6/21/2017

# NETZWERK-PRÜFUNG RISIKOBERICHT

## Test

Erstellt von: Musketier Systemhaus AG



Erstellt am: 01.04.2014

# Inhaltsverzeichnis

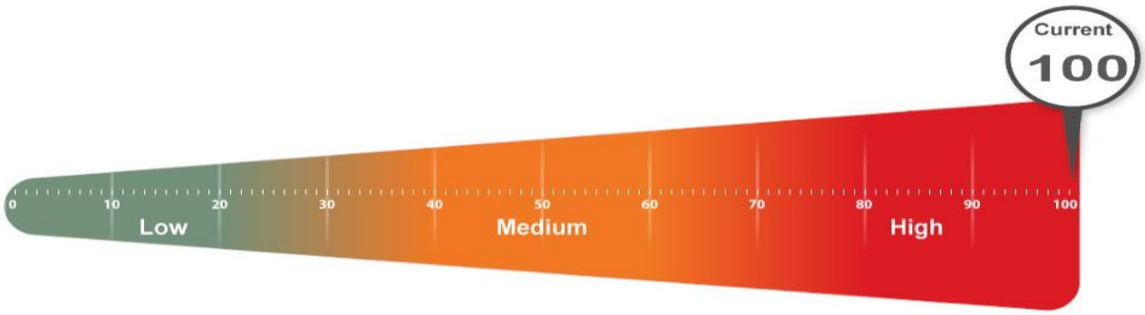
# Aufgaben

Die folgenden Analyse-Aufgaben wurden durchgeführt:

| | Aufgabe | Beschreibung |
|---|---|---|
| ✓ | Domain Controller finden | Identifiziert Domain-Controller und Online-Status |
| ✓ | FSMO-Rollenanalyse | Zählt FSMO-Rollen am Standort auf |
| ✓ | Zählt Organisationseinheiten und Sicherheitsgruppen auf | Listet die Organisationseinheiten und Sicherheitsgruppen mit Mitgliedern auf |
| ✓ | Nutzer-Analyse | Liste von Nutzern im AD, Status und letzte Anmeldung/Nutzung, welche bei der Identifikation von potentiellen Sicherheitsrisiken hilft |
| ✓ | Lokale Mail-Server ermitteln | Mail-Server im Netzwerk ermitteln |
| ✓ | Zeit-Server ermitteln | Zeit-Server im Netzwerk ermitteln |
| ✓ | Netzwerk-Freigaben ermitteln | Umfassende Liste von Netzwerk-Freigaben |
| ✓ | Haupt-Anwendungen ermitteln | Wichtigste Anwendungen/Versionen mit Anzahl der Installationen |
| ✓ | Detaillierte Domain-Controller-Ereignis-Log-Analyse | Liste von Ereignis-Log-Einträgen für die letzten 24 Stunden für Directory Service- , DNS-Server- und Datenreplikationsdienste |
| ✓ | Webserver-Feststellung und Identifizierung | Liste von Webservern und Typ |
| ✓ | Netzwerk-Discovery für Non-A/D-Geräte | Liste von Non-Active Directory - Geräten, die auf Netzwerk-Anfragen reagieren |
| ✓ | Internet-Zugang und Geschwindigkeitstest | Test von Internet-Zugang und Geschwindigkeit |
| ✓ | SQL-Serveranalyse | Liste von SQL-Servern und zugehöriger/n Datenbank(en) |
| ✓ | Internet-Domain-Analyse | Abfragen Firma Domain (s) über eine "WHOIS"-Lookup. |
| ✓ | Passwort-Sicherheitsanalyse | Verwendet MBSA um Computer mit schwachen Passwörtern zu identifizieren, die ein Sicherheitsrisiko darstellen könnten |
| ✓ | Fehlende Sicherheits-Updates | Verwendet MBSA um Computer mit fehlenden Sicherheits-Updates zu identifizieren |
| ✓ | System für System Ereignis-Log-Analyse | Letzte 5 System- und App-Ereignis-Logfehler für die Server |
| ✘ | Externe Sicherheitslücken | Liste von Sicherheitslücken und Warnhinweisen vom Scan |

# Risikobewertung

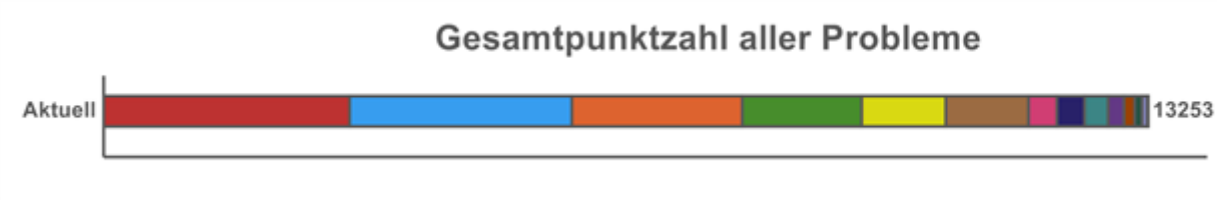
Die Risikoeinschätzung ist ein Wert von 1 bis 100, wobei 100 ein bedeutendes Risiko und potentielle Probleme bedeutet. Der Wert basiert auf dem höchsten Risiko.




