



## Sherlock Holmes Präventive Wartung



*Ihr persönlicher IT -  
Sherlock Holmes  
überwacht Ihr  
Netzwerk und bewahrt  
Sie vor unliebsamen  
Überraschungen*

## Inhaltsverzeichnis

1 Technische Hintergründe.....	3
1.1 Laufende Überprüfung der Hardware .....	3
1.2 Was enthält die Überwachung (Hardware) .....	4
1.3 Was kann überwacht werden.....	5
2 Voraussetzungen .....	7
2.1 Kunde .....	7
3 Welche Komponenten werden überwacht.....	7
3.1 Hardwareüberwachung.....	7
3.2 Softwareüberwachung: .....	7
3.3 Automatisierung: .....	8
4 Welchen Nutzen haben Sie.....	8
4.1 Reduzierung der Ausfallzeiten .....	8
4.2 Kein Wildwuchs von Programmen und damit weniger Softwarekonflikte.....	8
4.3 Planung der Liquidität (Ich weiß heute bereits was ich Morgen brauche .....	8
4.4 Transparente Übersicht der gesamten IT-Struktur.....	9
4.5 Erhöhung der Produktivität (weniger Ausfallzeiten) .....	9
4.6 Planbare Wartungszeiten.....	9
4.7 Erhöhte Sicherheit .....	9
5 Was ein Unternehmen schon immer haben wollte.....	9
6 Beispielreporte für das Berichtswesen.....	10

## 1 Technische Hintergründe

### 1.1 Laufende Überprüfung der Hardware durch präventive Wartung

Bei diesem Verfahren zur Überwachung eines Systems werden Informationen am Bus oder direkt im Speicher abgegriffen, ohne dass diese Informationsgewinnung Einfluss auf die Ausführung des überwachten Systems nimmt. Die präventive Wartung verfügt über eigene Betriebsmittel und muss somit nicht die des Zielsystems in Anspruch nehmen - es stellt daher keinen Störfaktor dar.

Wir schaffen die erforderliche Transparenz bezüglich des Zustandes des Netzwerkes und der einzelnen Komponenten, liefern wertvolle Informationen über die Historie und zeigen Trends und Tendenzen auf. Wir alarmieren die Systemverantwortlichen, wenn in Ihrem System kritische Zustände eintreten und Handlungsbedarf besteht. Dadurch kann das Unternehmen durch Sherlock Holmes:

- Probleme unmittelbar erkennen,
- ihre Ursachen schneller finden,
- gezielt und sicher handeln,
- agieren, statt reagieren.

Dies wirkt sich direkt auf die Qualität der durch die IT-Organisation bereitgestellten Dienste und Dienstleistungen aus. Unternehmen und Organisationen, die dieses professionelle Überwachungssystem einsetzen, verzeichnen bereits nach kurzer Zeit eine

- nachhaltige Erhöhung der IT-Verfügbarkeit,
- eine signifikante Senkung der Downtimes (System steht nicht zur Verfügung) und deren Folgekosten
- Senkung der IT-Betriebskosten.

## 1.2 Was enthält die Überwachung (Hardware)

- PING (Echo ICMP)  
Erreichbarkeit der Systeme, Response-Time
- SNMP GET (Polling)  
Auslesen beliebiger Variablen und Statusindikatoren
- SNMP TRAP  
Empfang, Bewertung, Collection
- WMI  
Auslesen definierter Werte und Stati von Microsoft-Systemen einschl. Performance-Counter, Eventlog-Einträge, Dienste etc.; Steuern von Windows-Systemen (Stop und Start von Diensten, Booten von Servern)
- TCP/UDP-Services  
Prüfen der Port-Verfügbarkeit
- Dienste/Prozesse (Windows)  
Prüfen des Status
- Eventlogs (Windows)  
Auswerten der Logs, Event-Filter; Senden von SNMP-Traps
- Netzwerk-Dienste  
Prüfen der Verfügbarkeit und Funktion von HTTP, HTTPS, SMTP, POP3, IMAP4, FTP, DNS, DHCP, NNTP, NTP, Telnet, NFS, RADIUS, LDAP, IRC, Gopher, Finger, WHOIS, RWHOIS...
- Datenbanken  
Erreichbarkeit von Tabellen; Betriebsparameter von Datenbanken (Tablespaces, Cachehits...); Login, Schreiben, Lesen, Logout in DB, damit Überwachung der kompletten Funktion möglich und auch Überwachung von Werten (Feldern) in DB's
- Systemparameter von Servern (je nach Betriebssystem)  
CPU-Last, Festplattenstatus, freier und belegter Speicher auf Festplatten/Partitionen/Volumes, RAM-Auslastung, Anzahl angemeldeter User, RAID-Status, Status/Durchsatz von LAN-Interfaces, System-Uptime, System-Handles (freie inodes, file handles) ...
- Filesysteme  
Verfügbarkeit von CIFS und NFS-Shares; freier Platz auf Laufwerk/Partition/Volume/Quota
- Files  
Existenz, Größe, Flags, Content; Lesen und Schreiben von Files

