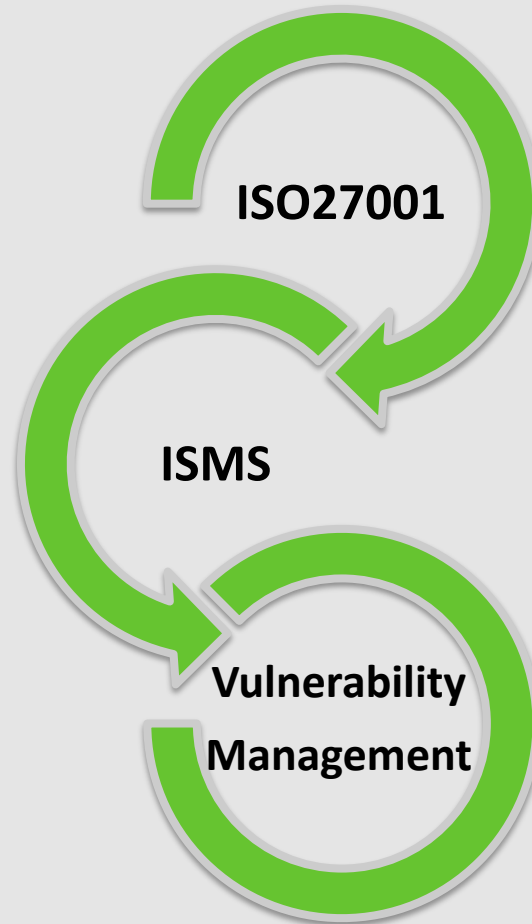




Greenbone
Sustainable Resilience



Kurz über uns/mich

▶ Greenbone Networks GmbH

- ▶ Deutscher Hersteller
- ▶ Produkt seit 2008 am Markt
Turn-key Appliance
- ▶ Entstanden in Zusammenarbeit
mit dem BSI
- ▶ Technologie auch als OpenVAS

▶ Dirk Schrader

- ▶ Chief Marketing Officer
- ▶ Seit 20+ Jahren in der IT-Sicherheit
- ▶ ISO 27001 Practitioner



Leitfaden: Schwachstellen-Management als Teil eines ISMS

▶ Fragen ans Publikum, Einleitung

- ▶ Wer von Ihnen betreibt ein ISMS? Unter diesen, wer nutzt Schwachstellen-Management?
- ▶ Gegenprobe: Wer nutzt ein Tool für Vulnerability Scans? Und wer davon betreibt ein ISMS?
- ▶ Welches Unternehmen ist ISO27001 zertifiziert?
- ▶ Kurze Abgrenzung von Begriffen

▶ Über ISO27001 bzw. ISMS zum Schwachstellen-Management

- ▶ Herleitung
- ▶ Möglicher Umfang

▶ Vom Schwachstellen-Management zum ISMS bzw ISO27001

- ▶ Wieso Schwachstellen-Management: der Blick des ‚Angreifers‘
- ▶ Angriffsflächen für gezielte und breitgestreute Attacken
- ▶ Vulnerability Management Prozess

▶ Randnotizen



VM vs. Pen Testing, Assessment oder Patch Management

- ▶ **Penetration Testing** ist ziel-orientiert; das Ziel ist die Übernahme der Kontrolle der IT-Infrastruktur. Ist das Ziel erreicht, wird nicht weiter nach der nächsten “offenen Tür” gesucht. VM sucht jede “offene Tür”.
- ▶ **Vulnerability Assessment** ist eine einmalige Evaluierung der IT-Infrastruktur, der jeweiligen “security posture”; **Vulnerability Management** ist der vollständige, kontinuierliche Prozess zur Steuerung, Regulierung und Verbesserung dieser Sicherheitslage.
- ▶ **Patch Management** ist ein wichtiger Baustein, doch was ist zuerst da: die Schwachstelle oder der Patch?



ISO27K: ISMS Anforderungen an Vulnerability Management

▶ Exec Summary in der ISO27001/2013

- ▶ In today's interconnected and mobile world, information is processed using systems and networks that employ state-of-the-art technology. It is vital to protect this information against both deliberate and accidental threats and vulnerabilities.

▶ A.12.6 Technical vulnerability management

- ▶ Objective: To prevent exploitation of technical vulnerabilities.

