



Sicherheit in virtualisierten Umgebungen

Enno Rey
erey@ernw.de



- **Heidelberg based security consulting and assessment company with currently 18 employees (as of Sep 2010).**

- Independent
- Deep technical knowledge
- Structured (assessment) approach
- Business reasonable recommendations
- We understand corporate



- **Blog: www.insinuator.net**
- **Conference: www.troopers.de**



- **Die wichtigsten Risiken in virtualisierten Umgebungen**
- **Veränderung vorhandener Sicherheitsarchitekturen**
- **Maßnahmen**



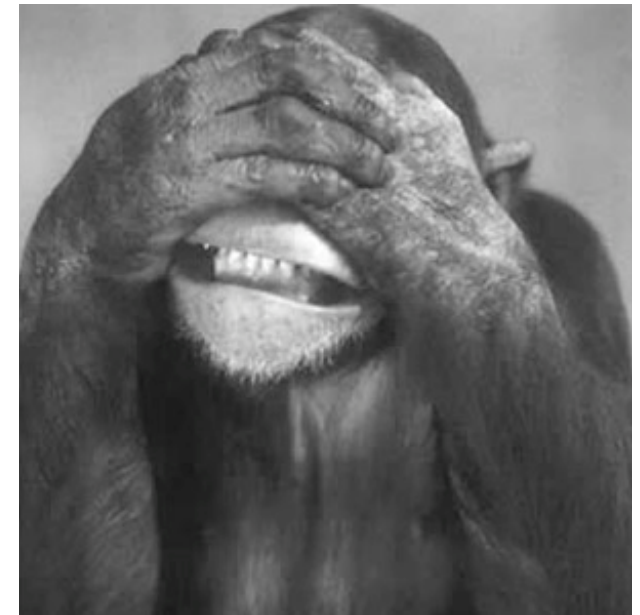
Gartner on Security Risks in Data Center Virtualization Projects

- **Gartner Research Report G00173434, published 01/25/2010**
- **Summary (with the risks) can be found here:**
 - <http://security.tekrati.com/research/10810/>
- **Full report, as usual, available at Gartner, for a fee.**



Information Security Isn't Initially Involved in the Virtualization Projects

- **Architectural changes should mandate for a review of risks and controls.**
- **Still, in many organizations this doesn't happen.**
- **Infosec people, be aware: virtualization is one of those “fights you can't win”.**



A Compromise of the Virtualization Layer Could Result in the Compromise of All Hosted Workloads

- In quite some discussions about virtualization security, this is “the big one”.
- The associated risk is *not* the same for all virtualization solutions.
- At least in VMware ESX space this *has* happened in the past!



The Lack of Visibility and Controls on Internal Virtual Networks Created for VM-to-VM Communications Blinds Existing Security Policy Enforcement Mechanisms

- **Remember some of the “basic building blocks of (network) security”:**
 - Access Control
 - Isolation / Segmentation
 - Filtering
- **Ask yourself**
 - Which of those are needed to achieve your security goals?
 - How to implement them if needed?



Workloads of Different Trust Levels Are Consolidated Onto a Single Physical Server Without Sufficient Separation

- This is an interesting one... as it contains a (pre-) judgement.
- That is: “mixing security levels on one platform is a bad thing”.
- Is it?
- If so why?
- Go back to previous slide.
- And, btw, remember: it’s all about risk.



Adequate Controls on Administrative Access to the Hypervisor/VMM Layer and to Administrative Tools Are Lacking

- In many environments management access to the virtualization platforms is *the Achilles' heel* of the overall environment.
- In the virtualization world this is further aggravated due to unclear roles & responsibilities.



There Is a Potential Loss of SOD for Network and Security Controls

- **And there's even one layer more now (the hypervisor).**
- **Clear roles & responsibilities are needed, as for securing the steps of the provisioning workflow and during operations.**
- **Again, a whole lot of the overall security architecture might change.**



Zusammengefasst gibt es zwei relevante Risikokategorien

■ Operationelle Probleme (e.g. Benutzerfehler)

- Virtualisierung = zusätzlicher Layer => Komplexität
- Human Errors treten je nach Umgebung häufig auf, mit unterschiedlicher Auswirkung
- Typischerweise Sicherheitsziel Verfügbarkeit gefährdet



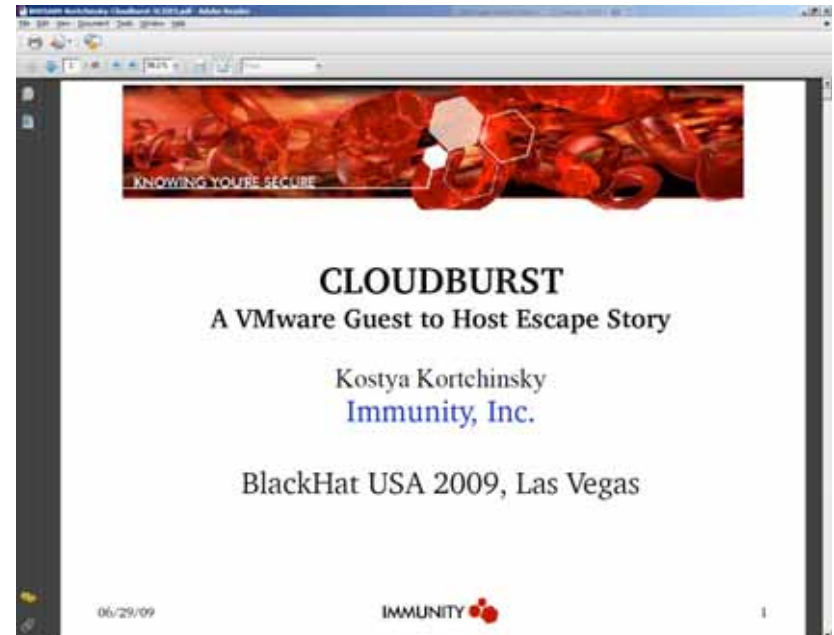
■ Angriffe, v.a. gegen Hypervisor

- Erfordern “skilled + motivated attacker”
- Sind gegen einige Plattformen schon erfolgreich demonstriert worden
 - *Cloudburst* gegen VMware ESX
- Gefährden Sicherheitsziele Vertraulichkeit und Integrität, mit potentiell gravierender Auswirkung

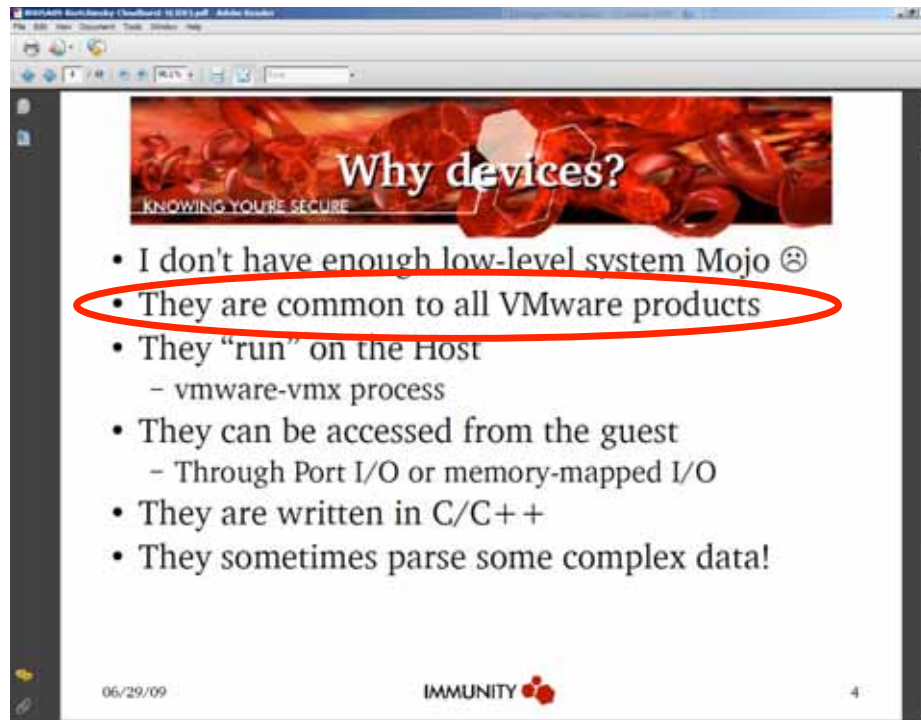


Exkurs: Cloudburst

- **Full guest → host escape on VMware ESX**
 - Call it “full [ESX] host compromise by guest attacker”, for that matter.
- **Initially shown at BH US 2009**
- **Illustrates some potential (real) problems of VMware ESX.**
- <http://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-SLIDES.pdf>



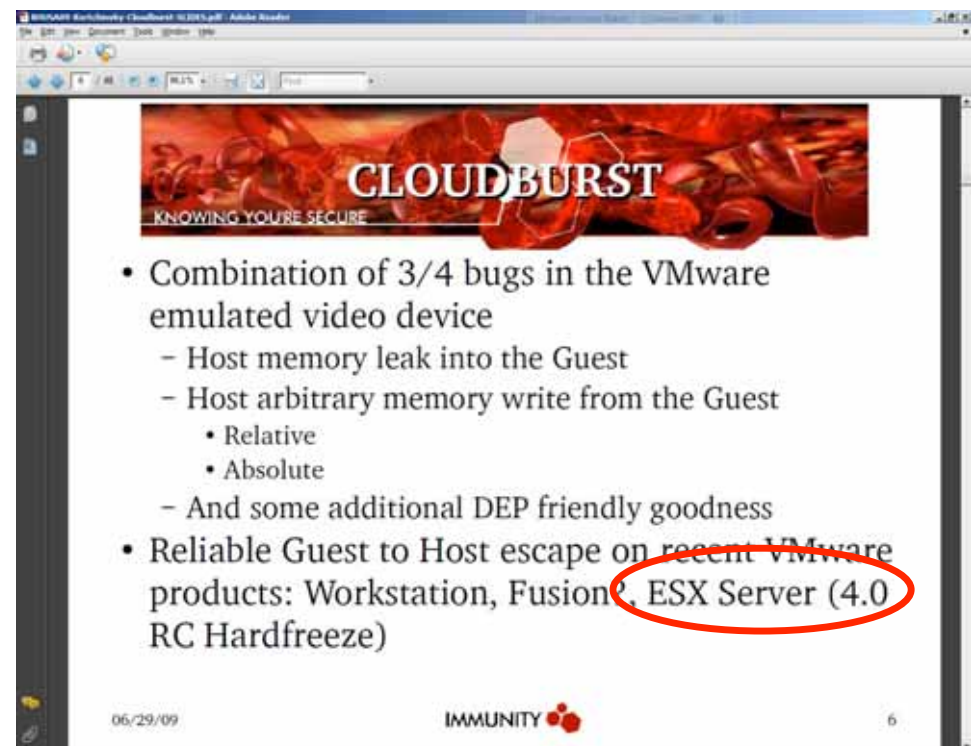
Devices ... and their use for attacks



Why devices?
KNOWING YOU'RE SECURE

- I don't have enough low-level system Mojo ☹
- They are common to all VMware products
- They "run" on the Host
 - vmware-vmx process
- They can be accessed from the guest
 - Through Port I/O or memory-mapped I/O
- They are written in C/C++
- They sometimes parse some complex data!

