1. Informationsveranstaltung:

Sicherheit im Internet - Wunsch und Wirklichkeit

Herzlich Willkommen!

Dipl. Ing. Pascal Mittner
IT Security Consultant, Astalavista Group

24. September 2003

Die Organisatoren

- Astalavista Group, IT-Sicherheitsunternehmen mit Sitz in Chur
- Dienstleistungsangebot der Astalavista Group
  - Managed Security Services
  - Sicherheitskonzepte
  - Virenlösungen
  - Security Audits
  - Firewalls, IDS und VPN
  - Beratung und Schulungen
  - Astalavista CMS - einfach sicher

Die Organisatoren

VORCON grafic&design AG Laax, Switzerland

- Vorcon AG, Kreativagentur für Digital und Printmedien mit Sitz in Laax
- Web- Abteilung mit eigenem Grafiker, Webpublisher, Mediamatiker und Datenbankprogrammierer
- Dienstleistungen im Webbereich
  - Konzeption und Planung
  - Webgestaltung und Design
  - Programmierung in HTML, ASP,PHP,ColdFusion, Java Script, SQL unter Verwendung von MySQL, MS SQL oder Access Datenbanken
  - Integration von Content Management Systemen (CMS)
  - Steuerbare Security Cam‘s für Internet und Intranet mit Archivierung
  - Suchmaschinen Eintragsoptimierungen

Agenda

- **Einleitung zum Thema IT-Sicherheit**
- **Die Risiken im Internet**
- **Schutzmöglichkeiten**
- **Live-Hacking Demos**

Definition von Sicherheit

- Sicherheit ist eine auf Erfahrungen gegründete Annahme, von gewissen Bedrohungen nicht vorrangig getroffen zu werden

Sie schützen sich in der realen Welt…

- Haben Sie eine Haustür?
- Schliessen Sie auch die Fenster?
- Ist Ihr Hausrat versichert?
- Ist eine Alarmanlage installiert?

…aber schützen Sie sich im Internet?

- Über 600 Mio. Menschen stehen direkt vor Ihrer Tür
- Pro Tag wird X mal geprüft ob abgeschlossen ist
- Bei offener Tür haben Sie in kürzester Zeit ungebetene Gäste

Wunsch

- Internetnutzung ohne Risiken
- Schnelle und bequeme Kommunikation
- Arbeitsprozesse optimieren
- Kosten einsparen
- Umsatz steigern durch neue Märkte

Wirklichkeit

- Das Internet ist „unsicher“
- Viren zerstören Daten
- Wieder neue Sicherheitslücken entdeckt
- Hacker greifen Webseiten an
- usw.

Was sind die Folgen davon?

- Diebstahl
- Betrug
- Vandalismus
- Verletzung der Privatsphäre
- Verletzung des Gesetzes

Wo liegt das Problem?

- Wir sind es gewohnt mit Risiken in der realen Welt umzugehen
  - Wir kennen den Wert unseres realen Vermögens
  - Wir können die Wahrscheinlichkeit einer Bedrohung abschätzen
  - Wir wissen, wie wir uns angemessen gegen eine Bedrohung schützen können
- In der virtuellen Welt versagt unser Sicherheitsinstinkt
  - Wir unterschätzen den Wert unserer Informationen
  - Wir haben keine Erfahrungen über Wahrscheinlichkeiten
  - Wir kennen die Schutzmassnahmen nur ungenügend

Agenda

- **Einleitung zum Thema IT-Sicherheit**
- **Die Risiken im Internet**
- **Schutzmöglichkeiten**
- **Live-Hacking Demos**

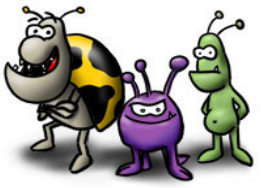
Grundsätzliche Entstehungen von Risiken

Entstehung von Gefahren durch :

- Konzeptfehler -> Entwickler
- Programmierfehler -> Entwickler
- Konfigurationsfehler -> Administrator
- Nutzungsfehler -> Anwender

Viren, Würmer und Trojaner

- Computerviren – effektiver Code auf kleinstem Raum
- Würmer – Virenverbreitung im Netzwerk
- Trojanische Pferde – die Einschleuser



