SECURITY

Kongress Security-IT

BSP. CONSULT

Aktuelle Bedrohungen

-

Viren, Würmer, Webbugs & Co.

Dipl. Wirt.-Inf. Michael Raith
IT-Security Consultant
Tel. (0941) 29 77 4 - 0
mr@bsp-consult.com
PGP Key-ID: 0x 83F0 5C6A

Überblick

- Hacker, Cracker und Script Kids
- Exploits
- Tarnmechanismen für ‚owned Systems' und Malware
- aktuelle Angriffsmethoden und Ausblick

Dipl. Wirt.-Inf. Michael Raith

Begriffsbestimmung

Hacker - ursprüngliche Definition:

Person, die mit hohem Technikwissen und noch größerer Neugierde die Arbeitsweise von Systemen und Netzwerken untersucht - und dadurch zwangsläufig auf Sicherheitslücken stößt.

Der idealtypische Hacker würde eine Sicherheitslücke in einem System entdecken und den Eigentümer des Systems umgehend über diese Lücke informieren.

-> Whitehat

Dipl. Wirt.-Inf. Michael Raith

Cracker:

Ziele eindeutig übler Natur
Lücken in Netzwerken werden explizit gesucht, um diese für:

- Vandalismus
- Stehlen von Informationen
- Diffamierung der Betroffenen
- finanzielle Interessen

ausnutzen zu können.

-> Blackhat

Dipl. Wirt.-Inf. Michael Raith

Script Kids:

Bezeichnung nicht Alters- sondern Know-How-bezogen

Auf Grund mangelnder technischer Kenntnisse nicht in der Lage, selbständig Schwachstellen zu finden oder diese für irgendwelche Aktivitäten auszunutzen.

Vielmehr nutzen sie die von anderen Hackern programmierten Tools für ihre Aktivitäten.

Beispiel: Sasser Autor

Dipl. Wirt.-Inf. Michael Raith

Exploits

Eine der potentesten Methoden, die Kontrolle über ein Zielsystem zu erlangen

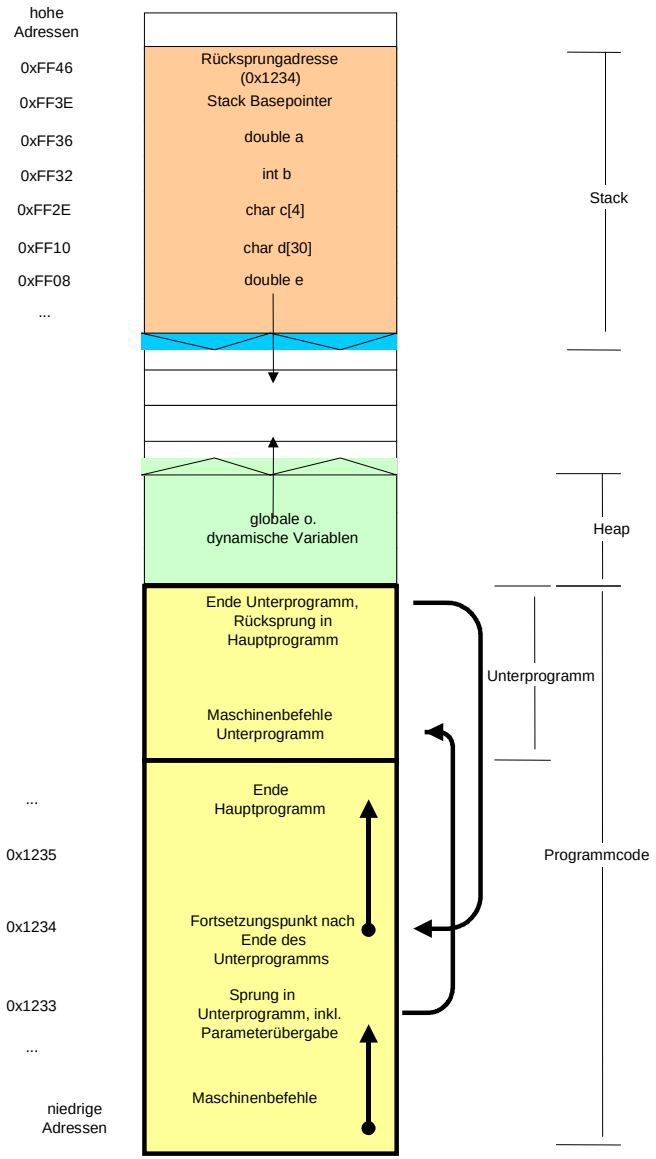
Grundlage meist Stack bzw. Bufferoverflows