Mehrere kritische Probleme wurden identifiziert.  Identifizierte Probleme sollten in Übereinstimmung mit dem Management-Plan überprüft und behoben werden.

# Problem-Zusammenfassung

Dieser Abschnitt enthält eine Zusammenfassung der Probleme, die bei dem Scan-Prozess erfasst worden sind und auf branchenweiten Best Practices für die Leistung und Sicherheit von Netzwerken basiert. Die Gesamtwertung bewertet das Niveau der Probleme in der Systemumgebung.




**Gesamtpunktzahl aller Probleme:** Risk Score x Anzahl der Vorfälle = Gesamtpunktzahl : Gesamt Prozent (%)

| | **Benutzerkennwörter sind so eingestellt, dass diese niemals ablaufen (80 Punkte pro Stück)** |
|---|---|
| 3120 | ***Zwischenstand:*** 80 Punkte x 39 = 3120: 23.54% |
| | ***Ausgabe:*** Benutzerkennwörter sind so eingestellt, dass diese niemals ablaufen. Dies kann ein Risiko darstellen, da diese durch die Nutzung durch nicht autorisierte Benutzer leichter verwendet werden können. Diese sind leichter zu hacken/umgehen, als Kennwörter, welche routinemäßig verändert werden. |
| | ***Empfehlung:*** Untersuchen Sie alle Konten mit Passwörtern die niemals ablaufen und konfigurieren Sie diese entsprechend. |

| | **Anti-Virus nicht installiert (94 Punkte pro Stück)** |
|---|---|
| 2820 | ***Zwischenstand:*** 94 Punkte x 30 = 2820: 21.28% |
| | ***Ausgabe:*** Es wurde keine Anti-Virus-Software auf einigen Computern erkannt. Ohne ausreichenden Anti-Virus- und Anti-Spyware-Schutz auf allen Workstations und Servern ist das Risiko erhöht von bösartiger Software infiziert zu werden. |
| | ***Empfehlung:*** Um Sicherheitsprobleme zu vermeiden empfehlen wir, einen AntiVirenschutz auf allen Geräten zu installieren |

| | **Anti-Spyware nicht installiert (94 Punkte pro Stück)** |
|---|---|
| 2162 | ***Zwischenstand:*** 94 Punkte x 23 = 2162: 16.31% |
| | ***Ausgabe:*** Anti-Spyware-Software wurde auf einigen Computern nicht erkannt. Ohne einen ausreichenden Anti-Virus- und Anti-Spyware-Schutz auf allen Workstations und Servern ist das Risiko bösartiger Software erhöht. |
| | ***Empfehlung:*** Um Sicherheitsprobleme zu vermeiden empfehlen wir, einen AntiSpywareschutz auf allen Geräten zu installieren |

| | **Inaktive Computer (15 Punkte pro Stück)** |
|---|---|
| 1515 | ***Zwischenstand:*** 15 Punkte x 101 = 1515: 11.43% |
| | ***Ausgabe:*** Computer haben sich innerhalb der letzten 30 Tage nicht angemeldet |
| | ***Empfehlung:*** Prüfen Sie die Liste der inaktiven Computer um festzustellen, ob sie aus dem Active Directory entfernt werden sollten. |

| | **Nicht unterstützte Betriebssysteme/Ausgelaufener Herstellersupport (97 Punkte pro Stück)** |
|---|---|

| | |
|---|---|
| 1067 | ***Zwischenstand:*** 97 Punkte x 11 = 1067: 8.05% |
| | ***Ausgabe:*** Es wurden Computer gefunden, welche ein nicht mehr unterstütztes Betriebssystem nutzen. Nicht unterstützte Betriebssysteme erhalten keine Sicherheitspatches mehr und stellen dadurch ein Sicherheitsrisiko dar. |
| | ***Empfehlung:*** Upgraden oder ersetzen Sie die Computer die ein nicht mehr unterstütztes Betriebssystem nutzen. |

| | |
|---|---|
| | **Signifikant hohe Anzahl von Domain-Administratoren (35 Punkte pro Stück)** |
| 1050 | ***Zwischenstand:*** 35 Punkte x 30 = 1050: 7.92% |
| | ***Ausgabe:*** Mehr als 30% der Nutzer sind in der Domain-Administrator-Gruppe und haben uneingeschränkten Zugriff auf Dateien und Systemressourcen. Kompromittierte Domänenadministratorkonten stellen eine höhere Gefahr als normale Benutzer dar. |
| | ***Empfehlung:*** Beurteilen Sie die Notwendigkeit, mehr als 30% der Nutzer in der Domänenadministratorgruppe zu haben und den administrativen Zugriff auf das notwendige Minimum zu beschränken. |

| | |
|---|---|
| | **Einige Sicherheitspatches fehlen auf einigen Computern (90 Punkte pro Stück)** |
| 360 | ***Zwischenstand:*** 90 Punkte x 4 = 360: 2.72% |
| | ***Ausgabe:*** Sicherheits-Patches fehlen auf eínigen Computern. Sicherheitspatches zu installieren unterstützt bei der Vermeidung von Sicherheitsrisiken. Einige ist definiert als fehlend von 3 oder weniger Patches. |
| | ***Empfehlung:*** Aktualisieren Sie die Computer mit fehlenden Sicherheitspatches |

