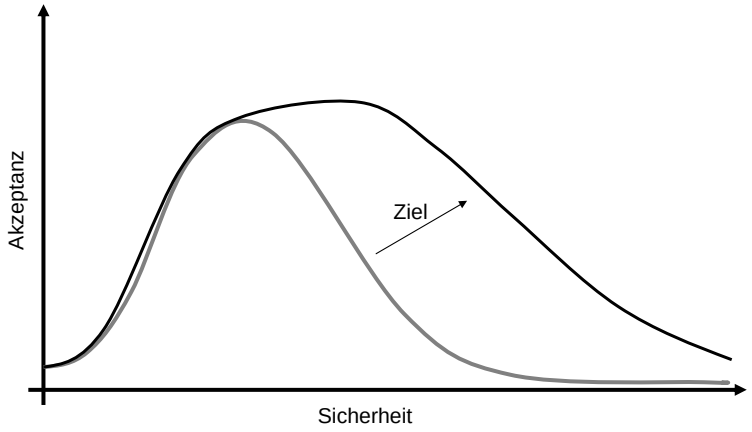
DESY Passwortpolicy

Carsten Porthun

Agenda

- Aktuelles
- DESY IT-Sicherheitspolitik: Ziele und Maßnahmen
- Accountsicherheit im Besonderen
  - Bedeutung
  - Gefahren
  - Maßnahmen
  - Notwendigkeit der Erweiterung der Passwortrichtlinie
  - Allgemeine Anmerkungen und Empfehlungen
- Zusammenfassung
- Diskussion

Userakzeptanz



Aktuelles I

Headlines

- Trojaner installiert sich über kritisches Sicherheitsleck in Word (heise, 20.05.06)
- Tendenzverschiebung bei der Entwicklung von Schadprogrammen (Kaspersky, 28.07.05)
- Botmaster zu 57 Monaten Haft verurteilt (heise, 09.05.06)
- Würmer im Wandel (heise, 27.12.2005)
- Jedes fünfte Unternehmen mit Keyloggern infiziert (heise, 09.05.06)
- Big Brother sitzt im Rechner (Computerwoche, 02.05.06)
- Neue Aladdin-Studie unterstreicht wachsende Keylogger-Gefahr (openPR, 08.09.05)

Aktuelles II

- **1. STOERENFRIEDE: Trojanisches Pferd gibt sich als Windows-Update aus**
- Ein neuer Schaedling sorgt derzeit fuer Unruhe im Netz: Das Trojanische Pferd [http://www.bsi-fuer-buerger.de/viren/04_04.htm] , das von verschiedenen Anti-Viren-Herstellern als "Trojan.Spy.Sinowal" bezeichnet wird, versteckt sich **im Anhang einer E-Mail** mit der Betreffzeile "Achtung! Wichtige Nachrichten von Microsoft Windows Update!". Oeffnet der Empfaenger das angehaengte Archiv "ms56.zip", welches die Datei "ms56.exe" enthaelt, um das vermeintliche Windows-Update zu installieren, laedt er sich den Schaedling auf seinen Rechner. **Der Eindringling protokolliert dann private Passwoerter und Bankdaten und gibt sie an den Programmierer des Trojanischen Pferdes weiter**. Das BSI warnt ausdruecklich davor, Anhaenge dieser Art zu oeffnen, da serioese Software-Hersteller niemals Updates oder Patches per E-Mail verschicken. Darueber hinaus sollten Sie darauf achten, immer aktuelle Virenschutzsoftware einzusetzen.

