
GFI LANguard 9.0 ReportPack

Handbuch

GFI Software Ltd.



<http://www.gfi.com>
E-Mail: info@gfi.com

Änderungen in diesem Dokument jederzeit vorbehalten. Firmen, Namen und Daten in den Beispielen sind frei erfunden, sofern nicht ausdrücklich anders angegeben. Kein Teil dieses Dokuments darf in irgendeiner Form oder mit elektronischen oder mechanischen Mitteln für irgendwelche Zwecke ohne ausdrückliche schriftliche Genehmigung der GFI SOFTWARE Ltd. reproduziert oder übertragen werden.

Zuletzt aktualisiert am: 4 September 2009
Version: LANSSRP-RP-DE-01.00.00

Inhalt

1.	Einführung	1
1.1	Über GFI ReportCenter	1
1.2	Über das GFI LANguard 9.0 ReportPack	2
1.3	Komponenten des GFI LANguard 9.0 ReportPack	2
1.4	Haupteigenschaften	4
2.	Installation	7
2.1	Systemanforderungen	7
2.2	Verfahrensweise bei der Installation	7
2.3	Starten der GFI LANguard-Berichte für das GFI ReportCenter	8
2.4	Auswählen eines Produkts	8
3.	Erste Schritte: Standardberichte	9
3.1	Einführung	9
3.2	Erzeugen eines Standardberichts	9
3.3	Analysieren des erzeugten Berichts	12
3.4	Hinzufügen von Standardberichten zur Liste der häufig benötigten Berichte	13
4.	Benutzerdefinierte Berichte	15
4.1	Einführung	15
4.2	Erstellen eines neuen benutzerdefinierten Berichts	15
4.3	Konfigurieren der Datenfilterbedingungen	18
4.4	Starten eines Benutzerdefinierten Berichts	23
4.5	Bearbeiten eines benutzerdefinierten Berichts	23
4.6	Löschen eines benutzerdefinierten Berichts	24
4.7	Hinzufügen benutzerdefinierter Bericht zu den häufig benötigten Berichten	24
5.	Zeitplanung von Berichten	25
5.1	Einführung	25
5.2	Zeitplanung eines Berichts	25
5.3	Konfigurieren der erweiterten Einstellungen	27
5.4	Anzeigen der Liste zeitabhängiger Berichte	30
5.5	Anzeigen der Aktivität zeitabhängiger Berichte	31
5.6	Aktivieren/Deaktivieren eines zeitabhängigen Berichts	32
5.7	Bearbeiten eines zeitabhängigen Berichts	32
5.8	Beispiel: Zeitplanung eines Berichts	33
6.	Konfiguration der Standardoptionen	39
6.1	Einführung	39
6.2	Konfigurieren der Datenbankquelle: Microsoft SQL Server	40
6.3	Konfigurieren der Datenbankquelle: Microsoft Access	41
6.4	Anzeigen der aktuellen Einstellungen für die Datenbankquelle	42
6.5	Konfigurieren der Standardzeitplanereinstellungen	42
6.6	Importieren/Exportieren der Konfiguration	43
7.	Allgemeine Optionen	47

7.1	Anzeigen der Produktversion des ReportPack	47
7.2	Suchen nach neuen Builds im Internet	47
8.	Anhang: Standardberichte in GFI LANguard	49
8.1	Berichte zur Bewertung des Sicherheitsrisikos	49
8.2	Netzwerk- und Softwareüberprüfung	66
8.3	Ergebnisvergleich	83
9.	Fehlerbehebung	85
9.1	Einführung	85
9.2	Knowledge Base	85
9.3	Web-Forum	85
9.4	Anforderung von technischem Support	85
9.5	Benachrichtigungen über Builds	86
	Index	87

1. Einführung

1.1 Über GFI ReportCenter

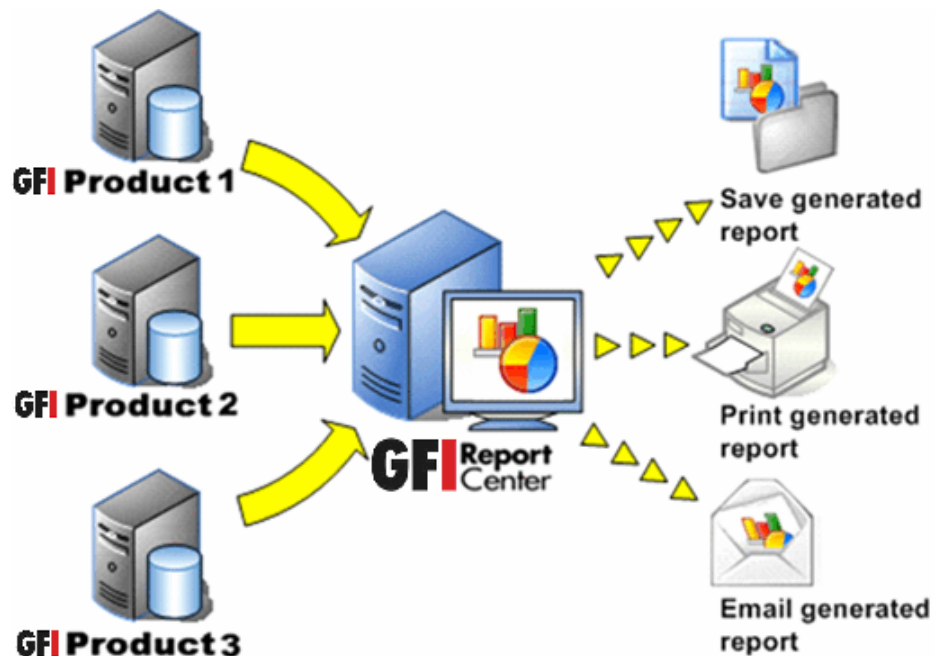


Abbildung 1 – Zentrales Reporting Framework

GFI ReportCenter ist ein zentrales Reporting Framework, mit dem Sie verschiedene Berichte aus den Daten erstellen können, die verschiedene GFI-Produkte erfasst haben. GFI bietet spezielle Berichte für jedes seiner Produkte in Form eines sogenannten ReportPacks. Es gibt beispielsweise das GFI LANguard ReportPack. Ein ReportPack kann als Ergänzung zu dem GFI-Produkt erworben werden.



Abbildung 2 – Mehrere ReportPacks in einem GFI ReportCenter Framework

Ein ReportPack installiert sich in dem GFI ReportCenter Framework; auf diese Weise können Sie die durch diese Berichte erstellten Informationen erzeugen, analysieren, exportieren und drucken.

1.2 Über das GFI LANguard 9.0 ReportPack

Das GFI LANguard ReportPack ist ein hoch leistungsfähiger Berichtsgenerator für GFI LANguard. Sie können damit grafische Berichte für die IT-Mitarbeiter, Techniker und das Management aus den Netzwerksicherheitsüberprüfungen erstellen, die GFI LANguard ausführt.

Sie können sowohl Trendberichte für das Management (zur Ermittlung der Kapitalrendite) sowie tägliche detaillierte Berichte für die Techniker erstellen; mit dem GFI LANguard ReportPack erhalten Sie die benötigten übersichtlichen Informationen, damit Sie jede Sicherheitslücke in Ihrem Firmennetzwerk identifizieren können.

Mit dem GFI LANguard ReportPack können Sie verschiedene grafische und Textberichte zu folgenden Aspekten erstellen:

- Berichte zur Auswertung von Sicherheitsrisiken
- Berichte zur Überprüfung des Netzwerks und der Software
- Berichte über Ergebnisvergleiche

1.3 Komponenten des GFI LANguard 9.0 ReportPack

Bei der Installation von GFI LANguard 9.0 ReportPack, werden die folgenden Komponenten installiert:

- GFI ReportCenter Framework

- GFI LANguard 9.0 Standardberichte
- Zeitabhängiger Berichtsdienst

GFI ReportCenter Framework

Das GFI ReportCenter ist die Verwaltungskonsole, mit der Sie die speziellen Produktberichte erzeugen, die zusammen mit dem ReportPack eines Produkts ausgeliefert werden. Mit dem GFI ReportCenter Framework verfügen Sie über eine gemeinsame Anwendungsoberfläche, in der Sie Berichte suchen, erzeugen, anpassen und zeitlich planen können.

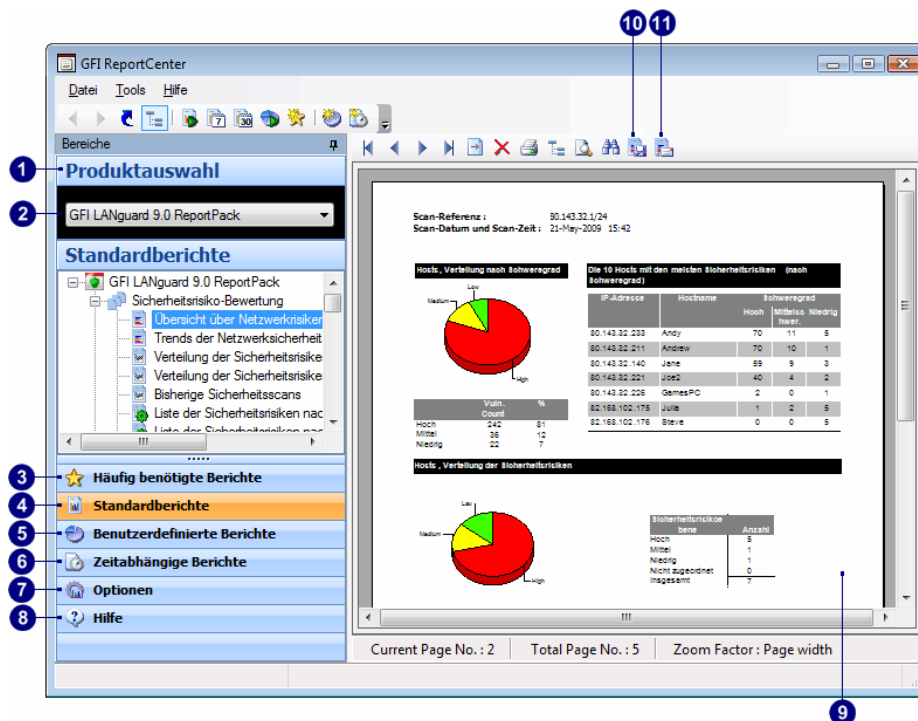


Bild 1 – Die GFI ReportCenter-Verwaltungskonsole

Die GFI ReportCenter-Verwaltungskonsole ist wie folgt gegliedert:

- 1 Navigationsseite** – Über diese Seite greifen Sie auf die Navigationsschaltflächen und Konfigurationsoptionen des GFI ReportCenter zu.
- 2 Dropdown-Liste zur Produktauswahl** – Mit dieser Dropdown-Liste wählen Sie das GFI-Produkt aus, für das Sie Berichte erstellen wollen. Die Dropdown-Liste zur Produktauswahl zeigt alle Produkte an, für die Sie ein ReportPack installiert haben.
- 3 Häufig benötigte Berichte** – Mit dieser Navigationsschaltfläche rufen Sie Ihre am häufigsten benötigten und bevorzugten Berichte auf. Weitere Informationen zum Hinzufügen von Berichten zu dieser Liste finden Sie in diesem Handbuch unter „Hinzufügen von Standardberichten zur Liste der häufig benötigten Berichte“ und „Hinzufügen von benutzerdefinierten Berichten zur Liste der häufig benötigten Berichte“.
- 4 Standardberichte** – Mit dieser Navigationsschaltfläche rufen Sie die Liste der Standardberichte auf, die für ein ausgewähltes Produkt erzeugt werden können. Weitere Informationen über Standardberichte finden Sie im Abschnitt „GFI LANguard-Standardberichte“ in diesem Handbuch.
- 5 Benutzerdefinierte Berichte** – Mit dieser Navigationsschaltfläche rufen Sie die Liste der benutzerdefinierten Berichte auf, die Sie für das ausgewählte Produkt erzeugen können. Weitere Informationen zur Erstellung

benutzerdefinierter Berichte finden Sie im Abschnitt „Benutzerdefinierte Berichte“ in diesem Handbuch.

-
- 6 Zeitabhängige Berichte** – Mit dieser Schaltfläche rufen Sie die Liste der zeitabhängigen Berichte auf, damit die automatisch erstellt und verteilt werden. Weitere Informationen, wie Sie zeitabhängige Berichte erstellen, finden Sie im Abschnitt „Zeitplanung von Berichten“ in diesem Handbuch.

 - 7 Optionen** – Mit dieser Navigationsschaltfläche rufen Sie die allgemeinen Konfigurationseinstellungen für das GFI-Produkt auf, das Sie in der Dropdown-Liste zur Produktauswahl gewählt haben.

 - 8 Hilfe** – Mit dieser Navigationsschaltfläche zeigen Sie diese Kurzreferenz auf der Berichtseite der GFI ReportCenter-Verwaltungskonsole an.

 - 9 Berichtseite** – Diese multifunktionale Seite nutzen Sie, um:
 - die erzeugten Berichte anzuzeigen und zu analysieren,
 - die Liste der zeitabhängigen Berichte zu pflegen,
 - Muster zu untersuchen und Beschreibungen der Standardberichte zu lesen.

 - 10 Exportieren** – Mit dieser Schaltfläche exportieren Sie erzeugte Berichte in verschiedene Formate, beispielsweise HTML, Adobe Acrobat (PDF), Excel (XLS), Word (DOC) und Rich Text Format (RTF).

 - 11 E-Mail versenden** – Mit dieser Schaltfläche verteilen Sie den zuletzt erzeugten Bericht sofort per E-Mail.
-

Standardberichte in GFI LANguard 9.0

Die Standardberichte für GFI LANguard 9.0 sind eine Sammlung spezieller vorkonfigurierter Berichte, die sich im GFI ReportCenter Framework installieren. Diese Berichte präsentieren die Ergebnisse der Netzwerksicherheitsscans von GFI LANguard und erlauben sowohl die Erstellung von grafischen Berichten als auch von Tabellen für IT-Mitarbeiter, Techniker und Management. Die Standardberichte dienen außerdem als Mustervorlagen für die Entwicklung benutzerdefinierter Berichte, die spezifische Anforderungen für die Netzwerk-Berichterstellung erfüllen sollen.

Zeitplanung für Berichte

Der Dienst zur Zeitplanung der Berichte steuert die zeitabhängige Erzeugung und automatische Verteilung der Berichte per E-Mail. Durch diesen Dienst erstellte Berichte können auch in einem besonderen Ordner der Festplatte in verschiedenen Formaten wie DOC, PDF, RTF und HTML gespeichert werden.

1.4 Haupteigenschaften

Zentrale Berichterstellung

GFI ReportCenter ist das zentrale Reporting Framework, das die Erstellung und Anpassung von grafischen Berichten und Tabellen für eine Vielzahl von GFI-Produkten erlaubt.

Durch Assistent unterstützte Konfiguration

Assistenten helfen Ihnen bei der Konfiguration, Zeitplanung und Anpassung der Berichte.

Zeitabhängige Berichte

Mit GFI ReportCenter können Sie Berichte zeitlich so planen, dass Sie entsprechend einem vordefinierten Schema sowie in spezifischen

Intervallen erzeugt werden. Sie können beispielsweise umfangreiche Berichte nach Arbeitsschluss erstellen lassen. Auf diese Weise optimieren Sie die Verfügbarkeit Ihrer Systemressourcen während der Arbeitszeit und vermeiden mögliche Unterbrechungen des Arbeitsablaufs.

Verteilung der Berichte per E-Mail

Mit GFI ReportCenter können Sie automatisch die erzeugten Berichte per E-Mail verteilen. Bei zeitabhängigen Berichten kann dies automatisch erfolgen, sobald ein zeitabhängiger Bericht erfolgreich erzeugt wurde.

Berichtsexport in verschiedene Formate

Standardmäßig können Sie mit GFI ReportCenter Berichte in verschiedene Formate exportieren. Unterstützte Formate sind HTML, PDF, XLS, Doc und RTF. Bei der Zeitplanung der Berichte können Sie bei Bedarf auch das bevorzugte Ausgabeformat für den Bericht konfigurieren. Die verschiedenen zeitabhängigen Berichte können Sie auch so konfigurieren, dass die erzeugten Berichte in verschiedenen Dateiformaten ausgegeben werden.

Standardberichte

Standardmäßig wird GFI LANguard ReportPack mit einem Satz von grafischen Berichten und Tabellenberichten ausgeliefert. Diese Berichte können Sie sofort erstellen, ohne dass nach der Installation eine weitere Konfiguration erforderlich ist. Die Standardberichte in diesem ReportPack lassen sich in drei verschiedene Berichtarten gliedern:

- Berichte zur Bewertung des Sicherheitsrisikos
- Berichte zur Netzwerk- und Softwareüberprüfung
- Berichte über Ergebnisvergleiche

Berichts Anpassung

Die Standardberichte, die mit jedem ReportPack ausgeliefert werden, können als Vorlagen zur Erstellung eigener Berichte verwendet werden. Die Anpassung von Berichten erreichen Sie durch benutzerdefinierte Datenfilter, die die Datenquelle analysieren und die Informationen ausfiltern, die bestimmte Kriterien erfüllen. Auf diese Weise erzeugen Sie Berichte, die genau Ihren Berichtsanforderungen entsprechen.

Häufig benötigte Berichte

Im GFI ReportCenter können Sie für Ihre am häufigsten benötigten Berichte Bookmarks setzen – sowohl für Standardberichte als auch benutzerdefinierte Berichte.

Drucken

Standardmäßig liegen alle von GFI ReportCenter erzeugten Berichte im druckfreundlichen Format vor und können über die Windows-Druckerdienste über das System ausgedruckt werden, auf dem GFI ReportCenter installiert ist.

2. Installation

2.1 Systemanforderungen

Installieren Sie GFI LANguard ReportPack auf einem Computer, der folgende Anforderungen erfüllt:

- Betriebssystem Windows 2000 (SP4), XP (SP2/SP3), 2003, 2008, VISTA (SP1)
- Internet Explorer 5.1 oder höher
- .NET Framework Version 2.0
- MDAC 2.8
- GFI ReportCenter 3.6

HINWEIS: Das GFI LANguard ReportPack erlaubt nur die Erzeugung von Berichten für Daten aus den Datenbanken mit den Scanergebnissen, die durch GFI LANguard erzeugt und gepflegt werden.

2.2 Verfahrensweise bei der Installation

Zum GFI LANguard ReportPack gehört ein Installationsassistent, der Sie bei der Installation unterstützt. Während der Installation führt dieser Assistent folgende Aufgaben aus:

- Er überprüft, ob Sie die aktuelle Version des GFI ReportCenter Framework installiert haben; wenn Sie das Framework erstmals installieren oder die zurzeit installierte Version des Reporting Framework veraltet ist, lädt der Installationsassistent automatisch die aktuellste Version für Sie herunter.
- Er installiert automatisch alle benötigten Komponenten, die mitgeliefert werden, beispielsweise das GFI ReportCenter Framework, die Standardberichte für GFI LANguard und den Dienst zur Zeitplanung der Berichte.

So starten Sie die Installation:

1. Doppelklicken Sie auf **LANguard9rp.exe**.
2. Wählen Sie die gewünschte Sprache aus.
3. Im Setup werden als nächstes alle fehlenden Systemvoraussetzungen aufgelistet (sofern zutreffend). Installieren Sie fehlende Komponenten, indem Sie diese betreffende Systemvoraussetzung auswählen und dann auf **Weiter klicken**.

HINWEIS: Ist die aktuelle Version Ihres GFI ReportCenter Framework nicht mit dem GFI LANguard ReportPack kompatibel, werden Sie aufgefordert, ein Update der Version herunterzuladen und zu installieren.

4. Klicken Sie im Begrüßungsbildschirm auf **Weiter**.

5. Lesen Sie die Lizenzvereinbarung für Endanwender, klicken Sie auf die Radioschaltfläche **Ich akzeptiere die Lizenzvereinbarung** und dann auf **Weiter**.

6. Bitte geben Sie die Registrierungsinformationen und den Lizenzschlüssel, falls Sie danach gefragt werden, während der Installation ein.

HINWEIS: Wenn GFILANguard bereits auf diesem System installiert ist, registriert sich das GFI ReportPack automatisch mit dem Lizenzschlüssel vom GFI LANguard.

7. Wählen Sie den Installationspfad aus oder übernehmen Sie die Standardvorgabe und klicken Sie auf **Weiter**.

8. Klicken Sie auf **GFI LANguard 9.0 ReportPack**, um das ReportPack nach Abschluss des Setups zu starten.

2.3 Starten der GFI LANguard-Berichte für das GFI ReportCenter

Starten Sie nach der Installation die GFI LANguard-Berichte für das GFI ReportCenter über **Start ► Programme ► GFI ReportCenter ► GFI LANguard 9 ReportPack**.

2.4 Auswählen eines Produkts

Wenn mehr als ein Produkt mit einem ReportPack installiert ist, wählen Sie über die Dropdown-Liste **Produktauswahl** das gewünschte ReportPack für Ihr GFI-Produkt aus.

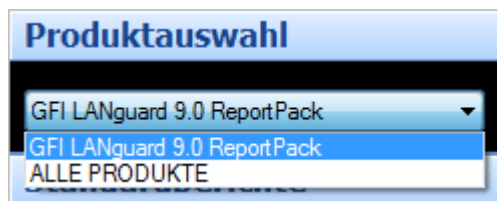


Bild 2 Dropdown-Liste zur Produktauswahl

So starten Sie beispielsweise die Berichte im GFI LANguard ReportPack:

1. Starten Sie das GFI ReportCenter über **Start ► Programme ► GFI ReportCenter**.

2. Wählen Sie 'GFI LANguard 9.0' über die Dropdown-Liste Produktauswahl.

HINWEIS: Klicken Sie auf die Option „Alle Produkte“, um alle ReportPacks anzuzeigen, die zurzeit im GFI ReportCenter installiert sind.

3. Erste Schritte: Standardberichte

3.1 Einführung

Nach Installation des GFI LANguard ReportPack können Sie sofort eine Reihe vorkonfigurierter Berichte aus den in dem Datenbank-Backend von GFI LANguard gespeicherten Daten erstellen. Diese Standardberichte sind in folgenden Kategorien sortiert:

- **Sicherheitsrisikobewertung:** Mit den Berichten dieser Kategorie identifizieren Sie erkannte Sicherheitsrisiken im Netzwerk, sowie Informationen über Netzwerk-Patches und Service Packs, die installiert sind oder installiert werden sollen. In den Berichten finden Sie Details zu Sicherheitsrisiken, beispielsweise die Hostcomputer, die betroffenen Betriebssysteme und den Schweregrad.
- **Netzwerk- und Softwareüberprüfung:** Mit den Berichten dieser Kategorie zeigen Sie detaillierte Informationen zu Hardware und Software im Netzwerk an. Diese Berichte helfen dem Management, die Einhaltung der Firmensicherheitsrichtlinie zu analysieren.
- **Ergebnisvergleichsberichte:** Mit den Berichten in dieser Kategorie vergleichen Sie die Ergebnisse verschiedener Netzwerkscans mit einem gemeinsamen Profil und gemeinsamen Ziel und die Computerscans mit einem als Vergleichsstandard verwendeten Computer.

Standardberichte von GFI LANguard rufen Sie durch Klicken auf die Navigationsschaltfläche **Standardberichte** auf der Navigationsseite auf.

3.2 Erzeugen eines Standardberichts

So erzeugen Sie einen Standardbericht:

1. Klicken Sie auf die Navigationsschaltfläche **Standardberichte**, um die Liste der verfügbaren Standardberichte anzuzeigen.

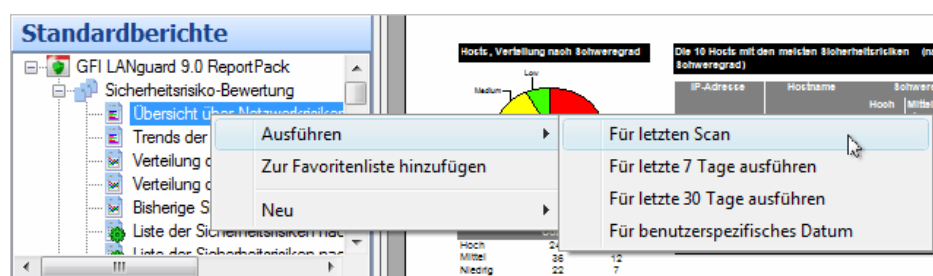


Bild 3 – Auswählen der Datensätze

2. Klicken Sie mit der rechten Maustaste auf den zu erzeugenden Bericht, dann auf **Ausführen** und geben Sie mit Scan-Datum und Uhrzeit den Zeitraum an, der im Bericht berücksichtigt werden soll.

Beispiel 1: Erzeugen eines „Übersichtsberichts zu Sicherheitsrisiken im Netzwerk“ aus den Daten des letzten Scans

Dieses Beispiel zeigt, wie Sie einen Übersichtsbericht zu Sicherheitsrisiken im Netzwerk aus den Daten des letzten Netzwerkscans erstellen:

1. Klicken Sie auf die Navigationsschaltfläche **Standardberichte**, um die Liste der verfügbaren Berichte anzuzeigen.
2. Klicken Sie mit der rechten Maustaste auf die Option **Übersicht über Sicherheitsrisiken im Netzwerk** und dann auf **Starten ► Für letzten Scan**.

Beispiel 2: Erzeugen eines Berichts „Übersicht über Sicherheitsrisiken im Netzwerk“ aus den Scandaten eines bestimmten Tages

Dieses Beispiel zeigt, wie Sie einen Übersichtsbericht über Sicherheitsrisiken im Netzwerk aus den Scandaten vom 11. Mai 2009 erzeugen.

1. Klicken Sie auf die Navigationsschaltfläche **Standardberichte**, um die Liste der verfügbaren Berichte anzuzeigen.
2. Klicken Sie mit der rechten Maustaste auf die Option „Übersicht über Sicherheitsrisiken im Netzwerk“ und dann auf **Starten ► Für benutzerdefiniertes Datum**.

Assistent für benutzerdefinierten Bericht

Datum Uhrzeit

Geben Sie Datum und Uhrzeit für den Zeitraum des Berichts an.

Berichte mit Datums- und Uhrzeitangabe erfassen alle Scans, in dem ausgewählten Zeitraum und erzeugen die Ergebnisse in Abhängigkeit von den bei diesen Scans gefundenen Informationen.

Relativ

Heute

Tag

11 May 2009

May 2009

Mon	Tue	Wed	Thu	Fri	Sat	Sun
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

Jahr: 2009

Heute: 16/01/2009

< Zurück Weiter > Abbrechen

Bild 4 – Konfigurieren eines benutzerdefinierten Zeitraums mit Datum und Uhrzeit

3. Klicken Sie auf die Option **Tag** und öffnen Sie die Dropdown-Liste. Es wird ein Kalender zur Datumsauswahl angezeigt.

- Suchen Sie den benötigten Monat (in diesem Fall Mai), und wählen Sie den gewünschten Tag aus (in diesem Fall 11).
- Klicken Sie auf **Weiter**, um den Bericht zu erstellen.

Beispiel 3: Erzeugen einer „Übersicht über Sicherheitsrisiken im Netzwerk“ aus den Daten für einen bestimmten Zeitraum (Datum/Uhrzeit)

Dieses Beispiel zeigt, wie Sie einen Übersichtsbericht zu Sicherheitsrisiken im Netzwerk aus den Netzwerksicherheits-Scans erstellen, die zwischen dem 1. Mai 2009 und dem 11. Mai 2009 ausgeführt wurden.

- Klicken Sie auf die Navigationsschaltfläche **Standardberichte**, um die Liste der verfügbaren Berichte anzuzeigen.
- Klicken Sie mit der rechten Maustaste auf die Option **Übersicht über Sicherheitsrisiken im Netzwerk** und dann auf **Starten ► Für benutzerdefiniertes Datum**.

Bild 5 – Konfigurieren eines benutzerdefinierten Zeitraums mit Datum und Uhrzeit

- Klicken Sie auf die Option „Datumsbereich“, und geben Sie die gewünschten Parameter ein:

- „Von“ – 5/1/2009 12:00:00 AM.
- „Bis“ – 5/11/2009 12:59:59 PM.

HINWEIS: Das Format für Datum und Uhrzeit richtet sich nach den Regionaleinstellungen, die für Ihren Computer konfiguriert sind.

- Klicken Sie auf **Weiter**, um den Bericht zu erstellen.