| | |
|---|---|
| | **Benutzer hat sich in 30 Tagen nicht angemeldet (13 Punkte pro Stück)** |
| 351 | ***Zwischenstand:*** 13 Punkte x 27 = 351: 2.65% |
| | ***Ausgabe:*** Benutzer, die sich in den letzten 30 Tagen nicht angemeldet haben, könnten Benutzerkonten von ehemaligen Mitarbeiter sein |
| | ***Empfehlung:*** Deaktivieren oder entfernen Sie Benutzerkonten, die sich nicht in den letzten 30 Tagen angemeldet haben. |

| | |
|---|---|
| | **Betriebssystem im erweiterten Support (20 Punkte pro Stück)** |
| 300 | ***Zwischenstand:*** 20 Punkte x 15 = 300: 2.26% |
| | ***Ausgabe:*** Es wurden Computer die ein Betriebssystem mit ausgelaufenen Herstellersupport nutzen entdeckt. Ausgelaufene Betriebssysteme erhalten keinen Herstellersupport mehr und werden nicht mehr gepatched. |
| | ***Empfehlung:*** Upgrade der Computer die ein Betriebssystem mit ausgelaufenen Herstellersupport nutzen bevor diese End-of-Life sind. |

| | |
|---|---|
| | **Mögliche Risiken durch Kennwortstärke (100 Punkte pro Stück)** |
| 200 | ***Zwischenstand:*** 100 Punkte x 2 = 200: 1.51% |
| | ***Ausgabe:*** Bei 2 Benutzerkonten wurde ein potenzial schwach Kennwort befunden. Unzureichend Starke oder schwache Passwörter auf lokale Konten können einem Hacker erlauben, das System zu kompromittieren. Es kann auch auf die Verbreitung von Schadsoftware hinweisen. |
| | ***Empfehlung:*** Wir empfehlen, eine ausreichend starke Kennwortrichtlinie zu verwenden um mögliche Risiken zu vermeiden. |

| | |
|---|---|
| | **Potenzieller Fehler beim Laufwerksspeicher (68 Punkte pro Stück)** |
| 136 | ***Zwischenstand:*** 68 Punkte x 2 = 136: 1.03% |
| | ***Ausgabe:*** 2 Computer wurden mit deutlich wenig freiem Speicherplatz gefunden. |
| | ***Empfehlung:*** Freier oder ergänzenden Speicherplatz für die angegebenen Laufwerke hinzufügen. |

| | |
|---|---|
| | **Anti-Virus nicht eingeschaltet (92 Punkte pro Stück)** |
| 92 | ***Zwischenstand:*** 92 Punkte x 1 = 92: 0.69% |
| | ***Ausgabe:*** Wir waren nicht in der Lage zu bestimmen, ob eine Anti-Viren-Software auf einigen Computern aktiviert ist und ausgeführt wird. |
| | ***Empfehlung:*** Feststellen ob AntiVirenschutz aktiviert ist |

| | |
|---|---|
| | **Unsichere offene Ports (10 Punkte pro Stück)** |
| 70 | ***Zwischenstand:*** 10 Punkte x 7 = 70: 0.53% |
| | ***Ausgabe:*** Computer verwenden potenziell unsichere Protokolle. |
| | ***Empfehlung:*** Es kann einen legitimen Grund geben, aber die Risiken sollten einzelnen bewerten werden. Bestimmte Protokolle sind von Natur aus unsicher da bspw. typischerweise die Verschlüsselung fehlt. Innerhalb des Netzwerks sollte ihre Verwendung so weit wie möglich minimiert werden, um die Ausbreitung von bösartiger Software zu verhindern. Natürlich kann es Gründe geben diese Dienste und andere Mittel zum Schutz der Systeme erforderlich sind.. Wir empfehlen eine Überprüfung aller Programme für jene die das Netzwerk nutzen um die Notwendigkeit und Sicherheit abzuschätzen. |