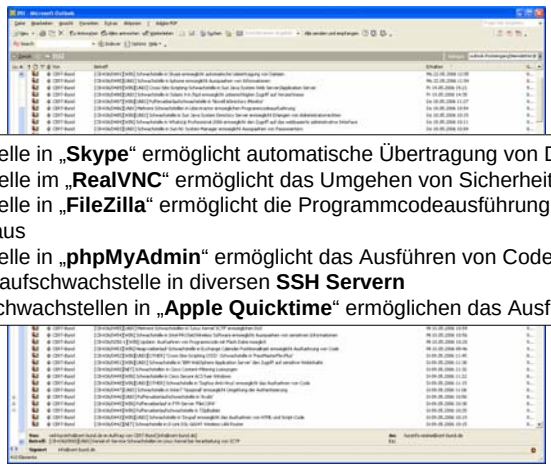
(Der Newsletter von www.buerger-cert.de
Ausgabe vom 08.06.2006)

Aktuelles III

- Abnahme der Verbreitung klassischer Viren und Massen-Mailing-Würmer gegenüber gezielten Attacken.
- Mai ’06: 1538 neue Schadprogramme
  Anteil Trojaner: 86%
- Cyberkriminelle nutzen Trojaner um vertrauliche Daten auszuspionieren

(http://www.sophos.de/pressoffice/news/articles/2006/06/20060601toptenmai.html)

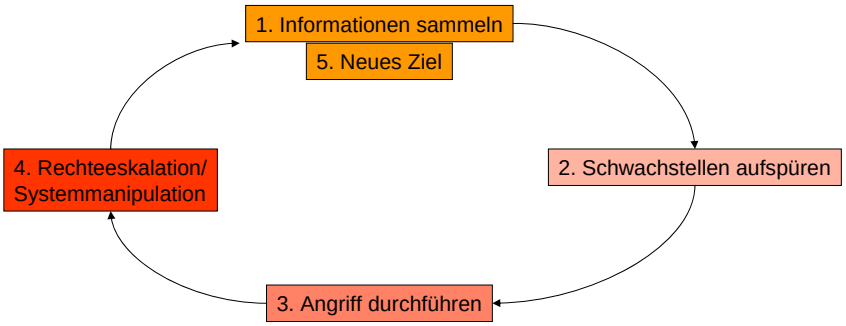
Aktuelles IV



- Schwachstelle in „**Skype**“ ermöglicht automatische Übertragung von Dateien
- Schwachstelle im „**RealVNC**“ ermöglicht das Umgehen von Sicherheitsvorkehrungen
- Schwachstelle in „**FileZilla**“ ermöglicht die Programmcodeausführung von entfernten Standorten aus
- Schwachstelle in „**phpMyAdmin**“ ermöglicht das Ausführen von Code
- Pufferüberlaufschwachstelle in diversen **SSH Servern**
- Mehrere Schwachstellen in „**Apple Quicktime**“ ermöglichen das Ausführen von Code

(Schwachstellenmeldungen des BSI)

