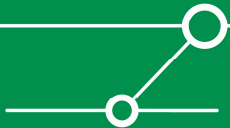


# **ESX (In-) Security**

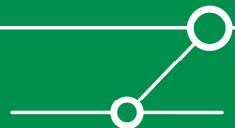
**[Aktuelle ESX Sicherheit]**

Roger Klose (rklose@ernw.de)

Gunther Niehues (gniehues@ernw.de)

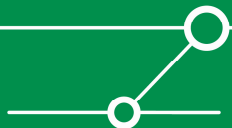


- **2001** gegründeter Netzwerk-Dienstleister mit **Sicherheits-Fokus**, Sitz in Heidelberg (+ kleines Büro in Lissabon)
- **Aktuell fünfzehn Mitarbeiter**
- **Schwerpunkte: Security Management, Audit/Revision, Penetrations-Tests, Security Research**
- **Kunden (Europa/USA): Industrie, Banken, Behörden, Provider**
- **Regelmäßige Sprecher auf internationalen Sicherheits-Konferenzen (Black Hat, IT Underground, HITB etc.)**



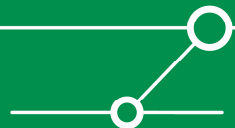
# Agenda

- **Betrachtung einer “neuen“ Technologie**
- **Virtualisierung**
- **Angriffs-Szenarien**
- **Historische Vorfälle**
- **BCP**
- **Untersuchung ESX**
- **Lessons Learned**
- **Ausblick**
- **Diskussion**



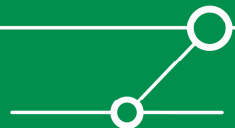
# Betrachtung einer "neuen" Technologie

- **Assets** (Das zu schützende Gut)
- **Objectives** (Ziele)
- **Threats** (Bedrohung)
- **Vulnerabilities** (Schwachstellen)
- **Risk** (Risiko)
- **Mitigating Controls** (Gegenmaßnahmen)



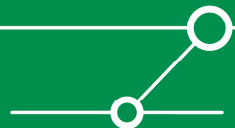
# Definition

“*Virtualization* is the creation of substitutes for real resources, that is substitutes that have the same functions and external interfaces as their counterparts, but that differ in attributes, such as size, performance, and cost. These substitutes are called *virtual resources*, and their users are typically unaware of the substitution.” [1]



genauer ...

- **Erzeugung von Ersatzressourcen für reale Ressourcen**
  - Gleiche Funktionen und externe Interfaces wie reales Gegenstück
  - Verschiedene Größe, Performance, Kosten
  - Werden als virtuelle Ressourcen bezeichnet
  - Transparenz für den Benutzer
- **Üblicherweise auf physikalische Hardware Ressourcen angewendet**
  - Mehrere physikalische Ressourcen werden zu einem shared pool zusammengefasst
  - Benutzer beziehen virtuelle Ressourcen aus shared pool



- **Microsoft**

- Virtual PC
- Virtual Server

- **VMware**

- Workstation
- Server
- Fusion
- Player
- ESX Server

- **Sun**

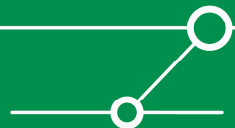
- xVM

- **InnoTek**

- VirtualBox

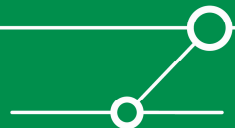
- **Open Source:**

- Xen
- KVM
- VirtualBox



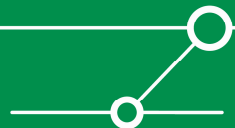
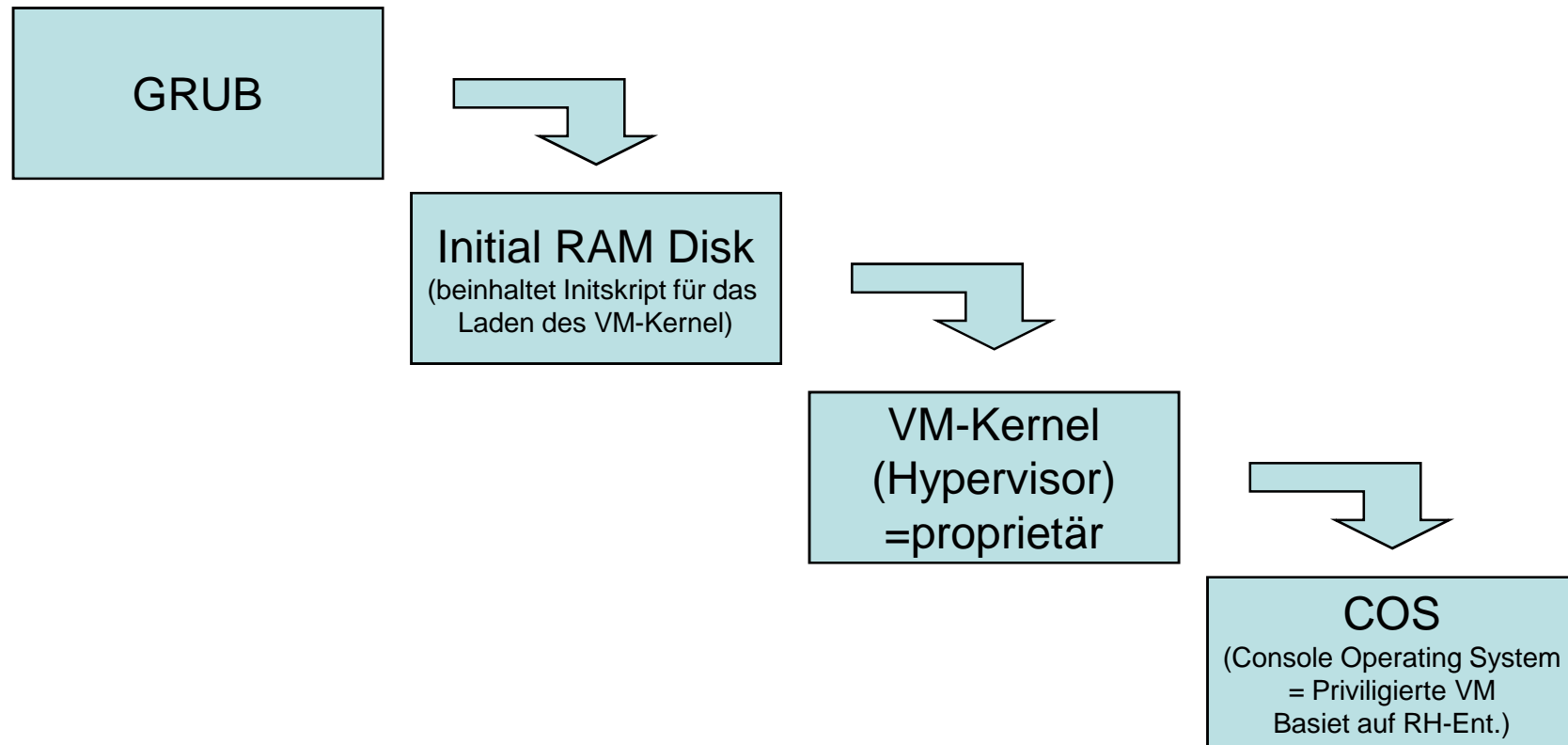
# Hypervisor

- **Zentrale Instanz bei Virtualisierungs-Plattformen**
- **Auch Virtual Machine Monitor (VMM) genannt**
- **Liegt als dünne Schicht zwischen physikalischer Hardware und den VMs**
- **Schlanker Code**
- **Stellt den VMs virtuelle Ressourcen bereit**
- **Dynamische Ressourcen Verteilung über “Shared Pool“**

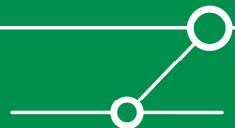
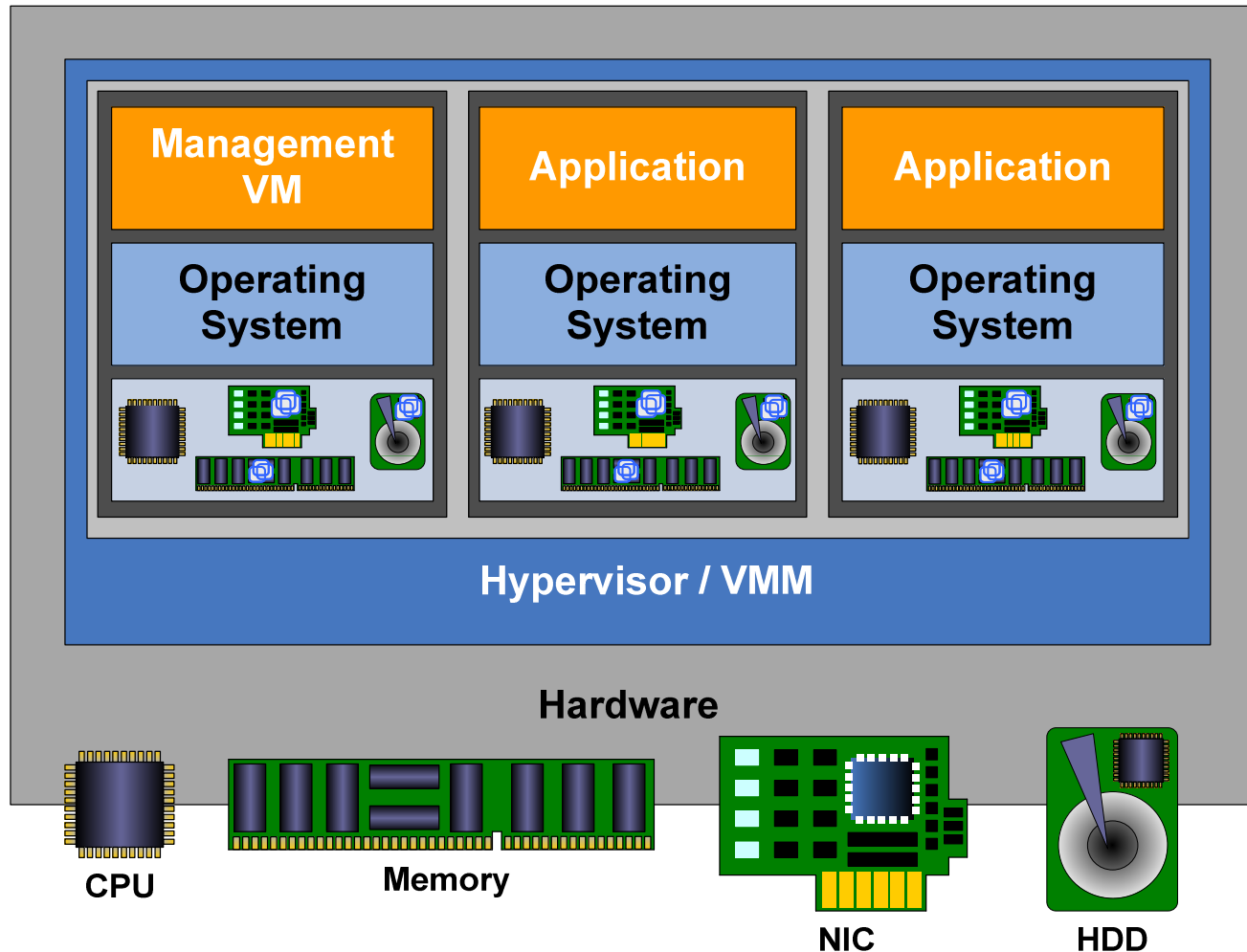