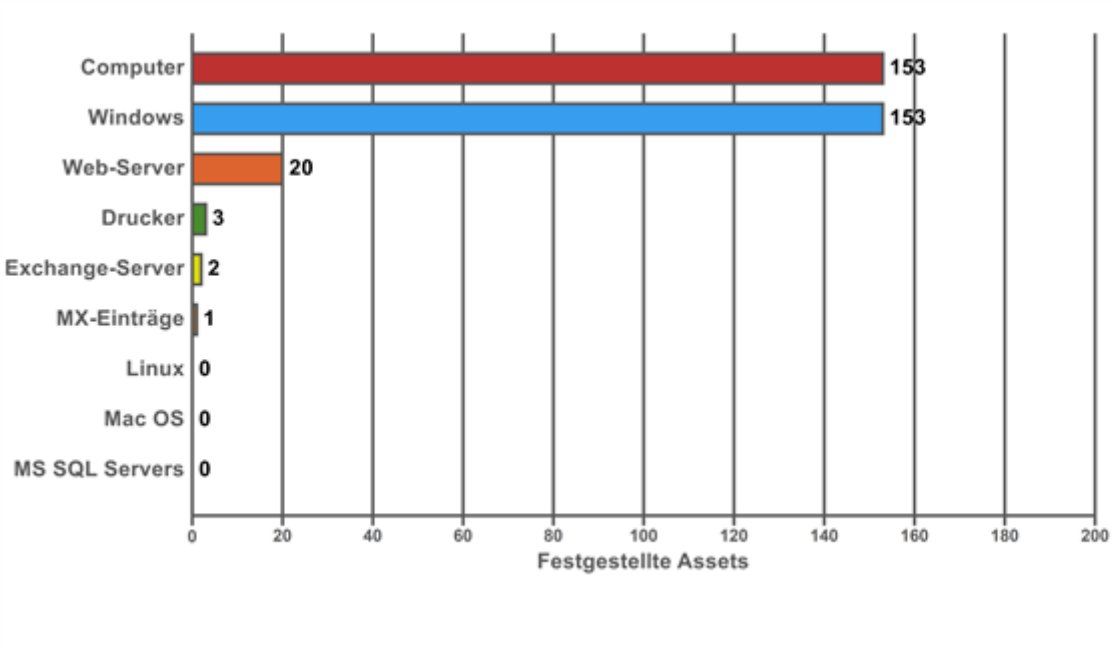
| | |
|---|---|
| | **Ungefüllte Organisationseinheiten (10 Punkte pro Stück)** |
| 10 | ***Zwischenstand:*** 10 Punkte x 1 = 10: 0.08% |
| | ***Ausgabe:*** Leere Organisationseinheiten (OU) im Active Directory gefunden. Diese könnten zu Fehlkonfigurationen führen |
| | ***Empfehlung:*** Entfernen oder füllen Sie Organisationseinheiten |

## Ergebnisse der Bandbreitenmessung

Download-Geschwindigkeit: **50.10 Mb/s**

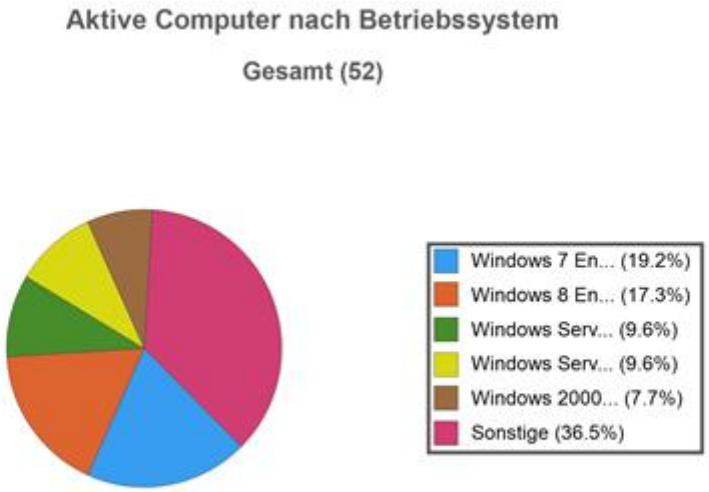

Upload-Geschwindigkeit: **22.02 Mb/s**


## Asset-Zusammenfassung: Festgestellte Assets

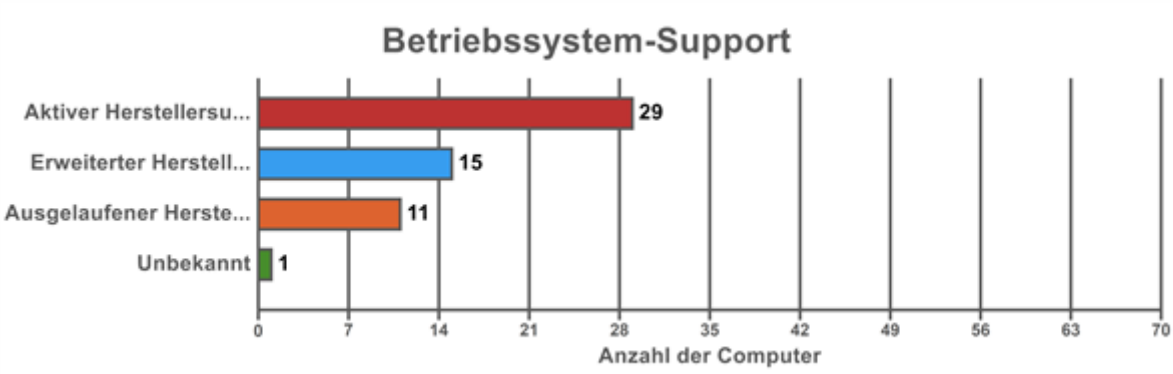


# Asset-Zusammenfassung: Aktive Computer

Aktive Computer werden als Computer definiert, die entweder aktiv zum Zeitpunkt des Scans reagiert haben oder die sich mit dem Active Directory innerhalb der letzten 30 Tage verbunden haben.