Weniger häufige Angriffspunkte:

Heap Overflows, Format-String-Schwächen und Injection-Angriffe

Dipl. Wirt.-Inf. Michael Raith

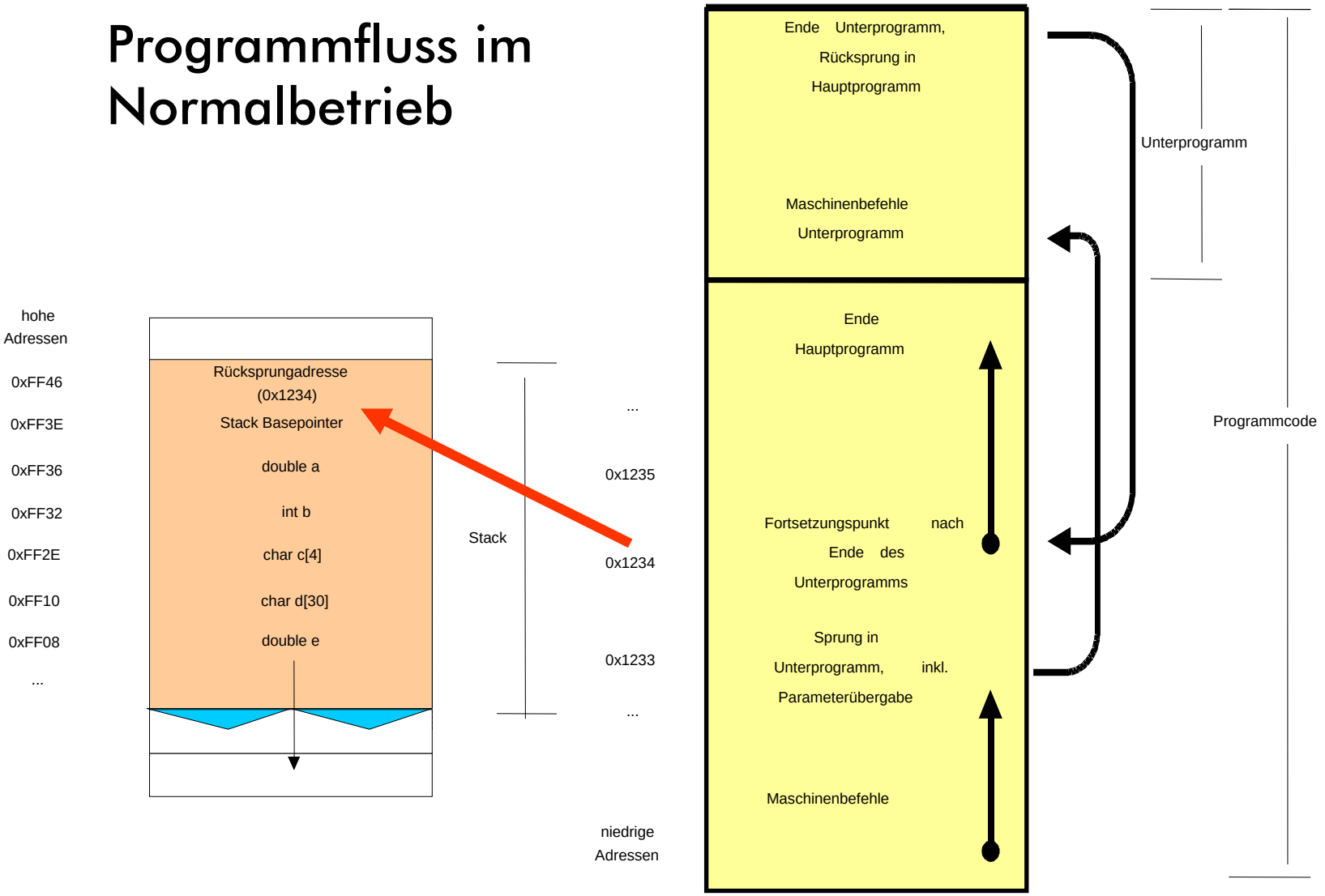
Aufbau eines normalen Programms



BSP. CONSULT

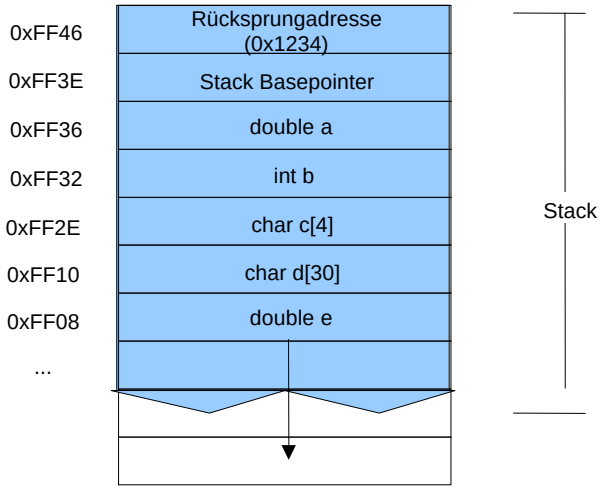
Dipl. Wirt.-Inf. Michael Raith

Programmfluss im Normalbetrieb

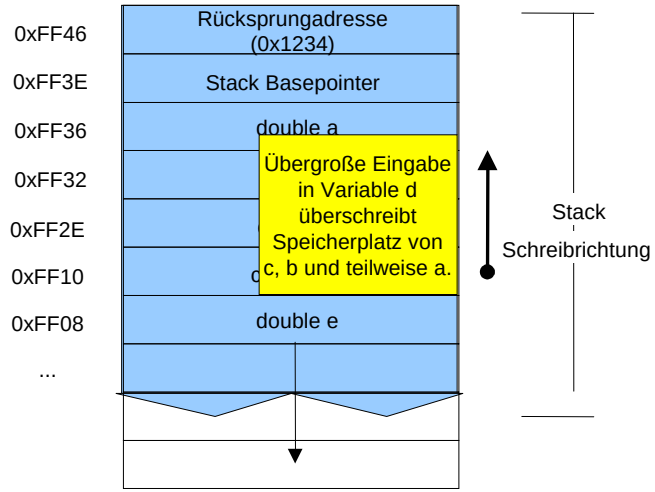


BSP. CONSULT
Dipl. Wirt.-Inf. Michael Raith

