(Un-) Sicherheit von Virtualisierungslösungen

IT-Virtualisierung Forum, 25.09.2007

Stefan Gora
stefan.gora@secorvo.de

secorvo
security consulting

Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
D-76137 Karlsruhe

Tel. +49 721 255171-0
Fax +49 721 255171-100
info@secorvo.de
www.secorvo.de

Secorvo Security Consulting

- **Unabhängiges Beratungsunternehmen für IT-Sicherheit und Datenschutz**
- **Ausbildungspartner von BSI, Bosch Sicherheitssysteme, SAP, Schering und T-Systems**
- **Landespreis Baden-Württemberg 2002**
- **Kunden: BMW, DaimlerChrysler, BASF, Heidelberger, Deutsche Bank, FinanzIT, Datev, Michelin, Toll Collect, Krones, Tchibo, SEW, Commerzbank, Bundesbank, BSI, Gardena, Deutsche Bahn, Benteler, Roland Berger, EZB, Linde, Liebherr, Novartis, Deutsche Post, WDR, FhG, RWE, BNetzA, DZ-Bank, Hartmann, SWR, ZF, ...**

L-BANK
Landespreis für junge Unternehmen

secorvo
security consulting

Inhaltsübersicht

- Risikotransfer bei Einsatz von Virtualisierung
- Im Fokus: Vor- und Nachteile aus Sicherheitssicht
- Neue Sicherheitsrisiken und –anforderungen
- Gefahren durch Hardware Virtualization Based Rootkits, Beispiele

secorvo
security consulting

Inhaltsübersicht

- **Risikotransfer bei Einsatz von Virtualisierung**
- Im Fokus: Vor- und Nachteile aus Sicherheitssicht
- Neue Sicherheitsrisiken und –anforderungen
- Gefahren durch Hardware Virtualization Based Rootkits, Beispiele

secorvo
security consulting

Risikotransfer

- **Einsatz von Virtualisierungslösungen ist nicht risikofrei**
  - **Verlagerung von Risiken Hardware -> Risiken Software (Servervirtualisierung)**
  - **Verlagerung von Risiken lokale Festplatten -> Risiken SAN (Storagevirtualisierung)**
  - **Sicherheitskonzepte für Virtualisierung fehlen oft**

secorvo
security consulting

Risikoreduktion

- Einfache Einführung von Netzwerksegmentierung bei Servervirtualisierung
  - Virtuelle Netzwerke anstatt flache Netzsegmente
- Vereinheitlichung von Hard- und Software bei Serversystemen (VM Bibliothek)
- Behebung von Ressourcenengpässen
- Ggf. kostengünstige Hochverfügbarkeit
- Sehr kurze Restore-Zeiten bei fehlerhaften Patches oder Konfigurationsänderungen
- ...

secorvo
security consulting

Unveränderte Risiken

- Sicherheitsprobleme bestehen nach wie vor für Serversysteme
  - Hardening
  - Patch-Management (ggf. deutlich vereinfacht)
  - Laufende Überwachung von Systemen, Logfileauswertung, Alarmierung, Eskalation bei Vorfällen
  - ...
- Sicherheitsprobleme bestehen nach wie vor für Anwendungen
  - Softwareschwachstellen
  - Konzeptfehler
- Schwachstellen sind inzwischen hauptsächlich auf Anwendungsebene zu finden

secorvo
security consulting

Unveränderte Risiken

- Sicherheitsprobleme bestehen nach wie vor für Serversysteme
  - Hardening
  - Patch-Ma
  - Laufende eauswertung, Alarmieru
  - ...
- Sicherheitsprobleme bestehen nach wie vor für Anwendungen
  - Softwareschwachstellen
  - Konzeptfehler
- Schwachstellen sind inzwischen hauptsächlich auf Anwendungsebene zu finden

