Sicherheit allgemein

Markus Krieger

Rechenzentrum Uni Würzburg

krieger@rz.uni-wuerzburg.de

Einführung

- Ziel der Veranstaltung
- Definition von Sicherheit und Gefahren
- Denkanstöße
- Angreifer, Angriffsmöglichkeiten & Motivationen
- Schritte eines erfolgreichen Angriffs
- Das Hochschulnetz
- Suche nach einer Strategie
- Sicherheit - warum und wieviel

Ziel der Veranstaltung

Was soll erreicht werden?

- Definition und Diskussion der wichtigsten sicherheitsrelevanten Problemstellungen.
- Was verbirgt sich hinter diversen Schlagwörtern?
- Wo sind die wesentlichen Sicherheitslöcher?
- Wie sehen erste Schritte aus, um die Sicherheit zu verbessern?
- Vorstellung von Utilities zur Verbesserung der Systemsicherheit.
- Informationen und Angebote des RZ zur Steigerung der Systemsicherheit.

Ziel der Veranstaltung

Was wird nicht erreicht?

- Ein ausgereiftes Sicherheitskonzept.
- Konkrete und genau definierte Schritte was zu tun ist.
- 100% sichere Rechner an der Universität.

Praktische Definition von Systemsicherheit

„Ein System ist sicher, wenn es sich so verhält wie man es von ihm erwartet. D.h. es erledigt die ihm übertragenen Auf-gaben und macht keine ungewollten Aktionen “

Sicherheitsansprüche von Benutzern / Administratoren:

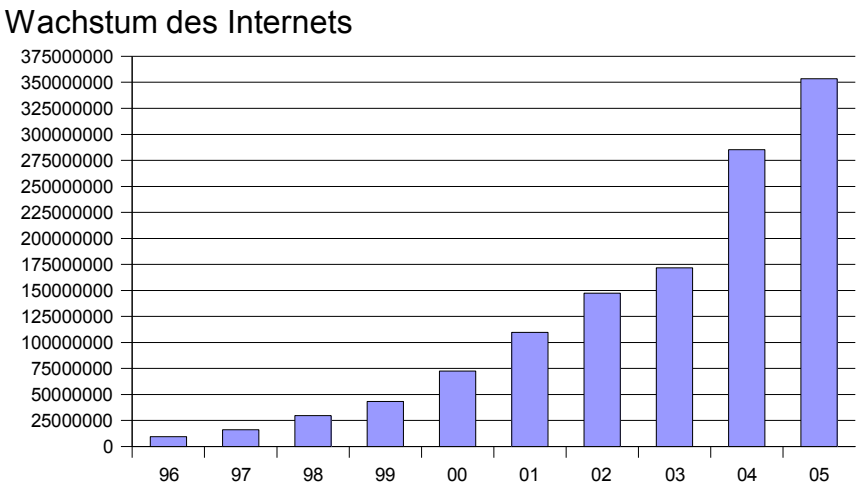
- Integrität von Daten und Programmen
- Verfügbarkeit
- Konsistenz
- Zugriffskontrolle
- Auditing

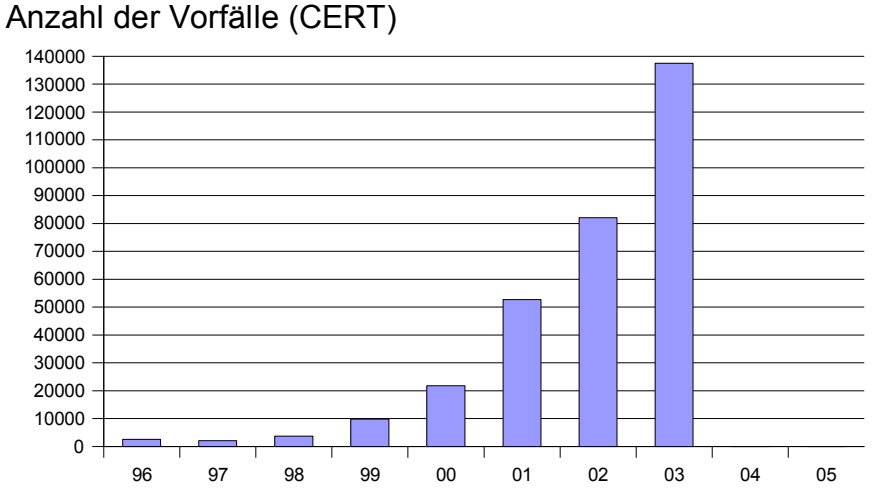
Gefahren für die Sicherheit

- Hardwarefehler
- Softwarefehler
- Fehler von Benutzern / Administratoren
- Äußere Einflüße (Feuer, Diebstahl, ...)
- Angriffe von Innen und von Außen

Dies führt zum Verlust von Integrität, Verfügbarkeit und Vertraulichkeit.

