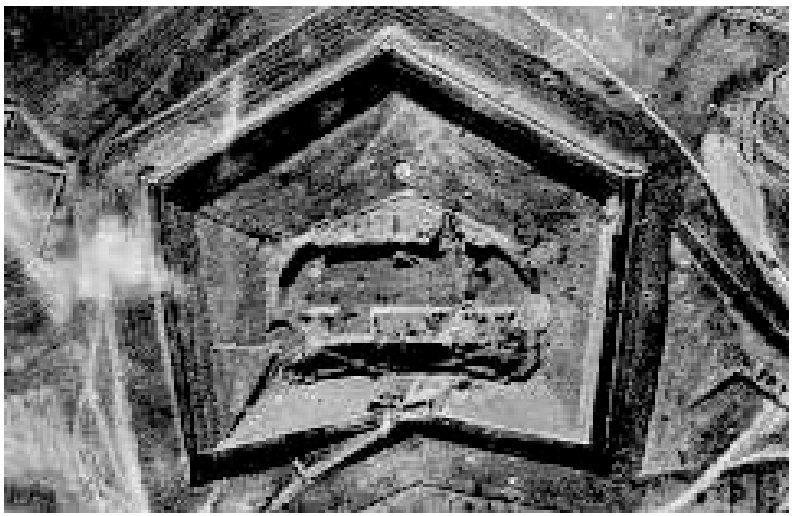
Netzwerksicherheit
Handhabung von Penetrationen

Stephen Wolthusen

IGD
Fraunhofer Institut Graphische Datenverarbeitung

Notwendigkeit der Vorbereitung auf Penetrationen

- Defensive Systeme sind gegenüber Angreifern massiv benachteiligt und **werden** umgangen oder durchbrochen



Angemessene Reaktionen (1)

- Die meisten Systeme werden täglich mehrfach angegriffen oder zumindest ausgespäht
- Herausforderung: Klassifizierung des Angriffstyps
  - Versuchte Ausnutzung nicht vorhandener/behobener Schwachstelle
    - gezielter Angriff auf das gesamte System
      - Der erkannte Angriff ist eventuell der einzige vom Revisionssystem erkannte - andere waren vielleicht erfolgreich
    - Resultat einer automatischen Abtastung durch script kiddies

Angemessene Reaktionen (2)

- Beurteilung der korrekten Handhabung erfordert neben Kenntnis verfügbarer Daten auch Heuristiken und Intuition
  - Erfordert Erfahrung, Kenntnisse der Gegenseite
  - Meist nicht oder nur bei wenigen Mitarbeitern vorhanden
  - Automatisierte Systeme sind nicht hinreichend
    - Bei hinreichend sensibler Kalibrierung und Instrumentierung sind die Ausgaben derartiger Systeme nur zur Datenreduktion dienlich
- Der Aufbau einer Organisation mit den erforderlichen personellen Ressourcen und Qualifikationen ist zwingend

Organisation der Mitarbeiterstruktur (1)

- Die Möglichkeiten zum Aufbau der Organisation hängen primär von Größe und Sensibilität der IT-Systeme ab, in kleineren Organisationen ist eine Zusammenlegung mehrerer Rollen unvermeidbar. Organisationselemente:
- Geschulte Mitarbeiter
  - Vermeidung von aktiv schädlichem, fahrlässigem Verhalten
  - Nutzer sollen Anomalien in System-,Netzwerkverhalten erkennen und melden: „biologische IDS-Sensoren“
  - Einbeziehung der Mitarbeiter kann antagonistisches Verhalten zur Sicherheitsadministration partiell vermeiden

Organisation der Mitarbeiterstruktur (2)

- Betriebsüberwachung
  - Ständige Überwachung von Netzwerk, Sensoren, Systemen
  - Wartungsarbeiten (Archivierung von Revisionsdaten...)
  - Regelmäßige Funktionsprüfung kritischer Systeme
  - Bei Erkennung von Anomalie/Angriff:
    - Klassifizierung, ggf. Einleitung von Schutzmaßnahmen
    - Bei vermutetem „ernstzunehmendem“ Angriff: Benachrichtigung Forensik, Krisenbewältigung
  - Während Krisenbewältigung: Gewährleistung des restlichen Betriebes, Suche nach weiteren Anomalien

Organisation der Mitarbeiterstruktur (3)

- Krisenbewältigung
  - muß hinreichend Ressourcen besitzen, um bei Anomalie--Analyse oder Abwehr von Angriffen andere Abläufe nicht zu be- oder verhindern
  - Ermittlung des Angriffspfades, Eliminierung der Schwachstelle
  - Untersuchung von Systemen, Datenbeständen auf Modifikation: Rekonstruktion eines bekannt sicheren Zustandes
  - Mitarbeiter müssen in der Lage sein, sich über Angriffs-mechanismen, Schwachstellen laufend zu informieren
  - Aktive Prüfung der defensiven Systeme („Red Teams“)

Organisation der Mitarbeiterstruktur (4)

