

# Greenbone Appliance am IT Center

Erste Erfahrungen mit einem Schwachstellenscanner

Guido Bunsen

IT Center der RWTH Aachen University

## Greenbone Appliance

### Schwachstellenmanagement

- Wo sind Schwachstellen?
- Welche Schwachstellen?
- Wie kann man sie schließen?

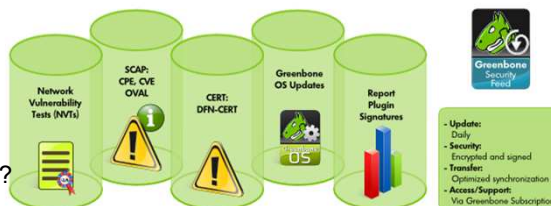


### Basis ist eine DB mit bekannten Schwachstellen

Greenbone Security Feed: Content

### Wir gewinnen Übersicht

- Wo stehen wir?
- Trends?
- Wird es besser? Schlechter?



- Update: Daily
- Security: Encrypted and signed
- Transfer: Optimized synchronization
- Access/Support: Via Greenbone Subscription


2


Oktober / November 2014  
Guido Bunsen | IT Center der RWTH Aachen University

Copyright 2014 Greenbone Networks GmbH, www.greenbone.net

20140421

## Beispiele (Wohnheim)



 Greenbone Security Assistant
Angemeldet als [User] Abmelden  
Tue Nov 25 14:21:47 2014 UTC


Scan-Management
Asset-Management
SecInfo-Management
Konfiguration
Extras
Administration
Hilfe

~ Bericht: Ergebnisse 1 - 100 von 148 (gesamt: 148) GVR PDF

Filter: sort=reverse=severity result\_hosts\_only=1 min\_cvss\_bas

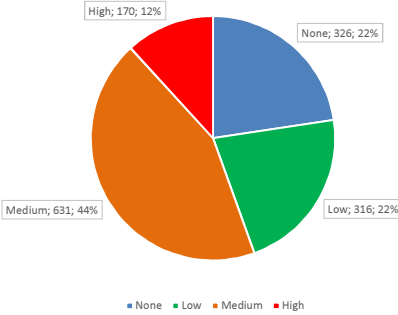
Schwachstelle	Schweregrad	Host	Ort	Aktionen
OpenSSL 'bn_wexpend()' Error Handling Unspecified Vulnerability	10.0 (Hoch)	134.130.180.5	80/tcp	🔍 🗑️
OpenSSL 'bn_wexpend()' Error Handling Unspecified Vulnerability	10.0 (Hoch)	134.130.180.5	443/tcp	🔍 🗑️
Detect talkd server port and protocol version	10.0 (Hoch)	134.130.180.5	518/udp	🔍 🗑️
OpenSSL Cryptographic Message Syntax Memory Corruption Vulnerability	7.5 (Hoch)	134.130.180.5	80/tcp	🔍 🗑️
OpenSSL Cryptographic Message Syntax Memory Corruption Vulnerability	7.5 (Hoch)	134.130.180.5	443/tcp	🔍 🗑️
NTP Stack Buffer Overflow Vulnerability	6.8 (Hoch)	134.130.180.5	123/udp	🔍 🗑️
NTP 'ntpd' Autokey Stack Overflow Vulnerability	6.8 (Hoch)	134.130.180.5	123/udp	🔍 🗑️
OpenSSL CCS Man in the Middle Security Bypass Vulnerability	6.8 (Hoch)	134.130.180.5	443/tcp	🔍 🗑️
OpenSSL CCS Man in the Middle Security Bypass Vulnerability	6.8 (Hoch)	134.130.180.5	10000/tcp	🔍 🗑️
NTP mode 7 MODE_PRIVATE Packet Remote Denial of Service Vulnerability	6.4 (Hoch)	134.130.180.5	123/tcp	🔍 🗑️
Missing Secure Attribute SSL Cookie Information Disclosure Vulnerability	6.4 (Hoch)	134.130.180.6	443/tcp	🔍 🗑️
http TRACE XSS attack	5.8 (Hoch)	134.130.180.5	80/tcp	🔍 🗑️
http TRACE XSS attack	5.8 (Hoch)	134.130.180.5	443/tcp	🔍 🗑️
http TRACE XSS attack	5.8 (Hoch)	134.130.180.5	3128/tcp	🔍 🗑️

## Erste Ergebnisse im Dez. u. Jan.



- **Stichtag 18. Januar:**
  - 2255 IP-Nummern haben eine Freischaltung in der ext. Firewall
  - 1443 lieferten beim Scannen einen Report
  - 170 hatten schwerwiegende Schwachstellen -> Handlungsbedarf
  - 631 hatten mittelschwere Schwachstellen