Denkanstöße

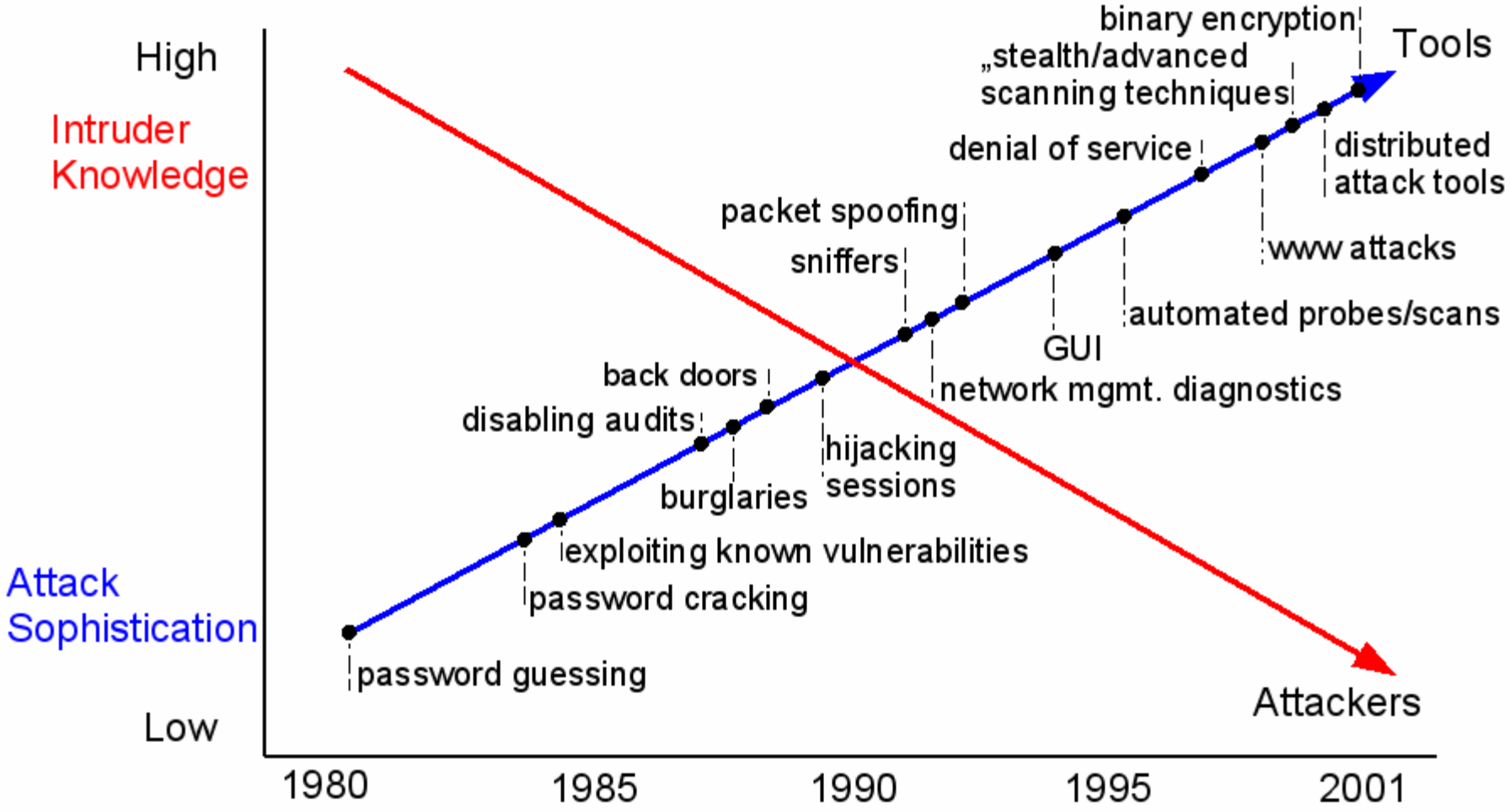




Überlegungen

- Was gibt es für Angriffe?
- Woher kommen die Angriffe?
- Wer greift mich an und warum?
- Wie wichtig sind die Daten meiner Rechner?
- Was kann ich tun und woher bekomme ich Know-how und Informationen?
- Kann ich verantwortlich gemacht werden?

Aufwand eines Angriffs



Angriffsmöglichkeiten

- Lokale / Remote Angriffe
- Trojaner / Viren / Würmer / Backdoors
- Buffer Overflow
- Code Injection
- Falsche Berechtigungen für Dateien / Verzeichnisse
- Fehlerhafte Umgebungsvariablen
- Trust Exploitation (ip-spoofing, hijacking, ...)
- Condition Race
- (D)DOS
- Passives Sniffen

Angreifer

- lokale Angreifer:
  - Studenten
  - Mitarbeiter
  - Erfolgreiche remote Angreifer ohne Root-Privilegien
- remote Angreifer:
  - Kriminelle
  - Hacker
  - Script Kiddies
  - Würmer

Motivation der Angreifer

- Spieltrieb / Neugier
- Zugriff auf Daten / Dienste
- Bandbreite
- Plattenplatz
- CPU für „distributed computing“
- Sprungbrett für weitere Angriffe
- Demonstration von Macht und Können
- Finanzielle Interessen
- Das Hochschulnetz ist offen und die Rechner sind schlecht gesichert

Schritte eines erfolgreichen Angriffs

- Sammeln von Informationen (Scannen nach OS / Diensten, DNS, ...)
- Informationen nach Verwundbarkeiten durchsuchen
- Zugang zum System verschaffen
- Einsatz von exploit-Scripten für root-Rechte
- Installieren von Backdoors, Sniffern und Rootkits und Verwischen von Spuren
- Ausnutzen des Systems für Keylogging, DDOS, ...