▶ A.12.6.1 – Control

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

▶ ISO27002 und ISO27004

- ▶ ..02 Code of Practice – Implementation Guidance: „... Systems at high risk should be addressed first ..“
- ▶ ..04 Monitoring, Measurement – Effectiveness measures:
„... the greater the number of known vulnerabilities and the longer that they are not addressed (e.g. patched), the greater the probability of their exploitation ..“



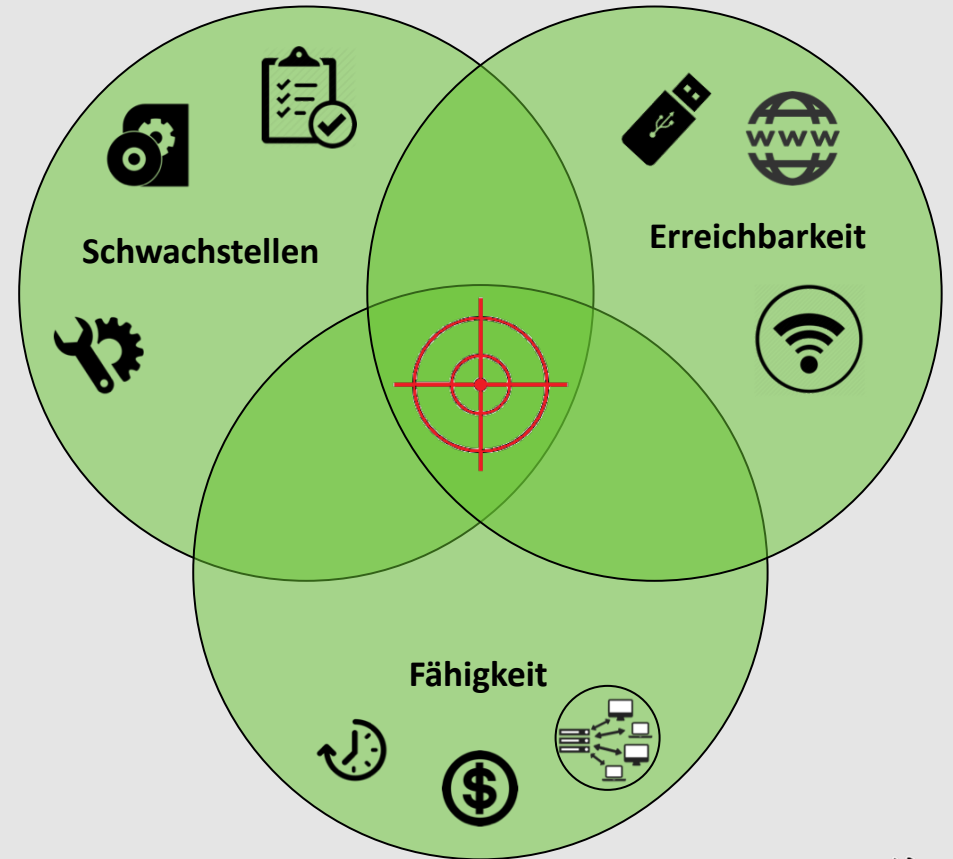
Arten von Schwachstellen für ‚erfolgreiche‘ IT-Angriffe

▶ Schwachstellen können sein:

- ▶ Software Fehler
- ▶ Grundeinstellungen oder fehlerhafte Konfigurationen
- ▶ Nicht genehmigte oder unvermutete Installationen (Systeme, SW, Dienste)
- ▶ Abweichung oder Nicht-Einhaltung von Richtlinien, Vorgaben oder Vorschriften

▶ Dazu braucht es noch:

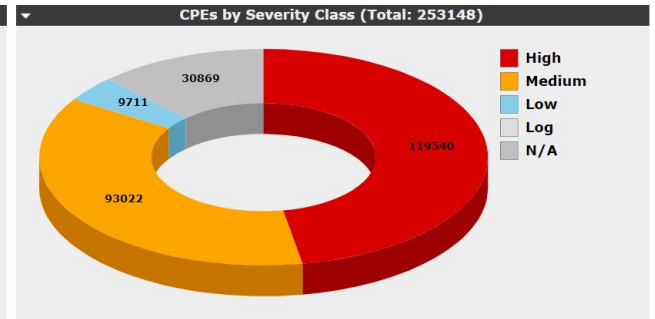
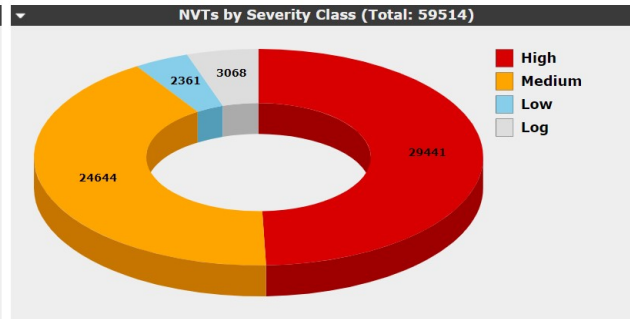
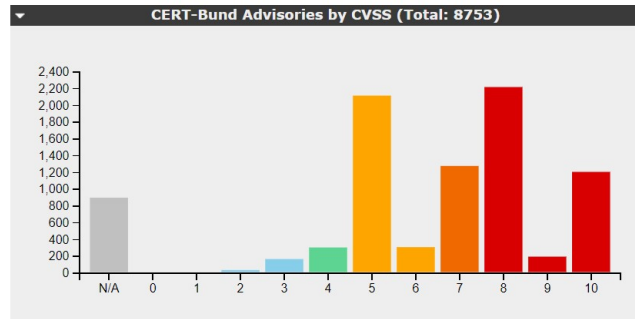
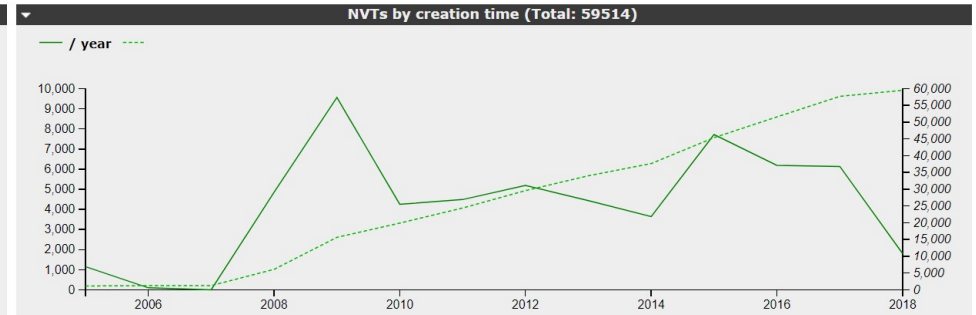
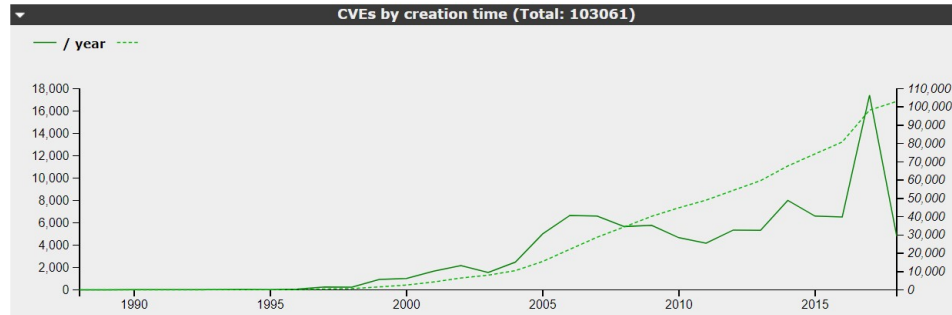
- ▶ Die Erreichbarkeit des Ziels über virtuelle oder physikalische Wege
- ▶ Die Fähigkeit des Angreifers, den Angriff auszuführen



,timely fashion'



SecInfo Dashboard



Backend operation: 0.05s

Greenbone Security Manager (GSA) Copyright 2009-2017 by Greenbone Networks GmbH, www.greenbone.net

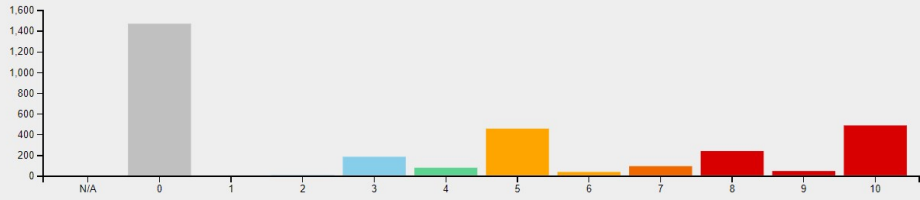


,exposure'