3.3 Analysieren des erzeugten Berichts

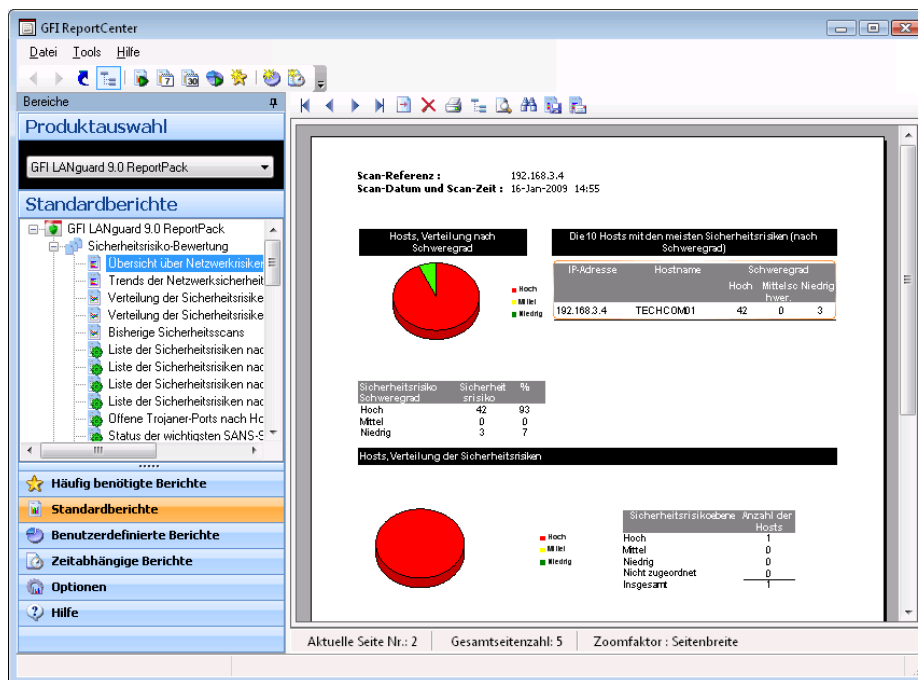


Bild 6 – Erzeugte Berichte werden auf der rechten Seite der Verwaltungskonsolle angezeigt.

Erzeugte Berichte werden auf der rechten Seite des GFI ReportCenter angezeigt. Über die Taskleiste am oberen Rand der Berichtsseite können Sie die wichtigsten Berichtsfunktionen aufrufen:

Durchsuchoptionen für Berichte



Den erzeugten Bericht Seite für Seite durchsuchen.



Vergrößern/Verkleinern



Bericht nach einem bestimmten Text oder nach bestimmten Zeichen durchsuchen.



Direkt zu einer bestimmten Seite springen.



Bericht in eine Baumgruppe aufteilen (beispielsweise nach Datum und Uhrzeit).



Bericht drucken.

Speicher- und Verteiloptionen für Berichte



Erzeugten Bericht in ein bestimmtes Dateiformat exportieren



Erzeugten Bericht per E-Mail versenden

HINWEIS: Informationen, wie Sie die Berichtsspeicher- und Verteilungsoptionen konfigurieren, finden Sie im Abschnitt „Konfigurieren der erweiterten Einstellungen“ in diesem Handbuch.

3.4 Hinzufügen von Standardberichten zur Liste der häufig benötigten Berichte

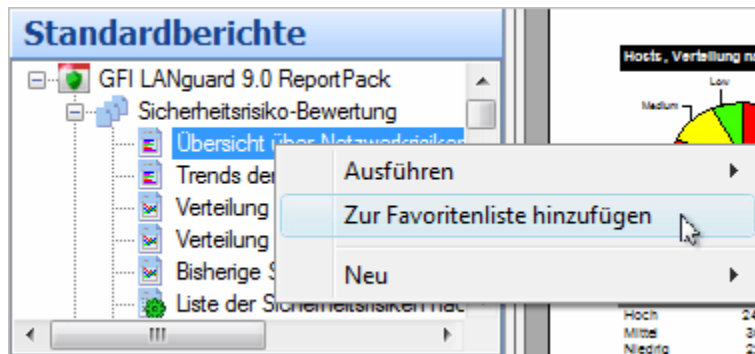


Bild 7 – Die Schaltfläche „Häufig benötigte Berichte“

Sie können häufig benötigte Berichte über die Schaltfläche **Häufig benötigte Berichte** zu Gruppen zusammenfassen und so leichter aufrufen. So ergänzen Sie einen Standardbericht in der Liste der häufig benötigten Berichte:

1. Klicken Sie auf die Navigationsschaltfläche **Standardberichte**, um die Liste der verfügbaren Berichte anzuzeigen.
2. Klicken Sie mit der rechten Maustaste auf den Standardbericht, den Sie zu den häufig benötigten Berichten hinzufügen wollen, und klicken Sie dann auf **Zur Liste der häufig benötigten Berichte hinzufügen**.
3. Klicken Sie zur Bestätigung auf **Ja**.

4. Benutzerdefinierte Berichte

4.1 Einführung

GFI ReportCenter erlaubt die Erstellung benutzerdefinierter Berichte entsprechend Ihren spezifischen Anforderungen an die Berichterstellung. Die Anpassung von Berichten erreichen Sie durch benutzerdefinierte Datenfilter, die die Datenquelle analysieren und die Informationen ausfiltern, die bestimmte Kriterien erfüllen.

4.2 Erstellen eines neuen benutzerdefinierten Berichts

Benutzerdefinierten Bericht erstellen:

1. Klicken Sie auf die Schaltfläche **Standardberichte**.
2. Klicken Sie mit der rechten Maustaste auf den Standardbericht, den Sie als Vorlage verwenden wollen, und dann auf **Neu ► Benutzerdefinierter Bericht**. Daraufhin wird der „Assistent für den benutzerdefinierten Bericht“ angezeigt.

Assistent für benutzerdefinierten Bericht

Scan oder Zeitraum (Datum/Uhrzeit)

Geben Sie den Scan bzw. den Zeitbereich (Datum/Uhrzeit) an, für die der Bericht gelten soll.

Die Berichte werten die Ergebnisse des Sicherheits-Scans aus, die bei den vergangenen Netzwerksicherheits-Scans gesammelt wurden.

Wählen Sie die Scan-Ergebnisse aus, die vom Bericht verwendet werden:

- Letzter Scan:**
Mit dieser Option erzeugen Sie Berichte aus den Daten, die während des letzten Netzwerksicherheits-Scans gesammelt wurden.
- Spezifischer Scan:**
Mit dieser Option erzeugen Sie Berichte aus den Daten, die bei einem bestimmten Netzwerksicherheits-Scan gesammelt wurden.
- Zeitraum (Datum/Uhrzeit) scannen:**
Erzeugen Sie mit dieser Option Berichte aus den Scan-Ergebnisdaten, die während eines bestimmten Zeitraumes gesammelt wurden.

< Zurück Weiter > Abbrechen

Bild 8 - Auswählen der Scandatenquelle

3. Geben Sie die Datenquelle an, die zur Erstellung des benutzerdefinierten Berichts verwendet werden soll. Diese Datenquelle lädt Scanergebnisse von:

- Dem letzten Scan,
- Einem spezifischen Scan

- Scans aus einem bestimmten Zeitraum (Datum/Uhrzeit)
Klicken Sie auf **Weiter**, um fortzufahren.

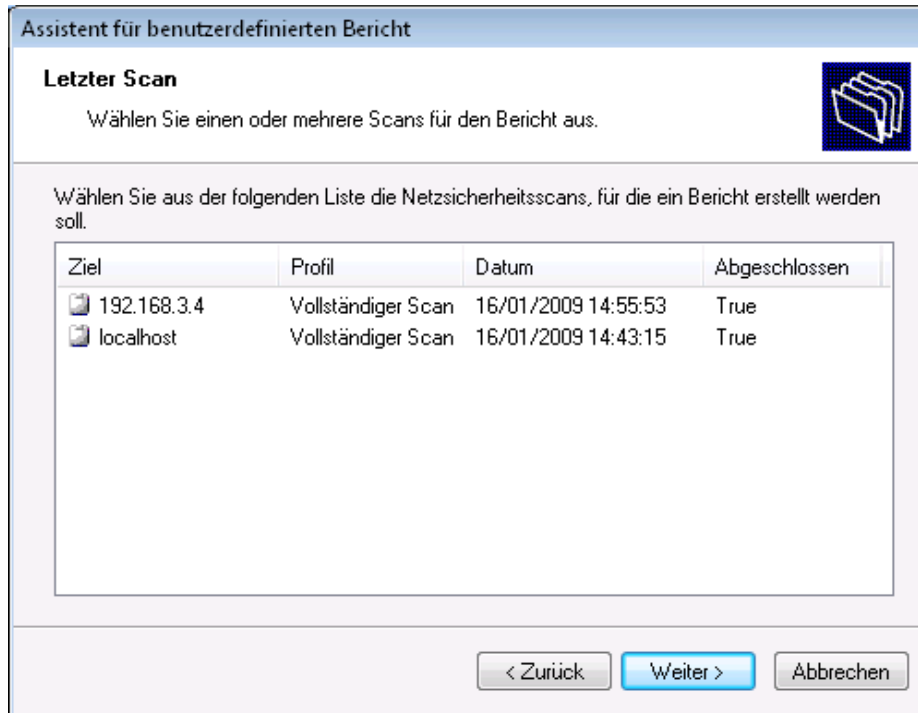


Bild 9 – Auswählen der gewünschten Scandatenquelle

4. Mit der Option „Spezifischer Scan“ wählen Sie die gewünschten Scanergebnisse aus der Liste der Netzwerksicherheits-Scans im Firmennetzwerk aus. Klicken Sie auf **Weiter**, um fortzufahren.

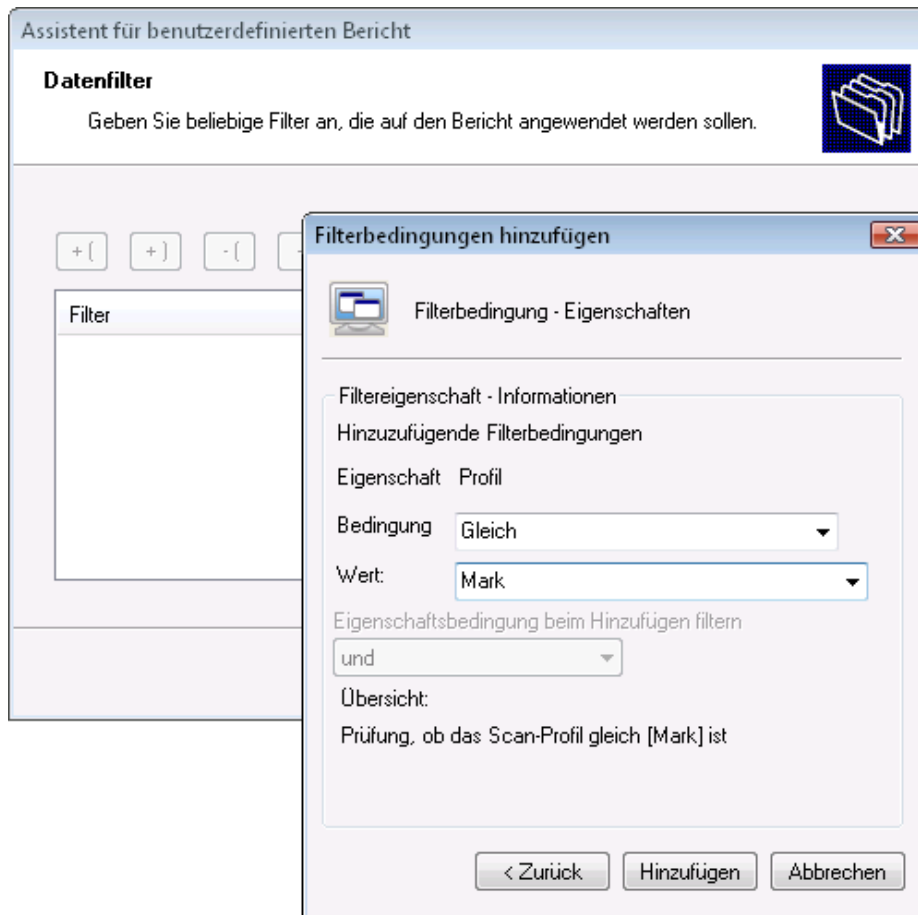


Bild 10 – Definieren der Datenfilterbedingungen

5. Konfigurieren Sie die Datenfilterbedingungen, die für die ausgewählte Datenquelle verwendet werden sollen. Klicken Sie auf **Weiter**, um fortzufahren.

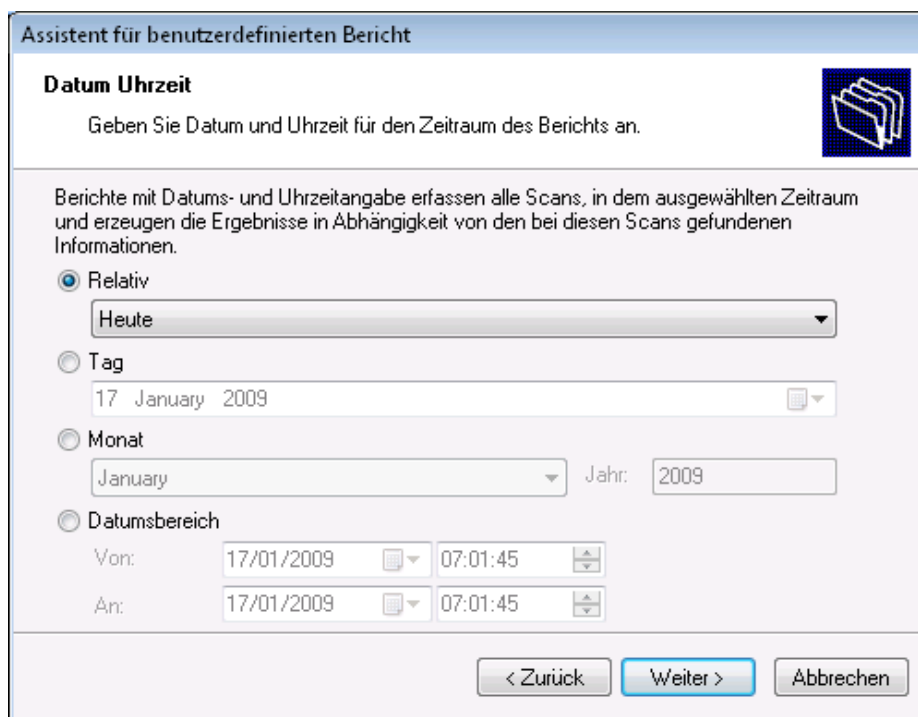


Bild 11 – Konfigurieren eines benutzerdefinierten Zeitraums mit Datum und Uhrzeit

6. Mit der Option „Zeitraum (Datum/Uhrzeit) scannen“ wählen Sie einen Zeitraum mit Datum und Uhrzeit aus, aus dem die Netzwerksicherheits-Scanergebnisse geladen werden. Klicken Sie auf **Weiter**, um fortzufahren.

HINWEIS: Weitere Informationen zur Konfiguration der Filterbedingungen finden Sie im Abschnitt „Konfigurieren der Datenfilterbedingungen“ in diesem Handbuch.

7. Geben Sie den Namen und die Beschreibung für diesen zeitabhängigen Bericht ein. Klicken Sie auf **Weiter**, um fortzufahren.

8. Klicken Sie auf **Fertig stellen**, um Ihre Konfiguration zu übernehmen.

4.3 Konfigurieren der Datenfilterbedingungen

Mit Datenfilterbedingungen legen Sie fest, welche Netzwerksicherheits-Scandaten und Ergebnisse in den Bericht aufgenommen werden. Nur Scans, die bestimmte Kriterien erfüllen, werden verarbeitet und im Bericht angezeigt.

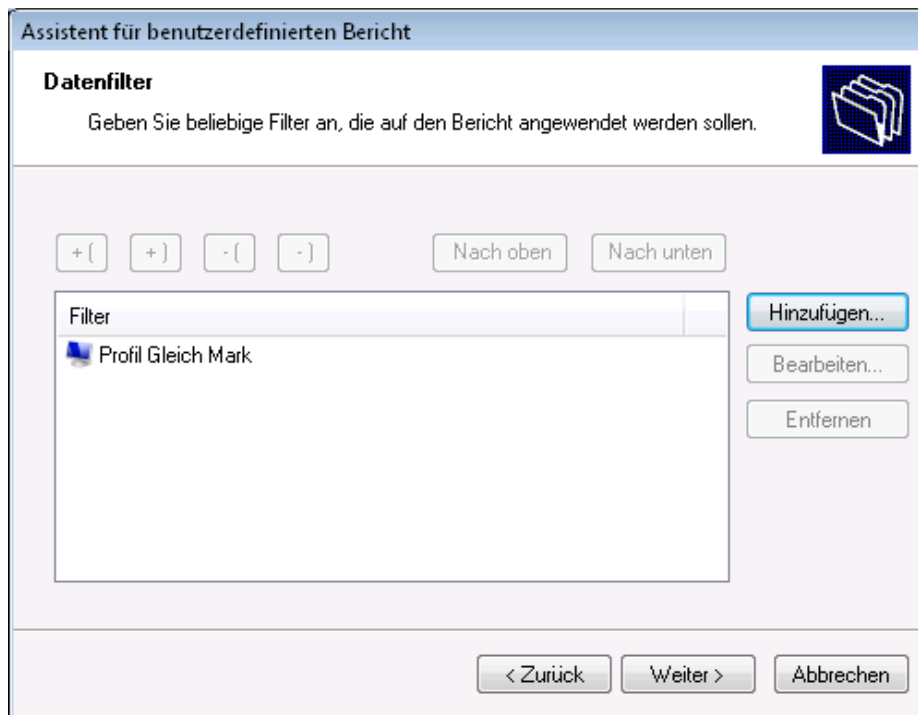


Bild 12 – Assistent für benutzerdefinierte Berichte mit Dialogfilter

Klicken Sie auf die Schaltfläche **Hinzufügen...**, um den Dialog „Filtereigenschaften bearbeiten“ anzuzeigen und die folgenden Bedingungen zu konfigurieren:

- **Filterbedingung** – Geben Sie den Datenquellenbereich an, auf den sich der Filter konzentrieren soll (wählen Sie beispielsweise als Filterbedingung „Betriebssystem“, um die Ereignisdaten nach einem bestimmten Betriebssystem zu filtern).
- **Bedingung** – Geben Sie einen Vergleichsparameter als Bedingung an.
- **Wert** – Geben Sie den String an, mit dem die Quelldaten verglichen werden sollen.

Wenn Sie beispielsweise einen Bericht erstellen wollen, der nur Informationen über Windows XP enthält, konfigurieren Sie Ihre Filterparameter wie folgt:

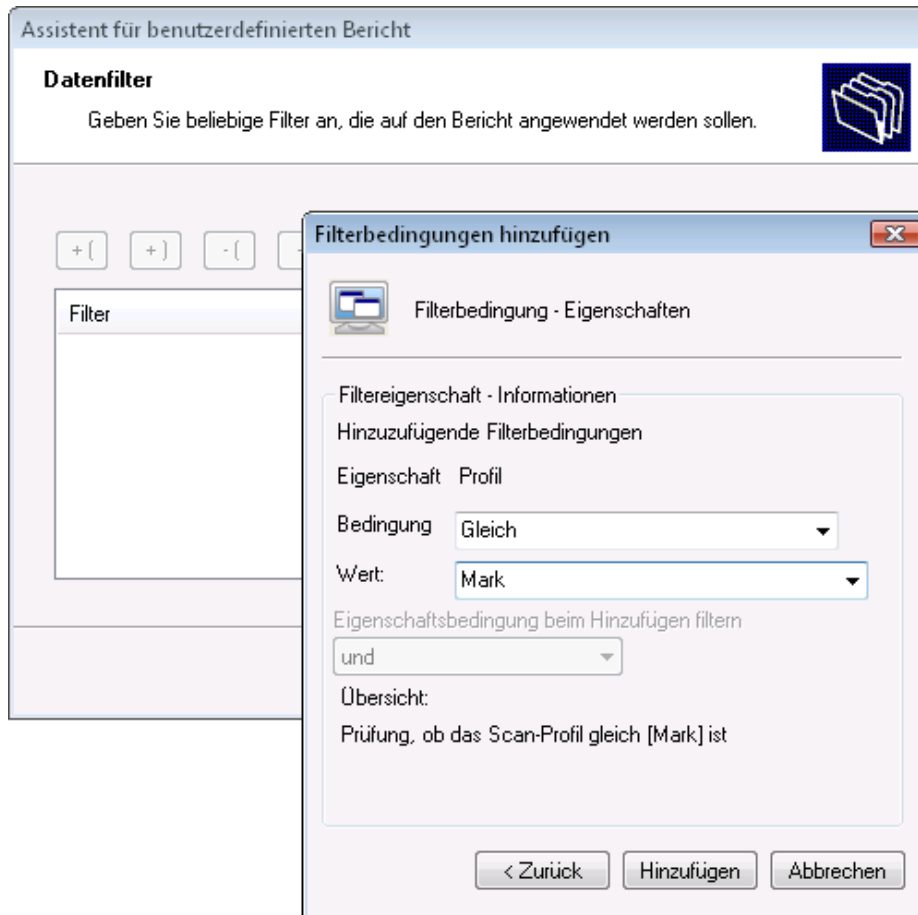


Bild 13 – Dialog „Konfiguration der Filterbedingungen“

Bei spezifischeren Berichten können Sie die angezeigte Informationsmenge begrenzen, indem Sie Ihre Suchkriterien/Bedingungen verschärfen. Dazu konfigurieren Sie mehrere Datenfilter für die ausgewählte Datenquelle und wenden diese an. Wenn Sie mehr als einen Filter verwenden, müssen Sie die logische Verknüpfung dieser Filter angeben. Dazu wählen Sie eine logische Gruppenverknüpfungsbedingung aus der Dropdown-Liste „Filtereigenschaft“ als Bedingung aus.

- Klicken Sie auf **Und**, um alle Scandaten zu berücksichtigen, die alle Bedingungen der Filter erfüllen.
- Klicken Sie auf **Oder**, um alle Scandaten zu berücksichtigen, die mindestens eine der angegebenen Filterbedingungen erfüllen.

Beispiel: Verwendung mehrerer Filter

Stellen Sie sich eine Situation vor, wo ein benutzerdefinierter Bericht mit zwei Filtern wie folgt konfiguriert ist:

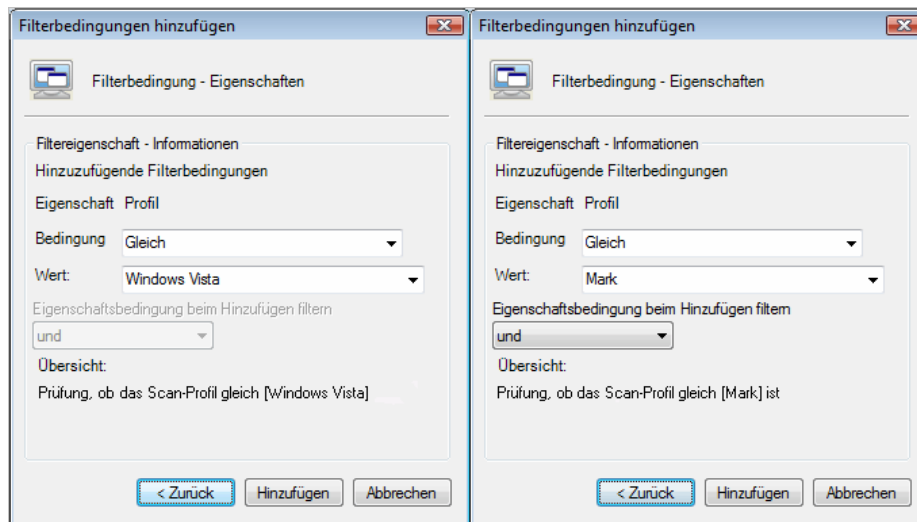


Bild 14 – Verwendung mehrerer Filter

Parameter	Filter 1	Filter 2
Filterbedingung	Hostname	Betriebssystem
Logische Beziehung	Gleich	Gleich
Wert	„Mark“	„Windows XP“

Welche Daten in diesem benutzerdefinierten Bericht berücksichtigt werden, richtet sich danach, wie diese Filter auf die Daten angewendet werden. Dazu definieren Sie die Anwendung in der Dropdown-Liste „Filtereigenschaftsbedingungen ...“.

Angewandte Filter			Datenausgabe
Filter 1	und	Filter 2	Der Bericht zeigt: Alle Scandaten, die sich auf einen Host mit der Bezeichnung „Marc“ beziehen, auf dem „Windows XP“ gestartet ist.
Filter 1	oder	Filter 2	Der Bericht zeigt: Alle Scandaten für „Windows XP“ (unabhängig davon, auf welchem Host). UND Alle Scandaten für einen Host mit der Bezeichnung „Mark“ (unabhängig vom installierten Betriebssystem).

Beispiel: Erstellen eines benutzerdefinierten Berichts aus den Netzwerksicherheits-Scandaten eines bestimmten Monats

Dieses Beispiel zeigt Ihnen, wie Sie einen Übersichtsbericht über Sicherheitsrisiken im Netzwerk mit der Bezeichnung „Übersicht über Sicherheitsrisiken im Netzwerk auf dem Host „Marc“ im Januar 2009“ erstellen. Dieser Bericht verwendet folgende Scanergebnisse:

- Scanergebnisse für einen Host mit dem Namen „Mark“,
- die zu einem Betriebssystem „Windows XP“ gehören,
- die während des Monats „Januar 2009“ gesammelt wurden.

So erstellen Sie diesen Bericht:

1. Klicken Sie auf die Navigationsschaltfläche **Standardberichte**.

2. Klicken Sie mit der rechten Maustaste auf den Bericht, den Sie anpassen wollen, und dann auf **Neu ► Benutzerdefinierter Bericht**. Daraufhin wird der „Assistent für benutzerdefinierte Berichte“ angezeigt.

3. Sobald der Begrüßungsdialog erscheint, klicken Sie auf **Weiter**.

Assistent für benutzerdefinierten Bericht

Scan oder Zeitraum (Datum/Uhrzeit)

Geben Sie den Scan bzw. den Zeitbereich (Datum/Uhrzeit) an, für die der Bericht gelten soll.

Die Berichte werden die Ergebnisse des Sicherheits-Scans aus, die bei den vergangenen Netzwerksicherheits-Scans gesammelt wurden.

Wählen Sie die Scan-Ergebnisse aus, die vom Bericht verwendet werden:

- Letzter Scan:
Mit dieser Option erzeugen Sie Berichte aus den Daten, die während des letzten Netzwerksicherheits-Scans gesammelt wurden.
- Spezifischer Scan:
Mit dieser Option erzeugen Sie Berichte aus den Daten, die bei einem bestimmten Netzwerksicherheits-Scan gesammelt wurden.
- Zeitraum (Datum/Uhrzeit) scannen:
Erzeugen Sie mit dieser Option Berichte aus den Scan-Ergebnisdaten, die während eines bestimmten Zeitraumes gesammelt wurden.

< Zurück Weiter > Abbrechen

Bild 15 – Auswählen der gewünschten Datenquellen

4. Klicken Sie auf die Option **Scans eines bestimmten Datums/Monats** und dann auf **Weiter**.

Assistent für benutzerdefinierten Bericht

Datum Uhrzeit

Geben Sie Datum und Uhrzeit für den Zeitraum des Berichts an.

Berichte mit Datums- und Uhrzeitangabe erfassen alle Scans, in dem ausgewählten Zeitraum und erzeugen die Ergebnisse in Abhängigkeit von den bei diesen Scans gefundenen Informationen.

- Relativ
Heute
- Tag
17 January 2009
- Monat
May Jahr: 2009
- Datumsbereich
Von: 17/01/2009 07:01:45
An: 17/01/2009 07:01:45

< Zurück Weiter > Abbrechen

Bild 16 – Auswählen des Zeitraums mit Datum und Uhrzeit

5. Klicken Sie auf die Option **Monat**, und geben Sie folgende Parameter ein:

- **Monat:** „Januar“.
- **Jahr:** „2009“.