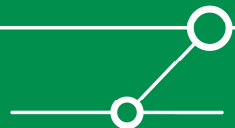
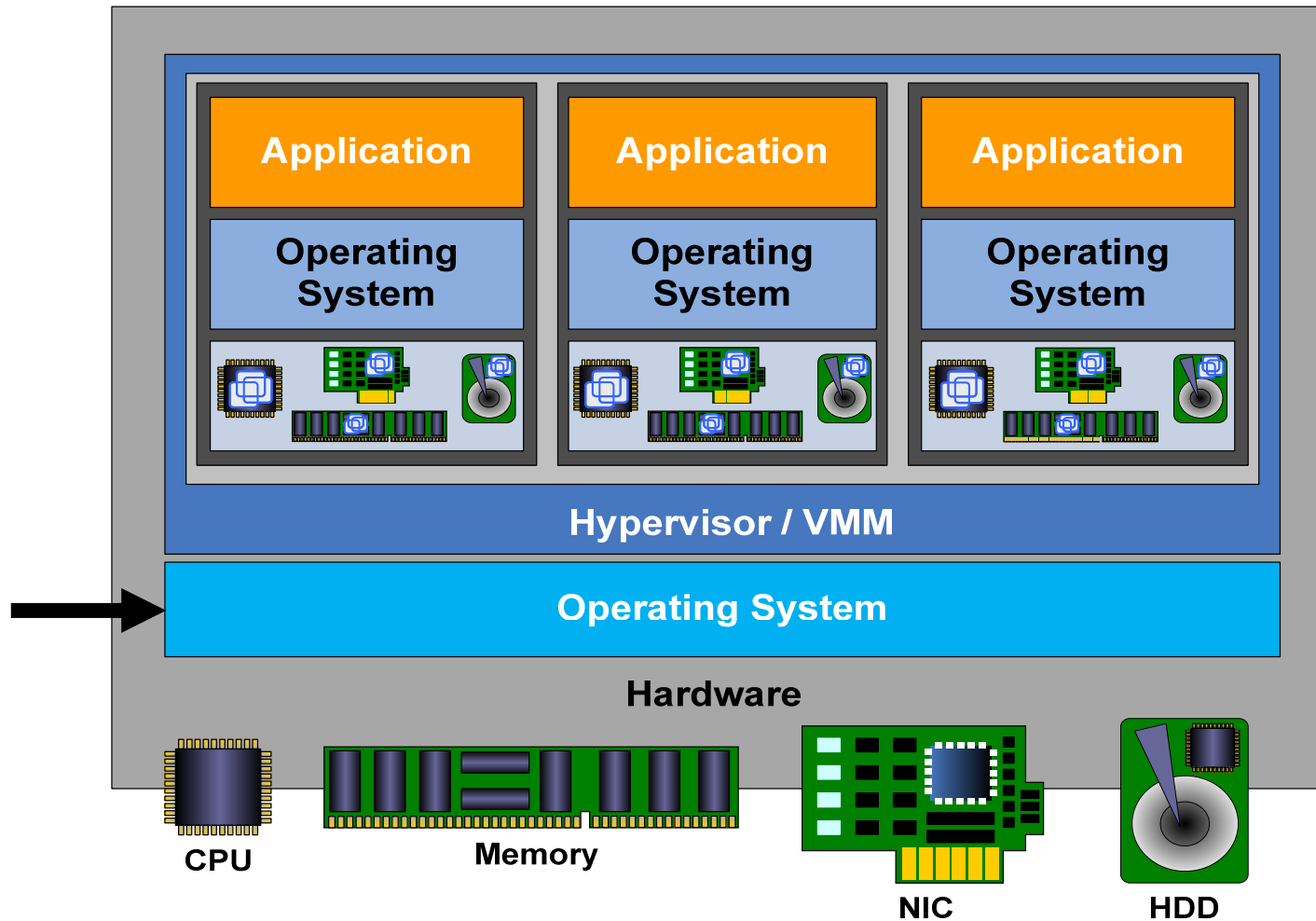
# Boot-Prozedur (anhand ESX)



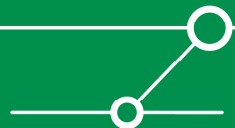
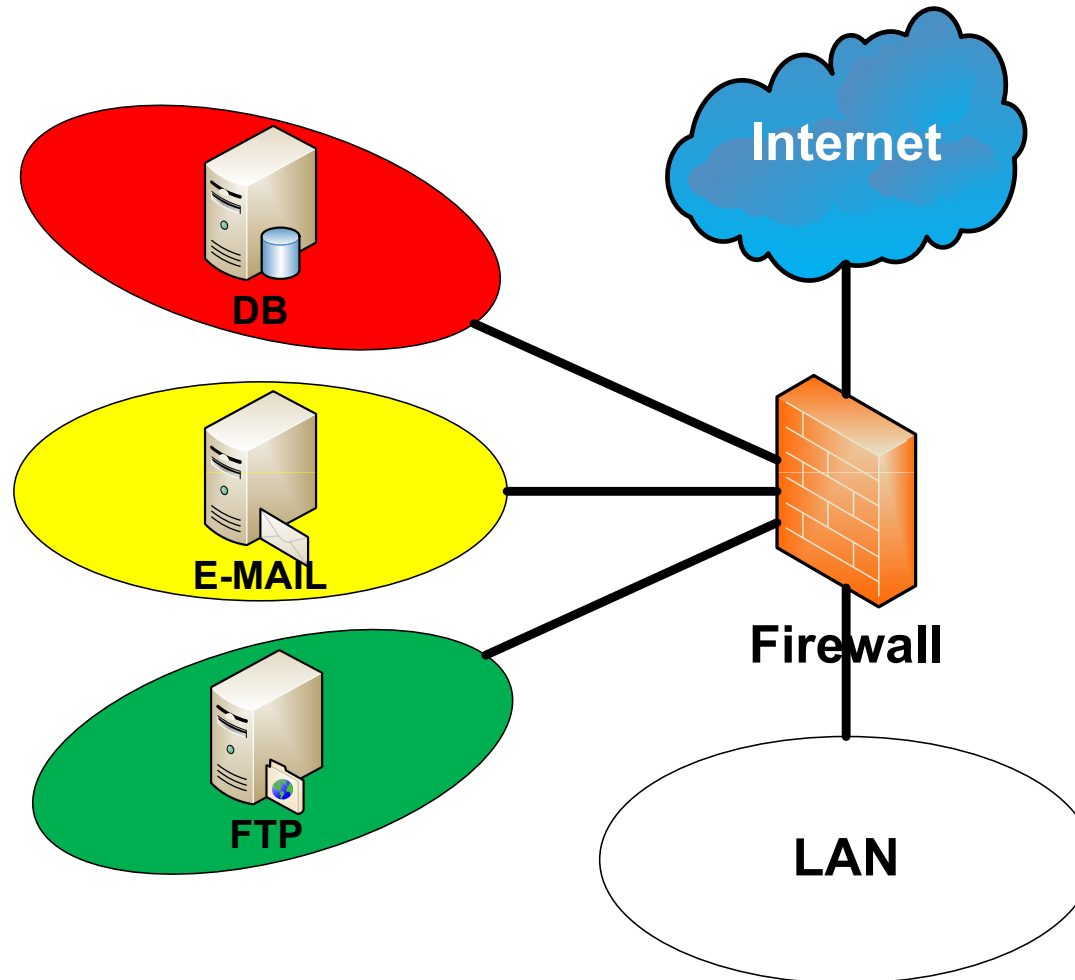
# Type 1 Hypervisor



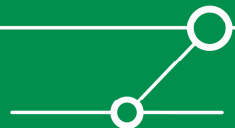
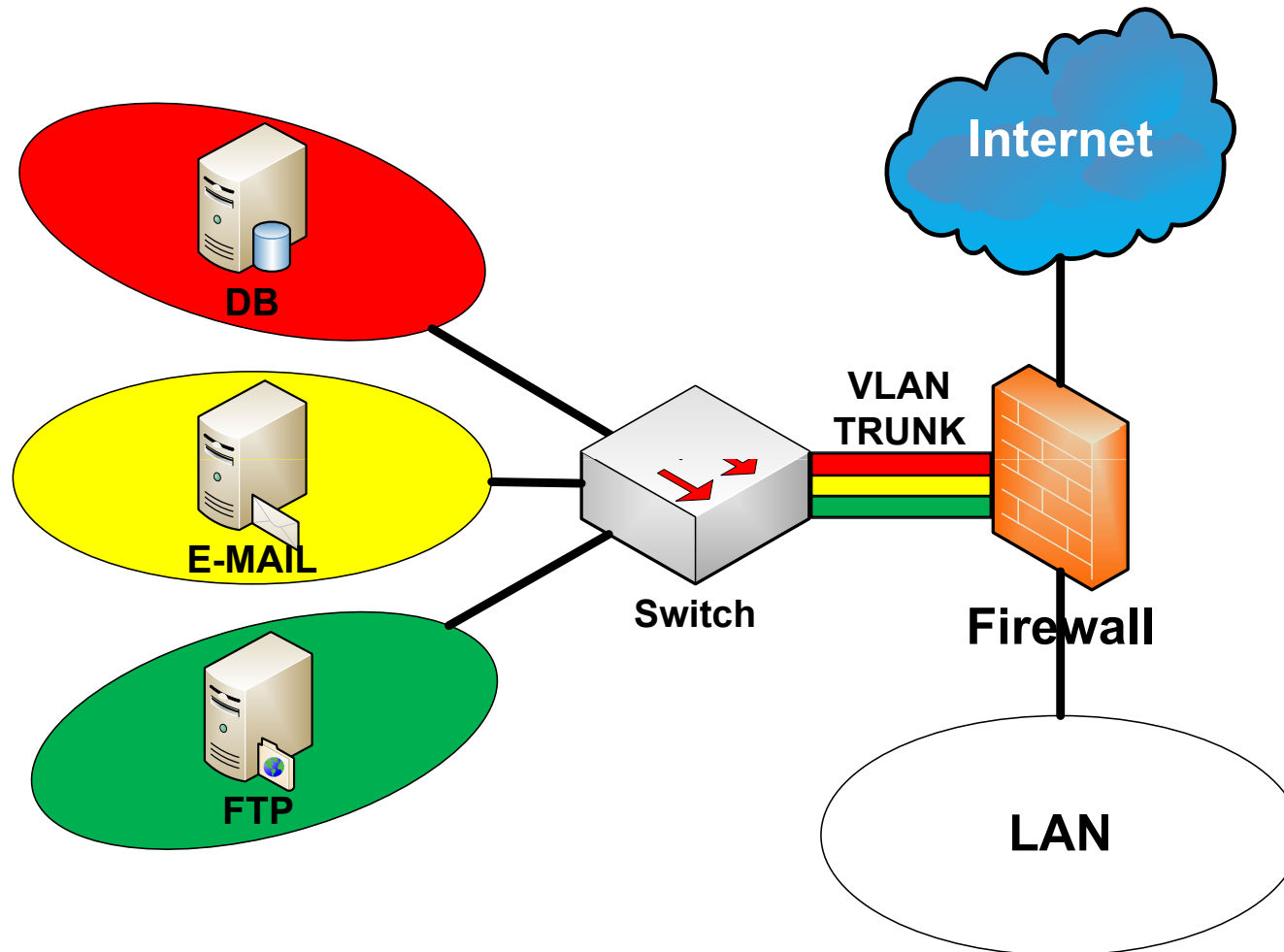
# Type 2 Hypervisor



