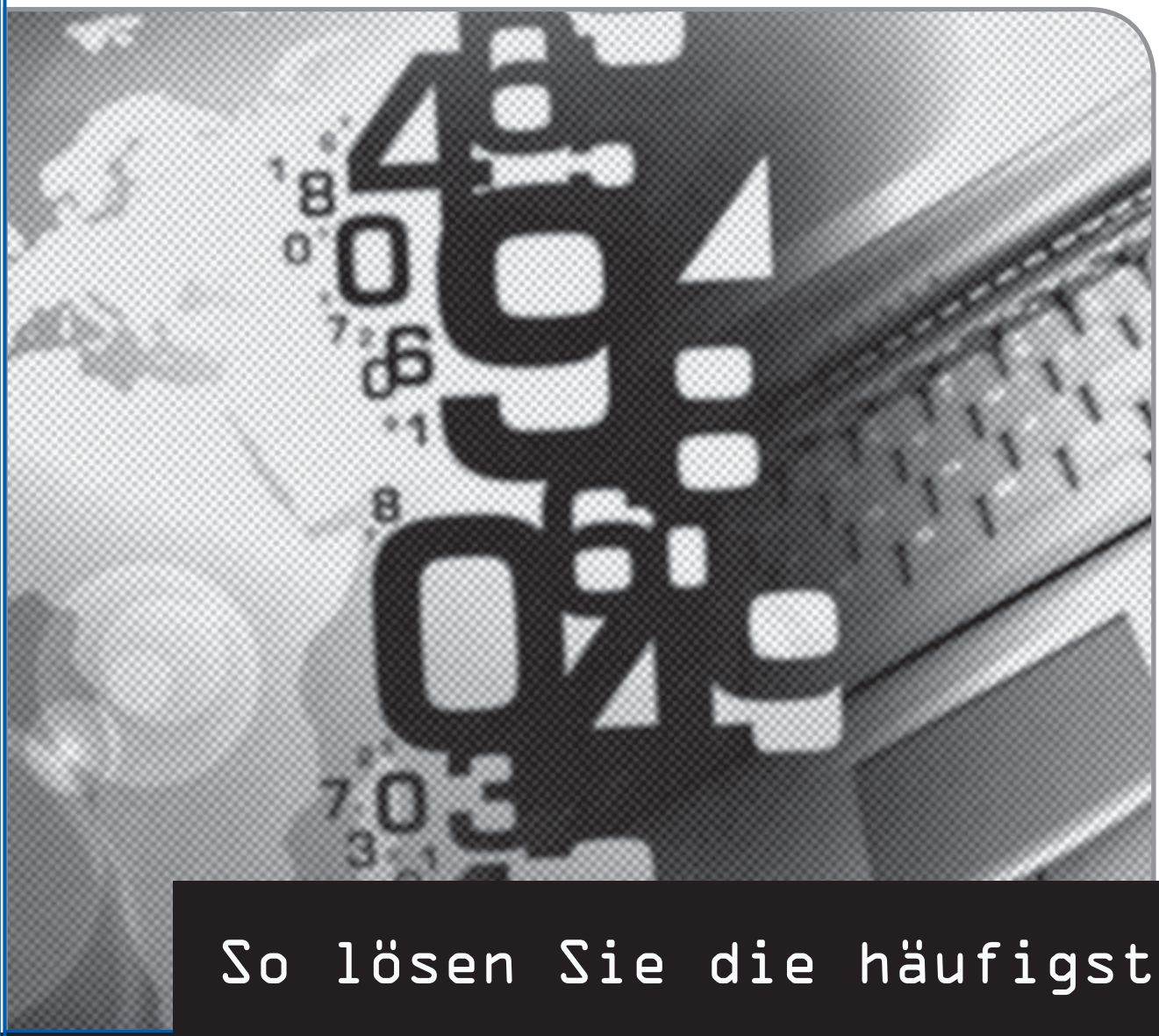
COMPUTERWISSEN



So lösen Sie die häufigsten Netzwerkprobleme dauerhaft

powered by **Computerwissen.de**

Verlag

VNR Verlag für die Deutsche Wirtschaft AG
Computerwissen
Theodor-Heuss-Straße 2-4
53095 Bonn

Telefon: (02 28) 9 55 01 90
Telefax: (02 28) 3 69 63 50

USt.-ID: DE 812639372
Amtsgericht Bonn, HRB 8165

Vorstand: Helmut Graf, Guido Ems
Vorsitzender des Aufsichtsrates: Norman Rentrop

Internet: www.computerwissen.de
E-Mail: info@computerwissen.de

Abonnementverwaltung

PSB/Presse Service Bonn GmbH & Co. KG
Theodor-Heuss-Straße 4
53177 Bonn

Internet: www.presseservicebonn.de
E-Mail: info@presseservicebonn.de

Inhaltsverzeichnis

Mit Schwachstellen-Management Schaden vom Unternehmen abwenden

Eine recht große Werbeagentur mit Sitz in Düsseldorf und verschiedenen Filialen im In- und Ausland hat mich vor einiger Zeit als Berater beauftragt, weil in dem Unternehmen ein neues Desktop-Publishing-Programm implementiert werden sollte.

Bei der Analyse des Unternehmens habe ich festgestellt, dass zwar die Datensicherung täglich durchgeführt wurde, die Datensicherungsbänder aber leer waren. Der Datensicherungs-Job wurde zwar täglich aufgerufen, die zu sichernden Daten waren aber nicht ausgewählt worden.

Außerdem konnte ich feststellen, dass zwar jede Menge Schriften auf den Computern der Mitarbeiter installiert waren, lizenziert waren aber nur einige wenige davon. Die Mitarbeiter und auch die Geschäftsführer sagten mir, dass dies in Werbeagenturen durchaus üblich sei.

Wie Sie mit einer vollständigen IT-Dokumentation Lücken in Ihrem Unternehmen aufdecken

Mein Einsatz bei der Werbeagentur hat mir etwas Grundsätzliches gezeigt: Eine umfassende und detaillierte Dokumentation der installierten Hard- und Software ist für ein Unternehmen unerlässlich. Bei dieser Art der Dokumentation geht es aber nicht ausschließlich darum, dass die Mitarbeiter der IT-Abteilung und die Geschäftsführung wissen, welche Programme und Computer in einem Unternehmen eingerichtet wurden. Wie das Beispiel recht eindrucksvoll zeigt, geht es auch um die Risiken, die ein Unternehmen eingeht, wenn eine Datensicherung unvollständig ist oder nicht lizenzierte Software im Unternehmen verbreitet wird.

Die Geschäftsführer der Werbeagentur erzählten mir sogar, dass einige andere Agenturen bereits mit sehr hohen Strafen belegt worden seien, weil dort nicht lizenzierte Schriften gefunden wurden. Es handelt sich hierbei schlichtweg um Raubkopien, die in einem Unternehmen nichts zu suchen haben.

Das zweite Risiko betrifft eine fehlende bzw. unvollständige Datensicherung. Eine Studie des Marktforschungsinstituts Vanson Bourne besagt, dass 54 Prozent der befragten Unternehmen bereits von Datenverlust betroffen waren, beispielsweise durch Stromausfall. 74 Prozent der IT-Manager dieser Unternehmen sind sich allerdings nicht sicher, ob die Daten bei einem Verlust vollständig wiederhergestellt werden können.

Befragt wurden 1.750 international tätige Unternehmen. Die Studie wurde im Jahr 2010 im Auftrag des US-amerikanischen Spezialisten für Speichersysteme EMC durchgeführt („**http://germany.emc.com/microsites/2011/emc-brs-survey/index.htm**“).

Erstellen Sie verständliche und verbindliche Sicherheitsrichtlinien

Nur eine ausführliche Dokumentation der Komponenten in Ihrem Unternehmen kann dazu beitragen, dass Sie die Risiken kennen und geeignete Schutzmaßnahmen treffen. Bevor Sie sich aber Gedanken über die Inhalte einer solchen Dokumentation machen, sollten Sie eindeutige Sicherheitsrichtlinien für Ihr Unternehmen festhalten. Die folgende Auflistung zeigt Ihnen wichtige Punkte und hilft Ihnen beim Festlegen dieser Sicherheitsrichtlinien.

- **Unternehmensstruktur**

Hier sollte beschrieben werden, über welche Schnittstellen die Mitarbeiter im Unternehmen und außerhalb des Unternehmens miteinander kommunizieren.

- **Prüfung der Informationssicherheit**

Hierbei sollen in erster Linie die folgenden Fragen geklärt werden: Welche Daten werden wo gespeichert? Welche mobilen Mitarbeiter gibt es? Werden Daten in der Cloud gespeichert?

- **Prüfung der Sicherheitsziele**

Aus der Sammlung der vorhandenen Speicherorte für diese Daten und der Kommunikationsschnittstellen ergibt sich, welche Sicherheitsziele für ein Unternehmen festgelegt werden müssen. Zur Festlegung der Sicherheitsziele gehört ebenfalls die Organisation der Datensicherung.

- **Prüfung der Sicherheitsrichtlinien**

In sehr vielen Unternehmen wird es Mitarbeitern gestattet, ihre privaten Laptops, Tablet-PCs oder Smartphones zur Erledigung ihrer Arbeit einzusetzen. Nur wenn Sie die Sicherheitsrichtlinien ständig überprüfen, können Sie auf neue Trends optimal reagieren.

- **Schulung der Mitarbeiter**

Nur wenn Ihre Kollegen umfassend über die Sicherheitsanforderungen in Ihrem Unternehmen informiert sind, können sie verstehen, dass die Sicherheitsrichtlinien zum Schutz und nicht zur Gängelung dienen. Eine Schulung kann ebenfalls dazu beitragen, den Bedarf der Mitarbeiter in Bezug auf die EDV zu klären.

- **Festlegen der Verantwortlichkeiten**

Holen Sie Ihre Kolleginnen und Kollegen mit ins Boot, indem Sie in jeder Abteilung einen Sicherheitsverantwortlichen nominieren. Die Sicherheitsverantwortlichen in den Abteilungen bekommen sehr viel schneller mit, wenn es Änderungen beim Sicherheitsbedarf gibt.
Sie sollten hier auch festlegen, welche Mitarbeiter aus der IT-Abteilung oder den anderen Abteilungen in einem Krisenfall verantwortlich sind. Ein solcher Krisenfall beinhaltet die Rücksicherung von Daten, die Reaktion auf Angriffe und die Eliminierung von Schad-Software.

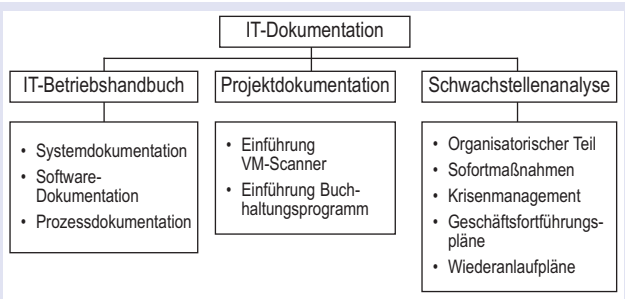
- **Sanktionen bei Verstößen**

Dies ist sicherlich der unangenehmste Teil der Sicherheitsrichtlinien, aber Sie müssen durch Ihre Geschäftsführung festlegen lassen, was geschehen soll, wenn ein Mitarbeiter gegen die Sicherheitsrichtlinien verstößt. Bei den Sanktionsmaßnahmen sollten Sie jedoch immer berücksichtigen, dass der betroffene Mitarbeiter einen Lerneffekt hat und nicht bloßgestellt wird.

Die professionelle Installation des SCCM 2012

Die Sicherheitsrichtlinien sind Teil der Dokumentation. Hauptbestandteil der Dokumentation sind das IT-Betriebshandbuch, die Projektdokumentation und die Schwachstellenanalyse. Das IT-Betriebshandbuch erfasst die Systemdokumentation, die Software-Dokumentation und die Prozessdokumentation. Die Projektdokumentation beinhaltet keine festen Punkte, sondern die Projekte, die entweder bereits laufen oder in naher Zukunft aufgesetzt werden.