Virtualisierung ist kein Allheilmittel um Sicherheit zu schaffen

secorvo security consulting

Inhaltsübersicht

- Risikotransfer bei Einsatz von Virtualisierung
- **Im Fokus: Vor- und Nachteile aus Sicherheitssicht**
- Neue Sicherheitsrisiken und –anforderungen
- Gefahren durch Hardware Virtualization Based Rootkits, Beispiele

secorvo
security consulting

Vorteile aus Sicherheitssicht

- **Hardwarekonsolidierung**
  - **Kosteneinsparung**
  - **Vereinheitlichung der Hardware (weniger Störgrößen)**
  - **potentiell Verringerung von Ausfallswahrscheinlichkeiten**
- **Schnelle Reaktionsmöglichkeiten bei kurzfristigen Anforderungen**
- **Zentrale Verwaltung**
- **Einfache Fall-Back-Mechanismen Patch-Management**
- **Eleganter Aufbau von Test- und Laborinfrastrukturen**
- **Weitere?**

secorvo
security consulting

Nachteile aus Sicherheitssicht

- Aufwände für Sicherheitskonzeption (Server-Virtualisierung, Netzwerk, SAN, ...) oft nicht eingeplant
- Erhöhte Anforderungen an administratives Personal und Administrationskonzepte
- Bei entsprechendem Schutzbedarf erhöhte Aufwände zur Durchführung sicherheitskritischer Änderungen
  - Vier-Augenprinzip
  - Trennung von Umsetzung und Abnahme
- Erhöhte Abhängigkeit von zentralen Infrastrukturen
- Zusätzliche Hard-/Software kann zusätzliche Probleme generieren
- Neue Risiken müssen betrachtet und bewertet werden

secorvo
security consulting

Inhaltsübersicht

- Risikotransfer bei Einsatz von Virtualisierung
- Im Fokus: Vor- und Nachteile aus Sicherheitssicht
- **Neue Sicherheitsrisiken und –anforderungen**
- Gefahren durch Hardware Virtualization Based Rootkits, Beispiele

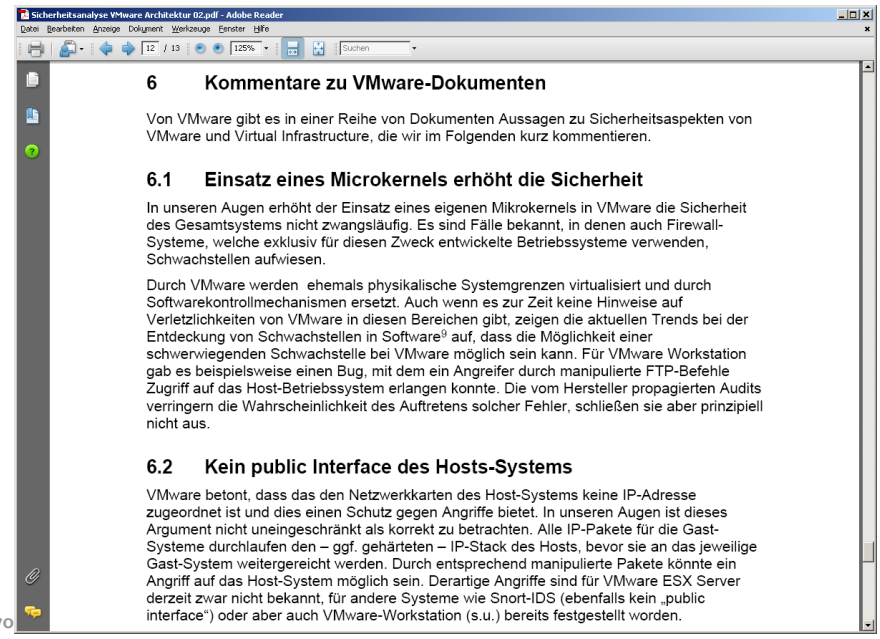
secorvo
security consulting

Neue Risiken

- Potentieller Einfluss von Gast auf Hostsystem und umgekehrt
- Gegenseitige Beeinflussung der Gastsysteme
  - Im Extremfall könnte ein gestörtes System weitere Systeme in Mitleidenschaft ziehen
  - Wie werden Minimalressourcen für Gastsysteme definiert?
- Hoher „impact“ bei Problemen der Virtualisierungs-software, ggf. zahlreiche Systeme betroffen
- Bugs/Softwareschwachstellen in Virtualisierungssoftware
  - Denial-of-Service
  - Übernahme von Systemen

secorvo
security consulting

Risikobewertung Hersteller-aussagen erforderlich


Sicherheitsanalyse VMware Architektur 02.pdf - Adobe Reader

Datei Bearbeiten Anzeige Dokument Werkzeuge Fenster Hilfe

12 / 13 125% Suchen

6 Kommentare zu VMware-Dokumenten

Von VMware gibt es in einer Reihe von Dokumenten Aussagen zu Sicherheitsaspekten von VMware und Virtual Infrastructure, die wir im Folgenden kurz kommentieren.

