Nutzen und Kosten von IT-Sicherheitsmaßnahmen

W. Held

Zentrum für Informationsverarbeitung

Universität Münster

Hagen, 13.09.2006

Münster, 29.09.2006

Jährliche Kosten der IT

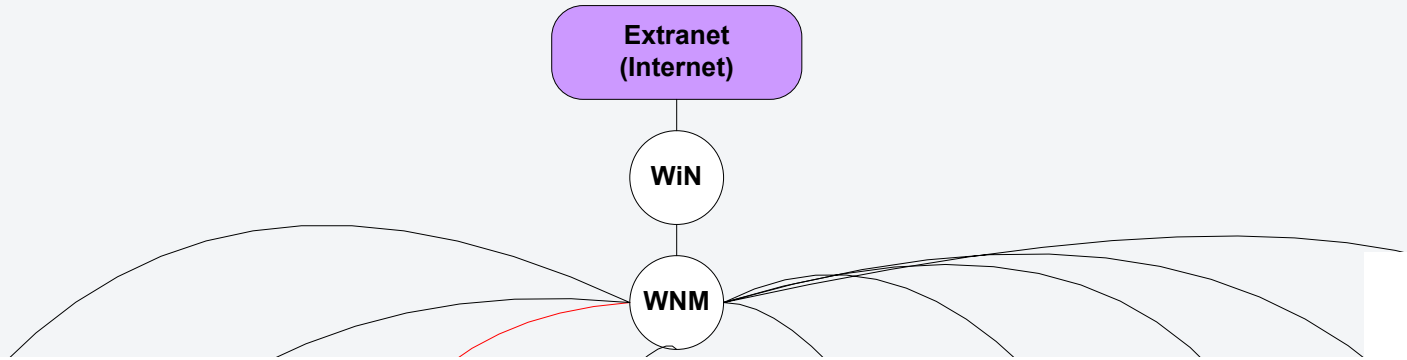
Universität Münster

Studierende	40.000
Netzanschlusspunkte	20.000
Rechner	13.000
Server (ohne Cluster)	500
Server-Redundanz (30 %)	150
Summe Server	**650**

Nebenher Klinikum:

Netzanschlusspunkte	13.000
Rechner	8.000

1. IT und ihre Kosten



1. IT und ihre Kosten

IT-Sachmittel ~ **23** % von Ti 547.94, ohne HBFG für LAN und Geräte	3.600.000 €
IT-Personal ~ **2,5 %** vom Personaletat	3.500.000 €
Summe	**7.100.000 €**

+ HBFG für LAN und Geräte stark schwankend: 1 – 2 Mio. €

2. Schäden und ihre Folgen

Schäden können entstehen durch

- mangelnde IT-Verfügbarkeit
- Verletzung der Integrität und Vertraulichkeit
- Angriffe gegen IT-Sicherheit (**Viren, Hacker, Diebstahl, …**)
- Belästigung durch Spam
- Höhere Gewalt und Ausfälle von Strom und Klima
- Ausfälle und von Hard- und Software
- menschliches Versagen
- Organisatorische Mängel
- …

2. Schäden und ihre Folgen

Schäden können

- **zu Verstößen gegen Gesetze führen**
- **zur Beeinträchtigung körperlicher Unversehrtheit führen**
- **die Aufgabenerfüllung beeinträchtigen**
- **finanzielle Auswirkungen haben**
- **Ruf der Universität schädigen**

Die Spannweite der Schäden ist in jedem Fall sehr groß

Von „ohne nennenswerte Konsequenzen“
bis zur
„schweren Beeinträchtigung der persönlichen Unversehrtheit oder gar bis zur Todesfolge“

2. Schäden und ihre Folgen

Daraus folgt u. a.:

- **Wer IT-Sicherheit vernachlässigt, kann große Schäden verursachen**
- **Wer zuviel für die IT-Sicherheit tut, wird unnötiges Geld ausgeben**

Aber:

- **Wer weiß schon, welcher Schutzbedarf in Universität existiert? Schätzen? Wer? Wie?**
- **Münster:**
  - **Ende 2002: Bericht zum Katastrophenschutz**
  - **Jetzt: Web-basiertes Sicherheits-Audit mit Fragen zu Arbeitsplatzrechnern, Servern, Räumen, Netzen und ihren Komponenten**

Schutzbedarf - Schutzmaßnahmen = Sicherheitslücke

3. Nutzen = Vermeidbare Schäden

- **Exakte Zuordnung der Kosten und des Nutzens nicht möglich, Kosten und Nutzen nicht immer zu quantifizieren**
  Was dient der Abwehr von Angriffen, Verlässlichkeit, Stabilität, Qualitätssicherung, Schäden durch höhere Gewalt?