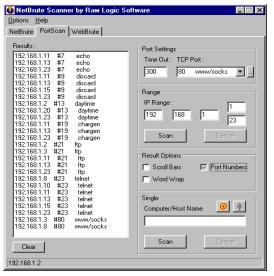
Beispiele

- Lovsan Wurm (Blaster)
  - Ausnutzung einer Sicherheitslücke im RPC von Windows
  - Verbreitet sich über das Netzwerk ohne Aktion des Benutzers
  - Führt dazu, dass der Rechner immer wieder neu startet
  - Angriff auf windowsupdate.com -> DDoS
- SoBig.F Wurm
  - Versendet sich per Email-Attachement
  - Verwendet eine beliebige Emailadresse als Absender
  - Sollte am 19. August 03 Updates von 20 Computern holen

Angriffe auf Netzwerke

Live-Hacking Demo

- Scannen
  - Portscans – Identifizierung der Systeme und Dienste
  - Vulnerability-Scans – Identifizierung der Sicherheitslücken
- Sniffing
- Spoofing
- TCP Hijacking (Man in the Middle)
- Denial-of-Service (DoS und DDoS)
- Diverse Kombinationen



Angriffe auf Passwörter

- Brute Force
- Reverse Brute Force
- Wörterbuch Angriffe
- Angriffe auf standard Passwörter

Client- und Webserverdienste Angriffe

Live-Hacking Demo

- Webseiten mit Formularen und eingebauter Logik
  - SQL-Injection
  - CSS (Cross-Site-Scripting)
  - HTTP Header Manipulationen
  - Session Hijacking
  - Path Traversal
  - Cookie Manipulation
- Dialer
- Sicherheitslücken in Web Browsern
- Angriffe per E-mail

Agenda

- **Einleitung zum Thema IT-Sicherheit**
- **Die Risiken im Internet**
- **Schutzmöglichkeiten**
- **Live-Hacking Demos**

Wann ist sicher sicher genug?

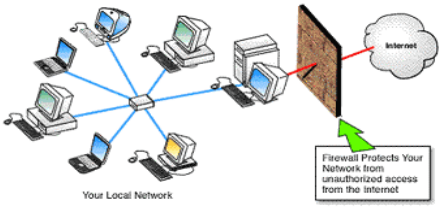
- 100% Sicherheit ist nie möglich
- Das Gesamtrisiko muss auf ein tragbares Mass reduziert werden
- Die Kosten für die Sicherheit dürfen den Wert der zu schützenden Güter nicht überschreiten

Sicherheitsstrategie festlegen

- Was soll geschützt werden?
- Wer ist für die Sicherheit verantwortlich?
- Wie soll die Sicherheit gewährleistet werden?
- Gewaltentrennungen festlegen
  - Richtlinien
  - Umsetzung
  - Kontrolle

Standard Schutz gewährleisten

- Installation einer aktuellen Antivirensoftware
- Einsatz einer Firewall (Appliance/Software)
- System aktuell halten (Patches/Updates)
- Keine Zugänge ohne Passwortschutz
- Sensitive und wichtige Daten periodisch Sichern



Sensibilisierung der Internetbenutzer

- Informationssammlung über aktuelle Gefahren
  - Bücher, Zeitschriften
  - Webseiten
- Verhaltensregeln erstellen
  - Merkblätter
  - Anleitungen
- Eigenes Sicherheitsempfinden entwickeln
  - Email Anhänge von Unbekannten nicht öffnen
  - Keine Downloads von unseriösen Anbietern

Präventiver Schutz der eigenen Infrastruktur

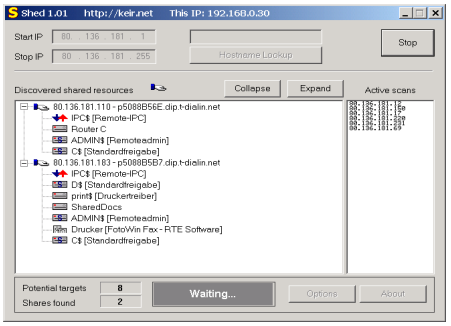
- Periodische Sicherheits-Checks durch unabhängige Experten
- Nicht benötigte Dienste deinstallieren oder deaktivieren
- Überwachung durch Intrusion Detection Systeme (IDS)
- Notfallplan erstellen und trainieren
- Informationen über aktuelle Sicherheitslöcher
  - www.securityfocus.com
  - www.microsoft.com/security
  - www.sans.org
  - www.astalavista.net
  - www.heise.de/security

Agenda

- Einleitung zum Thema IT-Sicherheit
- Die Risiken im Internet
- Schutzmöglichkeiten
- Live-Hacking Demos