Typisches Vorgehen von Hackern



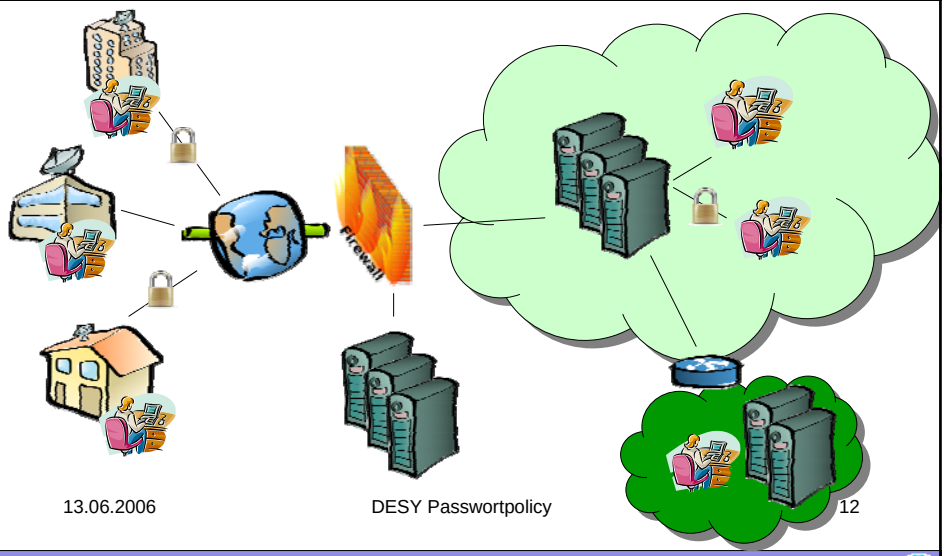
IT Sicherheitsmaßnahmen I

- **Firewall**
  - Übergang vom Intra- zum Internet
  - Kontrolle des ein- und ausgehenden Netzwerkverkehrs
  - Abschotten interner Netzdienste vor dem Zugriff von Außen
- **DMZ (Demilitarized Zone)**
  - „zwischen“ Inter- und Intranet
  - Schutz des internen Netzes vor gehackten Rechnern, die von Außen erreichbar sind (z.B. Webserver)
- **Mehrstufiger Virenschutz**
  - Content Scanner (keine ausführbaren Dateien)
  - Kette unterschiedlicher Virenscanner
  - Gateway, Mailserver, Client

IT Sicherheitsmaßnahmen II

- **Getrennte Netze**
  - Unterschiedliches Sicherheistniveau (z.B. Kontrollnetze, Verwaltung, Gästenetz)
  - Z.T. durch eigene Firewalls vom internen Netz getrennt
- Ziel: auch intern weitgehender Einsatz **verschlüsselter Protokolle**, wenn Login und Passwort übertragen werden
  - Remote Zugänge nur über verschlüsselte Verbindungen (VPN, SSH)
- Weitgehend **geswitchte Netze**
- Zentrale Verwaltung der Virenscanner Policy mit **ePO**
- **Zentrales Patchmanagment**
- **Personal Firewall** (XP SP2)
- **Account Sicherheit (Passwort Policy)**

Schema technische Maßnahmen



Accountsicherheit

- Wesentlicher Bestandteil der IT-Sichersmaßnahmen am DESY
  - Ausgewogenheit zwischen verschiedenen Sicherheitsmaßnahmen
  - Akzeptanz versus Sicherheit
- Schutz der „E“-Identität der User
- Datenschutz
- Schutz vor Regressforderungen
- Setzt auch auf Einsichtigkeit und Verantwortungsbewusstsein der User, da technisch nur begrenzt kontrollierbar
- **Grundsatz: Aufklärung ist besser als technische Kontrolle!**

Gefahren kompromittierter Accounts

- Zugriff auf DESY Ressourcen aus dem Internet
  - Webmail
  - SSH (Tunnel zu anderen Diensten im Netzwerk)
  - Remote Zugriff auf Rechner im internen Netz
- Ausnutzen lokaler Schwachstellen zur Erlangung höherer Rechte
- Bei ausreichender Berechtigung: Installation von Diensten (Bot Netz, Rootkits)
- Ausspähen und Angreifen von Rechnern im internen Netzwerk
- Vortäuschen einer falschen Identität
- Versenden von Spammails
- Ausspähen, Manipulieren oder Löschen von Daten
- Mögliche Verwicklung in Strafverfolgungsprozesse

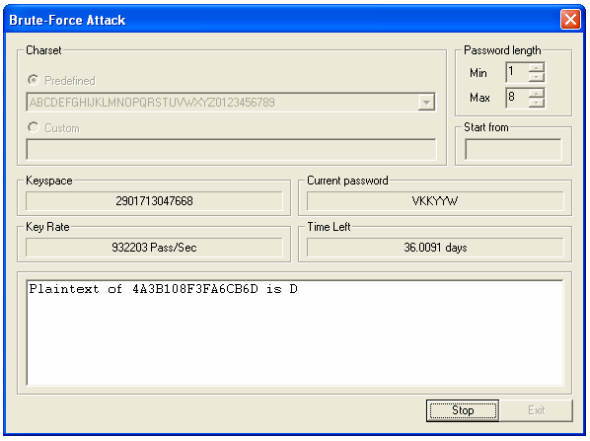
Mögliche Angriffszenarien

- **Brute Force Attacken**
  Systematisches Ausprobieren von Passworten
- **Wörterbuchattacken**
  Ausprobieren gängiger Begriffe (auch anderer Sprachen)
- Kombination aus **Brute Force und Wörterbuchattacken**
- **Social Engineering**
  Ausspähen von Gewohnheiten eines Anwenders
- **Phishing / Manipulation des Netzwerks**
  Preisgabe von Passworten, PINs etc. über gefälschte Webseiten
- **Sniffen** von nicht verschlüsseltem Netzwerkverkehr
- **Keylogger**
  „Mitschneiden“ der Keyboardeingabe
  (Bestandteil vieler Trojaner)