6. Klicken Sie auf **Weiter**, um zum Dialog „Datenfilter“ zu wechseln.

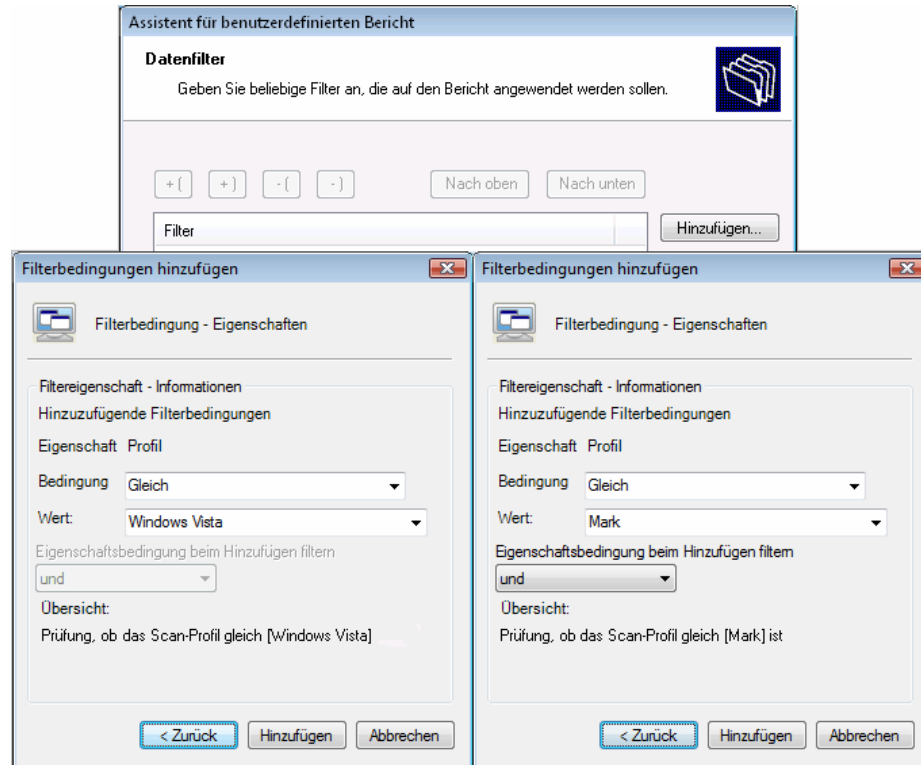


Bild 17 – Dialog „Filterbedingungen“

7. Klicken Sie auf die Schaltfläche **Hinzufügen**, und konfigurieren Sie die Parameter für Filter 1 wie folgt:

- **Filterbedingung:** Host-Name
- **Bedingung:** Gleich
- **Wert:** „Mark“.

8. Klicken Sie auf **Hinzufügen**, um die Filterkonfigurationseinstellungen zu übernehmen.

9. Klicken Sie erneut auf die Schaltfläche **Hinzufügen**, und konfigurieren Sie die Parameter für Filter 2 wie folgt:

- **Filterbedingung:** „Betriebssystem“
- **Bedingung:** „Gleich“
- **Wert:** „Windows Vista“
- **Filtereigenschaftsbedingungen:** „und“

10. Klicken Sie auf **Hinzufügen**, um die Filterkonfigurationseinstellungen zu übernehmen.

11. Klicken Sie auf **Weiter**, und geben Sie folgende Parameter ein.

- **Berichtname:** „Übersichtsbericht über Sicherheitsrisiken im Netzwerk für November 2008“
- **Berichtstitel:** „Netzwerksicherheits-Scans für den Host Mark“

- **Berichtbeschreibung:** „Dieser Bericht zeigt in einer Übersicht die für den Host „Mark“ im November 2008 gefundenen Sicherheitsrisiken.“
12. Klicken Sie auf **Weiter**, um zum letzten Dialog zu wechseln.
 13. Klicken Sie auf **Fertigstellen**, um die Konfigurationseinstellungen für den benutzerdefinierten Bericht zu übernehmen.

4.4 Starten eines Benutzerdefinierten Berichts

So starten Sie einen benutzerdefinierten Bericht:

1. Klicken Sie auf die Schaltfläche **Benutzerdefinierte Berichte**.
2. Klicken Sie mit der **rechten Maustaste** auf den **benutzerdefinierten Bericht**, den Sie erstellen wollen und dann auf „Erstellen“.

4.5 Bearbeiten eines benutzerdefinierten Berichts

So bearbeiten Sie die Konfigurationseinstellungen eines benutzerdefinierten Berichts:

1. Klicken Sie auf die Navigationsschaltfläche **Benutzerdefinierte Berichte**.

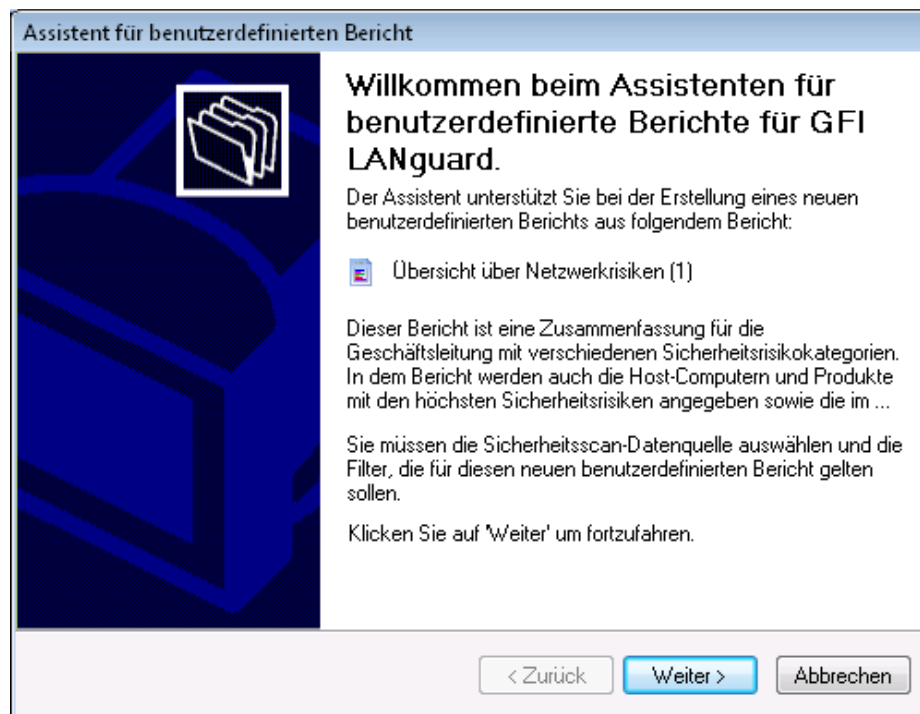


Bild 18 – Assistent für den benutzerdefinierten Bericht: Begrüßungsdialo

2. Klicken Sie mit der rechten Maustaste auf den benutzerdefinierten Bericht, den Sie verändern wollen und dann auf **Bearbeiten**. Es wird der „Assistent für benutzerdefinierte Berichte“ angezeigt, mit dem Sie die gewünschten Änderungen vornehmen können.

HINWEIS: Weitere Informationen zur Konfiguration der Parameter eines benutzerdefinierten Berichts finden Sie im Abschnitt „Erstellen eines benutzerdefinierten Berichts“ in diesem Kapitel.

4.6 Löschen eines benutzerdefinierten Berichts

Benutzerdefinierten Bericht löschen:

1. Klicken Sie auf die Navigationsschaltfläche **Benutzerdefinierte Berichte**.
2. Klicken Sie mit der rechten Maustaste auf den benutzerdefinierten Bericht, den Sie permanent aus der Liste entfernen wollen, und klicken Sie auf **Löschen**.
3. Klicken Sie zur Bestätigung auf **Ja**.

4.7 Hinzufügen benutzerdefinierter Bericht zu den häufig benötigten Berichten

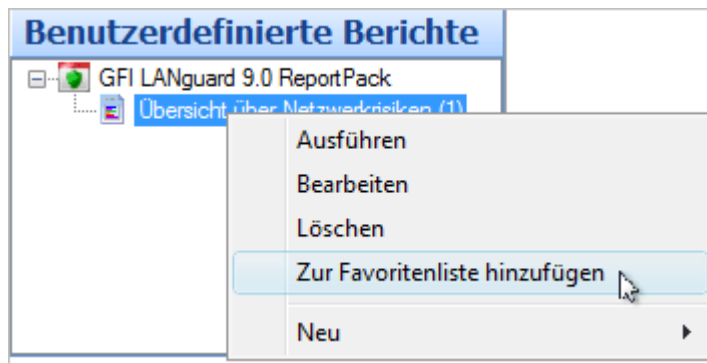


Bild 19 – Navigationsschaltfläche „Häufig benötigte Berichte“

Sie können häufig benötigte Berichte über die Schaltfläche **Häufig benötigte Berichte** zu Gruppen zusammenfassen und so leichter aufrufen. So ergänzen Sie einen benutzerdefinierten Bericht in der Liste der häufig benötigten Berichte:

1. Klicken Sie auf die Navigationsschaltfläche **Benutzerdefinierte Berichte**, um die Liste der verfügbaren Berichte anzuzeigen.
2. Klicken Sie mit der rechten Maustaste auf den benutzerdefinierten Bericht, um ihn zur Liste der häufig benötigten Berichte hinzuzufügen, und klicken Sie dann auf die Option **Zur Liste der häufig benötigten Berichte hinzufügen**.
3. Klicken Sie zur Bestätigung auf **Ja**.

5. Zeitplanung von Berichten

5.1 Einführung

Im GFI ReportCenter können Sie Berichte gemäß einem vordefinierten Zeitplan sowie in definierten Intervallen erstellen. Auf diese Weise können Sie Berichte automatisch erstellen, die regelmäßig benötigt werden.

Außerdem können Sie GFI ReportCenter so konfigurieren, dass die zeitabhängigen Berichte automatisch per E-Mail verteilt werden. Für jeden zeitabhängigen Bericht können Sie benutzerspezifische E-Mail-Parameter konfigurieren, beispielsweise eine Liste der Berichtempfänger und das Dateiformat (z. B. PDF), in dem der Bericht an die E-Mail angehängt wird.

Nutzen Sie die Funktion zur Berichtszeitplanung, um die Berichterzeugung zu automatisieren. Sie können beispielsweise umfangreiche Berichte zeitlich so planen, dass sie nach Arbeitsschluss erstellt werden und dann automatisch an die gewünschten Empfänger versenden. Auf diese Weise optimieren Sie die Verfügbarkeit Ihrer Systemressourcen während der Arbeitszeit und vermeiden mögliche Unterbrechungen des Arbeitsablaufs.

Sie können sowohl Standardberichte als auch benutzerdefinierte Berichte automatisch, zeitabhängig erzeugen.

5.2 Zeitplanung eines Berichts

So planen Sie einen zeitabhängigen Bericht:

1. Klicken Sie auf die Optionsseite **Standardberichte /benutzerdefinierte Berichte**.
2. Klicken Sie mit der rechten Maustaste auf den Bericht, für den Sie eine Zeit planen wollen, und dann auf **Neu ► Zeitabhängiger Bericht**. Daraufhin wird der „Assistent für zeitabhängige Berichte“ angezeigt. Klicken Sie auf **Weiter**, um fortzufahren.
3. Klicken Sie auf die Netzwerksicherheits-Scandaten, die von diesem Bericht verwendet werden sollen.

Assistent für zeitabhängige Berichte

Zeitplan

Geben Sie an, mit welchem Zeitplaner automatisch der Bericht erstellt werden soll.

Zeitabhängige Berichte können Sie entweder einmalig durch Angabe eines Datums und einer Uhrzeit erstellen oder in einem Zeitraum ab einer bestimmten Zeit immer wieder.

Diesen Bericht (einmal) zu folgendem Datum/folgender Uhrzeit erstellen:

Datum/Uhrzeit: 17/01/2009 07:38:58

Diesen Bericht erstellen - alle:

Intervall: 1 Stunden

Beginndatum/Beginn und Uhrzeit: 05/11/2009 05:19:56

< Zurück Weiter > Abbrechen

Bild 20 – Der Assistent für zeitabhängige Berichte mit dem Dialog „Zeitplanung“

4. Geben Sie die Parameter für die Zeitplanung des Berichts ein (Datum/Uhrzeit/Häufigkeit). Klicken Sie auf **Weiter**, um fortzufahren.

Assistent für zeitabhängige Berichte

Erweiterte Einstellungen

Passen Sie die Optionen für Berichtverteilung und Berichtspeicherung an.

Sie können den erzeugten Bericht per E-Mail an eine Empfängerliste senden oder in einem Ordner in Ihrem Dateisystem speichern. Klicken Sie auf die Schaltfläche 'Einstellungen' des betreffenden Dialogteils um die Send- und Speicheroptionen für den Bericht genauer zu konfigurieren.

In Datei exportieren

Klicken Sie auf die Schaltfläche 'Einstellungen' um die Optionen für die Berichtspeicherung benutzerspezifisch anzupassen, und geben Sie Dateiformat und

Einstellungen

Versand per E-Mail

Klicken Sie auf die Schaltfläche 'Einstellungen' um die E-Mail-Einstellungen für die Berichtverteilung benutzerdefiniert zu konfigurieren.

Einstellungen

< Zurück Weiter > Abbrechen

Bild 21 – Der Assistent für zeitabhängige Berichte mit dem Dialog „Erweiterte Einstellungen“

5. Um den erzeugten Bericht in eine Datei zu exportieren, klicken Sie auf die Option **In Datei exportieren**. Um die Konfigurationseinstellungen für den Bericht „Export anzupassen“, klicken Sie auf die Schaltfläche **Einstellungen** unter dieser Option.

HINWEIS: Weitere Informationen, wie Sie die Einstellungen zum Export in eine Datei konfigurieren, finden Sie in Abschnitt

„Konfigurieren der Optionen zum Berichtsexport in eine Datei“ in diesem Kapitel.

6. Um automatisch erzeugte Berichte per E-Mail zu verteilen, klicken Sie auf die Option „Per E-Mail versenden“. Um die E-Mail-Einstellungen für die Berichtverteilung anzupassen, klicken Sie auf die Schaltfläche **Einstellungen** unter dieser Option.

HINWEIS: Informationen zur Konfiguration der E-Mail-Einstellungen finden Sie unter „Konfigurieren der Bericht-E-Mail-Optionen“ in diesem Kapitel.

7. Geben Sie den Namen und die Beschreibung für diesen zeitabhängigen Bericht ein. Klicken Sie auf **Weiter**, um fortzufahren.

8. Klicken Sie auf **Fertig stellen**, um Ihre Einstellungen zu übernehmen.

5.3 Konfigurieren der erweiterten Einstellungen

Mit GFI LANguard ReportPack können Sie zeitabhängige Berichte in einem bestimmten Dateiformat exportieren und diese Berichte per E-Mail automatisch verteilen. Dazu benötigen Sie eine Reihe von Parametern (beispielsweise die E-Mail-Adressen der Empfänger), die Sie bei der Konfiguration der zeitabhängigen Berichte definieren oder als Standardeinstellung für den Berichtsexport und die Verteilung bei der Installation des ReportPack konfigurieren.

HINWEIS: Der Assistent zur Zeitplanung der Berichte ist standardmäßig so konfiguriert, dass er für die Parameter für den Berichtsexport und die Berichtverteilung die Standardeinstellungen verwendet.

Berichtsexportformate

Zeitabhängige Berichte können in diverse Formate exportiert werden. Unterstützt werden folgende Dateiformate:

	Format	Beschreibung
1	Adobe Acrobat (.PDF)	Mit diesem Format können Sie Berichte auf verschiedene Systeme verteilen, beispielsweise Macintosh- und Linux-Computer und dabei das Layout behalten.
2	MS Excel (.XLS)	Bei diesem Format können Sie den Bericht später weiterverarbeiten und umfangreichere Berechnungen mit einem anderen (externen Programm, wie Microsoft Excel) durchführen.
3	MS Word (.DOC)	Mit diesem Format können Sie über Microsoft Word auf den Bericht zugreifen.
4	Rich Text Format (*.RTF)	Mit diesem Format speichern Sie den Bericht in einem kleinen Format, das von den verschiedenen Textverarbeitungsprogrammen auf verschiedenen Betriebssystemen verwendet werden kann.

5.3.1 Konfigurieren der Optionen zum Export des Berichts in eine Datei

So konfigurieren Sie die Einstellungen zum Export eines zeitabhängigen Berichts in eine Datei:

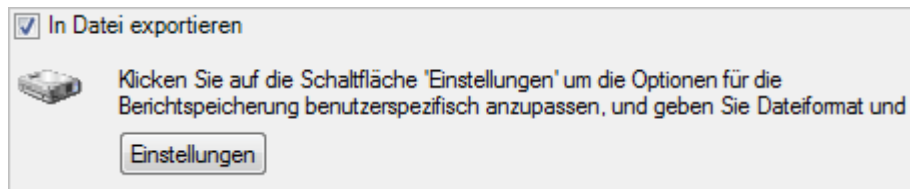


Bild 22 – Dialog „Erweiterte Einstellungen“ mit der Schaltfläche „In Datei exportieren“

1. Klicken Sie im Dialog **Erweiterte Einstellungen** auf die Schaltfläche **Einstellungen** unter der Option „In Datei exportieren“.

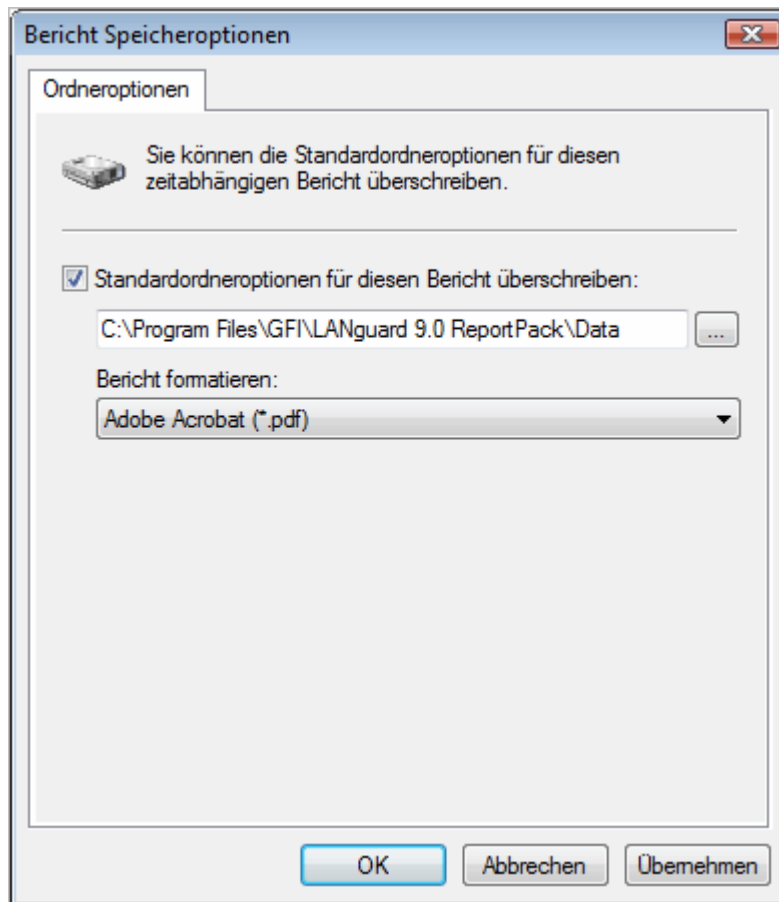


Bild 23 – Erweiterte Einstellungen: Optionen für den Export in eine Datei

2. Klicken Sie auf die Option **Standardordneroptionen für diesen Bericht überschreiben:**
3. Geben Sie den Computerpfad an, unter dem der exportierte Bericht gespeichert werden soll.
4. Geben Sie das Dateiformat an, in dem der exportierte Bericht gespeichert werden soll.
5. Klicken Sie auf **OK**, um die Konfigurationseinstellungen zu übernehmen.

HINWEIS: Informationen zur Konfiguration der Standardeinstellungen für den Export in eine Datei finden Sie in Abschnitt „Konfigurieren der Standardoptionen zeitabhängiger Berichte“ in diesem Handbuch.

5.3.2 Konfigurieren der E-Mail-Optionen für Berichte

So konfigurieren Sie die E-Mail-Optionen für einen zeitabhängigen Bericht:

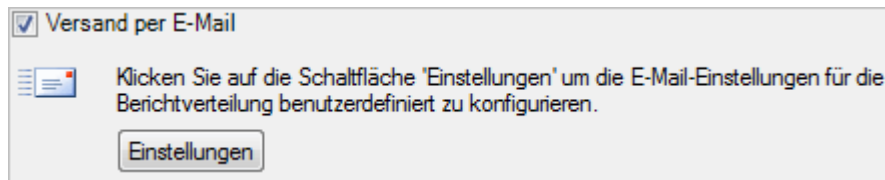


Bild 24 – Dialog „Erweiterte Einstellungen“ mit den Einstellungen „Per E-Mail versenden“.

1. Klicken Sie im Dialog **Erweiterte Einstellungen** auf die Schaltfläche **Einstellungen** unter der Option **Per E-Mail versenden**.

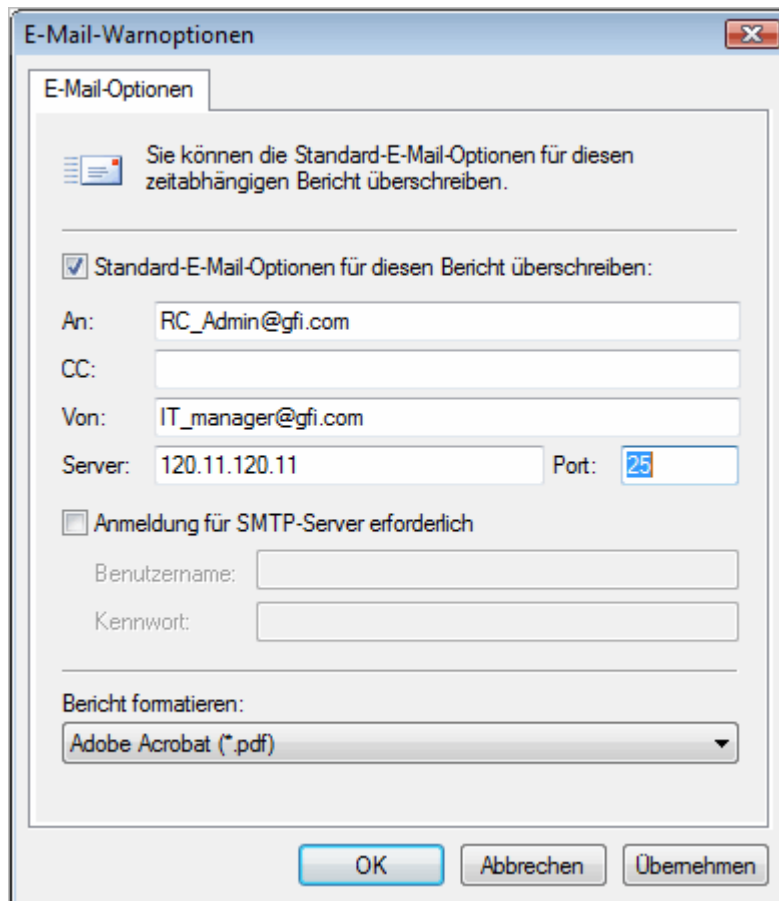


Bild 25 – Verteiloptionen für den Bericht

2. Klicken Sie auf die Option **Standard-E-Mail-Optionen für diesen Bericht überschreiben:**
3. Geben Sie die folgenden Parameter ein.
 - **An/cc:** Geben Sie die E-Mail-Adressen an, an die der erzeugte Bericht versendet werden soll.
 - **Von:** Geben Sie das E-Mail-Konto an, das zum Versand des Berichts verwendet werden soll.
 - **Server:** Geben Sie Name/IP-Adresse Ihres SMTP-E-Mail-Servers (für abgehende E-Mails) an. Wenn der angegebene Server eine Authentifizierung benötigt, klicken Sie auf die Option **SMTP-Server erfordert eine Anmeldung** und geben die Anmeldedaten in den Feldern **Benutzername** und **Kennwort** ein.
 - **Berichtformat:** Berichte werden als E-Mail-Anhänge versendet. Wählen Sie das Dateiformat aus, indem Sie Ihren Bericht versenden wollen.

4. Klicken Sie auf **OK**, um die Konfigurationseinstellungen zu übernehmen.

5.4 Anzeigen der Liste zeitabhängiger Berichte

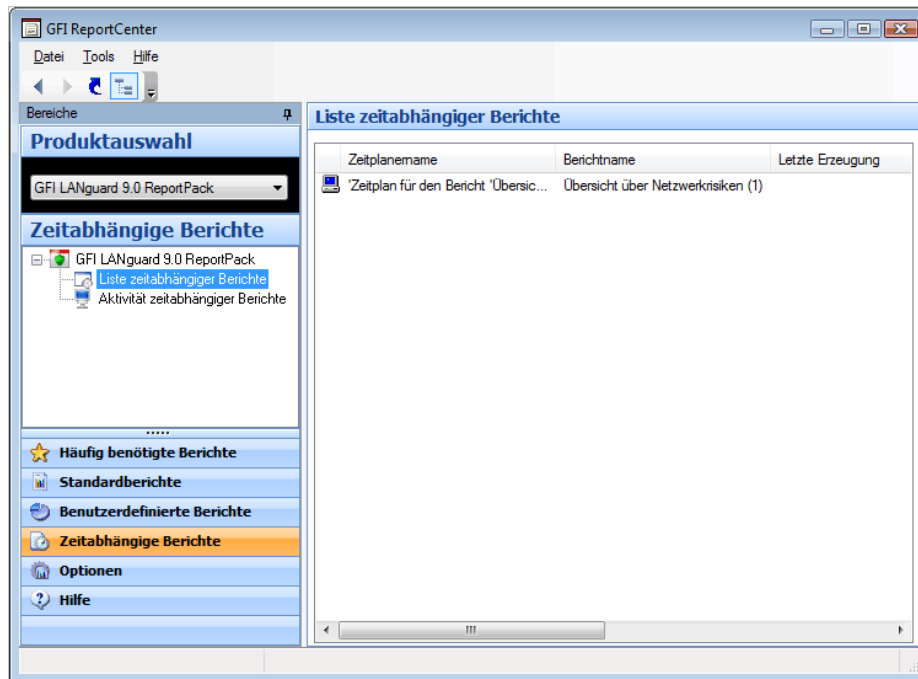


Bild 26 – Liste der zeitabhängigen Berichte

Klicken Sie auf die Navigationsschaltfläche **Zeitabhängige Berichte**, um die Liste der zeitabhängigen Berichte anzuzeigen, die zurzeit für automatische Erstellung konfiguriert sind. Diese Informationen finden Sie auf der rechten Seite der Verwaltungskonsolle mit folgenden Details:

- **Zeitplanname:** der benutzerdefinierte Name, der bei der Erstellung des neuen zeitabhängigen Berichts angegeben wurde.
- **Berichtname:** Die Namen des Standardberichts bzw. benutzerdefinierten Berichts, der erstellt wird.
- **Letzte Erstellung:** gibt die Zeit (Datum/Uhrzeit) an, zu der der Bericht das letzte Mal erstellt wurde.
- **Nächste Erstellung:** gibt den Zeitpunkt (Datum/Uhrzeit) an, zu dem der Bericht das nächste Mal erstellt werden soll.
- **Beschreibung:** Die Beschreibung, die Sie für jeden Zeitplan eingegeben haben.
- **ReportPack:** Die Version von GFI LANguard, die den Bericht erstellte.

5.5 Anzeigen der Aktivität zeitabhängiger Berichte

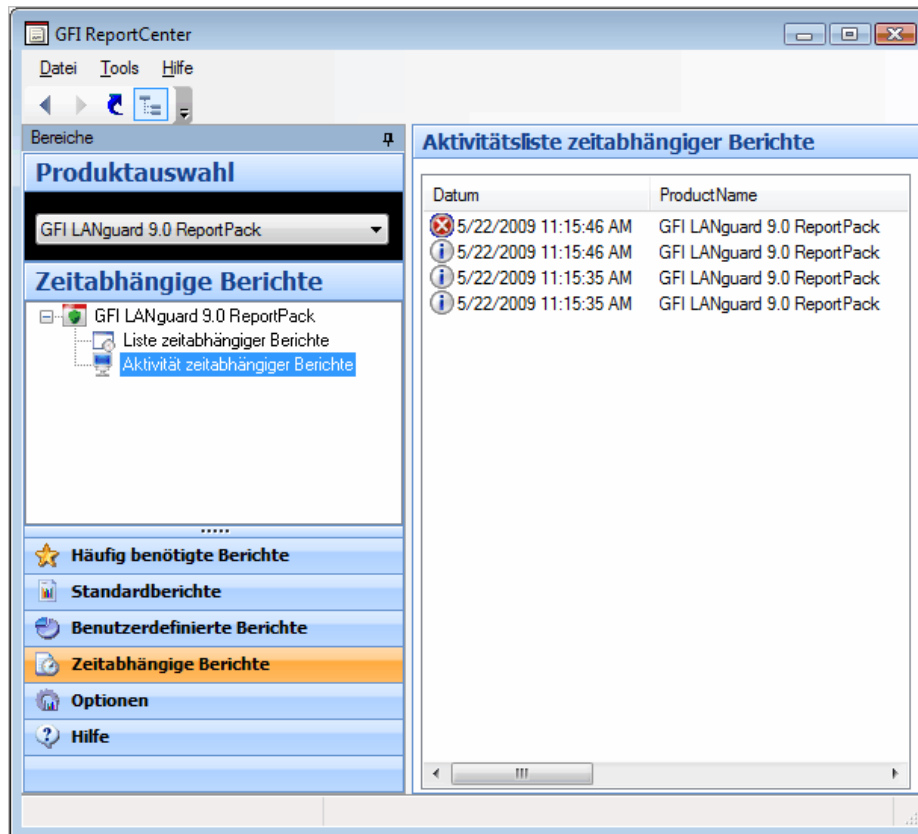





Bild 27 – Überwachung für zeitabhängige Aktivitäten

GFI ReportCenter enthält auch eine Überwachung für zeitabhängige Aktivitäten, mit der Sie Ereignisse anzeigen können, die mit allen zeitabhängigen Berichten zusammenhängen, die ausgeführt wurden.