(1) Angriff auf Windows Freigaben

- Shep – Laufwerksfreigaben Scanner



(2) Angriff auf einen Unix Webserver

- Ausgangslage : Webkonto bei einem massen Hosting Provider
- Ziel : Wir erhalten Lesezugriff auf über 2150 Webseiten!
- Welche Risiken werden ausgenutzt : Konfigurations- und Konzeptfehler

(3) SQL Injection Angriff

- Ausgangslage : Webbrowser, Suchmaschine
- Ziel : Auslesen von Passwortgeschützten, sensitiven Daten
- Welche Risiken werden ausgenutzt : Programmierfehler

„ Suchmaschinen als Hackerwerkzeug!
.... oder mittels ' OR '1'='1 zum Erfolg“

- inurl:login+asp -> 567‘000 Treffer
- Index of / password -> 3‘670‘000 Treffer
- inurl:admin "index of" -> 44‘000 Treffer

(3) SQL Injection Erklärung

Normaler Ablauf :

Sehen wir uns an, wie der SQL String aussieht, wenn sich der Administrator mit **admin** / **admin** einloggt:

```
SELECT * FROM users WHERE UserName='admin' AND
  UserPassword='admin'
```

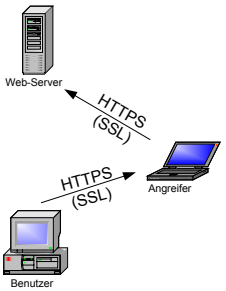
SQL Injection Ablauf:

Wie wär's mit folgender Benutzername und Passwort Kombination:
' OR '1'='1 und ' OR '1'='1.

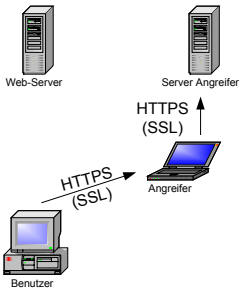
```
SELECT * FROM users WHERE UserName='' OR '1'='1' AND
  UserPassword='' OR '1'='1'
```


(4) Erlangen von gültigen Logininformationen eines e-banking accounts

Direkte Verbindung



Umleitung der Verbindung (Mitm)



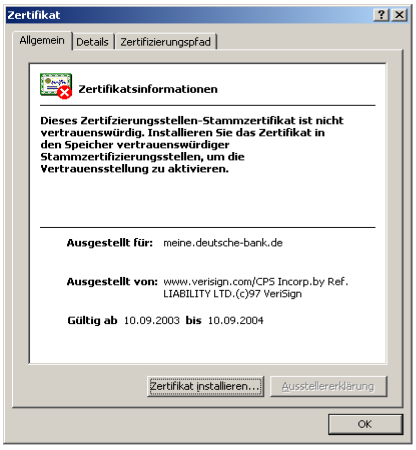
Umleitung und Spoofing

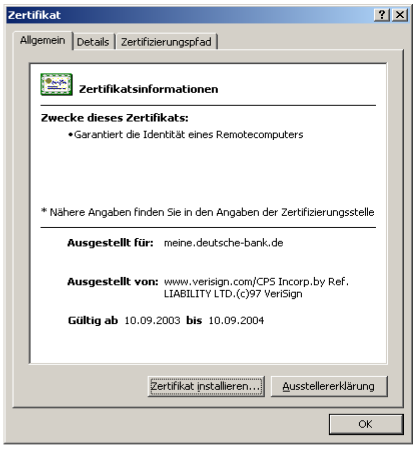
(4) Erlangen von gültigen Logininformationen eines e-banking accounts

- Ablauf des Angriffes
  - Zugriff zum Opfersystem via RPC-Exploit
  - Modifikation des Host-Files
  - Übernahme der verschlüsselten Verbindung mit gefälschtem Zertifikat
  - Umleitung auf eigenen Webserver mit gespoofter Webseite
  - Sniffen der Login-Informationen

Live-Hacking Demos

(4) Erlangen von gültigen Logininformationen eines e-banking accounts





Wird das Internet in Zukunft sicherer?

JA	NEIN
Sicherungssoftware wird immer besser	aber auch Hacker Tools
Budget für Security steigt	langsamer als die Anzahl und Komplexität der Systeme
IT-Security findet Beachtung	insbesondere bei jugendlichen Hackern
Neue Sicherheitsstandards	setzten sich nicht durch

Schlusswort

Sicherheit ist wie eine Kette

immer nur so sicher,

wie ihr schwächstes Glied