Auswirkungen eines Stack Overflows



Stack im Normalfall

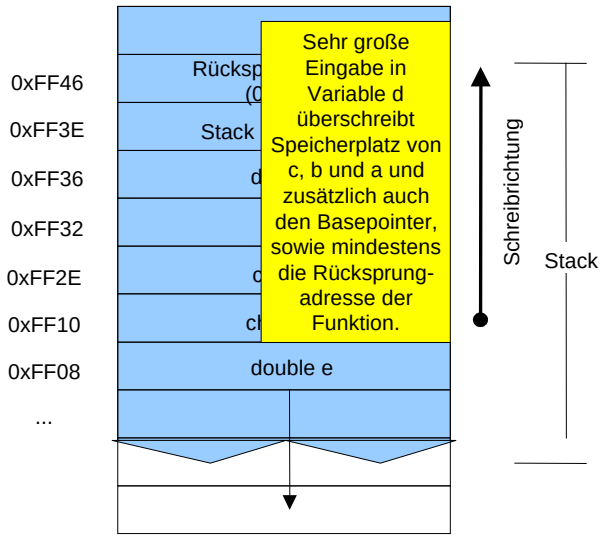


Stack Overflow

BSP. CONSULT

Dipl. Wirt.-Inf. Michael Raith

Überschreiben der Rücksprungadresse



Der ursprünglich korrekte Wert der Rücksprungadresse an 0xFF46 von 0x1234 wird mit dem Inhalt der Variablen char[d] überschrieben.

Beispiel: „Fu“ an 0xFF46 -> Wert 0x1234 wird zu 0x4675.

Nach Ende der Subroutine erfolgt Sprung nach 0x4675 und höchstwahrscheinlich Absturz.