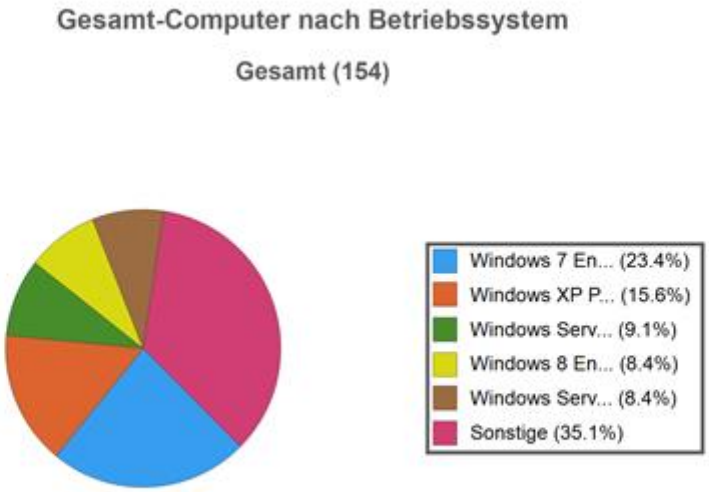



| Betriebssystem | Gesamt | Prozent |
|---|---|---|
| **Top fünf** | | |
| Windows 7 Enterprise | 10 | 19.2% |
| Windows 8 Enterprise | 9 | 17.3% |
| Windows Server 2003 | 5 | 9.6% |
| Windows Server 2012 R2 Standard | 5 | 9.6% |
| Windows 2000 Server | 4 | 7.7% |
| Gesamt - Top Fünf | **33** | **63.5%** |
| **Sonstige** | | |
| Windows Server 2012 R2 Datacenter | 4 | 7.7% |
| Windows Server 2012 Standard | 4 | 7.7% |
| Windows 8.1 Enterprise | 3 | 5.8% |
| Windows 7 Professional | 2 | 3.8% |
| Hyper-V Server 2012 | 1 | 1.9% |
| Windows 8.1 Pro | 1 | 1.9% |
| Windows Server 2008 R2 Datacenter | 1 | 1.9% |
| Windows Server 2008 R2 Enterprise | 1 | 1.9% |
| Windows Server 2012 Datacenter | 1 | 1.9% |
| Windows Vista Business | 1 | 1.9% |
| Gesamt - Sonstiges | **19** | **36.5%** |
| **Gesamt** | **52** | **100%** |


Betriebssystem-Support
Aktiver Herstellersu...
29
Erweiterter Herstell...
15
Ausgelaufener Herste...
11
Unbekannt
1
0
7
14
21
28
35
42
49
56
63
70
Anzahl der Computer

# Asset-Zusammenfassung: Alle Computer

Die Liste aller Computer enthält möglicherweise Computer, die nicht mehr aktiv sind, aber dennoch Einträge im Active Directory haben.

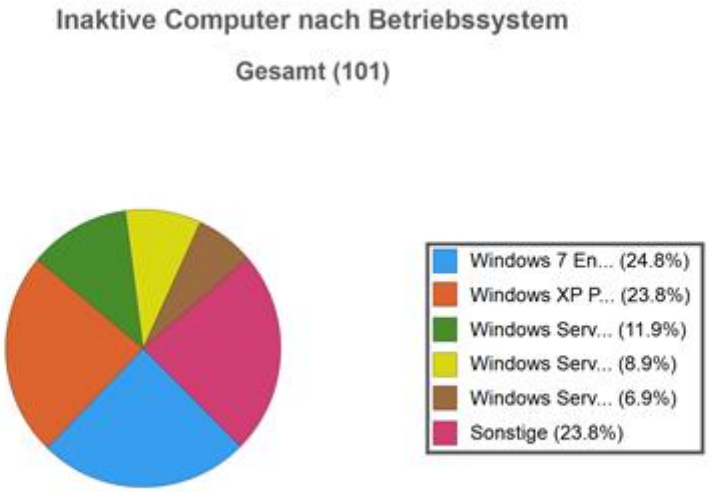



| Betriebssystem | Gesamt | Prozent |
|---|---|---|
| **Top fünf** | | |
| Windows 7 Enterprise | 36 | 23.4% |
| Windows XP Professional | 24 | 15.6% |
| Windows Server 2003 | 14 | 9.1% |
| Windows 8 Enterprise | 13 | 8.4% |
| Windows Server 2008 R2 Enterprise | 13 | 8.4% |
| Gesamt - Top Fünf | **100** | **64.9%** |
| **Sonstige** | | |
| Windows Server 2008 R2 Standard | 7 | 4.5% |
| Windows Server 2012 Standard | 7 | 4.5% |
| Windows 2000 Server | 6 | 3.9% |
| Windows Server 2012 R2 Datacenter | 5 | 3.2% |
| Windows Server 2012 R2 Standard | 5 | 3.2% |
| Windows 7 Professional | 4 | 2.6% |
| Windows 7 Ultimate | 4 | 2.6% |
| Unidentified OS | 3 | 1.9% |
| Windows 8.1 Enterprise | 3 | 1.9% |
| Windows Server 2012 Datacenter | 2 | 1.3% |
| Hyper-V Server 2012 | 1 | 0.6% |
| Windows 8 Consumer Preview | 1 | 0.6% |
| Windows 8.1 Pro | 1 | 0.6% |
| Windows Server 2008 Enterprise | 1 | 0.6% |
| Windows Server 2008 R2 Datacenter | 1 | 0.6% |

| Betriebssystem | Gesamt | Prozent |
|---|---|---|
| Windows Server 2008 Standard | 1 | 0.6% |
| Windows Vista Business | 1 | 0.6% |
| Windows Vista Ultimate | 1 | 0.6% |
| Gesamt - Sonstiges | **54** | **35.1%** |
| **Gesamt** | **154** | **100%** |