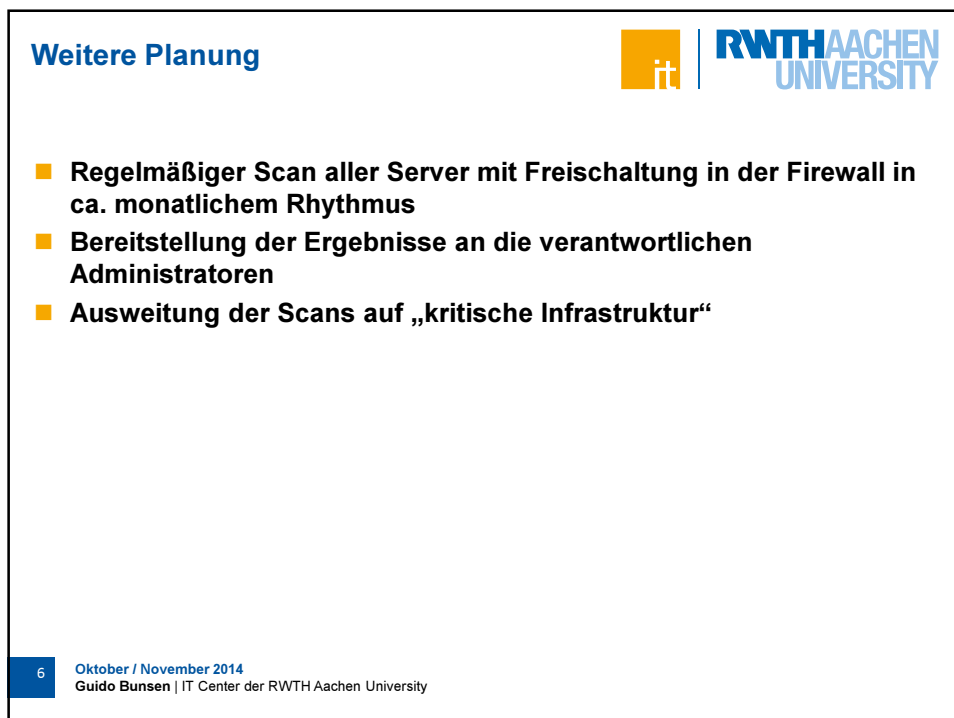
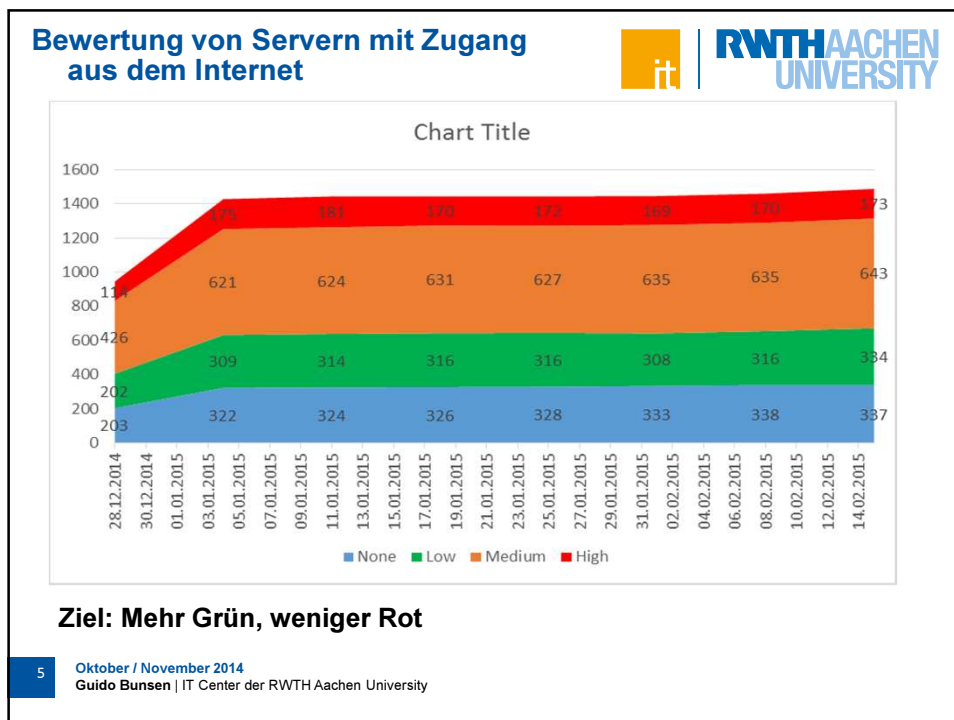
Schweregrad der Schwachstellen