06/29/09 IMMUNITY 4



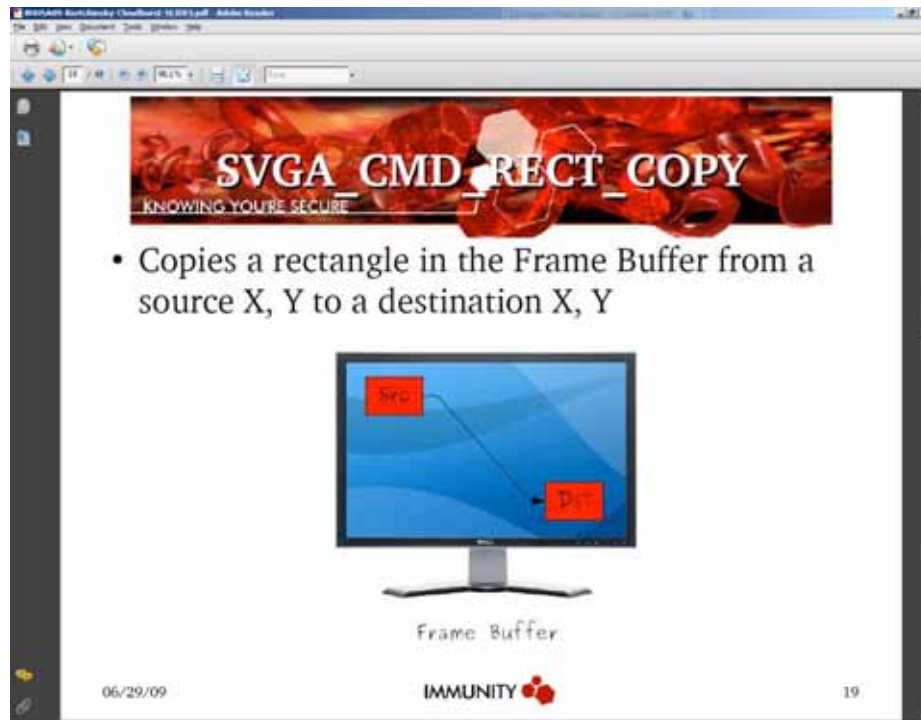
CLOUDBURST
KNOWING YOU'RE SECURE

- Combination of 3/4 bugs in the VMware emulated video device
 - Host memory leak into the Guest
 - Host arbitrary memory write from the Guest
 - Relative
 - Absolute
 - And some additional DEP friendly goodness
- Reliable Guest to Host escape on recent VMware products: Workstation, Fusion, ESX Server (4.0 RC Hardfreeze)

06/29/09 IMMUNITY 6




Rectangles ...



SVGA_CMD_RECT_COPY
KNOWING YOU'RE SECURE

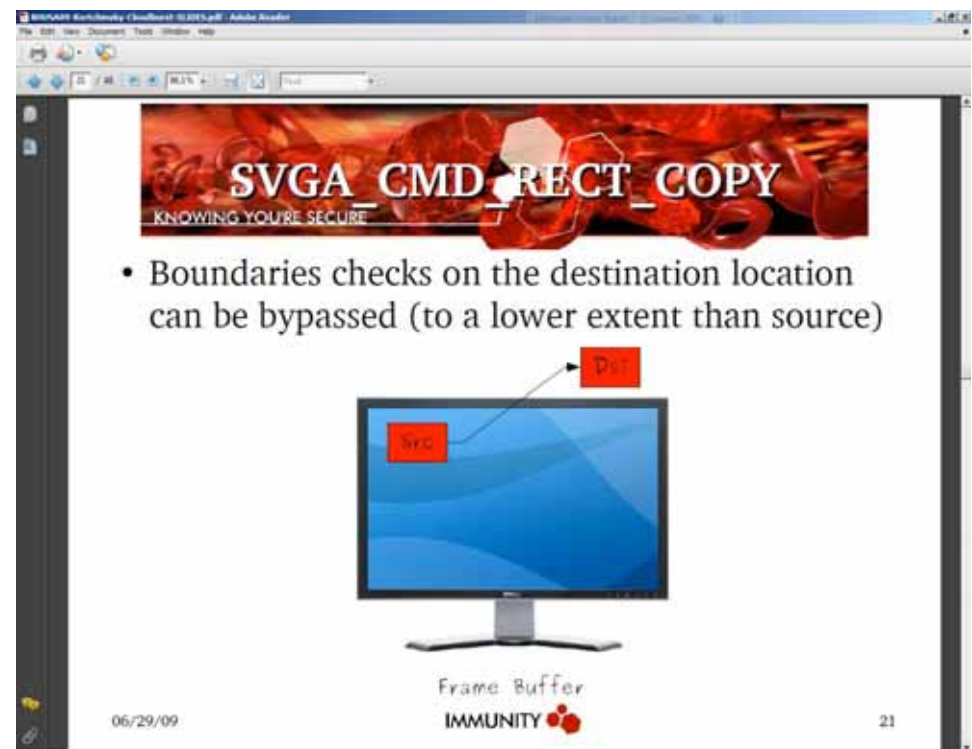
- Copies a rectangle in the Frame Buffer from a source X, Y to a destination X, Y



Frame Buffer


IMMUNITY

06/29/09 19



SVGA_CMD_RECT_COPY
KNOWING YOU'RE SECURE

- Boundaries checks on the destination location can be bypassed (to a lower extent than source)



Frame Buffer

IMMUNITY

06/29/09 21



... and glyphs...



SVGA_CMD_DRAW_GLYPH
KNOWING YOU'RE SECURE

- Draws a glyph into the frame buffer
- Requires `svga.yesGlyphs="TRUE"`

Virtual Screen

06/29/09 IMMUNITY 23



SVGA_CMD_DRAW_GLYPH
KNOWING YOU'RE SECURE

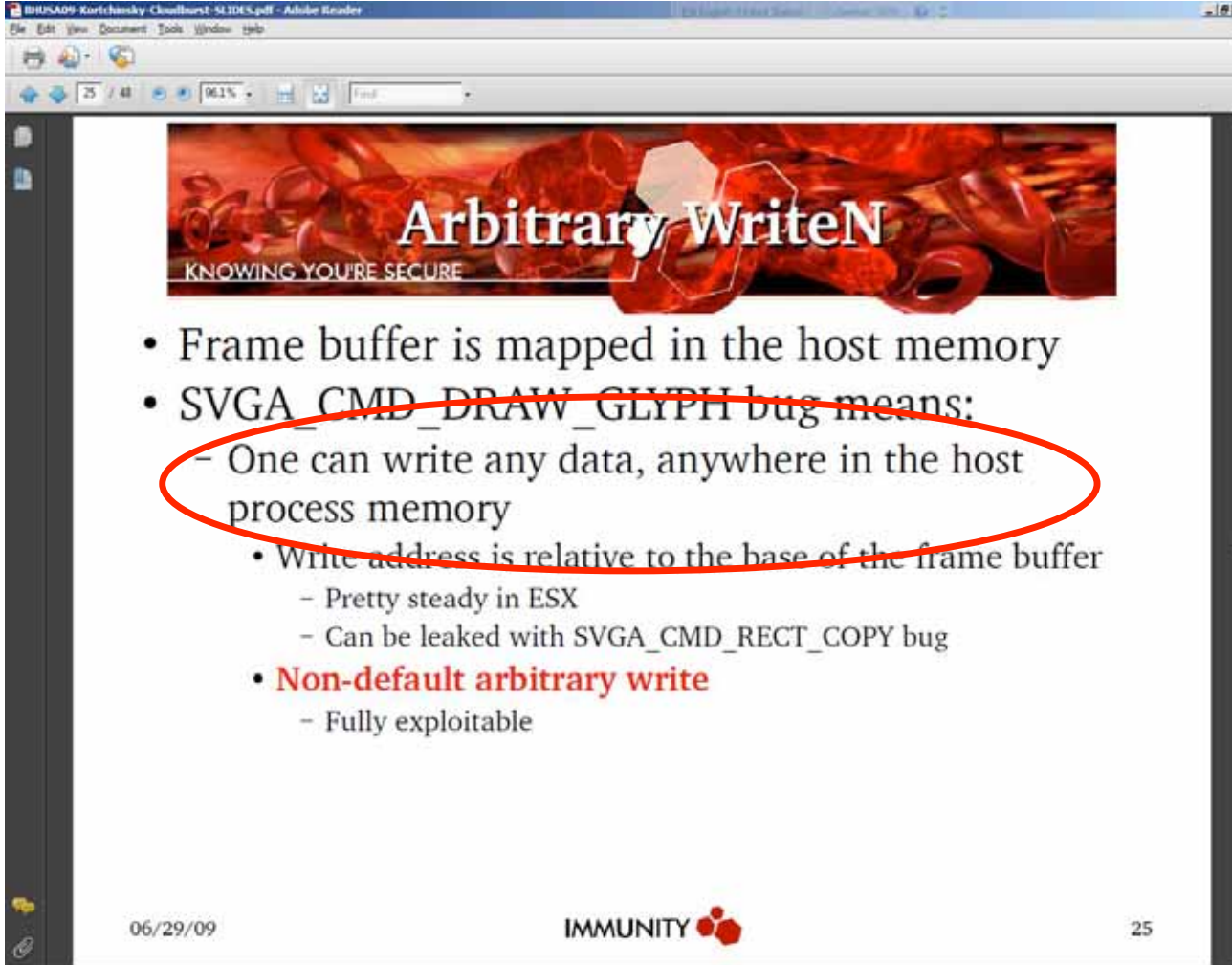
- There is no check on the X, Y where the glyph is to be copied