Um die Überwachung zeitabhängiger Aktivitäten zu öffnen, klicken Sie auf die Navigationsschaltfläche **zeitabhängiger Bericht** und dann auf den Knoten **Aktivität zeitabhängiger Berichte**. Daraufhin werden die Aktivitätsdaten auf der rechten Seite der Verwaltungskonsole des GFI ReportCenter angezeigt.

Die Aktivitätsüberwachung zeigt folgende Ereignisse an:

-  **Information:** Der zeitabhängige Bericht wurde erfolgreich ausgeführt und per E-Mail versendet bzw. auf Festplatte gespeichert.
-  **Vorsicht:** Der zeitabhängige Bericht wurde nicht ausgeführt, weil die Produktlizenz ungültig ist oder abgelaufen ist.
-  **Fehler:** Der zeitabhängige Bericht wurde nicht ausgeführt, weil eine bestimmte Bedingung/ein bestimmtes Ereignis eintrat. Typische Bedingungen:

- Fehler beim Versuch, den erzeugten Bericht in einem bestimmten Ordner zu speichern (beispielsweise bei fehlendem Speicherplatz).
- Fehler beim Versuch, den erzeugten Bericht per E-Mail zu versenden (weil beispielsweise der SMTP-Server, der in den

Einstellungen von GFI ReportCenter konfiguriert ist, nicht erreichbar ist).

Die Aktivitätsüberwachung erfasst die folgenden Informationen und listet diese auf:

- **Datum:** Datum und Uhrzeit des Zeitpunkts, als der zeitabhängige Bericht ausgeführt wurde.
- **Produktname:** Der Name des GFI-Produkts, zu dem der Bericht gehört.
- **Typ:** Die Ereignisklassifizierung – Fehler, Information oder Warnhinweis
- **Beschreibung:** Informationen zum Status des zeitabhängigen Berichts, der ausgeführt wurde. Format und Inhalt für die Aktivitätsbeschreibung richten sich nach der Ereignisart.

HINWEIS: Die Beschreibung ist oft die wertvollste Information, da sie angibt, was bei Ausführung eines zeitabhängigen Berichts passierte, oder auf die Bedeutung des Ereignisses hinweist.

5.6 Aktivieren/Deaktivieren eines zeitabhängigen Berichts

Zeitabhängige Berichte können nach Bedarf aktiviert oder deaktiviert werden. Mit der Navigationsschaltfläche **zeitabhängige Berichte** zeigen Sie die Liste der zeitabhängigen Berichte an sowie deren aktuellen Status. Das Symbol an der linken Seite jedes zeitabhängigen Berichts zeigt dessen Status an:



Dieses Symbol zeigt, dass der zeitabhängige Bericht deaktiviert ist.



Dieses Symbol zeigt, dass der zeitabhängige Bericht aktiviert ist bzw. noch aussteht.

Um einen zeitabhängigen Bericht zu aktivieren oder zu deaktivieren, klicken Sie mit der rechten Maustaste auf den betreffenden Bericht und dann auf **Aktivieren/Deaktivieren**.

5.7 Bearbeiten eines zeitabhängigen Berichts

So nehmen Sie Änderungen an den Konfigurationseinstellungen eines zeitabhängigen Berichts vor:

1. Klicken Sie auf die Navigationsschaltfläche **Zeitabhängige Berichte**.
2. Klicken Sie mit der rechten Maustaste auf den zeitabhängigen Bericht, den Sie neu konfigurieren wollen, und dann auf **Eigenschaften**. Daraufhin wird der „Assistent für zeitabhängige Berichte“ angezeigt.

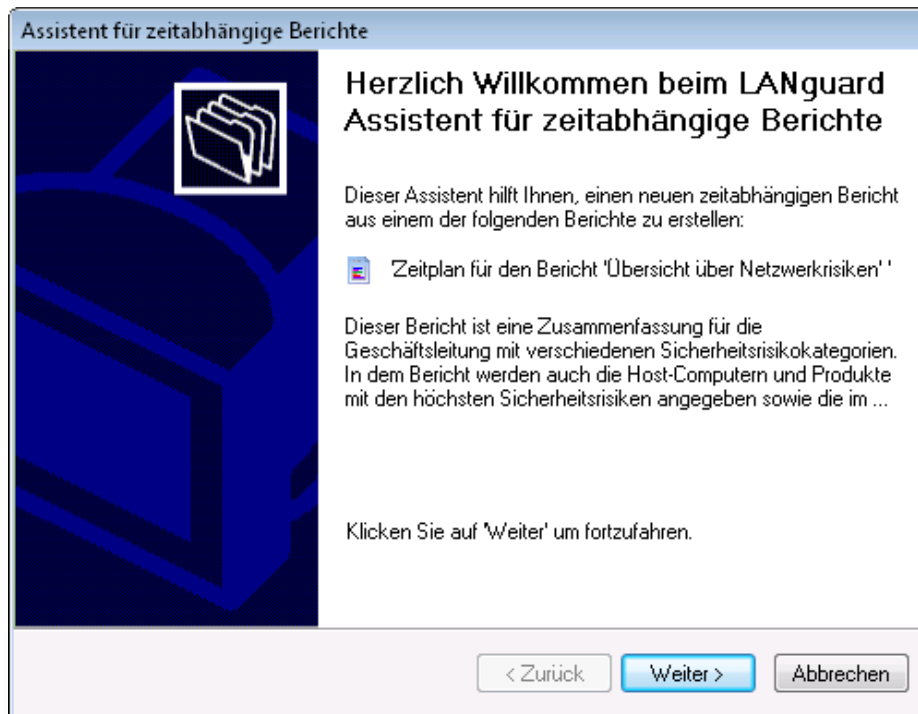


Bild 28 - Assistent für zeitabhängige Berichte

3. Klicken Sie auf **Weiter** und führen Sie die gewünschten Änderungen durch. Informationen zur Konfiguration der Parameter eines zeitabhängigen Berichts finden Sie im Abschnitt „Erstellen eines zeitabhängigen Berichts“ in diesem Kapitel.

Löschen eines zeitabhängigen Berichts

So löschen Sie einen zeitabhängigen Bericht:

1. Klicken Sie auf die Navigationsschaltfläche **Zeitabhängige Berichte**.
2. Klicken Sie mit der rechten Maustaste auf den zeitabhängigen Bericht, den Sie dauerhaft aus der Liste entfernen wollen, und klicken Sie dann auf **Löschen**.

5.8 Beispiel: Zeitplanung eines Berichts

Dieses Beispiel zeigt, wie Sie einen Softwareüberprüfungsbericht zeitlich planen, der folgende Aufgaben ausführt:

- Den ersten Bericht am 12.05.2009 um 20:00 Uhr erzeugen.
- Den gleichen Bericht jeweils monatlich wieder erzeugen.
- Den erzeugten Bericht bzw. die erzeugten Berichte im PDF-Format in den Ordner „C:\Monthly Reports“ exportieren.
- Den erzeugten Bericht mit folgenden benutzerdefinierten Parametern per E-Mail versenden:
- Von folgendem E-Mail-Konto versenden: „RC_Admin@gfi.com“
- An folgendes E-Mail-Konto senden: „IT_manager@gfi.com“
- SMTP-Server-Details: „120.11.120.11“.

So erstellen Sie den zeitabhängigen Bericht:

1. Klicken Sie auf die Navigationsschaltfläche **Standardberichte**.

2. Klicken Sie mit der rechten Maustaste auf die Option **Übersicht über Sicherheitsrisiken im Netzwerk** und dann auf **Neu ► Zeitabhängiger Bericht**. Sobald der Begrüßungsdialog angezeigt wird, klicken Sie auf Weiter.

The screenshot shows a dialog box titled "Assistent für zeitabhängige Berichte". The main heading is "Scan oder Zeitraum (Datum/Uhrzeit)". Below the heading, there is a text box: "Geben Sie den Scan bzw. den Zeitbereich (Datum/Uhrzeit) an, für die der Bericht gelten soll." To the right of this text is a folder icon. Below this, there is explanatory text: "Die Berichte werten die Ergebnisse des Sicherheits-Scans aus, die bei den vergangenen Netzwerksicherheits-Scans gesammelt wurden." and "Wählen Sie die Scan-Ergebnisse aus, die vom Bericht verwendet werden:". There are three radio button options:

- Letzter Scan: Mit dieser Option erzeugen Sie Berichte aus den Daten, die während des letzten Netzwerksicherheits-Scans gesammelt wurden.
- Spezifischer Scan: Mit dieser Option erzeugen Sie Berichte aus den Daten, die bei einem bestimmten Netzwerksicherheitsscan gesammelt wurden.
- Zeitraum (Datum/Uhrzeit) scannen: Erzeugen Sie mit dieser Option Berichte aus den Scan-Ergebnisdaten, die während eines bestimmten Zeitraumes gesammelt wurden.

 At the bottom right, there are three buttons: "< Zurück", "Weiter >", and "Abbrechen".

Bild 29 – Netzwerksicherheits-Scandaten auswählen

3. Klicken Sie auf die Option **Zeitraum (Datum/Uhrzeit) scannen**, um die Daten für diesen Bericht auszuwählen, und klicken Sie auf **Weiter**.

The screenshot shows the same dialog box, now at the "Datum Uhrzeit" step. The heading is "Datum Uhrzeit". Below it, the text says: "Geben Sie Datum und Uhrzeit für den Zeitraum des Berichts an." To the right is a folder icon. Below this, there is explanatory text: "Berichte mit Datums- und Uhrzeitangabe erfassen alle Scans, in dem ausgewählten Zeitraum und erzeugen die Ergebnisse in Abhängigkeit von den bei diesen Scans gefundenen Informationen." There are two radio button options:

- Relativ: This option has a dropdown menu currently showing "Heute". The dropdown list includes: "Heute", "Gestern", "Letzte sieben Tage", "Dieser Monat", and "Letzter Monat" (which is highlighted by a mouse cursor). Below the dropdown is a "Jahr:" field with "2009" selected.
- Datumsbereich: This option has two rows of input fields. The first row is "Von:" with a date field containing "17/01/2009" and a time field containing "07:42:39". The second row is "An:" with a date field containing "17/01/2009" and a time field containing "07:42:39".

 At the bottom right, there are three buttons: "< Zurück", "Weiter >", and "Abbrechen".

Bild 30 – Datum und Uhrzeit für den Netzwerkscan auswählen

4. Klicken Sie auf die Option **Relativ** und dann in der Dropdownliste auf „Letzter Monat“. Klicken Sie auf **Weiter**, um mit dem nächsten Dialog fortzufahren.

The screenshot shows the 'Assistent für zeitabhängige Berichte' dialog box with the 'Zeitplan' tab selected. The title bar reads 'Assistent für zeitabhängige Berichte'. Below the title bar, the section 'Zeitplan' is followed by the instruction: 'Geben Sie an, mit welchem Zeitplaner automatisch der Bericht erstellt werden soll.' To the right is a folder icon. The main text explains: 'Zeitabhängige Berichte können Sie entweder einmalig durch Angabe eines Datums und einer Uhrzeit erstellen oder in einem Zeitraum ab einer bestimmten Zeit immer wieder.' There are two radio button options: 'Diesen Bericht (einmal) zu folgendem Datum/folgender Uhrzeit erstellen:' and 'Diesen Bericht erstellen - alle:'. The first option has input fields for 'Datum/Uhrzeit' with values '17/01/2009' and '07:54:13'. The second option has an 'Intervall' field with '1' and a unit dropdown set to 'Stunden', and 'Beginndatum/Beginn und Uhrzeit' fields with values '05/12/2009' and '08:00:00'. At the bottom are three buttons: '< Zurück', 'Weiter >', and 'Abbrechen'.

Bild 31 – Zeitplanungsoptionen definieren

5. Um diesen Bericht monatlich zu erzeugen, klicken Sie auf die Option **Diesen Bericht erzeugen alle:** und legen das Intervall auf **30 Tage** fest.

6. Stellen Sie das Anfangsdatum ein auf '12.05.2009' und die Zeit auf '20:00 Uhr'. Klicken Sie auf **Weiter**, um fortzufahren.

The screenshot shows the 'Assistent für zeitabhängige Berichte' dialog box with the 'Erweiterte Einstellungen' tab selected. The title bar reads 'Assistent für zeitabhängige Berichte'. Below the title bar, the section 'Erweiterte Einstellungen' is followed by the instruction: 'Passen Sie die Optionen für Berichtverteilung und Berichtsspeicherung an.' To the right is a folder icon. The main text explains: 'Sie können den erzeugten Bericht per E-Mail an eine Empfängerliste senden oder in einem Ordner in Ihrem Dateisystem speichern. Klicken Sie auf die Schaltfläche 'Einstellungen' des betreffenden Dialogteils um die Sende- und Speicheroptionen für den Bericht genauer zu konfigurieren.' There are two checked checkboxes: 'In Datei exportieren' and 'Versand per E-Mail'. Each checkbox has an 'Einstellungen' button next to it. The 'In Datei exportieren' section includes a floppy disk icon and the text: 'Klicken Sie auf die Schaltfläche 'Einstellungen' um die Optionen für die Berichtsspeicherung benutzerspezifisch anzupassen, und geben Sie Dateiformat und'. The 'Versand per E-Mail' section includes an envelope icon and the text: 'Klicken Sie auf die Schaltfläche 'Einstellungen' um die E-Mail-Einstellungen für die Berichtverteilung benutzerdefiniert zu konfigurieren.' At the bottom are three buttons: '< Zurück', 'Weiter >', and 'Abbrechen'.

Bild 32 – Dialog „Erweiterte Einstellungen“

7. Klicken Sie im Dialog **Erweiterte Einstellungen** auf die Schaltfläche **Einstellungen** unter der Option **In Datei exportieren**.

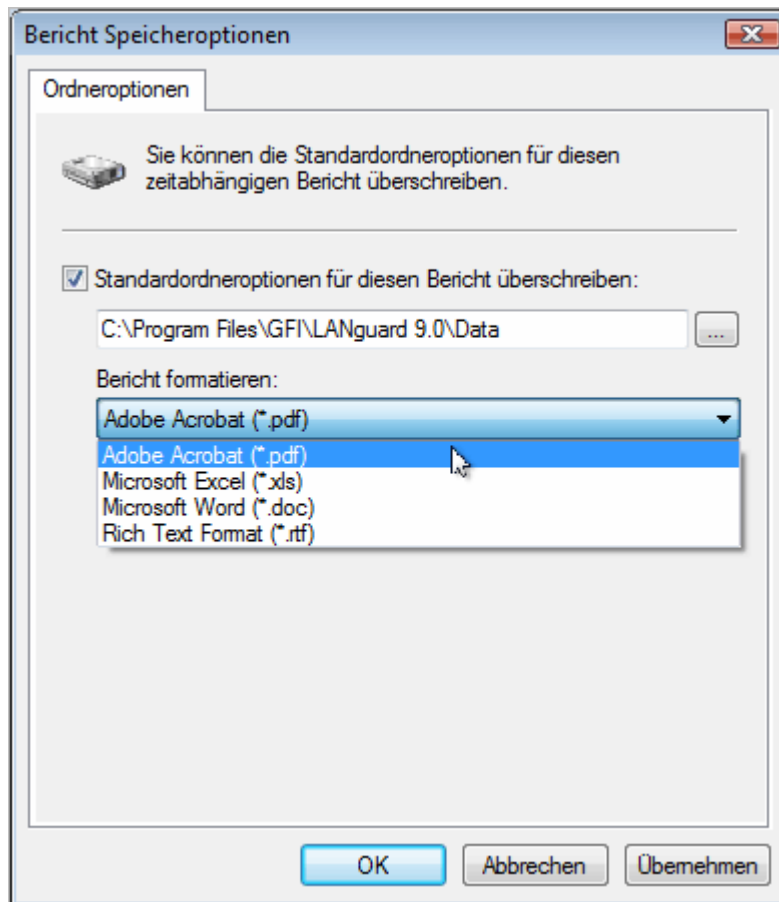


Bild 33 – Erweiterte Einstellungen: Optionen für den Export in eine Datei

8. Klicken Sie auf die Option **Standardordneroptionen für diesen Bericht überschreiben**:

9. Geben Sie den vollständigen Pfad zum Speichern des Berichts ein, beispielsweise „C:\Monthly Reports“.

10. Klicken Sie in dem Dropdownfeld für das Berichtformat auf die Option **PDF** und dann auf **OK**.

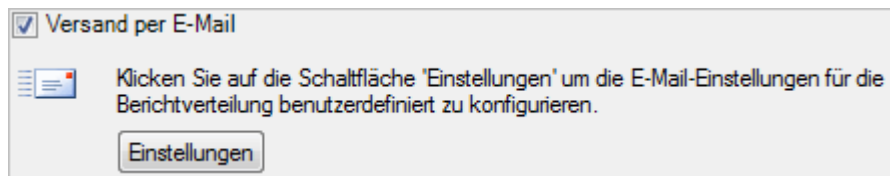


Bild 34 – Dialog „Erweiterte Einstellungen“ mit den Einstellungen „Per E-Mail versenden“.

11. Klicken Sie im Dialog **Erweiterte Einstellungen** auf die Schaltfläche **Einstellungen** unter der Option **Per E-Mail versenden**.

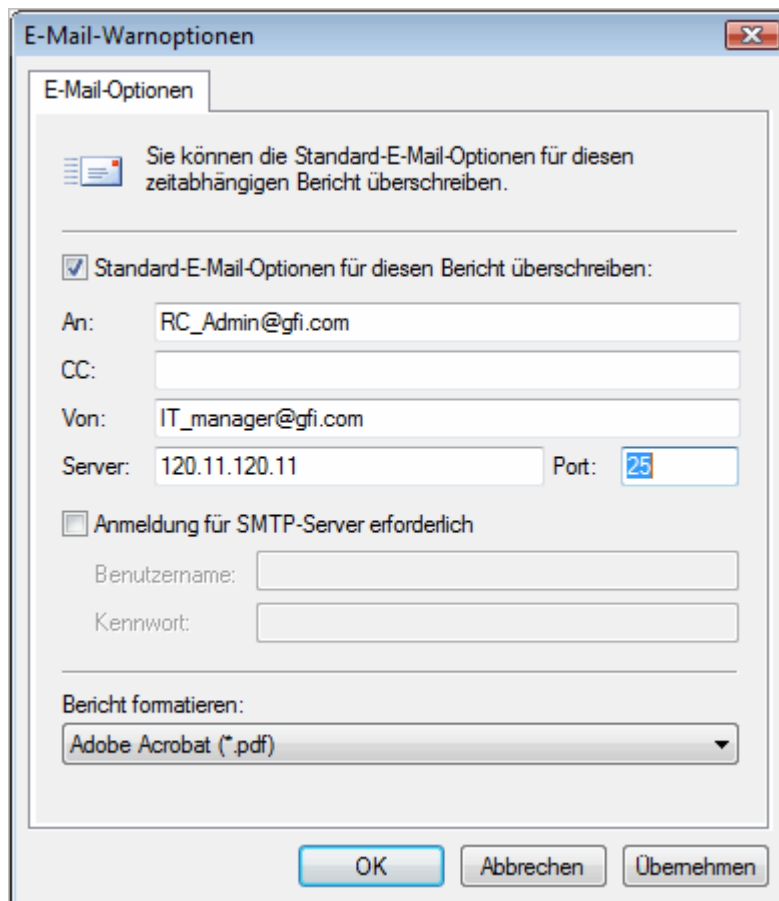


Bild 35 – Verteiloptionen für den Bericht


12. Klicken Sie auf die Option **Standard-E-Mail-Optionen für diesen Bericht überschreiben:**

13. Geben Sie die folgenden Parameter ein

- **An:** 'RC_Admin@gfi.com'
- **Von:** „IT_manager@gfi.com“
- **Server:** „120.11.120.11“.

14. Wählen Sie in dem Dropdownfeld für das Berichtformat **PDF** aus und klicken Sie dann auf **OK**, um Ihre E-Mail-Einstellungen zu übernehmen.

Assistent für zeitabhängige Berichte

Name und Beschreibung 

Geben Sie Name und Beschreibung für diesen benutzerdefinierten Bericht ein.

Name, Titel und Beschreibung eines benutzerdefinierten Berichts sollen den Bericht eindeutig in einer Gruppe benutzerdefinierter Berichte kennzeichnen. Der Name für den benutzerdefinierten Bericht muss einmalig sein.

Berichtname:

Berichtstitel:

Berichtbeschreibung:

Deckblatt anzeigen

< Zurück Weiter > Abbrechen

Bild 36– benutzerdefinierter Bericht, Name und Beschreibung

15. Klicken Sie auf **Weiter**, und geben Sie folgende Parameter ein.
- **Berichtname:** „Monatlicher Bericht: „Softwareüberprüfung“
 - **Berichtstitel:** „Softwareüberprüfung – Berichte für die Geschäftsleitung“
 - **Berichtbeschreibung:** Dieser Bericht wird monatlich erzeugt und zeigt in einer Übersicht für die Geschäftsleitung, welche Software im Netzwerk installiert ist.
16. Klicken Sie auf **Weiter**, um mit dem letzten Dialog fortzufahren.
17. Klicken Sie auf **Fertigstellen**, um die Konfigurationseinstellungen für den benutzerdefinierten Bericht zu übernehmen.

6. Konfiguration der Standardoptionen

6.1 Einführung

Mit GFI LANguard ReportPack können Sie einen Standardparametersatz konfigurieren, den Sie dann zum Erzeugen von Berichten verwenden. Diese Parameter werden bei der Installation erstmals definiert. Sie können jedoch diese Parameter über die Navigationsschaltfläche **Optionen** und das Menü **Tools** in der Verwaltungskonsole des GFI ReportCenter jederzeit neu konfigurieren.

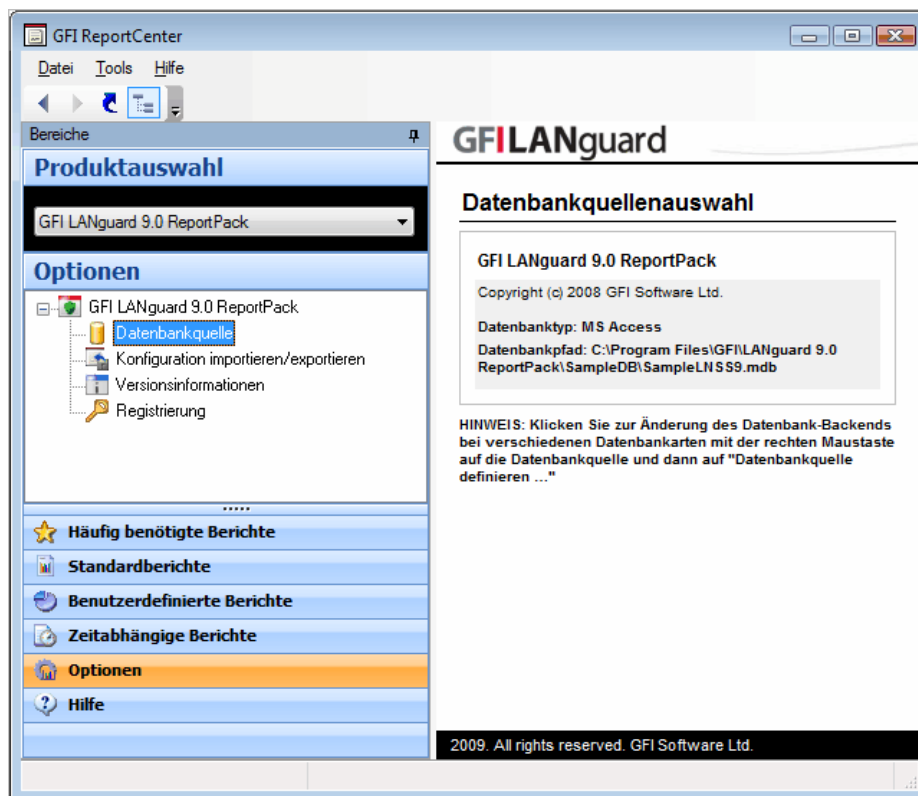


Bild 37 – Navigationsschaltfläche Optionen und Menü Tools

Über die Navigationsschaltfläche **Optionen** können Sie folgenden Parameter konfigurieren:

- **Datenbankquelle:** Definieren Sie mit diesem Knoten den Datenbank-Backend, von dem ReportPack die benötigten Berichtsdaten extrahiert.

Über das Menü **Tools** können Sie folgende Parameter konfigurieren:

- **Standard-Zeitplanereinstellungen:** Mit dieser Menüoption konfigurieren Sie die Standardparameter für den Export in eine Datei sowie den E-Mail-Versand der zeitabhängigen Berichte.

Sie können Ihre Konfigurationseinstellungen für ReportPack auch über den Knoten **Konfiguration importieren/exportieren** im Untermenü **Optionen** sichern. Exportierte Konfigurationen können Sie in eine separate Instanz von GFI ReportCenter importieren, sofern die gleichen ReportPacks auf beiden Instanzen installiert sind.

6.2 Konfigurieren der Datenbankquelle: Microsoft SQL Server

So konfigurieren Sie MS SQL-Server als Datenbankquelle:

1. Klicken Sie auf die Navigationsschaltfläche **Optionen**.
2. Klicken Sie mit der rechten Maustaste auf den Knoten **Datenbankquelle** und wählen Sie **Datenbankquelle festlegen ...** aus. Damit wird der Dialog für die Datenbankquellenkonfiguration angezeigt.

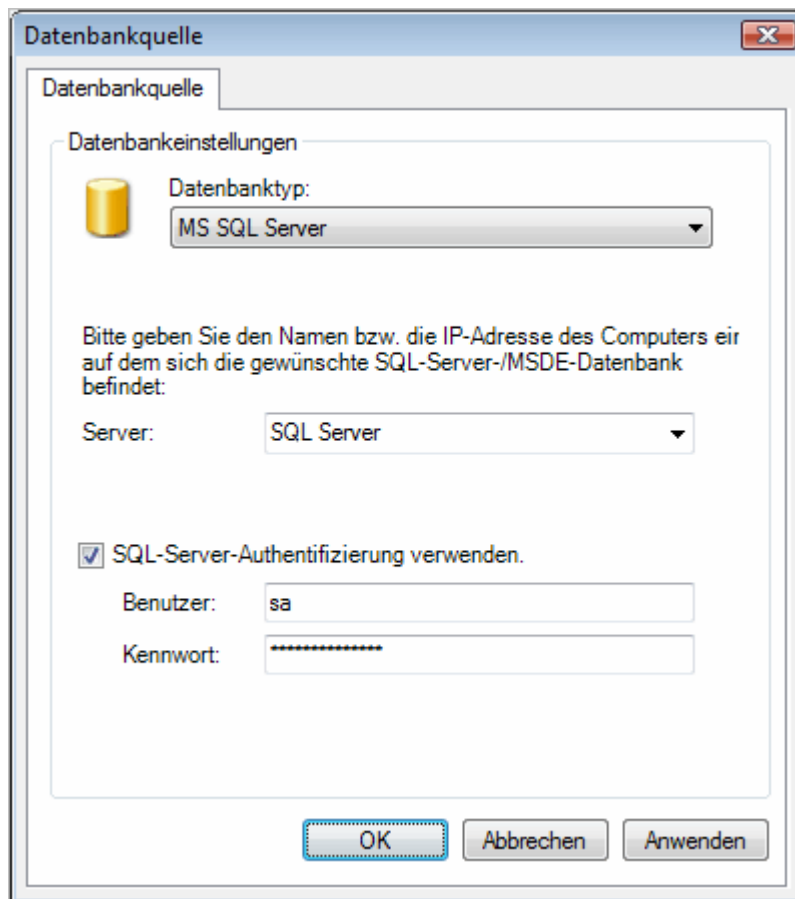


Bild 38 - Dialog „Datenbankquellenkonfiguration“ SQL Server

3. Wählen Sie MS SQL Server als Datenbanktyp aus der angebotenen Liste unterstützter Datenbanken.
4. Geben Sie den Namen bzw. die IP-Adresse für Ihr MSDE/MS SQL-Server Datenbank-Backend an.
5. Wenn Sie die Authentifizierungsdaten des SQL-Server-Kontos verwenden wollen, klicken Sie auf die Option „SQL-Server-Authentifizierung verwenden“ und geben Benutzernamen und Kennwort in den entsprechenden Feldern ein.