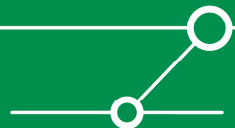
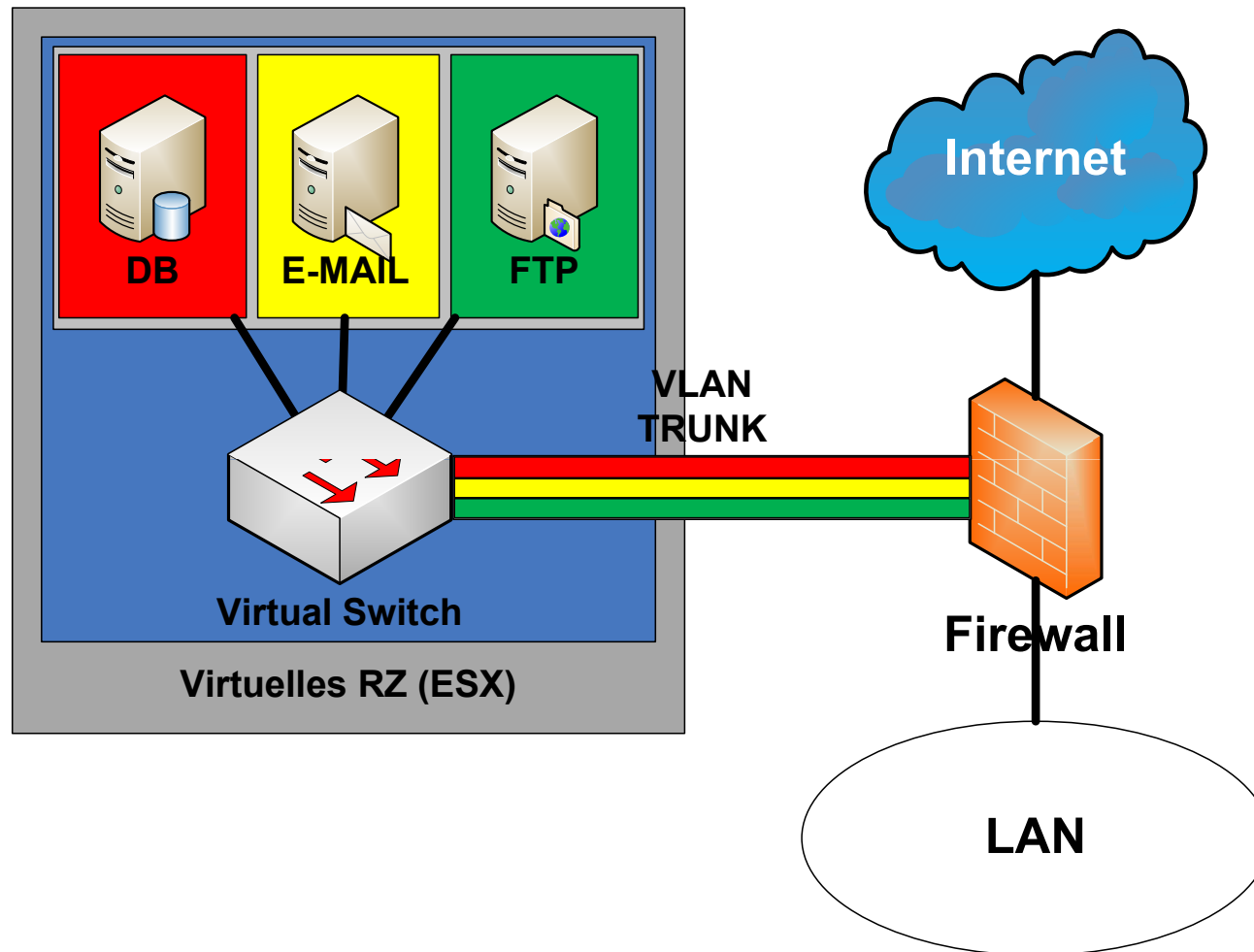
# Klassischer Ansatz



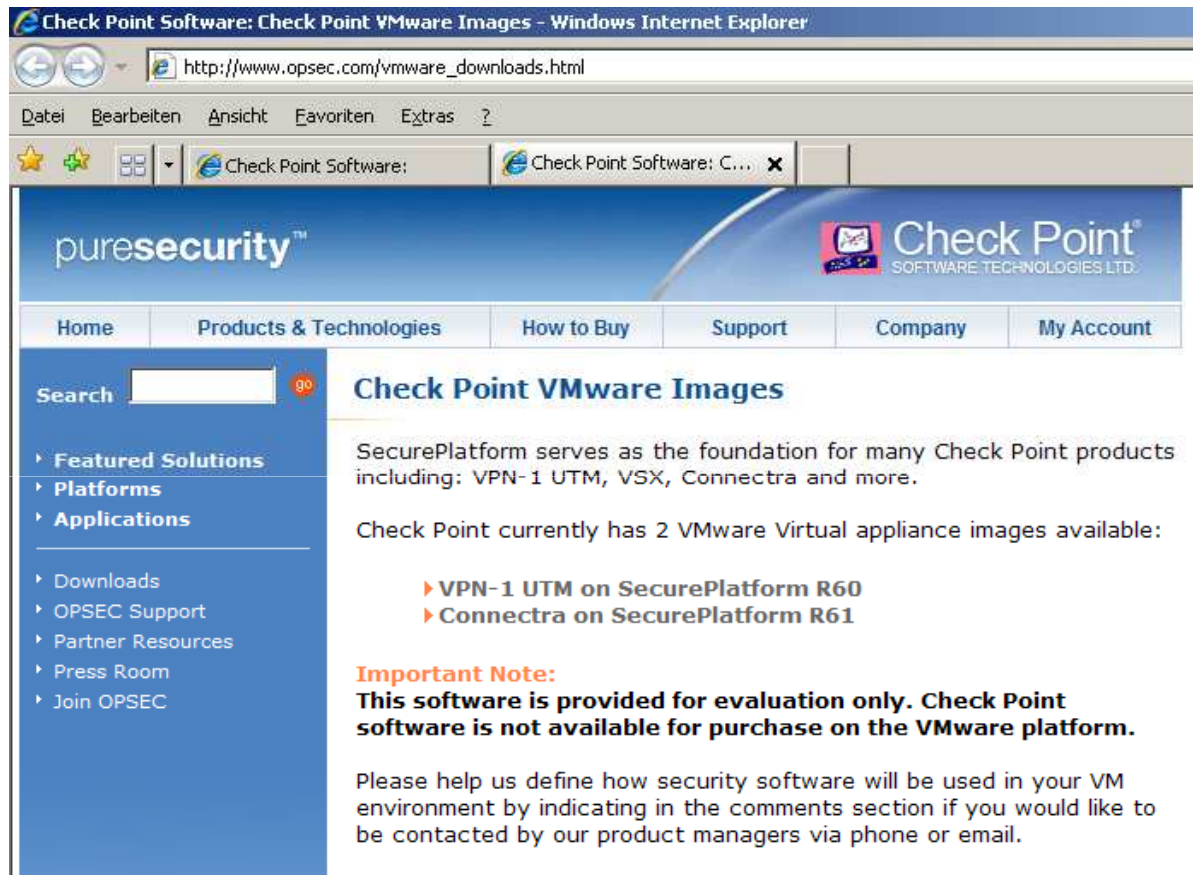
# Erste Virtualisierung (VLANs)



# Virtuelles RZ



# Virtual Appliances



Check Point Software: Check Point VMware Images - Windows Internet Explorer

http://www.opsec.com/vmware\_downloads.html

puresecurity™

Check Point®  
SOFTWARE TECHNOLOGIES LTD.

Home Products & Technologies How to Buy Support Company My Account

Search  go

▸ Featured Solutions  
▸ Platforms  
▸ Applications

▸ Downloads  
▸ OPSEC Support  
▸ Partner Resources  
▸ Press Room  
▸ Join OPSEC

## Check Point VMware Images

SecurePlatform serves as the foundation for many Check Point products including: VPN-1 UTM, VSX, Connectra and more.

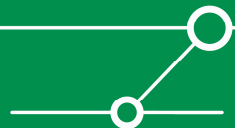
Check Point currently has 2 VMware Virtual appliance images available:

- VPN-1 UTM on SecurePlatform R60
- Connectra on SecurePlatform R61

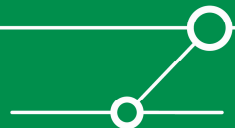
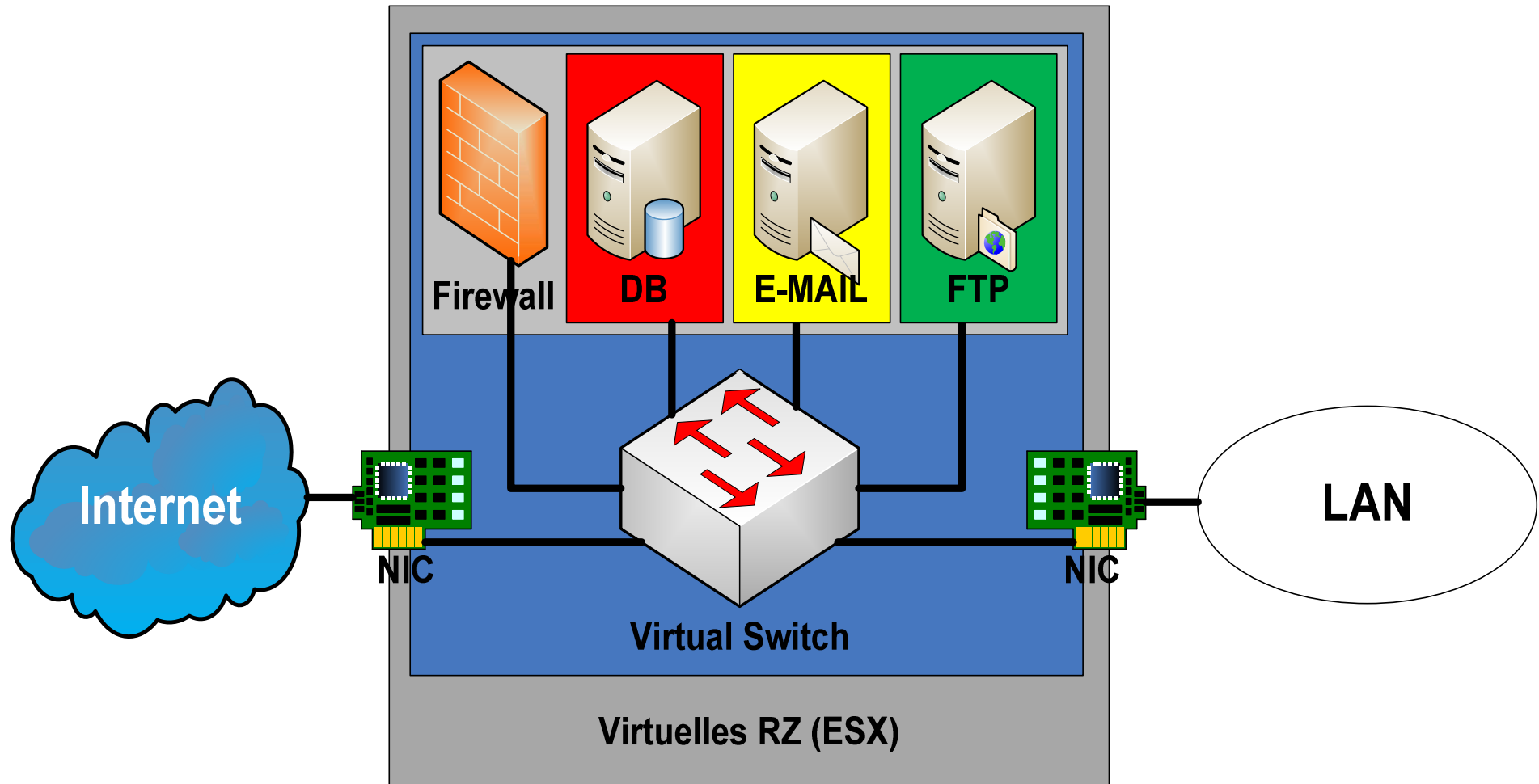
**Important Note:**  
**This software is provided for evaluation only. Check Point software is not available for purchase on the VMware platform.**

Please help us define how security software will be used in your VM environment by indicating in the comments section if you would like to be contacted by our product managers via phone or email.