- **Versuch einer Bewusstseinsbildung**

3. Nutzen = Vermeidbare Schäden

Berechnungs-Grundlagen

1 Personenjahr	47.000 €
Kauf Server	7.500 €
Kauf Arbeitsplatzrechner	1.000 €
Abschreibungszeit für Hardware und Software	5 Jahre
Abschreibungszeit für andere Geräte (USV, Klima, …)	8 Jahre
Abschreibungszeit für Glasfaserkabel	10 Jahre
Arbeitszeiten pro Jahr	220*8 Std

- **Investitionen auf Abschreibungszeiten verteilt, Sachmittel und Personalkosten berücksichtigt**
- **Kalkulationen liegen als Excel-Tabelle vor und können zur besseren Abschätzung der eigenen Situation abgegeben werden**

3. Nutzen = Vermeidbare Schäden

Nutzen von Schutzmaßnahmen, Kosten einiger Schäden, Teil I

Art	€/Jahr
1 Stunde Ausfall des Systems in der Universität (Summe der Einzelausfälle) mit Arbeitsunterbrechung	80.000
1 MJ durch Daten- und Arbeitszeitverlust	47.000
Abbrennen eines Serverraumes (Enschede), Beispiel ZIV 1 Serverraum, 180 Server; 10 % Ausfälle aller 13.000 Rechner in Universität 30 Tage, Wiederbeschaffung und -aufbau der Server 2 Mio. € ; einmal in 20 Jahren	180.000
Summe >	**307.000**

Abbrennen nicht regelmäßig,
Versicherungsmathematische Werte nicht bekannt.
Aber grundsätzliches Risiko.

3. Nutzen = Vermeidbare Schäden

Nutzen von Schutzmaßnahmen, Kosten einiger Schäden, Teil II

Art	€/Jahr
Manuelle Beseitigung von Spam-Mails (585.000 Mails/Tag, 520.000 Spam, 1 sec Arbeit pro Mail), 18 MJ	850.000
Beseitigung von Viren aus Dateien und Neuaufbau der Systeme (20.000/Tag - wir hatten schon 140.000 Viren/Tag -, davon 0,5 % Neuaufbau, 1 Stunde pro System, Rest durch Betriebssysteme und Nutzer abgefangen)	590.000
Diebstahl, Feuer- und Wasserschäden: 10 Arbeitsplatzrechner, 1 Server; ohne Baumaßnahmen	20.000
Schadensersatz bei Missbrauch persönlicher Daten, angenommener Wert	100.000
Vertrauensverlust bei Drittmittel-Gebern 0,5 %	200.000
Summe	**1.760.000**

3. Nutzen = Vermeidbare Schäden

Nutzen von Schutzmaßnahmen, Kosten einiger Schäden, Teil III

Art	€/Jahr
Mangel Verlässlichkeit oder Angriffe → Mangel Akzeptanz → Unzufriedenheit bei Nutzern, Stress bei Mitarbeitern. Wiederherstellung von Servern zwischen 2 Stunden und einigen Tagen, abhängig von der Datenmenge. Ausreichende Redundanz → Rufbereitschaft und Nachtdienst weniger wichtig	Nicht zu beziffern
Ausfall E-Learning: 650 Dozenten, 29.000 Studierende, 300 Nutzer Online (Stand 26.06.06). Ausfall 8 Std. mit je 10 € und zusätzlich Ausfall einer elektronischen Prüfung: 500 Studierende, 2 Stunden, je 10 €, Neue Prüfung vorbereiten 2 Tage des Dozenten:	34.000
Backup: 7,4 Mio Dateien wurden wieder hergestellt, Wert 0,10 €/Datei. Ausfall E-Mail 1 Tag…	1.480.000 Nicht zu beziffern
Summe >	**1.514.000**

3. Nutzen = Vermeidbare Schäden

Pro Jahr:

Kosten Schäden, I	> 0,3 Mio. €
Kosten Schäden, II	> 1,7 Mio. €
Kosten Schäden, III	> 1,5 Mio. €
Summe (mögliches Risiko)	> 3,5 Mio. €

Gesamtkosten der IT /Jahr	~ 8,6 Mio. €

(Inkl. HBFG und LAN)

3. Die Kosten der IT-Sicherheit

Grobe Abschätzung, Fehler sicher 20 %.

a. **Redundanz, Stabilität und Verlässlichkeit des Betriebes, höhere Gewalt**
b. **Sicherheit vor Angriffen (I)** - eindeutige Abwehr von Angriffen
c. **Sicherheit vor Angriffen (II)** - Abwehr von Angriffen und Redundanz
d. **Spam-Ärger**