HINWEIS: Standardmäßig unterstützt GFI LANguard ReportPack die Anmeldung über die Windows-Benutzerdaten zur Authentifizierung bei dem SQL-Server.

6. Klicken Sie auf **OK**, um Ihre Konfigurationseinstellungen zu übernehmen.

6.3 Konfigurieren der Datenbankquelle: Microsoft Access

So konfigurieren Sie Microsoft Access als Ihre Datenbankquelle:

1. Klicken Sie auf die Navigationsschaltfläche **Optionen**.
2. Klicken Sie mit der rechten Maustaste auf den Knoten **Datenbankquelle** und wählen Sie **Datenbankquelle festlegen ...** aus. Damit wird der Dialog für die Datenbankquellenkonfiguration angezeigt.

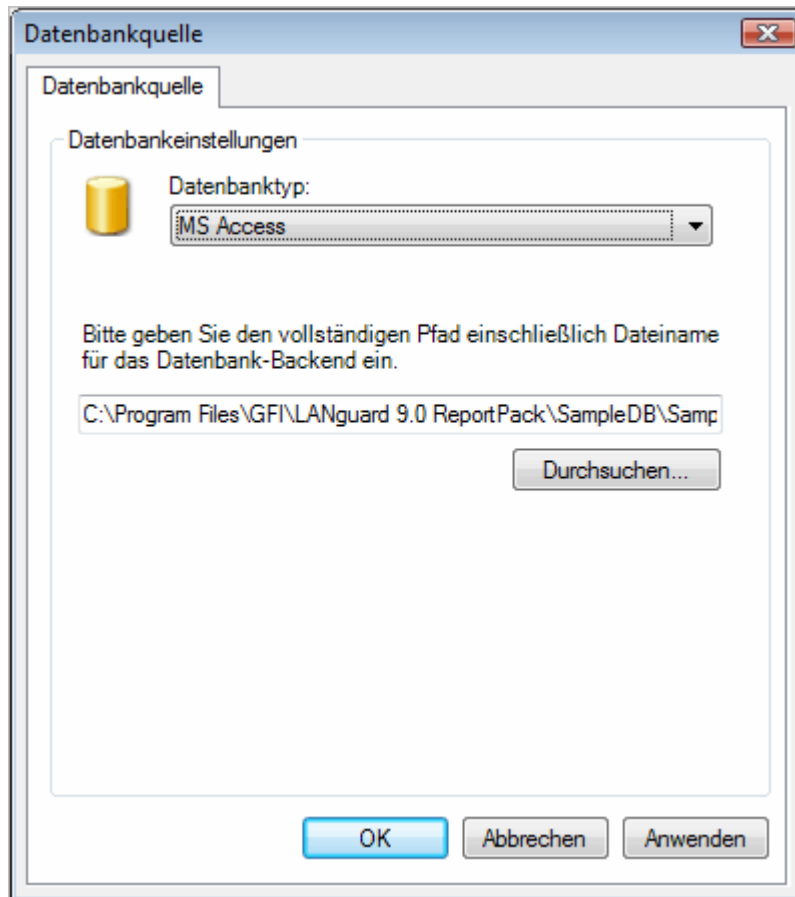


Bild 39 - Dialog „Datenbankquellenkonfiguration“ für MS Access

3. Wählen Sie in der Liste der unterstützten Datenbanken „MS Access“ als Datenbanktyp.

4. Geben Sie den kompletten Pfad zum Datenbank-Backend an. Wenn die Datenbankquelle nicht lokal gespeichert ist, geben Sie den vollständigen Pfad entsprechend der Universal Naming Convention (UNC) an.

Beispiel: \\Security_Server\Program Files\GFI\LANguard 9\Data\scanresults.mdb).

5. Klicken Sie auf **OK**, um Ihre Konfigurationseinstellungen zu übernehmen.

6.4 Anzeigen der aktuellen Einstellungen für die Datenbankquelle



Bild 40 – Konfigurationseinstellungen der Datenbankquelle

Nach der Konfiguration können Sie die aktuellen Einstellungen der Datenbankquelle durch einen Klick auf den Knoten **Datenbankquelle anzeigen**.

6.5 Konfigurieren der Standardzeitplanereinstellungen

So konfigurieren Sie die Standardeinstellungen für die zeitabhängigen Berichte:

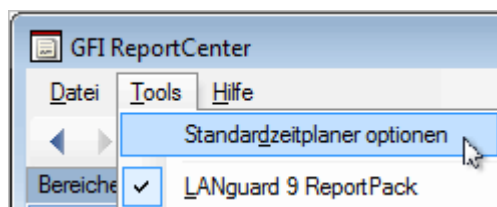


Bild 41 – Knoten „Standardzeitplanereinstellungen“

1. Klicken Sie im Pulldownmenü auf **Tools** ► **Standardzeitplaneroptionen**.
2. Konfigurieren Sie die benötigten Parameter wie im Abschnitt „Konfigurieren erweiterter Einstellungen“ im Kapitel „Zeitabhängige Berichte“ beschrieben.

6.6 Importieren/Exportieren der Konfiguration

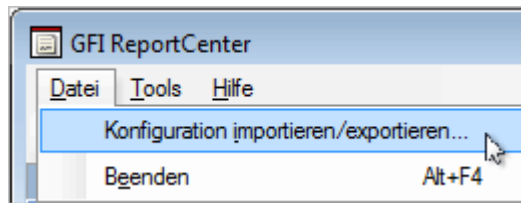


Bild 42 – Knoten „Konfiguration importieren/exportieren“

Im GFI ReportCenter können Sie Ihre Konfigurationseinstellungen für das ReportCenter und alle ReportPacks über die Option **Konfiguration importieren/exportieren ...** im Pulldownmenü **Datei** sichern. Folgende Einstellungen werden exportiert:

- Standardzeitplaneroptionen
- Benutzerdefinierte Berichte
- Zeitabhängige Berichte
- Häufig benötigte Berichte

Die Konfiguration wird in einer XML-Datei gesichert, die in eine separate Instanz von GFI ReportCenter importiert werden kann, sofern die gleichen ReportPacks auf beiden Instanzen installiert sind.

Sie können die Konfiguration auch für ein bestimmtes ReportPack importieren/exportieren, indem Sie den Knoten **Konfiguration importieren/exportieren** unter **Optionen** in ReportPack nutzen.

Exportieren der Konfiguration

So exportieren Sie die Konfiguration von GFI LANguard:

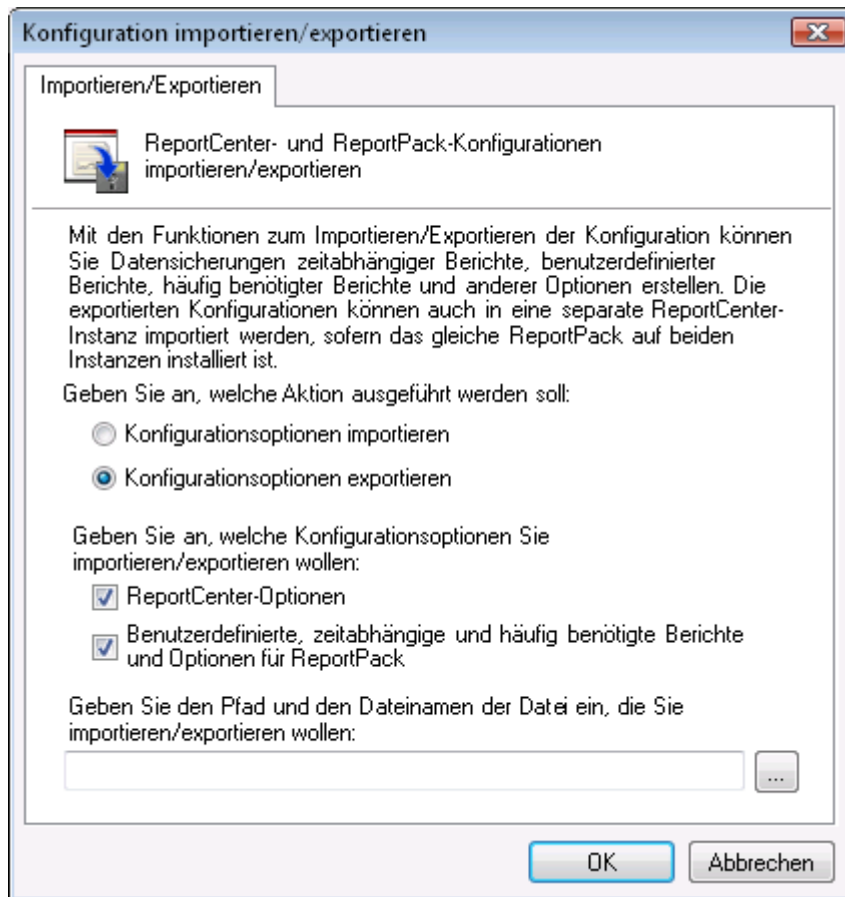


Bild 43 – Dialog „Konfiguration importieren/exportieren“

1. Klicken Sie im Pulldownmenü auf **Datei ► Konfiguration importieren/exportieren ...** . Daraufhin wird der Konfigurationsdialog angezeigt.
2. Klicken Sie auf die Option „**Konfigurationsoptionen exportieren**“.
3. Geben Sie an, welche Konfigurationsoptionen Sie exportieren wollen.
4. Geben Sie Pfad und Dateiname zu der XML-Datei an, in die exportiert werden soll. Klicken Sie auf **OK**, um mit dem Export fortzufahren.

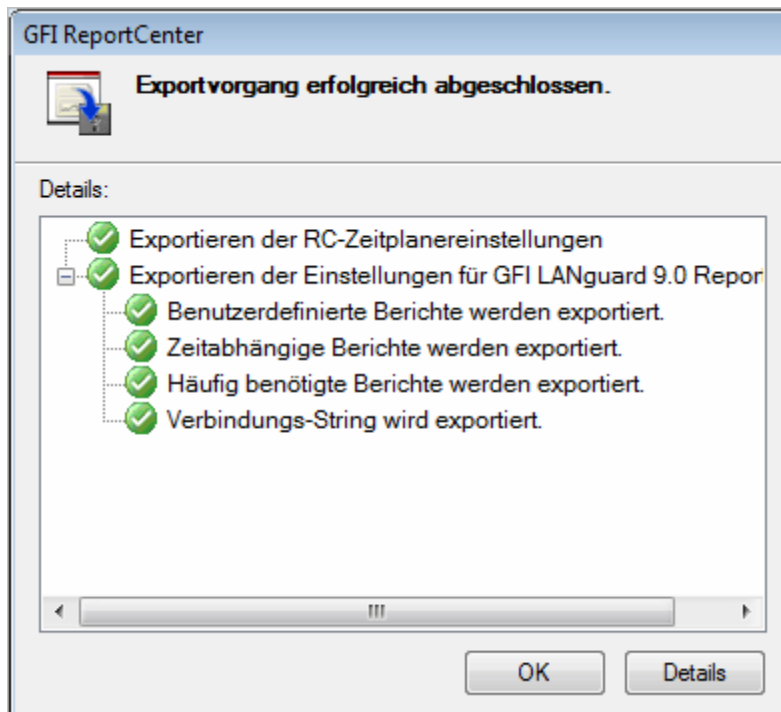


Bild 44 – Export der Konfiguration erfolgreich

Importieren der Konfiguration

So importieren Sie die Konfiguration von GFI LANguard:

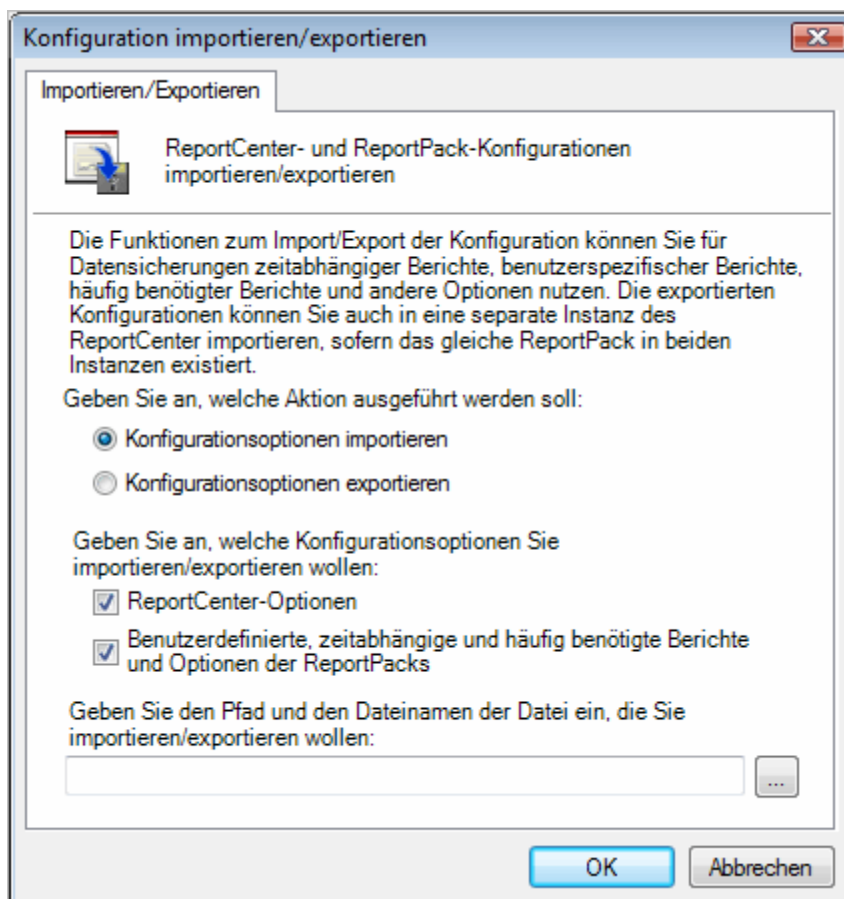


Bild 45 – Dialog „Konfigurationen importieren“

1. Klicken Sie im Pulldownmenü auf **Datei ► Konfiguration importieren/exportieren ...** . Daraufhin wird der Konfigurationsdialog angezeigt.
2. Klicken Sie auf Option **Konfigurationsoptionen importieren**.
3. Geben Sie an, welche Konfigurationsoptionen importiert werden sollen.
4. Geben Sie Pfad und Dateiname der XML-Datei für den Import an. Klicken Sie auf **OK**, um mit dem Import fortzufahren.

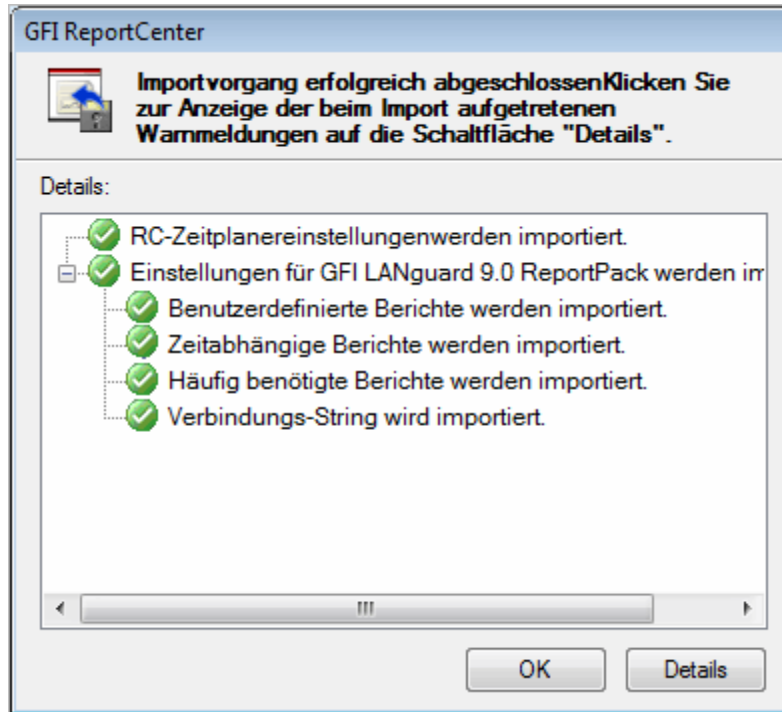


Bild 46 – Import der Konfiguration erfolgreich

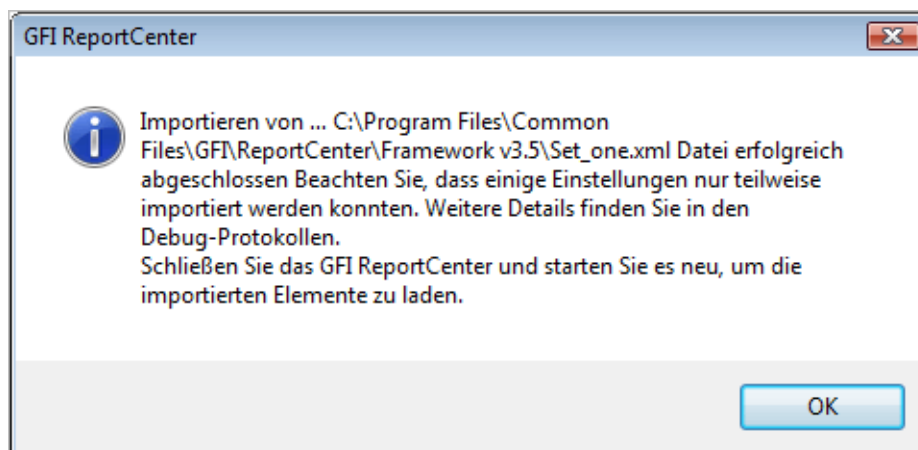


Bild 47 – Konfigurationsimport erfolgreich – Benachrichtigung neu starten

5. Schließen Sie GFI Report Center und starten Sie es neu, um die importierten Elemente zu aktivieren.

7. Allgemeine Optionen

7.1 Anzeigen der Produktversion des ReportPack

So zeigen Sie die Versionsinformationen Ihrer ReportPacks an:

1. Wählen Sie das Produkt für das ReportPack über die Dropdownliste **Produktauswahl**.
2. Klicken Sie auf die Navigationsschaltfläche **Optionen** und dann auf den Knoten **Versionsinformationen**. Die Versionsdetails werden auf der rechten Seite der Verwaltungskonsole angezeigt.

7.2 Suchen nach neuen Builds im Internet

GFI veröffentlicht regelmäßig Produkt- und ReportPack-Updates, die automatisch von der GFI-Website heruntergeladen werden können. So prüfen Sie, ob ein neuerer Build zum Download zur Verfügung steht:

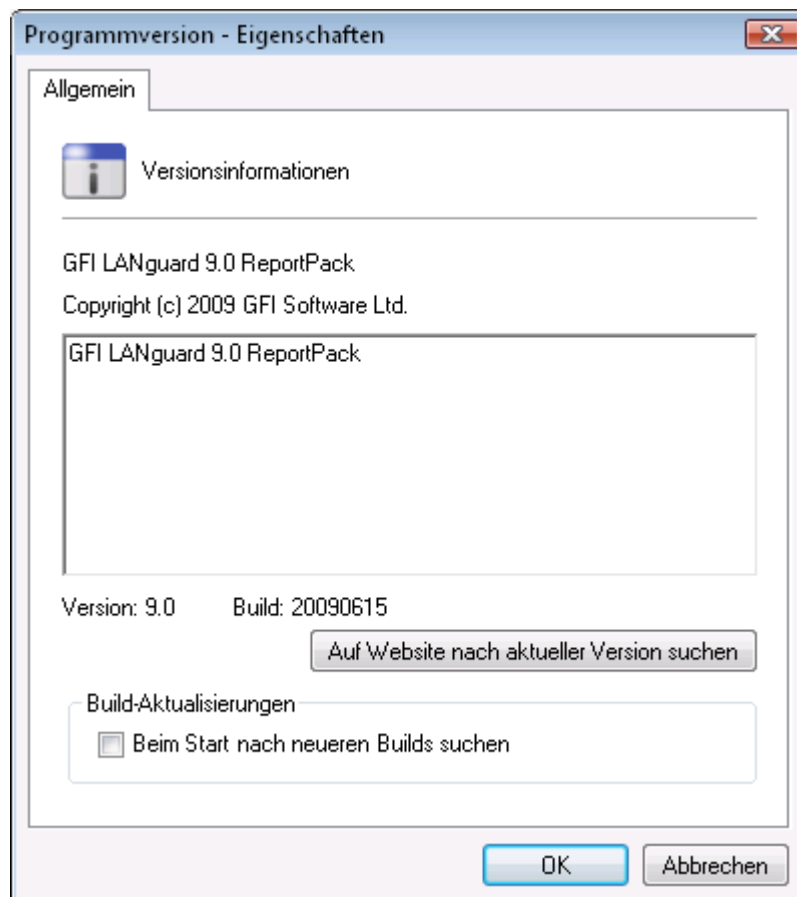


Bild 48 – Versionseigenschaften: Rufen Sie den Dialog für neuere Builds auf.

1. Wählen Sie das betreffende Produkt aus (beispielsweise Berichte für GFI LANguard 9.0) über die Dropdownliste **Produktauswahl**.
2. Klicken Sie auf die Navigationsschaltfläche **Optionen**.
3. Klicken Sie mit der rechten Maustaste auf den Knoten **Versionsinformationen** und dann auf „**Nach neueren Builds suchen ...**“

HINWEIS: GFI LANguard 9.0 ReportPack ist standardmäßig so konfiguriert, dass beim Start nach neuen Builds gesucht wird.

8. Anhang: Standardberichte in GFI LANguard

8.1 Berichte zur Bewertung des Sicherheitsrisikos

8.1.1 Übersicht über Netzwerkrisiken

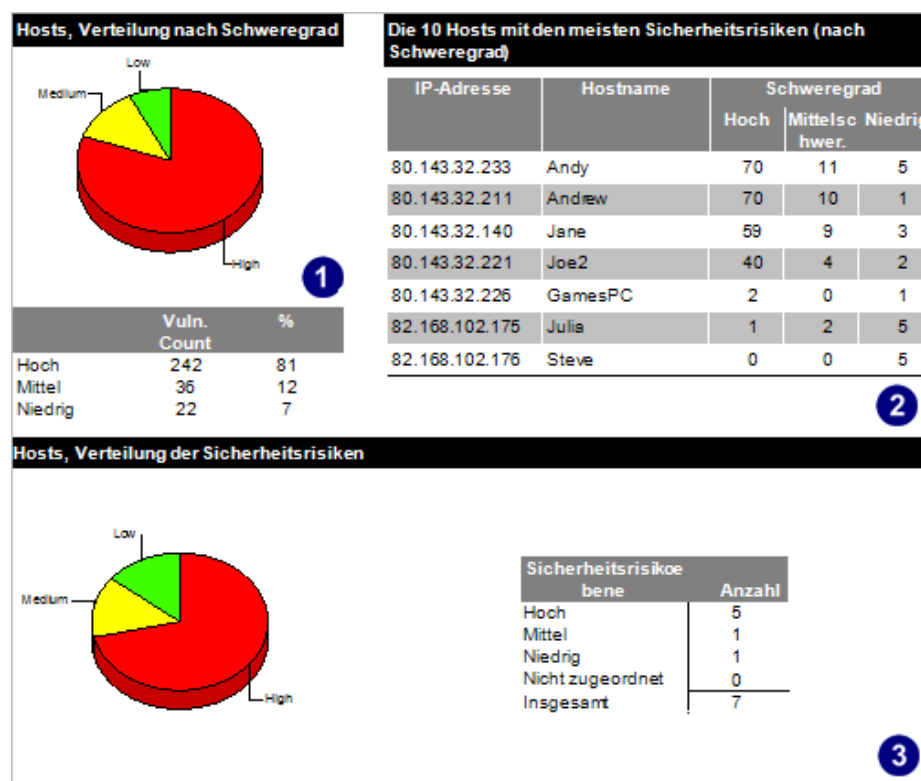


Bild 49 – Beispielbericht mit einer Übersicht über Sicherheitsrisiken im Netzwerk

1	Übersicht mit der Verteilung der Sicherheitsrisiken nach Schweregrad
2	Liste der 10 Rechner mit den meisten Sicherheitsrisiken, geordnet nach Schweregrad.
3	Eine Übersicht mit der Verteilung der Sicherheitsrisiken auf die Host-Computer im Netzwerk

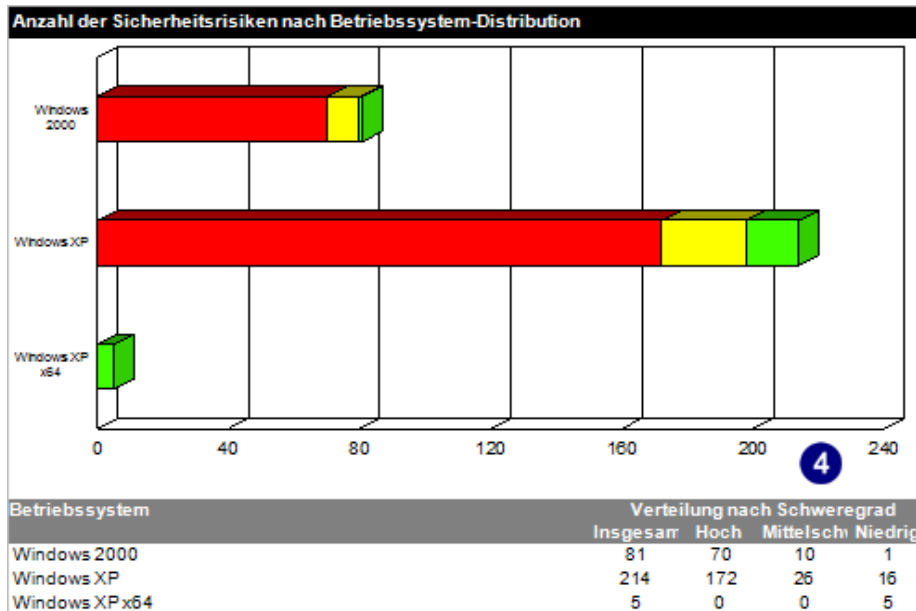


Bild 50 – Beispielbericht mit einer Übersicht über Sicherheitsrisiken im Netzwerk

4 Eine Übersicht mit der Verteilung der Sicherheitsrisiken im Netzwerk nach Betriebssystem

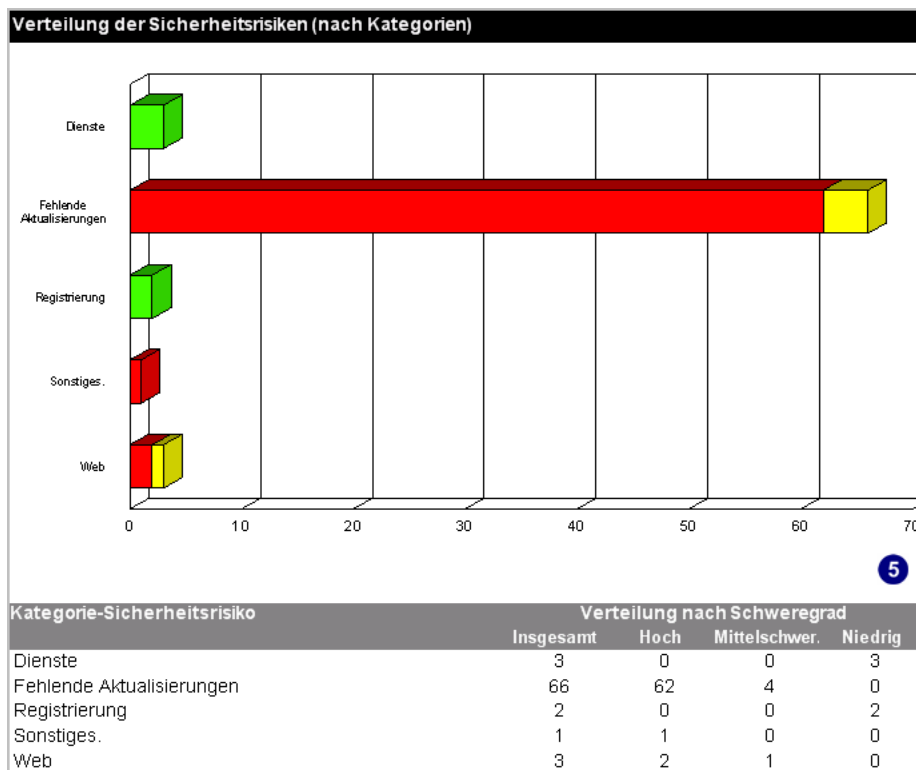


Bild 51 – Beispielbericht mit einer Übersicht über Sicherheitsrisiken im Netzwerk