- Forensische Analyse
  - Komplementär zur Krisenbewältigung
  - Wird diese Rolle nicht separat besetzt besteht ein Interessenkonflikt zwischen schneller Wiederherstellung des Regelbetriebs und einer gründlichen Analyse
  - Krisenbewältigungs-Gruppe kann nur eine Abschätzung der Penetrationstiefe vornehmen und danach handeln („Notfallchirurgie“)
  - Forensik überprüft die Hypothesen der Krisenbewältigungs-Gruppe, zieht notwendige Konsequenzen und überarbeitet Sicherheits-Strategie

Qualifikationsgruppen der Mitarbeiter (1)

- Problem der Abdeckung aller erforderlicher Qualifikationen (24/7-Betrieb, Mitarbeiter-Urlaub)
- Authentisierung
  - Kenntnis sämtlicher im System verwendeter Authentisierungs-Mechanismen, Abhängigkeiten
  - Nur Inhaber dieser Rolle dürfen Nutzerkonten pflegen
- Kommunikation
  - Information aller Betroffener, Verfügbarkeit von Kontaktinformationen

Qualifikationsgruppen der Mitarbeiter (2)

- Werkzeugentwickler
  - Systemspezifische Anpassungen meist unumgänglich
  - Kombination aus langfristigen und Notfall-Entwicklungen
- Dokumentation
  - Erstellung, Pflege der Sicherheitspolitik, Dokumentation sicherheitsrelevanter Komponenten und Abläufe
- Forensik-Experte
  - Kenntnisse aktueller Angriffstechniken, Werkzeuge
  - Kenntnisse der Soll-Konfigurationen der geschützten Systeme

Qualifikationsgruppen der Mitarbeiter (3)

- Host-Sicherheit
  - Schutz der Hosts selbst, analog Forensik-Experten für Netze
- Revision
  - Prüfung auf korrekte Umsetzung der festgelegten Maßnahmen, Korrektur der Umsetzung oder Dokumentation
  - Separate Rolle, da sonst Interessenkonflikt droht
- Firewall- und Netzwerksicherheit
  - Entwurf und Realisierung der Netzwerksicherheits-architektur (Konfiguration von Routern, Firewalls, etc.)

Qualifikationsgruppen der Mitarbeiter (4)

- Physische Sicherheit
  - Entwurf, Realisierung physischer Sicherheitsmechanismen
  - Kenntnisse auch transitiver Abhängigkeiten in physischer Infrastruktur
- Sicherheitspolitik
  - Zusammenführung der Anforderungen von Nutzern und Abgleich mit Sicherheits-Erkenntnissen
- Systemadministrator
  - Gewährleistung des Regelbetriebs. Disjunkt zu Sicherherheitsrollen

Realisierbarkeit

- Selbst wenn Unternehmen die Notwendigkeit einer derartigen strukturierten Vorgehensweise akzeptieren
  - Erhebliche Kosten mit nur begrenzt meßbarem unmittelbaren ROI
  - Schwierigkeit qualifizierte Mitarbeiter zu finden
    - Weiterbildung
- Alternative Konzepte: Managed Security Providers (MSP)
  - Bewertung der Qualität, Konsistenz der Dienstleistung schwierig
    - erfordert Fachwissen, ständige Überwachung
      - Mangel an diesen ist Grund für Dienstleistung des MSP...
  - Haftung verbleibt letztlich bei Kunden des MSP

Anomalien (1)

- Wichtigste Reaktion auf erkannte Anomalie ist nicht die Abwehr eines potentiellen Angriffs sondern Erfassung aller relevanter Daten, Spuren zur Erkennung des Angriffs und seines Umfangs
  - Viele Angriffe lassen sich erst aus weiteren Beobachtungsreihen oder durch genaue Prüfung der Revisionsdaten erkennen
- Revisionsmechanismen müssen schnell moduliert werden können
  - dies muß automatisiert geschehen können: Fehleranfälligkeit
  - erhöhte Revisionsdatenmengen dürfen nicht zu inakzeptabler Einschränkung des Regelbetriebes führen: Dimensionierung

Anomalien (2)

- Primäres Ziel qualifizierter Angreifer ist das Revisionssystem selbst
  - Bereitstellung mehrerer Pfade für Revisionsdaten, Synchronisation
  - Fehlen bekannter Datenmuster, Mengen kann Indiz für Manipulationen an Revisionssystem sein: Wiedereinspielung
- Autonom agierende Programme wie SETI@Home sowie diverse Anwendungsprogramme sorgen für ein „Hintergrundrauschen“ das die Erkennung deutlich erschwert
  - Angreifer können derartiges Verhalten bewußt zur Maskierung nutzen

Aktive Verteidigung

- Eigene offensive Maßnahmen sind verführerisch, aber
  - Identität des Angreifers ist selten zweifelsfrei festzustellen
  - Angreifer kann Adressen eines weiteren Gegners als Quelle ausweisen
  - Angriffe erfolgen meist von ihrerseits kompromittierten Systemen aus
  - Der Gesetzgeber trifft keine Unterscheidung, ob z.B. Computersabotage als Reaktion auf einen (vermeintlichen) Angriff durchgeführt wurde: Strafbar ist beides