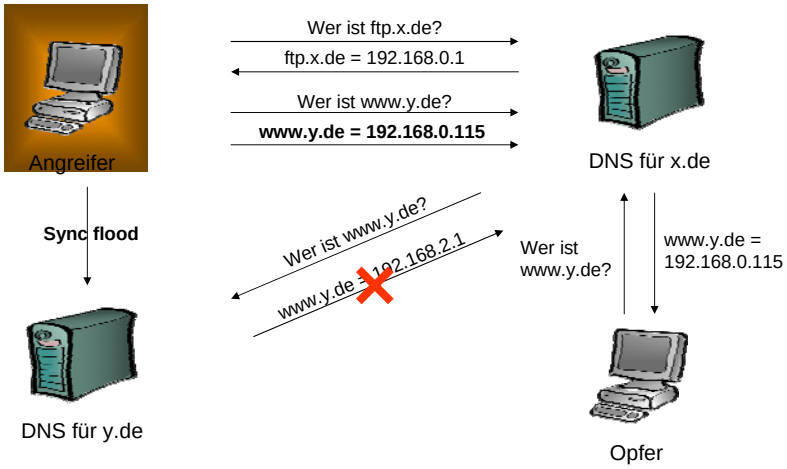
„Anforderungen“ an Passworte

- Passworte von persönlichen Accounts sollen nur dem Anwender bekannt sein
- Passworte sollen **nicht** leicht zu erraten sein (technisch und menschlich)
- Passworte sollen regelmäßig geändert werden
- Sie sollen sich trotzdem leicht merken lassen
- Unterschiedliche Passworte für verschiedene Sicherheitsstufen
  - Internetdienste
  - User Account
  - Administrativer Account