5 Eine Übersicht mit den Sicherheitsrisikokategorien und deren Verteilung

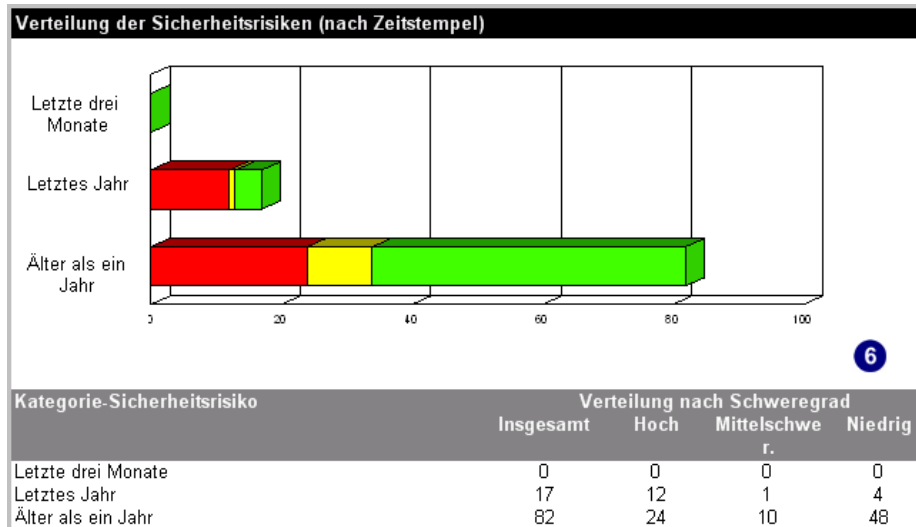


Bild 52 – Beispielbericht mit einer Übersicht über Sicherheitsrisiken im Netzwerk

6 Eine Übersicht mit der Verteilung der Sicherheitsrisiken in der Vergangenheit

Den 10 häufigsten Sicherheitsrisiken

Sicherheitsrisiko	Produkt	Zeitstempel	Verweise	Typ	Schweregrad	Zählerwert
Sicherheitsrisiko : DCOM is enabled	Entfällt	1999-06-07	CVE-1999-0658	Registry	Niedrig	8
Sicherheitsrisiko : AutoShareServer	Entfällt	2002-01-01	Entfällt	Registry	Niedrig	8
Sicherheitsrisiko : A connection could be opened using account Administrator without password !	Entfällt	Entfällt	Entfällt	Services	Hoch	6
Sicherheitsrisiko : Cached Logon Credentials	Microsoft Windows NT	2002-01-01	Entfällt	Registry	Niedrig	5
Sicherheitsrisiko : Auto Logon	Entfällt	2002-01-01	Entfällt	Registry	Hoch	4
Sicherheitsrisiko : LM Hash	Entfällt	2002-01-01	Entfällt	Registry	Mittel	4
Sicherheitsrisiko : OVAL:1538: Win2K/XP_SP1 DDS Library Shape Control Buffer Overflow	Microsoft Internet Explorer 5.01	2005-10-12	CVE-2005-2127	Web	Hoch	4
Sicherheitsrisiko : FTP anonymous access allowed	Entfällt	Entfällt	Entfällt	FTP	Niedrig	4

Die 10 Produkte mit den meisten Sicherheitsrisiken

Produkt	Verteilung nach Schweregrad			
	Insgesamt	Hoch	Mittelschwer	Niedrig
Windows	262	225	32	5
Microsoft Windows NT	1	0	0	1

Bild 53 – Beispielbericht mit einer Übersicht über Sicherheitsrisiken im Netzwerk

7 Eine Übersicht mit den 10 häufigsten Sicherheitsrisiken

8 Eine Übersicht der 10 Produkte mit den meisten Sicherheitsrisiken

Mit diesem Bericht können Sie:

- die Anzahl der Sicherheitsrisiken für verschiedene Kategorien anzeigen;
- die 10 Hostcomputer mit den meisten Sicherheitsrisiken identifizieren;
- die 10 Produkte mit den meisten Sicherheitsrisiken identifizieren;
- die 10 häufigsten Sicherheitsrisiken identifizieren.

8.1.2 Trends der Netzwerksicherheitsrisiken

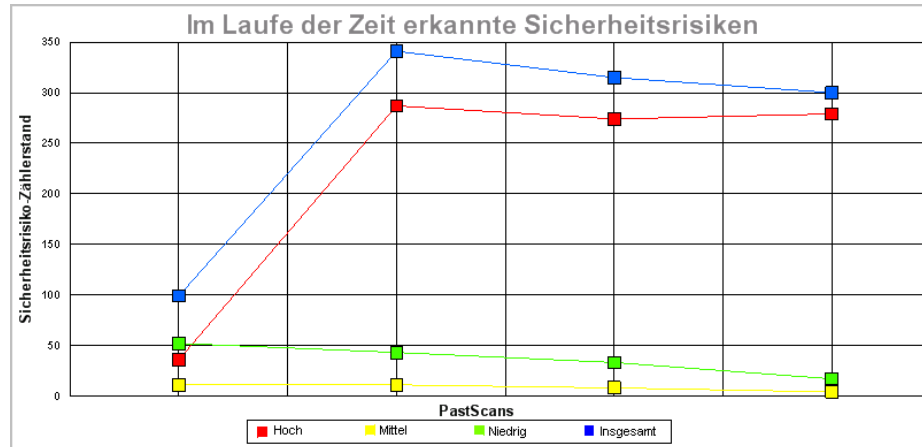


Bild 54 Beispielbericht mit Trends der Sicherheitsrisiken im Netzwerk

1	Eine Übersicht der Scanergebnisse der Vergangenheit und der Gesamtzahl der Sicherheitsrisiken pro Scanvorgang
2	Liste der Scans aus der Vergangenheit und der entsprechenden Scanprofile

Mit diesem Bericht können Sie:

- grafisch die Zahl der Sicherheitsrisiken im Netzwerk im Laufe eines bestimmten Zeitraums darstellen.

8.1.3 Verteilung der Sicherheitsrisiken nach Host

Scan-Referenz : 80.143.32.1/24
 Scan-Datum und Scan-Zeit : 5/21/2009 3:42:44PM

Betriebssystem/ ServicePack	Insgesamt	Verteilung nach			Kategorien von Sicherheitsrisiken															
		Niedrig	Mittelschwer	Hoch	E-Mail	FTP	Web	Reg.	Serv.	RPC	DNS	Soft.	Rtkit.	Sonst. ges.	Bkdr.	S. Prod.	Nicht genen.	USB Netzwerkk.	Fehl. Updk.	
80.143.32.140 Jane	71	3	9	59	0	0	0	1	1	0	0	0	0	0	4	0	0	2	3	60
80.143.32.211 Andrew	81	1	10	70	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	78
80.143.32.221 Joe2	46	2	4	40	0	0	0	3	1	0	0	0	0	0	1	0	0	0	0	41
80.143.32.226 GamesPC	3	1	0	2	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	1
80.143.32.233 Andy	86	5	11	70	0	0	0	3	1	1	0	0	0	0	0	0	0	0	0	81
82.168.102.175 Julia	8	5	2	1	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0	1
82.168.102.176 Steve	5	5	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0
Insgesamt	300	22	36	242	0	0	0	24	3	1	0	0	0	0	5	0	0	2	3	262

Bild 55 – Musterbericht mit der Verteilung der Sicherheitsrisiken nach Host

1	Liste der IP-Adressen und Hostnamen der Rechner, auf denen Sicherheitsrisiken erkannt wurden.
2	Die Anzahl der für jeden Host-Computer erkannten niedrigen, mittleren und hohen Sicherheitsrisiken

3 Die Anzahl der Sicherheitsrisiken, die auf jedem Host-Computer erkannt wurden, sortiert nach Sicherheitsrisikokategorie

Mit diesem Bericht können Sie:

- allgemeine statistische Daten zur Anzahl der Sicherheitsrisiken für jeden Hostcomputer erzeugen.

8.1.4 Verteilung der Sicherheitsrisiken nach Betriebssystem

Scan-Referenz : 80.143.32.1/24
Scan-Datum und Scan-Zeit :5/21/2009 3:42:44PM

Betriebssystem/ ServicePack	Verteilung nach Schwere				Kategorien von Sicherheitsrisiken																
	Insgesamt	Niedrig	Mittlere	Hoch	E-Mail	FTP	Web	Reg.	Serv.	RPC	DNS	Soft.	Rtzt.	Sonstige	Extr.	S. Prod.	Nicht genehm.	USB	Netzwerk	Fehl. Upd.	
Windows 2000 SP: 4	81	1	10	70	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	78
Windows XP SP: Gold	46	2	4	40	0	0	0	3	1	0	0	0	0	0	1	0	0	0	0	0	41
Windows XP SP: 2	82	9	11	62	0	0	0	10	1	0	0	0	0	4	0	0	2	3	0	0	62
Windows XP SP: 1	86	5	11	70	0	0	0	3	1	1	0	0	0	0	0	0	0	0	0	0	81
Windows XP x64 SP: 1	5	5	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0
Insgesamt	300	22	36	242	0	0	0	24	3	1	0	0	0	0	5	0	0	2	3	0	262

1: Liste der Betriebssysteme und Service Packs, für die mindestens ein Sicherheitsrisiko besteht.
2: Die Anzahl der niedrigen, mittleren und hohen Sicherheitsrisiken, die für jedes Betriebssystem erkannt wurde.
3: Die Anzahl der für jedes Betriebssystem erkannten Sicherheitsrisiken, sortiert nach Sicherheitsrisikokategorie.

Bild 56 – Musterbericht mit der Verteilung der Sicherheitsrisiken nach Betriebssystem

1	Liste der Betriebssysteme und Service Packs, für die mindestens ein Sicherheitsrisiko besteht.
2	Die Anzahl der niedrigen, mittleren und hohen Sicherheitsrisiken, die für jedes Betriebssystem erkannt wurde.
3	Die Anzahl der für jedes Betriebssystem erkannten Sicherheitsrisiken, sortiert nach Sicherheitsrisikokategorie.

Mit diesem Bericht können Sie:

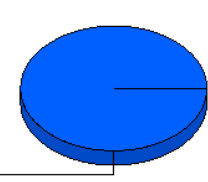
- allgemeine statistische Angaben zur Anzahl der Sicherheitsrisiken pro Betriebssystem darstellen.

8.1.5 Bisherige Sicherheitsscans

Die am häufigsten gescannten Systeme			Die am seltensten gescannten Systeme		
IP-Adresse	Hostname	Zählerwert	IP-Adresse	Hostname	Zählerwert
82.168.102.176	Steve	1	82.168.102.176	Steve	1
82.168.102.175	Julia	1	82.168.102.175	Julia	1
80.143.32.233	Andy	1	80.143.32.233	Andy	1
80.143.32.226	GamesPC	1	80.143.32.226	GamesPC	1
80.143.32.221	Joe2	1	80.143.32.221	Joe2	1
80.143.32.211	Andrew	1	80.143.32.211	Andrew	1
80.143.32.140	Jane	1	80.143.32.140	Jane	1

1: Die am häufigsten gescannten Systeme
2: Die am seltensten gescannten Systeme

Am häufigsten verwendete Profile	
Profil	Zählerwert
Vollständiger Scan	1



3: Am häufigsten verwendete Profile

Bild 57 – Musterbericht mit der History der Sicherheitsscans mit allen ausgeführten Scans

1	Liste der Host-Computer mit den meisten Scans und den entsprechenden Scanzahlen
2	Liste der Host-Computer mit den wenigsten Scans und den entsprechenden Scanzahlen
3	Eine Übersicht mit der Scanprofilnutzung

Letzter Scan für jedes System		
IP-adresse	Hostname	Letztes Scan-Datum
82.168.102.176	Steve	5/21/2009 3:42:44PM
82.168.102.175	Julia	5/21/2009 3:42:44PM
80.143.32.233	Andy	5/21/2009 3:42:44PM
80.143.32.226	GamesPC	5/21/2009 3:42:44PM
80.143.32.221	Joe2	5/21/2009 3:42:44PM
80.143.32.211	Andrew	5/21/2009 3:42:44PM
80.143.32.140	Jane	5/21/2009 3:42:44PM

4

Scan Listing			
Beginndatum/Uhrzeit	Ziel	Profil	Scan beendet
5/21/2009 3:42:44PM	80.143.32.1/24	Vollständiger Scan	Ja

5

Bild 58 – Musterbericht mit der History der Sicherheitsscans und allen ausgeführten Scans

4	Liste mit Datum und Uhrzeit des letzten auf dem jeweiligen Host-Computer ausgeführten Scans
5	Liste mit Anzeige aller ausgeführten Scans

Mit diesem Bericht können Sie:

- Informationen und Statistiken zu allen zur Netzwerksicherheit durchgeführten Scans anzeigen.

8.1.6 Liste der Sicherheitsrisiken nach Kategorie

KATEGORIE: Fehlende Aktualisierungen

Sicherheitsrisiko : **814078: Security Update (Microsoft Jscript version 5.6, Windows 2000, Windows XP)**

Produkt : Windows

Zeitstempel : 2003-11-21

Betroffene Hosts:	IP-Adresse	Hostname	Betriebssystem	SP
	80.143.32.221	Joe2	Windows XP	Gold

1

Sicherheitsrisiko : **816093: Security Update Microsoft Virtual Machine (Microsoft VM)**

Produkt : Windows

Schweregrad : Kritisch

Zeitstempel : 2004-06-08

Betroffene Hosts:	IP-Adresse	Hostname	Betriebssystem	SP
	80.143.32.211	Andrew	Windows 2000	4

2

Sicherheitsrisiko : **817787: Security Update Windows Media Player for XP**

Produkt : Windows

Zeitstempel : 2004-01-12

Betroffene Hosts:	IP-Adresse	Hostname	Betriebssystem	SP
	80.143.32.233	Andy	Windows XP	1

Bild 59 – Musterbericht mit der Liste der Sicherheitsrisiken nach Kategorie

1	Details zu den Sicherheitsrisiken mit Name, Beschreibung und Schweregrad
----------	--

2	Liste der Host-Computer, die durch jedes erkannte Sicherheitsrisiko betroffen sind.
----------	---

Mit diesem Bericht können Sie:

- erkannte Sicherheitsrisiken, sortiert nach Kategorie, und den Host-Computer mit dem jeweiligen Sicherheitsrisiko auflisten.

8.1.7 Liste der Sicherheitsrisiken nach Host

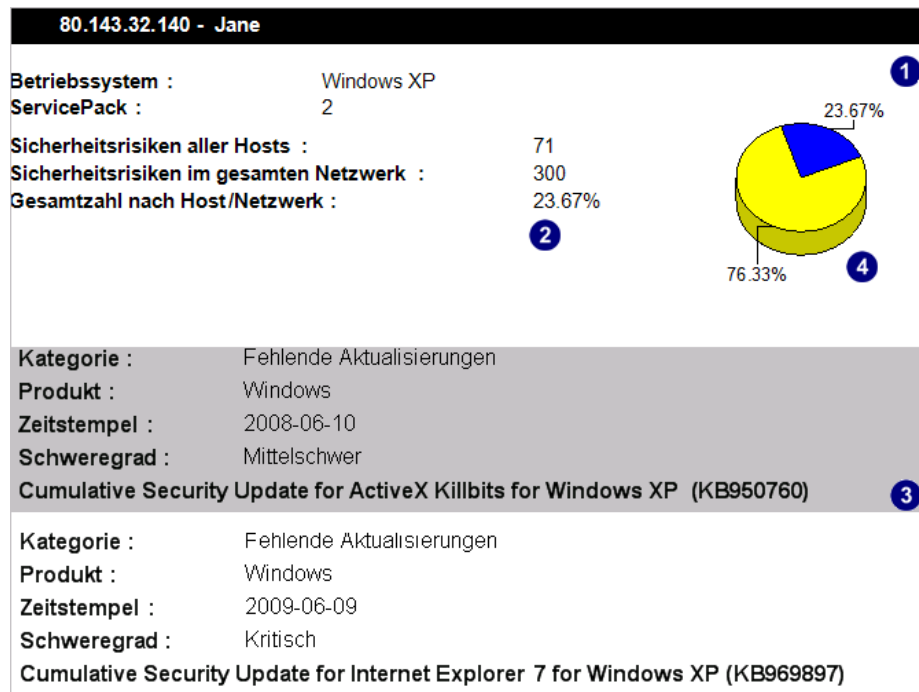


Bild 60 – Musterbericht mit einer Liste der Sicherheitsrisiken nach Host

1	Details des Host-Computers, auf dem Sicherheitsrisiken erkannt wurden.
2	Anzahl der Sicherheitsrisiken pro Host-Computer in Prozent der Gesamtzahl der Sicherheitsrisiken, die im Netzwerk erkannt wurden.
3	Liste der Details zu Sicherheitsrisiken auf jedem Host-Computer mit Namen, Beschreibung und Schweregrad
4	Eine Übersicht mit dem prozentualen Anteil der Sicherheitsrisiken, die auf jedem Host-Computer erkannt wurden, und Vergleich mit der Gesamtzahl der Sicherheitsrisiken, die im Netzwerk erkannt wurden.

Mit diesem Bericht können Sie:

- die Sicherheitsrisiken auflisten, die auf jedem Host-Computer im Netzwerk erkannt wurden.

8.1.8 Liste der Sicherheitsrisiken nach Produkt

PRODUKT : Entfällt			
Sicherheitsrisiko :	A connection could be opened using account Administrator without password! - You MUST set a password for the administrator account and/or disable guest logons .		
Kategorie :	Services		
Schweregrad :	Hoch		
Zeitstempel :	Entfällt		
Betroffene Hosts:	IP-Adresse	Hostname	Betriebssystem
	80.143.32.221	Joe2	Windows XP
	80.143.32.233	Andy	Windows XP
			SP
			Gold
			1
Sicherheitsrisiko :	Auto Logon - Automatic logon uses the domain , user name, and password stored in the registry to log users on to the computer when the system starts. The problem with automatic logon is the fact that any user can start your computer and log on using your account . Automatic logon proceeds differently from authenticated logon , and can cause timing conflicts. For example if one is loading several network transport protocols , automatic logon might cause Windows 2000 to attempt to connect to some network resources before the protocols' network transports are completely		
Kategorie :	Registry		
Schweregrad :	Hoch		
Zeitstempel :	2002-01-01		
Betroffene Hosts:	IP-Adresse	Hostname	Betriebssystem
	80.143.32.226	GamesPC	Windows XP
	82.168.102.175	Julia	Windows XP
			SP
			2
			2

Bild 61 – Musterbericht mit einer Liste der Sicherheitsrisiken nach Produkt

1	Name des Produkts, für das Sicherheitsrisiken erkannt wurden.
2	Sicherheitsrisiko-Details für jedes Produkt mit Name, Beschreibung und Schweregrad
3	Liste der Host-Computer, die durch jedes erkannte Sicherheitsrisiko betroffen sind.

Mit diesem Bericht können Sie:

- die erkannten Sicherheitsrisiken auflisten, sortiert nach Produkt, und die Hostcomputer, die von jedem Sicherheitsrisiko betroffen sind.

8.1.9 Liste der Sicherheitsrisiken nach Schweregrad

SCHWEREGRAD : Hoch			
Sicherheitsrisiko :	Microsoft .NET Framework 3.5 Service Pack 1 and .NET Framework 3.5 Family Update (KB951847) x86		
Kategorie :	Fehlende Aktualisierungen		
Produkt :	Windows		
Zeitstempel :	2009-01-27		
Betroffene Hosts:	IP-Adresse	Hostname	Betriebssystem
	80.143.32.221	Joe2	Windows XP
			SP
			Gold
Sicherheitsrisiko :	Microsoft .NET Framework 1.1 Service Pack 1		
Kategorie :	Fehlende Aktualisierungen		
Produkt :	Windows		
Zeitstempel :	2008-04-22		
Betroffene Hosts:	IP-Adresse	Hostname	Betriebssystem
	80.143.32.211	Andrew	Windows 2000
	80.143.32.233	Andy	Windows XP
			SP
			4
			1

Bild 62 – Musterbericht mit einer Liste der Sicherheitsrisiken nach Schweregrad

1	Schweregrad
2	Sicherheitsrisikodetails für jeden Schweregrad mit Name und Beschreibung

3	Liste der Host-Computer, die durch die für jede Sicherheitsstufe erkannten Sicherheitsrisiken betroffen sind.
----------	---

Mit diesem Bericht können Sie:

- die erkannten Sicherheitsrisiken auflisten, sortiert nach Schweregrad, und die von jedem Sicherheitsrisiko betroffenen Host-Computer.

8.1.10 Offene Trojaner-Ports nach Host

80.143.32.140 - Jane	
Betriebssystem :	Windows XP
ServicePack :	2
Anzahl der offenen Ports :	4 1
Offene Ports	
Err0r32	
Eclipse 2000, Sanctuary	
Exploiter, FreddyK, Kid Terror, Schwindler, Sensitive, Winsp00fer	
Ducktoy 2	

Bild 63 – Musterbericht mit Anzeige der offenen Trojaner-Ports nach Host

1	Details der Host-Computer mit offenen Ports, die von Trojanern verwendet werden könnten.
2	Liste der offenen Ports für jeden Host-Computer und die Namen der Trojaner, die den jeweiligen Port nutzen könnten.

Mit diesem Bericht können Sie:

- offene Ports auflisten, sortiert nach Host-Computer, die als Backdoor für Trojaner genutzt werden könnten.

8.1.11 Offene Trojaner-Ports

Die 20 am häufigsten verwendeten Backdoors	
Port-Beschreibung	Anzahl der offenen Ports
Exploiter, FreddyK, Kid Terror, Schwindler, Sensitive, Winsp00fer	2
Ducktoy	1
Eclipse 2000, Sanctuary	1
Err0r32	1 1

Bild 64 Musterbericht mit Anzeige der offenen Trojaner-Ports

1	Liste mit den am häufigsten von Trojanern verwendeten offenen Ports, die im Netzwerk erkannt wurden.
----------	--

Mit diesem Bericht können Sie:

- die 20 am häufigsten verwendeten offenen Ports im Netzwerk auflisten, die von Trojanern als Backdoor genutzt werden könnten.

8.1.12 Status der wichtigsten SANS-Sicherheitsrisiken

82.168.102.175 - Julia	
Betriebssystem Windows XP	ServicePack 2 1
SANS-Bericht, ja : 2006	
SANS-Bericht, Kapitel : W1	
Sicherheitsrisiken	
Name :	Auto Logon
Produkt :	Entfällt
Beschreibung :	Automatic logon uses the domain , user name , and password stored in the registry to log users on to the computer when the system starts . The problem with automatic logon is the fact that any user can start your computer and log on using your account . Automatic logon proceeds differently from authenticated logon , and can cause timing conflicts. For example if one is loading several network transport protocols , automatic logon might cause Windows 2000 to attempt to connect to some network resources before the protocols' network transports are completely loaded . In order to solve this vulnerability one should set AutoAdminLogon to 0, and delete the value of DefaultPassword . The latter is stored and displayed in the registry editor in plain , unencrypted text. 2

Bild 65 – Musterbericht mit Anzeige der wichtigsten SANS-Sicherheitsrisiken und deren Status

1	Details der Host-Computer, auf denen die von SANS gemeldeten Sicherheitsrisiken erkannt wurden.
2	Eine Liste mit den Details der SANS-Sicherheitsrisiken, wie Name, Beschreibung und betroffenes Produkt. SANS-Sicherheitsrisiken sind nach Jahr und Kapitel sortiert.

Mit diesem Bericht können Sie:

- die für jeden Host-Computer erkannten Sicherheitsrisiken entsprechend dem Bericht der wichtigsten 20 SANS-Sicherheitsrisiken auflisten.

8.1.13 Hosts mit Sicherheitslücken durch offene Ports

Die 20 Hosts mit den meisten Sicherheitsrisiken				
IP-Adresse	Hostname	Betriebssystem	ServicePack	Offene Ports
80.143.32.140	Jane	Windows XP	2	4
80.143.32.221	Joe2	Windows XP	Gold	1 1

Bild 66 – Musterbericht mit Anzeige der durch offene Ports gefährdeten Hosts

1	Eine Liste der wichtigsten 20 Host-Computer, bei denen ein Befall durch Trojaner am wahrscheinlichsten ist.
----------	---

Mit diesem Bericht können Sie:

- die Host-Computer mit den 20 wichtigsten Sicherheitsrisiken aufgrund der Anzahl der offenen Ports auflisten, die von Trojanern genutzt werden könnten.

8.1.14 Hosts mit Sicherheitslücken entsprechend Sicherheitsrisikoebene

Die wichtigsten 20 Hosts nach Sicherheitsrisikoebene												
IP-Adresse / Hostname	Grad	Betriebssystem	ServicePack	Sicherheitsrisiken				Fehlende Patches				
				Insgesamt	Hoch	Mittel	Niedrig	Insgesamt	Kritisch	Wichtig	Mittel	Niedrig
80.143.32.140 Jane	Hoch	Windows XP	2	11	10	1	0	60	27	22	8	3
80.143.32.221 Joe2	Hoch	Windows XP	Gold	5	2	1	2	41	31	7	3	0
80.143.32.233 Andy	Hoch	Windows XP	1	5	2	0	3	81	38	30	11	2
80.143.32.211 Andrew	Hoch	Windows 2000	4	3	1	1	1	78	35	34	9	0
80.143.32.226 GamesPC	Hoch	Windows XP	2	2	1	0	1	1	1	0	0	0
82.168.102.175 Julia	Mittel	Windows XP	2	7	1	1	5	1	0	0	1	0
82.168.102.176 Steve	Niedrig	Windows XPx64	1	5	0	0	5	0	0	0	0	

Bild 67 – Musterbericht mit Anzeige der gefährdeten Hosts, sortiert nach Sicherheitsrisikoebene

Details der Host-Computer mit Anzahl der Sicherheitsrisiken und der fehlenden Patches, die als kritisch eingestuft wurden.

Mit diesem Bericht können Sie:

- die 20 Host-Computer mit den meisten Sicherheitsrisiken für jeden Netzwerk-Sicherheitsscan auflisten, ausgehend von der Sicherheitsrisiko-Ebene.

8.1.15 Status der Netzwerkpatches

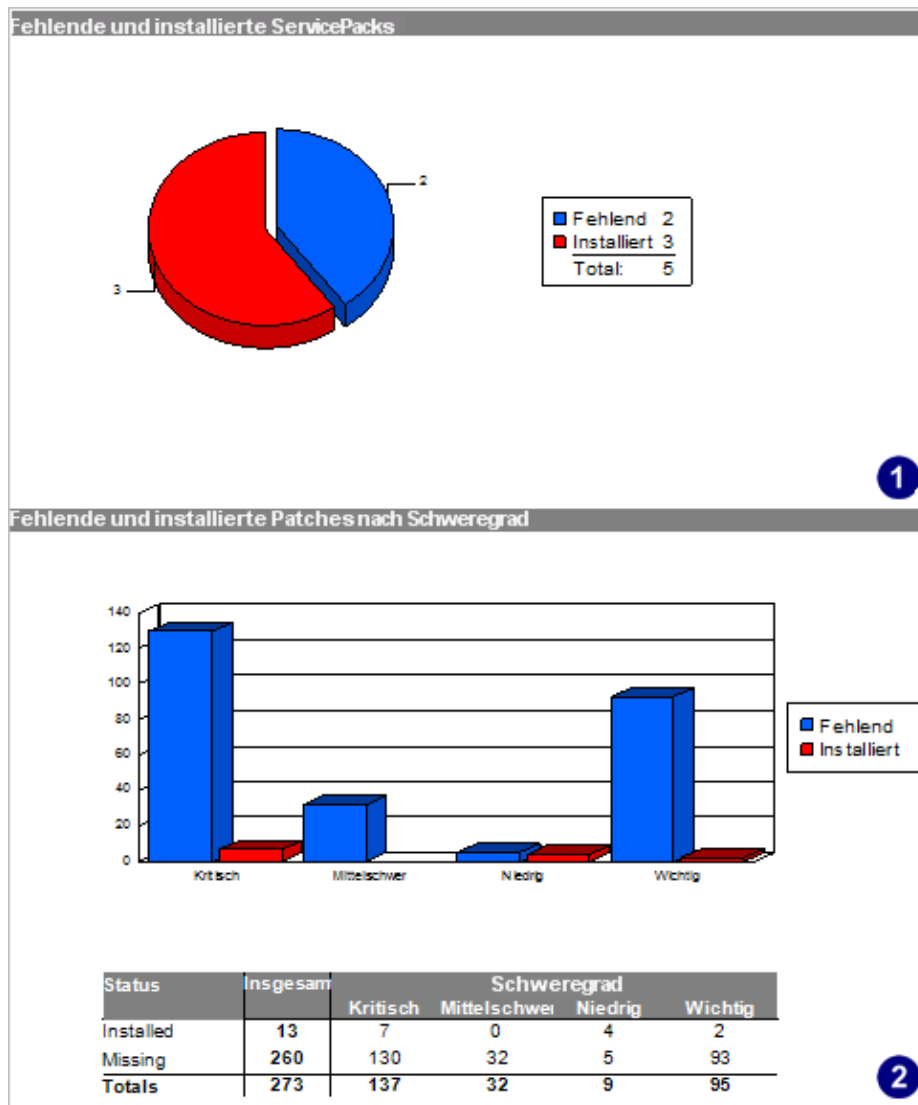


Bild 68 – Musterbericht mit Anzeige des Netzwerkpatchstatus

1	Eine Übersicht mit der Anzahl der installierten und fehlenden Service Packs
2	Eine Übersicht mit der Anzahl der installierten und fehlenden Patches, sortiert nach Schweregrad.