6.1 Einsatz eines Microkernels erhöht die Sicherheit

In unseren Augen erhöht der Einsatz eines eigenen Mikrokernels in VMware die Sicherheit des Gesamtsystems nicht zwangsläufig. Es sind Fälle bekannt, in denen auch Firewall-Systeme, welche exklusiv für diesen Zweck entwickelte Betriebssysteme verwenden, Schwachstellen aufwiesen.

Durch VMware werden ehemals physikalische Systemgrenzen virtualisiert und durch Softwarekontrollmechanismen ersetzt. Auch wenn es zur Zeit keine Hinweise auf Verletzlichkeiten von VMware in diesen Bereichen gibt, zeigen die aktuellen Trends bei der Entdeckung von Schwachstellen in Software[9] auf, dass die Möglichkeit einer schwerwiegenden Schwachstelle bei VMware möglich sein kann. Für VMware Workstation gab es beispielsweise einen Bug, mit dem ein Angreifer durch manipulierte FTP-Befehle Zugriff auf das Host-Betriebssystem erlangen konnte. Die vom Hersteller propagierten Audits verringern die Wahrscheinlichkeit des Auftretens solcher Fehler, schließen sie aber prinzipiell nicht aus.

6.2 Kein public Interface des Hosts-Systems

VMware betont, dass das den Netzwerkkarten des Host-Systems keine IP-Adresse zugeordnet ist und dies einen Schutz gegen Angriffe bietet. In unseren Augen ist dieses Argument nicht uneingeschränkt als korrekt zu betrachten. Alle IP-Pakete für die Gast-Systeme durchlaufen den – ggf. gehärteten – IP-Stack des Hosts, bevor sie an das jeweilige Gast-System weitergereicht werden. Durch entsprechend manipulierte Pakete könnte ein Angriff auf das Host-System möglich sein. Derartige Angriffe sind für VMware ESX Server derzeit zwar nicht bekannt, für andere Systeme wie Snort-IDS (ebenfalls kein „public interface“) oder aber auch VMware-Workstation (s.u.) bereits festgestellt worden.

secorvo
security consulting

Auszüge der Bewertung

- **„Einsatz eines Microkernels erhöht die Sicherheit“**
  - **Guter Ansatz: Dediziertes Betriebssystem für ESX Server**
  - **Dadurch nicht zwangsläufig Schutz vor Schwachstellen gegeben**
- **„Software wird regelmäßig extern auditiert“**
  - **Sehr guter Ansatz, dennoch kein Garant für Fehlerlosigkeit**
- **Kein „public interface“ des Hostsystems**
  - **Aber: Hostsystem steuert virtuelle Interfaces, Interaktion ist gegeben**
  - **Angriffsmöglichkeit prinzipiell gegeben**
    - **Beispiel 1: Angriffe auf Snort IDS-System (nur lauschende Netzwerkkarte)**
    - **Beispiel 2: Buffer Overflow bei NAT-Funktion von VMware Workstation**

secorvo
security consulting

- Links:
  - VNware NAT Schwachstellen http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4459