Die Schwachstellenanalyse (Vulnerability Assessment) wird zwar in der Grafik als eigener Bereich darstellt, ist aber immer in Abhängigkeit vom IT-Betriebshandbuch und von der Projektdokumentation zu sehen. Bei der Schwachstellenanalyse legen Sie fest, welche Schäden durch Angriffe von Schad-Software zu erwarten sind, wie diese Angriffe abgewehrt werden können und wie erfolgreich die Abwehr der Angriffe ist.



Nur mit einer gut strukturierten Dokumentation können Sie sicherstellen, dass Sie keine wichtigen Punkte vergessen.

Als Schwachstellen werden nicht nur Angriffe durch Hacker oder Schad-Software bezeichnet, sondern auch Ausfälle von Client-Computern oder Servern. Zudem ist der Verlust von Daten durch versehentliches oder absichtliches Löschen Teil der Schwachstellenanalyse. Und auch Stromausfälle oder Wasserschäden gehören in diese Analyse.

Organisatorischer Teil: Welche Schutzmaßnahmen werden in Ihrem Unternehmen getroffen?

Dieser Bereich beschreibt, welche Maßnahmen getroffen werden, um die IT-Infrastruktur zu schützen. Hierunter fallen Virenscanner und Firewalls und deren Funktionsweise. In diesem Teil der Schwachstellenanalyse wird auch festgelegt, welche Personen für welche Schutzmaßnahmen zuständig sind. Außerdem wird hier festgehalten, wie Sicherheits-Updates und Virendefinitionen auf die Systeme verteilt werden. Legen Sie ebenfalls fest, ob Sicherheits-Updates vor der Installation getestet werden sollen.

Sofortmaßnahmen: Wie soll auf einen Ausfall reagiert werden?

Als Sofortmaßnahmen werden die Schutzmaßnahmen angesehen, die ein System in kürzester Zeit wiederherstellen. Hierzu gehören z. B. Live-CDs mit Virenscannern oder redundante Systeme wie beispielsweise ein Cluster oder ein Spanning-Tree, die beim Ausfall eines Systems den Betrieb trotzdem aufrechterhalten.

Krisenmanagement: Welche Maßnahmen sind für einen Schadensfall vorgesehen?

In möglichst detaillierten Schritt-für-Schritt-Anleitungen sollten Maßnahmen erfasst werden, die bei einem Schadensfall durchzuführen sind. Diese Maßnahmen sollten Sie mit Ihrem Team von Zeit zu Zeit üben, damit der Ablauf möglichst reibungslos erfolgen kann.

Geschäftsfortführungspläne: Wie werden geschäftskritische Prozesse aufrechterhalten?

In diesem Bereich wird festgehalten, welche Geschäftsprozesse besonders kritisch für ein Unternehmen sind. Für diese Prozesse werden getrennte Maßnahmen aufgesetzt, die eine möglichst schnelle Wiederaufnahme der Geschäftstätigkeit ermöglichen. Die großen Internet-Provider betreiben beispielsweise ein redundantes Rechnerzentrum, um Ausfallzeiten möglichst niedrig zu halten.

Ein redundantes Rechenzentrum zu betreiben, ist selbst für große Unternehmen kaum realisierbar. Sie können aber durchaus darüber nachdenken, eine redundante Infrastruktur in der Cloud aufzubauen.

Wiederanlaufpläne: Welche Maßnahmen sind vorgesehen, um den Status quo wiederherzustellen?

Parallel zu den Sofortmaßen müssen ebenfalls Maßnahmen getroffen werden, mit denen der Normalbetrieb wiederhergestellt werden kann. Hierzu gehören beispielsweise die Beschaffung neuer Hardware oder das Zurücksetzen von Servern oder Programmen auf zuvor definierte Standardeinstellungen.

So werden Sie aus einem Schaden klug

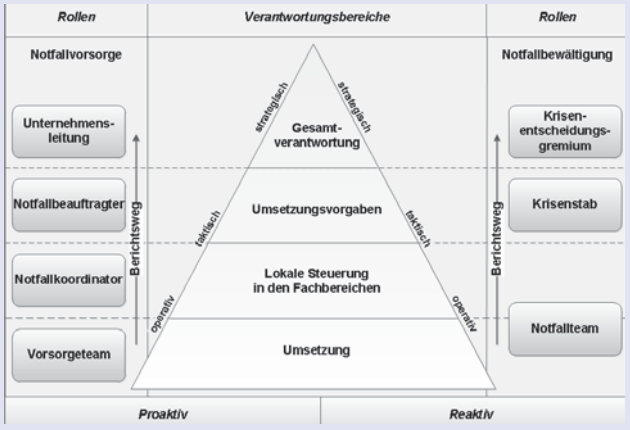
Ein wesentlicher Teil all dieser beschriebenen Punkte ist es, Melde- sowie Eskalationsprozesse festzuhalten. Der Meldeprozess beinhaltet eine Liste von Personen, die benachrichtigt werden müssen, wenn ein Schadensfall eintritt, z. B. die Hausverwaltung bei einem Wasserschaden oder die Geschäftsführung beim Ausfall eines geschäftskritischen Prozesses.

Bei einem Eskalationsprozess entscheiden Sie, welche Maßnahme Sie ergreifen, wenn eine andere Maßnahme fehlschlägt. So werden Sie im Allgemeinen einen Client-Computer oder Server mit den unterschiedlichsten Maßnahmen wiederherstellen, wenn das Betriebssystem ausfällt. Führen diese Maßnahmen nicht zum Ziel, werden Sie das Betriebssystem neu installieren. Diese Eskalationsprozesse werden in der Schwachstellenanalyse festgehalten

Nach einem behobenen Ausfall muss die Beseitigung des Schadens ebenfalls dokumentiert werden. Teile dieser Dokumentation sind Angaben zu folgenden Fragen:

- Was war die Ursache des Schadens?
- Wann und durch wen erfolgte die Schadensmeldung (Name, Datum, Uhrzeit)?
- Wann und durch wen erfolgte die Schadensbeseitigung (Name, Datum, Uhrzeit)?
- Wie wurde der Schaden behoben?
- Waren die Maßnahmen zur Beseitigung ausreichend beschrieben?
- Welche Eskalationsprozesse führten zum Ziel?

Wenn Sie beim Schreiben der Dokumentation feststellen, dass einige Maßnahmen unzureichend beschrieben sind oder dass wesentliche Teile fehlen, dann müssen diese Maßnahmen sofort korrigiert werden.



Wesentlich bei einer effizienten Schadensbehebung sind definierte Berichtswege und fest zugeteilte Rollen. (Quelle: Dr. Patrick Grete, BSI)

Mit diesen 4 Schritten optimieren Sie Ihre Fehlerbeseitigung durch Schwachstellenanalyse

Ein wesentlicher Nachteil der soeben beschriebenen Schwachstellenanalyse liegt darin, dass Sie immer nur auf Schwachstellen reagieren können. Einen Stromausfall oder Wasserschaden können Sie sicherlich nicht vorhersehen. Anders verhält es sich aber bei Schwachstellen, die durch das Betriebssystem oder Anwendungsprogramme verursacht werden. Die Fehler, die zu diesen Schwachstellen führen, sind in den Betriebssystemen und Programmen bereits vorhanden.

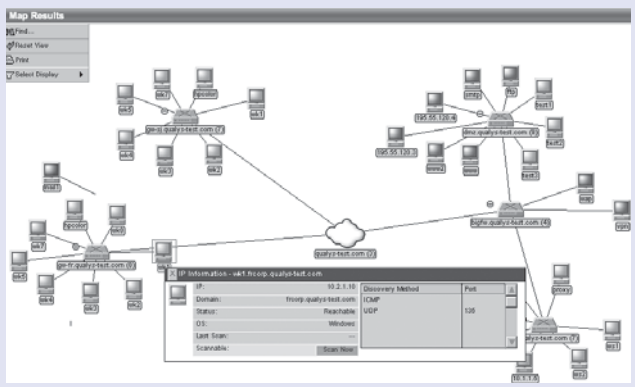
An dieser Stelle kommt das Schachstellen-Management (Vulneribility Management) mit den Schwachstellen-Scannern (Vulneribility Scanner) zum Einsatz. Das Schwachstellen-Management unter Zuhilfenahme von Schwachstellen-Scannern ist immer Teil der Dokumentation und sollte diese niemals ersetzen.

Hinweis: Wir zeigen Ihnen den typischen Ablauf eines Schwachstellen-Scans anhand des Programms „Qualys Guard“. Das Programm ist kostenpflichtig, ist aber als Trial-Version über die Webseite „**http://www.qualys.com/qualysguard-subscription-plans/**“ erhältlich. Sie müssen sich zuvor registrieren. Anstatt die Zugangsdaten aber über E-Mail zu verschicken, ruft Sie ein Mitarbeiter von Qualys an.

Die Schwachstellen-Scanner führen die folgenden Schritte durch, um mögliche Ausfälle herauszufinden:

1. Network Perimeter Map

Das gesamte Netzwerk wird gescannt und es wird eine Übersicht der gefundenen Geräte erstellt. Es können verschiedene Asset-Gruppen (Bestandsgruppen) angelegt werden und durch den Scan gefundene Geräte in diese Gruppen verschoben werden.



Diese Übersicht wird als Teil der Dokumentation abgelegt. (Quelle: Qualys)

2. Unbekannte interne Geräte

Hierbei handelt es sich möglicherweise um private Geräte, die Mitarbeiter zur Nutzung am Arbeitsplatz mitgebracht haben. Es können jedoch auch Geräte sein, die zu Spionage- oder anderen Zwecken eingeschleust wurden. In beiden Fällen wurden diese Geräte nicht von der IT-Abteilung freigegeben und entsprechen nicht den Sicherheitsanforderungen. Solche Geräte werden immer getrennt betrachtet und erst nach der Freigabe durch die IT-Abteilung ins Inventar aufgenommen.

3. Schwachstellenanalyse

Diese Analyse zeigt an, ob Dienste oder Programme Schwachstellen beinhalten. Die Berichte dieser Analyse enthalten Informationen zu Eigenschaften der Schwachstellen, Querverweise auf Schwachstellenklassifikationen und Informationsquellen mit Empfehlungen zur Beseitigung der Schwachstelle.

4. Report der anfälligsten Hosts

Die Scans der Schwachstellenanalyse werden gewichtet und es werden die besonders anfälligen Geräte aufgelistet.

5. Technischer Report zu Schwachstellen mit hohem Schweregrad

Neben der Liste der anfälligsten Hosts erhalten Sie eine Liste mit den Schwachstellen, die ein hohes Sicherheitsrisiko darstellen. Mit beiden Listen (anfälligste Hosts und Schwachstellen mit hohem Schweregrad) können Administratoren möglichen Ausfällen vorbeugen, indem sie sich zuerst um diese Geräte kümmern.

6. Web Application Scan

Die Besonderheit bei Webapplikationen ist, dass sowohl der Auslieferungs- als auch der Anlieferungszustand gescannt werden muss. Wenn Sie auf Ihren Web-Servern Programme oder Dateien zum Download bereitstellen, dann muss sichergestellt werden, dass die Schnittstelle fehlerfrei ist.

Sollen Mitarbeiter oder Besucher Daten auf einen Web-Server hochladen können, z. B. bei einem Content-Management-System, dann muss ebenfalls sichergestellt werden, dass über diese Schnittstelle keine Schad-Software auf den Web-Server geladen werden kann.

7. Schwachstellen-Trendreport

Wie bereits erwähnt können Sie bestimmte Geräte zu Asset-Gruppen zusammenfassen. Über diese Gruppen können Sie eine Trendanalyse durchführen, die Ihnen zeigt, wie sich das Risiko für einen bestimmten Zeitraum für Ihr Unternehmen verhält. In solchen Gruppen können Sie beispielsweise die BYOD-Geräte („**b**ring **y**our **o**wn **d**evice“) in Ihrem Unternehmen zusammenfassen und für diese Geräte dann eine Trendanalyse des Risikos durchführen.