Virtual Screen

06/29/09 IMMUNITY 24



The consequence



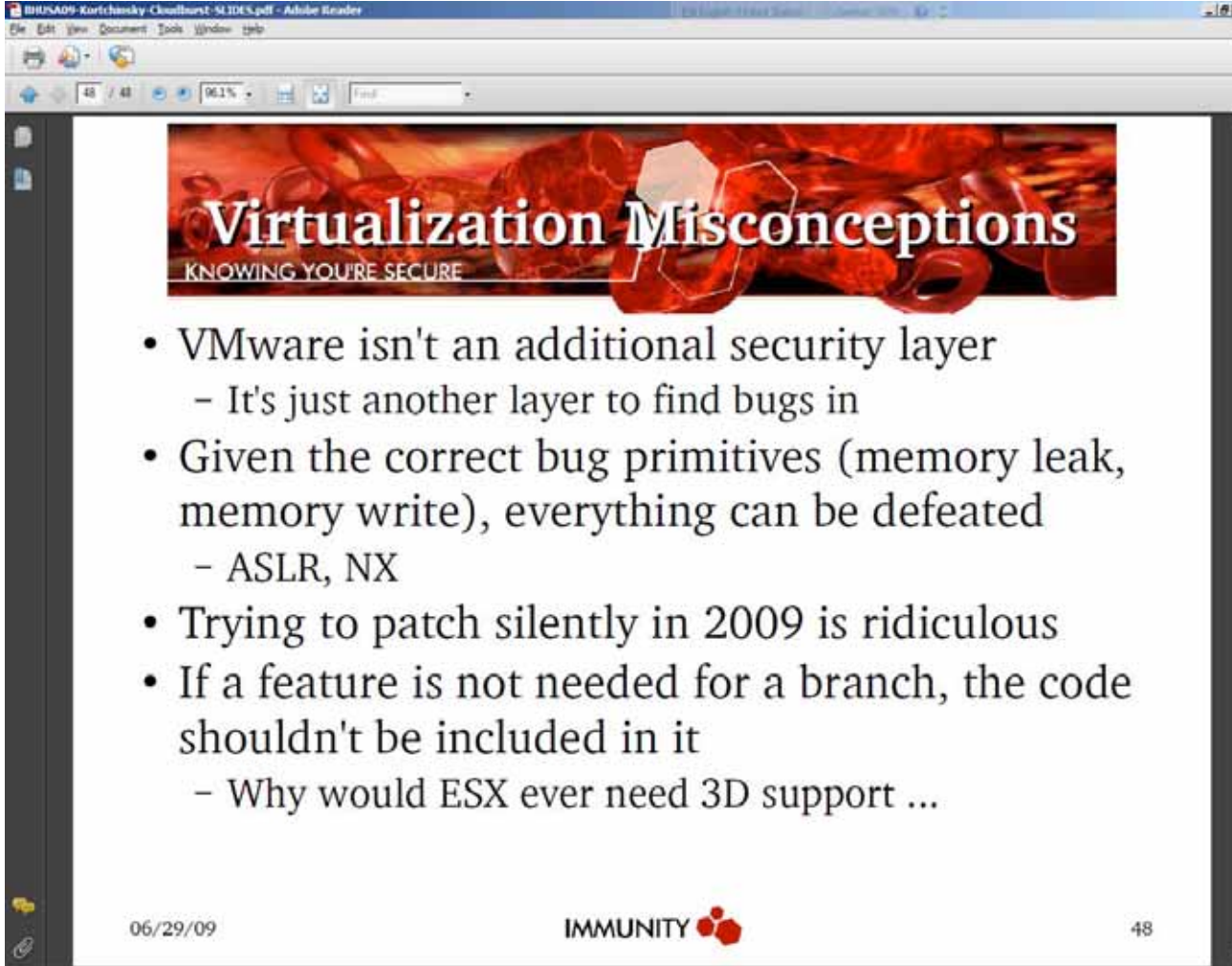
Arbitrary WriteN
KNOWING YOU'RE SECURE

- Frame buffer is mapped in the host memory
- SVGA_CMD_DRAW_GLYPH bug means:
 - One can write any data, anywhere in the host process memory
 - Write address is relative to the base of the frame buffer
 - Pretty steady in ESX
 - Can be leaked with SVGA_CMD_RECT_COPY bug
 - **Non-default arbitrary write**
 - Fully exploitable

06/29/09 IMMUNITY 25



Conclusions, as of Black Hat talk



The screenshot shows a presentation slide titled "Virtualization Misconceptions" with the subtitle "KNOWING YOU'RE SECURE". The slide is displayed in an Adobe Reader window. The slide content includes a list of four bullet points. At the bottom of the slide, there is a date "06/29/09", the "IMMUNITY" logo, and the number "48".

- VMware isn't an additional security layer
 - It's just another layer to find bugs in
- Given the correct bug primitives (memory leak, memory write), everything can be defeated
 - ASLR, NX
- Trying to patch silently in 2009 is ridiculous
- If a feature is not needed for a branch, the code shouldn't be included in it
 - Why would ESX ever need 3D support ...

06/29/09 IMMUNITY 48





Veränderung vorhandener Architekturen



Seven Sisters

Dei sju søstre, Norway



Seven Sisters of Infrastructure Sec



Access Control



Restriction (Filtering)