BSP. CONSULT

Dipl. Wirt.-Inf. Michael Raith

Aufbau von Exploitcode

Ziel:

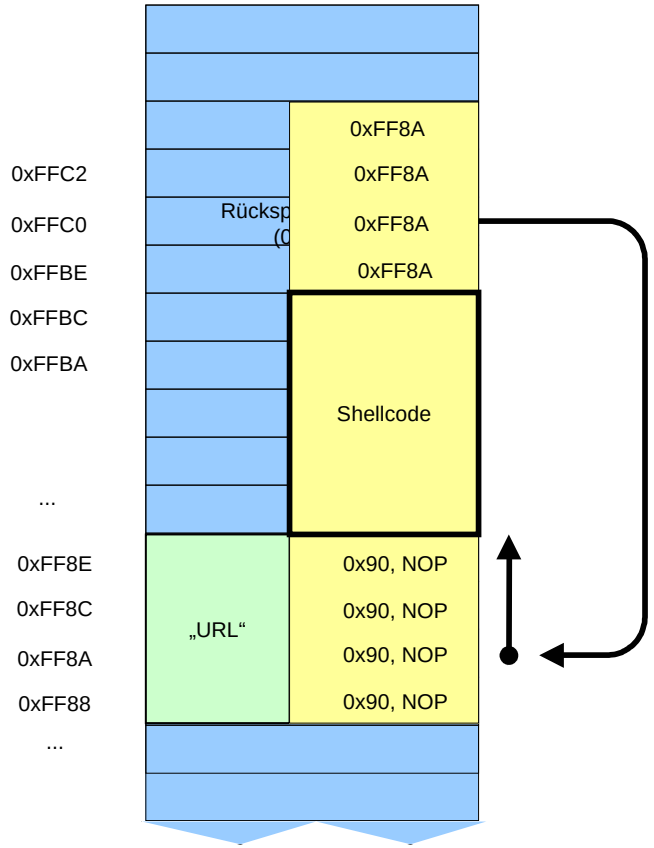
Der angegriffene Rechner springt zu Befehlen, die dem Wunsch des Angreifers entsprechen.

Idealerweise also Befehle, die der Angreifer mitsamt dem Code selbst übermittelt hat.

-> Netzwerk und Serversoftware / Betriebssysteme bzw. deren Kommunikationsroutinen sind ideale Opfer.