8. Risikoanalyse-Report

Bei der Risikoanalyse wird ein bestimmtes Gerät oder eine bestimmt Asset-Gruppe auf eine Schwachstelle hin untersucht. Ein Grund dafür, diese Analyse durchzuführen, ist, dass Sie befürchten, dass ver-

schiedene Geräte eine Schwachstelle aufweisen könnten, ohne dass diese Schwachstelle in der Schwachstellenanalyse angezeigt wird.

9. Report zu offenen Tickets

Sie können zu jeder gefundenen Schwachstelle für ein Gerät oder eine Asset-Gruppe den Zeitpunkt für die Beseitigung festlegen. Der Report zu den offenen Tickets zeigt Ihnen, ob die gefundene Schwachstelle tatsächlich beseitigt wurde. Ist die Schwachstelle beseitigt, dann wird das Ticket geschlossen. Ansonsten bleibt das Ticket offen und kann in eine höhere Eskalationsstufe übertragen werden.

10. Überblick über die Schwachstellenbeseitigung

In dieser Liste sehen Sie, welche Schwachstellen in Ihrem System gefunden und beseitigt wurden. Sie sehen ebenfalls sämtliche geschlossenen und noch offenen Tickets. Die Dauer der Beseitigung der Schwachstellen bzw. die abgelaufene Zeit für die offenen Tickets kann Ihnen ein Hinweis dafür geben, welche Maßnahmen Sie treffen müssen, um die Schwachstellen schneller zu beseitigen. Möglicherweise müssen Sie für bestimmte Schwachstellen die Hilfe von Dienstleistern in Anspruch nehmen.

Sämtliche Reporte dieser Scans sind Teil der Dokumentation. Sie sollten ebenfalls darüber nachdenken, die Tickets zum Teil der Dokumentation zu machen. Sie können dann sehr schnell feststellen, wie lange es gedauert hat, bis bestimmte Schwachstellen beseitigt wurden. Möglichweise müssen Sie dann über eine Optimierung Ihrer Prozesse nachdenken.

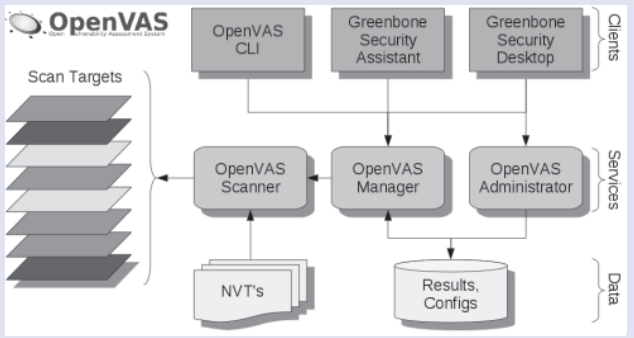
Mit diesen Scannern unterstützen Sie Ihre Schwachstellenanalyse

Schwachstellen-Scanner sind nach den verschiedensten Gesichtspunkten aufgebaut. So scannen einige ausschließlich Web-Server, andere stehen nur im Internet als Online-Scanner zur Verfügung. Die folgende Tabelle stellt Ihnen die wichtigsten Scanner vor:

Scanner	Beschreibung	Download
Freeware		
OpenVAS	**OpenVAS** (**Open V**ulnerability **A**ssessment **S**ystem) ist ein modulares System für die Schwachstellenanalyse. Der Scanner beinhaltet über 30.000 Tests (Stand April 2013), die ständig aktualisiert werden. Die Software ist über die GNU General Public License lizenziert. OpenVAS kann auf Linux- sowie Windows-Computern installiert werden. Unter Windows läuft aber nur das OpenVAS-CLI (**C**ommand **L**ine **I**nterface).	http://www.openvas.org/download-de.html Programmpaket und virtuelle Festplatte
Secunia PSI	Der **Personal Security Inspector** von Secunia ist ein Scanner, der die installierte Software auf einem Computer scannt und anschließend Lösungen für die Schwachstellenbeseitigung anbietet. Secunia PSI scannt nur den lokalen Rechner, auf dem das Programm installiert ist. Außerdem kann das Programm nur auf Windows-Computern installiert werden. Es steht eine Version für Android-Geräte zur Verfügung.	http://secunia.com/vulnerability_scanning/personal/
Kostenpflichtige Scanner		
Nessus 5.2	Mit über 55.000 Tests ist **Nessus** eines der mächtigsten Werkzeuge zur Schwachstellenanalyse. Das Programm lässt sich unter allen aktuellen Linux-, Unix-, Windows- und MAC-Betriebssystemen installieren. Bis zur Version 3 war das Programm kostenlos, aber mit der Version 4 wurde es kostenpflichtig.	http://www.tenable.com/products/nessus/select-your-operating-system
Nessus SecurityCenter	Anders als Nessus 5.2 beinhaltet das **SecurityCenter** eine Reihe zusätzlicher Programme. Hierzu gehört der **Nessus PVS** (**P**assiv **V**ulnerability **S**canner), der ähnlich wie ein Intrusion-Detection-System das Netzwerk in Echtzeit überwacht.	http://www.tenable.com/de/products/securitycenter/evaluate Die Testversion erhalten Sie nach Ihrer Registrierung bei Tenable.
Qualys Guard	Der Scanner ist in den Versionen Express Lite, Express und Enterprise erhält. Neben verschiedenen Funktionen, die in den einzelnen Versionen nicht implementiert sind, unterscheiden sich diese Versionen hauptsächlich darin, dass sie eine begrenzte Anzahl von Geräten scannen. Lediglich die Enterprise-Version erlaubt eine unbegrenzte Anzahl von Netzwerkgeräten.	http://www.qualys.com/qualysguard-subscription-plans/
Online-Scanner		
Qualys OVS (Online Vulnerability Scanner) **Secunia OSI (Online Security Inspector)**	Online-Scanner haben gemeinsam, dass sie einen Computer über die Webseite des jeweiligen Anbieters direkt scannen. Diese Variante der Schwachstellen-Scans bietet Ihnen einen ersten Überblick über die Anfälligkeit einzelner Geräte.	http://www.qualys.com/forms/freescan/de/
Web-Vulnerability-Scanner		
Acunetix	Der **Acunetix Web Vulnerabilty Scanner** untersucht ausschließlich Web-Server auf ihre Schwachstellen. Untersucht werden hierbei unter anderem das Cross Site Scripting, SQL Injection, Phishing und der Daten-Up- sowie -Downloads.	http://secunia.com/vulnerability_scanning/online/?task=load&lang=de

Die Praxis: So richten Sie „OpenVAS“ ein und führen gezielte Scans durch

Vor einigen Jahren hat das Bundesamt für Sicherheit in der Informationstechnik die „**B**SI **O**ss **S**ecurity **S**uite (BOSS)“ veröffentlicht. Die Suite diente zur Analyse der Sicherheit von Netzwerksystemen und basierte im Wesentlichen auf „Nessus“. Ab der Version basierte „BOSS“ ebenfalls auf „OpenVAS“, weshalb sich das BSI dazu entschieden hat, die Entwicklung von „BOSS“ aufzugeben und zukünftig die Nutzung von „OpenVAS“ zu empfehlen.



„OpenVAS“ basiert auf einer Reihe von Werkzeugen und Diensten, die modular aufgebaut sind. (Quelle: OpenVAS)

Über das „OpenVAS CLI“ (**C**ommand **L**ine **I**nterface) können eine Reihe von Kommandos abgesetzt werden, die die Vulnerability-Scans erweitern. Eine Liste der verfügbaren Kommandos inklusive Beispielen finden Sie unter der Webadresse „**http://www.openvas.org/omp-2-0.html**“. Klicken Sie dort auf den Link „**Command Details**“.

Außerdem können Sie verschiedene Plug-Ins einbinden. So erhalten Sie über die **N**etwork-**V**ulnerability-**T**ests (NVT), über 30.000 Tests, die Sie mit „OpenVAS“ durchführen können. Die NVTs werden bei der Installation aktualisiert.

Wie Sie „OpenVAS“ auf einem Debian-Server installieren

„OpenVAS“ können Sie als virtuelle Festplatte direkt auf einem Computer einbinden, dessen CPU die Virtualisierung zulässt. Die virtuelle Festplatte wurde im OVA-Format angelegt und kann über die Webadresse „**http://www.openvas.org/vm.html**“ abgerufen werden. Das Format stammt von der Virtualisierungs-Software „VMWare“ kann aber auch unter Oracles „VirtualBox“ eingebunden werden.

Hinweis: Wenn Sie die virtuelle Festplatte von „OpenVAS“ unter einem Hyper-V Server einbinden möchten, dann müssen Sie die virtuelle Festplatte zuerst in „VMWare“ konvertieren. Anschließend können Sie dann die virtuelle Festplatte auf dem Hyper-V Server einbinden.

„OpenVAS“ empfiehlt, die virtuelle Festplatte nur für Demo-Zwecke zu nutzen. Im Echtbetrieb benötigen die Scans zu viel Leistung, die eine virtuelle Maschine nicht hergeben würde.

Die Installation können Sie auf einem Linux-Server oder einem Windows-Computer vornehmen. Unter Windows steht aber lediglich das „OpenVAS CLI“ zur Verfügung. Wir empfehlen Ihnen die Installation von „OpenVAS“ auf einem Debian-Server. „OpenVAS“ kann sowohl unter „Debian Squeeze“ (Version 6) oder „Debian Wheezy“ (Version 7) installiert werden.

Hinweis: Wir haben beim Einsatz von „OpenVAS“ keinen Unterschied zwischen „Debian 6“ und „Debian 7“ herausfinden können. Sie sollten den Debian-Server aber ausschließlich für die Nutzung von „OpenVAS“ reservieren. Während der Installation werden Pakete installiert, die möglicherweise bereits mit einem anderen Programm in einer anderen Version installiert worden sind. Das kann dann zu Problemen führen.

In 7 Schritten einen „OpenVAS“-Server installieren und konfigurieren

Die Installation führen Sie mit den folgenden Schritten durch:

1. Öffnen Sie die Datei „**/etc/apt/sources.list**“ mit einem Editor und fügen Sie am Ende der Datei das Repository „**deb http://download.opensuse.org/repositories/security:/OpenVAS:/UNSTABLE:/v6/Debian_7.0/ ./**“ ein. Es soll die Version 6 von „OpenVAS“ auf einem Debian-7-Server installiert werden.
2. Mit dem Kommando „**wget http://download.opensuse.org/repositories/security:/OpenVAS:/UNSTABLE:/v6/Debian_7.0/Release.key**“ laden Sie den Release-Key von „OpenVAS“.
3. Diesen Key laden Sie in Ihre Debian-Schlüsselverwaltung mit dem Kommando „**apt-key add ./Release.key**“.
4. Mit dem Kommando „**apt-get update**“ aktualisieren Sie die Liste der Repositories aus der Datei „**/etc/apt/sources.list**“.

5. Der Befehl „**apt-get -y install greenbone-security-assistant openvas-cli openvas-manager openvas-scanner openvas-administrator sqlite3 xsltproc rsync**“ installiert schließlich unter anderem „OpenVAS“.
6. Mit den beiden folgenden Befehlen installieren Sie zusätzliche Programme. Diese werden unter anderem für das Reporting benötigt: „**apt-get -y install texlive-latex-base texlive-latex-extra texlive-latex-recommended htmldoc**“, „**apt-get -y install alien rpm nsis fakeroot**“.
7. Die Installation der benötigten Programmpakete ist damit abgeschlossen. In der Folge werden die Zertifizierungsschlüssel in „OpenVAS“ eingefügt und die aktuellsten Network-Vulnerability-Tests sowie die aktuellsten Plug-Ins geladen. Legen Sie für die folgenden Befehle am besten ein Skript an und führen Sie dieses Skript auf der Shell aus. Während der Ausführung werden Sie nach dem Passwort des neuen OpenVAS-Administrators „**admin**“ gefragt. Den Namen und das Passwort benötigen Sie für die Anmeldung an dem „OpenVAS“-Scanner.