Sammlung forensischer Daten

- Ausschließlicher Rückgriff auf Erfahrungen und Publikationen Dritter ist problematisch
  - Erfolgt nicht immer zeitnah - wenn überhaupt
  - Meist unvollständig, keine Veröffentlichung von Revisionsdaten, die Wiedererkennung erleichtern
  - Wahrheitsgehalt häufig nur partiell verifizierbar
- Aufbau eigener Datenverkehrsmuster-, auch Angriffsmuster-Datenbank ist notwendig
  - Baselining des eigenen Netzwerkes über längere Zeit zur Erkennung auch seltener „normaler“ Verkehrsmuster

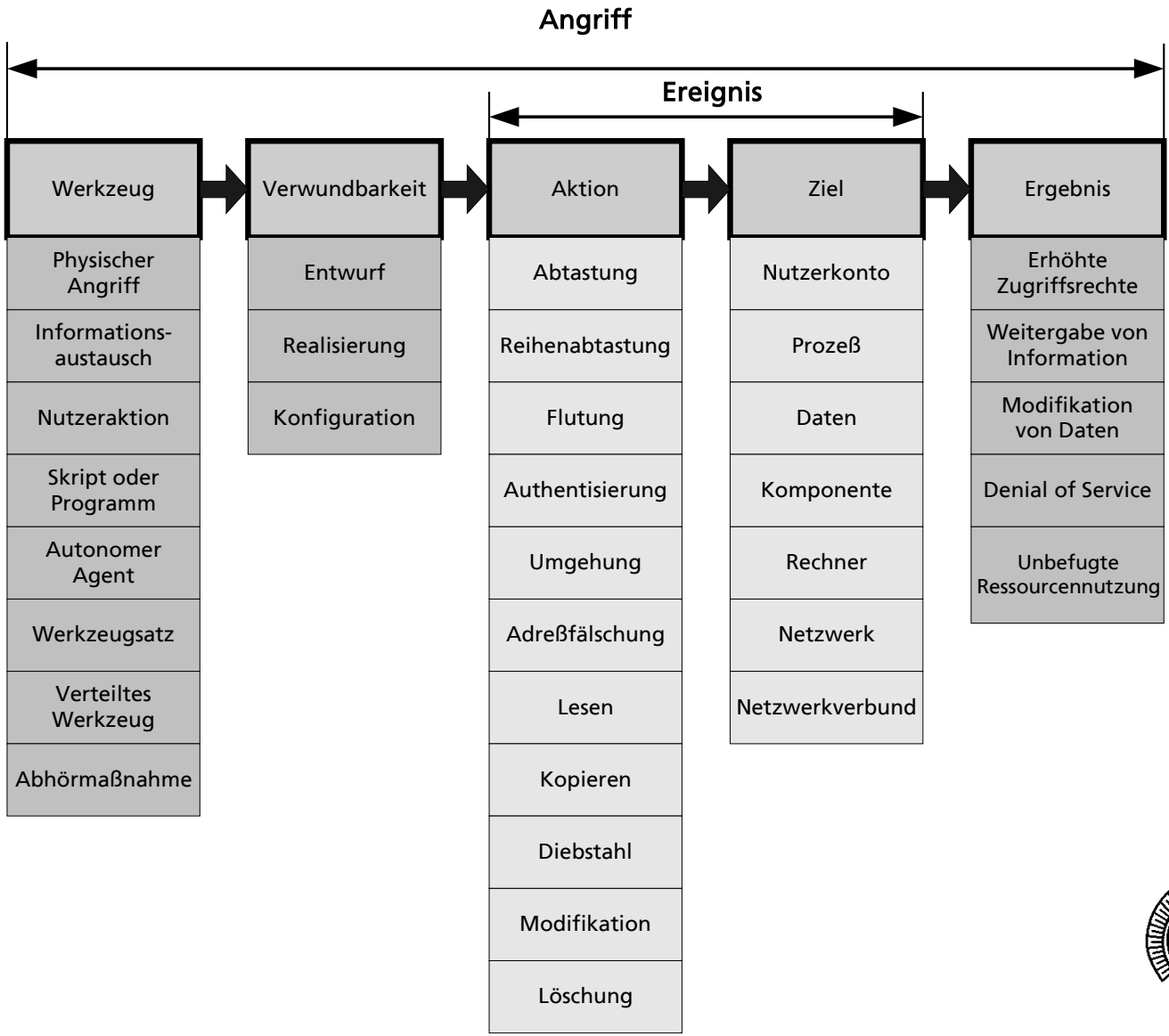
Austauschbarkeit forensischer Daten

- Berichte über Angriffe, Angriffsmuster und Anomalien sollten austauschbar sein
  - Koordinierung über Firmen-, nationale etc. CERTs (Computer Emergency Response Teams)
  - CERTs können untereinander über CERT-CC (Coordination Center) Informationen austauschen
  - Notwendigkeit der Authentisierung von Berichten, Handlungsanweisungen
- Austauschbarkeit und Wiederfindung erfordert gemeinsame oder zumindest konvertierbare Taxonomie