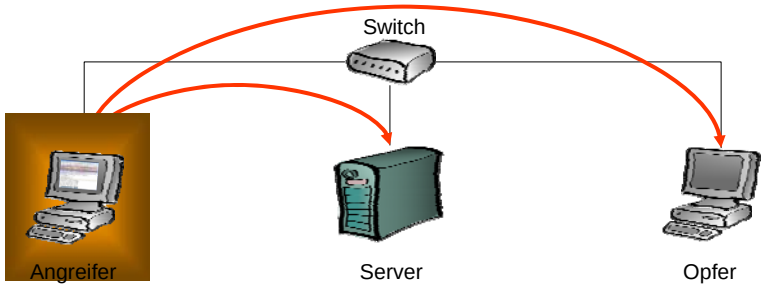
Brute Force



DNS Spoofing

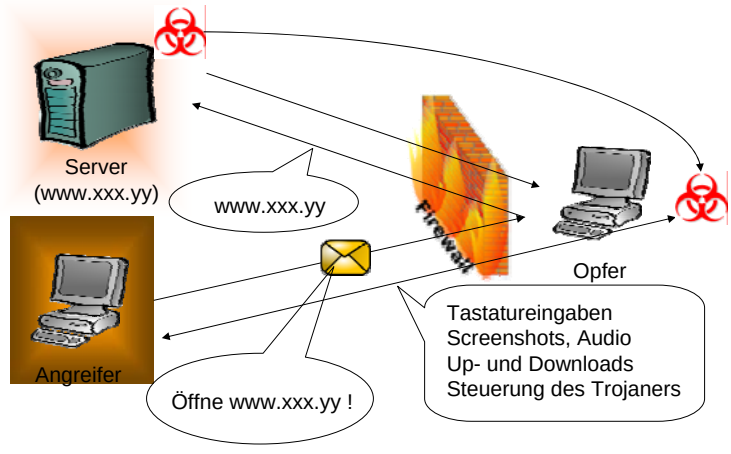


ARP Poisoning



Angreifer	Server	Opfer
IP: 192.168.0.3 MAC: CC:CC:CC:CC:CC	IP: 192.168.0.2 MAC: BB:BB:BB:BB:BB	IP: 192.168.0.1 MAC: AA:AA:AA:AA:AA
ARP Tabelle: 192.168.0.1 -> AA:AA:AA:AA:AA 192.168.0.2 -> BB:BB:BB:BB:BB	ARP Tabelle: 192.168.0.1 -> CC:CC:CC:CC:CC 192.168.0.3 -> CC:CC:CC:CC:CC	ARP Tabelle: 192.168.0.2 -> CC:CC:CC:CC:CC 192.168.0.3 -> CC:CC:CC:CC:CC

Trojaner



Bsp. Back Orifice

Abacus-Forum diskutiert.

Back Orifice: Eigenschaften und Funktionsweise

Back Orifice) besteht aus einem Server- und einem Client-Programm, welches zur remote Bedienung von Rechnern in einem Netzwerk (Intra- oder Internet) eingesetzt werden kann. *BO* ist selbstinstallierend und kann an andere Programme angehängt werden, so daß eine Verbreitung u.U. unbemerkt erfolgt. *BO* wird in der Task-Liste nicht angezeigt und wir beim Hochfahren des Rechners unter einem beliebigen Namen gestartet. Während der *Back Orifice-Client* auf allen möglichen Betriebssystemen lauffähig ist, gibt es den *Back Orifice-Server* nur für Windows 95/98.
Back Orifice hat u.a. folgende Funktionalitäten:

- Aufzeichnen von Tastatureingaben
- Steuern von Multimedia-Funktionen, wie z.B.
  - Erstellen von Screen-Shots
  - Bedienung angeschlossener Video-Kameras etc.
  - Abspielen von Wav-Dateien
- Rebooten des Rechners
- Auslesen von Systeminformationen, wie z.B.
  - CPU
  - Windows Version
  - Speicherauslastung
  - Passwords des Bildschirmschoners, Netzwerk-Zugängen, Web etc.
- Up- und Download von Files
- Aktivieren eines HTTP-Servers (auf einem beliebigen Port)
- Manipulationen am Filesystem, wie z.B.
  - Kopieren
  - Löschen
  - Umbenennen
  - Suchen
- Modifikation von Registry-Schlüsseln und -Werten, also
  - Auflisten
  - Erstellen
  - Löschen
- Prozeßkontrolle
- Netzwerkkontrolle (incl. Umleiten von Paketen!)
- Monitoring von Netzwerkpaketen (mit Plug-In "BUTTSniffer")
- Scannen eines Netzes nach aktiven BO-Servern (Vorsicht! - s.u.)

Desweiteren besitzt *Back Orifice* ein PlugIn-Interface, über das ein beliebiger Programm-Code unentdeckt ausgeführt werden kann. Über diese Schnittstelle ist BO jederzeit remote "updatebar".
"Back Orifice" nutzt in der Default-Einstellung den Port Nr. **31337** des UDP-Prokolles. Allerdings kann die Portnummer beliebig verändert werden. Die Übertragung der Pakete zwischen *BO-Server* und *BO-Client* erfolgt mit einer schwachen Verschlüsselung.