Inhalt des Skripts:

```
1  test -e /var/lib/openvas/CA/cacert.pem || openvas-mkcert -q
2  openvas-nvt-sync
3  test -e /var/lib/openvas/users/om || openvas-mkcert-client -n om -i
4  /etc/init.d/openvas-manager stop
5  /etc/init.d/openvas-scanner stop
6  openvassd
7  openvasmd —rebuild
8  openvas-scapdata-sync
9  openvas-certdata-sync
10 test -e /var/lib/openvas/users/admin || openvasad -c add_user -n admin -r Admin
11 killall openvassd
12 sleep 15
13 /etc/init.d/openvas-scanner start
14 /etc/init.d/openvas-manager start
15 /etc/init.d/openvas-administrator restart
16 /etc/init.d/greenbone-security-assistant restart
```

So wird es gemacht: Zwei Web-Server auf Schwachstellen prüfen

Die Installation ist damit abgeschlossen und der „OpenVAS“-Server kann jetzt als „**localhost**“ über einen Web-Browser gestartet werden. Zuvor sollten Sie die Kommunikation aber noch so einstellen, dass von jedem Rechner in Netz der „OpenVAS“-Server über einen Web-Browser aufgerufen werden kann.

Öffnen Sie die Datei „**/etc/default/greenbone-security-assistant**“ und tragen Sie für die Variable „**GSA_ADDRESS**“ die IP-Adresse oder den Host-Namen Ihres „Open-VAS“-Servers ein: „**GSA_ADDRESS=*openvas-server***“. Schließen Sie die Datei und starten Sie „OpenVAS“ mit dem Kommando „**/etc/init.d/greenbone-security-assistant restart**“ neu.

Öffnen Sie einen belieben Browser und geben Sie in die Adresszeile „**https://*openvas-server*:9392**“ ein. Anstelle von „**openvas-server**“ müssen Sie natürlich die IP-Adresse oder den Host-Namen des „OpenVAS“-Servers eintragen.

Hinweis: Starten Sie einen Web-Browser direkt auf dem „OpenVAS“-Server, dann können Sie auch „**localhost**“ anstelle von „**openvas-server**“ eingeben. Der Start eines Web-Browsers auf dem „OpenVAS“-Server ist aber aus Sicherheitsgründen nicht zu empfehlen.

Es wird das Login-Fenster von „OpenVAS“ angezeigt. Tragen Sie hier den Namen und das Passwort ein, die Sie mit dem Kommando „**openvasad –c add_user**“ angelegt haben. „OpenVAS“ zeigt die Startseite an.

Richten Sie neue Hosts für die Schwachstellen-Scans ein

Wenn Sie weitere Tests durchführen möchten, dann müssen Sie zuerst neue Hosts im Bereich „**New Targets**“ einrichten. Bewegen Sie die Maus hierzu über das Menü „**Configuration**“, klicken Sie aber noch nichts an. Es öffnet sich ein Untermenü, hier klicken Sie auf „**Tasks**“.

Auf der jetzt angezeigten Webseite sehen Sie, dass „**localhost**“ bereits als Host eingetragen ist.

Hinweis: Ich möchte Ihnen im Folgenden zeigen, wie Sie zwei Web-Server scannen und dann auf Schwachstellen prüfen. Der eine Host ist ein Windows Server 2003, auf dem die **I**nternet **I**nformation **S**ervices (IIS) eingerichtet sind. Der zweite Host ist ein Windows Server 2008 auf dem ein Apache-Server installiert wurde. Auf diesem Server läuft das Content-Management-System „Joomla“.

Zum Einrichten von weiteren Hosts klicken Sie auf der Webseite „**Targets**“ auf den kleinen Stern in der Symbolleiste.

Es wird die Webseite „**New Targets**“ angezeigt. Vergeben Sie in dem Feld „**Name**“ einen Namen für den Host und tragen Sie in das Feld „**Hosts**“ hinter der Option „**Manual**“ den Namen oder die IP-Adresse des zu scannenden Hosts ein. Klicken Sie auf „**Create Target**“, um die Angaben für den Host zu speichern.

Hinweis: Wenn Sie die Option „**From file**“ auswählen, dann können Sie eine Datei angeben, in die Sie zuvor sämtliche Hosts in Ihrem Netz eingetragen haben. In diese Datei tragen Sie entweder die IP-Adressen oder die Host-Namen ein und trennen die Einträge durch ein Komma voneinander (beispielsweise: „**192.168.100.1, Apache-Server, IIS-Server, 192.168.100.100**“).

Klicken Sie auf „**Create Target**“, um die Angaben zu dem neuen Host zu speichern.

Legen Sie für jeden Host eine Aufgabe fest

Nachdem Sie die Hosts angelegt haben, müssen Sie für jeden Host eine neue Aufgabe einrichten. Teil dieser Aufgabe ist unter anderem die Genauigkeit des durchzuführenden Scans.

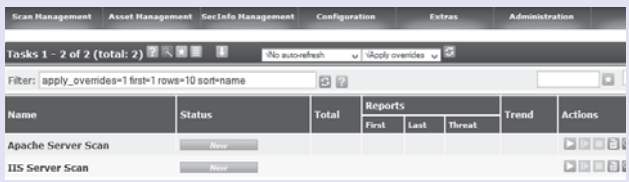
Bewegen Sie die Maus über das Menü „**Scan Management**“ und wählen Sie den Menüpunkt „**New Task**“ aus. Vergeben Sie einen Namen für die Aufgabe und wählen Sie den Server aus, der zu dieser Aufgabe gehört.

In dem Feld „**Scan Config**“ können Sie die Tiefe der Scans einstellen. Es stehen vier Optionen zur Verfügung:

- „**Full and fast**“,
- „**Full and fast ultimate**“,
- „**Full and very deep**“,
- „**Full and very deep ultimate**“.

Klicken zum Abschluss auf „**Create Task**“ um die Einträge für die Aufgabe abzuspeichern.

Auf der Startseite sehen Sie jetzt die beiden neuen Aufgaben mit den dazugehörigen Servern.



Klicken Sie auf das grüne Rechteck mit dem kleinen weißen Dreieck, um den Scanvorgang zu starten.

Führen Sie einen Scan durch und analysieren Sie die gefundenen Schwachstellen

Sie können beide Scanvorgänge parallel durchführen. Es ist aber besser, den Schwachstellen-Scan auf jedem Server getrennt durchzuführen.

Wenn Sie auf den Link der Task („**Apache Server Scan**“ oder „**IIS Server Scan**“) klicken, dann sehen Sie die Details zu dem gerade ausgeführten Scan. Auf dieser Webseite erhalten Sie nach dem abgeschlossen Scan auch die Berichte zu den gefundenen Schwachstellen.

Nach dem abgeschlossenen Schwachstellen-Scan zeigen beide Server ein hohes Sicherheitsrisiko an. Klicken Sie auf der Webseite „**Task Details**“ im Bereich „**Actions**“ unten rechts auf die Lupe, um sich anzeigen zu lassen, worin die Schwachstellen bestehen.

Auf dem Apache-Server erhalten wir die Meldung, dass eine PHP-Version installiert wurde, die kleiner als die aktuelle ist. Derzeit ist die Version 5.5 die aktuellste Version. Auf dem Apache-Server ist aber noch die Version 5.3.1 installiert. Der Grund dafür ist aber nicht der, dass die Administratoren nicht mit ihrer Arbeit nachgekommen wären. In der Version 5.5 sind deutliche Änderungen in einigen Funktionen gemacht worden, sodass die Administratoren sich dazu entschieden haben bei der Version 5.3.1 zu bleiben.

Der Apache-Server wird also die Version 5.3.1 so lange beibehalten, bis die Fehler beseitigt sind.

Sie sehen an diesem Bespiel sehr deutlich, dass die Hinweise des Schwachstellen-Scans zwar korrekt sind, aber nicht immer mit der Anforderungen eines Unternehmens übereinstimmen müssen.

Der zweite Server hat ebenfalls eine Warnung mit der Stufe „**High**“ erzeugt. Ursache dieser Meldung ist aber nicht die PHP-Version, sondern ein fehlender Sicherheits-Patch. Da es sich um einen fehlenden Sicherheits-Patch für das Remote Desktop Protocol handelt, muss in diesem Fall sofort nachgebessert.

Der Fehler auf dem IIS-Server zeigt, dass der organisatorische Teil der IT-Dokumentation unter Umständen noch Lücken besitzt. In diesem Bereich der Dokumentation wird festgehalten, in welchen Abständen die Sicherheits-Patches auf die Client-Computer und Server verteilt werden müssen. Entweder wurde für diesen Server eine Ausnahme definiert oder die Updates wurden schlichtweg vergessen.

Führen Sie eine Trendanalyse Ihrer Schwachstellen durch

Wenn Sie mit die Maus auf das Menü „**Asset Management**“ bewegen und anschließend den Menüpunkt „Hosts“ auswählen, wird die Webseite „**Host Filtering**“ angezeigt. Durch einen Klick auf die stilisierte Kristallkugel können Sie sich eine Trendanalyse der gefunden Schwachstellen anzeigen lassen.

Dieser Bericht zeigt Ihnen, wie sich eine bestimmte Schwachstelle auswirkt – immer vorausgesetzt, dass diese Schwachstelle nicht rechtzeitig beseitigt wird. Die Trendanalyse spricht Empfehlungen aus und verweist auf Internetseiten, damit Sie sich ein umfassendes Bild der möglichen Risiken machen können.

Wie das Beispiel des Apache-Servers zeigt, bleibt die Befolgung der Trendanalyse ganz alleine Ihre Sache.

Der schnelle Netzwerk-Check mit den Netzwerkdiagnose-Tools von Windows

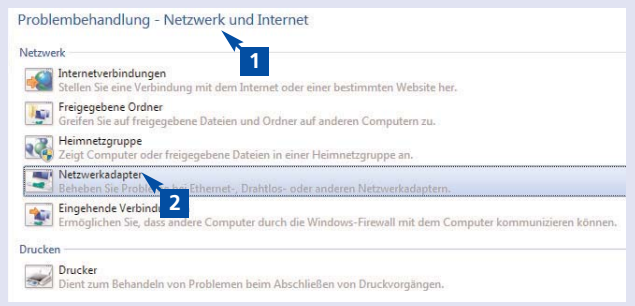
Sie müssen nicht unbedingt gleich Profi-Tools wie „PING“ oder „NETSH“ einsetzen, um die Ursache von Netzwerkfehlern aufzuspüren. Windows verfügt bereits über interne Diagnose-Tools, mit denen Sie Netzwerkprobleme schnell und erfolgreich lösen können. Mit der in Windows integrierten Tool-Sammlung für die Netzwerkdiagnose stehen Ihnen dazu grafische, HTML- und windowsbasierte Tools zur Verfügung, die sich per Mausklick einfach einsetzen lassen. Besonders in kleinen Netzwerken hat sich diese Tool-Sammlung als äußerst effektiv erwiesen.

Die Ursachen für ein fehlerhaftes Netzwerk sind oft banal. Eine falsche Einstellung kann schon ausreichen, um einen erfolgreichen Verbindungsaufbau zu unterbinden. Doch Windows ist mit einem ganzen Sortiment an Tools ausgestattet, mit denen Sie die Ursache von Netzwerkproblemen ausfindig machen können.

Neben den bekannten Tools wie „PING“ etc. finden Sie in Windows vier zusätzliche Tools: Die „**Netzwerkdiagnose**“, die Registerkarte „**Support**“ unter „**Netzwerkverbindungen**“ bzw. im „**Netzwerk- und Freigabecenter**“, den Link „**Reparieren**“ unter „**Netzwerkverbindungen**“ und die Registerkarte „**Netzwerk**“ im Task-Manager.