BSP. CONSULT
Dipl. Wirt.-Inf. Michael Raith

Schemaaufbau Exploitcode

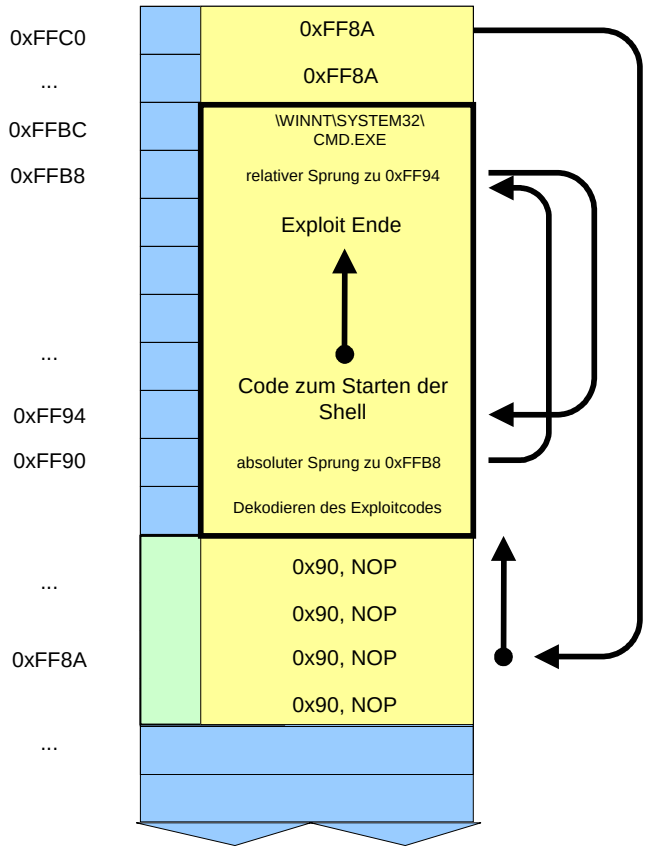


- da die exakte Rücksprungadresse unbekannt ist, wird eine geratene mehrfach übermittelt.
- die Landezone wird mit NOP aufgefüllt um durch NOP-Sliding den Startpunkt des Shellcodes wahrscheinlicher zu erreichen.

BSP. CONSULT

Dipl. Wirt.-Inf. Michael Raith

Exploitcode Detailstruktur



- Exploitcode darf keine binären Nullen enthalten, da diese das Ende eines Strings markieren würden.
- -> z.B. Codierung per XOR

- Absolute Adresse von Stringvariablen nicht bekannt
- -> Sprung zur Stelle VOR dem String, anschliessend ‚Subroutinenaufruf' zurück -> absolute Adresse wird als Rücksprungadresse gespeichert.

- Shell kann gestartet werden

BSP. CONSULT

Dipl. Wirt.-Inf. Michael Raith

- Ein- und Ausgabe der Shell wird an die IP-Adresse des Angreifers umgeleitet -> Remote Control

- Shell wird vom Zielsystem mit den Rechten der betroffenen Software ausgeführt (bei Serversoftware in der Regel System- oder Rootrechte)

-> uneingeschränkter Zugriff zum System

Dipl. Wirt.-Inf. Michael Raith

Exploits Fazit

- das Entdecken von in Frage kommenden Lücken und Entwickeln passender Exploitcodes setzt extrem hohes Fachwissen über das Zielsystem voraus

- Effizienz eines Angriffs hängt von den Rechten der attackierten Software ab

Dipl. Wirt.-Inf. Michael Raith

Tarnmechanismen - Cracker

- Vor Systemübernahme: Relaying, Spoofing etc.
- Nach Systemübername (‚rooting') Verschleierung der Spuren durch Manipulation von Logfiles oder mit Hilfe von Skripten

- Komfortvariante: Rootkits

-> Modifikationen des Betriebssystems in der Art, dass sämtliche Prozesse und Dateien, die dem Cracker zuzuordnen wären, bei Protokollierung oder Auflistung nicht mehr berücksichtigt wären