Momentan nicht mehr erhältlich

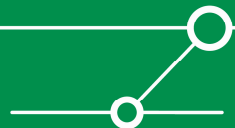


# RZ der Zukunft ?/!

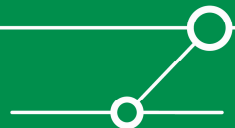
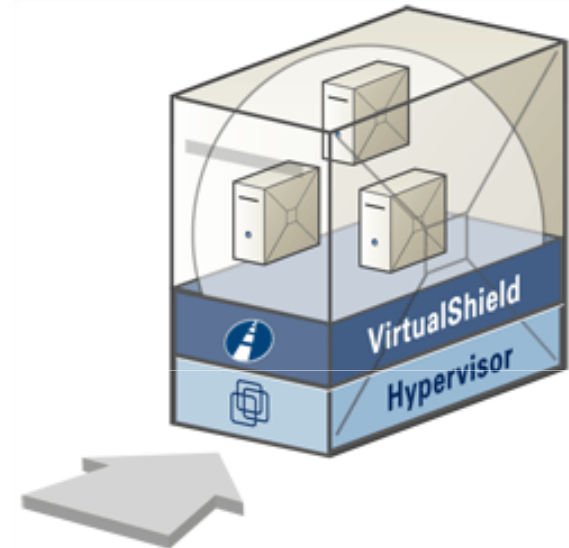




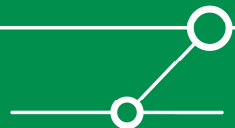
- **Der Hypervisor sollte in der Firmware speicherbar sein**
- **Einbindung eines TPM (Trusted Platform Module)**
- **Manipulationssicherer Hypervisor**
- **Hypervisor muss sämtliche Funktionalitäten der CPU/der Prozessoren unterstützen**
  
- **Feste Zuweisung von HW-Ressourcen (CPU/RAM/NW)**
- **Keine dynamische Teilung von Systemressourcen zwischen den Virtuellen Systemen**
- **Unveränderbarkeit dieser Ressourcen**
- **Aufsplittung von I/O-Geräten**



- **Zusätzliche Schicht die sich zwischen dem Gast-OS und dem Hypervisor befindet**
- **Bietet Sicherheitsfunktionalitäten wie**
  - Paketfilterung
  - Überwachung von offenen Ports
  - Rudimentäre IDS/IPS
- **vSafe-Initiative von VMware greift diese Funktionalität auf**
- **Blue Lane “Virtual Shield” []wird gerade von uns im Labor evaluiert 😊**

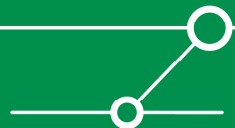


- ***secure Hypervisor***
- **Forschungsprojekt von *IBM Research***
- **2600 Zeilen Code**
- **Fügt *Mandatory Access Control (MAC)* Funktionalitäten (bei XEN) hinzu**
- **Entwickelt um mittlere Sicherheit zu erreichen (CC EAL4)**
- **Mehr Info unter [Sailer2005] oder [1]**

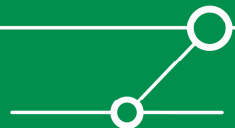
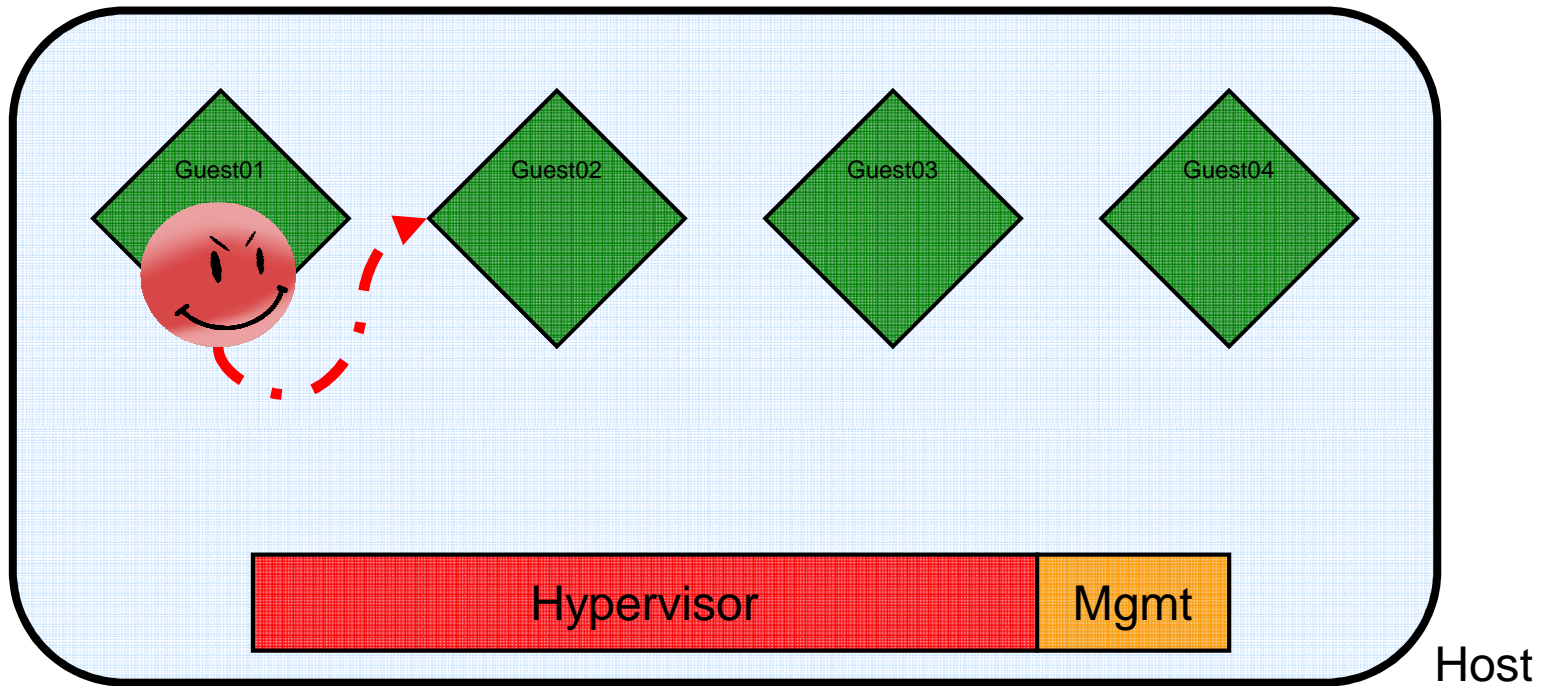


# Bedrohungen ....

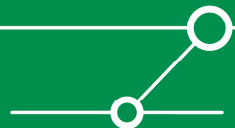
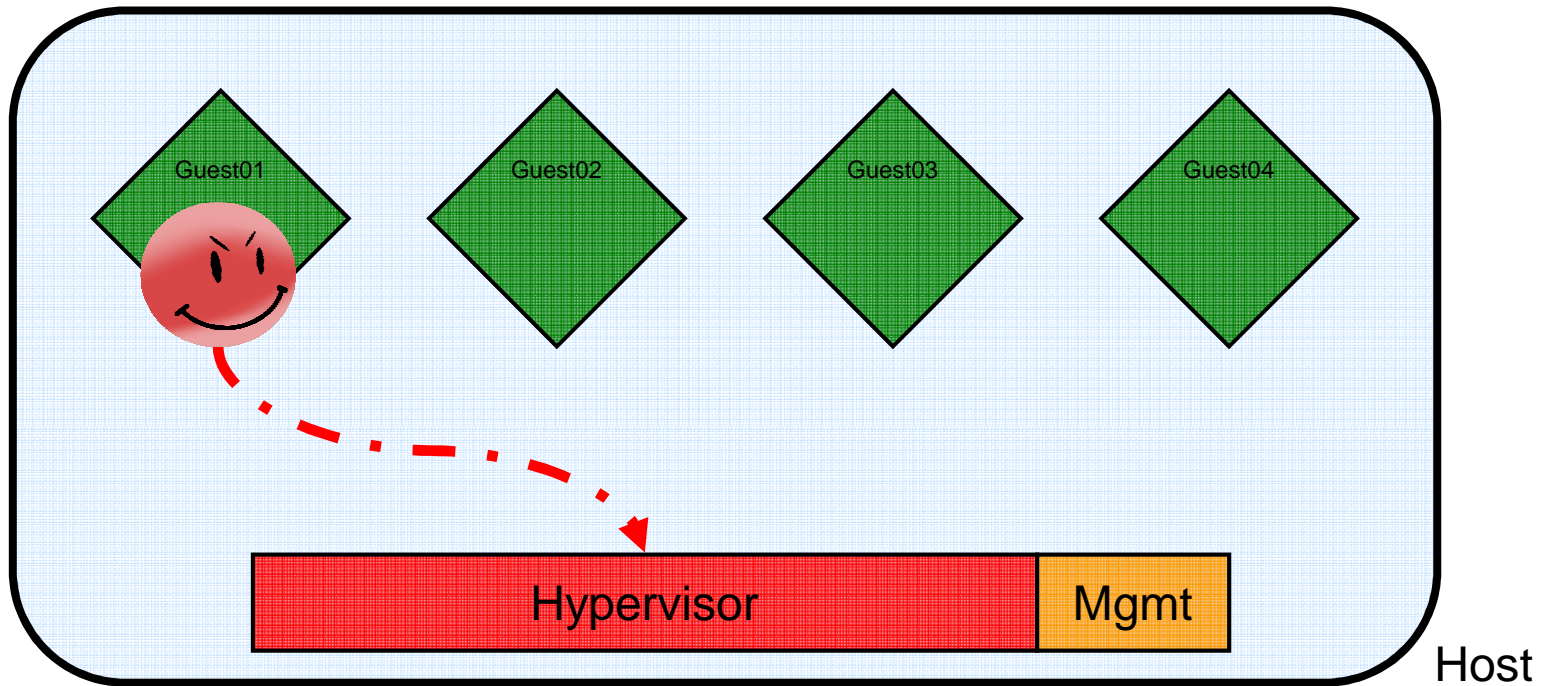
- **Angriffe gegen die Mgmt.-Infrastruktur**
- **Angriffe gegen das Host-OS**
- **Angriffe gegen das Gast-OS**
- **Konfigurations-Fehler (neu und unbekannt)**
- **Verstoß gegen rechtliche Vorgaben oder interne Richtlinien [Compliance ;-)]**