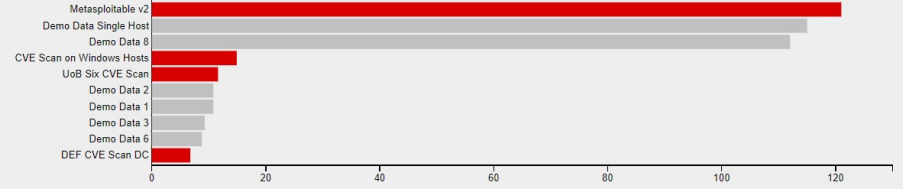


Dashboard

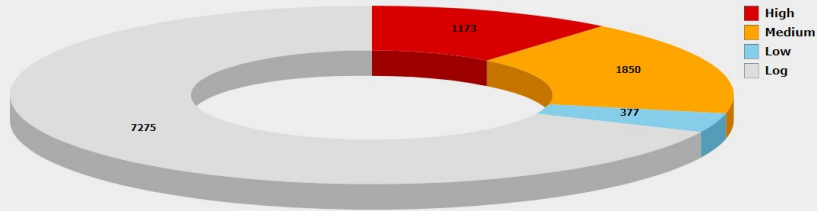
Results by CVSS : Subnets 10. and 172. Results (Total: 3142)



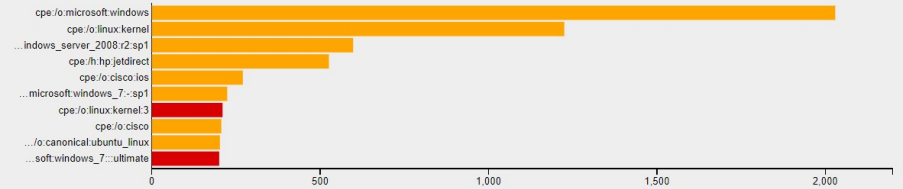
Tasks with most High results per host



Results by Severity Class - New in 2016 - Result (Total: 10675)



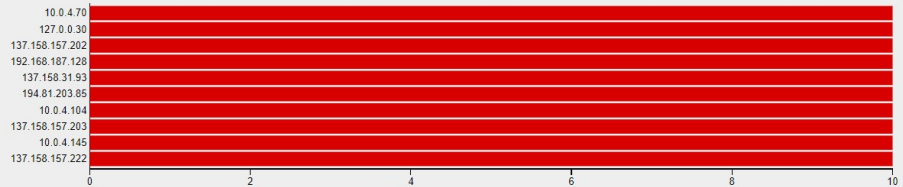
Operating Systems by Vulnerability Score : Severity > 7



Hosts topology : PhyLoc-BO1



Most vulnerable hosts





Scan

Task Name: Demo Data University

Comment: Container Data UK University

Scan Time: Fri, Mar 4, 2016 12:58 PM - Fri, Mar 4, 2016 3:11 PM

Scan Duration: 2:12 h

Hosts scanned: 119

Filter: host=127.0.0.26 min_qod=70 apply_overrides=1 autofp=0

Timezone: Europe/London (UTC)



Results 50 of 3710

Entries per Page 10

Local Search

1 - 10 of 50

Vulnerability	Severity	QoD	Host	Location	Created
VMMSA-2015-0007: VMware ESXi OpenSLP Remote Code Execution (remote check)	10.0 (High)	97 %	127.0.0.26	general/tcp	
Summary VMware vCenter and ESXi updates address critical security issues.					
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.					
Solution Solution Type: <input checked="" type="checkbox"/> Vendorfix Apply the missing patch(es).					
Affected Software/OS VMware ESXi 5.5 without patch ESXi550-201509101 VMware ESXi 5.1 without patch ESXi510-201510101 VMware ESXi 5.0 without patch ESXi500-201510101 VMware vCenter Server 6.0 prior to version 6.0 update 1 VMware vCenter Server 5.5 prior to version 5.5 update 3 VMware vCenter Server 5.1 prior to version 5.1 update u3b VMware vCenter Server 5.0 prior to version 5.0 update u3e					
Vulnerability Insight VMware ESXi OpenSLP Remote Code Execution VMware ESXi contains a double free flaw in OpenSLP's SLPDProcessMessage() function. Exploitation of this issue may allow an unauthenticated attacker to execute code remotely on the ESXi host. VMware vCenter Server JMX RMI Remote Code Execution VMware vCenter Server contains a remotely accessible JMX RMI service that is not securely configured. An unauthenticated remote attacker that is able to connect to the service may be able use it to execute arbitrary code on the vCenter server. VMware vCenter Server void denial-of-service vulnerability VMware vCenter Server does not properly sanitize long heartbeat messages. Exploitation of this issue may allow an unauthenticated attacker to create a denial-of-service condition in the vpxd service.					
Vulnerability Detection Method Check the build number Details: VMMSA-2015-0007_VMware ESXi OpenSLP Remote Code Execution (remote check)_OID: 1.3.6.1.4.1.25623.1.0.105394 Version used: \$Revision: 2748 \$					
References CVE CVE-2015-5177 CVE-2015-2342 CVE-2015-1047					
VMMSA-2013-0014 VMware Workstation, Fusion, ESXi and ESX patches address a guest privilege escalation (remote check)	7.5 (High)	97 %	127.0.0.26	general/tcp	
VMMSA-2013-0003 VMware vCenter Server, ESXi and ESX address an NFC Protocol memory corruption and third party library security issues. (remote check)	7.6 (High)	97 %	127.0.0.26	general/tcp	

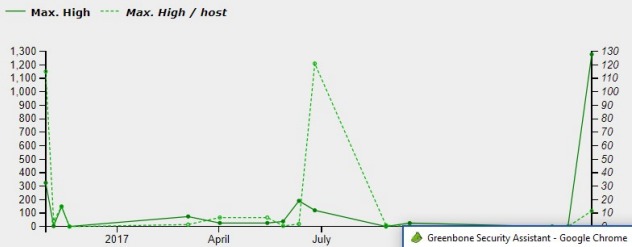


,high risk'

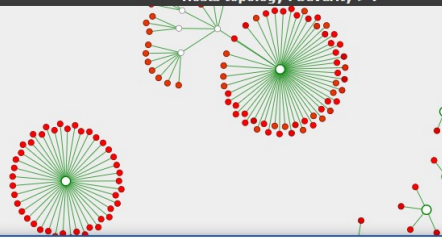


Dashboard

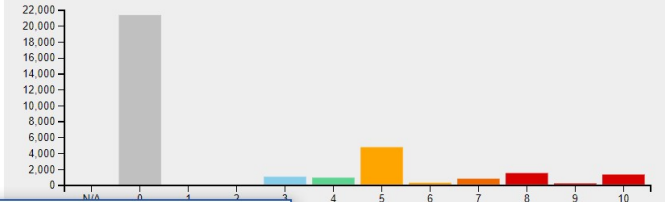
Reports: High results timeline



Hosts topology : Severity > 7



Results by CVSS (Total: 32771)



Backend operation: 0.32s

Greenbone Security Assistant - Google Chrome

Nicht sicher | https://192.168.253.128/omp?cmd=get_assets_chart&asset_type=host&no_filter_history=1&ignore_pagination=1&no_chart_links=0&chart_type=topology&chart_template=&chart_title=Hosts%20topology%20%3A%20...

Hosts topology : Severity > 7 : Severity > 7

Detailed network topology diagram showing hosts with severity > 7. The diagram shows a complex network structure with many nodes (red dots) and connections. The nodes are labeled with IP addresses, such as 192.168.187.113, 192.168.187.134, 63.96.200.193, 137.158.157.216, 137.158.157.215, 137.158.157.214, 137.158.157.213, 137.158.157.212, 137.158.157.211, 137.158.157.210, 137.158.157.209, 137.158.157.208, 137.158.157.207, 137.158.157.206, 137.158.157.205, 137.158.157.204, 137.158.157.203, 137.158.157.202, 137.158.157.201, 137.158.157.200, 137.158.157.199, 137.158.157.198, 137.158.157.197, 137.158.157.196, 137.158.157.195, 137.158.157.194, 137.158.157.193, 137.158.157.192, 137.158.157.191, 137.158.157.190, 137.158.157.189, 137.158.157.188, 137.158.157.187, 137.158.157.186, 137.158.157.185, 137.158.157.184, 137.158.157.183, 137.158.157.182, 137.158.157.181, 137.158.157.180, 137.158.157.179, 137.158.157.178, 137.158.157.177, 137.158.157.176, 137.158.157.175, 137.158.157.174, 137.158.157.173, 137.158.157.172, 137.158.157.171, 137.158.157.170, 137.158.157.169, 137.158.157.168, 137.158.157.167, 137.158.157.166, 137.158.157.165, 137.158.157.164, 137.158.157.163, 137.158.157.162, 137.158.157.161, 137.158.157.160, 137.158.157.159, 137.158.157.158, 137.158.157.157, 137.158.157.156, 137.158.157.155, 137.158.157.154, 137.158.157.153, 137.158.157.152, 137.158.157.151, 137.158.157.150, 137.158.157.149, 137.158.157.148, 137.158.157.147, 137.158.157.146, 137.158.157.145, 137.158.157.144, 137.158.157.143, 137.158.157.142, 137.158.157.141, 137.158.157.140, 137.158.157.139, 137.158.157.138, 137.158.157.137, 137.158.157.136, 137.158.157.135, 137.158.157.134, 137.158.157.133, 137.158.157.132, 137.158.157.131, 137.158.157.130, 137.158.157.129, 137.158.157.128, 137.158.157.127, 137.158.157.126, 137.158.157.125, 137.158.157.124, 137.158.157.123, 137.158.157.122, 137.158.157.121, 137.158.157.120, 137.158.157.119, 137.158.157.118, 137.158.157.117, 137.158.157.116, 137.158.157.115, 137.158.157.114, 137.158.157.113, 137.158.157.112, 137.158.157.111, 137.158.157.110, 137.158.157.109, 137.158.157.108, 137.158.157.107, 137.158.157.106, 137.158.157.105, 137.158.157.104, 137.158.157.103, 137.158.157.102, 137.158.157.101, 137.158.157.100, 137.158.157.99, 137.158.157.98, 137.158.157.97, 137.158.157.96, 137.158.157.95, 137.158.157.94, 137.158.157.93, 137.158.157.92, 137.158.157.91, 137.158.157.90, 137.158.157.89, 137.158.157.88, 137.158.157.87, 137.158.157.86, 137.158.157.85, 137.158.157.84, 137.158.157.83, 137.158.157.82, 137.158.157.81, 137.158.157.80, 137.158.157.79, 137.158.157.78, 137.158.157.77, 137.158.157.76, 137.158.157.75, 137.158.157.74, 137.158.157.73, 137.158.157.72, 137.158.157.71, 137.158.157.70, 137.158.157.69, 137.158.157.68, 137.158.157.67, 137.158.157.66, 137.158.157.65, 137.158.157.64, 137.158.157.63, 137.158.157.62, 137.158.157.61, 137.158.157.60, 137.158.157.59, 137.158.157.58, 137.158.157.57, 137.158.157.56, 137.158.157.55, 137.158.157.54, 137.158.157.53, 137.158.157.52, 137.158.157.51, 137.158.157.50, 137.158.157.49, 137.158.157.48, 137.158.157.47, 137.158.157.46, 137.158.157.45, 137.158.157.44, 137.158.157.43, 137.158.157.42, 137.158.157.41, 137.158.157.40, 137.158.157.39, 137.158.157.38, 137.158.157.37, 137.158.157.36, 137.158.157.35, 137.158.157.34, 137.158.157.33, 137.158.157.32, 137.158.157.31, 137.158.157.30, 137.158.157.29, 137.158.157.28, 137.158.157.27, 137.158.157.26, 137.158.157.25, 137.158.157.24, 137.158.157.23, 137.158.157.22, 137.158.157.21, 137.158.157.20, 137.158.157.19, 137.158.157.18, 137.158.157.17, 137.158.157.16, 137.158.157.15, 137.158.157.14, 137.158.157.13, 137.158.157.12, 137.158.157.11, 137.158.157.10, 137.158.157.9, 137.158.157.8, 137.158.157.7, 137.158.157.6, 137.158.157.5, 137.158.157.4, 137.158.157.3, 137.158.157.2, 137.158.157.1, 137.158.157.0.

Copyright 2009-2017 by Greenbone Networks GmbH, www.greenbone.net



ISMS Reporting

Assets SecInfo Configuration Extras Adr

Filter:
rows=100 first=1 sort=name

New Alert

Name

Comment

Event Task run status changed to
 New NVTs arrived

Condition Always
 Severity at least
 Severity level
 Filter matches at least result(s) NVT(s)
 Filter matches at least result(s) more than previous scan