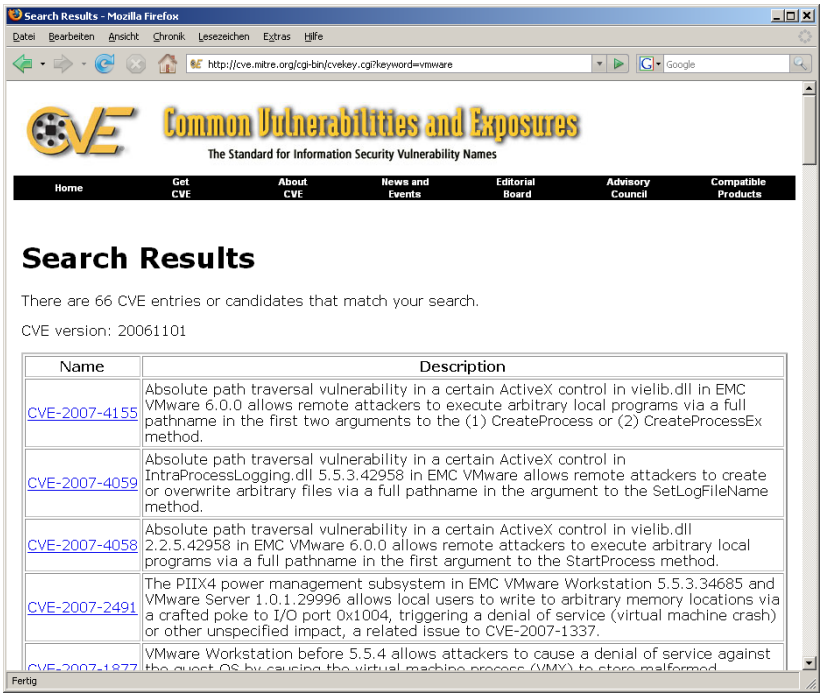
Auszüge der Bewertung

- **Verwendung von OpenSource Kerneltreiber**
  - **Positiv: Offen einsehbar, prinzipielle Prüfmöglichkeiten**
  - **Auch kein Garant für Aufdeckung von Schwachstellen**
  - **Ermöglicht ggf. sogar gezielte Angriffe, vgl. Übernahme von Systemen durch Ausnutzung Schwachstellen WLAN-Treiber**
- **Fazit**
  - **VMware legt hohen Wert auf Sicherheit, einige Aussagen kommen aber eher aus dem Bereich Marketing...**
  - **Schwachstellen können nicht ausgeschlossen werden**

secorvo
security consulting

- Links:
  - Schwachstellen WLAN-Treiber http://www.802.11mercenary.net/~johnycsh/publications/DC-devicedrivers.ppt

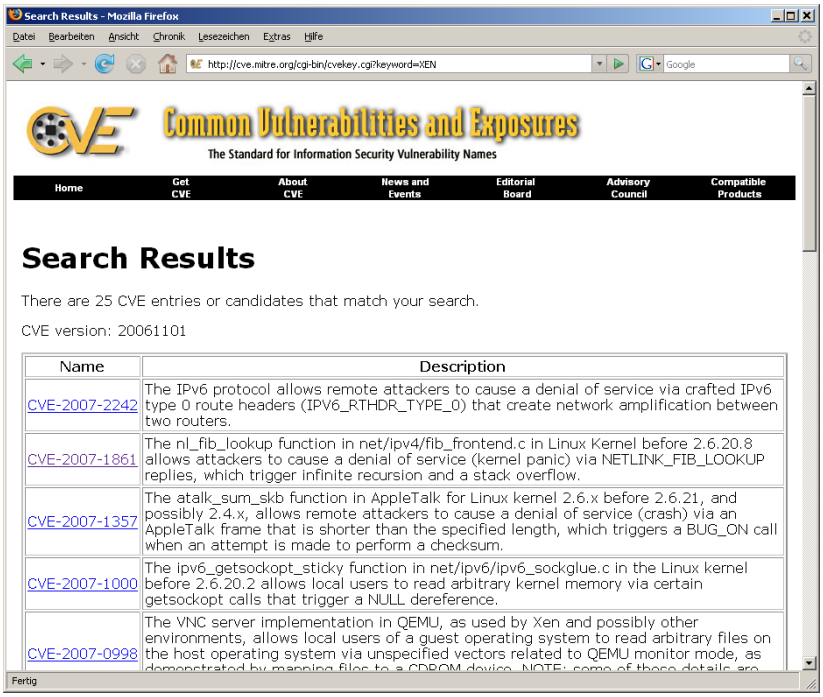
Schwachstellen VMware



secorvo
security consulting

- Links:
  - Schwachstellendatenbanken, z. B. http://cve.mitre.org/

Schwachstellen XEN



secorvo security consulting

- Links:
  - Schwachstellendatenbanken, z. B. http://cve.mitre.org/

Schwachstellen

- **Sind prinzipiell bedingt (100% fehlerfreie Software ist ein Idealziel), egal welcher Hersteller**
- **Sind kein Grund Virtualisierung nicht einzusetzen (-> Risikotransfer)**
- **Erfordern vernünftiges Patch-Management**