Nutzen Sie die „Netzwerkdiagnose“ in Windows 78/

Wenn Sie in Windows 7 in der „**Systemsteuerung**“ das „**Netzwerk- und Freigabecenter**“ öffnen und auf den Link „**Probleme beheben**“ 1 klicken, bestimmen Sie als Nächstes, welches Netzwerkproblem 2 Sie beheben möchten.



Klicken Sie das zu lösende Netzwerkproblem an und folgen Sie den Anweisungen.

Je nach gewählter Problemart erscheinen im nächsten Schritt einige Fragen, die das Problem näher spezifizieren. Markieren Sie die entsprechenden Antworten und klicken Sie anschließend auf „**Weiter**“.

Wenn das Problem nicht behoben werden konnte, listet die Windows-7-Problembehandlung mehrere Optionen auf, mit denen Sie online nach einer Antwort suchen können. Beachten Sie auch die Liste der vorgenommenen Änderungen.

Konnte das Problem nicht gelöst werden, starten Sie die Problembehandlung erneut und klicken auf den Link „**Erweitert**“. Anschließend können Sie die Option „**Als Administrator ausführen**“ verwenden. Diese Option führt mehr Reparaturaktionen aus und löst auch hartnäckige Probleme.

Klicken Sie auf den Link „**Erweitert**“ in einer Problembehandlung und deaktivieren dann das Kontrollkästchen „**Reparaturen automatisch anwenden**“, wird eine Liste der Korrekturen zur Auswahl angezeigt, wenn Probleme gefunden wurden.

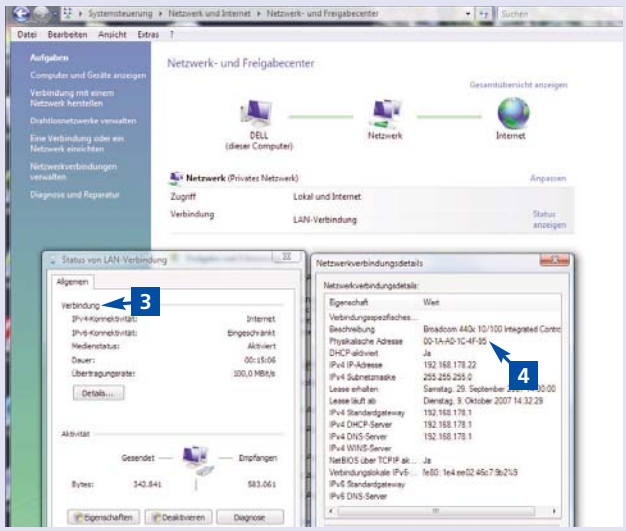
Die „Netzwerkunterstützung“ leistet wirkungsvolle Hilfe

Zur Fehlersuche in einem Netzwerk benötigen Sie Informationen über wichtige IP-Konfigurationseinstellungen im LAN- bzw. WLAN-Adapter. In Windows 7/8 öffnen Sie dazu das „**Netzwerk- und Freigabecenter**“

Im oberen Teil des Fensters finden Sie die Darstellung Ihres Netzwerks in grafischer Form. Diese zeigt alle Verbindungen ins Netzwerk und ins Internet. Über jede in Ihrem Rechner eingebaute Netzwerkkarte können Sie sich mit einem eigenen Netzwerk verbinden.

In der rechten Spalte des „**Netzwerk- und Freigabecenters**“ finden Sie eine Übersicht über die Zustände verschiedener Einstellungen, wie die Freigabe von Verzeichnissen und Druckern 3.

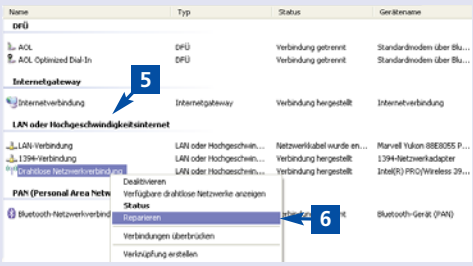
Im „**Netzwerk- und Freigabecenter**“ können Sie sich durch den Doppelklick auf verschiedene Elemente im Detail über die IP- und MAC-Adressen von Computern, Routern etc. informieren 4.



So können Sie in Windows 7/8 den Netzwerkstatus überprüfen.

Die Schnellreparatur mit dem Link „Reparieren" für Netzwerkverbindungen

Mit der Schnellreparatur beheben Sie mehrere mögliche Netzwerkprobleme auf einen Schlag. Öffnen Sie dazu das „**Netzwerk- und Freigabecenter**", klicken Sie am linken Rand des Fensters auf „**Adaptereigenschaften ändern**", wählen Sie den fehlerhaften Adapter aus 5, klicken Sie ihn mit der rechten Maustaste an und klicken Sie anschließend im Kontextmenü auf „**Reparieren**" 6.



So starten Sie den Link „**Reparieren**" 6.

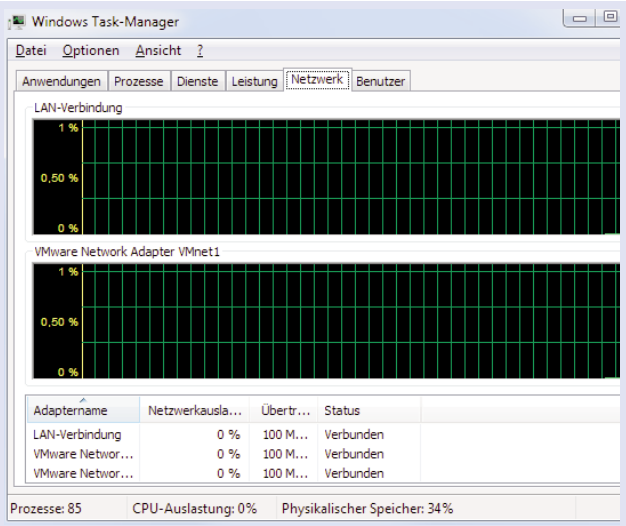
Die automatische Reparaturfunktion führt sechs Schritte zur Fehlerbehebung durch, die in der folgenden Tabelle in der Reihenfolge ihrer Ausführung beschrieben werden.

Maßnahme	Beschreibung
DHCP-Lease-Erneuerung per Broadcast	Hierbei handelt es sich um das Äquivalent einer DHCP-Broadcast-Erneuerung bei 87,5 Prozent der Lease-Dauer. Diese Option wurde ausgewählt, weil sie weit sicherer als eine tatsächliche DHCP-Freigabe mit anschließender DHCP-Erneuerung ist. Wenn ein DHCP-Server nicht zur Erneuerung der Adresse verfügbar ist, behält Ihr Computer die gegenwärtig verwendete bei. Wenn ein neuer DHCP-Server online ist, kann dieser ein NACK-Signal an den Client senden und den Lease-Prozess neu starten und damit potenziell die IP-Adressprobleme eines Computers beheben.
Leeren des ARP-Caches	Gelegentlich ist ein ARP-Cache-Eintrag so veraltet, dass keine Datenübertragung mehr möglich ist, bis der fehlerhafte ARP-Cache-Eintrag abgelaufen ist. Außerdem besteht die Möglichkeit, dass ein fehlerhafter statischer ARP-Cache-Eintrag auf dem Computer gespeichert wurde, dessen Gültigkeit nicht abläuft. Der ARP-Cache wird normalerweise in Zwei- und Zehn-Minuten-Intervallen geleert, sodass dieser Vorgang als sicher eingestuft wird.
Nbtstat –R	Oftmals sind im NetBIOS-Cache veraltete Einträge vorhanden, die eine Datenübertragung verhindern. In diesem Schritt wird einfach der NetBIOS-Namens-Cache gelöscht und alle NetBIOS-Namenseinträge in der Datei „Lmhosts" mit dem Flag „#PRE" werden neu geladen.
Nbtstat -RR	Dieser Schritt entspricht der Neuregistrierung der Computernamen auf einem WINS-Server. Dies kann beim Beheben von Problemen mit der NetBIOS-Namensauflösung sehr hilfreich sein. Es sollte beachtet werden, dass „Nbtstat -RR" – und damit die Reparaturfunktion – die Namensaktualisierung einfach entsprechend dem Zeitplan des Betriebssystems durchführt und die Ausgabe erfolgt, ohne dass überprüft wird, ob die Aktualisierung erfolgreich war.
Leeren des DNS-Caches	Hierdurch werden die DNS-Cache-Einträge aus dem Arbeitsspeicher gelöscht und alle potenziell alten oder fehlerhaften Name-IP-Zuordnungen geleert. Dies kann beim Beheben von Problemen mit der DNS-Namensauflösung sehr hilfreich sein.
Registrieren des DNS-Namens	Dieser Schritt entspricht einer Neuregistrierung des DNS-Namens des Computers auf einem dynamischen DNS-Server.

Kontrollieren Sie alle Aktivitäten im Netzwerk mit dem Task-Manager

Fehler bei Netzwerkverbindungen können Sie auch über die Analyse des Netzwerkverkehrs aufspüren. Der Task-Manager unterstützt Sie dabei, beispielsweise bei der Fehleranalyse einer Netzwerküberlastung, denn das Tool gibt grafisch einen schnellen Überblick über die Netzwerkverfügbarkeit. Es zeigt alle LAN-Verbindungen und ausgehenden WAN-Verbindungen an. Eingehende WAN-Verbindungen werden aber nicht überwacht.

Um die Netzwerkaktivitäten zu überprüfen, drücken Sie gleichzeitig die Tasten Strg+Alt+Entf. Öffnen Sie den „**Task-Manager**" und wechseln Sie auf die Registerkarte „**Netzwerk**".



Die Registerkarte „**Netzwerk**" im Task-Manager von Windows 7.

Einsatz der Netzwerkdiagnose-Tools in der Praxis

Die Netzwerkdiagnose-Tools sind mit etlichen Mechanismen zur Unterstützung bei der Diagnose und Behebung von Netzwerkproblemen ausgestattet. Wenn Sie ein Netzwerkproblem zu lösen haben, so versuchen Sie erst einmal, sich einen Überblick über die Netzwerkkonfiguration zu verschaffen. Diese Analyse nehmen Ihnen die Analyse-Tools vollkommen ab, denn sie ermitteln:

- worauf Sie zugreifen möchten.
- wie Ihre IP-Adresse lautet.
- ob Sie WINS oder DNS verwenden.
- ob Sie Namen auflösen können.
- ob Sie IP-Adressen auflösen können.

Damit kombinieren die Netzwerkdiagnose-Tools mehrere Standard-Tools, wie z. B. „PING", für die Fehlerbehebung. Anhand dieser Informationen können Sie dann versuchen, den Fehler zu beheben.

Lösen Sie mit drei Standard-Tools jeden Netzwerkfehler

Sparen Sie sich das Geld für teure Netzwerk-Troubleshooting-Tools. Windows verfügt mit „ipconfig“, „nbtstat“ und „net view“ über drei Profi-Werkzeuge, mit denen Sie Ihr Netzwerk jederzeit reparieren können. Es kommt nur auf die Reihenfolge der Befehle und die passenden Parameter an und schon läuft das Netzwerk wieder.

Überprüfen Sie bei Problemen in einem Netzwerk die Einstellungen der TCP/IP-Netzwerkkonfiguration mit diesen drei Diagnose-Tools:

- „Ipconfig.exe“ zeigt die aktuelle TCP/IP-Konfiguration an.
- „Nbtstat.exe“ zeigt alle Verbindungsinformationen an.
- Mit „net view“ testen Sie die Netzwerkverbindungen.
- „Tracert.exe“ prüft die Verbindung zu einem Server oder Router und gibt den Pfad dorthin aus.
- „Ping.exe“ prüft die Verbindung zu einem Server oder Router und gibt die Verbindungsgeschwindigkeit aus.