Report Result
Filter

Method

verinice.PRO URL

Credential *

verinice.PRO Report



Der Blickwinkel des Angreifers

.. von Innen nach Außen

.. von Außen nach Innen

ca. 500 mil Malware Varianten in 4 Jahren

etwa 800 Schwachstellen in den Exploit Kits

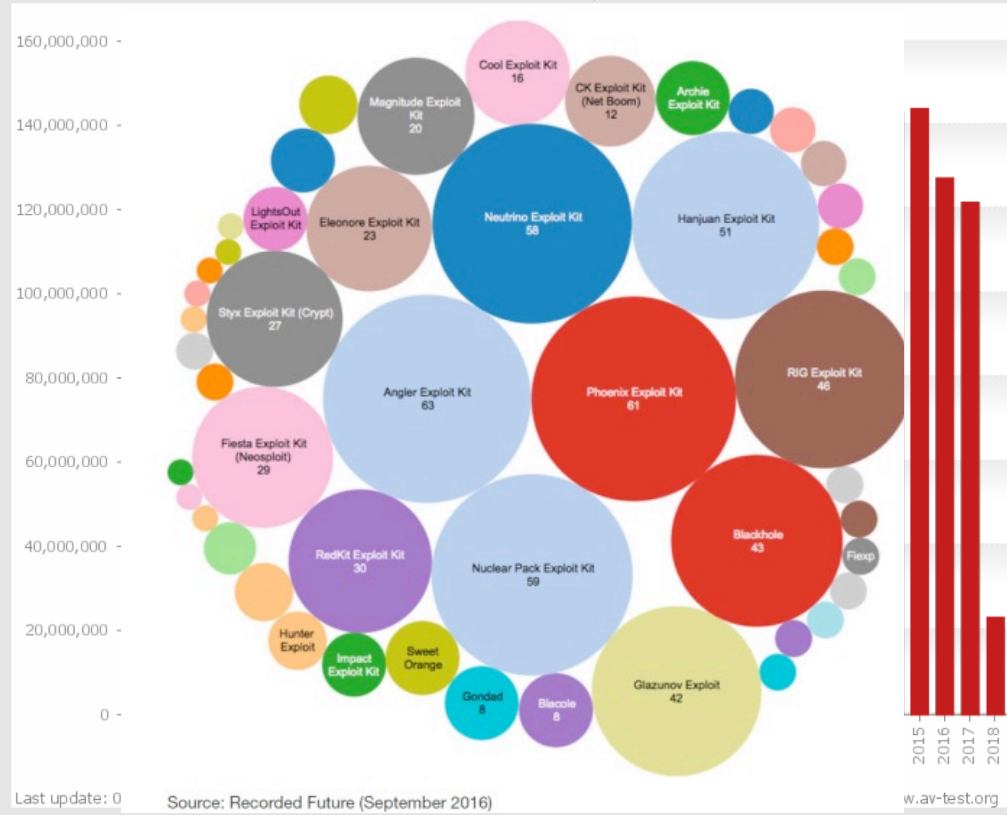
Authentifizierung

NG-FW

N-IDPS

H-IDPS

AV-Systeme



Schwachstellen-Management



Resistent gegen breitgestreute Attacken (Bsp. WannaCry)

Greenbone Security Manager No auto-refresh Logged in as Admin gsm | Logout
Mon Jun 26 15:35:02 2017 Europe

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Filter: ms17-010 [Icons]

sort-reverse=created rows=1000 first=1

NVTs (5 of 54200)

NVTs by Severity Class (Total: 5)

■ High
■ Log

NVTs by creation time (Total: 5)

— NVTs / day — Total NVTs

NVTs by Family (Total: 5)




NVTs by CVSS (Total: 5)

Name	Family	Created	Modified	Version	CVE	Severity	QoD
Double Pulsar Infection Detect	Windows : Microsoft Bulletins	Tue Apr 18 2017	Tue Apr 18 2017	\$Revision: 5972 \$	CVE-2017-0146 CVE-2017-0147	9.3	95%
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	Windows : Microsoft Bulletins	Wed Mar 22 2017	Fri May 26 2017	\$Revision: 6223 \$	CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148	9.3	95%
Microsoft Windows SMB Server Multiple Vulnerabilities (4013389)	Windows : Microsoft Bulletins	Wed Mar 15 2017	Fri May 26 2017	\$Revision: 6225 \$	CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148	9.3	80%
SMBv1 enabled.	Windows	Wed Feb 15 2017	Thu May 18 2017	\$Revision: 6154 \$		0.0	97%
SMBv1 enabled (Remote Check)	Windows	Sat Feb 4 2017	Thu May 18 2017	\$Revision: 6154 \$		0.0	80%

(Applied filter: ms17-010 sort-reverse=created rows=1000 first=1)





Side step: Cyber Crime Umsätze


rtseite  Mitteilungen  Nachrichten  Twitter durchsuche





actual ransom
[@actual_ransom](#)


Tweets **437** Follower **6.618**

 **actual ransom** @actual_ransom · 3. Aug. 2017 ⌵


 7.34128314 BTC (\$20,055.52 USD) has just been withdrawn from a bitcoin wallet tied to #wcry ransomware. [blockchain.info/address/115p7U...](#)