Segmentation/Isolation



Encryption



Hardening



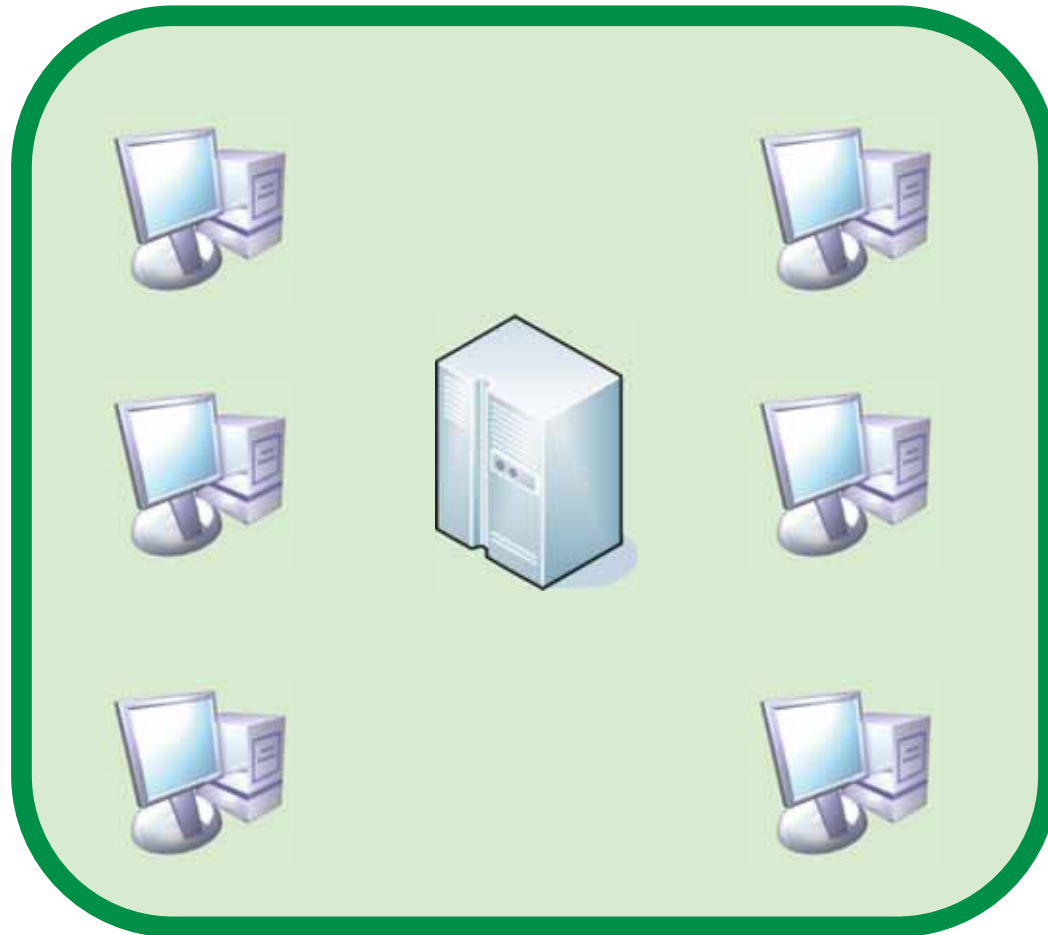
Secure Management



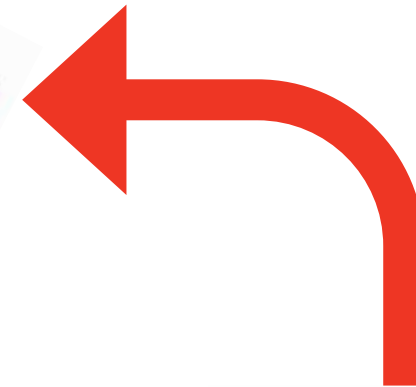
Visibility



Access Control



Some Complex System

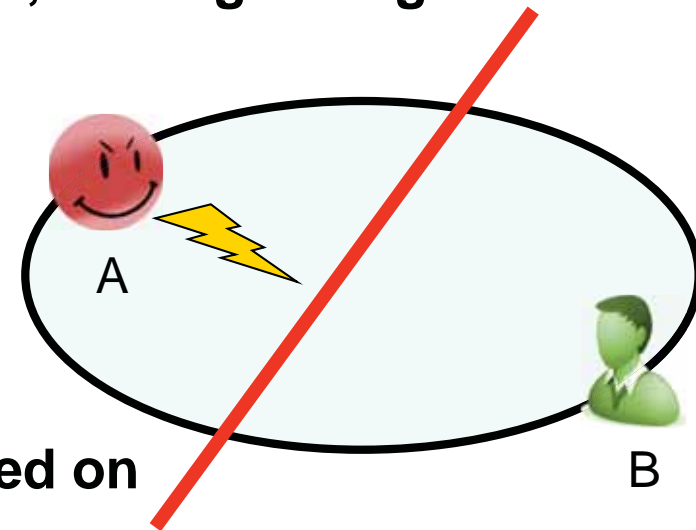


Threat



Isolation

- If some traffic (based on network design, routing config and/or traffic's properties) can't reach a destination... you won't have a problem there...



- **Isolation / Segmentation should be based on**

- Different protection needs
- Different threat potential

[that's why one uses "DMZs"]

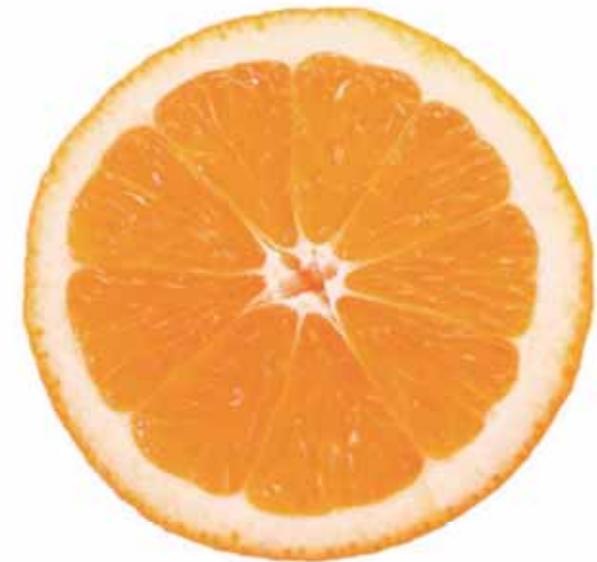
- Overall most important network security mechanism.
- Often combined with filtering.



Segmentation Approaches (on network level)

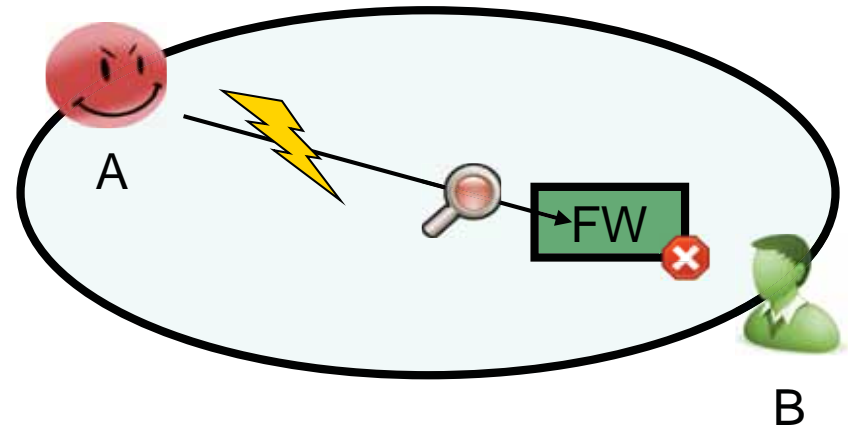
■ Segmentation as of

- Functions
 - E.g. surveillance mechanism in banks
 - Test vs. production
 - Voice VLAN
- (Different) Protection needs (“Schutzbedarf”)
 - Core banking systems
 - Domain controllers
 - “Server VLAN”
- Business relationship
 - Dedicated segments for customer(s)
- (Different) Threat potential
 - DMZs
 - Dedicated segments for WLAN clients



Restriction (Filtering)

- If you don't want that some traffic reaches some destination... filter it!
- Preferably implemented on existing hardware than on dedicated one (which would add complexity).
- If conflict *manageability vs. 'security'* arises, opt for manageability (fewer + coarse rules better than more + accurate rules).



Encryption

- **Best (and mostly) only method if you don't trust the transport path.**
- **Again: manageability is key.**
- **Think about key mgmt processes *before* deploying.**
- **Performance might be a factor, too.**
→ **Perform risk analysis if highest key length needed.**



Hardening

- **Unsecure nodes (still) one of the weakest points in many environments.**
- **It's not rocket science to harden nw devices, basic rules apply...**
- **And don't forget all those protocols**
 - Routing protocols
 - Layer 2 (STP, VTP/DTP, LLDP etc.)
 - NTP, syslog
 - DNS, DHCP
 - LDAP / AD stuff



Secure Management

- **Restriction of source addresses authorized for mgmt access.**
- **Choice of protocols (SSH vs. Telnet, HTTPS vs. HTTP, SNMPv3 vs. community-based SNMP).**
- **Use of good passwords and personalized accounts (for accountability).**
- **Logging of all successful/failed logins and – if possible – performed actions.**



- You do this extensively for *compliance reasons*, don't you? ;-)
- If you can't really prevent/control stuff you should at least be able to detect or track.



- Ask yourselves: Would you notice if the configuration of a network device was modified?
- Lots of free and powerful tools available, usually no need to “buy another appliance“ ...





Access Control



Hardening



Secure Management



Segmentation/Isolation



Encryption



Restriction (Filtering)