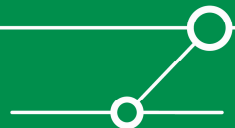
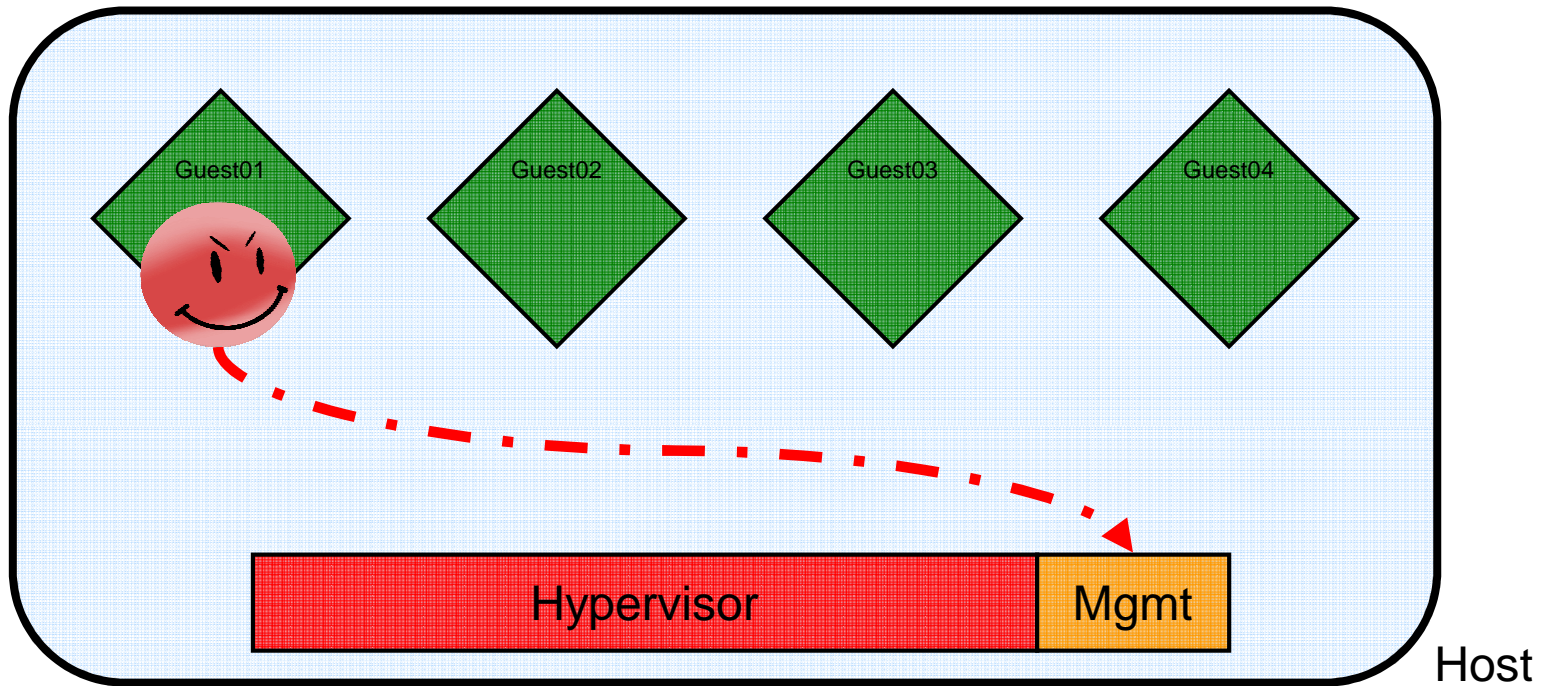
# Gast vs. Gast



# Gast vs. Host/Hypervisor

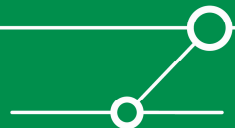


# Gast vs. Mgmt.



# Historische Vorfälle

- **VMware ESX Server**
  - 73 Schwachstellen seit 01.12.2003 [2]
  
- **VMware Workstation**
  - 38 Schwachstellen seit 26.06.2003 [2]
  
- **VMware Player**
  - 17 Schwachstellen seit 10.01.2006 [2]
  
- **Xen**
  - 6 Schwachstellen seit 02.11.2007 [2]
  
- **Virtual PC**
  - 2 Schwachstellen seit 06.09.2007 [2]





# Nutzung von Open Source...

Vulnerabilities (Page 1 of 3) 1 2 3 Next >

**Vendor:** VMWare  
**Title:** ESX Server  
**Version:** Select Version

---

**Search by CVE**

**CVE:**

---

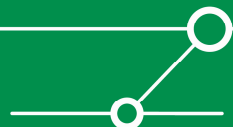
**Apache HTTP Server Arbitrary HTTP Request Headers Security Weakness**  
2008-04-07  
<http://www.securityfocus.com/bid/19661>

**libxml2 'xmlCurrentChar()' UTF-8 Parsing Remote Denial of Service Vulnerability**  
2008-03-31  
<http://www.securityfocus.com/bid/27248>

**Linux Kernel AACRAID Driver Local Security Bypass Vulnerability**  
2008-03-28  
<http://www.securityfocus.com/bid/25216>

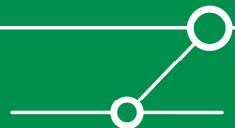
**OpenSSL Public Key Processing Denial of Service Vulnerability**  
2008-03-18  
<http://www.securityfocus.com/bid/20247>

[2]



# VMware Security im Jahr 2007

- April: Presentation “An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments“ von Tavis Ormandy - CanSecWest 2007
- July: Demonstration einiger „Tools“ auf der SANSFIRE 2007
- August: VMware übernimmt den HIPS Hersteller *Determina* [8]
- September: (Jede Menge :- ) VMware Security Advisory VMSA-2007-0006
- September: VMware kündigt das API Sharing Programm *Vsafe* an



# Übernahme des Hostsystems

VMware vulnerability in NAT networking Dec 21 2005 07:47AM  
vmware-security-alert vmware.com

-----BEGIN PGP SIGNED MESSAGE-----  
Hash: SHA1

## VULNERABILITY SUMMARY

A vulnerability has been discovered in `vmnat.exe` on Windows hosts and `vmnet-natd` on Linux systems.

The vulnerability makes it possible for a malicious guest using a NAT networking configuration to execute unwanted code on the host machine.

## AFFECTED SYSTEMS:

VMware Workstation, VMware GSX Server, VMware ACE, and VMware Player.

## RESOLUTION:

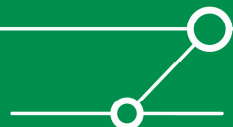
VMware believes that the vulnerability is very serious, and recommends that affected users update their products to the new releases or change the configuration of the virtual machine so it does not use NAT networking.

The new releases are now available for download at [www.vmware.com/download](http://www.vmware.com/download)

If you choose not to update your product but want to ensure that the NAT service is not available, you can disable it completely on VMware Workstation or VMware GSX Server by following the instructions in the Knowledge Base article (Answer ID 2002) at <http://www.vmware.com/support/kb>.

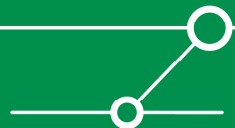
VMware thanks Tim Shelton of ACS Security Assessment Engineering, Affiliated Computer Services, Inc., for reporting this vulnerability.

Warum sollte dies nicht auch zukünftig in ESX möglich sein?!....

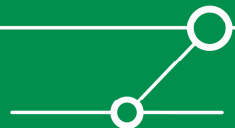


# Und da ist er ...

- **Aus dem Advisory [6]:**
  - `"This release fixes a security vulnerability that could allow a guest operating system user with administrative privileges to cause memory corruption in a host process, and thus potentially execute arbitrary code on the host. (CVE-2007-4496)"`
- Hmm... Denken Sie nicht auch, dass dies eine "ernsthafte Schwachstelle" ist?**



- **Ed Skoudis:**
- `"The tools we presented have names based on their functionality: VMchat, VMcat, VM Drag-N-Hack (which undermines drag-and-drop, altering a file going from guest to host), VM Drag-N-Sploit (which alters a dragged file into something that shovels a shell into the guest), and, finally VMftp. That last one (VMftp) exploited the directory traversal flaw to provide FTP-style file access to the host from the guest, representing a true escape. I do not think that VMftp is an overhyped name."` [4]
- **Die Presentation, weitere Informationen und Tools werden *nicht* zur Verfügung gestellt...**



English | [Japanese](#) Author: Ken Kato  
Mail: [chitchat@vdk.at](mailto:chitchat@vdk.at) [gmail.com](mailto:gmail.com)

**VM Back**  
Virtualization Tricks and Tools

---

## VM Back

---

VM Back

---

### What's New

Feb. 6, 2008

Updated [VMware Command Line Tools](#)

- [Patch and pre-built binaries for SCO OpenServer 5.0.x](#) by John Morris
- Added a comment about the Open Virtual Machine Tools

Updated [VMware Backdoor I/O Port](#)

- Added a comment about the Open Virtual Machine Tools

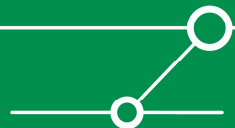
Updated [Virtual Floppy Drive](#)

- Version [2.1.2008.206](#) with the latest zlib library and a few minor UI changes

Updated [Links](#) Section:

- Added [Open Virtual Machine Tools](#) link.
- Added [Virtual Machine Disk Format](#) link.

[5]

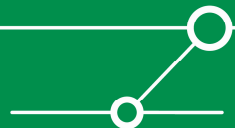


# Der kleine „ERNW“ Katechismus

- Keep it simple
- Patch-Level
- Minimal Machine
- Segregation of Duties
- Least Privilege
- Defense in Depth
- Starke Authentifizierung

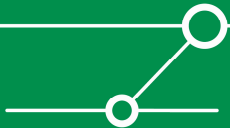


- **The Center for Internet Security**
  - VMware ESX Server 3.x Benchmark (70 Seiten)
  - Virtual Machine Security Guidelines (30 Seiten)
  
- **Defence Systems Information Agency**
  - VIRTUAL MACHINE (VM) Checklist (99 Seiten)
  
- **VMware**
  - Infrastructure 3 – Security Hardening (19 Seiten)