1. Schritt: Prüfen Sie die aktuelle TCP/IP-Konfiguration mit „Ipconfig.exe“

„Ipconfig“ zeigt Ihnen DNS-Suffix, IP-Adresse, Subnetzmaske und Standard-Gateway des Computers an. Und so setzen Sie das Tool ein:

1. Öffnen Sie eine Eingabeaufforderung und geben Sie dort „**ipconfig**“ ein.
2. Benötigen Sie zusätzliche Informationen und einen detaillierten Konfigurationsbericht, geben Sie „**ipconfig /all**“ ein.
3. Vergewissern Sie sich, dass der Computer die richtigen Einstellungen für DNS- (**D**omain **N**ame **S**ystem) und WINS-Server (**W**indows **I**nternet **N**ame **S**ervice), eine verfügbare IP-Adresse, die richtige Subnetzmaske, das richtige Standard-Gateway und den richtigen Host-Namen aufweist.

2. Schritt: Verbindungsinformationen mit „Nbtstat.exe“ anzeigen

Bei NetBIOS über TCP/IP (NetBT) werden NetBIOS-Namen in IP-Adressen aufgelöst. TCP/IP stellt viele Optionen für die NetBIOS-Namensauflösung zur Verfügung, z. B. lokalen Cache-Lookup, WINS-Server-Abfrage, Broadcast, DNS-Server-Abfrage sowie LMHOSTS- und HOSTS-Lookup.

„Ntbtstat“ ist ein nützliches Tool zur Behandlung von Problemen mit der NetBIOS-Namensauflösung. Sie können „Ntbtstat“ zum Entfernen oder Korrigieren von vorab geladenen Einträgen verwenden.

So setzen Sie „Ntbtstat“ in der Eingabeaufforderung wirkungsvoll ein:

- Mit dem Befehl „**nbtstat –n**“ erhalten Sie die NetBIOS-Namenstabelle des lokalen Computers. Dieser Tabelle können Sie entnehmen, ob es sich bei den jeweiligen Namen um eindeutige Namen oder um Gruppennamen handelt. Außerdem können Sie feststellen, ob die Namen im Netzwerk registriert sind oder nicht.
- Mit „**nbtstat –c**“ wird Ihnen der Inhalt des NetBIOS-Namenszwischenspeichers angezeigt, also die Zuordnungen von Namen zu Adressen für andere Computer.
- Mit „**nbtstat –R**“ („**R**“ als Großbuchstabe) löschen Sie den Inhalt des NetBIOS-Namenszwischenspeichers mit dem Ergebnis, dass die Namen neu aus der Datei „LMHOSTS“ geladen werden.
- Mit „**nbtstat –a Remote-Computer-Name**“ wird Ihnen die Namenstabelle eines Remote-Computers angezeigt (dabei steht „**Remote-Computer-Name**“ für den NetBIOS-Computernamen des Remote-Computers). Sie erhalten die lokale NetBIOS-Namenstabelle für diesen Computer und die MAC-Adresse des Netzwerkadapters zurück.
- Mit „**nbtstat –s**“ wird Ihnen eine Liste der Client- und Server-Verbindungen angezeigt, also die aktuellen NetBIOS-Sitzungen und ihr Status einschließlich Statistiken.

Lokaler Name	Zustand	Ein/Aus	Remotehost	Eingabe	Ausgabe
PC-MAC1 <00>	Verbunden	Aus	CNSSUP1<20>	6MB	5MB
PC-MAC1 <00>	Verbunden	Aus	CNSPRINT<20>	10KB	16KB
PC-MAC1 <00>	Verbunden	Aus	CNSSRC1<20>	299KB	19KB
PC-MAC1 <00>	Verbunden	Aus	STH2NT<20>	324KB	19KB
PC-MAC1 <03>	Abhören				

„Nbtstat.exe“ zeigt Ihnen alle Verbindungsinformationen.

3. Schritt: Verbindungen testen mit dem Befehl „net view“

Der Befehl „**net view**“ erstellt eine Liste der Datei- und Druckerfreigaben des jeweiligen Computers, indem eine temporäre NetBIOS-Verbindung aufgebaut wird.

Geben Sie dazu in der Eingabeaufforderung „**net view \\Computername**“ ein, wobei „**Computername**“ der Name des Computers ist, zu dem Sie eine Verbindung herstellen wollen.

Wenn keine Datei- oder Druckerfreigaben auf dem angegebenen Computer verfügbar sind, erhalten Sie die Meldung: „Es sind keine Einträge in der Liste.“

Falls der Befehl „**net view \\Computername**“ nicht funktioniert und Ihnen die Meldung „Ein Systemfehler ist aufgetreten“ angezeigt wird, gehen Sie bitte folgendermaßen vor:

- Überprüfen Sie, ob Sie den richtigen Namen für den Remote-Computer eingegeben haben.
- Vergewissern Sie sich, dass die Datei- und Druckerfreigabe für den Microsoft-Netzwerkdienst auf dem Computer ausgeführt wird.
- Prüfen Sie mit „**ping**“, dass alle Gateways (Router) zwischen dem lokalen Computer und dem Remote-Host funktionsfähig sind.

In manchen Fällen ist zwar eine direkte Verbindung mit einer Netzwerkressource möglich, wenn Sie jedoch einen Ping an die Ressource senden, wird immer „Zeitüberschreitung der Anforderung“ zurückgegeben.

Wahrscheinlich wurde aus Sicherheitsgründen die Rückgabe von ICMP-Paketen (Ping) blockiert. Deshalb erhalten Sie keine Antwort auf eine „Ping“- oder „Tracert“-Nachricht.

So testen Sie die Verbindungen mit Remote-Servern

Bei Problemen bei einer Verbindung zu einem Remote-Server testen Sie zuerst mit „**ping**“ die Verbindung zu diversen Netzwerkressourcen. In die Eingabeaufforderung geben Sie dazu den Befehl „**ping**“ ein, gefolgt von der IP-Adresse des Remote-Netzwerk-Hosts oder des Host-Namens, beispielsweise:

```
ping 192.168.104
ping www.microsoft.com
```

Bei einer funktionierenden Verbindung sieht die Antwort folgendermaßen oder ähnlich aus:

```
Antwort von 192.168.1.104: Bytes=32 Zeit=40ms TTL=61
Antwort von 192.168.1.104: Bytes=32 Zeit=40ms TTL=61
```

Können Sie keine Verbindung zu der Ressource herstellen, grenzen Sie das Problem ein, indem Sie mit einem Ping die Verbindung zu verschiedenen Netzwerkressourcen testen:

- Pingen Sie die Loopback-Adresse mit „**ping 127.0.0.1**“ an.
- Senden Sie einen Ping an die IP-Adresse eines lokalen Computers.
- Senden Sie den Ping-Befehl an die IP-Adresse des Standard-Gateways.

Mit „Tracert.exe“ ermitteln Sie die Route des Netzwerkpfades zu einem bestimmten Ziel. Das Tool zeigt an, welche IP-Router bei der Übermittlung von Paketen von Ihrem Computer zu einem bestimmten Ziel verwendet werden. Außerdem wird die Zeitspanne angezeigt, die das Paket zum Erreichen der einzelnen Netzwerksegmente benötigt hat. Sollten Pakete das gewünschte Ziel nicht erreichen, gibt der Befehl „**tracert**“ den Namen des letzten Routers zurück, der das Paket erfolgreich weiterleiten konnte. So ermitteln Sie den Pfad, den ein Paket im Netzwerk durchläuft, und das mögliche Endes dieses Pfades. Geben Sie dazu in der Eingabeaufforderung den Befehl „**tracert**“ gefolgt von der IP-Adresse des Remote-Netzwerk-Hosts ein, z. B. „**tracert 192.168.120.200**“.

3 Befehle für fehlerfreie TCP/IP-Verbindungen in Ihrem Netzwerk

In nahezu jedem Netzwerk läuft der Datentransfer über das Standard-Netzwerkprotokoll TCP/IP. Doch nicht immer funktioniert ein Netzwerk fehlerfrei. Nun sind Sie als Administrator gefragt: Mit nur drei Befehlen führen Sie eine Schnelldiagnose durch und überprüfen alle Einstellungen der TCP/IP-Netzwerkkonfiguration.

Windows und die Server-Betriebssysteme stellen Ihnen verschiedene Diagnosetools und Techniken für die Netzwerkanalyse zur Verfügung:

- Überprüfen Sie die aktuelle TCP/IP-Konfiguration mit „**Ipconfig.exe**“.
- Prüfen Sie die Verbindungsinformationen mit „**Nbtstat.exe**“.
- Testen Sie die Verbindungen zu Ihren Remoteservern.
- Kontrollieren Sie TCP/IP-Verbindungen mit dem Befehl „**NET VIEW**“.

Überprüfen Sie die aktuelle TCP/IP-Konfiguration mit „Ipconfig.exe“

„IPCONFIG“ zeigt Ihnen DNS-Suffix, IP-Adresse, Subnetzmaske und Standardgateway des Computers an.

1. Öffnen Sie eine Eingabeaufforderung (**cmd**) und geben dort „**ipconfig**“ ein.
2. Benötigen Sie zusätzliche Informationen und einen detaillierten Konfigurationsbericht, geben Sie „**ipconfig /all**“ ein.
3. Vergewissern Sie sich, dass der Computer die richtigen Einstellungen für DNS- (DNS = **D**omain **N**ame **S**ystem) und WINS-Server (WINS = **W**indows **I**nternet **N**ame **S**ervice), eine verfügbare IP-Adresse, die richtige Subnetzmaske, das richtige Standardgateway und den richtigen Hostnamen aufweist.

fernen oder Korrigieren von vorab geladenen Einträgen verwenden. So setzen Sie NBTSTAT in der Eingabeaufforderung wirkungsvoll ein:

- Mit dem Befehl „**nbtstat –n**“ erhalten Sie die NetBIOS-Tabelle des lokalen Computers. Durch diesen Befehl wird die lokale NetBIOS-Namenstabelle angezeigt. Dieser Tabelle können Sie entnehmen, ob es sich bei den jeweiligen Namen um eindeutige Namen oder Gruppennamen handelt. Außerdem können Sie feststellen, ob die Namen im Netzwerk registriert sind oder nicht.
- Mit „**nbtstat –c**“ wird Ihnen der Inhalt des NetBIOS-Namenzwischenspeichers angezeigt, also die Zuordnungen von Namen zu Adressen für andere Computer.
- Mit „**nbtstat –R**“ („R“ als Großbuchstabe) löschen Sie den Inhalt des NetBIOS-Namenzwischenspeichers mit dem Ergebnis, dass die Namen neu aus der Datei „LMHOSTS“ geladen werden.
- Mit „**nbtstat –a Remotecomputername**“ wird Ihnen die Namenstabelle eines Remotecomputers angezeigt (dabei steht Remotecomputername für den NetBIOS-Computernamen des Remotecomputers). Sie erhalten die lokale NetBIOS-Namenstabelle für diesen Computer und die MAC-Adresse des Netzwerkadapters zurück.
- Mit „**nbtstat –s**“ wird Ihnen eine Liste der Client- und Serververbindungen angezeigt, also die aktuellen NetBIOS-Sitzungen und ihr Status einschließlich Statistiken.

Lokaler Name	Zustand	Ein/ Aus	Remotehost	Eingabe	Ausgabe
PC-MAC1 <00>	Verbunden	Aus	CNSSUP1<20>	6MB	5MB
PC-MAC1 <00>	Verbunden	Aus	CNSPRINT<20>	108KB	116KB
PC-MAC1 <00>	Verbunden	Aus	CNSSRC1<20>	299KB	19KB
PC-MAC1 <00>	Verbunden	Aus	STH2NT<20>	324KB	19KB
PC-MAC1 <03>	Abhören				

„Nbtstat.exe“ zeigt Ihnen alle Verbindungsinformationen

Testen Sie die Verbindungen zu Ihren Remoteservern

Bei Problemen bei einer Verbindung zu einem Remoteserver kommen zwei Tools zum Einsatz:

- Mit **PING** vergewissern Sie sich, dass ein Hostcomputer eine Verbindung mit dem TCP/IP-Netzwerk und den Netzwerkressourcen herstellen kann.
- Mit **TRACERT** untersuchen Sie die Route, auf der ein bestimmtes Ziel erreicht wird.