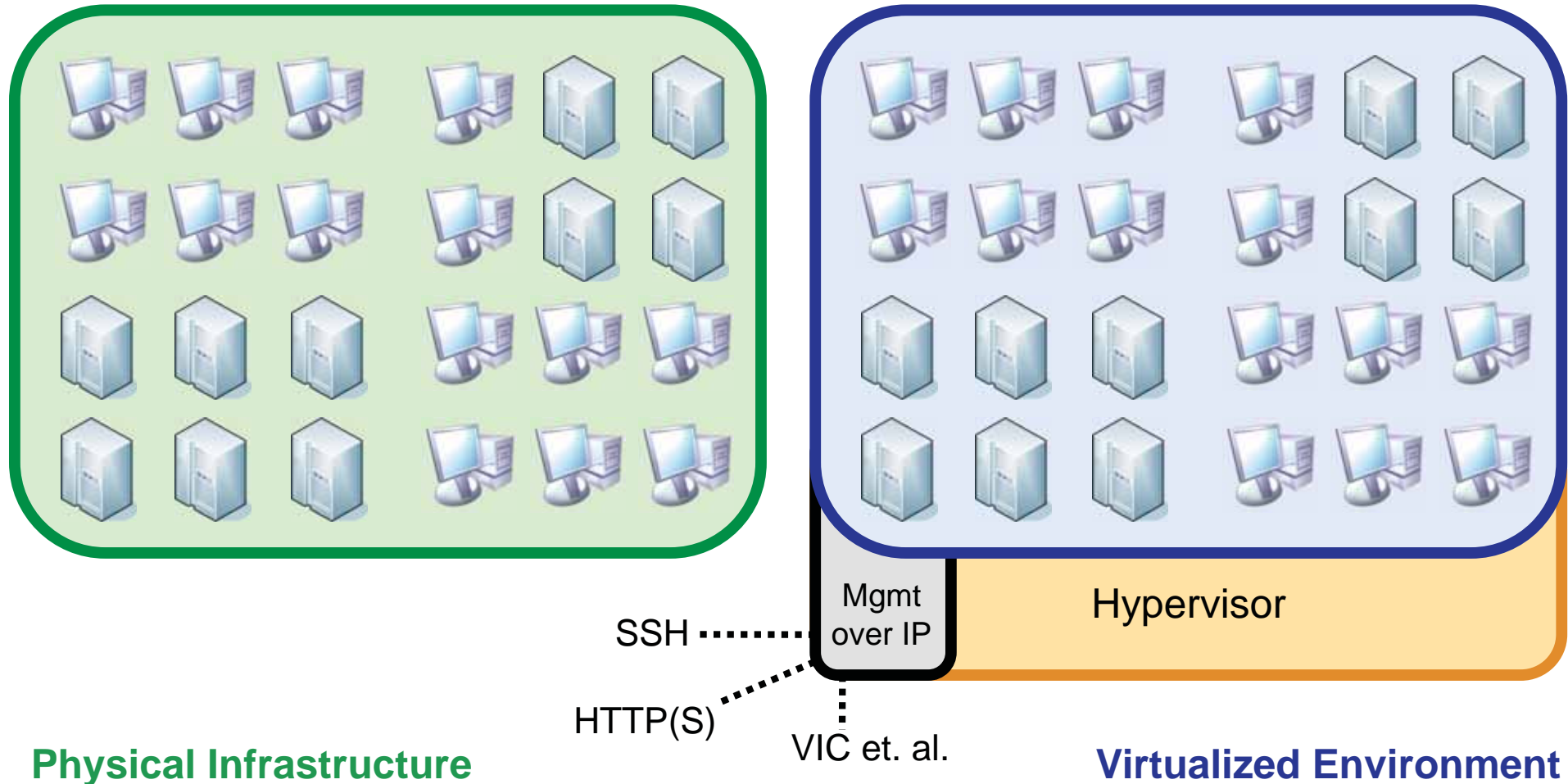
Logging/Monitoring

**In the Virt_World
some of the
sisters change...**



Access Control, Diskussion

Datacenter

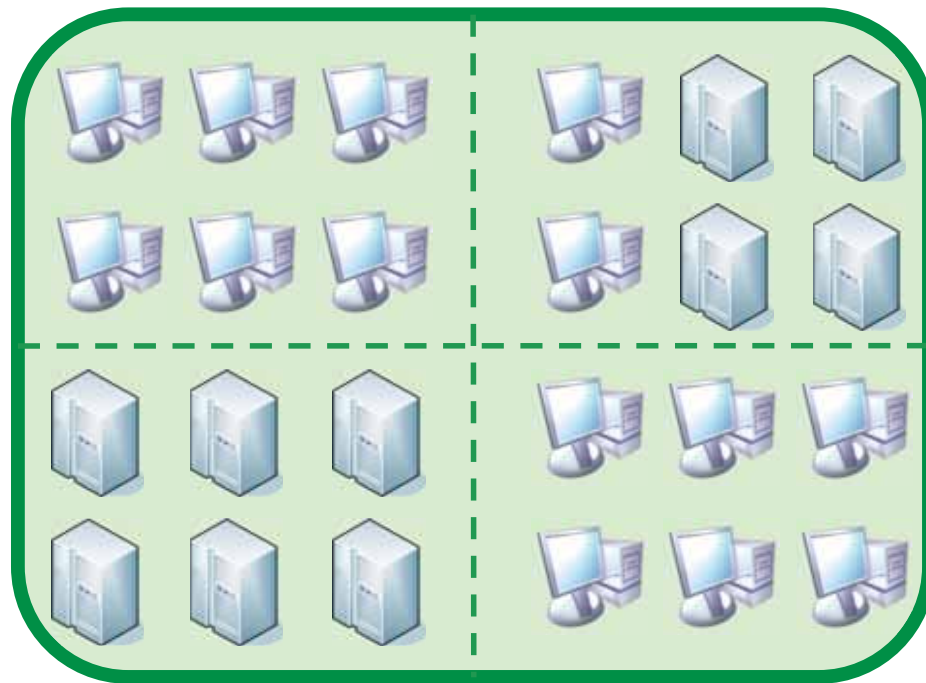


Physical Infrastructure

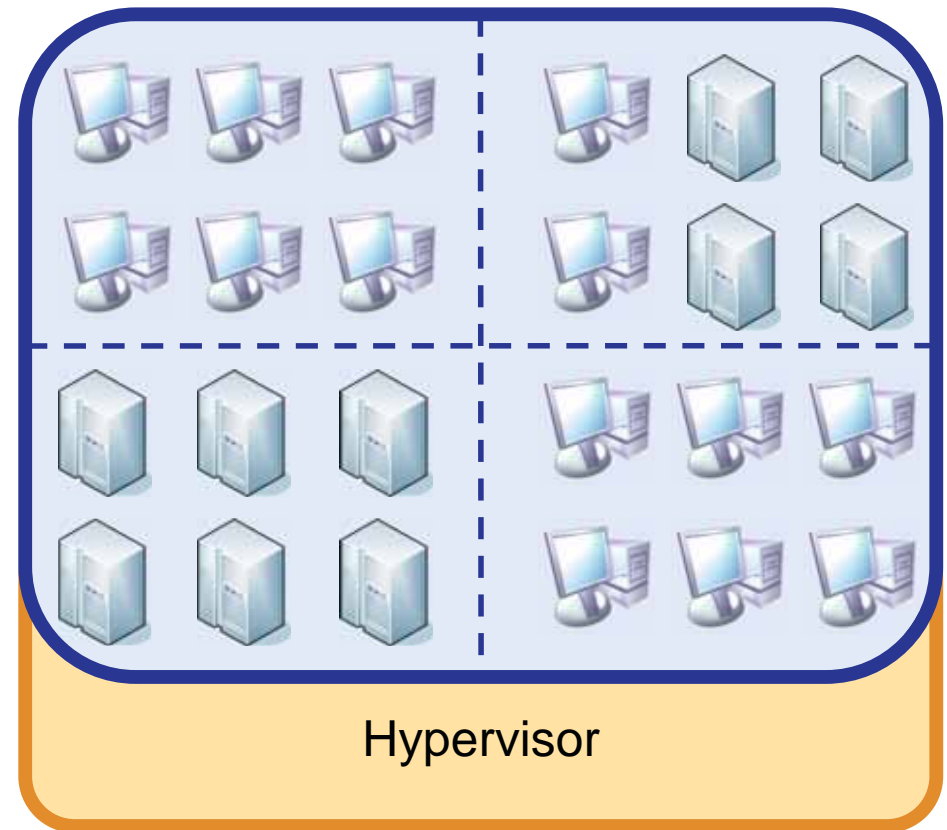
Virtualized Environment



Isolation, Diskussion



--- e.g. VLANs

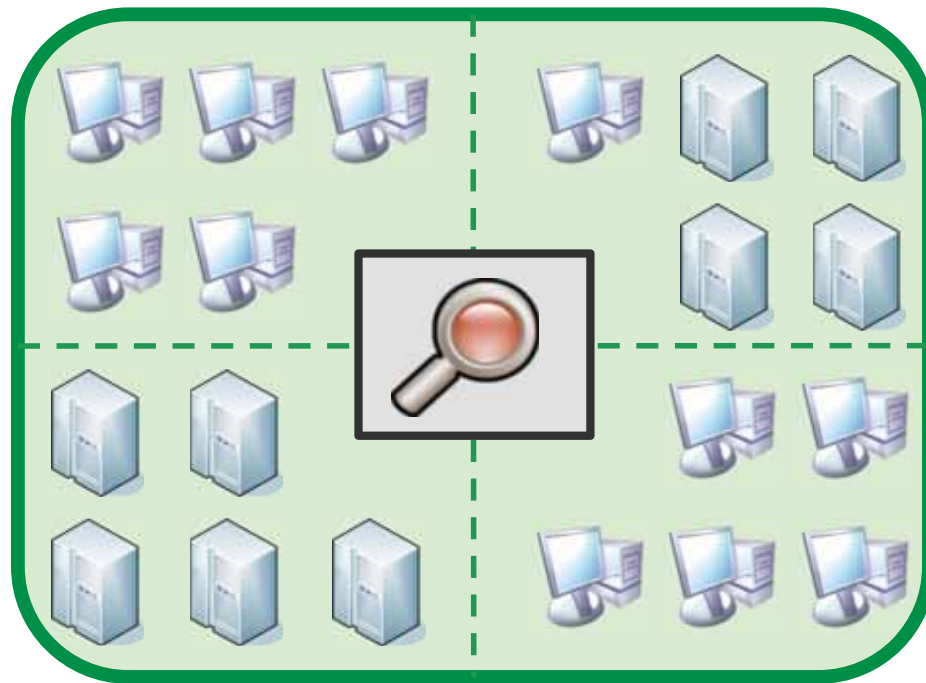


Physical Infrastructure

Virtualized Environment



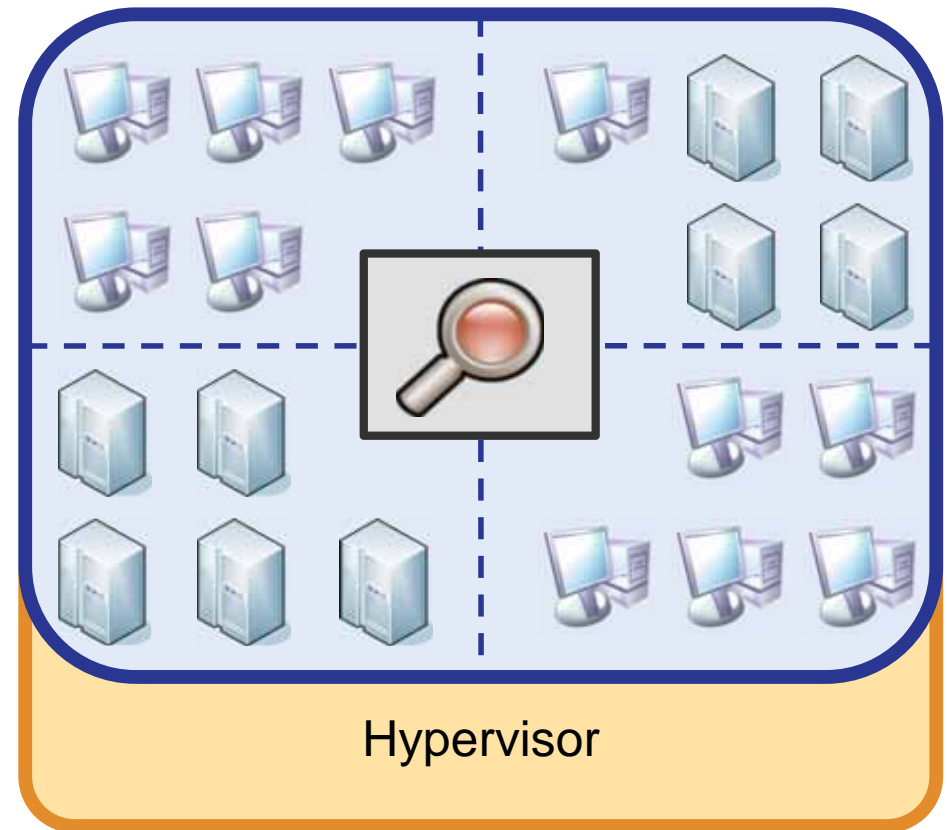
Isolation, Diskussion



--- e.g. VLANs

 Packetfilter

Physical Infrastructure



Hypervisor

Virtualized Environment



