

# RRZN-Dienste

## Sicherheitstage SS 2007

RRZN

22.06.2007

## „Die UH-CA in der 3. Generation“

[http://www.rrzn.uni-hannover.de/fileadmin/it\\_sicherheit/pdf/SiTSS07-Dienste-CA.pdf](http://www.rrzn.uni-hannover.de/fileadmin/it_sicherheit/pdf/SiTSS07-Dienste-CA.pdf)

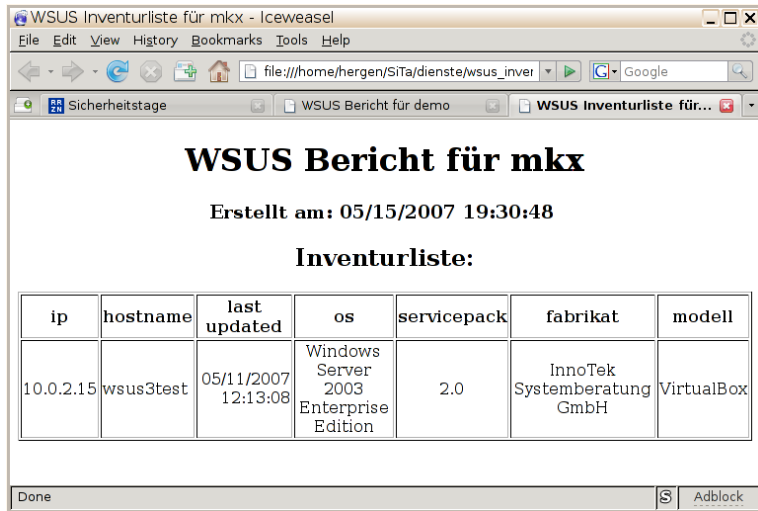
## derzeitiger Betrieb

[http://www.rrzn.uni-hannover.de/fileadmin/it\\_sicherheit/pdf/SiTSS07-Dienste-WSUS-SAV.pdf](http://www.rrzn.uni-hannover.de/fileadmin/it_sicherheit/pdf/SiTSS07-Dienste-WSUS-SAV.pdf)

## geplantes Reporting

- automatische Zuordnung zu Instituten anhand der Client-IP und deren Subnetz-Zugehörigkeit
- automatisches Entfernen alter Einträge (nach 30 Tagen)
- Verteilung von Reports zunächst über Sec-Serv (Netzschutz), später evt. Mail o.Ä.
- Inventar-Report: Daten über Clients (OS-Version, BIOS etc.)
- Status Windows-Update:  
je Client Update-Anzahl, „Problem-Ampel“
- derzeit Testinstallation mit WSUS 3.0 RRZN-intern,  
Einführung mit WSUS 3.0 & Umstellung Sec-Serv

## Inventar-Report



The screenshot shows a web browser window titled "WSUS Inventurliste für mkx - Iceweasel". The address bar contains the file path "file:///home/hergen/SiTa/dienste/wsus\_inver". The browser has three tabs open: "Sicherheitstage", "WSUS Bericht für demo", and "WSUS Inventurliste für...". The main content area displays the following report:

## WSUS Bericht für mkx

Erstellt am: 05/15/2007 19:30:48

### Inventurliste:

ip	hostname	last updated	os	servicepack	fabrikat	modell
10.0.2.15	wsus3test	05/11/2007 12:13:08	Windows Server 2003 Enterprise Edition	2.0	InnoTek Systemberatung GmbH	VirtualBox

At the bottom of the browser window, the status bar shows "Done" and an "Adblock" button.

## Update-Status

WSUS Bericht für demo - Iceweasel

file:///home/hergen/SiTa/dienste/wsus\_beric

Sicherheitstage WSUS Bericht für demo WSUS Inventurliste für mxk

## WSUS Bericht für demo

Erstellt am: 06/15/2007 19:30:44

### Zusammenfassung:

installed	downloaded	failed	not installed	unknown
244	4	3	4	1

### Details:

ip	hostname	installed	downloaded	failed	not installed	un
Done						

Done Adblock

## Update-Status

WSUS Bericht für demo - Iceweasel

file:///home/hergen/SiTa/dienste/wsus\_bericht\_20070615\_ks.html

Sicherheitsstage WSUS Bericht für demo WSUS Inventurliste für mxk

ip	hostname	installed	downloaded	failed	not installed	unknown	last updated
130.75.x.4	host-4.demo.uni-hannver.de	14	0	0	0	0	06/15/2007 16:23
130.75.x.5	host-5.demo.uni-hannver.de	14	0	0	0	0	06/15/2007 15:57
130.75.x.6	host-6.demo.uni-hannver.de	11	0	3	0	0	06/15/2007 18:43
130.75.x.7	host-7.demo.uni-hannver.de	14	0	0	0	0	06/15/2007 12:13
130.75.x.8	host-8.demo.uni-hannver.de	14	0	0	0	0	06/14/2007 10:11
130.75.x.9	host-9.demo.uni-hannver.de	14	0	0	0	0	06/15/2007 13:08
130.75.x.10	host-10.demo.uni-hannver.de	14	0	0	0	0	06/15/2007 21:11
130.75.x.11	host-11.demo.uni-hannver.de	14	0	0	0	0	06/15/2007 9:32
130.75.x.12	host-12.demo.uni-hannver.de	14	0	0	0	0	05/20/2007 15:56
130.75.x.13	host-13.demo.uni-hannver.de	14	0	0	0	0	06/11/2007 13:53
130.75.x.14	host-14.demo.uni-hannver.de	14	0	0	0	0	06/15/2007 8:23
130.75.x.15	host-15.demo.uni-hannver.de	10	4	0	4	0	06/13/2007 10:51