Wichtigste 10 fehlende Sicherheitsaktualisierungen		
Mitteilungs-ID	Beschreibung	Veröffentlichungsdatum
Not Available	Windows Malicious Software Removal Tool - January 2007 (KB890830)	2007-01-09
MS04-003	Security Update for Microsoft Data Access Components (KB832483)	2005-02-17
MS03-034	Security Update for Microsoft Windows (KB824105)	2003-09-09
MS06-006	Security Update for Windows Media Player Plug-in (KB911554)	2006-02-14
MS06-053	Security Update for Windows XP (KB920685)	2006-09-12
MS03-011	816093: Security Update Microsoft Virtual Machine (Microsoft VM)	2004-06-08
MS03-018	Q811114: Security Update (Windows XP or Windows XP Service Pack 1)	2005-03-25
MS03-041	Security Update for Microsoft Windows (KB823182)	2003-10-13
MS03-043	Security Update for Microsoft Windows XP (KB828035)	2003-11-20
MS06-078	Security Update for Windows Media Player 6.4 (KB925398)	2006-12-12

3

Die wichtigsten 20 Hosts mit den meisten Sicherheitsrisiken durch fehlende Patches					
IP-Adresse	Hostname	Schweregrad			
		Kritisch	Wichtig	Mittelschwer	Niedrig
80.143.32.233	Andy	38	30	11	2
80.143.32.211	Andrew	35	34	9	0
80.143.32.221	Joe2	31	7	3	0
80.143.32.140	Jane	27	22	8	3
80.143.32.226	GamesPC	1	0	0	0
82.168.102.175	Julia	0	0	1	0
82.168.102.176	Steve	0	0	0	0

4

Bild 69 – Musterbericht mit Anzeige des Netzwerkpatchstatus

3	Liste mit den zehn wichtigsten fehlenden Sicherheitsupdates
4	Liste der 20 Host-Computer mit den meisten Sicherheitsrisiken durch fehlende Patches und Service Packs; die Anzahl der erkannten Sicherheitsrisiken wird nach Schweregrad unterteilt.

Mit diesem Bericht können Sie:

- den Patch-Status und den Status der Service Packs für Host-Computer im Netzwerk auflisten.

8.1.16 Fehlende Patches nach Host

80.143.32.140 - Jane				
Betriebssystem	ServicePack	Patch-Nummer		
Windows XP	2	60	1	
Mitteilungs-ID	Beschreibung	Veröffentlichungsdatum	Schweregrad	
MS06-778	Windows Malicious Software Removal Tool - January 2007 (KB890830)	2007-01-09	Kritisch	
MS07-004	Security Update for Windows XP (KB929969)	2007-01-09	Kritisch	
MS06-065	Windows Internet Explorer 7.0 for Windows XP	2007-01-02	Kritisch	
MS06-078	Security Update for Windows XP (KB923689)	2006-12-12	Kritisch	
MS06-007	Security Update for Windows Media Player 6.4 (KB925398)	2006-12-12	Kritisch	
MS06-076	Cumulative Security Update for Outlook Express for Windows XP (KB923694)	2006-12-12	Wichtig	
MS06-075	Security Update for Windows XP (KB926255)	2006-12-12	Wichtig	
MS06-066	Security Update for Windows XP (KB923980)	2006-12-12	Wichtig	
MS06-072	Cumulative Security Update for Internet Explorer for Windows XP (KB925454)	2006-12-12	Kritisch	

2

Bild 70 – Musterbericht mit Anzeige der fehlenden Patches, sortiert nach Host

1	Details des Host-Computers, auf dem Sicherheitsrisiken erkannt wurden.
2	Eine detaillierte Liste der fehlenden Patches für jeden Host-Computer, mit Angabe des Schweregrads und der URL mit weiteren Informationen.

Mit diesem Bericht können Sie:

- die fehlenden Patches auflisten, sortiert nach Host-Computer, sowie die URL-Links, die weitere Informationen zu jedem fehlenden Patch enthalten.

8.1.17 Fehlende Patches nach Betriebssystem

Windows 2000		
Patch : 929969	Mitteilungs-ID :	MS07-004
Veröffentlichungsdatum : 2007-01-09	Schweregrad :	Kritisch
Beschreibung : Security Update for Internet Explorer 5.01 Service Pack 4 (KB929969) 1		
Host IP-Adresse	Hostname	ServicePack
80.143.32.211	Andrew	4

Bild 71 – Musterbericht mit Anzeige der fehlenden Patches, sortiert nach Betriebssystem

1	Details fehlender Patches für jedes Betriebssystem
2	Eine Liste der Host-Computer, auf denen spezifische Patches fehlen.

Mit diesem Bericht können Sie:

- die fehlenden Patches auflisten, sortiert nach Betriebssystem mit den Namen der Host-Computer für jeden fehlenden Patch.

8.1.18 Fehlende Patches nach Schweregrad

Wichtig			
Patch : 970238	Mitteilungs-ID :	MS09-026	
Veröffentlichungsdatum : 2009-06-09			
Beschreibung : Security Update for Windows Server 2008 x64 Edition (KB970238)			1
Host IP-Adresse	Hostname	Betriebssystem	ServicePack
192.168.3.4	TECHCOM01	Windows Server 2008 x64	1

Mittelschwer			
Patch : 969897	Mitteilungs-ID :	MS09-019	
Veröffentlichungsdatum : 2009-06-09			
Beschreibung : Cumulative Security Update for Internet Explorer 7 for Windows Server 2008 x64 Edition (KB969897)			2
Host IP-Adresse	Hostname	Betriebssystem	ServicePack
192.168.3.4	TECHCOM01	Windows Server 2008 x64	1

Bild 72 Musterbericht mit Anzeige der fehlenden Patches, sortiert nach Schweregrad

1	Details fehlender Patches, sortiert nach Schweregrad
2	Eine Liste der Host-Computer, auf denen spezifische Patches fehlen.

Mit diesem Bericht können Sie:

- fehlende Patches auflisten, sortiert nach Schweregrad, und die Namen der Host-Computer, auf denen der jeweilige Patch fehlt.

8.1.19 Installierte Patches nach Host

80.143.32.140 - Jane				
Betriebssystem		ServicePack	Patch-Nummer	
Windows XP		2	2	
1				
Mitteilungs-ID	Beschreibung	Veröffentlichungsdatum	Schweregrad	Nicht installierbar
MS06-009	Security Update for Windows XP (KB901190)	2006-02-14	Wichtig	Nein
MS07-004	MDAC 2.8 Service Pack 1	2006-02-01	Kritisch	Nein
2				

Bild 73 – Musterbericht mit Anzeige der installierten Patches, sortiert nach Host

1	Details des Host-Computers, auf dem Sicherheitsrisiken erkannt wurden.
2	Eine detaillierte Liste der installierten Patches für jeden Host-Computer mit Schweregrad, URL-Link zu weiteren Informationen und dem Hinweis, ob der Patch deinstalliert werden kann.

Mit diesem Bericht können Sie:

- die installierten Patches auflisten, sortiert nach Host-Computer, mit URL-Links, unter denen Sie weitere Informationen zu jedem installierten Patch finden.

8.1.20 Installierte Patches nach Betriebssystem

Windows 2000		
Patch : 911565	Mitteilungs-ID :	MS06-005
Veröffentlichungsdatum : 2006-02-14	Schweregrad : Kritisch	Nicht installierbar : No
Beschreibung : Security Update for Windows Media Player 9 (KB911565)		
1		
Host IP -Adresse	Hostname	ServicePack
80.143.32.211	Andrew	4
Patch : 330994	Mitteilungs-ID :	MS03-014
Veröffentlichungsdatum : 2004-04-09	Schweregrad : Kritisch	Nicht installierbar : No
Beschreibung : 330994 : April 2003, Security Update for Outlook Express 5.5 Service Pack 2		
2		
Host IP -Adresse	Hostname	ServicePack
80.143.32.211	Andrew	4

Bild 74 – Musterbericht mit Anzeige der installierten Patches, sortiert nach Betriebssystem

1	Details des installierten Patches für jedes Betriebssystem
2	Liste der Host-Computer, auf denen spezifische Patches installiert werden sollen.

Mit diesem Bericht können Sie:

- die installierten Patches auflisten, sortiert nach Betriebssystem, mit den Namen der Host-Computer für jeden installierten Patch.

8.1.21 Installierte Patches nach Schweregrad

Kritisch			
Patch : 811113		Mitteilungs-ID : MS06-065	
Veröffentlichungsdatum : 2006-04-25		Nicht installierbar : Nein	
Beschreibung : Windows XP Service Pack 2			
Host IP-adresse	Hostname	Betriebssystem	ServicePack
80.143.32.140	Jane	Windows XP	2
Patch : 911565		Mitteilungs-ID : MS06-005	
Veröffentlichungsdatum : 2006-02-14		Nicht installierbar : Nein	
Beschreibung : Security Update for Windows Media Player 9 (KB911565)			
Host IP-adresse	Hostname	Betriebssystem	ServicePack
80.143.32.233	Andy	Windows XP	1

Bild 75 – Musterbericht mit Anzeige der installierten Patches, sortiert nach Schweregrad

1	Liste der installierten Patches, sortiert nach Schweregrad mit Angaben zum jeweiligen Patch.
2	Liste der Host-Computer, auf denen spezifische Patches installiert werden sollen.

Mit diesem Bericht können Sie:

- die installierten Patches auflisten, sortiert nach Schweregrad, und die Namen der Host-Computer für jeden installierten Patch.

8.1.22 Bisherige Autokorrekturen nach Host

Ziel-Host : Jane			
MS-Patch-Installation			
Beginndatum	Enddatum	Status 'Abgeschlossen'	Ist geplant
5/21/2009 3:42:44PM	5/21/2009 3:42:44PM	Erfolgreich	Ja
Installierte Patches			
MS08-062 (953155) - Security Update for Windows 2000 (KB953155)			
MS08-063 (957095) - Security Update for Windows 2000 (KB957095)			
MS08-065 (951071) - Security Update for Windows 2000 (KB951071)			
MS08-067 (958644) - Security Update for Windows 2000 (KB958644)			
Not Available (890830) - Windows Malicious Software Removal Tool - October 2008 (KB890830)			
Not Available (956391) - Cumulative Security Update for ActiveX Killbits for Windows 2000 (KB956391)			

Bild 76 – Musterbericht mit Anzeige der Installations-History, sortiert nach Host

1	Hostcomputer, auf dem Installationen erfolgten
2	Liste der Installationsdetails für jeden Host mit den Namen der installierten Dateien und dem Installationsstatus

Mit diesem Bericht können Sie:

- Patchinstallationsinformationen, sortiert nach Hostcomputer anzeigen, beispielsweise Installationsdetails wie Datum und Status

8.1.23 Bisherige Autokorrekturen nach Datum

Beginndatum : 5/21/2009 3:42:44PM				
1				
MS-Patch-Installation				
Ziel	Enddatum	Status 'Abgeschlossen'	Ist geplant	
Jane	5/21/2009 3:42:44PM	Erfolgreich	Ja	
Installierte Patches				
MS08-062 (953155) - Security Update for Windows 2000 (KB953155)				
MS08-063 (957095) - Security Update for Windows 2000 (KB957095)				
MS08-065 (951071) - Security Update for Windows 2000 (KB951071)				
MS08-067 (958644) - Security Update for Windows 2000 (KB958644)				
Not Available (890830) - Windows Malicious Software Removal Tool - October 2008 (KB890830)				
Not Available (956391) - Cumulative Security Update for ActiveX Killbits for Windows 2000 (KB956391)				
2				

Bild 77 – Musterbericht mit Anzeige der Installationshistory nach Datum

1	Datum des Installationsbeginns
2	Liste der Installationsdetails, sortiert nach Host, mit den Namen der installierten Dateien und dem Installationsstatus

Mit diesem Bericht können Sie:

- Angaben zur Autokorrektur mit Datum und Uhrzeit anzeigen, beispielsweise Details wie die Namen der Host-Computer für jede Installation.

8.1.24 Bisherige Autokorrekturen nach Patch/Anwendung

MS-Patch-Installation				
MS08-062 (953155) - Security Update for Windows 2000 (KB953155)				
Ziel :	Beginndatum	Enddatum	Status 'Abgeschlossen'	Ist geplant
Jane	5/21/2009 3:42:44PM	5/21/2009 3:42:44PM	Erfolgreich	Ja
1				
MS08-063 (957095) - Security Update for Windows 2000 (KB957095)				
Ziel :	Beginndatum	Enddatum	Status 'Abgeschlossen'	Ist geplant
Jane	5/21/2009 3:42:44PM	5/21/2009 3:42:44PM	Erfolgreich	Ja
2				

Bild 78 – Musterbericht mit Anzeige der Installationshistory nach Patch

1	Name des installierten Patches
2	Liste der Hostcomputer, auf denen der Patch installiert wurde, sowie Installationsdetails, beispielsweise Installationsstatus

Mit diesem Bericht können Sie:

- die Informationen zur Patchinstallation anzeigen, sortiert nach Patches, beispielsweise Details wie die Namen der Host-Computer für jede Installation.

8.2 Netzwerk- und Softwareüberprüfung

8.2.1 Softwareüberprüfung

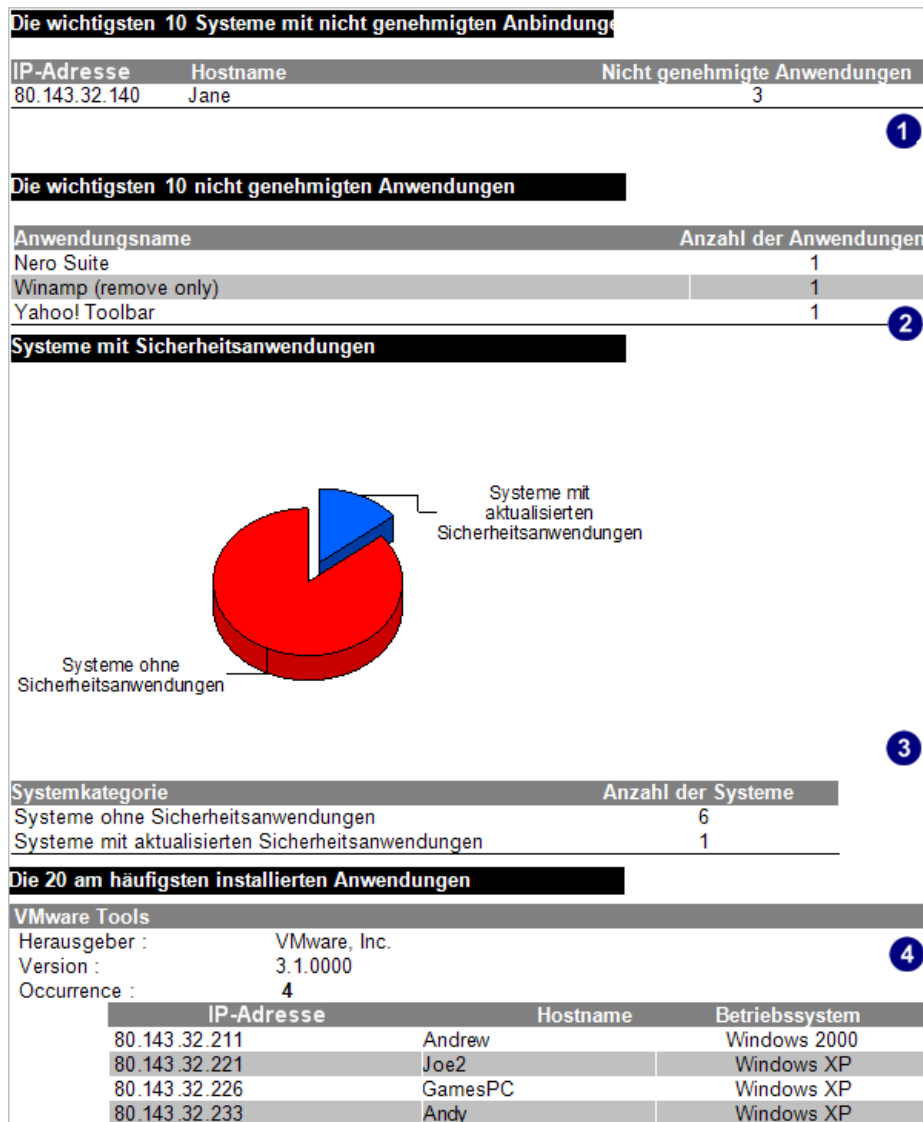


Bild 79 – Musterbericht mit Anzeige der Softwareüberprüfung

1	Liste mit den zehn wichtigsten Host-Computern mit nicht genehmigten Anwendungen
2	Zeigt die 10 wichtigsten nicht genehmigten Anwendungen
3	Übersicht mit Anzeige des Sicherheitsstatus der Anwendungen auf den Hostcomputern
4	Liste mit den 20 wichtigsten installierten Anwendungen

Mit diesem Bericht können Sie:

- nicht genehmigte Anwendungen identifizieren, die auf den Host-Computern installiert sind und bei Netzwerk-Sicherheitsscans erkannt wurden;
- die 10 wichtigsten Computer mit nicht genehmigten Anwendungen identifizieren;

- die 10 wichtigsten nicht genehmigten Anwendungen mit der höchsten Installationszahl identifizieren;
- die 20 wichtigsten installierten Anwendungen identifizieren;
- die Hostcomputer ohne Sicherheitsanwendungen oder mit veralteten Sicherheitsanwendungen grafisch darstellen.

8.2.2 Betriebssystem- und Service Pack-Verteilung

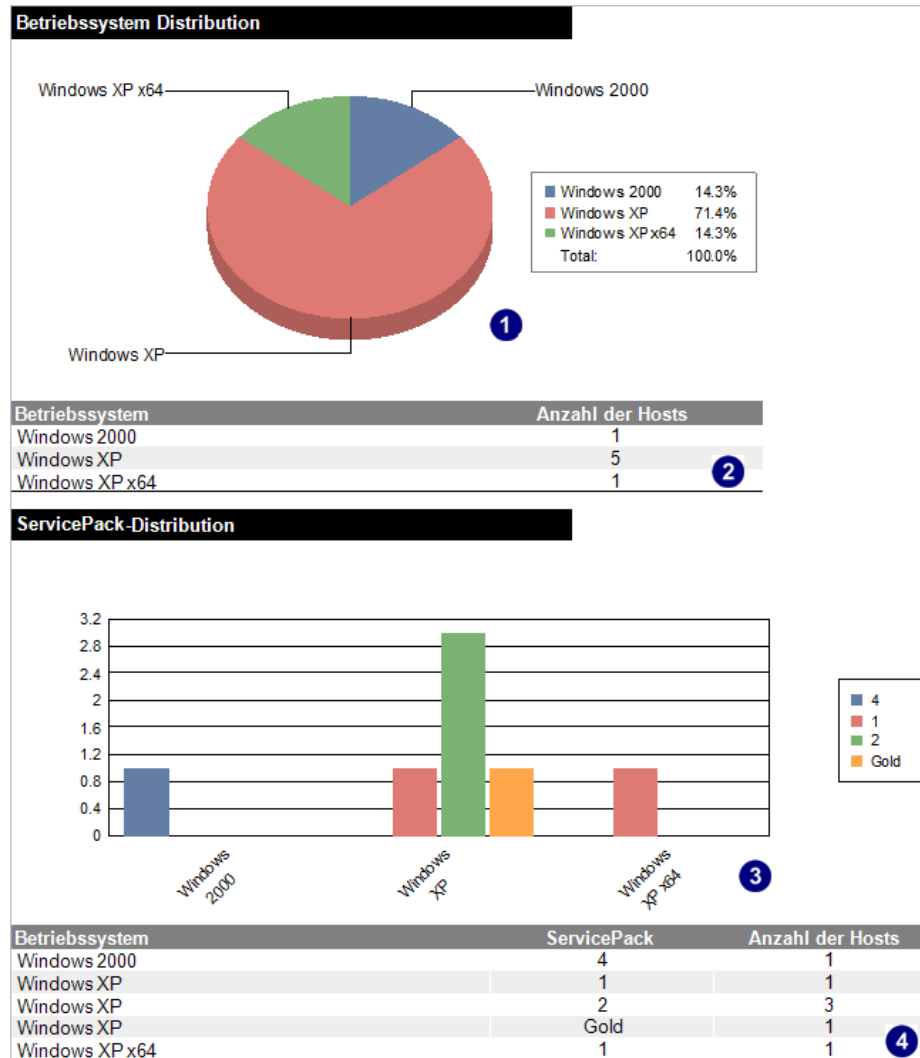


Bild 80 – Musterbericht mit Anzeige des Betriebssystems und der Service Pack-Verteilung

1	Übersicht mit Anzeige der Verteilung der einzelnen Betriebssysteme im Netzwerk
2	Liste der Betriebssysteme mit Anzahl der Hostcomputer, auf denen sie installiert sind.
3	Übersicht mit Anzeige der Service Pack-Verteilung pro Betriebssystem
4	Liste der Service Packs für das Betriebssystem mit Anzahl der Hostcomputer, auf denen sie installiert sind.

Mit diesem Bericht können Sie:

- Im Netzwerk erkannte Betriebssysteme grafisch darstellen;
- Anzahl der Hostcomputer pro Betriebssystem auflisten;

- Im Netzwerk erkannte Service Packs für jedes Betriebssystem grafisch darstellen;
- Die Anzahl der Hostcomputer für jedes installierte Service Pack auflisten.

8.2.3 Systeminformationen

80.143.32.140 - Jane 1

Betriebssystem SP
Windows XP 2

Computereigenschaften 2

80.143.32.140 - [Jane] Windows XP ServicePack 2

MAC-Adresse : 00-0E-2E-56-AF-AE ("Edimax Technology Co., Ltd.")
 Gültigkeitsdauer : 128 (128)
 Netzwerkrolle : Workstation
 Domäne : WORKGROUP
 LAN-Manager : Windows 2000 LAN Manager

Verfügbarkeit 3

Keine Verfügbarkeitsinformationen gefunden.

Festplattennutzung 4

Name	Gesamtspeicherplatz	Freier Speicherplatz	Dateisystem
C:	14.65 GB	5.20 GB	NTFS
D:	23.62 GB	312.30 MB	NTFS

'Gruppen und Benutzer' 5

Name	Beschreibung
Administrators	Administrators have complete and unrestricted access to the computer/domain Members: HX3\Administrator, HX3\LNSS_MONITOR_USR, HX3\Sorin
Backup Operators	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files
Guests	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted

Bild 81 – Musterbericht mit Anzeige der Systeminformationen

1	Host-Computer IP-Adresse und Name
2	Details des Host-Computers, beispielsweise MAC-Adresse und Domäne
3	Verfügbarkeitsdetails zu jedem Host-Computer mit Tageszeit und Betriebszeit
4	Angaben zur Nutzung der Datenträger auf jedem Host-Computer mit Laufwerkname, Dateisystem, Gesamtspeicherplatz und freiem Speicherplatz
5	Gruppen- und Benutzerdetails für jeden Host-Computer mit Gruppenname, Gruppenmitgliedern, Benutzerrechten und Anzahl der Falscheingaben beim Benutzerkennwort

SNMP-Informationen 6			
Keine SNMP-Informationen gefunden.			
Dienste 7			
Alerter			
Beschreibung	Status	Startart	Kontoname
Alerter	Gestartet	Deaktiviert	NT AUTHORITY\LocalService
ALG			
Beschreibung	Status	Startart	Kontoname
Application Layer Gateway Service	Gestartet	Deaktiviert	NT AUTHORITY\LocalService
AppMgmt			
Beschreibung	Status	Startart	Kontoname
Application Management	Gestartet	Deaktiviert	LocalSystem
AudioSrv			
Beschreibung	Status	Startart	Kontoname
Windows Audio	Gestartet	Deaktiviert	LocalSystem
BITS			
Beschreibung	Status	Startart	Kontoname
Background Intelligent Transfer Service	Gestartet	Deaktiviert	LocalSystem
Verarbeitet 8			
alg.exe			
PID : 260			
PPID : 948			
Benutzername : LOCAL SERVICE			
Domäne : NT AUTHORITY			
Handle-Anzahl : 119			
Thread-Anzahl : 8			
Priorität : 8			
csrss.exe			
PID : 880			
PPID : 816			
Benutzername : SYSTEM			
Domäne : NT AUTHORITY			
Handle-Anzahl : 572			
Thread-Anzahl : 10			
Priorität : 13			

Bild 82 – Musterbericht mit Anzeige der Systeminformationen

6	SNMP-Details für jeden Host-Computer mit Name und Beschreibung
7	Dienstdetails für jeden Host-Computer mit Name, Beschreibung, Status, Startart und Kontoname
8	Prozessdetails für jeden Host-Computer mit Prozess-ID und Kontoname

Geräte 9	
Prozessoren	
Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GHz	
Anbieter:	GenuineIntel
Geschwindigkeit:	2405 MHz
Anbieter:	GenuineIntel
Geschwindigkeit:	2405 MHz
Anbieter:	GenuineIntel
Geschwindigkeit:	2405 MHz
Anbieter:	GenuineIntel
Geschwindigkeit:	2405 MHz
Hauptplatinen	
Freigaben 10	
Name	Anmerkung
ADMIN\$	Remote Admin
C\$	Default share
D\$	Default share
e	N/A
E\$	Default share
Offene Ports 11	
TCP-Ports	
139 [Netbios-ssn => NETBIOS Session Service]	
445 [Microsoft-Ds]	
3,389 [Terminal Services]	
135 [epmap => DCE endpoint resolution]	

Bild 83 – Musterbericht mit Anzeige der Systeminformationen

9	Liste mit Anzeige der USB-Geräte, der USB-Geräte der Blacklist, der Netzwerkkarten und der drahtlosen Geräte auf der Blacklist
10	Details des Freigabeordners für jeden Host-Computer mit Name und Anmerkungen
11	Details zu offenen Ports auf jedem Host-Computer mit Port-Nummer und Name

Installierte Anwendungen 12				
Installierte Anwendungen				
Adobe Flash Player 9				
Herausgeber :	Adobe Systems Inc.			
Version :	9			
Authorisiert :	Ja			
AVG AntiVirus				
Herausgeber :	AVG Technologies			
Version :	7.1.428			
Authorisiert :	Ja			
GFI LANguard Network Security Scanner 8.0				
Herausgeber :	GFI			
Version :	8.0			
Authorisiert :	Ja			
Nero Suite				
Authorisiert :	Nein			
VIA Integrated Setup Wizard				
Herausgeber :	VIA Technologies, Inc.			
Version :	0.99			
Authorisiert :	Ja			
VMware Workstation				
Herausgeber :	VMware, Inc.			
Version :	5.5.0.19175			
Authorisiert :	Ja			
Seriennummer :	1123AHG-234789			
Winamp (remove only)				
Authorisiert :	Nein			
Seriennummer :	win198765-098			
Benutzername :	Administrator			
Yahoo! Toolbar				
Authorisiert :	Nein			
Richtlinien 13				
Kennwortrichtlinie				
Mindestkennwortlänge	Maximales Kennwortalter	Minimales Kennwortalter	Abmeldung erzwingen	Kennwortverlauf
0 chars	42 tage, 22 stunden, 47 minuten, 31 sekunden	no delay	never force	no history
Sicherheits-Überwachungsrichtlinie				
Überwachungsrichtlinie			Erfolgreich	Fehler
'Registry-Informationen' 14				
Knotenname	Registry-Eintrag			
	~MHz : 1802			
	CSDVersion : Service Pack 2			
	CurrentBuildNumber : 2600			
	CurrentType : Uniprocessor Free			
	VendorIdentifier : AuthenticAMD			
Run	NeroFilterCheck : C:\WINDOWS\system32\NeroCheck.exe			
Run	Ptiipbmf : rundll32.exe ptiipbmf.dll,SetWriteCacheMode			
Run	PtiuPbmd : Rundll32.exe ptiipbm.dll,SetWriteBack			
Run	SoundMan : SOUNDMAN.EXE			
Run	WinampAgent : C:\Program Files\Winamp\winampa.exe			

Bild 84 – Musterbericht mit Anzeige der Systeminformationen

12	Details zur installierten Anwendung auf jedem Host-Computer mit Name, Anbieter und Version
13	Liste mit Details zur Kennwortrichtlinie und IT-Sicherheit sowie zu den Überwachungsrichtlinien
14	Detaillierte Liste mit den Registry-Einträgen für jeden Host-Computer

Mit diesem Bericht können Sie:

- die technischen Details für jeden Host-Computer mit Diensten, installierten Anwendungen, Richtlinien und Geräten auflisten.