Taxonomie für Angriffe

- Separierung von Angriffen in Komponenten
  - Werkzeug
  - Verwundbarkeit
  - Aktion
  - Ziel
  - Ergebnis
    - Zusammengesetztes Tupel aus (Aktion,Ziel)
- Angriffe können aus Sequenzen/Mengen von Ereignissen bestehen

Taxonomie für Angriffe



Taxonomie für Aktionen (1)

- Abtastung
  - Zugriff auf ein Ziel mit dem Zweck, dessen Charakteristiken zu bestimmen
- Reihenabtastung
  - Abtastung einer Menge von Zielen zur Bestimmung von Charakteristiken der Einzelziele oder der Zielmenge
- Flutung
  - Wiederholte Zugriffe mit dem Zweck, das Ziel zu überlasten
- Authentisierung
  - Angabe von Authentisierungsinformationen mit dem Zweck, Zugriff auf weitere Zielelemente zu erhalten

Taxonomie für Aktionen (2)

- Umgehung
  - Vermeidung eines (geschützten) Zugriffspfades auf ein Ziel mit dem Zweck, dieses über alternativen Pfad zu erreichen
- Adreßfälschung
  - Angabe falscher Ursprungsadresse bei Netz-Kommunikation
- Lesen
  - Zugriff auf geschützte Information unter Kontrolle des Ziels
- Kopieren
  - Duplikation geschützter Informationen unter Kontrolle des Ziels ohne daß diese dem Ziel verloren gehen

Taxonomie für Aktionen (3)

- Diebstahl
  - Entfernung von Informationen aus dem Kontrollbereich des Zieles
- Modifikation
  - Modifikation des Zieles oder von Ressourcen unter der Kontrolle des Zieles
- Löschung
  - Entfernung oder Zerstörung von Ressourcen unter der Kontrolle des Zieles stehen oder des Zieles selbst

Taxonomie für Ziele (1)

- Nutzerkonto
  - Erlangung von I&A-Merkmalen
- Prozeß
  - In Ausführung befindliches Programm, Stack, Register, Dateien
- Daten
  - Rechnerlesbare Repräsentationen von Informationen, sonstige für Betrieb notwendige Ressourcen
- Komponente
  - Bestandteil eines Rechner- oder Netzwerksystems

Taxonomie für Ziele (2)

- Rechner
  - System bestehend aus mehreren Komponenten, insbesondere einer CPU, Speichermechanismen
- Netzwerk
  - Verbund aus Rechnern, (evtl. aktiven) Verbindungselementen
- Netzwerkverbund
  - Verbund aus Netzwerken

Definition Angriff, Taxonomie für Werkzeuge (1)

- Ein Angriff ist in diesem Modell eine Reihe von Schritten bestehend aus einem oder mehreren Ereignissen sowie drei weiteren Elementen. Werkzeug:
- Physischer Angriff
  - Physischer Zugriff auf System oder Netzwerk, dessen Komponenten oder notwendiger Infrastruktur
- Informationsaustausch
  - Erlangung von Informationen die zur erfolgreichen Durchführung des Angriffs notwendig sind („social engineering“)

Taxonomie für Werkzeuge (2)

- Nutzeraktion
  - Ausnutzung von Verwundbarkeit durch Erteilung direkter Befehle an Prozeß
- Skript oder Programm
  - Ausnutzung von Verwundbarkeit durch Erteilung von Befehlen via ausführbaren Dateien, Skripten (z.B. Trojaner)
- Autonomer Agent
  - Ausnutzung von Verwundbarkeit durch Programm (-Fragment) das unabhängig von Interaktion mit Nutzer agieren kann (Viren, Würmer)

Taxonomie für Werkzeuge (3)

- Werkzeugsatz
  - Sammlung von anderen Werkzeugen (z.B. root kits)
- Verteiltes Werkzeug
  - Werkzeuge die auf mehreren Systemen parallel zum Einsatz kommen und koordiniert verwendet werden (z.B. DDoS)
- Abhörmaßnahme
  - Abhören von Abstrahlungen oder elektrischen Verbindungen (z.B. Bluetooth, 802.11*x*)