secorvo
security consulting

Sicherheitsanforderungen

- Durchdachtes Sicherheitskonzept Virtualisierung
- Vorab Anforderungen genau klären
  - Ziele?
  - Ressourcen?
  - Verfügbarkeitsanforderungen?
  - Budgets?
  - Einsatzszenarien?
- Prozesse für Change-Management
- Prozesse für Patch-Management
- Schulungen für Betreiber neuer Infrastrukturen (Aufwände und Kosten einplanen)

secorvo
security consulting

Netzwerkkonzeption VMware

- **Empfehlung: Getrennte Host-Systeme für LAN und DMZ**
  - Oft nur geringfügig erhöhte Kosten Hardware/Lizenzen
  - Erhöhte administrative Aufwände
  - Vorbeugung von Fehlkonfiguration
  - Beschränkung von Risiken bei Schwachstellen der Virtualisierungssoftware
  - Umgehung der Firewall prinzipiell nicht möglich
- **Empfehlung: Getrennte Produktiv- und Testnetzsegmente**
  - Gesondertes physikalisches Interface für VMware Workstation ohne Protokoll-Bindungen an Hostsystem

secorvo
security consulting

Inhaltsübersicht

- Risikotransfer bei Einsatz von Virtualisierung
- Im Fokus: Vor- und Nachteile aus Sicherheitssicht
- Neue Sicherheitsrisiken und –anforderungen
- Gefahren durch Hardware Virtualization Based Rootkits, Beispiele

secorvo
security consulting

Rootkits allgemein

- Angreiferwerkzeug (Software) welches dauerhaft den Zugang zu einem kompromittierten System ermöglicht
- Für die Übernahme/Kompromittierung eines Systems sind Schwachstellen (Konfigurationsfehler, Konzeptfehler, Softwarefehler) und ggf. weitere Angriffswerkzeuge wie Exploits erforderlich
- Rootkits werden in der Regel versteckt, so dass sie von den Systemverantwortlichen möglichst nicht erkannt werden
  - Beispiel: Austausch Befehl *ps* durch veränderte Version unter Linux, so dass Rootkit-Prozess nicht angezeigt wird

secorvo
security consulting

Beispiele

- **Windows**
  - **AFX Rootkit**
  - **FU**
  - **Hacker Defender**
  - **He4Hook**
  - **NT Rootkit**
  - **Vanquish**
- **Linux**
  - **Linux Rootkit (lrk3, lrk4, lrk5)**
  - **T0rnkit**
  - **Knark**
  - **Adore**
- **Virtual Machine Based Rootkits (VMBR)**
  - **Subvirt**
- **Hardware Virtualization Based Rootkits (HVBRK)**
  - **BluePill**
  - **(New) BluePill**
  - **Vitriol**

secorvo security consulting

- AFX Rootkit: http://www.iamaphex.net/
- FU: http://www.egocrew.de/download-file-182.html
- Hacker Defender: http://hxdef.czweb.org/
- He4Hook: http://www.egocrew.de/download-file-178.html
- NT Rootkit: http://www.megasecurity.org/Tools/Nt_rootkit_all.html
- Vanquish: http://www.egocrew.de/download-file-176.html