Mit PING testen Sie die Verbindung zu diversen Netzwerkressourcen. In der Eingabeaufforderung geben Sie dazu den Befehl PING ein, gefolgt von der IP-Adresse des Remote-Netzwerkhosts oder des Hostnamens, beispielsweise:

```
ping 192.168.104
ping www.netzwerk-administrator.com
```

Bei einer funktionierenden Verbindung sieht die Antwort folgendermaßen oder ähnlich aus:

```
Antwort von 192.168.1.104: Bytes=32 Zeit=40ms TTL=61
Antwort von 192.168.1.104: Bytes=32 Zeit=40ms TTL=61
```

Können Sie keine Verbindung zu der Ressource herstellen, grenzen Sie das Problem ein, indem Sie mit PING die Verbindung zu verschiedenen Netzwerkressourcen testen:

- Pingen Sie die Loopback-Adresse an, um sicherzustellen, dass TCP/IP auf dem lokalen Computer installiert ist und korrekt funktioniert. Geben Sie hierzu „**ping 127.0.0.1**“ ein.
- Senden Sie den Ping-Befehl an die IP-Adresse des lokalen Computers, um sicherzustellen, dass dieser dem Netzwerk ordnungsgemäß hinzugefügt wurde.
- Senden Sie den Ping-Befehl an die IP-Adresse des Standardgateways, um sicherzustellen, dass das Gateway funktioniert und dass eine Verbindung mit einem lokalen Host im lokalen Netzwerk hergestellt werden kann. Sie können die IP-Adresse des lokalen Standardgateways mit dem Befehl IPCONFIG ermitteln.
- Senden Sie den Ping-Befehl an die IP-Adresse eines anderen Remotehosts, um sicherzustellen, dass die Kommunikation über einen Router möglich ist.

Mit „**Tracert.exe**“ ermitteln Sie die Route des Netzwerkpfades zu einem bestimmten Ziel. Das Tool zeigt an, welche IP-Router bei der Übermittlung von Paketen von Ihrem Computer zu einem bestimmten Ziel verwendet werden. Außerdem wird die Zeitspanne angezeigt, die das Paket zum Erreichen der einzelnen Netzwerksegmente benötigt hat. Sollten Pakete das gewünschte Ziel nicht erreichen, gibt der Befehl TRACERT den Namen des letzten Routers zurück, der das Paket erfolgreich weiterleiten konnte. So ermitteln Sie den Pfad, den ein Paket im Netzwerk durchläuft, und das mögliche Endes dieses Pfades. Geben Sie dazu in der Eingabeaufforderung den Befehl TRACERT, gefolgt von der IP-Adresse des Remote-Netzwerkhosts ein, z. B. „**tracert 192.168.120.200**“.

Kontrollieren Sie TCP/IP-Verbindungen mit dem Befehl „NET VIEW“

Der Befehl „NET VIEW“ erstellt eine Liste der Datei- und Druckerfreigaben des jeweiligen Computers, indem eine temporäre NetBIOS-Verbindung aufgebaut wird.

Geben Sie dazu in der Eingabeaufforderung „**net view \\Computername**“ ein, wobei „Computername“ der Name des Computers ist, zu dem Sie eine Verbindung herstellen wollen.

Wenn keine Datei- oder Druckerfreigaben auf dem angegebenen Computer verfügbar sind, erhalten Sie die Meldung „Es sind keine Einträge in der Liste“.

Schnelles Exchange-Troubleshooting mit einem neuen kostenlosen Tool

Was tun, wenn Exchange meldet, dass der Server inaktiv oder nicht erreichbar sei? Ursachen dafür gibt es viele: von den klassischen Netzwerkproblemen bis hin zu fehlerhaften Exchange-Konfigurationen. Microsoft hat sich dieser Problematik angenommen und ein webbasiertes Tool erstellt, das sich „ExRCA“ nennt. Nutzen Sie „ExRCA“, wenn Ihr Exchange nicht mehr funktioniert.

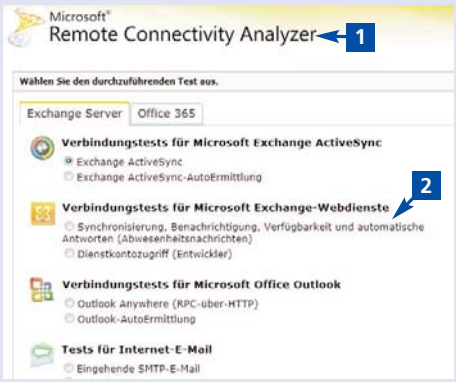
„ExRCA“ steht für „**Ex**change Server **R**emote **C**onnectivity **A**nalyzer“ und testet die Remote-Konnektivität von Exchange. Sie können „ExRCA“ zum Testen sowohl von cloudbasierten als auch von lokalen Exchange-Organisationen verwenden. Der „Exchange Server Analyzer“ trägt remote Konfigurationsdaten von allen Servern in der Topologie zusammen und analysiert diese Daten automatisch. Der aus der Analyse erstellte Bericht enthält ausführliche Informationen zu bestehenden Konfigurationskonflikten, möglichen Problemen und Einstellungen, die nicht den Standardvorgaben entsprechen. Nutzen Sie die Empfehlungen des Berichts, um damit die Leistung, Skalierbarkeit und Zuverlässigkeit Ihres Exchange-Servers zu verbessern. Getestet werden dabei

- die Übermittlung eingehender SMTP-Nachrichten,
- die Outlook-Verbindungen mit einem Postfach,
- die Exchange-ActiveSync-Verbindungen mit einem Postfach,
- die Verbindungseinstellungen für einen lokalen E-Mail-Server, wenn Sie die Postfächer und E-Mails in eine cloudbasierte Organisation migrieren wollen.

So testen Sie Ihr Exchange online

Der Test wird online über die URL „**https://www.testexchangeconnectivity.com/**“ 1 ausgeführt. Auf der Webseite können Sie den auszuführenden Test 2 dann starten.

Je nach ausgewähltem Test geben Sie in der nächsten Eingabemaske die für den Test erforderlichen Daten



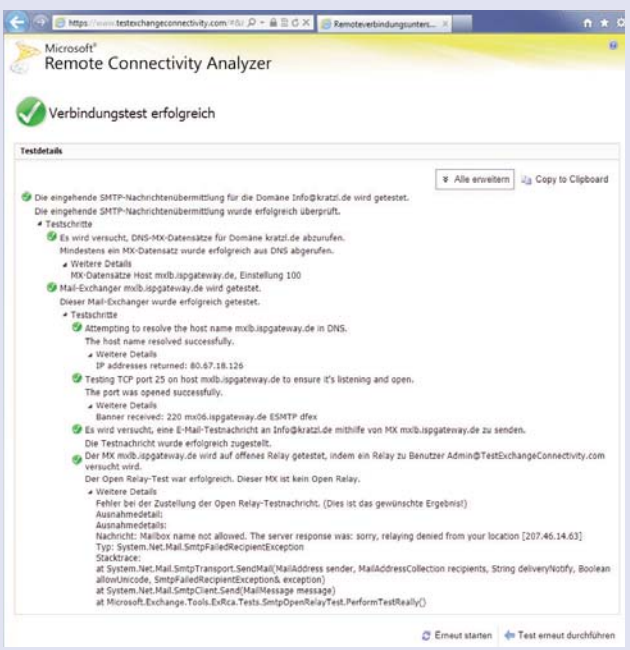
Starten Sie das webbasierte Tool „ExRCA“ über die angegebene Webadresse und markieren Sie den gewünschten Test.

ein, wie beispielsweise die E-Mail-Adresse, die Domäne, das Administratorkonto und das dazugehörige Passwort.

Sicherheitstipp: Da es sich um ein webbasiertes Tool handelt, sollten Sie für den Test ein neues Benutzerkonto anlegen, das Sie nach Abschluss aller Tests wieder löschen. Denn für die Durchführung der Tests sind Angaben wie das Administratorpasswort unerlässlich und die Eingabe solch hochsensibler Daten in einem webbasierten Tool birgt enorme Risiken.

Wie Sie die Testergebnisse auswerten

Egal, ob der Test erfolgreich oder nicht erfolgreich ausgeführt wurde, Sie erhalten im Anschluss einen zusammenfassenden Bericht.



Bei diesem Test wurden laut Bericht keine Fehler festgestellt.

Anhand der einzelnen Testschritte können Sie bei Problemen die Fehlerursache schnell ausfindig machen. Mehr Detailinformationen erhalten Sie durch Öffnen der Details über „+“.

Lösen Sie Probleme mit „ExRCA“ schnell und erfolgreich

Nicht immer funktioniert „ExRCA“ einwandfrei. Unter Umständen erhalten Sie eine Fehlermeldung, dass auf die Registrierung auf einem Cluster-Knoten nicht remote zugegriffen werden konnte. Ein Zugriff ist aber erforderlich, denn „ExRCA“ trägt die Konfigurationsdaten von allen Servern in der Topologie zusammen und analysiert diese Daten automatisch. Um dieses Problem zu beheben, führen Sie folgende Schritte aus:

- ☐ Vergewissern Sie sich, dass der Remote-Registrierungsdienst auf allen Knoten im Cluster ausgeführt wird.
- ☐ Vergewissern Sie sich, dass der Server-Dienst aktiviert ist und auf dem Computer mit dem Exchange-Server ausgeführt wird.
- ☐ Stellen Sie sicher, dass die Datei- und Druckerfreigabe für Microsoft-Netzwerke für den Netzwerkadapter aktiviert ist, der in der Bindungsreihenfolge an erster Stelle aufgeführt wird.
- ☐ Vergewissern Sie sich, dass die Werte für die folgenden Registrierungsschlüssel auf jedem Knoten im Cluster gleich und für die relevante Grupperichtlinie gültig sind:
  - „**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanworkstation\parameters\RequireSecuritySignature**“,
  - „**HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\EnableSecuritySignature**“.

Mit diesen Einstellungen sollte „ExRCA“ die Tests einwandfrei ausführen. Dabei liest das Tool mithilfe von Remote-Prozeduraufrufen (RPCs) den Zeichenfolgenwert „**CurrentVersion**“ aus dem folgenden Registrierungsschlüssel auf dem Exchange-Server-Computer aus:

„**HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\CurrentVersion**“

Sollte weiterhin ein Fehler angezeigt werden, kann „ExRCA“ den Registrierungswert aus einem beliebigen Grund nicht lesen. Beheben Sie diesen Fehler wie folgt:

- ☐ Stellen Sie sicher, dass der Exchange-Server-Computer gestartet wurde und mit dem Netzwerk verbunden ist.
- ☐ Verwenden Sie den Befehl „**Ping**“, um festzustellen, ob eine Verbindung mit dem Exchange-Server-Computer hergestellt werden kann.
- ☐ Wenn eine Firewall vorhanden ist, überprüfen Sie, ob die RPC-Anschlüsse blockiert sind.
- ☐ Stellen Sie sicher, dass der Remote-Registrierungsdienst auf dem Exchange-Server-Computer gestartet wurde.
- ☐ Überprüfen Sie die Berechtigungen für das Konto, unter dem „ExRCA“ ausgeführt wird, um sicherzustellen, dass Sie über ausreichende Berechtigungen zum Lesen der Registrierung auf dem Exchange Server-Computer verfügen.

Fazit: Mit „ExRCA“ können Sie alle Aktivitäten simulieren, die für eine Client-Exchange-Verbindung erforderlich sind, wobei das Tool den genauen Zeitpunkt des Ausfalls festhält. Mit den Lösungsvorschlägen beheben Sie anschließend schnell mögliche Konfigurationsprobleme.