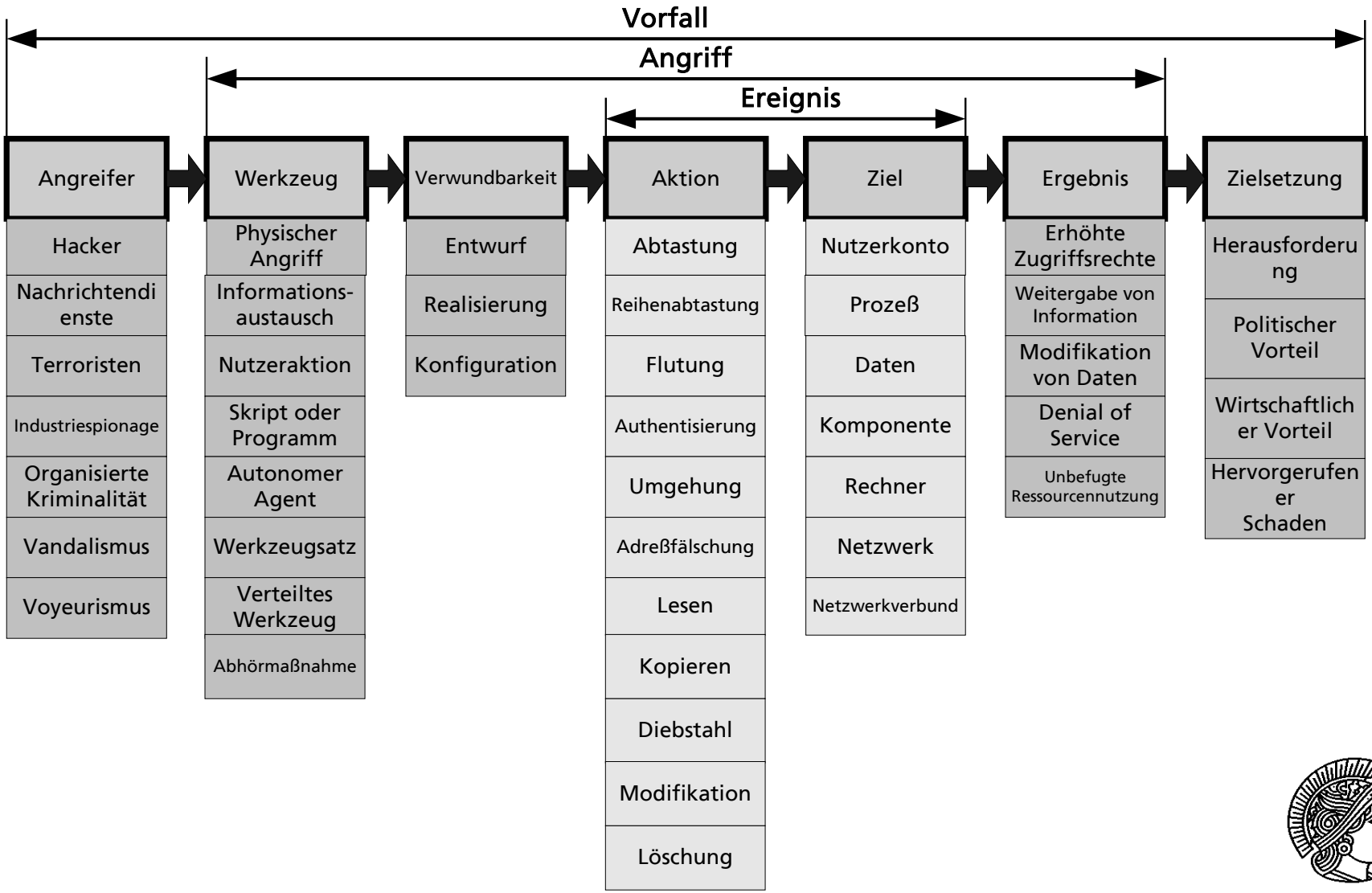
Taxonomie für Verwundbarkeiten

- Entwurf
  - Verwundbarkeit, die selbst bei fehlerfreier Implementierung und Konfiguration existieren würde
- Realisierung
  - Verwundbarkeit, die durch fehlerhafte Implementierung eines nicht selbst verwundbaren Entwurfes entstanden ist
- Konfiguration
  - Verwundbarkeit, die durch fehlerhafte Konfiguration einer nicht selbst verwundbaren Implementierung entstanden ist

Taxonomie für Ergebnisse von Angriffen

- Erhöhte Zugriffsrechte
  - Erweiterung der Rechte des Angreifers für Ressourcenzugriff
- Weitergabe von Information
  - Offenlegung von Daten, Informationen an Unbefugte
- Modifikation von Daten
  - Unbefugte Änderung oder Löschung von Daten
- Denial of Service
  - Reduzierung von Verfügbarkeit, Geschwindigkeit etc. für befugte Nutzer
- Unbefugte Ressourcennutzung

Taxonomie für Sicherheitsvorfälle



Taxonomie für Angreifer (1)

- Hacker
  - Primäre Motivation ist Herausforderung des Angriffs, Anerkennung durch Gleichgesinnte, Gefahr der Erkennung
- Nachrichtendienst
  - Ziel ist Erlangung direkter oder mittelbarer strategischer oder taktischer Informationen, oder Durchführung von Handlungen zum Vorteil des Staates
- Terroristen
  - Nichtstaatliche Gruppen, deren Ziel direkte, mittelbare strategische oder taktische Informationen oder Handlungen zur Durchsetzung nachgeordneter Ziele