8.2.4 Computereigenschaften

80.143.32.140 - [Jane] Windows XP ServicePack 2	
MAC-Adresse :	00-0E-2E-56-AF-AE ("Edimax Technology Co., Ltd.")
Gültigkeitsdauer :	128 (128)
Netzwerkrolle :	Workstation
Domäne :	WORKGROUP
LAN-Manager :	Windows 2000 LAN Manager

Bild 85 Musterbericht mit Anzeige der Computereigenschaften

1	Host-Computer IP-Adresse und Name
2	Details des Host-Computers, beispielsweise MAC-Adresse und Domäne

Mit diesem Bericht können Sie:

- Informationen über jeden Host-Computer, beispielsweise MAC-Adresse, Netzwerkrolle und Domäne auflisten.

8.2.5 Verfügbarkeit

82.168.102.175 - Julia	
Betriebssystem	ServicePack
Windows XP	2
Tageszeit	Aktive Zeit
07 Feb 2007, 17:37:00	1 Tag, 12 Stunden, 26 Minuten, 8 Sekunden

82.168.102.176 - Steve	
Betriebssystem	ServicePack
Windows XP x64	1
Tageszeit	Aktive Zeit
07 Feb 2007, 17:48:18	8 Stunden, 41 Minuten, 13 Sekunden

Bild 86 – Musterbericht mit Anzeige der Betriebszeiten

1	Host-Computer IP-Adresse und Name
2	Verfügbarkeitsdetails zu jedem Host-Computer mit Tageszeit und Betriebszeit

Mit diesem Bericht können Sie:

- die Betriebszeit pro Hostcomputer, sortiert nach Netzwerkscan, auflisten.

8.2.6 Festplattennutzung

80.143.32.140 - Jane			
Betriebssystem	ServicePack		
Windows XP	2		
Name	Gesamtspeicherplatz	Freier Speicherplatz	Dateisystem
C:	14.65 GB	5.20 GB	NTFS
D:	23.62 GB	312.30 MB	NTFS

Bild 87 – Musterbericht mit Anzeige der Festplattennutzung

1	Host-Computer IP-Adresse und Name
2	Angaben zur Nutzung der Datenträger auf jedem Host-Computer mit Laufwerkname, Dateisystem, Gesamtspeicherplatz und freiem

	Speicherplatz
--	---------------

Mit diesem Bericht können Sie:

- die Datenträgernutzung für jeden Host-Computer auflisten, mit Dateisystem, Gesamtspeicherplatz und freiem Speicher.

8.2.7 Gruppen und Benutzer

80.143.32.140 - Jane		1
Betriebssystem Windows XP	ServicePack 2	
Gruppen		2
Name	Beschreibung	
Administrators Members: HX3\Administrator, HX3\LNSS_MONITOR_USR, HX3\Sorin	Administrators have complete and unrestricted access to the computer/domain	
Backup Operators	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files	
Guests Members: HX3\Guest	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted	
Network Configuration Operators	Members in this group can have some administrative privileges to manage configuration of networking features	
Power Users	Power Users possess most administrative powers with some restrictions. Thus, Power Users can run legacy applications in addition to certified applications	
Remote Desktop Users Members: HX3\Administrator	Members in this group are granted the right to logon remotely	
Replicator	Supports file replication in a domain	
Users Members: NT AUTHORITY\INTERACTIVE, NT AUTHORITY\Authenticated Users	Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run certified applications, but not most legacy applications	
HelpServicesGroup Members: HX3\SUPPORT_388945a0	Group for the Help and Support Center	
Benutzer		3
Administrator()		
Berechtigung :	Administrator (*)	
Flags :	SCRIPT,NORMAL_ACCOUNT	
Kommentar :	Built-in account for administering the computer/domain	
Letzte Anmeldung :	25 Jan 2007, 20:20:13	
Kennwortalter :	34 days, 8 hours, 17 minutes, 10 seconds	
Anzahl der Anmeldungen :	56	
Anzahl der falschen Kennwörter :	1	
Guest()		
Berechtigung :	Guest	
Flags :	ACCOUNT_DISABLED,PASSWORD_NOT_REQUIRED,PASSWORD_CANNOT_BE_CHANGED,NORMAL_ACCOUNT	
Kommentar :	Built-in account for guest access to the computer/domain	
Letzte Anmeldung :	Never	
Kennwortalter :		
HelpAssistant (Remote Desktop Help Assistant Account)		
Vollständiger Name :	Remote Desktop Help Assistant Account	
Berechtigung :	Guest	

Bild 88 – Musterbericht mit Anzeige der Gruppen und Benutzer

1	Host-Computer IP-Adresse und Name
2	Liste der Details zu Sicherheitsrisiken auf jedem Host-Computer mit Namen, Beschreibung und Schweregrad.
3	Liste der Benutzerdetails für jede Benutzergruppe, beispielsweise Benutzername, Benutzerrechte, letzte Anmeldung und Anzahl falscher Kennworteingaben

Mit diesem Bericht können Sie:

- die Gruppen- und Benutzerinformationen für jeden Hostcomputer auflisten.

8.2.8 SNMP-Informationen

80.143.32.211 - Andrew	
Betriebssystem	ServicePack
Windows 2000	4
Name	Beschreibung
Object_ID	1.3.6.1.4.1.311.1.1.3.1.2 (NT Server)
sysDescr	Hardware : x86 Family 15 Model 4 Stepping 8 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 UniprocessorFree)
sysName	MG7
sysUpTime	4 Stunden, 43 Minuten, 18 Sekunden
Vendor	Microsoft

Bild 89 – Musterbericht mit Anzeige der SNMP-Informationen

1	Host-Computer IP-Adresse und Name
2	SNMP-Details für jeden Host-Computer mit Name und Beschreibung

Mit diesem Bericht können Sie:

- die SNMP-Daten für jeden Host-Computer mit Name, Beschreibung und Betriebszeit auflisten.

8.2.9 Dienste

80.143.32.140 - Jane			
Betriebssystem	ServicePack		
Windows XP	2		
Alerter			
Beschreibung	Status	Startart	Kontoname
Alerter	Gestartet	Deaktiviert	NT AUTHORITY\LocalService
ALG			
Beschreibung	Status	Startart	Kontoname
Application Layer Gateway Service	Gestartet	Deaktiviert	NT AUTHORITY\LocalService
AppMgmt			
Beschreibung	Status	Startart	Kontoname
Application Management	Gestartet	Deaktiviert	LocalSystem
wuauerv			
Beschreibung	Status	Startart	Kontoname
Automatic Updates	Gestartet	Deaktiviert	LocalSystem

Bild 90 – Musterbericht mit Anzeige der Dienste

1	Host-Computer IP-Adresse und Name
2	Dienstdetails für jeden Host-Computer mit Name, Beschreibung, Status, Startart und Kontoname

Mit diesem Bericht können Sie:

- Dienstinformationen für jeden Host-Computer mit Beschreibung, Status, Startart und Kontoname anzeigen.

8.2.10 Verarbeitet

80.143.32.140 - Jane	
Betriebssystem Windows XP	ServicePack 2 1
System Idle Process	
Thread-Anzahl : 1	
System	
PID : 4 Benutzername : SYSTEM Domäne : NT AUTHORITY Handle-Anzahl : 540 Thread-Anzahl : 60 Priorität : 8 2	
spoolsv.exe	
PID : 160 PPID : 948 Benutzername : SYSTEM PATH : C:\WINDOWS\system32\spoolsv.exe Domäne : NT AUTHORITY Befehlszeile : C:\WINDOWS\system32\spoolsv.exe Handle-Anzahl : 114 Thread-Anzahl : 11 Priorität : 8	

Bild 91 – Musterbericht mit Anzeige der Prozesse

1	Host-Computer IP-Adresse und Name
2	Prozessdetails für jeden Host-Computer mit Prozess-ID und Kontoname

Mit diesem Bericht können Sie:

- die Prozesseigenschaften für jeden Hostcomputer auflisten.

8.2.11 Hardwareüberprüfung

80.143.32.140 - Jane			
Betriebssystem Windows XP		ServicePack 2	1
Prozessoren			
Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GHz			
Anbieter :	GenuineIntel		
Geschwindigkeit :	2405 MHz		
Anbieter :	GenuineIntel		
Geschwindigkeit :	2405 MHz		
Anbieter :	GenuineIntel		
Geschwindigkeit :	2405 MHz		
Anbieter :	GenuineIntel		
Geschwindigkeit :	2405 MHz		
2			
Hauptplatinen			
Name :	P5K		
Hersteller :	ASUSTeK Computer INC.		
Version :	Rev 1.xx		
Seriennummer :	MS6C7AB34400944		
BIOS-Name :	BIOS Date: 07/03/07 10:01:10 Ver: 08.00.12		
BIOS-Anbieter Name :	American Megatrends Inc.		
BIOS-Version :	0603		
BIOS-Freigabedatum :	2007/07/03 00:00:00		
BIOS-Seriennummer :	System Serial Number		
3			
Speicher			
Physischer Speicher :	4.00 GB		
Freier physischer Speicher :	2.05 GB		
Virtueller Arbeitsspeicher :	8.22 GB		
Freier virtueller Speicher :	5.91 GB		
4			
Grafikkarten			
NVIDIA GeForce 7600 GT			
Hersteller :	NVIDIA		
Aktuelle Auflösung :	1280 x 1024 x 32 x 0 Hz		
Seriennummer :	198281672673624		
5			
Speichergeräte			
Floppy disk drive			
Beschreibung :	Floppy disk drive		
Hersteller :	(Standard floppy disk drives)		
Medientyp :	Floppy disk drive		
ASUS DRW-2014L1T ATA Device			
Beschreibung :	CD-ROM DriveDVD Writer		
Hersteller :	(Standard CD-ROM drives)		
Schnittstellenart :	SCSI		
Medientyp :	Optical disk drive		
Laufwerke :	F:		
Seriennummer :	1119283277-2039		
LV0403T FVZ043D SCSI CdRom Device			
Beschreibung :	CD-ROM DriveDVD-ROM		
6			
Laufwerke			
Name	Gesamtspeicherplatz	Freier Speicherplatz	Dateisystem
C:	14.65GB	5.20GB	NTFS
D:	23.62GB	312.30MB	NTFS
7			

Bild 92 – Musterbericht mit Anzeige der Hardwareüberprüfung – Teil 1 von 2

1	Host-Computer IP-Adresse und Name
2	Prozessorinformationen
3	Hauptplatineninformationen
4	Physischer und virtueller Arbeitsspeicher
5	Grafikkarten
6	Speichergeräte
7	Laufwerkname, Speicherzuordnung und Dateisystem
8	USB-Geräteinformationen
9	USB-Geräte auf der Blacklist
10	Physische und virtuelle Netzwerkgeräte
11	Netzwerkgeräte auf der Blacklist
12	Weitere Geräte

Mit diesem Bericht identifizieren Sie alle im Netzwerk beim Scannen der Computer erkannten Geräte.

HINWEIS: Die Geräte sind nach Kategorien sortiert. Kategorien ohne erkannte Geräte werden nicht angezeigt.

8.2.12 Freigaben

80.143.32.140 - Jane	
Betriebssystem Windows XP	ServicePack 2 1
Name	Anmerkung
ADMIN\$	Remote Admin
C\$	Default share
D\$	Default share
e	Entfällt
E\$	Default share
F\$	Default share
IPC\$	Remote IPC 2

Bild 94 – Musterbericht mit Anzeige der freigegebenen Laufwerke

1	Host-Computer IP-Adresse und Name
2	Details des Freigabeordners für jeden Host-Computer mit Name und Anmerkungen

Mit diesem Bericht können Sie:

- die Informationen über freigegebene Laufwerke für jeden Hostcomputer auflisten.

8.2.13 Offene Ports

80.143.32.140 - Jane	
Betriebssystem Windows XP	ServicePack 2 1
TCP-Ports	
135 [epmap => DCE endpoint resolution]	
139 [Netbios-ssn => NETBIOS Session Service]	
445 [Microsoft-Ds] 2	
3,389 [Terminal Services]	

Bild 95 – Musterbericht mit Anzeige der offenen Ports

1	Host-Computer IP-Adresse und Name
2	Details zu offenen Ports auf jedem Host-Computer mit Port-Nummer und Name

Mit diesem Bericht können Sie:

- die offenen Ports auflisten, die auf jedem Hostcomputer im Netzwerk erkannt wurden, mit Portnummer und Name.

8.2.14 Installierte Anwendungen nach Host

80.143.32.140 - Jane	
Betriebssystem Windows XP	ServicePack 2 1
Installierte Anwendungen	
Adobe Flash Player 9	
Herausgeber :	Adobe Systems Inc.
Version :	9
Authorisiert :	Ja
AVG AntiVirus	
Herausgeber :	AVG Technologies
Version :	7.1.428
Authorisiert :	Ja
GFI LANguard Network Security Scanner 8.0	
Herausgeber :	GFI
Version :	8.0
Authorisiert :	Ja 2

Bild 96 – Musterbericht mit Anzeige der installierten Anwendungen

1	Host-Computer IP-Adresse und Name
2	Details zur installierten Anwendung auf jedem Host-Computer mit Name, Anbieter und Version

Mit diesem Bericht können Sie:

- die erkannten installierten Anwendungen für jeden gescannten Netzwerkhost mit Hersteller und Versionsangaben auflisten.

8.2.15 Anwendungsübersicht

Adobe Flash Player 9 - Installiert auf 1 Computer(n)			
Anwendungs-Herausgeber :		Adobe Systems Inc.	
Versionsnummer :		9	
Autorisiert :		Ja	
1			
IP-Adresse	Hostname	Betriebssystem	SP
80.143.32.140	Jane	Windows XP	2
2			
Adobe Flash Player 9 ActiveX - Installiert auf 1 Computer(n)			
Anwendungs-Herausgeber :		Adobe Systems	
Versionsnummer :		9	
Autorisiert :		Ja	
IP-Adresse	Hostname	Betriebssystem	SP
82.168.102.175	Julia	Windows XP	2

Bild 97 – Musterbericht mit Anzeige des Anwendungsverzeichnisses

1	Name und Details zur installierten Anwendung
2	Liste der Computer mit der installierten Anwendung

Mit diesem Bericht können Sie:

- Alle Computer identifizieren, auf denen eine bestimmte Software installiert ist.

8.2.16 Antivirenanwendungen

80.143.32.140 - Jane					
Betriebssystem		ServicePack			
Windows XP		2			
1					
Name/Herausgeber	Version	Definitionsd teilen aktuell	Letztes	Automatischer	
AVGAntiVirus	7.1.428	Ja	5/22/2009 5:31:02AM	Nicht unterstützt	
AVG Technologies					
2					

Bild 98 – Musterbericht mit Anzeige der installierten Antivirus-Anwendungen

1	Host-Computer IP-Adresse und Name
2	Details zur installierten Anwendung auf jedem Host-Computer mit Name, Anbieter und Version

Mit diesem Bericht können Sie:

- die für jeden gescannten Netzwerkhost erkannten Antivirus-Anwendungen mit Name des Herstellers und Versionsangaben auflisten.

8.2.17 Überwachungsrichtlinie

80.143.32.211 - Andrew				
Betriebssystem Windows 2000		ServicePack 4		1
Kennwortrichtlinie				
Mindestkennwortlänge	Maximales Kennwortalter	Minimales Kennwortalter	Abmeldung erzwingen	Kennwortverlauf
0 chars	42 Tage, 22 Stunden, 47 Minuten, 31 Sekunden	Keine Verzögerung	Nie erzwingen	Kein Verlauf
2				
Sicherheits-Überwachungsrichtlinie				
Überwachungsrichtlinie		Erfolgreich	Fehler	
Kontenanmelde-Ereignisse überprüfen		Richtig	Richtig	
Kontoverwaltung überprüfen		Richtig	Richtig	
Dienstezuflussüberprüfen		Richtig	Richtig	
Anmeldeereignisseüberprüfen		Richtig	Richtig	
Objektzuflussüberprüfen		Richtig	Richtig	
Richtlinienänderungüberprüfen		Richtig	Richtig	
Rechteverwendungüberprüfen		Richtig	Richtig	
Prozessverfolgungüberprüfen		Richtig	Richtig	
Systemereignisseüberprüfen		Richtig	Richtig	
3				

Bild 99 – Musterbericht mit Anzeige der Richtlinien

1	Host-Computer IP-Adresse und Name
2	Details der Kennwortrichtlinie für jeden Host-Computer mit Mindestkennwortlänge und Kennwortverlauf
3	Liste mit Details zu den Sicherheitsüberwachungsrichtlinien für jeden Host-Computer

Mit diesem Bericht können Sie:

- die Einstellungen für die Kennwort- und Sicherheitsrichtlinie für jeden gescannten Netzwerkhost auflisten.

8.2.18 Registry-Informationen

80.143.32.140 - Jane	
Betriebssystem	ServicePack
Windows XP	2
Knotenname	Registry-Eintrag
	~MHz : 1802
	CSDVersion : Service Pack 2
	CurrentBuildNumber : 2600
	CurrentType : Uniprocessor Free
	CurrentVersion : 5.1
	Default : 0409
	DriverDesc : Media Control Devices
	DriverDesc : NVIDIA GeForce4 MX 4000 (Microsoft Corporation)
	Identifier : x86 Family 15 Model 31 Stepping 0
	InstallLanguage : 0409
	PathName : C:\WINDOWS
	ProductId : 76487-640-8145557-23290
	ProductName : Microsoft Windows XP
	RegisteredOrganization : ts
	RegisteredOwner : ts
	SoftwareType : SYSTEM
	SourcePath : G:\I386
	SystemRoot : C:\WINDOWS
	VendorIdentifier : AuthenticAMD
Run	NeroFilterCheck : C:\WINDOWS\system32\NeroCheck.exe
Run	Ptipbmf : rundll32.exe ptipbmf.dll,SetWriteCacheMode
Run	PtiuPbmd : Rundll32.exe ptipbm.dll,SetWriteBack
Run	SoundMan : SOUNDMAN.EXE
Run	WinampAgent : C:\Program Files\Winamp\winampa.exe

Bild 100 – Musterbericht mit Anzeige der Registry-Informationen

1	Host-Computer IP-Adresse und Name
2	Liste der Einträge in der Registry für jeden Hostcomputer

Mit diesem Bericht können Sie:

- die systemrelevanten Registry-Informationen für jeden gescannten Netzwerkhost auflisten.

8.3 Ergebnisvergleich

8.3.1 Netzwerksicherheitsprotokoll nach Datum

Scans folgender Tage vergleichen :	28/10/2008 14:07:54 und 30/10/2008 14:07:54	
Scan-Referenz :	80.143.32.1/24	
Scan-Profil :	Vollständiger Scan	1
Andrew		
NetBIOS-Warnmeldungen		
Service-Sicherheitsrisiken OVAL:1079: MS CIFS Spoofed Browse Frame Request Vulnerability wurde entfernt. Service-Sicherheitsrisiken OVAL:999: Hyperlink Object Buffer Overflow Vulnerability wurde entfernt. Service-Sicherheitsrisiken SNMP service is enabled on this host wurde entfernt.		
Registry-Warnmeldungen		
Registrierung-Sicherheitsrisiken AutoShareServer wurde entfernt. Registrierung-Sicherheitsrisiken Cached Logon Credentials wurde entfernt. Registrierung-Sicherheitsrisiken Guest users have access to the application log wurde entfernt. Registrierung-Sicherheitsrisiken LM Hash wurde entfernt. Neues Registry-Sicherheitsrisiko gefunden: Windows AutoUpdate is not enabled. Neues Registry-Sicherheitsrisiko gefunden: AutoShareWKS.		
3		

Bild 101 – Musterbericht mit Anzeige des Netzwerksicherheitsprotokolls, sortiert nach Datum

1	Netzwerksicherheitsscans, mit denen verglichen werden soll
2	Host-Computer, für den der Vergleich durchgeführt wurde.
3	Liste der Unterschiede, die bei Vergleichen mit jedem Hostcomputer gefunden wurden. Die Abweichungen werden nach Kategorien sortiert, beispielsweise nach Backdoors, fehlenden Hotfixes, Kennwortrichtlinie, USB-Geräten und Anwendungen.

Mit diesem Bericht können Sie:

- die Ergebnisse der aufeinanderfolgenden Scans mit einem gemeinsamen Profil und Ziel vergleichen und diese nach Scan-Datum zusammenfassen.

8.3.2 Netzwerksicherheitsprotokoll nach Host

Jane		1
Scans folgender Tage vergleichen :	5/17/2009 3:42:44PM and 5/18/2009 3:42:44PM	
Scan-Referenz :	80.143.32.1/24	
Scan-Profil :	Vollständiger Scan	2
Autokorrektur		
Autokorrektur durchgeführt: 'Patch Installation - Not Available (956391) - Cumulative Security Update for ActiveX Killbits for Windows 2000 (KB956391)'. Autokorrektur durchgeführt: 'Patch Installation - MS08-063 (957095) - Security Update for Windows 2000 (KB957095)'. Autokorrektur durchgeführt: 'Patch Installation - Not Available (890830) - Windows Malicious Software Removal Tool - October 2008 (KB890830)'. Autokorrektur durchgeführt: 'Patch Installation - MS08-062 (953155) - Security Update for Windows 2000 (KB953155)'. Autokorrektur durchgeführt: 'Patch Installation - MS08-065 (951071) - Security Update for Windows 2000 (KB951071)'. Autokorrektur durchgeführt: 'Patch Installation - MS08-067 (958644) - Security Update for Windows 2000 (KB958644)'.		
3		

Bild 102 – Musterbericht mit Anzeige des Netzwerksicherheitsprotokolls nach Host

1	Host-Computer, für den der Vergleich durchgeführt wurde.
----------	--

2	Verglichene Netzwerk-Sicherheitsscans
3	Liste der bei Vergleichen mit jedem Hostcomputer festgestellten Abweichungen ; die Abweichungen werden nach Kategorie sortiert, beispielsweise nach Backdoors, fehlenden Hotfixes, Kennwortrichtlinie, USB-Geräten und Anwendungen.

Mit diesem Bericht können Sie:

- die Ergebnisse aufeinander folgender Scans mit einem gemeinsamen Profil und Ziel vergleichen und diese nach Hostcomputer zusammenfassen.

8.3.3 Vergleich der Änderungen der Ausgangsdaten

80.143.32.211 - Andrew

Scan-Datum und Scan -Zeit : 5/21/2009 3:42:44PM
Scan-Referenz : 80.143.32.1/24
Scan-Profil : Vollständiger Scan

Betriebssystem : Windows 2000
ServicePack : 4

1

Vergleich des Benchmark -Computers mit den Hosts der Scan -Sitzung :

Scan-Datum und Scan -Zeit : 5/17/2009 3:42:44PM
Scan-Referenz : 80.143.32.1/24
Scan-Profil : Vollständiger Scan

2

80.143.32.140 - Jane

Betriebssystem	ServicePack
Windows XP	2

3

Allgemeiner Host

Bild 103 – Musterbericht mit Anzeige der Sicherheitseinstellungen im Vergleich

1	Details des als Vergleichsstandard verwendeten Computers mit Scan-Datum und Scan-Profil
2	Eine Liste mit den Host-Computern, mit denen der Standardcomputer verglichen wurde.
3	Liste der beim Vergleich der Host-Computer mit dem Standardcomputer festgestellten Abweichungen. Die Abweichungen werden nach Kategorien sortiert, beispielsweise nach Backdoors, fehlenden Hotfixes, Kennwortrichtlinie, USB-Geräten und Anwendungen.

Mit diesem Bericht vergleichen Sie die Ergebnisse zwischen einem bestimmten Computer, der als Standard verwendet wird, und den gescannten Hostcomputern mit dem gleichen Profil und dem gleichen Ziel.

9. Fehlerbehebung

9.1 Einführung

Das Kapitel Fehlerbehebung erläutert, wie Sie Softwareprobleme beheben, die eventuell auftreten. Die Hauptinformationsquellen für Benutzer sind:

- Das Handbuch – die meisten Probleme können durch Nachschlagen im Handbuch beseitigt werden.
- Die Artikel in der GFI Knowledge Base
- Web-Forum
- Kontakt zum technischen Support von GFI

9.2 Knowledge Base

GFI pflegt eine Knowledge Base, die Antworten auf häufige Probleme enthält. Bei Problemen schlagen Sie bitte zuerst in der Knowledge Base nach. Die Knowledge Base enthält die aktuellste Liste der Fragen an den technischen Support und die aktuellen Patches. Die Knowledge Base finden Sie unter <http://kbase.gfi.com/>.

9.3 Web-Forum

Technischer Support der Benutzer untereinander ist über das GFI Web-Forum verfügbar. Das Forum finden Sie unter <http://forums.gfi.com/>.

9.4 Anforderung von technischem Support

Wenn Sie im Handbuch nachgeschlagen haben und in den Artikeln der Knowledge Base nachgelesen haben, aber immer noch Probleme mit der Software auftreten, wenden Sie sich bitte an das Team für den technischen Support von GFI, indem Sie über ein Online-Formular technischen Support anfordern oder Sie können sich auch telefonisch an uns wenden.

- **Online:** Das Formular zur Anforderung von technischem Support füllen Sie bitte hier aus: <http://support.gfi.com/supportrequestform.asp>. Folgen Sie den Anweisungen auf dieser Seite, um Ihre Supportanforderungen abzusenden.
- **Telefonischer Support:** Die korrekte Telefonnummer für den technischen Support Ihrer Region finden Sie unter: <http://www.gfi.com/company/contact.htm>.

HINWEIS: Bevor Sie Kontakt mit unserem technischen Support aufnehmen, halten Sie bitte Ihre Kunden-ID bereit. Ihre Kunden-ID ist die Online-Kontonummer, die Ihnen zugewiesen wurde, als Sie Ihren Lizenzschlüssel in Ihrem Kundenbereich erstmals registrierten: <http://customers.gfi.com>.

GFI bemüht sich, Ihre Anfrage innerhalb von maximal 24 Stunden zu beantworten, je nach Ihrer Zeitzone.

9.5 Benachrichtigungen über Builds

Wir empfehlen Ihnen wärmstens, unsere Benachrichtigungsliste für Builds zu abonnieren. Auf diese Weise werden Sie laufend über neue Produkt-Builds informiert. Abonnieren Sie unsere Build-Benachrichtigungen unter: <http://www.gfi.com/pages/productmailing.htm>.

Index

A

Assistent 7, 34

B

benutzerdefinierte Berichte 24
Benutzerdefinierte Berichte 3, 5, 15,
25
Benutzeroberfläche 3, 30, 31, 39
Berichte exportieren 5

D

Das Produkt ReportPack 3
Datenbankquelle 40, 41, 42
Datenfilter 5, 15
Die Dropdown-Liste "Produktauswahl"
8, 47, 48

F

Fehlerbehebung 85
Filterbedingungen 18
Framework 1, 2, 3, 4, 7

H

Häufig benötigte Berichte 3, 13, 24

I

Installation 5, 7, 8, 39

K

Konfigurationseinstellungen 42

L

Lizenz 31

N

Navigationsschaltfläche 3, 4, 9, 10,
11, 13, 15, 20, 23, 24, 28, 29,
30, 31, 32, 33, 36, 39, 40, 41,
47, 48

Navigationsschaltfläche 3

S

Sicherheits-Scan 18
Standardberichte 3, 9, 13
Systemanforderungen 7

U

Überwachung zeitabhängiger
Aktivitäten 31

V

Verteilung von Berichten 4, 5

Z

Zeitabhängige Berichte 3, 4, 5, 30, 32