So umgehen Sie diese fiese Falle bei der dynamischen IP-Adressierung

Autor: Olaf Reuter

Vor einiger Zeit bin ich von einem Kunden zu einem Notfall gerufen worden, weil sämtliche Client-Computer keine Internetverbindung und keine Anbindung an die Server-Laufwerke mehr hatten. Das Problem betraf alle Computer, die eine dynamische IP-Adresse erhalten hatten. Computer mit einer statischen IP-Adresse hatten das Problem nicht.

Was war passiert? Der Kunde bekommt sehr viel Besuch und dieser Besuch bringt eigene Laptops mit, die dann über das WLAN Zugang zum Unternehmensnetzwerk haben.

Außerdem ermutigt die Geschäftsleitung die Mitarbeiter, ihre persönlichen Tablet-PCs oder Smartphones ins Unternehmen mitzubringen und mit diesen zu arbeiten.

Alle diese Geräte erhalten ihre IP-Adressen von einem DHCP-Server. Die Kontrolle der Adressverwaltung der jeweiligen Clients mit dem Befehl „**ipconfig –all**“ über die Eingabeaufforderung ergab, dass sämtliche Geräte lediglich eine „Link-local“-Adresse aus dem Bereich „169.254.“ erhalten hatten.

Ein Blick in die Konsole des DHCP-Servers zeigte dann, dass sämtliche IP-Adressen vergeben waren und keine freien IP-Adressen mehr zur Verfügung standen.

Das Problem war, dass die Lease-Dauer für die DHCP-Clients auf 14 Tage eingestellt war. Selbst wenn ein Gerät nur ein paar Stunden im Unternehmen war, belegte dieses Gerät die IP-Adresse für mehrere Tage und war erst nach Ablauf der Lease-Dauer wieder frei.

Wie Sie einen IPAM-Server gezielt einsetzen

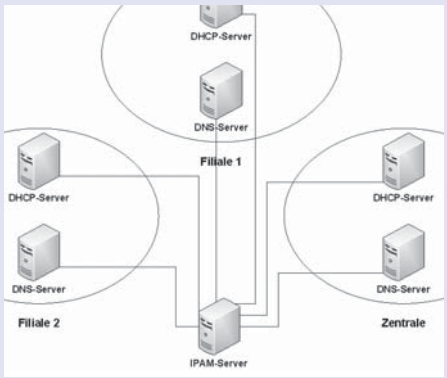
Der Windows Server 2012 besitzt eine Funktion, mit der Sie unter anderem die dynamische IP-Adressierung überwachen können. Diese Funktion heißt **IP** **A**ddress **M**anagement (IPAM, IP-Adressverwaltung) und wird auf einem eigenständigen Windows-Server betrieben.

Die Kommunikation erfolgt über die Schnittstellen

- RCP (**R**emote **P**rocedure **C**all),
- WMI (**W**indows **M**anagement **I**nstruments),
- SMB (**S**erver **M**essage **B**lock),
- WS-Management (**W**eb **S**ervices-**M**anagement) und
- LDAP (**L**ightweight **D**irectory **A**ccess **P**rotocol).

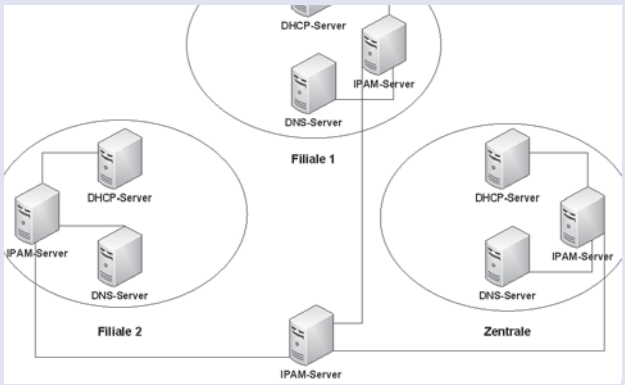
Ein IPAM-Server kommuniziert direkt mit den im Netz implementierten DHCP- (**D**ynamic **H**ost **C**onfiguration **P**rotocol) sowie DNS-Servern (**D**omain **N**ame **S**ervice) und kann entweder zentral an einem Standort oder verteilt über mehrere Standorte betrieben werden.

1. Zentraler Standort



Ein zentraler IPAM-Server in der Firmenzentrale oder bei einem externen Dienstleister verwaltet sämtliche Server in einer Active-Directory-Gesamtstruktur.

2. Verteilter Standort



In der Zentrale sowie in den Filialen steht jeweils ein eigener IPAM-Server. Die dezentralen IPAM-Server schicken zur besseren Verwaltung ihre Daten an einen zentralen IPAM-Server.

Das alles bietet ein IPAM-Server

Die folgenden Voraussetzungen müssen erfüllt sein, damit ein IPAM-Server zuverlässig arbeitet:

- Auf allen zu verwalteten Server muss mindestens Windows Server 2008 installiert sein.
- Ein IPAM-Server kann nur eine Active-Directory-Gesamtstruktur überwachen.
- Es können bis zu 500 DNS- und bis zu 150 DHCP-Server mit bis zu 6.000 Adressbereichen verwaltet werden.
- IPAM bietet eine eigene Datenbank, die für maximal 100.000 Benutzer ausgelegt ist. Diese Datenbank kann jederzeit in eine MSSQL-Datenbank übertragen werden.
- Es können nur IPv4-Adressen von IPAM zurückgenommen bzw. wieder freigegeben werden.

Ein IPAM-Server übernimmt die folgenden Aufgaben der Verwaltung:

- Die Verfügbarkeit der DHCP- und DNS-Server wird überprüft..
- Er werden Berichte über die im Netz vergebenen dynamischen IPv4- und IPv6-Adressen erstellt.

- Die Verwaltung der einzelnen Server kann aktiviert oder deaktiviert werden.
- Es können jederzeit die Konfigurationsdaten der einzelnen Server ausgegeben werden.

Die Installation: In 7 Schritten einen IPAM-Server bereitstellen

IPAM ist ein Server-Feature, das auf einem Windows Server 2012 über den „**Server-Manager**“ installiert wird. Achten Sie darauf, dass der IPAM-Server lediglich ein Mitglieds-Server in der Active-Directory-Domäne ist.

Das Server-Feature heißt „**IP-Adressverwaltungsserver (IPAM-Server)**“. Folgen Sie den Schritten des Installations-Assistenten.

Nach der Installation muss der IPAM-Server konfiguriert werden, und das geht so:

1. Klicken Sie auf den Link „**IPAM**“ in der Konsolenstruktur des „**Server-Managers**“ und klicken Sie in den „**IPAM-Serveraufgaben**“ auf den Link „**Verbindung mit dem IPAM-Server herstellen**“. Wählen Sie die Server aus, mit denen Sie sich verbinden möchten.
2. Nachdem Sie die Server ausgewählt haben, klicken Sie auf den Link „**IPAM-Server bereitstellen**“. Über diesen Schritt konfigurieren Sie die Datenbank und die Bereitstellungsmethoden. Wählen Sie als Bereitstellungsmethode „**Gruppenrichtlinienbasiert**“ aus und geben Sie als „**Präfix des Gruppenrichtliniennamens**“ das Präfix „**IPAM1**“ an. Folgen Sie im Übrigen den Anweisungen des Assistenten.
3. Über den Punkt 3 der Server-Aufgaben legen Sie fest, für welche Domäne der IPAM-Server die Verwaltung übernehmen soll. Klicken Sie auf „**Serverermittlung konfigurieren**“ und wählen Sie die Stammdomäne aus. Klicken Sie auf „**OK**“, um die Auswahl abzuschließen.
4. Über den Link „**Serverermittlung starten**“ legen Sie die Aufgabenplanung für den IPAM-Server fest. Warten Sie, bis die Ermittlung abgeschlossen ist.
5. Anschließend wählen Sie die Server aus, die in die Verwaltung einbezogen werden sollen. Klicken Sie auf den Link „**Server zum Verwalten und Überprüfen des IPAM-Zugriffs auswählen und hinzufügen**“. Es werden die Server angezeigt, die mit dem IPAM-Server verwaltet werden.

   Hinweis: Wenn der Zugriffsstatus auf „**Blockiert**“ steht, dann geben Sie in PowerShell-Konsole das folgende Cmdlet ein: „**Invoke-IpamGpoProvisioning -Domain *edv* -GpoPrefixName IPAM1 -DelegatedGpoUser user1 -IpamServerFqdn ipam1.edv**“ ↵.

   Für den Parameter „**Domain**“ müssen Sie den Namen Ihrer Domäne eingeben und für den Parameter „**IpamServerFqdn**“ den Namen Ihres IPAM-Servers.
6. Im letzten Schritt rufen Sie über den Link „**Daten von verwalteten Servern abrufen**“ die Daten der DHCP- sowie der DNS-Server für die Verwaltung mit IPAM ab.

So verwalten Sie Ihre IP-Adressen optimal

Neue IP-Adressen legen Sie in IPAM an, indem Sie im Navigationsbereich mit der rechten Maustaste auf „**IPv4**“ klicken. Wählen Sie anschließend den Befehl „**IP-Adressblock hinzufügen**“. Folgen Sie dem Assistenten zum Anlegen eines IPv4-Adressblocks.

Nachdem Sie die Adressblöcke angelegt haben, können Sie benutzerdefinierte logische Gruppen einrichten und die einzelnen IP-Adressen diesen Gruppen zuweisen. Das geht so:

1. Klicken Sie im Navigationsbereich der IPAM-Konsole des „**Server-Managers**“ unter dem Bereich „**IP-ADRESSRAUM**“ auf den Link „**IP-Adressbereichsgruppen**“.
2. Klicken Sie in der Menüleiste auf „**Verwalten**“ und wählen Sie den Menübefehl „**IPAM-Einstellungen**“.
3. In dem sich öffnenden Dialog „**IPAM-Einstellungen**“ klicken Sie auf „**Benutzerdefinierte Felder konfigurieren**“.
4. Unter „**Schritt 1**“ in der Tabelle „**Benutzerdefinierte Felder hinzufügen**“ bewegen Sie den vertikalen Rollbalken ganz ans Ende der Tabelle und geben in das leere Feld einen Namen ein.
5. Wählen Sie in der Tabellenspalte „**Mehrere Werte**“ die Option „**Ja**“ aus.
6. Tragen Sie in der unteren Tabelle im Bereich „**Schritt 2**“ „**Benutzerdefinierte Feldwerte**“ ein. Das können z. B. die Abteilungen Ihres Unternehmens sein.
7. Wenn Sie Ihre Werte eingetragen, klicken Sie auf „**OK**“, um den Vorgang abzuschließen.
8. Zurück in der IPAM-Konsole klicken Sie mit der rechten Maustaste auf den IP-Adressbereich und wählen den Befehl „**IP-Adressbereich bearbeiten**“ aus.
9. Klicken Sie auf „**Benutzerdefinierte Konfiguration**“ und wählen Sie den soeben angelegten benutzerdefinierten Feldnamen aus.
10. Wählen Sie ein benutzerdefiniertes Feld aus und klicken Sie auf „**Hinzufügen**“.
11. Klicken Sie in der IPAM-Konsole mit der rechten Maustaste auf „**IPv4**“ und wählen Sie den Befehl „**IP-Adressbereichsgruppen hinzufügen**“ aus.
12. Geben Sie einen Namen ein und wählen Sie das benutzerdefinierte Feld aus.
13. Klicken Sie zum Abschluss auf „**OK**“.

Die verschiedenen Abteilungen sind jetzt dem IP-Adressbereich zugeordnet. Klicken Sie zur Überprüfung auf den Pfeil neben dem Eintrag „**IPv4**“. Sie können jetzt der Reihe nach Ihre benutzerdefinierten Felder öffnen und sich den dazugehörigen IP-Adressbereich ausgeben lassen.