Entwurf einer

IT-Sicherheitsleitlinie

für die Technische Universität Hamburg-Harburg

Motivation – Beispiele 1

- **Microsoft SQL-Server Wurm**
  - Juli 2002: öffentliche Warnungen vor Sicherheitslücke, Update verfügbar
  - Januar 2003: Wurm nutzt Sicherheitslücke aus
  - TUHH Rechner werden infiziert und lassen mehrmals für Stunden unsere Verbindung zum Internet zusammenbrechen

- **Beschwerde der Uni Kassel**
  - System aus der TUHH versucht Sicherheitslücken an der Uni Kassel auszuspähen
  - System wurde für ein Projekt von dritter Seite in einem AB aufgestellt, niemand fühlt sich für das System im AB verantwortlich

- **Missbrauch der Internet-Anbindung**
  - wiederholt fallen Systeme durch sehr hohes Datentransfer-Volumen auf
  - Weiterverbreitung und Download urheberrechtlich geschützter Werke durch private Nutzung oder durch „Hacker“ aus dem Internet
  - Verwendung von „Peer-to-Peer-Software“

Motivation – Beispiele 2

- **Wurm W32/Blaster**
  - Juli 2003: öffentliche Warnungen vor Sicherheitslücke, Update verfügbar
  - 11. August: Wurm W32/Blaster infiziert viele Systeme im Internet, gelangt zunächst aber nicht ins TUHH-Netz
  - 20. August: noch 300 Systeme ohne Update, Warnung des RZ
  - 1. Sept.: W32/Blaster sickert ins TUHH-Netz, 2. Warnung des RZ, noch 200 Systeme ohne Update und infizieren sich gegenseitig
  - Kosten (geschätzt): 1 Manntag pro 20 Windows-Systeme zur Beseitung
  - 6. Oktober: noch mind. 6 infizierte Systeme

- **Virus Sobig-F**
  - Aug/Sept 2003: Virus Sobig-F überflutet das Internet
  - 4. September 2003: von insgesamt 30.000 E-Mails aus dem Internet in das TUHH-Netz wird jede dritte als infiziert zurückgewiesen
  - Virus sickert immer wieder durch z.B. Laptops und Datenträger in das TUHH-Netz

Motivation – Schlussfolgerungen 1

- **Technische Maßnahmen reichen nicht aus, um die IT-Sicherheit zu verbessern**
  - Jedes System für das sich niemand verantwortlich fühlt, stellt eine Gefährdung dar
  - Mangelnde Sensibilität führt zu fahrlässigem und naiven Umgang mit IT
  - Beseitigung von Sicherheitslücken erfolgt nur mit niedriger Priorität
  - Pflegeaufwand für Systeme wird unterschätzt
  - Qualifikation und Information der Mitarbeiter
  - Vertretungsregelungen fehlen

- **Alle diese Ereignisse fallen durch Seiteneffekte und massive Wirkung auf**
  - Dunkelziffer ?!
  - nicht ausreichende Möglichkeiten zur Überwachung und Kontrolle
  - Überwachung und Kontrolle technisch möglich aber datenschutzrechtlich heikel

Motivation – Schlussfolgerungen 2

- **IT-Sicherheit muss als Ziel durch die Hochschulleitung festgelegt werden**
  - sonst gehen Entscheidungen immer zu Lasten der IT-Sicherheit
- **Verantwortlichkeiten für die IT-Sicherheit müssen festgelegt werden**
  - sonst ist IT-Sicherheit immer ein Problem „der anderen“
- **Die Aufgabe „IT-Sicherheit“ muss definiert und zugewiesen werden**
  - sonst bleiben Systeme ungepflegt und ohne Schutz
- **Kompetenzen müssen festgelegt werden**
  - sonst können Maßnahmen nicht durchgesetzt werden

IT-Sicherheitsleitlinie

IT-Sicherheitsleitline

- **Festlegung einer IT-Sicherheitsleitlinie wird durch das *Bundesamt für Informationstechnik* für alle Behörden und Unternehmen empfohlen**