Alternativ: Ausnutzen von Fehlern in Clientprogrammen durch manipulierte Webseiten oder Dateien (Bilder, Filme, PDF, ...)

Uni-Rechner als beliebte Ziele

- Heterogene Umgebung macht zentrale Absicherung schwierig
- Viele Insellösungen erschweren Pflege/Diagnose
- Bieten die optimale Anbindung ans Internet
- Laufen oft in einer Defaultinstallation und sind somit angreifbar
- Heterogene Ansprüche/Applikationen bieten viele Möglich-keiten der Fehlkonfiguration durch den Administrator/Benutzer
- Arbeit geht vor Sicherheit
- Lange Laufzeiten
- Feste IPs

Suche nach einer Strategie

- Erhöhung der lokalen Sicherheit durch Vorsorgemaßnahmen
  - Physische Sicherheit des Rechners und Netzzuganges
  - Regelmäßige Backups
  - Einspielen aktueller Patches und deaktivieren nichtbenötigter Accounts / Dienste
  - Aktivierung von effektivem Logging
  - Weitergabe von Sicherheitsinformationen
  - Einsatz von Tools um die Rechnersicherheit zu überprüfen und um die Grundlage zur Erkennung von Sicherheitsproblemen zu schaffen
  - Einsatz von Kryptographie
  - Führen eines Logbuchs

Suche nach einer Strategie

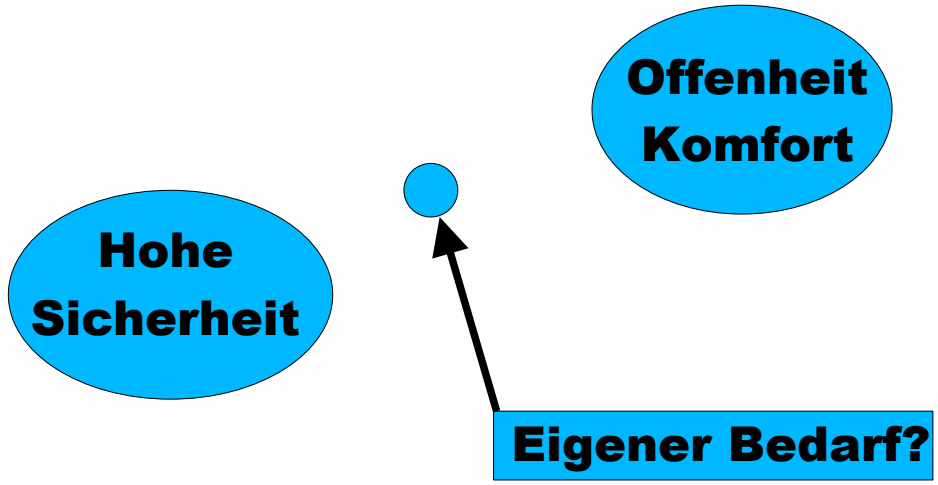
- Erkennen sicherheitsrelevanter Vorfälle
  - Auswerten von Logdateien
  - Regelmäßiges Überprüfen der Rechnerkonfiguration (Dienste und Dateisystem)
  - abnormales Verhalten (Abstürze, hohe Last, ...)
  - externe Informationsquellen (IDS, Meldungen)
- Problematisch dabei:
  - Ist der Rechner gehackt, läßt sich der Zustand mit Bordmitteln nicht mehr verläßlich überprüfen.

Suche nach einer Strategie

- Reagieren auf einen Vorfall
  - Ruhe bewaren! Durch voreiliges Handeln kann sonst mehr Schaden als durch den eigentlichen Vorfall angerichtet werden.
  - Befolgen von vorhandenen Sicherheitsrichtlinien
  - Sicherung von Spuren
  - Wiederherstellung des Sollzustands
  - Analyse und Suche nach weiteren betroffenen Rechner im lokalen Netz
  - Meldung an Rechenzentrum / Rechtsabteilung / Provider / CERT (Koordination / Strafverfolgung)

Sicherheit - warum und wieviel?

- PRO hohe Sicherheit
  - Schutz der eigenen Ressourcen
  - Erhaltung der Verfügbarkeit
  - Schutz der Vertraulichkeit
  - Verhinderung von Mißbrauch
  - Rechtliche Situation z. Zt. Unklar
- CONTRA hohe Sicherheit
  - Fragwürdigkeit des Nutzens
  - Einschränkung des bequemen Arbeitens
  - Implementierung zeitaufwendig und schwierig
  - Widerspricht dem offenen Charakter eines Hochschulnetzes



Probleme:
- Entscheidungsfindung
- Konzept
- Realisierung
- Maintenance

www.rz.uni-wuerzburg.de