## 1.3 Was kann überwacht werden

- Alle Systeme mit einer IP-Adresse (auch Drucker). Überprüfung auf Erreichbarkeit mittels ping. Ermittlung der Response-Zeiten

### Netzwerkinfrastruktur-Komponenten

- Alle managbaren Router, Switches, Access-Points usw.
- Status von Ports, Status von Redundanzen
- Traffic, Übertragungsfehler
- Status von Modulen, Lüftern, Netzteilen, Temperatur
- Systemperformance
- Empfang und Bewertung von SNMP-Traps (Fehleralarmen)

### Server

- Systeme aller Prozessor-Architekturen (intel, RISC, Alpha, Power, SPARC...) aller Hersteller (HP, FSC, IBM, DELL, Sun, Compaq, DEC, Apple...), Blade Server
- Status von Disks, RAID-Controllern, LAN-Controllern, RAM, Systemboard, Netzteilen, Lüftern...
- Status von Redundanzen
- CPU-Last, Systemperformance
- Systemtemperatur
- alle weiteren Performancewerte und Statusindikatoren, die via SNMP verfügbar sind
- Empfang und Bewertung von SNMP-Traps (Fehleralarmen)

### Storage-Systeme

- NAS- und SAN Lösungen, Tape-Libraries
- Status von Disks, RAID-Controllern, LAN-Controllern, RAM, Systemboard, Netzteilen, Lüftern...
- Status von Redundanzen
- Systemperformance
- Auslastung von Volumens, Partitionen, SnapShots, Quotas
- Status von Ports (LAN, FC, iSCSI...)
- alle weiteren Performancewerte und Statusindikatoren, die via SNMP verfügbar sind
- Tape-Libraries: Band-, Laufwerks- und mechanische Fehler
- Empfang und Bewertung von SNMP-Traps (Fehleralarmen)

### USV-Systeme

- Systeme von APC, Online, MGE, HP, IBM.... (Voraussetzung SNMPmanagementfähig)
- USV-Status (online/offline)
- Last, maximale Pufferzeit, Zustand der Akkus

## Lösungsvorschlag Sherlock Holmes – präventive Wartung

---



- Temperatur
- alle weiteren Statusindikatoren, die via SNMP verfügbar sind
- Empfang und Bewertung von SNMP-Traps (Fehleralarmen)

## 2 Voraussetzungen

### 2.1 Kunde

Voraussetzung ist eine Internetverbindung.

## 3 Welche Komponenten werden überwacht

Die beschriebenen Funktionalitäten sind nur eine grobe Zusammenstellung. Details können nur in einem persönlichen Gespräch geklärt werden.

### 3.1 Hardwareüberwachung

- Unterstützung sämtlicher gängiger Hardware und Überwachung der Funktionen
- Besserer Überblick über IT Infrastruktur durch Prozess-Visualisierung
- Überwachung der Festplattenkapazität und bei Bedarf automatische Archivierung der LOG-Dateien
- Überwachung Biosmonitoring an Servern/Clients (Ausfall von Lüftern, Netzteilen, Spannungsschwankungen etc.)
- Aktuelle Übersicht über installierte Hard- und Software
- Neustart und Synchronisation der Rechner im Netzwerk
- Regelmäßige Überprüfung des Fragmentierungsgrades der Festplatten und automatische Reorganisation derselben
- Neustart und Synchronisation der Server im Netzwerk mit Überprüfung der Funktionalitäten nach dem Neustart bei einem Stromausfall die Server kontrolliert herunterfahren, solange die USV noch aktiv ist