Schweregrad	Anzahl	Prozent
High	170	12%
None	326	22%
Medium	631	44%
Low	316	22%

4
Oktober / November 2014  
Guido Bunsen | IT Center der RWTH Aachen University

■ None
 ■ Low
 ■ Medium
 ■ High



## ■ Fragen?

7

Oktober / November 2014  
Guido Bunsen | IT Center der RWTH Aachen University

## Metrik CVSS

### ■ Berechnung Basis-CVSS

- Verwertbarkeit der Schwachstelle
  - Zugangsvektor (Physikalischer Zugang, Broadcast Domain, Internet)
  - Komplexität in der Ausnutzung (Low, Medium, High)
  - Authentifizierung erforderlich
- Auswirkungen (None, Partial, Complete)
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit

8

Oktober / November 2014  
Guido Bunsen | IT Center der RWTH Aachen University

## Greenbone Appliance




- **Schwachstellenmanagement**
  - Wo sind Schwachstellen? Welche Schwachstellen haben wir? Wie kann man sie schließen?
- **Übersicht**
  - Wo stehen wir? Wird es besser oder schlechter?




9 Oktober / November 2014  
Guido Bunsen | IT Center der RWTH Aachen University

## Mehrwert im Abo...




- **Details über mehr als 40.000 Schwachstellen:**


Greenbone Security Feed: Content




Network Vulnerability Tests (NVTs)




SCAP: CPE, CVE OVAL




CERT: DFN-CERT



Greenbone OS Updates



Report Plugin Signatures



Greenbone Security Feed

- Update: Daily
- Security: Encrypted and signed
- Transfer: Optimized synchronization
- Access/Support: Via Greenbone Subscription

- Common Platform Enumeration (CPE)
- Security Content Automation Protocol (SCAP)
- Common Vulnerabilities and Exposures (CVE)<sup>421</sup>

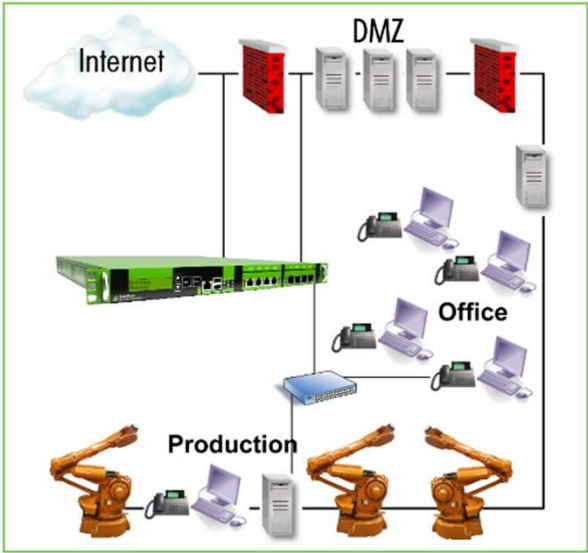
Copyright 2014 Greenbone Networks GmbH, www.greenbone.net

10 Oktober / November 2014  
Guido Bunsen | IT Center der RWTH Aachen University

## Greenbone in der Gesamtarchitektur

it | RWTH AACHEN UNIVERSITY

- **Arbeitsschritte**
  - Portscan
  - Discovery
  - Schwachstellen identifizieren
  - Report erstellen
  - Admin informieren
- **Verschiedene Views bzw. Perspektiven**



The diagram illustrates a network architecture with four main zones: Internet, DMZ, Office, and Production. The Internet zone is represented by a cloud icon. The DMZ zone contains several server racks. The Office zone includes multiple desktop computers and printers. The Production zone features robotic arms and a server rack. A central switch and server rack are connected to all zones, and the Internet zone is connected to the DMZ zone.

11 Oktober / November 2014  
Guido Bunsen | IT Center der RWTH Aachen University

## Konfiguration der Appliance

it | RWTH AACHEN UNIVERSITY

- Leihgabe von TUDD / begrenzte Leistungsfähigkeit / Kein Support
- Bislang Einbindung der Appliance in ein eigenes „Scannernetz“
- Geplant sind „Beinchen“ in verschiedenen Netzen:
  - Vor der Firewall (Sicht des Außentäters)
  - Im unprivilegierten Netz innerhalb der Hochschule (z.B. Eduroam / Sicht des Innetäters)
  - Im NOC-Netz (weitgehend ungehinderter Zugang)
- Bisher erworbene Skills: Scriptgesteuerte Einrichtung von Tests und Scriptgesteuerte Auswertung von Tests
- Erfahrung mit Nutzern in der RWTH war im Okt./Nov. 2014 positiv