Taxonomie für Angreifer (2)

- Industriespionage
  - Ziel ist Erlangung von Vorteilen gegenüber dem Opfer zur Sammlung des Opfers ist, Rückverfolgbarkeit ist kritisch
- Organisierte Kriminalität
  - Erlangung von Informationen oder aber auch Bedrohung des Betriebes selbst
- Vandalismus
  - Primäres Ziel ist die Anrichtung von Schäden, meist ungezielt
- Voyeurismus
  - Erlangung von Informationen ohne direkten Gewinn oder Vorteil

Juristische Verfolgung

- Fast alle Delikte sind Antragsdelikte, Aufwand für Verfolgung in Verbindung mit Erfolgswahrscheinlichkeit läßt dies selten gerechtfertigt erscheinen
  - Mitarbeiter der IT-Sicherheit müssen für die Dauer von Ermittlungs- und Strafverfahren abgestellt werden
  - Durch Veröffentlichung entsteht eventuell größerer Schaden als durch den Angriff selbst
  - Selbst bei klarer Beweislage ist Auslieferung aus Drittstaaten nur dann möglich, wenn die Straftat im Drittstaat selbst eine Straftat darstellt

Sammlung von Beweismaterial

- Beweismaterial muß Angriff, resultierende Schäden dokumentieren
  - tragfähige Verknüpfung des beobachteten Verhaltens mit Angriff und Quelle des Angriffes
- Beweismaterial muß derart gesichert sein, daß nachträgliche Manipulation der Revisionsdaten unwahrscheinlich sind
  - Hinterlegung bei Dritten, Absicherung durch digitale Signaturen und Zeitstempel von Dritten
- Manipulation kann auch „harmlose“ Korrektur, Auslassung, Nachbearbeitung sein

Fernwartungswerkzeuge

- Nach erfolgreicher Kompromittierung des Netzwerkes oder aber durch Datenträger eingeschleppter Code
  - ermöglichen Vertiefung von Angriffen in Zielnetzwerk
  - bessere Werkzeuge maskieren Kommunikation mit Steuerungssystem, Erkennung durch Firewall schwierig
- Back Orifice
  - Im August 1998 von „Cult of the Dead Cow“ veröffentlicht
  - Zunächst nur unter Windows 95/98 einsetzbar: Programmierfehler
  - Seit 1999: BO2K (ff.), auch unter NT (3.x, 4.0, 2000, XP)

Maskierungstechniken von BO2K

- Verwendet Dateinamen, die regulär nicht sichtbar sind
- Ausführung erfolgt als Parasiten-Thread innerhalb eines anderen Prozesses - Default: EXPLORER.EXE
  - Initialer eigener Prozeß wird nach Infektion des Wirtsprozesses beendet, Trägerprogramm wird nach initialer Infektion gelöscht
  - BO2K kann bei Beenden des Wirtes zu einem anderen Prozeß migrieren
  - Installiert sich für automatischen Neustart, unter NT auch als System Service (keine EXE-Signatur erforderlich)

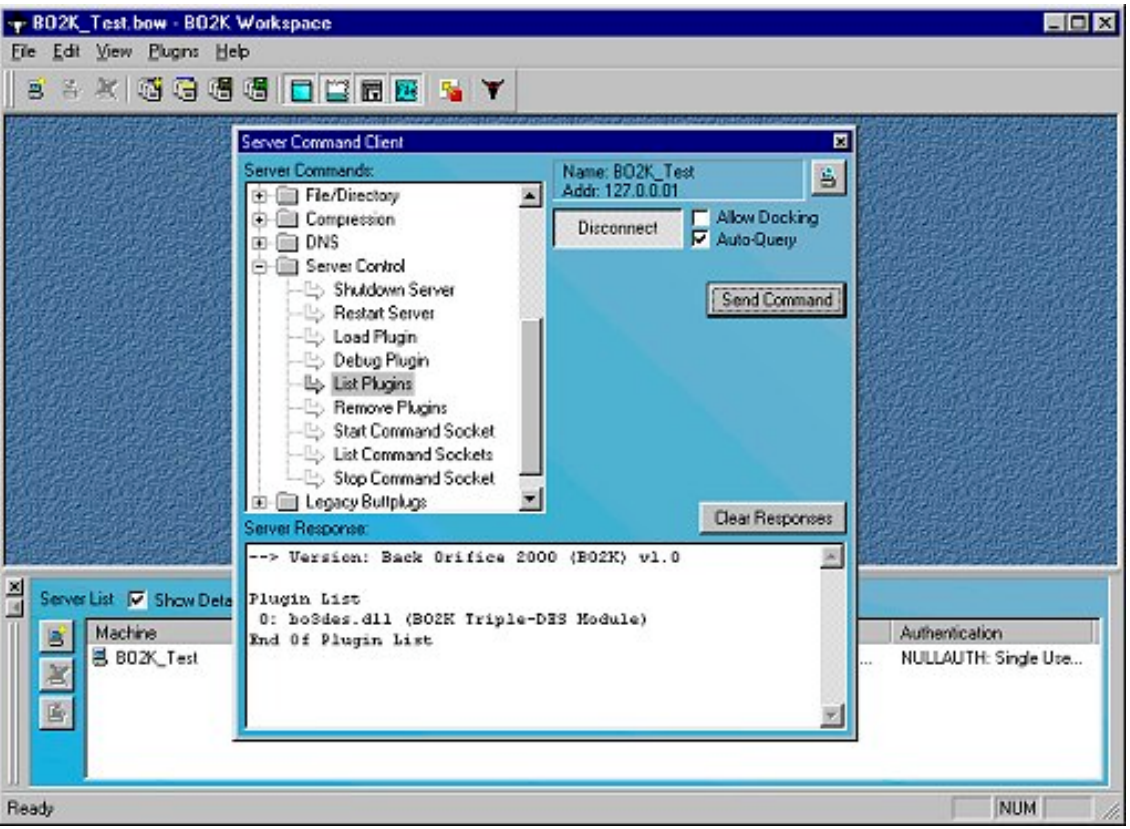
Fähigkeiten von BO2K (1)