### 3.2 Softwareüberwachung

- Neustart der Windows- und Unix- Dienste bei Ausfall, oder in Abhängigkeit zu anderen Komponenten im Rechenzentrum
- Überwachung von kompletten Anwendungen, unter Beachtung der Abhängigkeiten untereinander sowie der darunter liegenden Infrastruktur mit entsprechenden Aktionen wo nötig (z.B. Neustart)
- Aktuelle Übersicht der Hardware und der Software mit Meldung bei Installieren unerlaubter Software Komponenten
- Statusüberwachung der Datenbanken von Exchange, Oracle, SQL, Active - Directory etc. in Form von Erreichbarkeit, Auswertung von Log`s
- Monitoring von USV`s, Firewalls, Ereignisanzeigen, Windows Update Service durch Auswertung der LOG`s
- Überwachung komplexer Anwendungen, die über mehrere Rechner laufen
- Softwareverteilung von Installationen, Updates etc.

## 3.3 Automatisierung

- Meldung über alle Vorfälle per Email oder SMS
- Automatisches Skripting
- Zeitgesteuerte automatische Verteilung verschiedener Inhalte div. Dateierarten (doc,xls, html, ppt) im Netzwerk mit Dokumentation der einzelnen Versionen
- Durchsetzung interner Richtlinien durch Überwachung und automatisierte Aktionen
- Regelmäßiges automatisches Überprüfen der Antiviren Software und des Zustandes des Update Services, auch Bei Ausfall Neustart und Antivirus Update
- Automatisierter Arbeitsablauf für alle sich wiederholenden Tätigkeiten (Updates, Serverneustarts, Reporting (Mails), Fehlverhalten)

## 4 Welchen Nutzen haben Sie

### 4.1 Reduzierung der Ausfallzeiten

Durch die ständige Überwachung des Systems werden Produktionsausfälle auf ein Mindestmaß reduziert

### 4.2 Kein Wildwuchs von Programmen und damit weniger Softwarekonflikte

- Jeder Anwender benutzt denselben Programmstand (Version)
- Reduzierung von Betriebskosten:
- Überwachung von nicht autorisierter Software
- Kontrolle der Mitarbeiter von nicht erlaubten Downloads (MP3-Files, Filme, Spiele, ...)
- Anstieg von Onlinegebühren durch Filesharing
- Gewährleistung von standardisierter Softwareinstallation

### 4.3 Planung der Liquidität (Ich weiß heute bereits was ich Morgen brauche)

- Planen der finanziellen Mittel, die ich in Zukunft benötige um den gemessenen Engpass zu beseitigen. z.B.:
- Thermische Probleme (Lüfterdefekt, Netzteil, Prozessor)
- Verfügbare Speicherkapazität der Festplatte (Trendanalyse)
- Geringe Performance (Auslastung des Prozessors)
- Netzwerkauslastung

### 4.4 Transparente Übersicht der gesamten IT-Struktur

In monatliche Reports werden die überwachten IT-Prozesse dokumentiert. Dadurch ist auch in der IT, ein monatliches Berichtswesen gewährleistet.

### 4.5 Erhöhung der Produktivität (weniger Ausfallzeiten)

Durch weniger Ausfallzeiten erhält das Unternehmen eine höhere Kundenzufriedenheit. Ausfall der EDV-Anlage bedeutet immer, Kundenwünschen nicht zu entsprechen.

### 4.6 Planbare Wartungszeiten

Sie Wissen heute bereits was morgen kaputt ist, dadurch können Wartungsarbeiten kundenfreundlich geplant werden.

### 4.7 Erhöhte Sicherheit

- Durch kontrolliertes Patchmanagement werden nur Updates von Microsoft installiert, die vorher durch die PRAXIS AG getestet und freigegeben wurden. Damit erhöhte Stabilität der WDV 2010.
- Schließen von Sicherheitslücken von außen wie innen
- Anzeigen von Trends / Engpässen
- Speicherauslastung
- Zuwachs von Daten
- Netzwerkauslastung
- Prozessorauslastung
- Datensicherung