3. Die Kosten der IT-Sicherheit

a. Redundanz, Stabilität und Verlässlichkeit des Betriebes, höhere Gewalt

Allgemeine Infrastruktur: Alarmierung Feuer und Einbruch, Zugangskontrolle und Einbruchsicherung, Wasserschaden, Unterbrechungsfreie Stromversorgung usw.
Viele kleine Räume deutlich teuerer als wenige größere Räume.
Rechnernetze: Netzmanagement, ohne LAN-Backbone
Server und Arbeitsplatzsysteme: Spannweite der Redundanz von 0 %, über 10 % zukünftig mit VM-Ware, bis zu 30 % (= 150 Server von 650) heute.
Backup und Archivierung
Datenspiegelung: Im 2. Raum (SAN), für spezielle Daten wie File, Backup, Datenbanken. Extreme Datensicherheit. Zeit-Vorteile bei Wiederherstellung verlorener Daten oder bei Katastrophen mit Geräteverlusten.
PKI, Kryptografie, Digitale Unterschrift, Zeitstempel

0 % Server-Red.	10 % Server-Red.	30 % Server-Red.
532.000 €/Jahr	612.000 €/Jahr	762.000 €/Jahr
Fahrlässig	Ziel	Heute

3. Die Kosten der IT-Sicherheit

b. Sicherheit vor Angriffen (I) – eindeutig Agriffe

Organisation: Regelungen in Gremien und Vorarbeiten; Web-Pflege, Ausbildung rudimentär; Sicherheits-Audit
Rechnernetze: Strukturierung/Virtualisierung mit Firewall (Stateless u. Statefull Packet screening), IDS, IPS, VPN, Prüfung Rechner bei Netzzugang, Sicherheit Funknetze
Server und Arbeitsplatzrechner: Virenschutz, Personal Firewall, Host IDS und IPS
Sonstiges: Identitätsmanagement (teilweise), Revision der Sicherheitsanforderungen und der Bestände alle 3 Jahre

288.000 €/Jahr

- VPN (Virtual private network): Sicherer/verschlüsselter Transport von Daten
- IDS, IPS (Intrusion detection/prevention system):
  Überwachung bzw. Verhinderung unerwünschter Datenpakete (Sicherheit)
  IPS-Kosten 32.000 €/ Jahr ↔ CERT-Einsparungen: ~ 80.000 €/Jahr
  CERT (Computer Emergency Response Team): Anlaufstelle bei Missbrauch, Angriffen und Beschwerdefällen, u. a. Begrenzung von Virusinfektionen, Stoppen von Spam, Urheberrechtsverletzungen

3. Die Kosten der IT-Sicherheit

c. Sicherheit vor Angriffen (II) – Angriffe und Redundanz

Personen: System- Netzmanagement (10 %), Backup und Archivierung von Daten (10 %), Technisch Verantwortliche, Administratoren (10 %), CERT

177.000 €/Jahr

d. Spam-Ärger (Betrag ändert sich demnächst)

30.000 €/Jahr

3. Die Kosten der IT-Sicherheit

Zusammenfassung (€/Jahr)

	„0 %“	„10 %“	„30 %“
a. Redundanz, ohne LAN-Backbone	523.000	603.000	753.000
b. Angriffe (I)	288.000	288.000	288.000
c. Angriffe (II)	177.000	177.000	177.000
d. Spam-Ärger	30.000	30.000	30.000
Summe	**1.018.000**	**1.098.000**	**1.248.000**

Mögliche Schäden/Risiken	>	3.500.000
Gesamtkosten der IT	~	8.600.000

In welchem Umfang sichern wir mit (~ 1 Mio. €) die Risiken oder mit welcher Wahrscheinlichkeit treten die Risiken ein?

3. Die Kosten der IT-Sicherheit

Zahlen für andere Universitäten ?

K = Kosten Münster, 40.000 Studierende

- **10.000 Studierende: K*0,31 - nicht: K*0,25**
- **20.000 Studierende: K*0,58 - nicht: K*0,50**
- **30.000 Studierende: K*0,81 - nicht: K*0,75**

3. Die Kosten der IT-Sicherheit

Kostensenkungen durch Kooperationen im RV-NRW sind möglich

- Sicherheits-Audit (Fragestellungen und Web-Struktur)
- IPS, IDS
- Statefull und Stateless Packet-Screening
- Netzzugangssicherung
- Virenschutz
- Spam-Schutz
- Identitätsmanagement
- PKI (public key infrastructure, Kryptografie)

} Werden praktiziert

- …

4. Verantwortung

- **Hochschulleitung und/oder RZ-Leiter?**
- **Fachaufsicht beim RZ, deshalb Verantwortung zunächst dort**
- **Was ist, wenn vom RZ genannte Mängel nicht behoben werden? Dann liegt die Verantwortung sicher nicht beim RZ?**

Vielen Dank !

Hinter der o. a. abgedeckten Folie: