

Task: IT-Grundschutz

Inhalt

- [Prüfung IT-Grundschutz, 11. Ergänzungslieferung](#)
- [Übernahme der Ergebnisse in eine Tabellenkalkulation](#)
- [Übernahme der Ergebnisse in IT-Grundschutz Tools](#)
- [Ergebnis-Klassen der IT-Grundschutz Prüfung](#)
- [Unterstützte Maßnahmen](#)

Einleitung

Über den [Greenbone Security Manager](#) können automatische Prüfungen zu den IT-Grundschutz-Katalogen des [Bundesamt für Sicherheit in der Informationstechnik](#) (BSI) ausgeführt werden.

Unterstützt wird die aktuelle 11. Ergänzungslieferung mit Prüfungen für derzeit 102 Maßnahmen. Das ist die maximale Zahl von Maßnahmen die sich überhaupt mit automatischen Test unterstützen lassen.

Einige Maßnahmen sind recht umfangreich, so dass weitaus mehr als 100 Einzeltests pro System ausgeführt werden. Die Anzahl der geprüften Systeme spielt für den Greenbone Security Manager dabei keine Rolle.

Damit wird der Greenbone Security Manager zum schnellen Mitarbeiter bei der Durchführung eines IT-Grundschutz Audits und erlaubt überhaupt erst eine automatische Prüfung auf Verstöße als regelmäßiger Vorgang im Hintergrund.

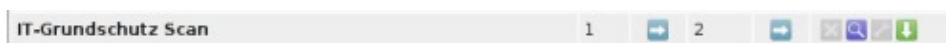
Prüfung IT-Grundschutz, 11. Ergänzungslieferung

Dieses Beispiel führt eine einfache Prüfung gemäß der 11. Ergänzungslieferung der IT-Grundschutz-Kataloge durch.

1. Importieren Sie die Scan Configuration [IT-Grundschutz Scan](#).



Sie beinhaltet die Einstellungen um sämtliche Prüfungen auszuführen. Die eigentlichen Prüfungen sind nicht direkt einzeln ausgewählt sondern es wird ein Gesamtergebnis erstellt.





2. Der größte Teil der Maßnahmenprüfungen basiert auf lokalen Sicherheitstests. Dafür muss ein entsprechender Zugang konfiguriert werden. Falls noch nicht geschehen, erstellen Sie dafür einen

entsprechenden Anwender auf den Zielsystemen (je höher das Benutzer-Konto privilegiert ist, desto mehr Maßnahmen können geprüft werden).

- Legen Sie die Zielsysteme (Targets) fest und verknüpfen Sie sie ggf. mit den eben erstellten Credentials.

- Nun können Sie die Aufgabe (Task) erstellen. Dafür kombinieren Sie die oben importierte Scan Configuration mit den entsprechend erstellten Zielsystemen.

- Die Prüfung wird gestartet indem Sie für den eben erstellten Task auf  klicken. Es kann einige Zeit dauern, bis der Scan abgeschlossen ist. Den aktuellen Stand des Scans erhalten Sie indem Sie auf  klicken.

Report	Threat	Scan Results				Download	Actions
		High	Medium	Low	Log		
Tue Mar 2 09:54:58 2010 Done	Low	0	0	4	8	PDF Download	

- Sobald der Status auf "Done" wechselt, ist der vollständige Bericht verfügbar. Sie können aber auch schon während des Scans die bereits gefundenen Ergebnisse einsehen. **Beachten Sie**, dass für die Textform des Berichtes im Filter die Kategorie "Low" eingeschaltet werden muss.

Mit der importierten Scan Configuration werden 2 Varianten des Ergebnisses erstellt: eine Übersicht in Textform (unter "general/IT-Grundschatz") und eine Tabelle für weitere Verarbeitung (unter "general/IT-Grundschatz-T"). Für letztere muss im Filter die Kategorie "Log" eingeschaltet werden.

```

Low general/IT-Grundschatz
NVT: IT-Grundschatz_11_EL (OID: 1.3.6.1.4.1.25623.1.0.895000)

Prüfergebnisse gemäß IT-Grundschatz, 11. Ergänzungslieferung:

IT-Grundschatz M4.001: Passwortschutz für IT-Systeme
Ergebnis: nicht erfüllt
Details: Folgende Benutzer entsprechen nicht den Anforderungen des IT-Grundschatz-Katalogs:
:
Keine Passwort: Guest, Kein Admin Passwort, Kein-Passwort,
Unsicheres Passwort: slad, SUPPORT_388945a0, Testuser,

IT-Grundschatz M4.002: Bildschirmsperre (Win)
Ergebnis: nicht erfüllt
Details: Für folgende Benutzer ist die Bildschirmsperre mit Passwortschutz nicht aktiviert:
:
LABXPPROX86SP2\\GSHB;LABXPPROX86SP2\\SvcCOPSSH;

IT-Grundschatz M4.003: Einsatz von Viren-Schutzprogrammen
Ergebnis: nicht erfüllt
Details: Das System hat einen Virenschanner installiert, welcher läuft aber veraltet ist.

IT-Grundschatz M4.004: Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern (Win)
Ergebnis: nicht erfüllt
Details: Dienste für Wechseldateinträger sind nicht deaktiviert.

IT-Grundschatz M4.005: Protokollierung der TK-Administrationsarbeiten
Ergebnis: unvollständig
Details: Eventlog läuft auf dem System. Bitte prüfen Sie ob Ihre TK-Anlage das Eventlog zum Abspeichern der Events benutzt.

IT-Grundschatz M4.006 Revision der TK-Anlagenkonfiguration
Ergebnis: Prüfung dieser Maßnahme ist nicht implementierbar.
Details: Prüfung diese Maßnahme ist nicht implementierbar.

IT-Grundschatz M4.007 Änderung voreinstellter Passwörter

```

```

Log general/IT-Grundschatz-T
NVT: IT-Grundschatz_11_EL (OID: 1.3.6.1.4.1.25623.1.0.895000)

"192.168.81.104"|"M4.001"|"FAIL"|"Folgende Benutzer entsprechen nicht den Anforderungen des IT-Grundschatz-Katalogs:
Keine Passwort: Guest, Kein Admin Passwort, Kein-Passwort,
Unsicheres Passwort: slad, SUPPORT_388945a0, Testuser, "
"192.168.81.104"|"M4.002"|"FAIL"|"Für folgende Benutzer ist die Bildschirmsperre mit Passwortschutz nicht aktiviert:
LABXPPROX86SP2\\GSHB;LABXPPROX86SP2\\SvcCOPSSH;"
"192.168.81.104"|"M4.003"|"FAIL"|"Das System hat einen Virenschanner installiert, welcher läuft aber veraltet ist."
"192.168.81.104"|"M4.004"|"FAIL"|"Dienste für Wechseldateinträger sind nicht deaktiviert."
"192.168.81.104"|"M4.005"|"NC"|"Eventlog läuft auf dem System. Bitte prüfen Sie ob Ihre TK-Anlage das Eventlog zum Abspeichern der Events benutzt."
"192.168.81.104"|"M4.006"|"NA"|"Prüfung diese Maßnahme ist nicht implementierbar."
"192.168.81.104"|"M4.007"|"NI"|"Prüfroutine für diese Maßnahme ist nicht verfügbar."

```

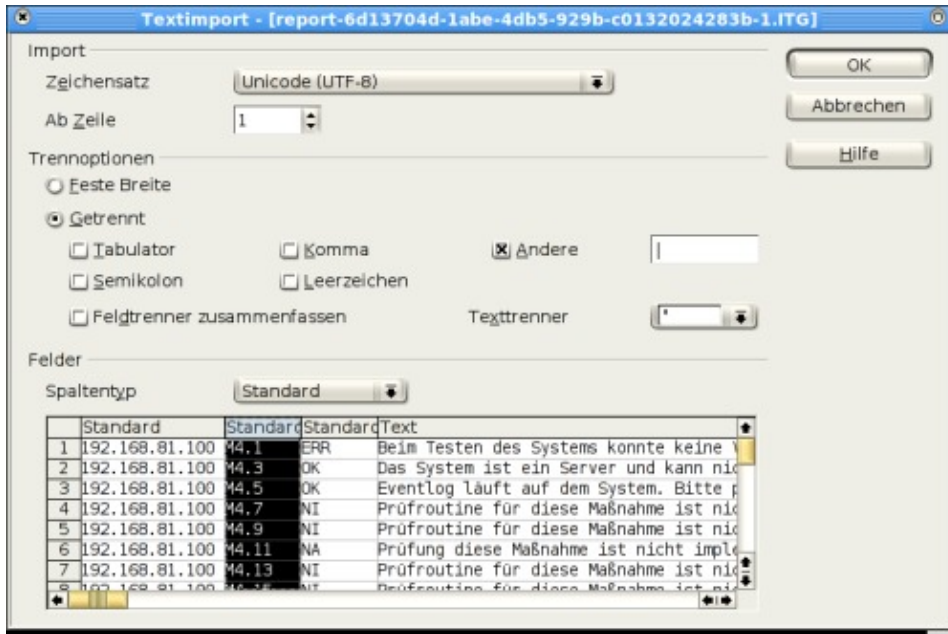
Übernahme der Ergebnisse in eine Tabellenkalkulation

1. Wählen Sie entweder im Report-Filter oder in der Task-Übersicht das Download-Format "ITG".
Hinweis: Bei Verwendung über den Report-Filter muss unbedingt die Kategorie "Log" aktiviert sein.

Reports for "ITG Scan"							
Report	Threat	Scan Results				Download	Actions
		High	Medium	Low	Log		
Wed Mar 31 07:37:20 2010 Done	Low	0	0	4	4	ITG <input type="button" value="Download"/>	

Bei diesem Download werden die tabellarischen Ergebnisse für sämtliche Zielsysteme automatisch herausgesucht und zusammengeführt.

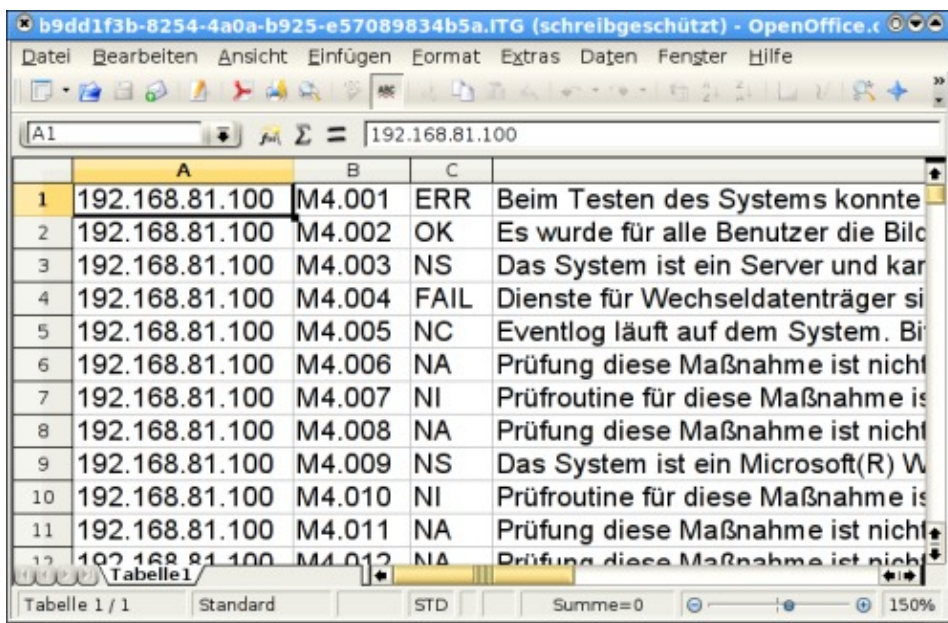
2. Importieren Sie nun die ITG-Datei als sogenannte CSV-Tabelle in Ihre Tabellenkalkulation.



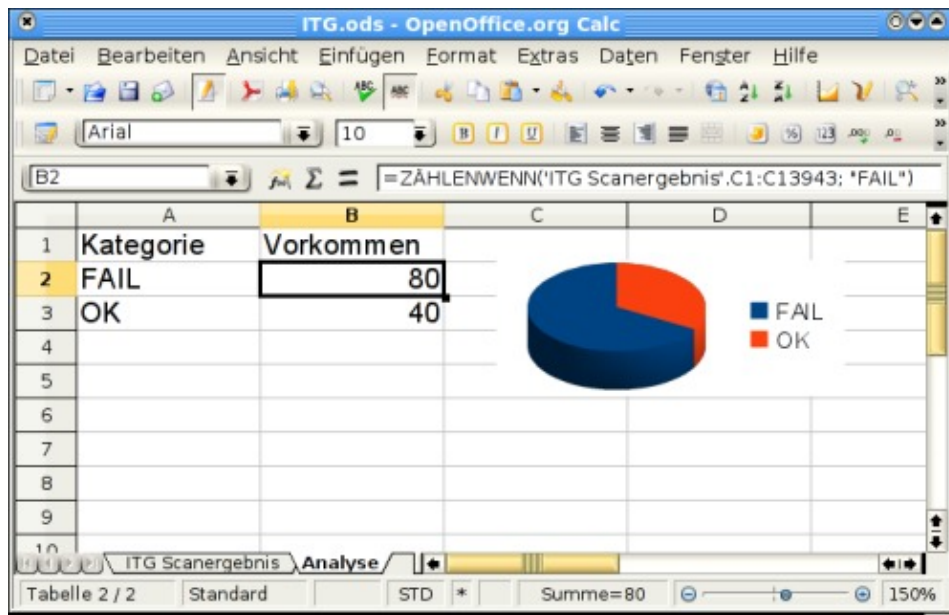
Obiges Beispiel zeigt den Import in OpenOffice 3.2. Beachten Sie insbesondere, dass Sie folgende Einstellungen vornehmen sofern nicht bereits vorausgewählt:

- ◆ Zeichensatz: UTF-8
- ◆ Trenner: Das "Pipe"-Symbol (senkrechter Strich)
- ◆ Texttrenner: Das doppelte Anführungszeichen
- ◆ Letzte Spalte vom Typ "Text"

3. Nun stehen die Ergebnisse in der Tabellenkalkulation zur Verfügung:



4. Daraus lassen sich je nach belieben einfache (wie im folgenden Screenshot) oder natürlich auch recht umfangreiche, individuelle Analysen oder Berichte gestalten.



Übernahme der Ergebnisse in IT-Grundschutz Tools

Es gibt eine Reihe von Anwendungen die dabei Helfen das Vorgehen gemäß IT Grundschutz zu strukturieren, zu erfassen und zu steuern.

Das Bundesamt für Sicherheit in der Informationstechnik bietet auf dessen Website eine [Übersicht über IT-Grundschutz Tools](#) an.

Für einen Import der Resultate des IT-Grundschutz-Scans in das jeweilige Tool kontaktieren Sie bitte den Hersteller des Tools und bei weitergehenden Fragen auch gerne den Support von Greenbone.

Ergebnis-Klassen der IT-Grundschutz Prüfung

Die Folgenden Ergebnis-Klassen können bei der Prüfung entstehen:

- *nicht erfüllt (FAIL)*: Für das Zielsystem wurde festgestellt, dass die Maßnahme nicht erfüllt ist.
- *erfüllt (OK)*: Für das Zielsystem wurde festgestellt, dass die Maßnahme erfüllt ist.
- *Fehler (ERR)*: Die Prüfroutine konnte nicht ordnungsgemäß ausgeführt werden. Z.B. benötigen die Prüfungen einiger Maßnahmen wie etwa M4.001 einen installierten Agenten auf den Zielsystemen. Ist der Agent nicht installiert, kann die Prüfung aus technischen Gründen nicht ausgeführt werden. Falls keine Credentials mitgegeben werden, dann werden recht viele Prüfungen diesen Status haben.
- *Prüfung für diese Maßnahme ist nicht verfügbar (NI)*: Grundsätzlich wird davon ausgegangen, dass diese Maßnahme automatisiert prüfbar ist. Es ist jedoch noch keine Implementierung erfolgt. Bei neu erschienenen Ergänzungslieferungen gilt dies zunächst für eine Reihe von Maßnahmen. Der Greenbone Security Feed wird jedoch zügig aktualisiert bis diese Ergebnis-Klasse nicht mehr vorkommt.
- *Prüfung dieser Maßnahme ist nicht implementierbar (NA)*: Eine Reihe von Maßnahmen der IT-Grundschutzkataloge sind zu allgemein gehalten um eine konkrete automatische Prüfung durchzuführen. Andere Maßnahmen beschreiben eine rein manuell machbare Prüfung und fallen damit ebenfalls in die Klasse der nicht implementierbaren Tests.

- *Prüfung für das Zielsystem nicht passend (NS)*: Einige Maßnahmen beziehen sich ausschließlich auf einen konkreten Betriebssystem-Typ. Ist das Zielsystem ein anderes, so wird die Kennzeichnung NS gesetzt.
- *Diese Maßnahme ist entfallen (DEP)*: Im Rahmen neuer Ergänzungslieferungen kommt es vor, dass einige Maßnahmen ersatzlos entfallen. Maßnahmen-Nummern werden dabei prinzipiell nicht neu vergeben. Mit DEP gekennzeichnete Einträge sind also nur der Vollständigkeit halber vorhanden und können ansonsten ignoriert werden.

Unterstützte Maßnahmen

Die Übersicht bezieht sich auf die 11. Ergänzungslieferung. Die Maßnahmen-Kennungen verweisen auf die auf den Webseiten des BSI angebotenen Detailinformationen.

Folgende Test-Typen werden unterschieden:

- Remote: Für Prüfung ist lediglich eine Netzwerkverbindung zum Zielsystem notwendig.
- Credentials: Für Prüfung ist ein Zugangskonto auf dem Zielsystem notwendig.
- Agent: Für Prüfung ist die Installation eines Agenten (SLAD oder WinSLAD) auf dem Zielsystem notwendig.

	Titel	Test-Typ	Hinweis
<u>M4.1</u>	Passwortschutz für IT-Systeme	Credentials	Vista und Windows 7 bei aktiviertem UAC zur Zeit noch nicht möglich.
<u>M4.2</u>	Bildschirm Sperre	Credentials	Windows: Kann nur für Lokale Konten getestet werden. Linux: Nur voreingestellte Bildschirmschoner bei Gnome und KDE.
<u>M4.3</u>	Einsatz von Viren-Schutzprogrammen	Credentials	
<u>M4.4</u>	Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern	Credentials	
<u>M4.5</u>	Protokollierung der TK-Administrationsarbeiten	Credentials	
<u>M4.7</u>	Änderung voreingestellter Passwörter	Remote	Test nur über SSH und Telnet.
<u>M4.9</u>	Einsatz der Sicherheitsmechanismen von XWindow	Credentials	
<u>M4.14</u>	Obligatorischer Passwortschutz unter Unix	Credentials	
<u>M4.15</u>	Gesichertes Login	Credentials	
<u>M4.16</u>	Zugangsbeschränkungen für Accounts und oder Terminals	Credentials	
<u>M4.17</u>	Sperren und Löschen nicht benötigter Accounts und Terminals	Credentials	
<u>M4.18</u>		Credentials	

	Administrative und technische Absicherung des Zugangs zum Monitor- und Single-User-Modus		
<u>M4.19</u>	Restriktive Attributvergabe bei Unix-Systemdateien und -verzeichnissen	Credentials	
<u>M4.20</u>	Restriktive Attributvergabe bei Unix-Benutzerdateien und -verzeichnissen	Credentials	
<u>M4.21</u>	Verhinderung des unautorisierten Erlangens von Administratorrechten	Credentials	
<u>M4.22</u>	Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten im Unix-System	Credentials	
<u>M4.23</u>	Sicherer Aufruf ausführbarer Dateien	Credentials	
<u>M4.23</u>	Sicherer Aufruf ausführbarer Dateien	Agent	
<u>M4.25</u>	Einsatz der Protokollierung im Unix-System	Agent	
<u>M4.26</u>	Regelmäßiger Sicherheitscheck des Unix-Systems	Agent	
<u>M4.33</u>	Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung	Credentials	
<u>M4.36</u>	Sperren bestimmter Faxempfänger-Rufnummern	Credentials	Cisco Geräte können nur über telnet getestet werden, da sie SSH blowfish-cbc encryption nicht unterstützen.
<u>M4.37</u>	Sperren bestimmter Absender-Faxnummern	Credentials	Cisco Geräte können nur über telnet getestet werden, da sie SSH blowfish-cbc encryption nicht unterstützen.
<u>M4.40</u>	Verhinderung der unautorisierten Nutzung des Rechtermikrofons	Credentials	Nur für Linux Umgesetzt. Es ist unter Windows nicht möglich den Status des Microfons über Registry/WMI auszulesen.
<u>M4.48</u>	Passwortschutz unter NT-basierten Windows-Systemen	Credentials	
<u>M4.48</u>	Passwortschutz unter NT-basierten Windows-Systemen	Agent	
<u>M4.49</u>	Absicherung des Boot-Vorgangs für ein NT basiertes Windows-System	Credentials	
<u>M4.52</u>	Geräteschutz unter NT-basierten Windows-Systemen	Credentials	
<u>M4.57</u>		Credentials	

	Deaktivieren der automatischen CD-ROM Erkennung		
<u>M4.80</u>	Sichere Zugriffsmechanismen bei Fernadministration	Remote	
<u>M4.93</u>	Regelmäßige Integritätsprüfung	Agent	
<u>M4.94</u>	Schutz der WWW-Dateien	Remote	
<u>M4.96</u>	Abschaltung von DNS	Credentials	
<u>M4.97</u>	Ein Dienst pro Server	Remote	
<u>M4.98</u>	Kommunikation durch Paketfilter auf Minimum beschränken	Credentials	Getestet wird auf die Microsoft Windows Firewall. Für Vista und Windows 7 auf jegliche Firewall die sich systemkonform installiert.
<u>M4.106</u>	Aktivieren der Systemprotokollierung	Credentials	
<u>M4.135</u>	Restriktive Vergabe von Zugriffsrechten auf Systemdateien	Credentials	
<u>M4.146</u>	Sicherer Betrieb von Windows 2000/XP / Sicherer Betrieb von Windows Client-Betriebssystemen	Agent	Vista und Windows 7 bei aktiviertem UAC zur Zeit noch nicht möglich.
<u>M4.147</u>	Sichere Nutzung von EFS unter Windows	Credentials	Die Maßnahme ist in der 11. EL technisch fehlerhaft. Eine Korrektur ist für die kommende 12. EL bereits berücksichtigt. Der Test führt abweichend von der Maßnahme den korrekten Test aus.
<u>M4.178</u>	Absicherung der Administrator- und Benutzerkonten beim IIS-Einsatz	Credentials	Es wird lediglich ein Hinweis auf SYSKEY und Passpro.exe gegeben.
<u>M4.179</u>	Schutz von sicherheitskritischen Dateien beim IIS-Einsatz	Credentials	
<u>M4.186</u>	Entfernen von Beispieldateien und Administrations-Scripts des IIS	Credentials	
<u>M4.189</u>	Schutz vor unzulässigen Programmaufrufen beim IIS-Einsatz	Credentials	
<u>M4.190</u>	Entfernen der RDS-Unterstützung des IIS	Credentials	
<u>M4.192</u>	Konfiguration des Betriebssystems für einen Apache-Webserver	Credentials	
<u>M4.195</u>	Konfiguration der Zugriffssteuerung beim Apache-Webserver	Credentials	
<u>M4.196</u>	Sicherer Betrieb eines Apache-Webservers	Credentials	
<u>M4.197</u>	Servererweiterungen für dynamische Webseiten beim Apache-Webserver	Credentials	

<u>M4.200</u>	Umgang mit USB-Speichermedien	Credentials	
<u>M4.227</u>	Einsatz eines lokalen NTP-Servers zur Zeitsynchronisation	Credentials	
<u>M4.238</u>	Einsatz eines lokalen Paketfilters	Credentials	Getestet wird auf die Microsoft Windows Firewall. Für Vista und Windows 7 auf jegliche Firewall die sich systemkonform installiert.
<u>M4.244</u>	Sichere Systemkonfiguration von Windows Client-Betriebssystemen	Credentials	
<u>M4.249</u>	Windows XP Systeme aktuell halten / Windows Client-Systeme aktuell halten	Agent	Vista und Windows 7 bei aktiviertem UAC zur Zeit noch nicht möglich.
<u>M4.277</u>	Absicherung der SMB-, LDAP- und RPC-Kommunikation unter Windows Server 2003	Credentials	
<u>M4.284</u>	Umgang mit Diensten unter Windows Server 2003	Credentials	
<u>M4.285</u>	Deinstallation nicht benötigter Client-Funktionen von Windows Server 2003	Credentials	
<u>M4.287</u>	Sichere Administration der VoIP-Middleware	Remote	
<u>M4.288</u>	Sichere Administration von VoIP-Endgeräten	Agent	Test muss explizit über Voreinstellungen aktiviert werden.
<u>M4.300</u>	Informationsschutz bei Druckern, Kopierern und Multifunktionsgeräten	Remote	
<u>M4.305</u>	Einsatz von Speicherbeschränkungen (Quotas)	Credentials	
<u>M4.310</u>	Einrichtung des LDAP-Zugriffs auf Verzeichnisdienste	Remote	
<u>M4.313</u>	Bereitstellung von sicheren Domänen-Controllern	Credentials	
<u>M4.315</u>	Aufrechterhaltung der Betriebssicherheit von Active Directory	Agent	
<u>M4.325</u>	Löschen von Auslagerungsdateien	Credentials	
<u>M4.326</u>	Sicherstellung der NTFS-Eigenschaften auf einem Samba-Dateiserver	Credentials	
<u>M4.328</u>	Sichere Grundkonfiguration eines Samba-Servers	Credentials	
<u>M4.331</u>	Sichere Konfiguration des Betriebssystems für einen Samba-Server	Credentials	

<u>M4.332</u>	Sichere Konfiguration der Zugriffssteuerung bei einem Samba-Server	Credentials	
<u>M4.333</u>	Sichere Konfiguration von Winbind unter Samba	Credentials	
<u>M4.334</u>	SMB Message Signing und Samba	Credentials	
<u>M4.338</u>	Einsatz von Windows Vista File und Registry Virtualization	Credentials	Nur ein genereller Test, ob Vista File und Registry Virtualization aktiviert ist.
<u>M4.339</u>	Verhindern unautorisierter Nutzung von Wechselmedien unter Windows Vista	Credentials	
<u>M4.340</u>	Einsatz der Windows Vista Benutzerkontensteuerung - UAC	Credentials	
<u>M4.341</u>	Integritätsschutz unter Windows Vista	Credentials	Soweit technisch möglich umgesetzt (aktiviertes UAC und geschützter Modus in verschiedenen Zonen).
<u>M4.342</u>	Aktivierung des Last Access Zeitstempels unter Windows Vista	Credentials	
<u>M4.344</u>	Überwachung eines Windows Vista Systems	Credentials	Die Maßnahme ist in der 11. EL technisch fehlerhaft. Eine Korrektur ist für die kommende 12. EL bereits berücksichtigt. Der Test führt abweichend von der Maßnahme den korrekten Test aus.
<u>M5.8</u>	Regelmäßiger Sicherheitscheck des Netzes	Remote	Es wird lediglich ein Meldung ausgegeben, dass mit aktuellsten Plugins getestet werden soll.
<u>M5.9</u>	Protokollierung am Server	Agent	
<u>M5.17</u>	Einsatz der Sicherheitsmechanismen von NFS	Credentials	
<u>M5.18</u>	Einsatz der Sicherheitsmechanismen von NIS	Credentials	
<u>M5.19</u>	Einsatz der Sicherheitsmechanismen von sendmail	Remote	
<u>M5.19</u>	Einsatz der Sicherheitsmechanismen von sendmail	Credentials	
<u>M5.20</u>	Einsatz der Sicherheitsmechanismen von rlogin, rsh und rcp	Credentials	
<u>M5.21</u>	Sicherer Einsatz von telnet, ftp, tftp und rexec	Credentials	
<u>M5.34</u>	Einsatz von Einmalpasswörtern	Credentials	
<u>M5.37</u>	Einschränken der Peer-to-Peer-Funktionalitäten in einem	Credentials	

	servergestützten Netz		
<u>M5.53</u>	Schutz vor Mailbomben	Remote	
<u>M5.55</u>	Kontrolle von Alias-Dateien und Verteilerlisten	Credentials	
<u>M5.59</u>	Schutz vor DNS-Spoofing	Credentials	
<u>M5.63</u>	Einsatz von GnuPG oder PGP	Credentials	
<u>M5.64</u>	Secure Shell	Remote	
<u>M5.66</u>	Verwendung von SSL	Remote	
<u>M5.72</u>	Deaktivieren nicht benötigter Netzdienste	Agent	Lediglich Anzeige der in Frage kommenden Dienste.
<u>M5.90</u>	Einsatz von IPSec unter Windows	Credentials	
<u>M5.91</u>	Einsatz von Personal Firewalls für Internet-PCs	Credentials	Getestet wird auf die Microsoft Windows Firewall. Für Vista und Windows 7 auf jegliche Firewall die sich systemkonform installiert. Auf Linux, soweit möglich, anzeige der iptables Regeln.
<u>M5.101</u>	Entfernen nicht benötigter ODBC-Treiber beim IIS-Einsatz	Credentials	
<u>M5.102</u>	Installation von URL-Filtern beim IIS-Einsatz	Credentials	
<u>M5.103</u>	Entfernen sämtlicher Netzwerkfreigaben beim IIS-Einsatz	Credentials	
<u>M5.104</u>	Konfiguration des TCP/IP-Filters beim IIS Einsatz	Credentials	
<u>M5.105</u>	Vorbeugen vor SYN-Attacken auf den IIS	Credentials	
<u>M5.107</u>	Verwendung von SSL im Apache-Webserver	Remote	
<u>M5.109</u>	Einsatz eines E-Mail-Scanners auf dem Mailserver	Remote	
<u>M5.123</u>	Absicherung der Netzkommunikation unter Windows	Credentials	
<u>M5.131</u>	Absicherung von IP-Protokollen unter Windows Server 2003	Credentials	
<u>M5.145</u>	Sicherer Einsatz von CUPS	Credentials	
<u>M5.147</u>	Absicherung der Kommunikation mit Verzeichnisdiensten	Remote	