## 5 Was Ihr Unternehmen schon immer haben wollte

- Wie wäre es, wenn Sie voraussagen könnten, wann ihre EDV-Anlage eine Schwächephase erreicht?
- Wäre es nicht schön, wenn Sie vor der Verarbeitung wüssten, dass Ihre Festplatte nur noch geringe Kapazitäten hat?
- Wollten Sie schon immer mal wissen, ob Ihre Mitarbeiter am arbeiten oder am Filme schauen oder am Musik hören sind?
- Wäre es nicht schön, wenn sich kein Kunde mehr beschwert, nur weil Ihre EDV Anlage nicht störungsfrei läuft?
- Kundentreue durch eine stabile IT!
- Haben Sie keine Lust mehr, ständig Mitarbeiter für die IT abzustellen, um aufgetretene Störungen zu prüfen und zu beheben?
- Wollen Sie nicht auch eine stabile EDV, um ihre Kapitalressourcen zu schützen?
- Wollten Sie ein EDV-System, welches Störungen selber erkennt und behebt?
- Wollen Sie wirklich sicher sein, dass Ihre Sicherungen auch fehlerfrei funktionieren?
- Wollen Sie wissen, ob Mitarbeiter ohne Berechtigung lokal Software installieren und damit Viren, instabile Systeme, Abstürze oder Lizenzverletzungen provozieren?

## 6 Beispielreporate des Berichtswesens

Im Folgenden werden verschiedene, aber nur provozierte mögliche Auswertungen über die ermittelten Werte dargestellt. Die Zahlen sind nicht aussagekräftig, da es nur Beispiele sind. Alle Arten von Statistiken sind von uns frei definierbar und können nach Wunsch verändert werden. So ist es auch möglich, eigene Abstimmungen z.B. nach ITIL (IT-Infrastructure Library) zu definieren:

- Verfügbarkeit des Gesamtsystems
- In wie vielen Tagen ist meine Festplatte voll
- Wie viele Störungen im Bereich Hardware sind aufgetreten
- Welche Dienste wurden wie oft automatisch neu gestartet
- Wie oft gab es Virenbefall im Monat, Quartal und jährlich
- Welcher Arbeitsplatz hat wie oft Software installiert
- Wann und wie oft wurde an der Struktur der WDV 2010 etwas verändert

Dies sind nur Beispiele und je nach Wunsch veränderbar.

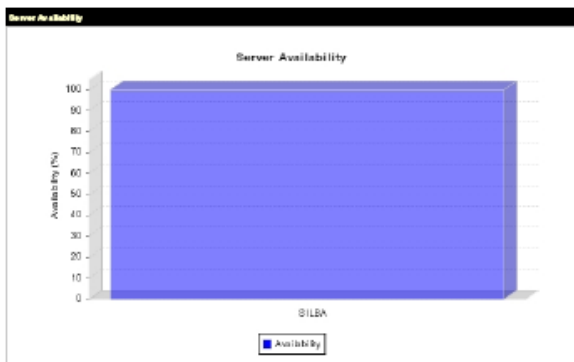


Bild: Verfügbarkeit des Servers SILBA

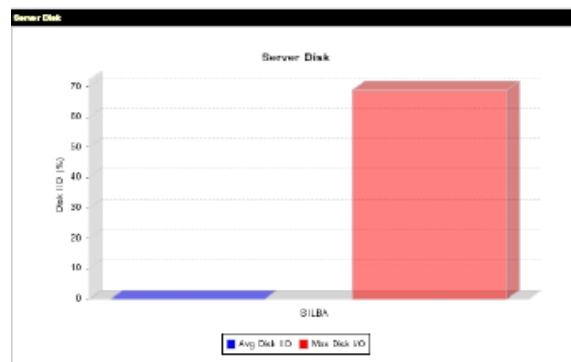
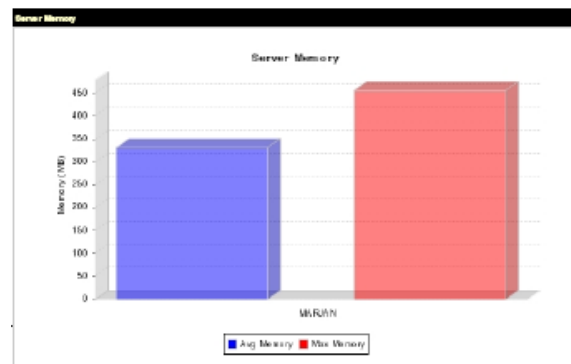
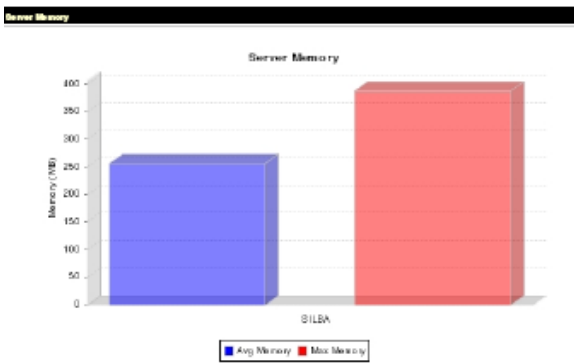


