

Kassel Codemeetup 13.07.2016 Schwachstellenmanagement

Sebastian Brabetz,
Teamleiter Professional Security Solutions
mod IT GmbH

Bevor es losgeht:

3. IT Security Meetup nächste Woche Mittwoch (20.07)
bei Micromata!

<http://www.meetup.com/de-DE/IT-Security-Kassel-und-Nordhessen/>

Kurz: <http://bit.ly/29Cn0Bj>

Vorträge:

1. Data URI Firefox Schwachstelle
2. Zed Attack Proxy
3. WiFi Pineapple
4. PWs Cracken in der Cloud

- Vorstellung
- Unterschied Pentest <-> Schwachstellenscan
- 3 Kategorien von Schwachstellen
- Was ist Patchmanagement
- Was ist Schwachstellenmanagement
- Vulnerability Management Maturity Curve
- Schwachstellenmgmt-(„Best“)-Practices

Vorstellung Sebastian Brabetz

30 Jahre alt

Seit August 2014 bei mod IT

Vorher bei produzierenden Unternehmen in Kassel:

Ausbildung -> Firewall Admin -> Security Admin

Schwachstellenscans, Schwachstellenmgmt, Pentests

OSCP+TCSE (wer kennt OSCP?)

Community:

- Kassel Codemeetup (Vorträge)
- Metasploit Workshops
- uvm.: siehe <https://itunsecurity.wordpress.com>



Disclaimer: Nessus+Security Center Fanboy!

Ziel dieses Vortrags / „Die Message“

Nicht hier um etwas zu verkaufen!

Schwachstellenmanagement ist in Europa noch nicht annähernd so etabliert wie in den USA. Das können wir ändern!

Meine Sichtweise auf Definitionen und Begrifflichkeiten teilen!

Meine Herangehensweise an das Thema Schwachstellenmanagement teilen!

Andere Sichtweisen und Herangehensweisen sind natürlich willkommen!

Usergroup und Community stärken!

Mit gleichgesinnten über das Thema sprechen, neue Sichtweisen vermitteln und (noch viel wichtiger) neue Sichtweisen vermittelt bekommen!

3 Arten von Schwachstellen: 1. Software Schwachstellen

CVE-2016-2118



POODLE Badlock
ASPA-1601
getaddrinfo MS08-067 0Day
Sandworm/MS14-060 Heartbleed
MS14-068 Flashplayer
Shellshock GHOST
glibc

3 Arten von Schwachstellen: 2. Unsichere Konfigurationen

Dateifreigaben auf sensitive Daten
Ganze Festplatten freigegeben
Öffentlich lesbare Webseitenbackups
Uvm!....

Info

Beispiele:

Plugin 72771 – Web Accessible Backups (Info)
Plugin 10437 – NFS Share Export List (Info)
Plugin 11032 – Web Server Directory Enumeration (Info)
Plugin 53513 – Link-Local Multicast Name Resolution (LLMNR) Detection (Info)

3 Arten von Schwachstellen: 3. Keine-/ Standard-/ Unsichere Passwörter

(Info, Critical, High,)



Beispiele:

Plugin 26925 – VNC Server Unauthenticated Access (High)

Plugin 80101 – IPMI (*iLO, iDrac, uvm...) v2.0 Password Hash Disclosure (High)

Plugin 11245 – Unpassworded ‘root’ Account (Critical)

(Filter Pluginname: „unrpvi“, „default“, „unauth“)

Manches auch nicht unbedingt mit Nessus auffindbar oder nur indirekt über informative Nessus Plugins:

Bsp.: Domänenadmin Kennwort 5 Zeichen und in einer phpmyadmin Instanz gefunden
gpp-Encrypted Local Admin Passwort auf Sysvol

Password Re-Use, uvm...

Was ist Patchmanagement?

Was ist Patchmanagement?

- Betriebssystem Patch-Infrastruktur (WSUS, Linux Update Repositories)
- 3rd Party Applikation Patch-Infrastruktur (Secunia PSI+CSI, Empirum, Aptitude*)
- Management ist mehr als Software!
- Prozesse + Kennzahlen
- Testgruppen + Testuser
- Messen von Effektivität

Magic Quadrant

Figure 1. Magic Quadrant for Client Management Tools



- Patchmanagement ist Fundament!
- Sind alle Systeme im Patchmanagement?
- Verteidiger haben viele Lücken zu schließen!
- Angreifer brauchen nur eine/wenige Lücken!
- Schwachstellenmanagement ist der Spiegel zum Patchmanagement

Begrifflichkeiten: Schwachstellenscan vs. Penetrationstests

Schwachstellenmanagement in Deutschland noch nicht wirklich überall etabliert.

Pentests deutlich geläufiger.

Kunden fragen häufig aktiv nach Pentests, selten nach Schwachstellenmanagement.

BSI Studie „Durchführungskonzept für Penetrationstests“ aus Jahr 2003!

Begrifflichkeiten: Schwachstellenscan vs. Penetrationstests

Penetrationstests:

Sehr spezialisiert und tiefgehend.

Kleine Anzahl von Systemen + Tiefgang

Unrealistisch 500 Server und 1000+ Clients intensiv zu prüfen

Was findet der Pentester in Unternehmen ohne Schwachstellenmanagement?

Schwachstellenscans:

Sollten am besten alles erfassen!

Einzelaudits einmal im Jahr (Sinnvoll?!)

Besser: Scans automatisch und sollten möglichst häufig laufen!

Begrifflichkeiten: Schwachstellenscan vs. Penetrationstests

Häufige Realität bei Pentests: Domänenadmin nach 0,5 – 1,5 Tagen

Pentests haben natürlich auch ihren Platz!

Firmen sollten aber zuerst Schwachstellenmanagement beherrschen

Pentester sollen dann für ihr Geld auch wirklich arbeiten und nicht nur „Low Hanging Fruits“ sammeln!

Mehr dazu gleich in der Vulnerability Maturity Curve!

Schwachstellenscan vs. Schwachstellenmanagement

Einzelner Schwachstellenscan:

- Momentaufnahme der Umgebung und in ihr gefundener Schwachstellen
- Hilft Schwachstellen zu Identifizieren und gibt Informationen zum Schließen
- Daten sind schnell veraltet, da:
 - Schwachstellen und Patches nahezu täglich veröffentlicht werden
 - Serversysteme kontinuierlich angepasst werden (Virtualisierung!)
 - Clientsysteme kontinuierlich angepasst und neuinstalliert werden

Schwachstellenscan vs. Schwachstellenmanagement

Schwachstellenmanagement beinhaltet neben dem Scannen auch den kompletten Prozess um das Scannen herum:

Schwachstellenmanagement sollte sicherstellen:

- Das Schwachstellen auch zuverlässig an Zuständige verteilt und von den Zuständigen zuverlässig geschlossen werden (**kontinuierlicher Überblick, Reporting**)
- Trend in der Sicherheit / Qualität des Unternehmens wiederspiegeln
- Kennzahlen einfach erheben und kommunizieren (**KPIs, Reports, Dashboards**)

Technik macht nur ca. 30% (?) vom Schwachstellenmanagement aus!

Mit Tenable Produkten ist die Technik gefühlt das Einfachste am Schwachstellenmanagement!

Die restlichen 70% sind: Prozesse, Menschen, Politik, Operative „Zwänge“, uvm...

Vulnerabilitymanagement Maturity Curve:
Zuerst vielen Dank an Security Weekly Podcast!

<http://securityweekly.com>

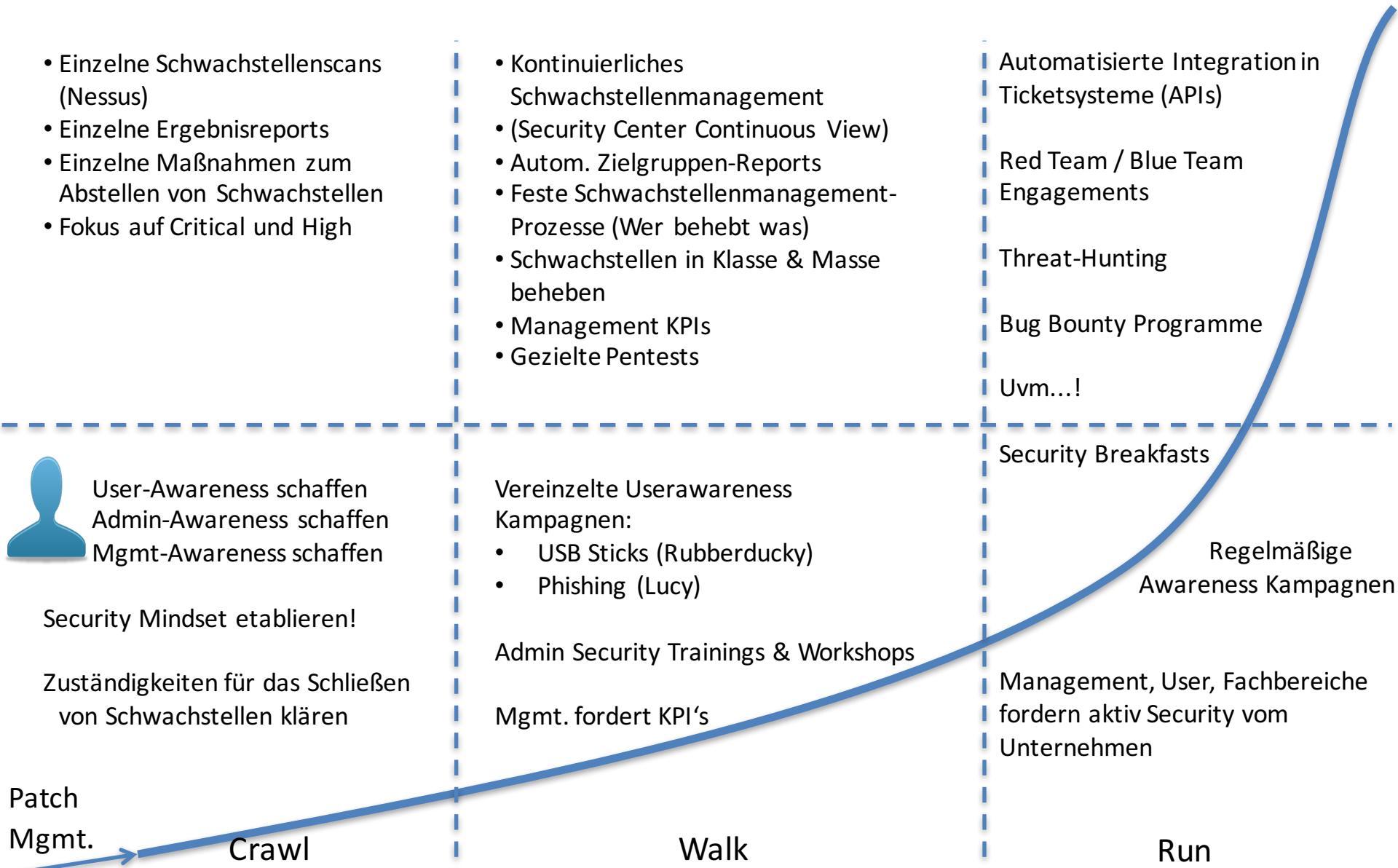


Vulnerabilit
Zuerst viele

<http://security>

**BUT WHEN I DO I WATCH
SECURITY WEEKLY!**

Vulnerabilitymanagement Maturity Curve (my take on it...)



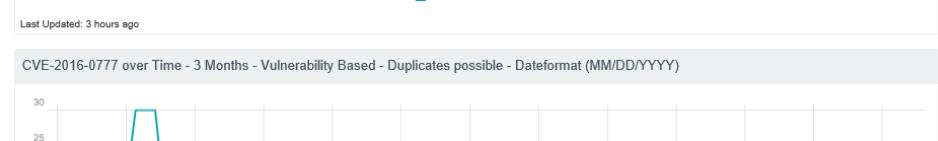
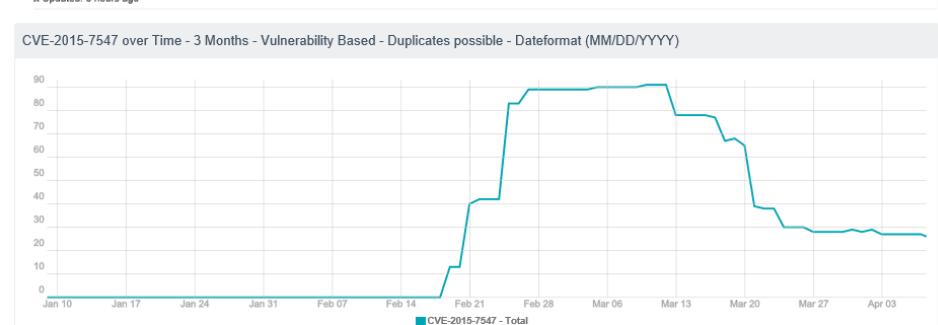
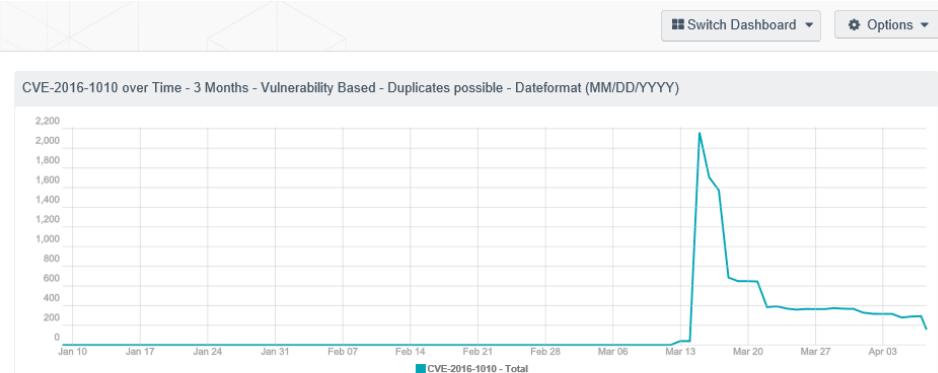
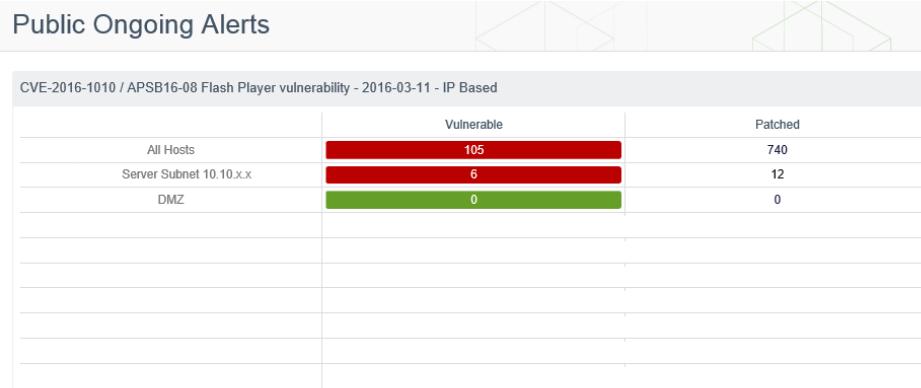
Best Practices:

- Fokussierung auf Klasse (Kritikalität)
- Fokussierung auf Masse (Anzahl betroffene Systeme)
- Tracken von Software-Versionen (speziell veraltete & out-of-support)
- Unautorisierte Zugriffe minimieren
- Zielgruppengerechte und „Handelbare“-Reports
- Security Relevante Alarne aus Schwachstellenscan Ergebnissen
- Schwachstellenmanagement Prozesse im Alltag

Best Practices: Fokussierung auf Klasse (Kritikalität)

Kritische Schwachstellen systematisch überwachen und ausdünnen....

Public Ongoing Alerts



Best Practices: Fokussierung auf Klasse (Kritikalität)

....auch auf Dauer nachdem sie einmal eliminiert wurden! (MS08-067 anyone?)

Consolidated Vulnerabilities 1/2		
	Vulnerable	Patched
Heartbleed	0	7
Shellshock	0	2
GHOST	2	7
APSB15-16 (Flash)	0	22
MS08-067	0	3
MS14-064, -066, -068	4	53
eDell Root CA	0	5

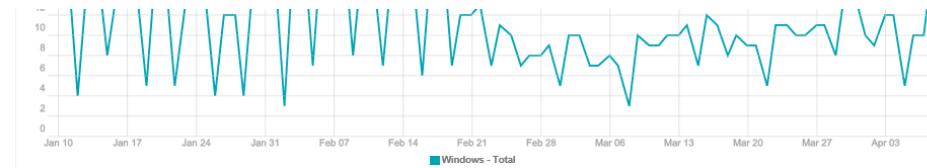
Last Updated: 9 hours ago

Consolidated Vulnerabilities 2/2		
	Vulnerable	Patched
N.N.		
-		
-		
-		
-		
-		
-		
-		

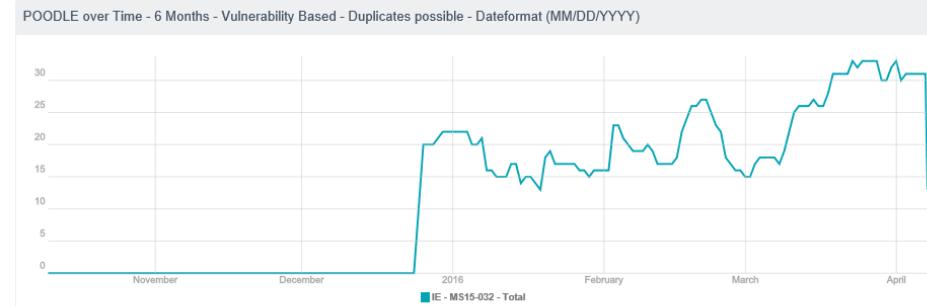
Last Updated: 1 hour ago

Blindspot - No Credentialed Scans - Approved Exceptions already filtered - IP Based					
	# of Systems w/o Login	# smb protocol error	# Systems with Login	# Systems Exception	# RedLabel
All Linux	71		111	83	1
All Windows	301		136	2136	5
Subsidiaries Linux (1...	25			2	
Subsidiaries Window...	214		119	1047	
Linux	0			86	1
Win...	1		3	35	
Domain Controllers (v...	9		10	0	

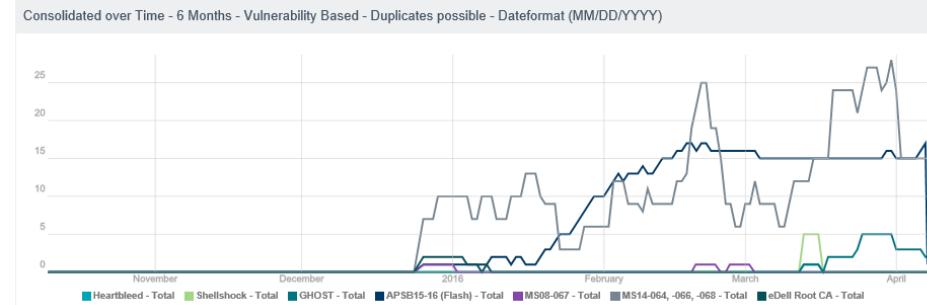
Last Updated: 9 hours ago



Last Updated: 9 hours ago



Last Updated: 6 hours ago



Best Practices: Fokussierung auf Masse

Security Center Auswertung nach Kritikalität und Anzahl

Vulnerability Analysis

Jump to Vulnerability Detail List
Total Results: 809

Plugin ID	Name	Family	Severity	Total
87253	MS15-124: Cumulative Security Update for Internet Explorer (3116180)	Windows : Microsoft...	High	2109
48762	MS KB2269637: Insecure Library Loading Could Allow Remote Code Execution	Windows	High	1949
88955	Microsoft EMET < 5.5 Security Bypass Vulnerability	Windows	High	1610
89875	Firefox < 45 Multiple Vulnerabilities	Windows	High	1050
61487	IBM Lotus Notes < 8.5.3 FP2 URL Handler Unspecified Remote Code Execution	Windows	High	349
70744	IBM Notes 8.5.x < 8.5.3 FP5 Multiple Vulnerabilities	Windows	High	349
66944	IBM Notes PNG Integer Overflow	Windows	High	348
63281	IBM Lotus Notes 8.5.1 / 8.5.2 / 8.5.3 < 8.5.3 FP3 Multiple Vulnerabilities	Windows	High	347
89830	Adobe Acrobat < 11.0.15 / 15.006.30121 / 15.010.20060 Multiple Vulnerabilities (APSB16-09)	Windows	High	255

Filters

- Patch Published: More than 30 days ago
- Severity: High
- Address: All
- Asset: All
- Plugin Name:
 - Select Filters
 - Clear Filters
 - Load Query

Best Practices: Software Versionen im Blick behalten

Aus dem Support laufende Schwachstellen systematisch von hinten aufräumen!

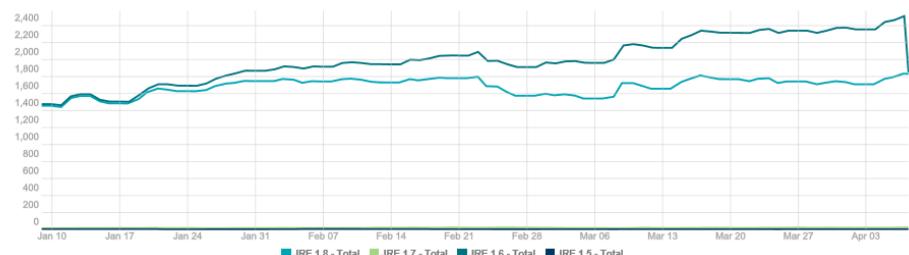
Software Tracking

Java - Multiple Java Versions on Same Machine Possible

JRE 1.8	1831
JRE 1.7	23
JRE 1.6	12
JRE 1.5	3
JRE 1.4	0
Java Vulns 2016 (older 90 days)	0
Java Vulns 2015	95
Java Vulns 2014	39
Java Vulns 2013	16
Java Vulns <= 2012	11

Last Updated: 23 minutes ago

JAVA - 90 days



Last Updated: 6 hours ago

Internet Explorer Versions

Internet Explorer 11	2134
Internet Explorer 10	42
Internet Explorer 9	44
Internet Explorer 8	11
Internet Explorer 7	1
Internet Explorer 6	0

Last Updated: 23 hours ago

Unsupported Internet Explorer - 90 days



Last Updated: 6 hours ago

Webserver Tracking - 90 days



Best Practices: Unautorisierte Zugriffe minimieren

Unpriv. Access

Default Credentials				
Plugin ID	Name	Family	Severity	Total
10264	SNMP Agent Default Community Names	SNMP	Critical	16
41028	SNMP Agent Default Community Name (public)	SNMP	High	170
32315	Firebird Default Credentials	Databases	High	2
25927	Sybase ASA Default Database Password	Databases	High	1
10483	PostgreSQL Default Unpassworded Account	Databases	High	1
12085	Apache Tomcat servlet/JSP container default files	Web Servers	Medium	2
11422	Web Server Unconfigured - Default Install Page Present	Web Servers	Info	143

Unauth. Access				
Plugin ID	Name	Family	Severity	Total
25124	Sun Java Web Start Unauthorized Access (102881)	Wind...	High	2
26925	VNC Server Unauthenticated Access	Misc.	High	2
51368	iSCSI Unauthenticated Target Detection	Misc.	High	2
64568	IBM Tivoli Storage Manager Client 6.3 < 6.3.1.0 / 6.4 < 6.4.0.1 Unauthorized Access	Wind...	Medium	86
81492	Tivoli Storage Manager Server Unauthorized Access Vulnerability	Misc.	Medium	2

Best Practices: Reports

Security Center Reports:

- Zielgruppengerecht
- Klare Anweisungen
- Klare Zielvorgaben
- Reports sollten klare Handlungen vorschreiben

SecurityCenter™

Weekly Location Vuln. Report

April 24, 2016 at 6:38am EDT

Sebastian Brabetz [brabetz]
ORG

Best Practices: Reports

About - PLEASE READ THIS!

---- DISCLAIMER ----

Confidential: The following report contains confidential information. Do not distribute, email, fax, or transfer via any electronic mechanism unless it has been approved by the recipient company's security policy. All copies and backups of this document should be saved on protected storage at all times. Do not share any of the information contained within this report with anyone unless they are authorized to view the information. Violating any of the previous instructions is grounds for termination.

---- FILTERING EXPLANATION ----

All elements of this Report will be filtered to only show Medium, High and Critical Vulnerabilities. Also it will only show vulnerabilities for which a patch exists for more than 30 days and that have been observed actively in within the last 30 days. All newer vulnerabilities are expected to be patched through the regular monthly patch windows.

---- QUESTIONS? CONTACT: ----

If you have any questions or suggestions regarding this report feel free to contact Sebastian Brabetz (mod IT) at any time! Your support is greatly appreciated!

WSUS

[Task] Please apply the missing Windows Updates listed below

[Info] If you see systems in the blow Table that do not show any pending Updates in the Control Panel and that have been rebooted since last updates please raise a ticket with mod IT Support containing the detailed Informations (Attach this Security Report and a Screenshot of the WSUS Dialogue showing no pending updates and no missing reboot)

Missing Windows Updates by System

IP Address	NetBIOS Name	DNS Name	Score	Low	Med.	High	Crit.	Total	Vulns
192.168.0.210	WORKGROUP\HOMESERVER	homeserver.fritz.box	10	0	0	1	0	1	1

Missing Windows Updates by Updates

MS Bulletin	Severity	Total
MS15-124	High	1

Overview

[Task] if you see Systems with High and Critical vulnerabilities please log into Security Center and drill down to review the vulnerabilities and how to mitigate them. Please Note that this Table does _not_ only represent Windows Updates but other Vulnerabilities as well! (missing 3rd Party Updates or Configuration Issues)

[Task] Please close all Critical Vulnerabilities immediately and then proceed with high vulnerabilities (Critical First, then High)

Top Ten Threatened Systems - sorted by Score

IP Address	NetBIOS Name	DNS Name	MAC Address	Score	Med.	High	Crit.
192.168.0.79				1004	8	70	7
192.168.0.88				587	9	44	3
192.168.0.37				320	10	21	2
192.168.0.87				317	9	21	2
192.168.0.210	WORKGROUP\HOMESERVER	homeserver.fritz.box	68:b5:99:72:d5:27	56	2	5	0
192.168.0.2				13	1	1	0
192.168.0.72				3	1	0	0
192.168.0.254			a0:f3:c1:5e:ae:64	3	1	0	0

Incompletely Tested Systems

[Task] please check the following systems and make sure that the "domain\nessus" user is part of the local administrators group.

invalid credentials

IP Address	NetBIOS Name	DNS Name	MAC Address
192.168.170.6	WORKGROUP\MFPP-07201268		00:80:91:6d:e1:f4

non sufficient privileges

IP Address	NetBIOS Name	DNS Name	MAC Address

Best Practices: Security Relevante Alarme

Alarming auf Backdoors (Plugin Family):

General

Name* Alerting Backdoors

Description

Schedule Every 30 minutes 

Behavior Perform actions only on first trigger

Condition

Type Vulnerability

Trigger* IP Count ≥ 1

Query Select a Query

Filters

Plugin Family	Backdoors
Severity	Critical, High

+ Add Filter

Best Practices: Security Relevante Alarme

Alarming auf Proxy Anzahl (Rouge Proxy detection, Informatives Plugin):

General

Name*

Description

Schedule 

Behavior

Condition

Type

Trigger*

Query

Filters

Plugin ID

 [+ Add Filter](#)

Best Practices: Schwachstellenmanagement Prozesse im Alltag

Regelmäßig (z.B. wöchentlich):

- Durchgehen der etablierten Dashboards
- Neue Schwachstellen aus den Medien/Findings/sonstige Quellen aufnehmen
- Maßnahmen zur weiteren Reduktion ableiten und auf den Weg bringen:
 - Tickets erstellen
 - Verantwortliche anschreiben
 - Reports nachjustieren

Zusätzlich:

- Immer mal wieder eine Auszeit nehmen und kreativ auf die Schwachstellen-Datenbank schauen (Drilldowns im Security Center)
- Was rutscht noch durch die Dashboards durch?

→ Schwachstellenmanagement ist ein Endlosspiel!
→ KPIs niedrig halten ist „das Ziel“! (ein Ziel?)

Live Demo Nessus

(Wenn noch Zeit ist)

VULNERABILITY MANAGEMENT?

Vielen Dank für Ihre
Aufmerksamkeit!



Sebastian Brabetz
Teamleiter PSS
Telefon 0 55 61/922-397
s.brabetz@it-mod.de

mod IT GmbH
Grimsehlstraße 23
37574 Einbeck

© 2016 mod IT GmbH. Alle Rechte vorbehalten.