Dipl. Wirt.-Inf. Michael Raith

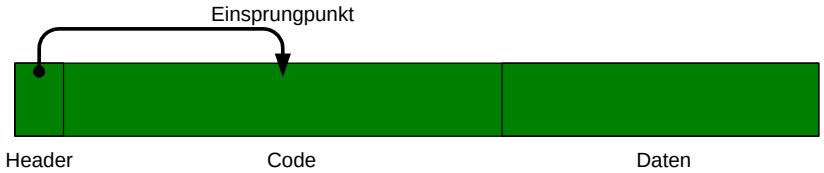
Tarnmechanismen - Viren

In der Vergangenheit stetige Evolution der Tarnmechanismen von Viren:

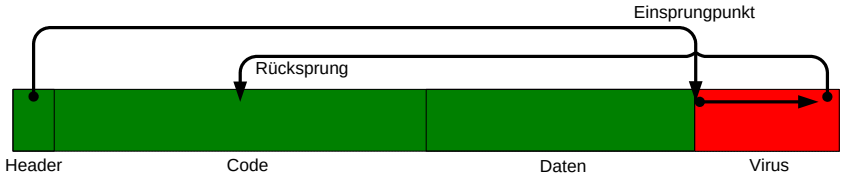
Bootsektor, TSR, FAT-Modifying, Overlay, Slack, Polymorphismus, Self-Encryption, Stealth

Dipl. Wirt.-Inf. Michael Raith

Tarnmethoden Fileinfektoren

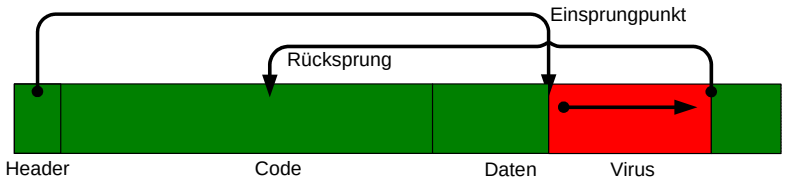


normale Programmdatei

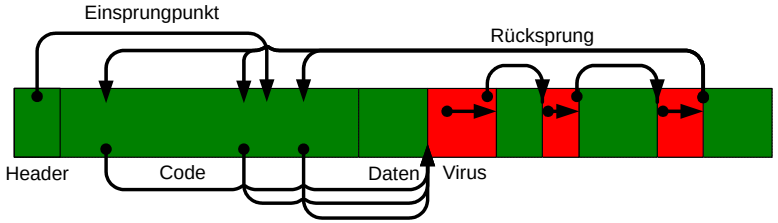


normaler PE-Infecting Virus

Dipl. Wirt.-Inf. Michael Raith



Overlay Infector



Dark Avenger, Multisegment – Overlay, modifiziert Subroutinenaufrufe

Dipl. Wirt.-Inf. Michael Raith

Stealth Viren

Stealth Viren bleiben nach dem Start im Betriebssystem und modifizieren sämtliche Funktionsaufrufe derart, dass alle Aktionen, die zu ihrer Entdeckung führen könnten, manipuliert werden.

(Analogie Rootkit)

Dipl. Wirt.-Inf. Michael Raith

Aktuelle Lage

Welcher Virentyp hat Stealth und Dark Avenger-Derivate verdrängt?

2002 – 2003: eMail Massenmailer mit eingebetteten IE-HTML-Exploits

seit 2004: einfache File Attachments

Dipl. Wirt.-Inf. Michael Raith

Typischer Virus im Frühjahr 2004

- Verbreitung per eMail
- Virus als Attachment: pif, exe, scr
- teilweise gepackt in zip oder rar Archiven
- teilweise passwortgeschützt, Passwort im eMailtext oder als Grafik