Isolation – Three Layers

- **Computing (Memory, CPU)**



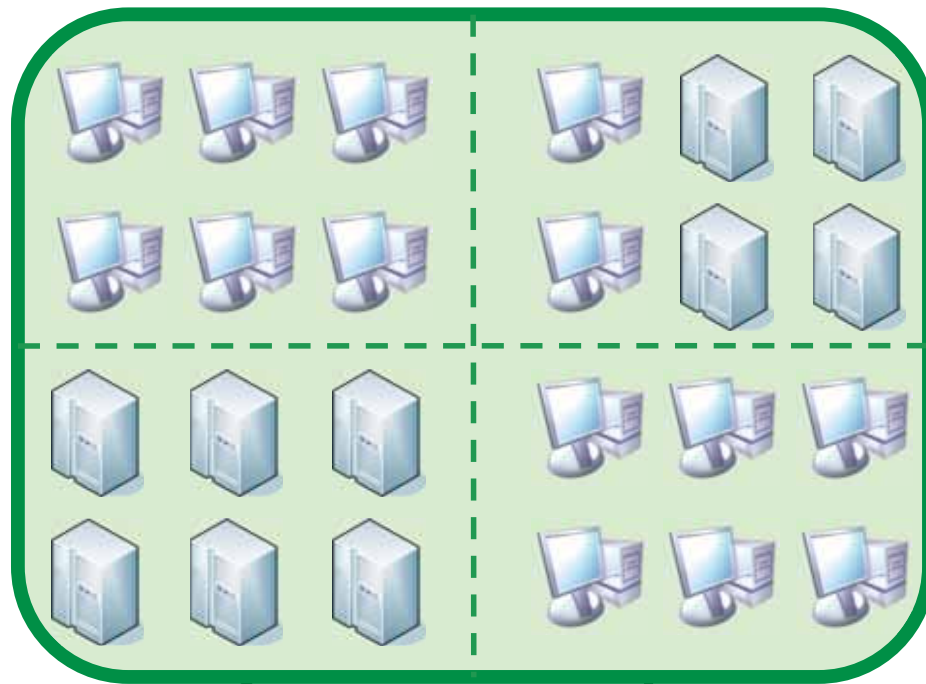
- **Network**



- **Storage**



Isolation, Diskussion



Mgmt



Storage

Physical Infrastructure

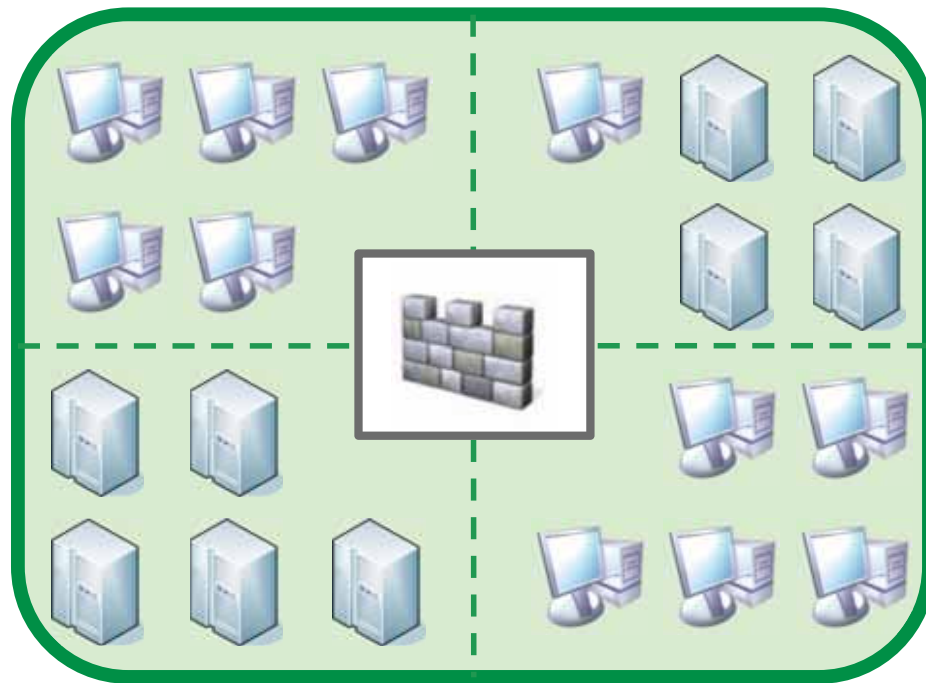


Hypervisor

Virtualized Environment



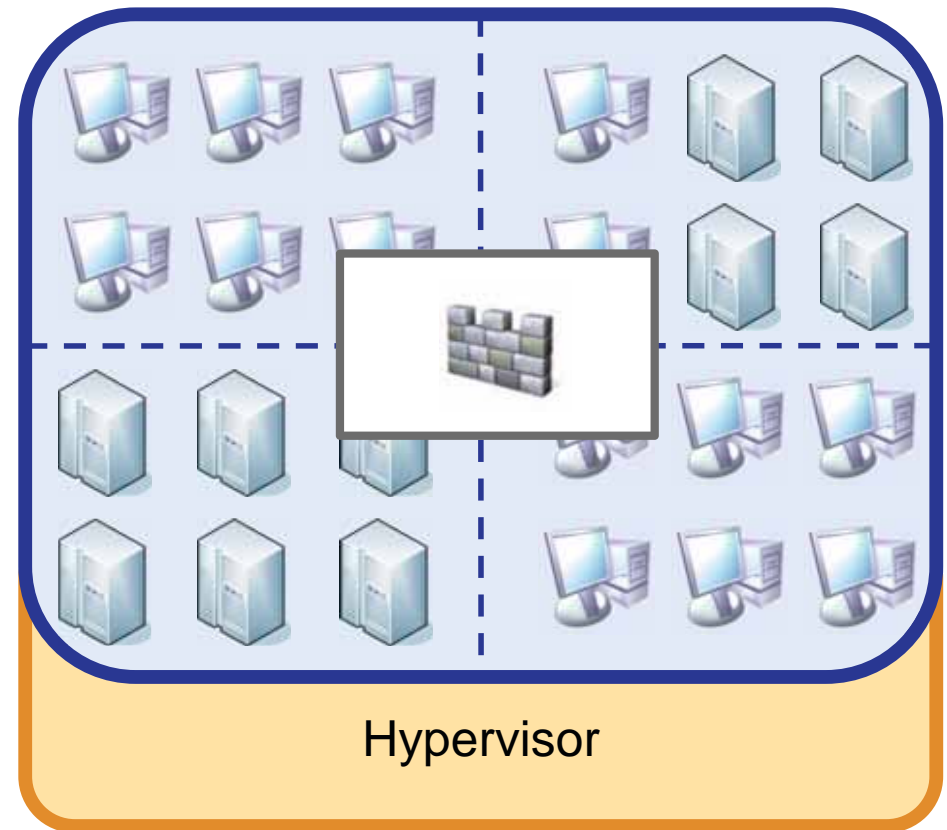
Restriction, Diskussion #1



--- e.g. VLANs

 Firewall

Physical Infrastructure

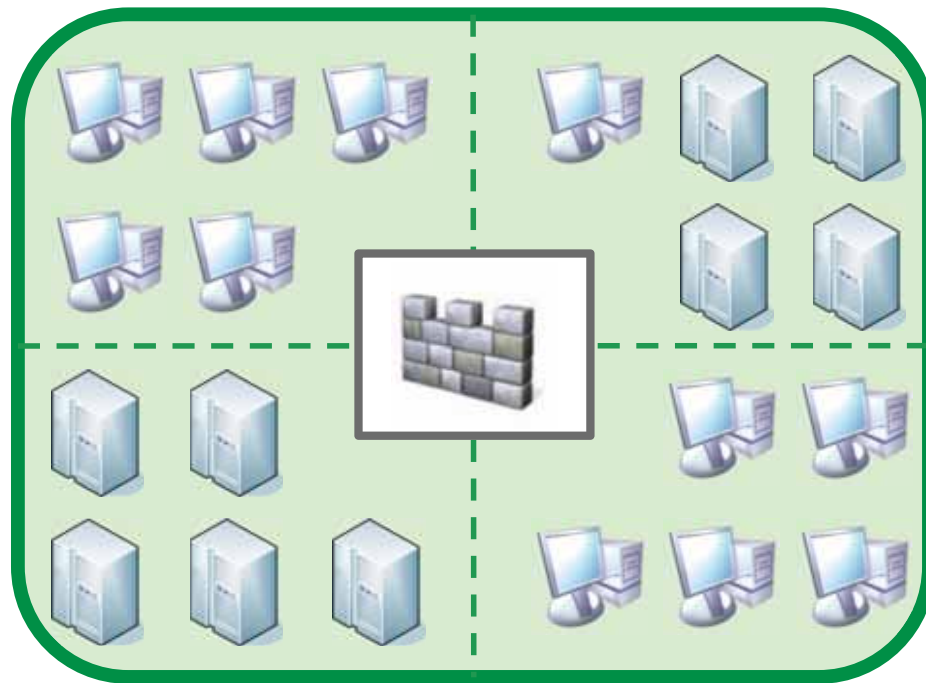



Hypervisor

Virtualized Environment

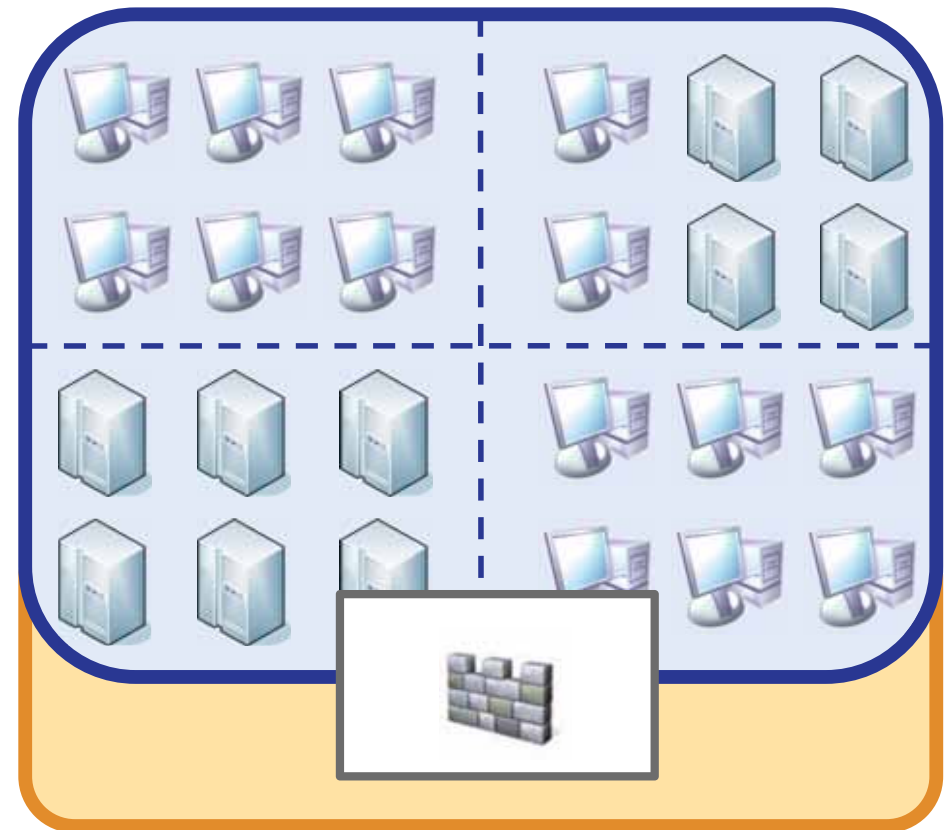


Restriction, Diskussion #2



--- e.g. VLANs