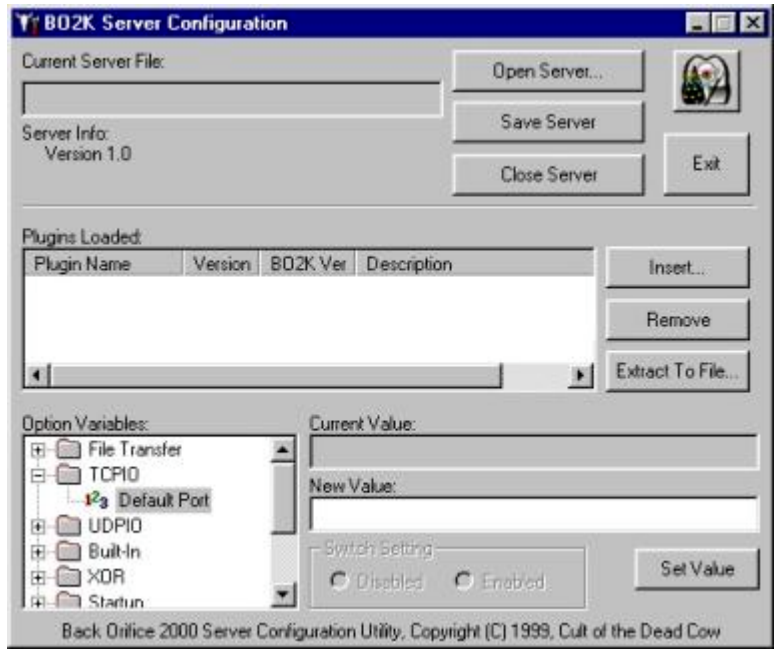
- Zugriff auf kompromittiertes System kann sogar von einem graphischen Werkzeug auch erfolgen
- Angriffsmuster: Angreifer oder Trittbrettfahrer durchsuchen Netzwerkblöcke auf beabsichtigte (auch durch andere Angreifer) oder unbeabsichtigte Infektionen
  - Schnittstelle kann auch mit kryptographischen Mechanismen gesichert sein
  - Ports können dynamisch konfiguriert werden
  - Gesammelte Daten können bei Aktivierung eines Ports durch Opfer mitgesendet „piggybacked“ werden
  - Kommunikation ist auch mit anderen Protokollen (z.B. IPX) möglich

Fähigkeiten von BO2K (2)

- Protokollierung von Tastenanschlägen
- Überwachung, Durchführung von CIFS-Zugriffen
- Auslesen, Modifizieren der lokalen Registry
- Umleiten von TCP-Verbindungen
- Umleitung von Ein-/Ausgabe von Konsolenanwendungen
- Umleitung von Audio-/Videodaten
- Start, Neustart von Prozessen
- Neustart des gesamten Systems
- Steuerung angeschlossener Telephone und Modems

BO2K





Fraunhofer IGD Institut Graphische Datenverarbeitung

Weitere Fernwartungswerkzeuge

- Quellcode von BO2K war verfügbar, viele Nachahmer
  - Deep Throat, Acid Shivers, Back Door, Baron, Blade Runner, Devil, Hack‘a‘Tack, Master‘s Paradise, NetBus, SubSeven,...
- Maskierungstechniken für Code ähnlich dem von Viren sind mittlerweile verbreitet
- Datenverkehr wird durch autonom agierende Programme oder auch Dienste wie z.B. RC-Challenges, SETI@Home unbeabsichtigt maskiert
  - In Verbindung mit Piggybacking-Fähigkeit stellen derartige Anwendungen perfekte Ablenkmanöver dar