- Schwachstelle im System: der Benutzer

Dipl. Wirt.-Inf. Michael Raith

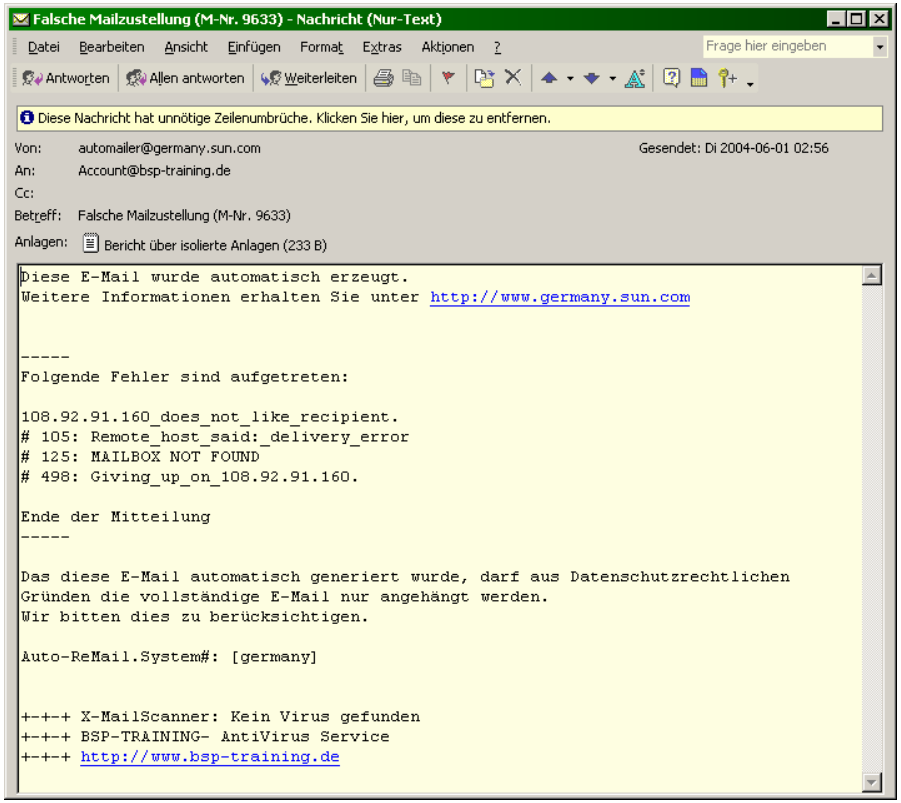
Social Engineering

- Social Engineering zunehmend verbreitet
- Trifft auf fruchtbare Basis von halb- bzw. unwissenden Computernutzern
- selbe Verbreitungsmethodik wie Hoaxes

- Trittbrettfahrer im Social Engineering: Phishing

Dipl. Wirt.-Inf. Michael Raith

Virusmail



- gibt vor, eine SMTP-Fehlermeldung zu sein
- angebliche Nachricht befindet sich im Attachment „<dateiname>.txt .pif“
- gefälschte Signatur täuscht eine Überprüfung auf Viren vor

BSP. CONSULT

Dipl. Wirt.-Inf. Michael Raith

Professionalisierung

- Viren und Crackerszene professionalisiert sich zunehmend
- „Mietangebot“ für Spammer: 25000€/Monat für Benutzung gerooteter PCs
- auftauchen modularer Quellcodes für Viren (Phatbot) – neue Schadfunktionen u. Exploits können schnell eingelinkt werden

Dipl. Wirt.-Inf. Michael Raith

Fazit

- Steigendes Schadenspotential durch Professionalisierung der Szene
- unzureichendes Patchmanagement in Kombination mit nicht existierenden oder sinnlos konfigurierten Firewalls lässt auch nach Wochen und Monaten ungepatchte und verwundbare Systeme für Attacken offen stehen
- hohe Verwundbarkeit gegenüber Social Engineering durch fehlendes Sicherheitswissen
- Social Engineering Malware ist mit deutlich weniger technischem Knowhow zu realisieren, als Exploits, Stealthfunktionen etc...

Dipl. Wirt.-Inf. Michael Raith

Dipl. Wirt.-Inf. Michael Raith

Social Engineering Specialist

because there is no patch for human stupidity!

... Wissen und Erfahrung ist der Patch!