Hinweis:

RSR Beschluss vom 21.04.2006

- **Keine Trivialänderungen:**
  - In Worten:
    „Ein neues Passwort soll sich gravierend von dem vorherigen unterscheiden, so dass bei bekanntem alten Passwort nicht auf das neue geschlossen werden kann.“
- Ziel: Schutz vor variieren bekannt gewordener Passworte
- **Gilt ab 19.06.2006**

Passwortarithmetik

Zeichen\Länge	7	8	9	10
10	1E+07	1E+08	1E+09	1E+10
25	6,1E+09	1,5E+11	3,8E+12	9,5E+13
50	7,8E+11	3,9E+13	1,9E+15	9,7E+16
60	2,8E+12	1,7E+14	1E+16	6E+17
100	1E+14	1E+16	1E+18	1E+20

$(N = Z^{L)}$

8 Zeichen, Änderung an nur einer Stelle -> 800 verschiedene Passworte !!

Allgemeine Anmerkungen

- Ein Passwort, dass ich mir schlecht merken kann, ist noch lange kein gutes Passwort.
- Ein Passwort, dass ich mir gut merken kann ist nicht zwangsläufig ein schlechtes Passwort.
- Technisch erstellte Passwort sind nicht besser als Eigenkreationen.
- Gegen das Aufschreiben von Passworten ist nichts einzuwenden, wenn sie sicher und nicht für jedermann zugänglich aufbewahrt werden.
- Ziel sollte **nicht** sein, nach Erfüllung der Minimalanforderungen zu suchen, sondern aus eigenem Interesse diese Energie und Kreativität in das Finden eines neuen Passwortes zu stecken.

Empfehlungen

- Passworte nach Möglichkeit nur verschlüsselt über das Netzwerk übertragen (kein Telnet, kein FTP)
  - > Schutz vor Sniffern
- Passwort bei Webanwendungen nur via SSL (Https) und vertrauenswürdigen Zertifikaten angeben
  - > Schutz vor Sniffern und Phishing
- Keine Passworte in Applikationen für automatische Anmeldung speichern
- Passworte ändern, wenn sie aus „unbekannten“ Umgebungen heraus genutzt worden sind (Internetcafe, Fremdinstitute)
- Bei Verlassen des Arbeitsplatzes Bildschirm sperren
- Gruppen sind besser als Gruppenaccounts

Beispiel HTTP over SSL (https)

3. Kontrolle des Zertifikats
   - DNS
   - vertrauenswürdiges Stammzertifikat
   - Gültigkeit
   - eventueller Rückruf
4. Auslesen des öffentlichen Schlüssels aus dem Zertifikat
5. Erzeugen eines Vorschlüssels
6. Verschlüsseln des Vorschlüssels mit öffentlichem Schlüssel des Servers
8. Entschlüsseln des Vorschlüssels
9. Erzeugen des sym. Sitzungsschlüssels auf Grundlage des Vorschlüssels

9. Erzeugen des sym. Sitzungsschlüssels auf Grundlage des Vorschlüssels

Studien zeigen:

- Weniger Viren, mehr Trojaner (Kaspersky)
- Zunahme des Versendens von Schadprogrammen an lokal begrenzte Empfänger (Kaspersky)
- Zunahme des Diebstahls von Benutzeridentitäten (Aladdin)
- Trend weg von aggressiven und großflächigen Virenausbrüchen hin zu einer Vielzahl von Angriffen mit kleineren Zielgruppen mit spezialisierter und trickreicher Malware (heise)
- Zunahme der organisierten Internetkriminalität (ETH Zürich im Auftrag von McAfee)
  (Vermietung von Bot Netzen)
- Für 2005 6000 verschiedene Keylogger-Programme (+ 65% 2004; iDefense)

Zusammenfassung

- IT Sicherheit ist ein Komplex aus technischen und organisatorischen Maßnahmen, die regelmäßig an aktuellen Entwicklungen angepasst werden müssen
- Accountsicherheit spielt eine besondere Rolle, da sie von jedem einzelnen umgesetzt werden muss und technisch nur bedingt kontrollierbar ist
- Eine zunehmende Anzahl von Angriffen auf Passworte kleinerer Gruppen von Anwendern erfordert besondere Sorgfalt im Umgang mit Passworten und weitere Maßnahmen zum Schutz vor unberechtigtem Gebrauch der Logindaten
- Deshalb: Keine Trivialänderungen in Passworten

Fragen und Diskussion

Vielen Dank für die Aufmerksamkeit!