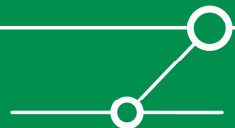


# Untersuchung des ESX

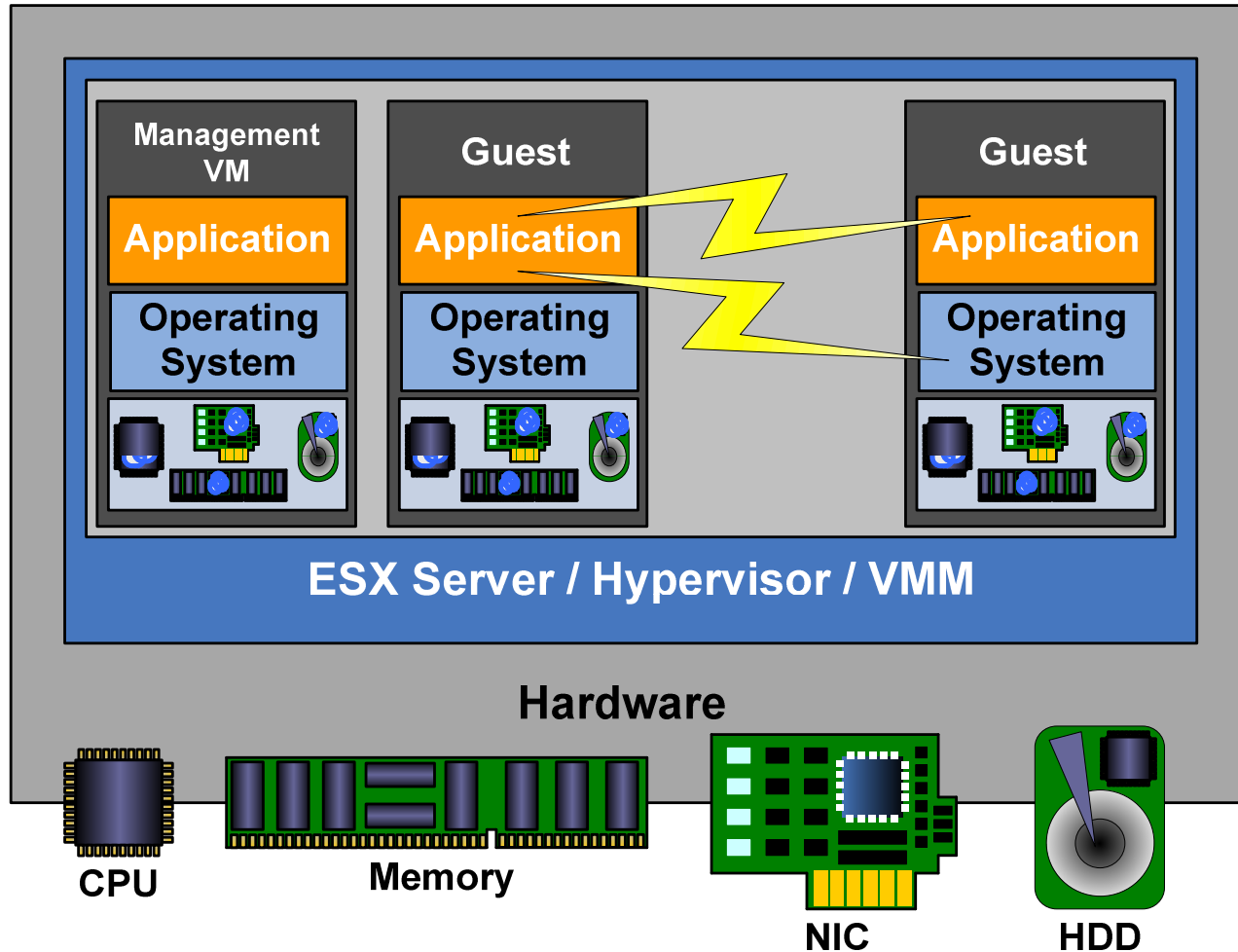


- **Bei der Untersuchung wurden folgende Szenarien geprüft**

- Gast vs. Gast
- Gast vs. Host
- Any vs. Management



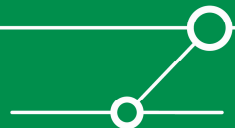
# Gast vs. Gast



konventionelle Angriffe

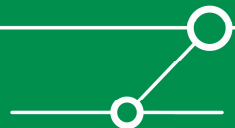
z.B. Exploits

DOS Angriffe



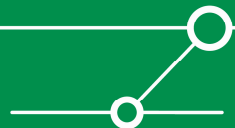
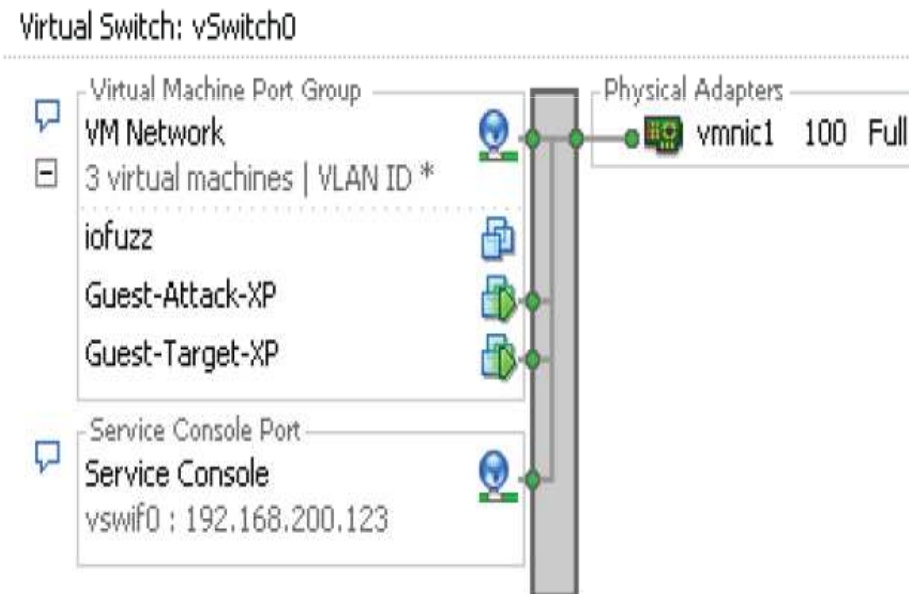
## ■ Promiscuous Mode

- Disabled per default
- Bei Konfigurationsfehler Sicherheitsrisiko
- Wenn enabled → mitlesen sämtlichen Netzwerkverkehrs auf dem vSwitch möglich
- (De-)aktivierung nicht pro VM möglich

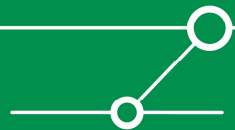
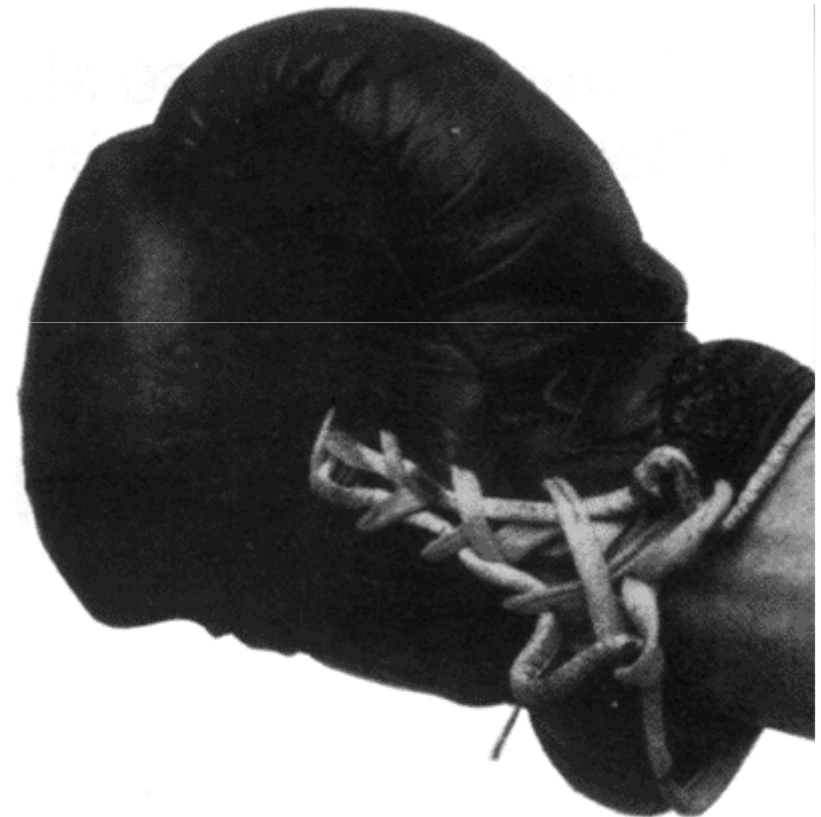


## ■ Virtual Switch

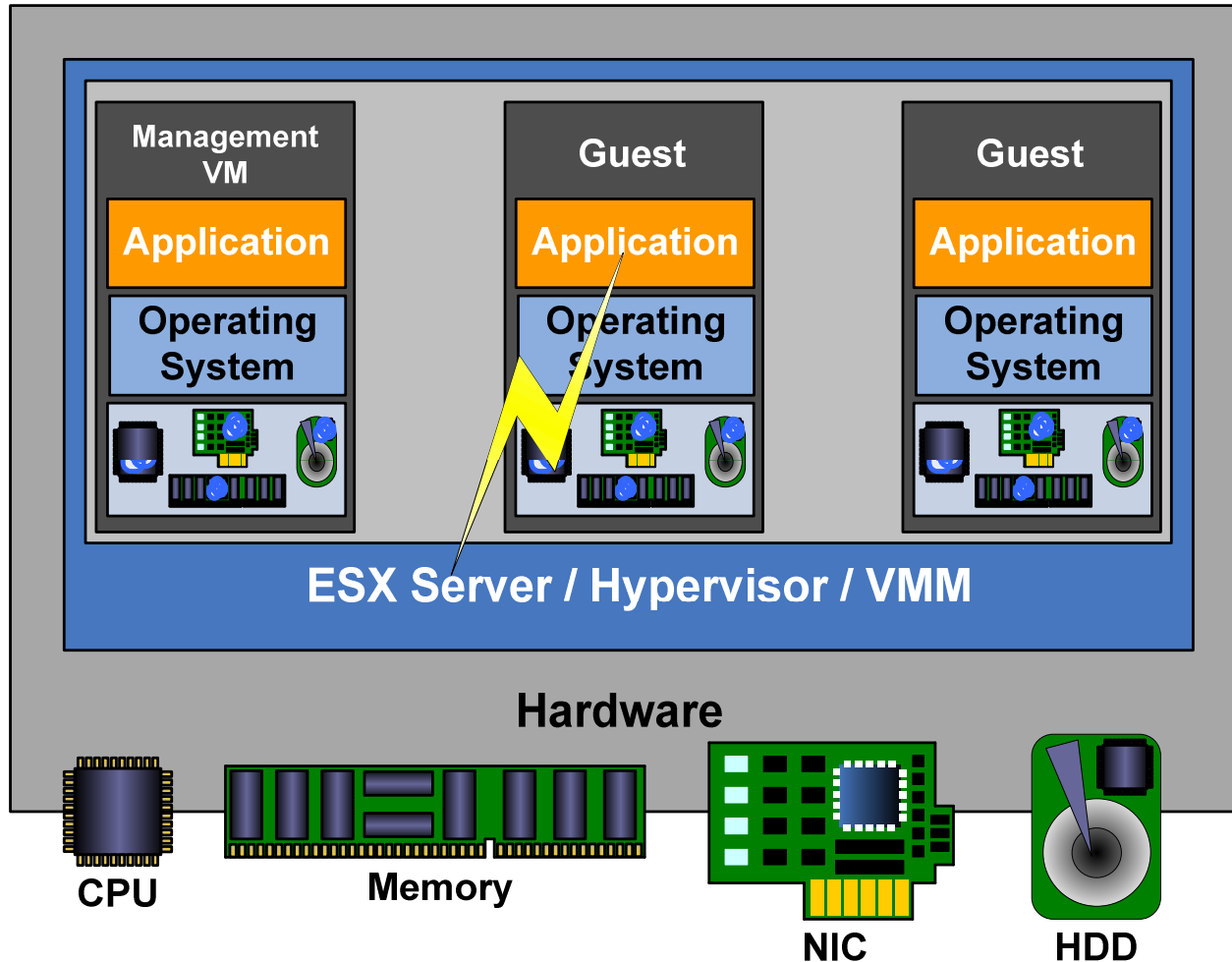
- Funktionsweise gleicht einem Hub
- Keine Mechanismen gegen ARP-, MAC-Spoofing oder MITM
- Erwartungsgemäß auch keine Mechanismen gegen Exploiting