 Firewall

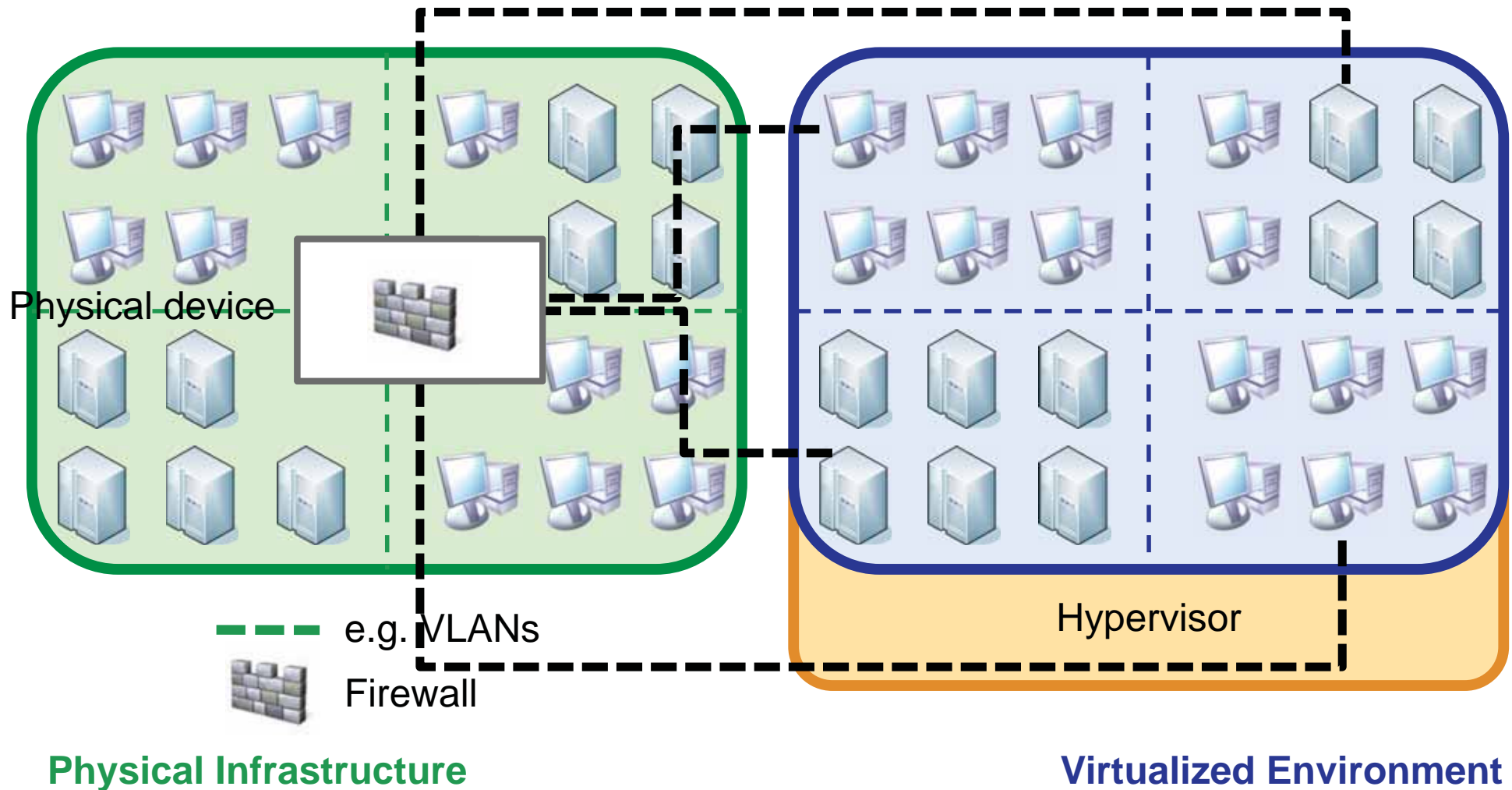
Physical Infrastructure



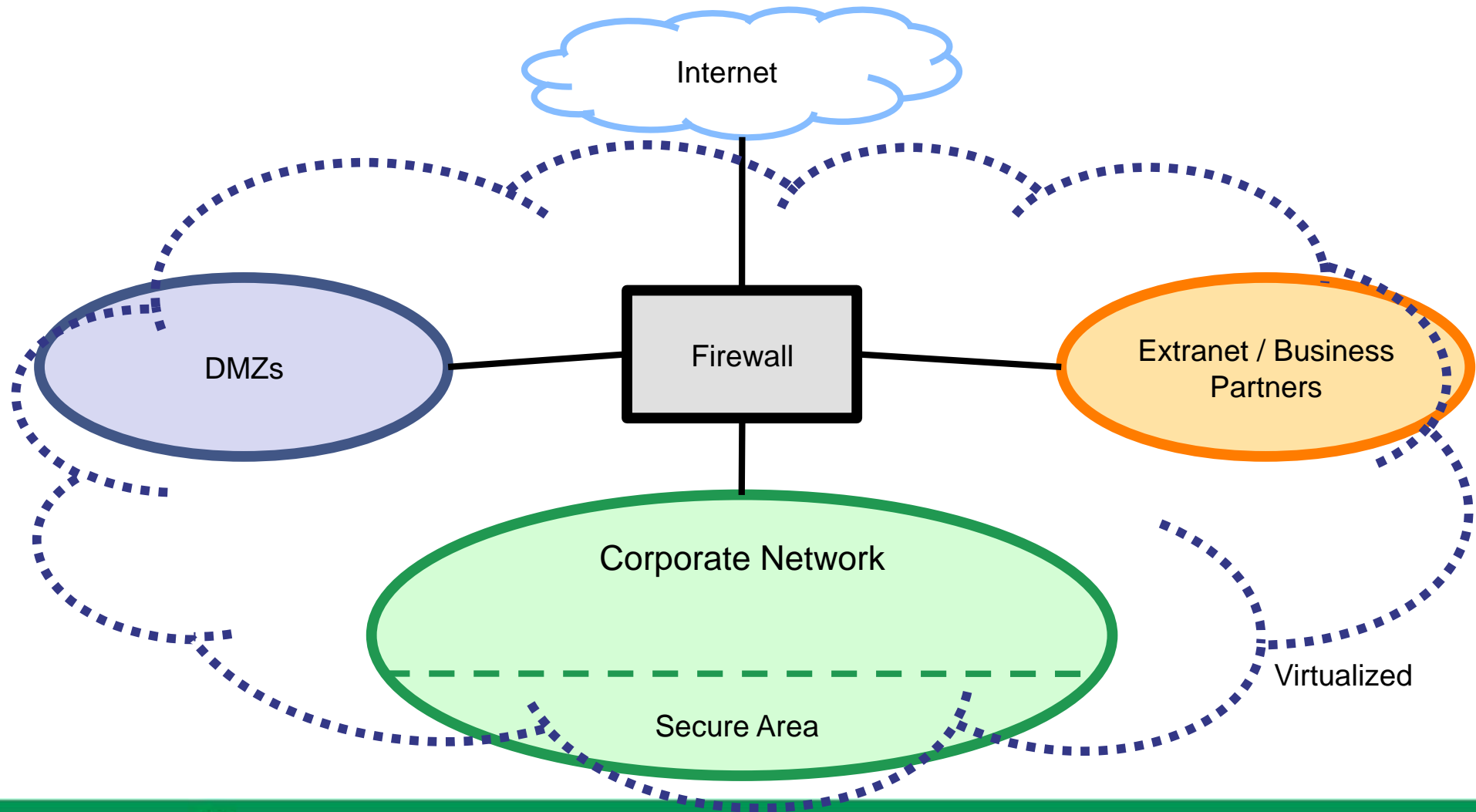
Virtualized Environment



Restriction, Diskussion #3



Netzwerkzonen, exemplarisch



General Use

- The building blocks can be “applied“ to all components / technologies / protocols.

Just ask yourselves:

- What is the “scope“? Can it be limited?
- Can (the traffic) be filtered / restricted?
- Are there authentication mechanisms?
- How’s the stuff being managed?
- Any hardening (of a device or service) possible?
- What about logging / monitoring?