- Viele Linux-Rootkits:
  - http://www.eviltime.com/hx-rootkits.htm

Virtual Machine Based RK

- Erste Generation der Virtualisierung von Rootkits
- Bekanntestes Beispiel: „Subvirt“ (März 2006)
- Entwickelt von Forschern der Universität Michigan und Microsoft Research
- Eigenschaften:
  - installiert sich persistent auf Festplatte
  - ursprüngliches Betriebssystem wird als Gastsystem in VM-Instanz (Virtual PC) verlagert
  - Reboot erforderlich
  - längere Bootzeiten (erst neues Host-System, dann ursprüngliches OS als Gastsystem)
  - vollständige Kontrolle über das ursprüngliche OS gegeben (Dateneinsicht, Datenveränderung)
  - weitere VM-Instanzen mit Schadfunktionen möglich

secorvo security consulting

- Link: http://www.eecs.umich.edu/virtual/papers/king06.pdf

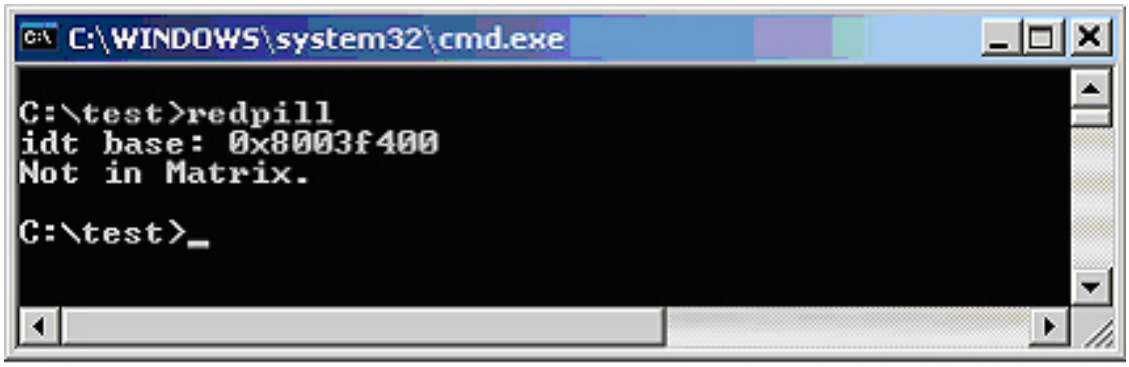
Eigenschaften Subvirt

- Rootkit kann vom Gastsystem aus nicht verändert werden, Reboot führt nur zu Neustart der VM-Instanz
- Für die Installation sind Administrator-Berechtigungen erforderlich
  - in der Praxis leider oft der Fall
- Erkennungsmöglichkeiten sind gegeben
  - längere Bootzeiten
  - verminderte Performance, insbesondere im 3D-Bereich
  - veränderte Hardware
  - forensische Festplattenuntersuchungen
  - (Netz-Überwachung der Systemaktivitäten auf Auffälligkeiten – aufwendig, schwierig)
  - Tools zur Identifikation von VM-Umgebungen

secorvo
security consulting

Beispiel „Redpill“

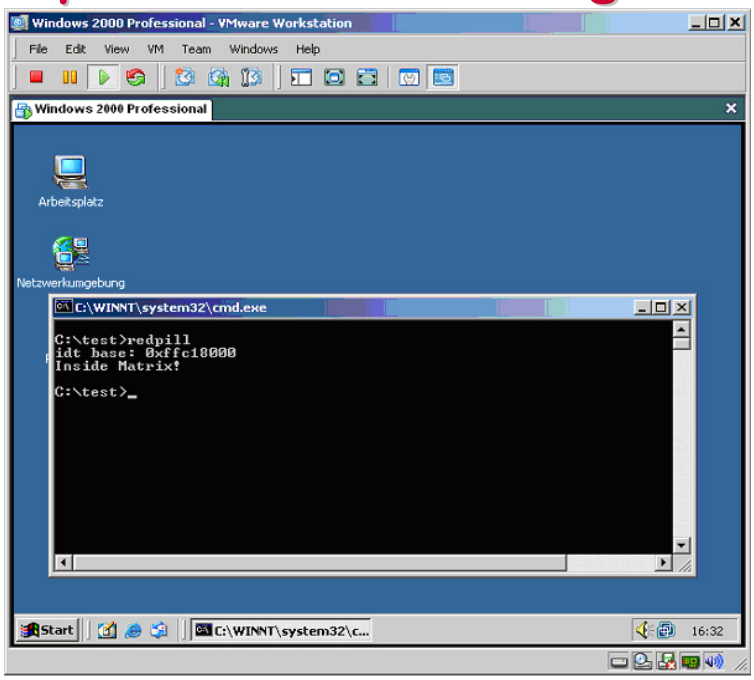
- **Tool zur Erkennung von VM-Umgebungen**
- **Auf nativer Hardware:**