# Demo



# Gast vs. Host



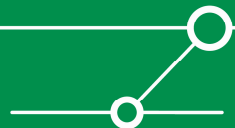
Fehlerhaft  
implementierte  
virtuelle  
Ressourcen,

z.B. Buffer Overflow

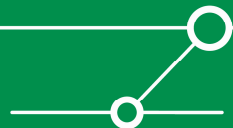
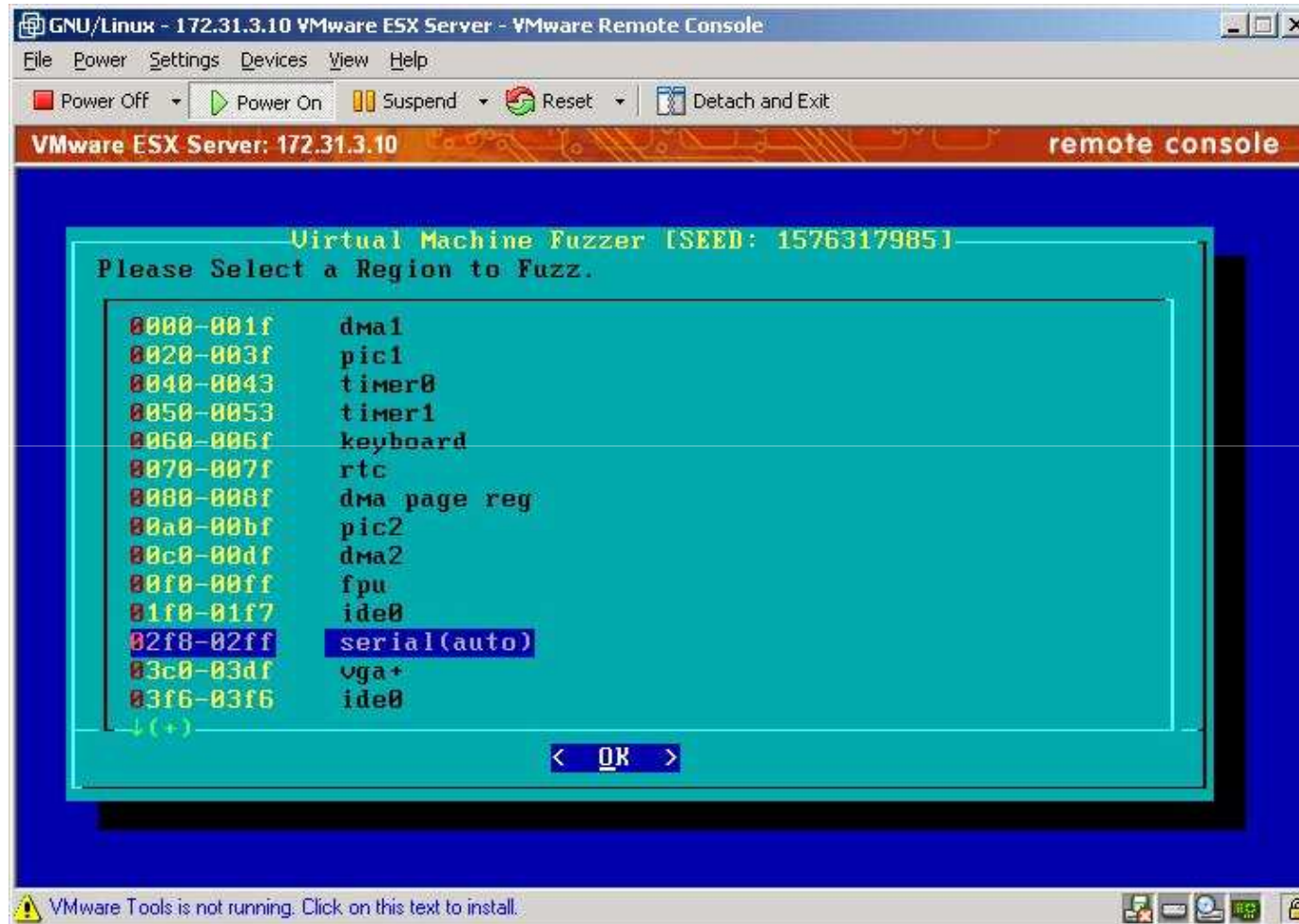
Tools:

Crashme

lofuzz

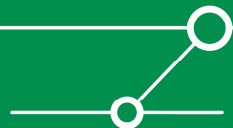
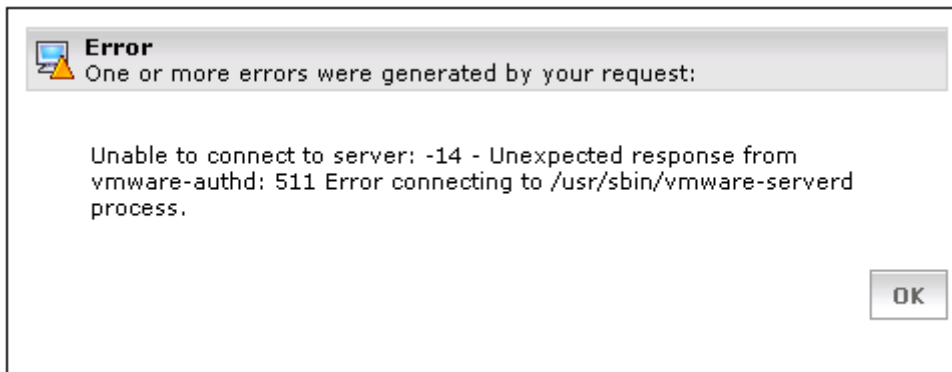


# lofuzz...



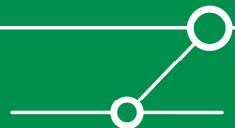


# ... Auswirkung

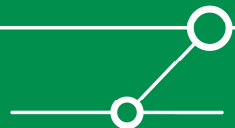


# Das sieht nicht gut aus ;-))

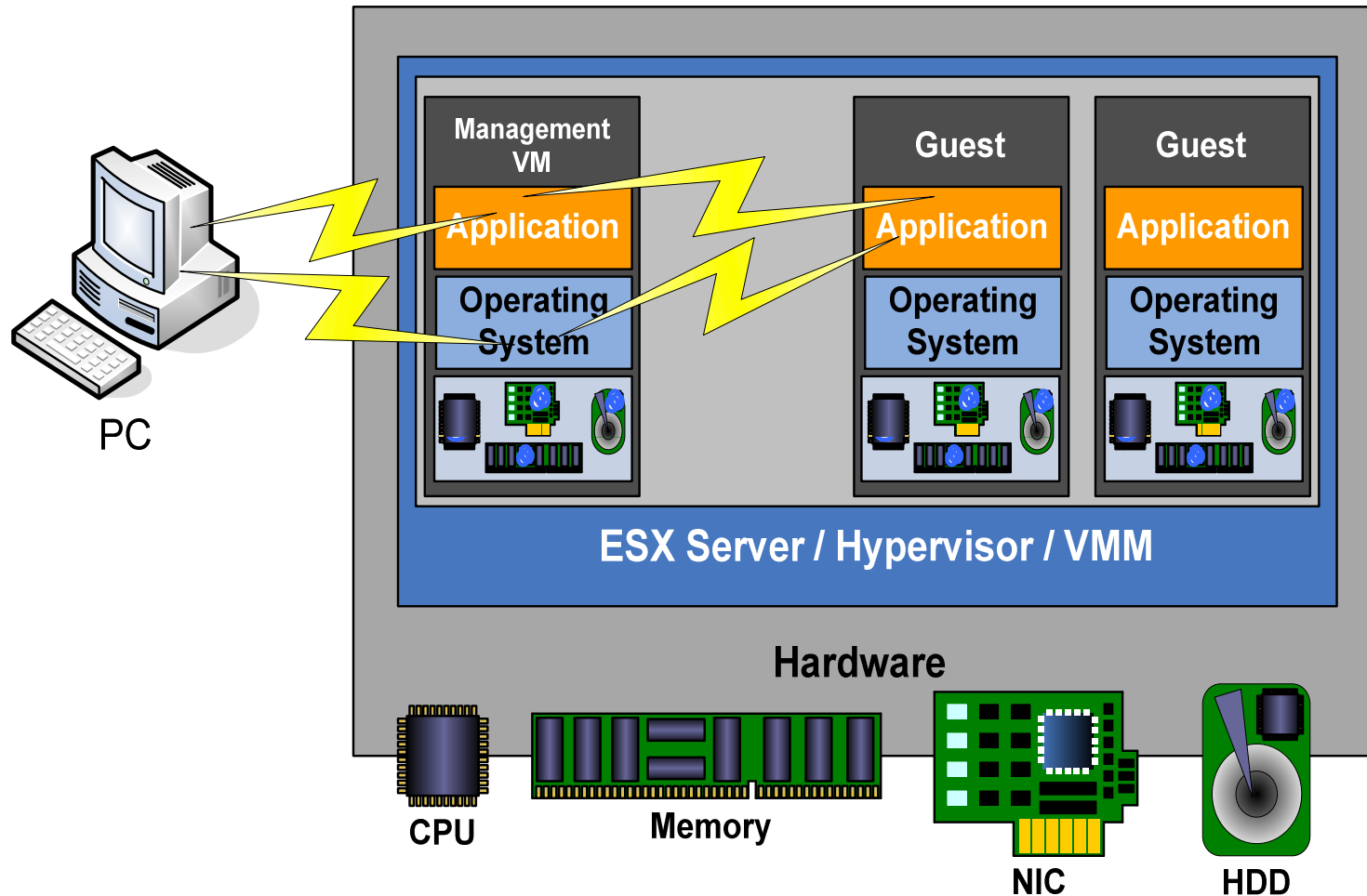
```
Jun 29 11:05:15: vcpu-0 | Backtrace[6] 0xbf7ffa94 eip 0x8084e7a
Jun 29 11:05:15: vcpu-0 | Backtrace[7] 0xbf7ffab4 eip 0x807e848
Jun 29 11:05:15: vcpu-0 | Backtrace[8] 0xbf7ffb24 eip 0x80e3d08
Jun 29 11:05:15: vcpu-0 | Backtrace[9] 0xbf7ffbf4 eip 0x40047fb7
Jun 29 11:05:15: vcpu-0 | Backtrace[10] 00000000 eip 0x4015acba
Jun 29 11:05:15: vcpu-0 | Msg_Post: error
Jun 29 11:05:15: vcpu-0 | [msg.log.vmxpanic] VMware ESX server unrecoverable
error: (vcpu-0)
Jun 29 11:05:15: vcpu-0 | BUG F(553):566 bugNr=431
Jun 29 11:05:15: vcpu-0 | Please request support and include the contents of
the
log file: "/root/Vmware/fuzz/Vmware.log". We will respond on the basis of
your support entitlement.
Jun 29 11:05:15: vcpu-0 | -----
Jun 29 11:05:26: vcpu-0 | VTHREAD thread 4 start exiting
Jun 29 11:05:26: vcpu-0 | VTHREAD counting thread 0
Jun 29 11:05:26: vcpu-0 | VTHREAD counting thread 1
Jun 29 11:05:26: vcpu-0 | VTHREAD thread 4 exiting, 2 left
Jun 29 11:05:26: vmx | VTHREAD watched thread 4 "vcpu-0" died
Jun 29 11:05:26: vmx | VTHREAD thread 0 start exiting
```



- **Fuzzing der virtuellen Hardware provoziert Absturz der VM**
  
- **Abstürze u.a durch:**
  - \*\*\* VMware ESX Server internal monitor error \*\*\*
  - VMware ESX Server unrecoverable error
  - Asserts
    - hauptsächlich benutzt zu debugging Zwecken
    - sollten im Ausgelieferten Produkt entfernt werden, falls sie nicht implementiert sind um das Programm vor “schlimmerem“ zu bewahren
  
- **Hinweis auf unsaubere Implementierung sowie mögliche Buffer Overflows**



# Angriffe gegen Management



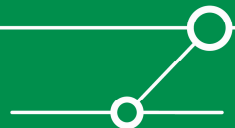
Tools:

Nessus

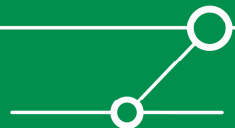
Appscan

Exploits

DOS

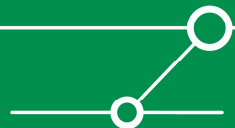


- **MITM gegen Web MUI möglich**
  - Setzt User-Interaktion voraus
- **Virtual Switch**
  - Keine Mechanismen gegen ARP-, MAC-Spoofing oder MITM
  - Erwartungsgemäß auch keine Mechanismen gegen Exploiting
- **Relevante Ports lassen sich blockieren → erschwerte Managebarkeit**
  - Secure by Design oder DOS?