Summary

For large organizations' network security some things are relevant:

- **Understanding of risks.**
- **Applying trust & control where appropriate.**
- **Finding the right balance of operational feasibility and security benefit.**
- **Security is built from simple rules.**

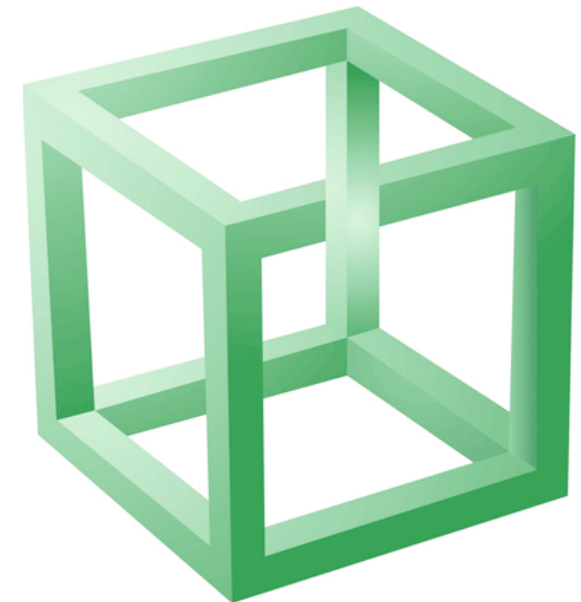


■ Ein Cluster mit jeweils eigenem Mgmt pro Zone

- Entspricht “altem Modell” → “kein Policy-Verstoss”
- Potentiell ineffizient
- Nicht das, was der CIO/IT-Infrastructure wollen ;-)

■ Ein grosser Cluster über alles

- Nicht das, was InfoSec will ;-)
- Ggf. mit Recht...
- Policy-Verstoß
- “Non-Compliance”?
 - BSI: unklar
 - NIST: unklar



- **Var 3 “Kompromiss”**: verschiedene Zonen werden **zusammengefasst, aber nicht alle.**
 - → Frage: Welche zusammenfassen?
 - Und: “Was machen wir mit dem Mgmt?” Eines? Mehrere?



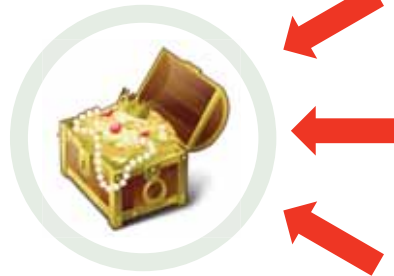
Welche Zonen zusammenfassen?

- **Drei relevante Entscheidungsfaktoren:**

- **Schutzbedarf**

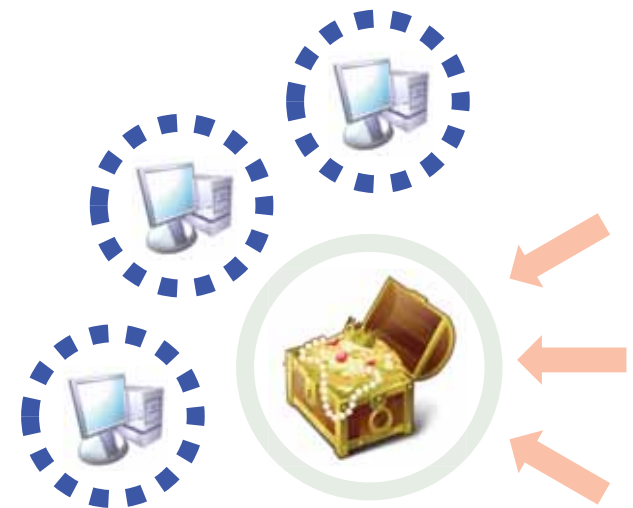


- **Bedrohungspotential**



- **Trust (worthiness)**

- “Zu welchem Grad können wir Systemen in dieser Zone vertrauen?”



Beispiel

Number	Name	Protection Need	Threat Potential	Level of Trust
5	Public Internet	low	high	low
4	External DMZs	high	medium	medium
3	Business Partner DMZs	medium	medium	medium
2	Internal default, CN	high	low -medium	medium-high
1	High Security	high	low	high



Die Gretchenfrage

■ Isolation ausreichend?

BSI:

“Wurden vor der Virtualisierung Netze aufgrund unterschiedlichen Schutzbedarfs physikalisch getrennt, müssen diese Netze auch in virtuellen Umgebungen voneinander isoliert werden. Es ist dann zu prüfen, ob die Mechanismen zur Netztrennung, sowie der Kapselung und Isolation der virtuellen IT-Systeme in der eingesetzten Virtualisierungslösung ausreichen, um virtuelle IT-Systeme mit hohem Schutzbedarf gemeinsam mit solchen niedrigen Schutzbedarfs auf einem Virtualisierungsserver betreiben zu können.

Diese Prüfung kann z. B. darin bestehen, dass der Hersteller der betreffenden Virtualisierungslösung die genannten Mechanismen für diesen Einsatzzweck (Trennung von Maschinen unterschiedlichen Schutzbedarfs) als geeignet bezeichnet und dies durch eine entsprechende Zertifizierung nachweist.“

Welche Zertifizierung denn?



Damit stellen sich folgende Fragen

- **Wird ein bestimmtes Security Principle überhaupt zur Erreichung der Sicherheitsziele benötigt?**
 - Oder ist nur eine (aus sog. Best Practices abbeschriebene) Altlast?
 - Beispiel: DMZ-Systeme, die auf einen gemeinsamen Datenbestand im Backend zugreifen. → Wo ist der Isolation-Need?
- **Wenn es benötigt wird**
 - Ist es “per default” / laut Hersteller “automatisch vorhanden”?
→ Weitere Fragen schliessen sich an, s.u.
 - Kann/muss es konfiguriert werden?
 - Weitere Fragen schliessen sich an, s.u.



Hersteller sagt: “ist vorhanden”

- **Neue Frage: Vertrauen wir dieser Aussage/dem Hersteller?**

- **Ansätze zur Beantwortung/Lösung**

- Trust Metrik (etwa die von ISECOM →
 - www.packetstormsecurity.org/papers/presentations/Mastering_Trust_Sampler.pdf)
- Zertifizierung (e.g. Common Criteria)
 - → neue Fragen, s.u.
- Entscheidung “ja, tun wir” (etwa durch CIO)
- Risk Acceptance (eigentlich ist hier ein Widerspruch ;-)



In the end of the day...

- ... it's all about risk
- ➔ **Saubere Risiko-Analyse ist der absehbar zielführendste Weg zur Beantwortung der o.g. Fragen**
- ... erfordert aber geeignete Instrumente (e.g. *ERNW Rapid Risk Assessment*) und entsprechendes Prozess-Knowhow



- **ERNW RRA:**

http://troopers.de/content/e728/e897/e907/TROOPERS10_Rapid_Risk_Assessment_Enno_Rey.pdf



Var2: “Muss konfiguriert werden”

→ Neue Fragen

- **Wie wird das operationell sichergestellt?**
 - Für den Initialzustand.
 - Im laufenden Betrieb.



→ Neue Fragen

- **Steht der Sicherheitsgewinn in vernünftigem Verhältnis zu Capex/Opex/Komplexitätserhöhung?**
 - Häufig: “nein!”
- **→ Risikoanalyse ;-)**



- **Ansonsten: siehe Zusatzfragen bei “Muss konfiguriert werden”.**



Wichtige Maßnahmen

- **Auf Design-Ebene**



- **Infrastruktur**



- **Host**



Für diejenigen, die gerne eine 30sec-Aussage dieses Vortrags hätten: Unsere fünf Grundregeln (VMware)

- **Höchste Klassifizierung/Zone nicht virtualisieren.**
 - Zumindest nicht mit VMware ESX.
- **Nur nebeneinanderliegende Klassifizierungsstufen/Zonen.**
- **Nicht DMZ mit CN mischen.**
- **“DMZ in sich” nur bei homogenem Schutzbedarf.**
- **Mixed Mgmt ist hinsichtlich Gesamtrisiko i.A. vertretbar.**



Some important hardening steps

- Prevent other users from spying on administrator remote consoles: `RemoteDisplay.maxConnections=1`
- Prevent unauthorized removal, connection and modification of devices:
 - `isolation.device.connectable.disable=TRUE`
 - `isolation.device.edit.disable=TRUE`
- Ensure that vSphere management traffic is on a restricted network.
- Ensure that the 'Promiscuous Mode' policy is set to reject.
- Use 'reliable' certificates for VIC communication.



What else can we do for you?

- **ERNW Virt-Audit Checkliste**
 - Kann bei Bedarf zugesendet werden.

- **Troopers 2011 ;-))**



www.troopers.de



- **Virtualisierung führt zu einer veränderten Risiko-Lage.**
 - Operations is key.
- **Rolle und Funktion bisheriger Sicherheitsansätze und -instrumente ändern sich.**
 - Verständnis der Änderungen ist elementar.
- **Design und Infrastruktur-Entscheidungen haben die grösste Auswirkung auf die Gesamtsicherheit.**
 - Nicht “Hardening”!



There's never enough time...

THANK YOU...



...for yours!



- **Vorabversion des Grundschutzbausteins B3.40 *Virtualisierung*:**
https://www.bsi.bund.de/cae/servlet/contentblob/938954/publicationFile/60461/baustein_virtualisierung_entwurf.pdf
- **NIST Special Publication 800-125 (Draft): Guide to Security for Full Virtualization Technologies (Draft) Recommendations:**
<http://csrc.nist.gov/publications/drafts/800-125/Draft-SP800-125.pdf>
- **Claudio Criscione:
The Good, The Bad, The Virtual**
http://troopers.de/content/e728/e897/e911/TROOPERS10_The_Good_The_Bad_The_Virtual_Claudio_Criscione.pdf
- **DayCon 2008:
Microsoft Hyper-V – A first Security Inspection**
http://ernw.de/content/e7/e181/e1245/download1351/ERNW_DayConII_microsoft_hyperV_security_ger.pdf
- **Security Day:
Virtualisierungs-Sicherheit**
http://ernw.de/content/e7/e181/e1391/download1393/ERNW_BechtleSecDay_Virtualisierungssicherheit_ger.pdf