Root Kits

- Ähnliche Problematik wie unter Windows existiert seit langem in Form von Root Kits unter Unix.
  - Bereitstellung direkten Zugriffs für Angreifer
    - Verfügbar selbst dann, wenn ursprünglich ausgenutzte Verwundbarkeit entfernt wird
  - Verbergen von Aktivitäten des Angreifers vor anderen Nutzern und Administratoren
- Traditionell: Austausch von Verwaltungswerkzeugen wie `ls`, `ps`
  - Unterdrücken von setuid-Programmen, Prozessen mit Verbindung nach außen: Entfernen eigener Spuren aus Logs

Moderne Root Kits

- Traditionelle Root Kits decken nicht alle Möglichkeiten der eigenen Erkennungen ab, z.B. **`procfs`**
- Moderne Unix-Derivate und Linux weisen modularen Kernel auf
  - Kernel muß bei Änderungen nicht übersetzt werden
  - Häufig können Module zur Laufzeit hinzugefügt werden
- Loadable Kernel Module (LKM) Root Kits können dies nutzen: Nur system calls müssen Verhalten maskieren
- Beispiel: **`getdents(2)`**: Jedes Programm zur Anzeige des Inhalts von Dateisystemen muß hierauf zurückgreifen
- LKM Root Kits auch unter Windows NT: NullSys, NTROOT,...

LKM Root Kits unter Linux (1)

- Linux Root Kits sind besonders populär und häufig anzutreffen (hier nur eine kleine Auswahl)
- Heroin
  - Trotzdem leicht zu erkennen, da Programmname im Klartext zu finden: **`cat /proc/kmsys | grep -i heroin`**
- Sysnapsis
  - Verbirgt erfolgreich Dateien, Prozesse, Nutzer, verwendete Ports, ist in **`lsmod`** nicht zu finden
  - Durch Hintertür in cat(1) zu steuern
  - Entwickler hat jedoch wieder etwas übersehen: **`cat /proc/modules`**

LKM Root Kits unter Linux (2)

- itf
  - Publikation in Phrack 52 (Februar 2000)
  - Verbergen von Dateien und Prozessen, maskiert auch PROMISC-Flag auf Netzwerkschnittstellen
  - Verbergen vor Anzeige in **`/proc/modules`** erfolgt durch Löschen des Namens und Referenzen in **`init_module()`:** Kernel sieht diese als Basismodul an und unterdrückt diese
  - Modifikation von **`get_kernel_symbols()`** vermeidet Anzeige in **`/proc/kmsys`**
  - Mehrere Hintertüren, z.B. setuid auf 31337, Empfang eines Datagramms mit Inhalt **`w00w00T$!`**

LKM Root Kits unter Linux (2)

- SucKIT
  - Publikation in Phrack 58 (Dezember 2001)
  - Bekannt geworden z.B. durch Kompromittierung von Debian-Server, FSF-Server (August...November 2003)
    - versteckt Netzwerkverbindungen (z.B. Backdoor-Shells) vor Rest des Systems

Schutz vor LKM Root Kits: BSD Security Levels

- Einschränkungen für Modifikationen des Kernels, z.B. OpenBSD:
- -1: Permanently insecure mode
  - security level kann nicht modifiziert werden, sonst wie 0
- 0: Insecure mode
  - Gerätedateien dürfen gelesen, geschrieben werden, Attribute von Systemdateien dürfen geändert werden
- 1: Secure mode
  - Keine Verringerung möglich außer durch **`init(1M)`**, Beschreiben von **`/dev/mem`**, **`/dev/kmem`** verboten, Laden, Entfernen von kernel modules verboten
- 2: Highly secure mode
  - Verbietet Schreiben auf raw devices, Korrektur von **`settimeofday`**, Firewall-, NAT-Regeln

Analyse der Penetrationstiefe

- Wann wurde welches System kompromittiert, welche Angriffsmechanismen wurden verwendet ?
  - Erkennung von Root Kits ist hier besonders schwierig
  - Meist wird keine interne Tiefenstaffelung der Verteidigung verwendet: Interne Systeme verwenden prinzipiell unsichere Protokolle wie CIFS und NFS
- Gefahren durch (subtile!) Modifikationen von Datenbeständen: Plausibilität, interne Konsistenz, Abgleich mit älteren Beständen
  - Notwendigkeit weitreichender unabhängiger Sicherungen
  - Wiedereinschleppung von Viren, Trojaner durch Backups

Wiederherstellung des Regelbetriebes

- Muß schnellstmöglich erfolgen, unmittelbare Bedrohung muß abgewehrt werden
- Detailierte Analyse des Vorfalls,Feststellung von Zeitpunkt und Umfang der Kompromittierung erfordern jedoch erheblichen zeitlichen und personellen Aufwand
  - Dies ist Aufgabe der Forensik-Gruppe
- Problem: Eventuell ist erneute Unterbrechung und Rückführung des Systems nach Analyse durch Forensik-Gruppe erforderlich
  - Schwierigkeit politischer Durchsetzbarkeit