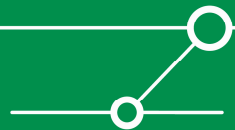


## ■ SSH Bruteforcing

```
Hydra v5.4 (c) 2006 by van Hauser / THC - use allowed only for legal purposes.  
Hydra (http://www.thc.org) starting at 2008-04-08 12:11:03  
[DATA] 16 tasks, 1 servers, 1754 login tries (l:1/p:1754), ~109 tries per task  
[DATA] attacking service ssh2 on port 22  
[STATUS] 208.52 tries/min, 212 tries in 00:01h, 1542 todo in 00:08h  
[STATUS] 248.62 tries/min, 750 tries in 00:03h, 1004 todo in 00:05h  
[STATUS] 228.37 tries/min, 1610 tries in 00:07h, 144 todo in 00:01h  
[STATUS] attack finished for 192.168.83.10 (waiting for childs to finish)  
[22][ssh2] host: 192.168.83.10  login: admin  password: letmein  
Hydra (http://www.thc.org) finished at 2008-04-08 12:18:35
```

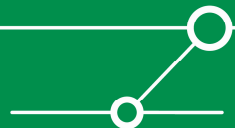


# Demo



# Lessons Learned (1)

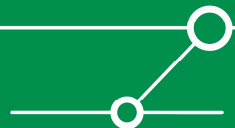
- **Sicherheit spielt bei der Entwicklung meist eine untergeordnete Rolle**
- **Keine Ansätze gegen alte Probleme wie ARP-Spoofing und MITM**
- **Gefahr durch Konfigurationsfehler**
- **Gefahr durch Implementierungsfehler durchaus akut**



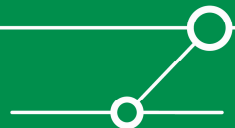
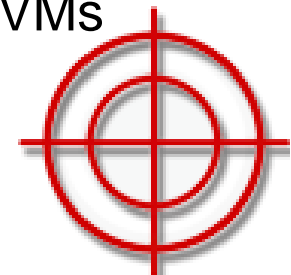


# Lessons Learned (2)

- **Argus Pitbull**
- **Security BCP sollten immer mit einbezogen werden**
- **Einbindung von Virtualisierung in Unternehmens Policy**
- **Hardening Guides beachten [3]**

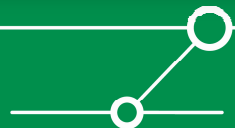


- **Trend sollte in Richtung Standardisierung von Virtualisierungs-Plattformen und Protokollen gehen**
- **Schwenk von Einzel-Maschinen-Virtualisierung in Richtung der Service-Orientierten-Virtualisierung**
- **Embedded Virtualisierungs-Plattformen wie VMware ESX Server 3i**
- **Zugriff von Außen auf virtuelle Hardware durch APIs**
  1. Entwicklung von Sicherheitssoftware die diese APIs nutzt
  2. Mögliche neue Kategorie von Angriffsszenarien gegen die VMs

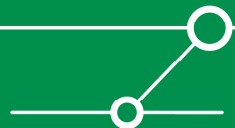


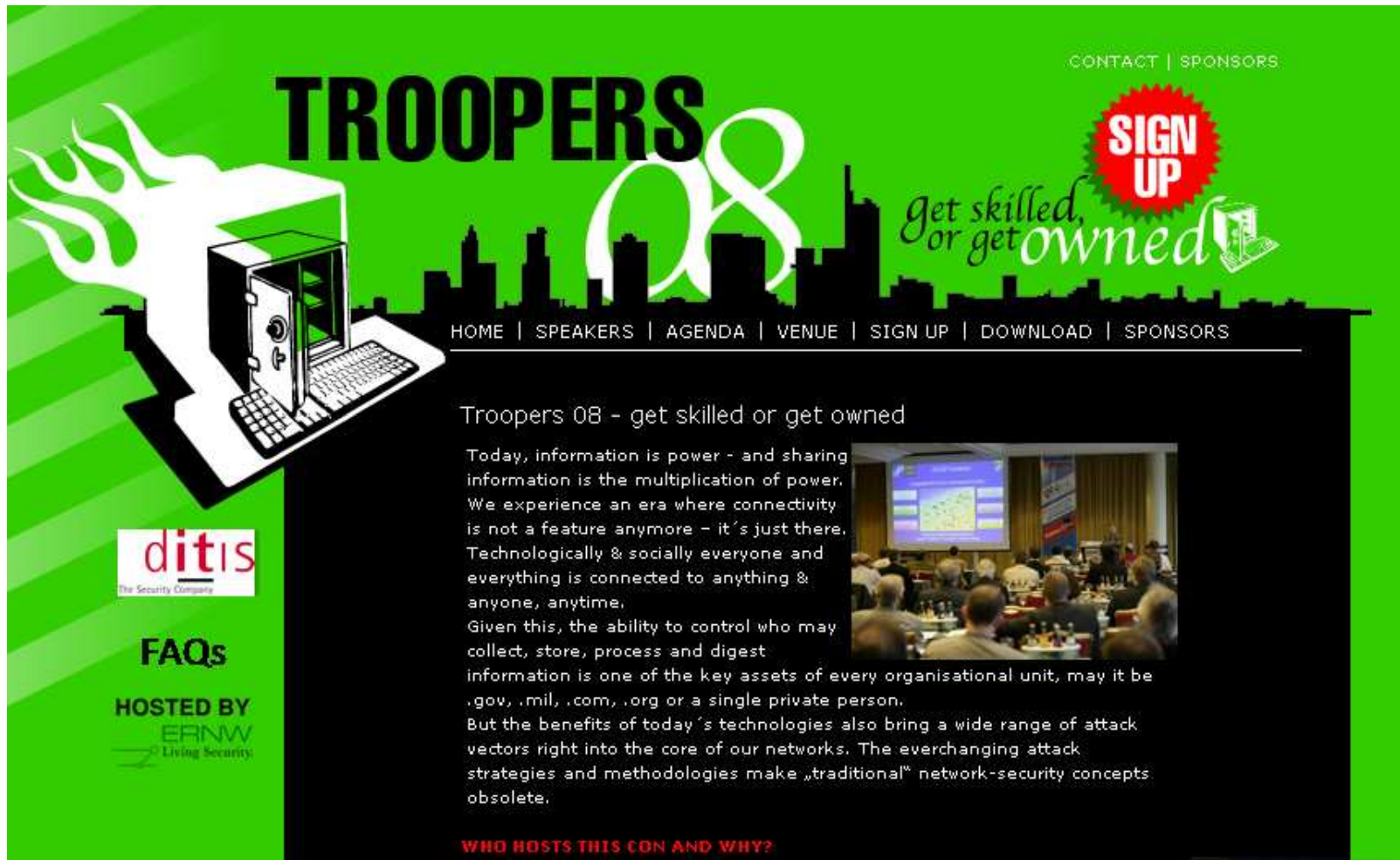


# Fragen? Und Antworten...



rklose@ernw.de  
gniehues@ernw.de





The banner features a green background with a white silhouette of a city skyline. On the left, a computer monitor displays a white flame-like graphic. The word "TROOPERS" is written in large, bold, black letters, with a large white "08" to its right. In the top right corner, there is a red starburst graphic with the text "SIGN UP" in white. Below it, the phrase "get skilled, or get owned" is written in a white, cursive font. A navigation menu is located in the top right, with links for "CONTACT | SPONSORS". A second navigation menu is positioned below the main text, with links for "HOME | SPEAKERS | AGENDA | VENUE | SIGN UP | DOWNLOAD | SPONSORS". The central text reads "Troopers 08 - get skilled or get owned". To the right of this text is a photograph of a conference room with people seated at tables, facing a presentation screen. Below the main text, there is a section titled "WHO HOSTS THIS CON AND WHY?". Logos for "ditis The Security Company" and "ERANW Living Security" are visible in the bottom left corner.

CONTACT | SPONSORS

# TROOPERS 08

get skilled, or get owned

SIGN UP

HOME | SPEAKERS | AGENDA | VENUE | SIGN UP | DOWNLOAD | SPONSORS

## Troopers 08 - get skilled or get owned

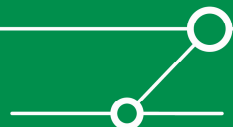
Today, information is power - and sharing information is the multiplication of power. We experience an era where connectivity is not a feature anymore - it's just there. Technologically & socially everyone and everything is connected to anything & anyone, anytime. Given this, the ability to control who may collect, store, process and digest information is one of the key assets of every organisational unit, may it be .gov, .mil, .com, .org or a single private person. But the benefits of today's technologies also bring a wide range of attack vectors right into the core of our networks. The everchanging attack strategies and methodologies make „traditional“ network-security concepts obsolete.

WHO HOSTS THIS CON AND WHY?

ditis  
The Security Company

FAQs

HOSTED BY  
ERANW  
Living Security



# Quellen

- [1] <http://publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/eicay/eicay.pdf>
  
- [2] <http://www.securityfocus.com>
  
- [3] [http://www.vmware.com/pdf/vi3\\_security\\_hardening\\_wp.pdf](http://www.vmware.com/pdf/vi3_security_hardening_wp.pdf)  
[http://cisecurity.org/tools2/vm/CIS\\_VMware\\_ESX\\_Server\\_Benchmark\\_v1.0.pdf](http://cisecurity.org/tools2/vm/CIS_VMware_ESX_Server_Benchmark_v1.0.pdf)  
[http://www.cisecurity.org/tools2/vm/CIS\\_VM\\_Benchmark\\_v1.0.pdf](http://www.cisecurity.org/tools2/vm/CIS_VM_Benchmark_v1.0.pdf)  
<http://iase.disa.mil/stigs/checklist/vmchk1st-v2r12-APR06.doc>
  
- [4] <http://www.cutawaysecurity.com/blog/archives/170>
- [5] <http://chitchat.at.infoseek.co.jp/vmware/index.html#top>
- [6] <http://lists.vmware.com/pipermail/security-announce/2007/000001.html>
- [7] <http://www.bluelane.com/products/virtualshield/>
- [8] [http://searchsecurity.techtarget.com/originalContent/0,289142,sid14\\_gci1268544,00.html](http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1268544,00.html)

[Sailer2005]: IBM Research Report [RC23511](#):

*R. Sailer, E. Valdez, T. Jaeger, R. Perez, L. van Doorn, J. L. Griffin, S. Berger: sHype: Secure Hypervisor Approach to Trusted Virtualized Systems.*