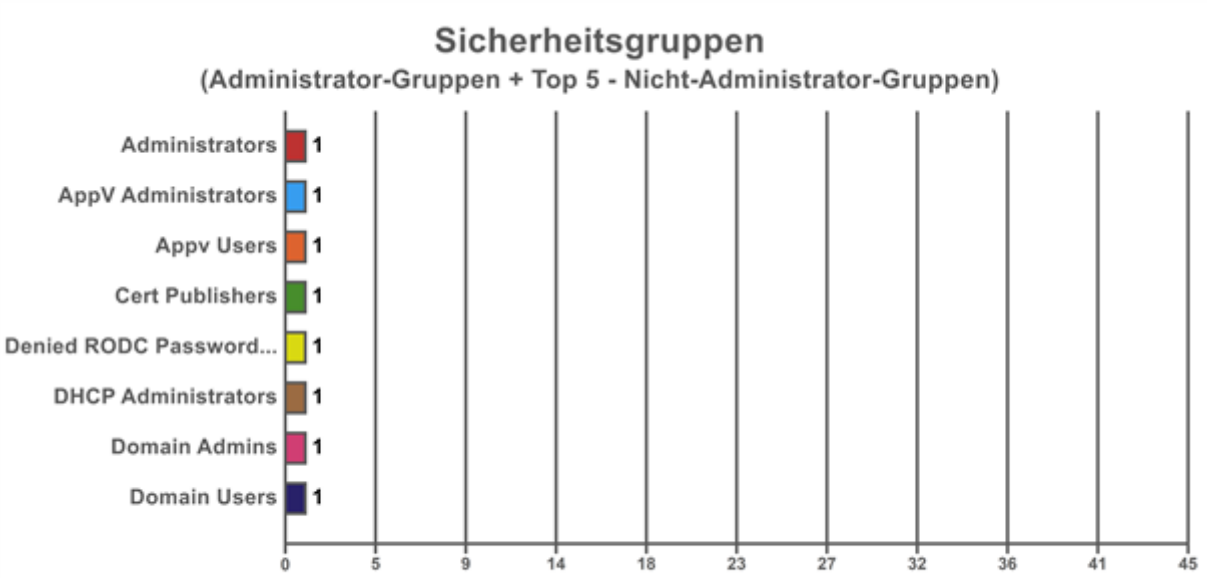
# Asset-Zusammenfassung: Inaktive Computer

Inaktive Computer sind Computer, die nicht gescannt werden konnten oder nicht im Active Directory sind.

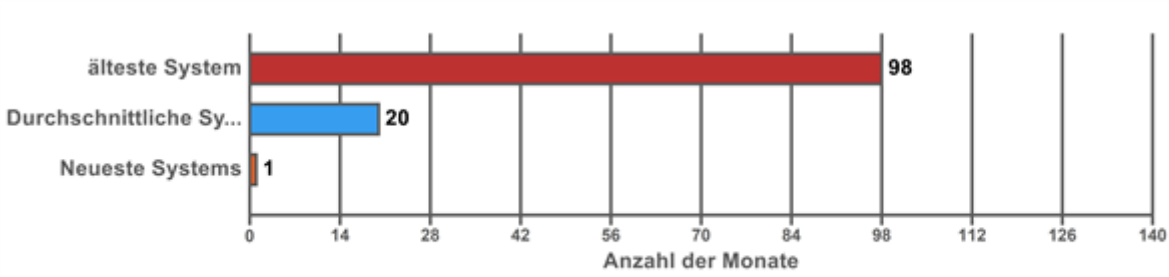



| Betriebssystem | Gesamt | Prozent |
|---|---|---|
| **Top fünf** | | |
| Windows 7 Enterprise | 25 | 24.8% |
| Windows XP Professional | 24 | 23.8% |
| Windows Server 2008 R2 Enterprise | 12 | 11.9% |
| Windows Server 2003 | 9 | 8.9% |
| Windows Server 2008 R2 Standard | 7 | 6.9% |
| Gesamt - Top Fünf | **77** | **76.2%** |
| **Sonstige** | | |
| Windows 7 Ultimate | 4 | 4% |
| Windows 8 Enterprise | 4 | 4% |
| Unidentified OS | 3 | 3% |
| Windows Server 2012 Standard | 3 | 3% |
| Windows 2000 Server | 2 | 2% |
| Windows 7 Professional | 2 | 2% |
| Windows 8 Consumer Preview | 1 | 1% |
| Windows Server 2008 Enterprise | 1 | 1% |
| Windows Server 2008 Standard | 1 | 1% |
| Windows Server 2012 Datacenter | 1 | 1% |
| Windows Server 2012 R2 Datacenter | 1 | 1% |
| Windows Vista Ultimate | 1 | 1% |
| Gesamt - Sonstiges | **24** | **23.8%** |
| **Gesamt** | **101** | **100%** |

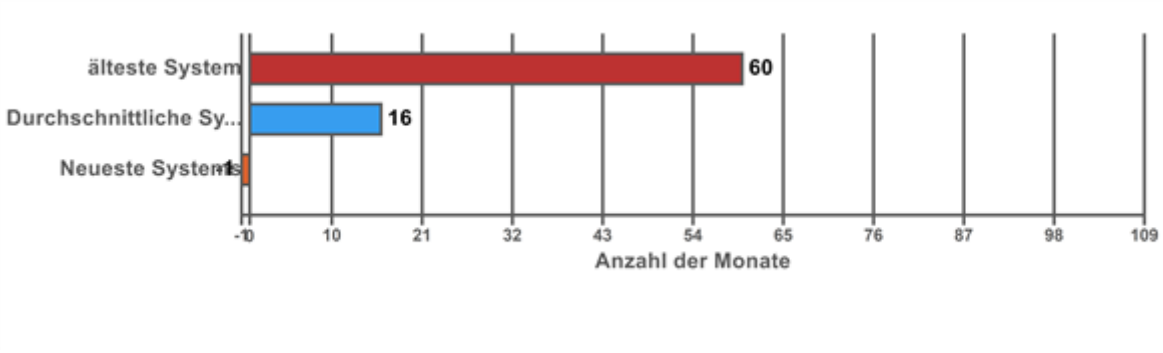
# Asset-Zusammenfassung: Nutzer



Sicherheitsgruppen
(Administrator-Gruppen + Top 5 - Nicht-Administrator-Gruppen)
Administrators
1
AppV Administrators
1
Appv Users
1
Cert Publishers
1
Denied RODC Password...
1
DHCP Administrators
1
Domain Admins
1
Domain Users
1
0
5
9
14
18
23
27
32
36
41
45

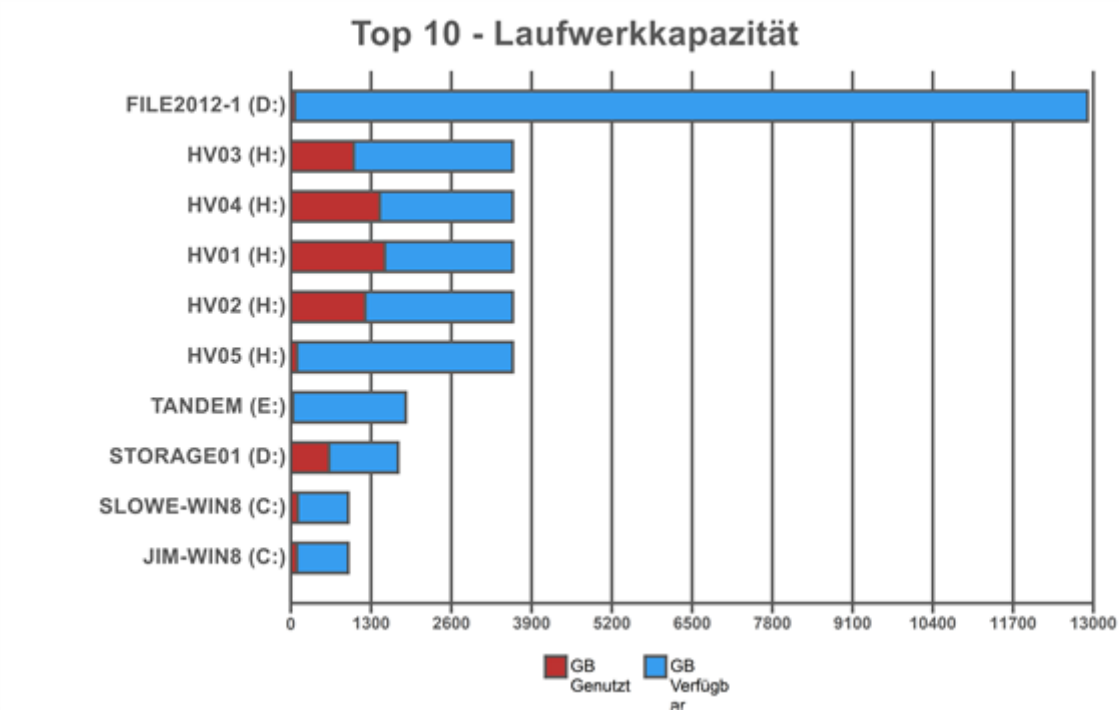
# Server-Altersstruktur

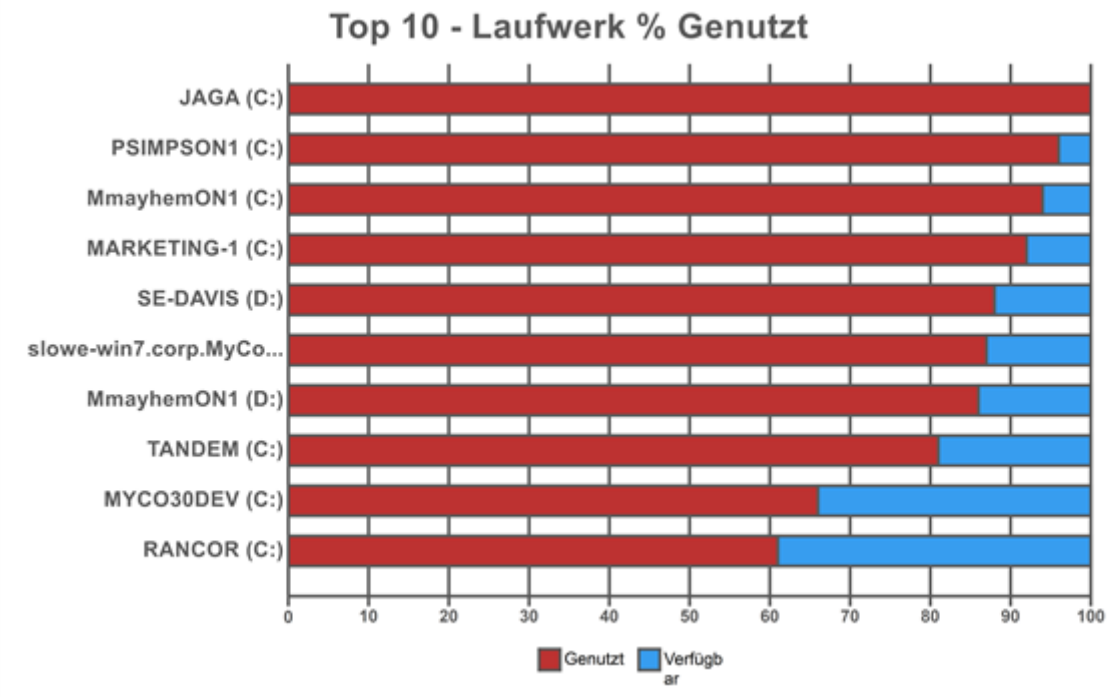


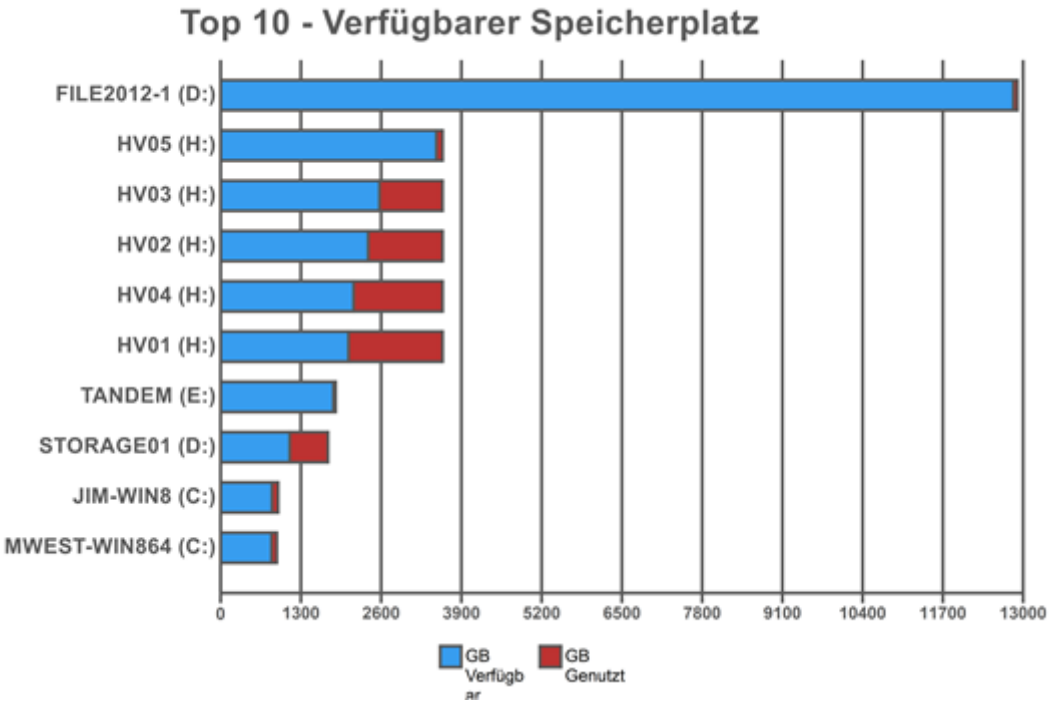
# Arbeitsplatz-Altersstruktur



# Asset-Zusammenfassung: Speichernutzung




Top 10 - Verfügbarer Speicherplatz
FILE2012-1 (D:)
HV05 (H:)
HV03 (H:)
HV02 (H:)
HV04 (H:)
HV01 (H:)
TANDEM (E:)
STORAGE01 (D:)
JIM-WIN8 (C:)
MWEST-WIN864 (C:)
0
1300
2600
3900
5200
6500
7800
9100
10400
11700
13000
GB Verfügbar
GB Genutzt