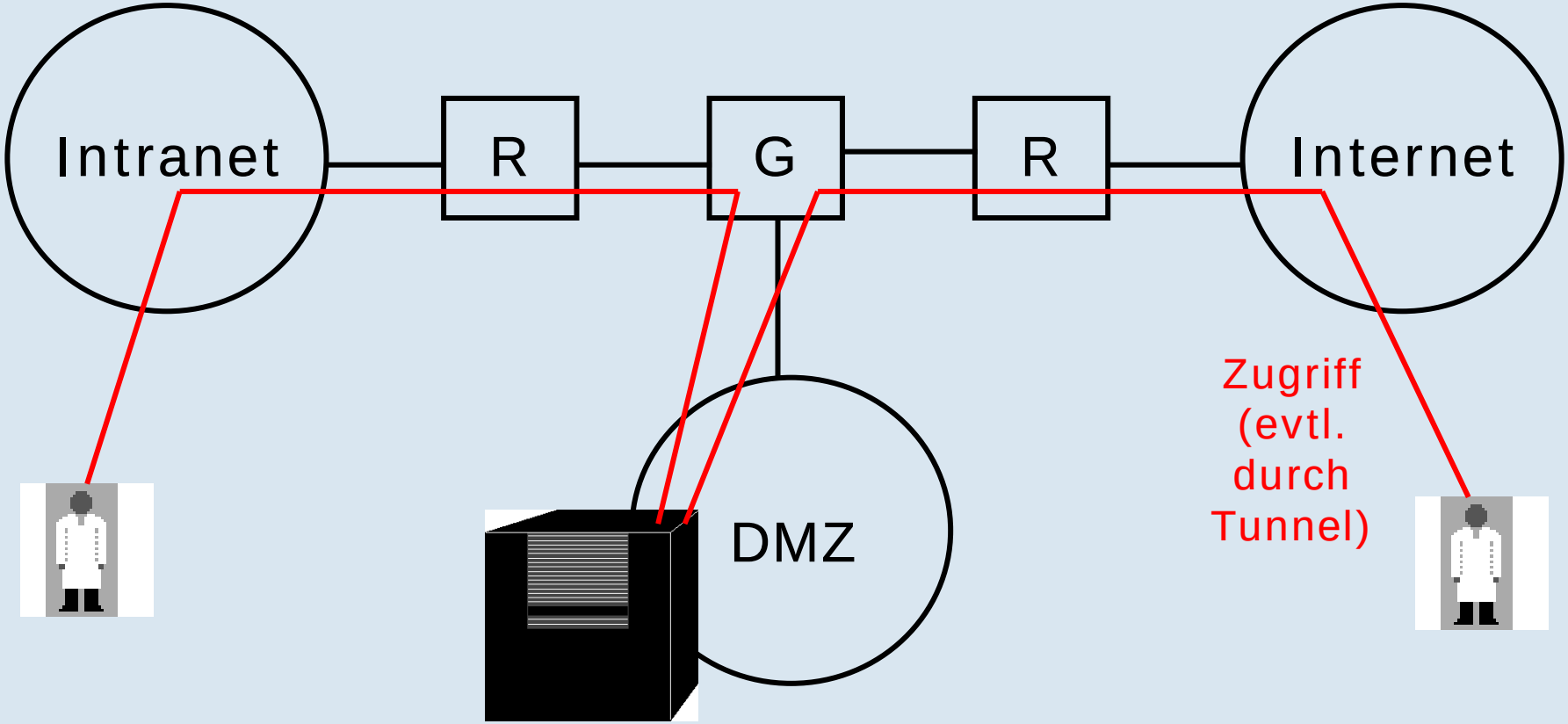
- Theoretisch perfekt, praktisch schwerfällig und nicht sicher vor Übergriffen: Hinterlegen von Daten beim Notar.
  - Fraglich: Gilt das auch für beim Notar aufgestellte Server?
- Weniger perfekt: Beschlagnahmeschutz für Patientendaten nur im Behandlungskontext, und auch dort fragil („versehentliche“ Beschlagnahme)
  - Klinik-RZ nur beschlagnahmesicher für Patientenakten der Klinik, nicht für Forschungsdaten
- Praktisch: Informationelle Gewaltenteilung
  = verteilte Speicherung an unabhängigen Orten,
  z. B. in medizinischen Rechenzentren in verschiedenen Bundesländern
  - Beschlagnahme müsste an vielen Orten koordiniert passieren,
  - ... und dann fehlt noch ein Schlüssel.

Sicherheitsausstattung eines RZ-Maschinensaals

- Zugangssystem mit Protokollierung
- Einbruchsicherheit
- Tresor intern und extern (feuerfest)
- Ausfallsicherheit, z. B. USV, Klimaanlage
  - 7x24- oder 5x8-Stunden-Bereitschaft
- Katastrophenvorsorge
  - Brandmelder, Warnanlagen
  - Löschsysteme
  - Fernüberwachung
- Backup-Konzept
  - mit Auslagerung
- Vernetzung über mehrstufige Firewall-Systeme
  - Paket-Filterung im Router
  - Anwendungsfilter im Proxy/Gateway
  - „Personal Firewall“ völlig ungeeignet.

Firewall-Konfiguration nach dem Stand der Technik

- Router (R) – Gateway (G) – Router (R)
- Neutrale Zone (Demilitarisierte Zone, DMZ)
- Tunnel für Ende-zu-Ende verschlüsselte Verbindungen



Situation des IMBEI (typisches MI-Institut)

- Universitätsinstitut, im Klinikum angesiedelt
- Eigener Maschinensaal vom RZ-Typ,
  - Nachbarraum zum RZ des IT-Dezernats (zentrale Patientenverwaltung)
  - mit typischer Sicherheitsinfrastruktur
  - 5x8-Stunden-Betreuung reicht i. a. für medizinische Forschungsnetze
- Deutsches Kinderkrebsregister
- Krebsregister Rheinland-Pfalz (Registerstelle)
- Große eigene epidemiologische Studien


DELL
DELL


LAMPERTZ
DATA SAFE


XS

Dienste des IMBEI

- IT für Krebsregister und eigene Studien
- Beteiligung an anderen Studien des FB Medizin, insbesondere IT-Unterstützung
- „Hosting“ für andere Projekte des FB Medizin
  - z. B. Skelnet, [KKS]
- Dienstleistungen für das Universitätsklinikum
  - z. B. Kommunikationsserver, Archivserver, [Firewall]
- Dienstleistungen für Forschungsnetze
  - typisch: PID-Dienst für KPOH
  - Nutzer-DB für KPOH mit Verzeichnis, Rechteverwaltung, Mail-Listen, ...