Done Adblock

## Offline-Update

- inoffizielle Patch-CDs / SPs durch Microsoft verboten
- bisherige Kopie aus Göttingen (GWDG) entfällt
- eigene ISO-Images werden vom RRZN automatisiert erstellt, angelehnt am ctupdate-Verfahren aber nach Linux portiert
- neue Images bereits im üblichen FTP-Verzeichnis  
`ftp://ftp.rrzn.uni-hannover.de/pub/uni-intern/Sicherheit`
- Dokumentation zur Nutzung folgt
- nach OS-Version aufgeteilt, 2003 muss bereits DVD sein



## derzeitiger Betrieb, SAU & Vista

[http://www.rrzn.uni-hannover.de/fileadmin/it\\_sicherheit/pdf/SiTSS07-Dienste-WSUS-SAV.pdf](http://www.rrzn.uni-hannover.de/fileadmin/it_sicherheit/pdf/SiTSS07-Dienste-WSUS-SAV.pdf)

## zu erwarten

### SAV-Clients

- Umstellung für Windows 2000, 2003, XP auf neue Version 7
- Einführung neuer SAV-Linux-Version 6, daher anders als angekündigt hier nichts zu Linux-SAV 5

### Update-Server

- Umstellung auf neue EM/EC-Version
- evt. Einführung Client-Management, bisher nur Updates
- mind. 2 Policies für Clients (wählbar bei Installation):
  - Update-Policy und weiche, änderbare Vorgaben
  - Update-Policy und vorgeschriebene, harte SAV-Einstellungen
- geplant ist Reporting (ähnlich wie oben für WSUS)

- Policy-Report:
    - Tool zur Regelaufbereitung erstellt
    - Integration in Sec-Serv geplant
  - wenn Reporting in Betrieb wäre Policy-Review wünschenswert
  - bei Änderungen bitte angeben:
    - IPs/Netze, Protokolle (TCP/UDP), Ports, Richtung
    - aber auch Zweck, Dienste, Produkte
- ermöglicht Policy-Kommentierung und Risiko-Bewertung

## FW-Policy

## inside\_access\_in

Nr.	Mode	Protokoll	Quell Host	Quell Port	Ziel Host	Ziel Port	Log
1.1	permit	ip	any		224.0.0.0/4		
1.2	deny	tcp	any		any	WinFS-TCP-SG	
1.3	permit	tcp	any		Mailserver-RRZN-HG	25	log
1.4	permit	tcp	any		130.75.6.240	Mailuser-send-empf-SG	log
1.5	permit	tcp	any		130.75.6.240	Mailuser-empfangen-SG	log
1.6	permit	tcp	any		any	Mailuser-empfangen-SG	log
1.7	permit	tcp	any		DNS-RRZN-HG	53	
1.8	permit	tcp	any		130.75.2.1	119	
1.9	permit	tcp	any		Time-RRZN-HG	123	
1.10	permit	tcp	130.75.41.1		130.75.6.20		
1.11	permit	tcp	any		any	TCP-allgemein-SG	
1.12	permit	tcp	Druckernutzer-HG		Drucker-HG	Drucker-TCP-SG	
Externe Drucker, die aus dem 41er-Netz ansprechbar sein sollen / Mai 2005							
1.25	permit	udp	any		Time-RRZN-HG	123	
1.26	permit	udp	any		RRZN1	Novell-Netstorage-UDP-SG	
1.27	deny	udp	any		any	WinFS-UDP-SG	
1.28	deny	udp	any		any	P2P-udp-SG	
1.29	deny	udp	any		any		log
1.30	permit	icmp	any		any	8	

## derzeit

Log-Dateien und Log-Auswertung nach Traffic & Sessions der Netzschutz-Firewalls. Zugriff per SSH & HTTP(S).

## geplant

- Zugriff nur noch per HTTPS
- Log-Dateien nach Policy-Verstößen auswerten
- Netzschutz-Policy als Webseite (s.o.)
- Sammelpunkt von (Log-) Informationen für Einrichtungen:
  - Netzschutz
  - WSUS
  - Sophos
  - ... ?

## Faltblatt IT-Sicherheit

- richtet sich an Nutzer
- bitte an Ihre Nutzer verteilen,  
jetzt mitnehmen oder bei uns anfordern
- als PDF verfügbar
  - Verschicken per E-Mail
  - Nachdrucken

## Hinweise

- Folien aller Sicherheitstage unter <http://www.rrzn.uni-hannover.de/sicherheitstage.html>
- Workshop kommenden Mittwoch (27.6.) 14–17 Uhr  
Themen: PXE, IPTables
- Sicherheitstage WS 07/08 am 19.–21.11.2007
- „IT-Sicherheit und Administration“ in StudIP