- **Beispiele an anderen Hochschulen:**

  - Uni Hannover: Ordnung zur IT-Sicherheit
  - Uni Erlangen: Leitlinie und Einrichtung IT-Sicherheitsmanagement
  - TU Braunschweig: Ordnung zur IT-Sicherheit

- **IT-Sicherheitsleitlinie soll Ziele und Organisationsstrukur (IT-Sicherheitsmanagement) festlegen**

- **2. Schritt (später): Regelwerk zur Nutzung der Netz-Infrastruktur als Erweiterung der Benutzerordnung für das Rechenzentrum**

- **Verantwortung liegt bei der Leitung des Arbeitsbereiches/Einrichtung**
  - Nur Vorgesetzte können Ressourcen verteilen und Maßnahmen durchsetzen
  - Aufgabe „IT-Sicherheit“ wird an „dezentrale IT-Sicherheitsbeauftragte“ delegiert

- **Aufgaben der „Dezentralen IT-Sicherheitsbeauftragten“**
  - Beratung der Leitung und Anwender
  - Kontrolle der Systeme und Einhaltung von Maßnahmen
  - Kommunikation mit dem zentralen IT-Sicherheitsbeauftragten

- **Studentische Einrichtungen**
  - weitgehend analog zu Arbeitsbereichen

- **Aufgaben der „Zentralen IT-Sicherheitsbeauftragten“**
  - übergreifende Bedrohungen analysieren
  - übergreifende Maßnahmen ausarbeiten, vorschlagen und ggf. technisch durchsetzen
  - Information, Empfehlungen, Beratung und Weiterbildung
  - Koordination
  - Kontrolle, Überprüfungen und Gefahrenabwehr
- **Aber:**
  - übergreifende technische und organisatorische Maßnahmen müssen durch die Leitung der Universität verbindlich beschlossen werden, sonst sind diese nicht durchsetzbar

- **Kosten durch Schäden**
  - Internet-Kosten durch übermäßige private Nutzung, verlorene Arbeitszeit
  - Beseitigung von Computerviren und Würmern
  - Neuinstallation kompromittierter Systeme
  - Behinderung der bestimmungsgemäßen Nutzung kostet Arbeitszeit
    - Beispiel: (Ende September) 5 Tage Netzwerkstörung DE15/DE17
  - Weiterverbreitung vertraulicher Informationen (z.B. NDA)
  - Ansehensverlust ?

- **Kosten für die Arbeitsbereiche und Einrichtungen**
  - Abhängig vom Umfeld und Qualifikation der Mitarbeiter
  - Ziel: nicht mehr als 10 – 30 Minuten Arbeitszeit pro Woche und System
    - Weiterbildung und Qualifikation der Mitarbeiter
    - Einspielen der Sicherheitsupdates
    - Beratung und Kontrolle
    - Reaktion auf Sicherheitsvorfälle

IT-Sicherheit – Technische Maßnahmen

- **Strategie: „defense in depth“ und „containment“**

- **Computerviren:**
  - Automatische Filterung auf Computerviren für eingehende und abgehende Email
    - siehe: http://www.tu-harburg.de/rzt/net/public/dienste/mail/virus.shtml
  - Automatische Kennzeichnung von Werbemails (Spam) im Probebetrieb
    - siehe: http://www.tu-harburg.de/rzt/net/public/dienste/mail/spam/
  - Campusweite Lizenz (mit erlaubter Privatnutzung) für Anti-Virus Software und stündliche Verteilung neuer Virenmuster
    - http://www.tu-harburg.de/rzt/it-sicherheit/computerviren/sophos.html

- **Internet-Firewall (im Aufbau)**
  - Abwehr von einfachen Angriffen aus dem Internet
  - Erzwingen einer Registrierung für öffentlich angebotene Dienste

- **Arbeitsbereich-Firewall (im Aufbau)**
  - Angebot der Dienstleistung „Firewall“ an Arbeitsbereiche, um diese vom TUHH-Netzwerk zu entkoppeln