secorvo
security consulting

- Links:
  - http://invisiblethings.org/papers/redpill.html

„Redpill“ in virtueller Umgebung



secorvo
security consulting

Hardware Virtualization Based RK

- **Aktuelle Generation von Rootkits**
- **Nutzen Hardware Virtualisierung aktueller CPUs aus**
  - **Bluepill (AMD64-SVM)**
  - **Vitriol (IA-32/64 Intel VT-x)**
- **Im laufenden Betrieb (!) wird eine Hypervisor-Schicht etabliert und das ursprüngliche Betriebssystem virtualisiert**
- **Kein Reboot erforderlich**
- **Keine Veränderungen der Festplatte feststellbar**
- **Keine Veränderungen der Hardware feststellbar**
- **Daher als „Stealth Malware“ bezeichnet**

secorvo
security consulting

- Links:
  - Bluepill: http://www.invisiblethings.org/papers/joanna%20rutkowska%20-%20subverting%20vista%20kernel.ppt
  - Vitriol: https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Zovi.pdf

Neue Risiken

- **Obwohl das Verfahren bekannt ist, ist eine Erkennung nur sehr schwer möglich**
  - **beispielsweise über Abfrage EFER-Register (Extended Feature Register bei AMD, Bit 12 zeigt Nutzung von SVM an)**
  - **Abfrage könnte jedoch auch vom Hypervisor abgefangen und verfälscht werden -> Zusätzliche Messung des Timingverhaltens mit einer externen Uhr erforderlich**
- **Weitere Schadfunktionen wie Remote Zugriff, Keylogger, Dateneinsicht etc. können fast unsichtbar implementiert werden**

secorvo
security consulting

Entwicklungen Q3/2007

- **Umfangreiche Diskussionen zu Erkennungs-möglichkeiten von HVBRK im Vorfeld der Blackhat**
  - **Viele diskutierte Ansätze funktionieren in der Praxis nicht**
  - **Gegenstand von Diskussionen im Forschungsumfeld**
- **(New) BluePill wurde von Joanna Rutkowska und Alexander Tereshkin auf der Blackhat 2007 vorgestellt**
  - **„Blue Chicken“ als Abwehr von bestimmten Erkennungs-maßnahmen implementiert**
  - **„Nested Hypervisors“: Rootkit erkennt wenn ein neuer Hypervisor eingerichtet werden soll (mögliche Erkennungsmethode) und nutzt Verschachtelung mehrerer Hypervisoren**
  - **Source Code als Proof-of-Concept und weitere Info‘s unter http://bluepillproject.org**