12 Oktober / November 2014  
Guido Bunsen | IT Center der RWTH Aachen University

## Einsatzszenarien



### ■ Initialer und dann regelmäßiger Schwachstellenscan für Geräte mit Freigaben in der Firewall

- Verknüpfung mit Changemanagement (Lifecycle von Freigaben)
- Durchführung der Freigaben ev. an Scanergebnis gekoppelt
- Automatische Übermittlung von Schwachstellen an zuständige Admins /  
Verknüpfung mit Ansprechpartnern in Netzdatenbank/Verinice

### ■ Regelmäßiger Discovery-Scan des Hochschulnetzes von „außen“ um die Perspektive eines Angreifers einzunehmen.

- Stimmt die Sicht mit der CMDB überein?

### ■ Regelmäßiger Discovery-Scan von schutzbedürftigen Netzen aus NOC-Perspektive

- Scan nach Geräten, ev. nach Softwarepaketen
- Stimmt die Sicht mit der CMDB überein?

13

Oktober / November 2014  
Guido Bunsen | IT Center der RWTH Aachen University

## Einsatzszenarien 2



### ■ Verknüpfung von Scanergebnissen mit Nagios

- Alarmierung ist etabliert
- Admins kennen und nutzen Nagios

### ■ Verknüpfung mit Verinice

- Informationen über gefundene Schwachstellen und umgesetzte oder nicht umgesetzte Sicherheitsmaßnahmen gebündelt

### ■ Verknüpfung mit Webshop

- Anforderung von Scans...

14

Oktober / November 2014  
Guido Bunsen | IT Center der RWTH Aachen University

## Beispiele 2 (Kawo)

| **RWTH AACHEN UNIVERSITY**

---

Greenbone Security Assistant
Angemeldet als Admin **guido** | Abmelden  
Tue Nov 25 14:23:01 2014 UTC

Scan-Management Asset-Management SecInfo-Management Konfiguration Extras Administration Hilfe

Berichte Refresh alle 60 Sek

Filter: `task_id=65779843-d0bd-4886-8f7f-6a80e78b0f99 apply_c`

Datum	Status	Aufgabe	Schweregrad	Scan-Ergebnisse					Aktionen
				Hoch	Mittel	Niedrig	Log	Falsch Pos.	
Wed Oct 29 21:07:57 2014	Abgeschlossen	H kawo2 Server FnF	10.0 (Hoch)	5	30	3	110	0	⚠️ ✖️
Tue Oct 21 07:05:46 2014	Abgeschlossen	H kawo2 Server FnF	10.0 (Hoch)	5	27	3	109	0	⚠️ ✖️
Mon Oct 20 09:57:41 2014	Abgeschlossen	H kawo2 Server FnF	10.0 (Hoch)	5	24	3	109	0	⚠️ ✖️

(Angewandter Filter: task\_id=65779843-d0bd-4886-8f7f-6a80e78b0f99 apply\_overrides=1 sort=reverse=name first=1 rows=10)

Greenbone Security Assistant (GSA) Copyright 2009-2014 by Greenbone Networks GmbH, www.greenbone.net

15 Oktober / November 2014  
Guido Bunsen | IT Center der RWTH Aachen University

## Beispiele 3 (ZHV)

| **RWTH AACHEN UNIVERSITY**

---

Greenbone Security Assistant
Angemeldet als Admin **guido** | Abmelden  
Tue Nov 25 14:20:27 2014 UTC

Scan-Management Asset-Management SecInfo-Management Konfiguration Extras Administration Hilfe

Berichte Refresh alle 60 Sek

Filter: `task_id=cc8c75ec-1b60-462f-9d87-94af2c2c5587 apply_c`

Datum	Status	Aufgabe	Schweregrad	Scan-Ergebnisse					Aktionen
				Hoch	Mittel	Niedrig	Log	Falsch Pos.	
Thu Nov 13 15:16:57 2014	Abgeschlossen	C ZHV Server	6.4 (Hittel)	0	59	53	1110	0	⚠️ ✖️
Mon Nov 10 13:37:55 2014	Abgeschlossen	C ZHV Server	10.0 (Hoch)	4	69	54	1107	0	⚠️ ✖️

(Angewandter Filter: task\_id=cc8c75ec-1b60-462f-9d87-94af2c2c5587 apply\_overrides=1 sort=reverse=name first=1 rows=10)

Greenbone Security Assistant (GSA) Copyright 2009-2014 by Greenbone Networks GmbH, www.greenbone.net

16 Oktober / November 2014  
Guido Bunsen | IT Center der RWTH Aachen University