 Original (Englisch) übersetzen


 7  66  38 

 **actual ransom** @actual_ransom · 3. Aug. 2017 ⌵

Status of WannaCry wallets:
52.19666422 BTC (\$142,361.51)
338 payments, 0 withdraws
Last payment:
2017-07-24 at 10:07 AM ET

 Original (Englisch) übersetzen

  6  3 

 **actual ransom** @actual_ransom · 2. Aug. 2017 ⌵



SCA gegen gezielte Angriffe

Edit Scan Config NVT

Name: Windows Registry Check
Config: Full and fast Clone 1
Family: Policy
OID: 1.3.6.1.4.1.25623.1.0.105988
Version: \$Revision: 4928 \$
Notes: 0
Overrides: 0

Summary

Checks the presens of specified Registry keys and values.

Vulnerability Scoring

CVSS base: **0.0**
CVSS base vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Preferences

Name	New Value	Default Value	Actions
Timeout	<input checked="" type="radio"/> Apply default timeout <input type="radio"/> <input type="text"/>		
Policy registry file	<input type="checkbox"/> Upload file: <input type="button" value="Choose file"/> No file chosen		

- ▶ Definierte sichere Konfiguration, regelmäßig überprüft
- ▶ Prüfen der kryptographischen Verfahren (MITM)
- ▶ Verifikation der Infrastruktur nach Compliance Richtlinien (zB. IT-Grundschutz)



Schwachstellen-Management



Widerstandsfähigkeit erhöhen, Angriffsfläche verkleinern

prepare



prepare

- Festlegen der Ziele zur eigenen IT-Sicherheit
- Was darf sein / was nicht
- Verknüpfen mit technischen Kontrollen

identify



identify, classify, prioritize

- Welcher Fund muss zuerst bearbeitet werden
- Welcher hat die größte Wirkung

classify



prioritize



assign, mitigate & remediate

- Die richtige Person nimmt die notwendigen Veränderungen vor, hat dabei alle notwendigen Informationen zur Verfügung

assign



mitigate & remediate



store & repeat



store & repeat, improve

- Automatisierte, zeitgesteuerte Abläufe
- Darstellbare Verbesserung der IT-Sicherheit; Erweiterung und Ergänzung der Zielsetzung

improve





IT-Sicherheit als Prozess und die DSGVO

Präventive Anforderungen

- ▶ **Artikel 32**
Sicherheit der Verarbeitung
 - ▶ „[...] regelmäßige[n] Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen [...]“
- ▶ **Artikel 35**
Datenschutz-Folgeabschätzung
 - ▶ „[...] insbesondere bei Verwendung neuer Technologien[...]“
- ▶ **Artikel 36**
Vorherige Konsultation
 - ▶ „[...] die Verarbeitung [...] ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.“

Reaktive Anforderungen

- ▶ **Artikel 33**
Meldung [...] an die Aufsichtsbehörde
 - ▶ „[...] unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde [...]“
 - ▶ „Erfolgt die Meldung [...] nicht binnen 72 Stunden, [...] ist eine Begründung [...] beizufügen“
- ▶ **Artikel 34**
Benachrichtigung der [...] betroffenen Person
 - ▶ „[...] benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.“





Greenbone
Sustainable Resilience

*Vielen Dank!
Ihre Fragen?*

dirk.schrader@greenbone.net



Greenbone
Sustainable Resilience

Effektivität und Effizienz mit VM

- prepare 
- identify 
- classify 
- prioritize 
- assign 
- mitigate & remediate 
- store & repeat 
- improve 

500 Systeme	ohne	mit
identify	41 h	4 h
classify	5 h	20 min
prioritize	30 min	10 min
assign	3 h	30 min
Erster Durchlauf	50 h	5 h
store&repeat (zyklisch)	24 h	2 h



Einfluss auf das IT-Sec Betriebskonzept

- ▶ **Risk Assessment bzw. Risk Register**
 - ▶ Umfasst nicht mehr nur Geschäftsrisiken, sondern ebenso Datenschutzrisiken
- ▶ **Vorhersage und Vermeidung**
 - ▶ Wo könnte angegriffen werden und wie kann ein solcher Angriff entschärft bzw. unterbunden werden
 - ▶ Ist IT-Sec frühzeitig in neue Abläufe eingebunden, die relevant sind
- ▶ **Erkennung und Meldung**
 - ▶ Zugriff auf Geschäftsgeheimnisse zu kontrollieren reicht nicht mehr
 - ▶ Wie lässt sich ein Verlust von personen-bezogenen Daten zeitnah erkennen und melden