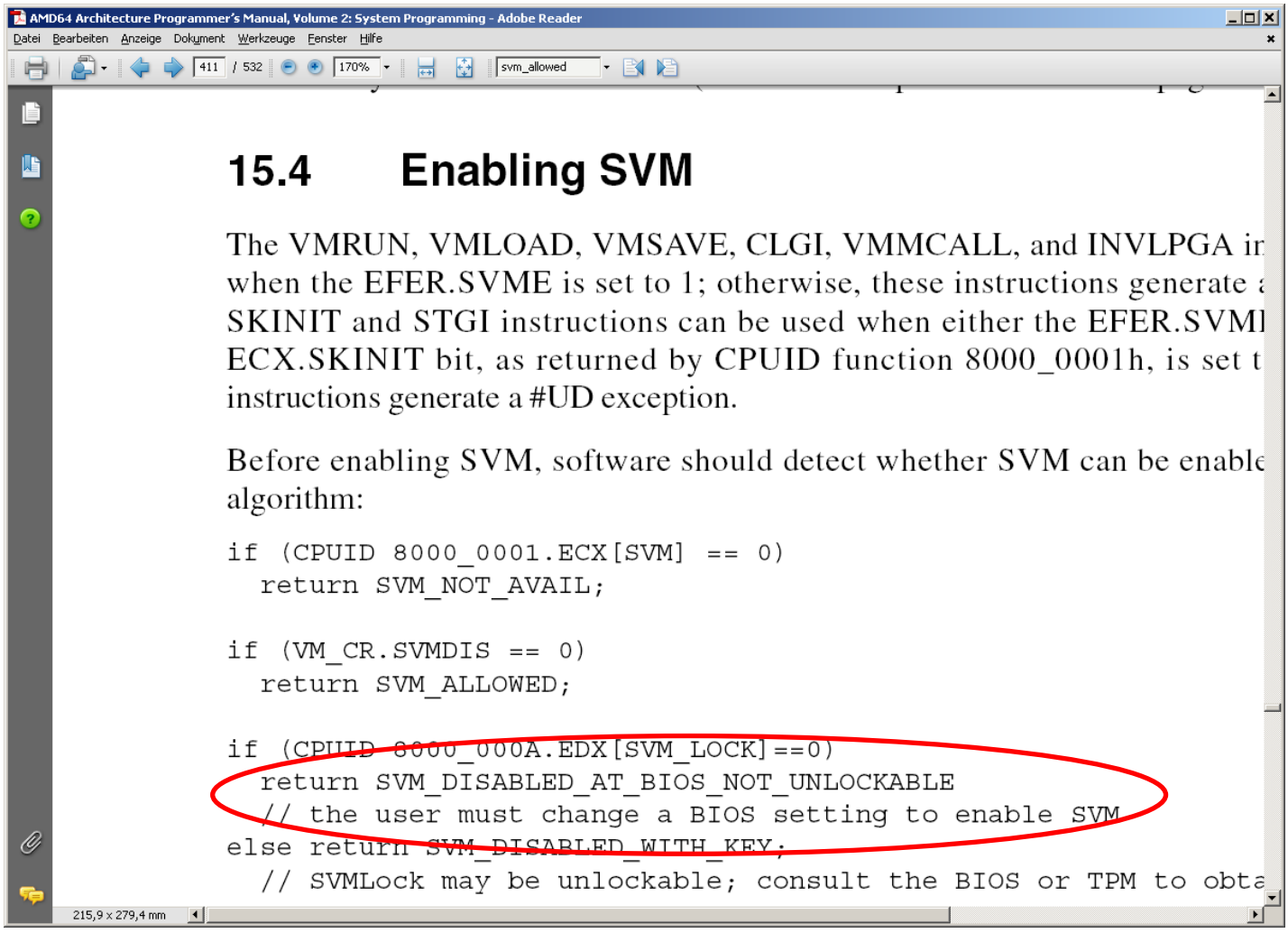
secorvo
security consulting

Präventive Gegenmaßnahmen

- **„know your enemy“: Beobachtung der aktuellen Entwicklungen; „in the wild“ (bisher) keine gemeldeten Vorkommen**
- **Wenn Virtualisierung potenziell genutzt werden soll: Virtualisierung von Anfang an einsetzen, vorhandener Hypervisor kann nicht überschrieben werden**
- **Wenn Virtualisierung nicht genutzt werden soll – sofern möglich – im BIOS deaktivieren**
- **Standardmaßnahmen zur Reduktion der Angriffsmöglichkeiten (Patch Management, Netzsegmentierung, organisatorische Anweisungen, Awareness, etc.)**

secorvo
security consulting

- Im Juli 2007 wurde im AMD-Handbuch (http://www.amd.com/us-en/assets/content_type/white_papers_and_tech_docs/24593.pdf) veröffentlicht wie der SVM-Modus geschützt werden kann:



Fazit

- Virtualisierung vereinfacht viele Aufgabenstellungen
- Virtualisierung hat Charme und bietet viele Vorteile, ...
- ... schafft aber neue Problemfelder und Risiken...
- ... welche aber durchaus lösbar und eingrenzbar sind

secorvo
security consulting

Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
D-76137 Karlsruhe

Tel. +49 721 255171-0
Fax +49 721 255171-100
info@secorvo.de
www.secorvo.de