Bild: Festplattenauslastung des Servers SILBA



# Lösungsvorschlag Sherlock Holmes – präventive Wartung

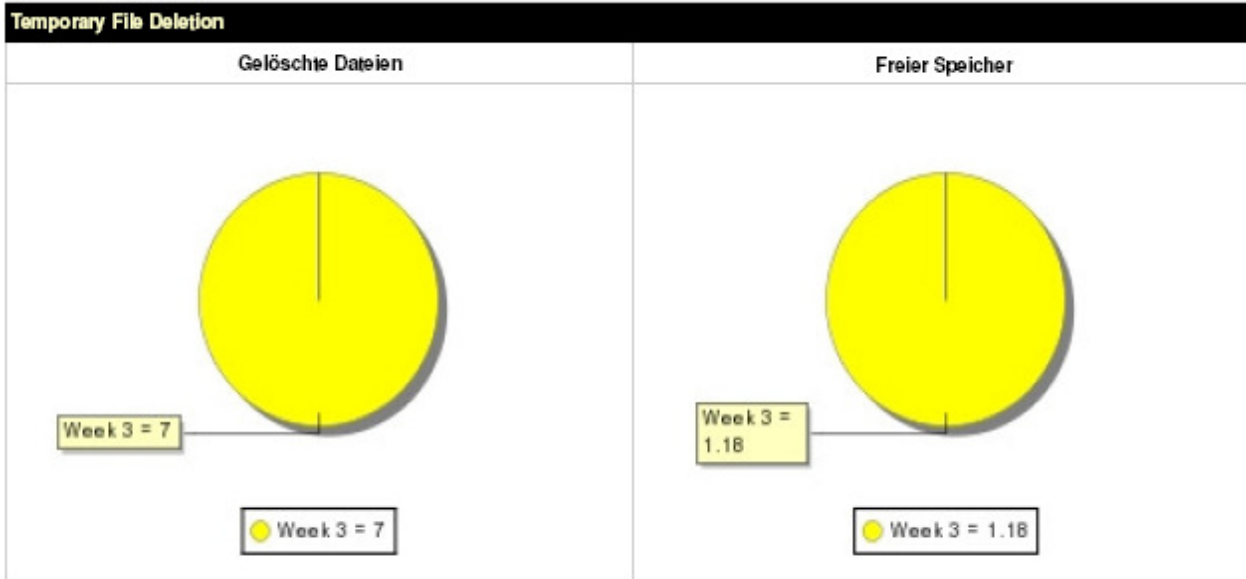
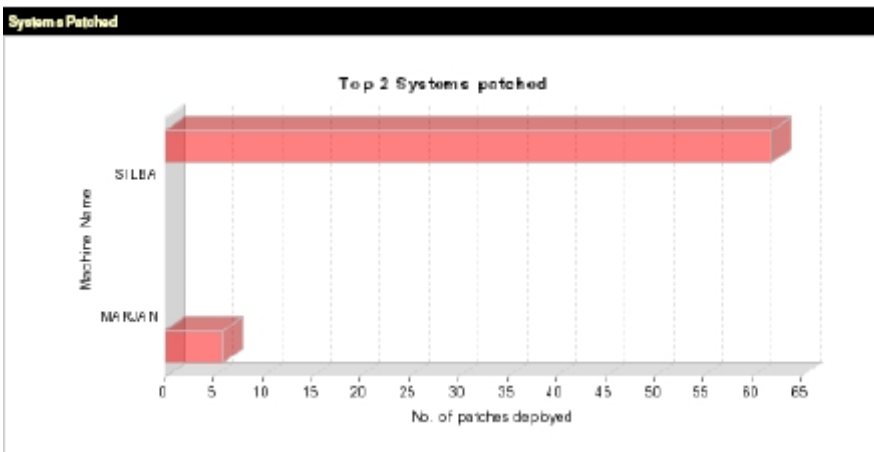


Bild: Gelöschte Temporäre Daten und Darstellung des dadurch gewonnen freien Speichers



(Note: This graph will show Top 20 systems on the basis of patches deployed.)

Bild: Darstellung der gepatchten Systeme SILBA und MARJAN

# Lösungsvorschlag Sherlock Holmes – präventive Wartung

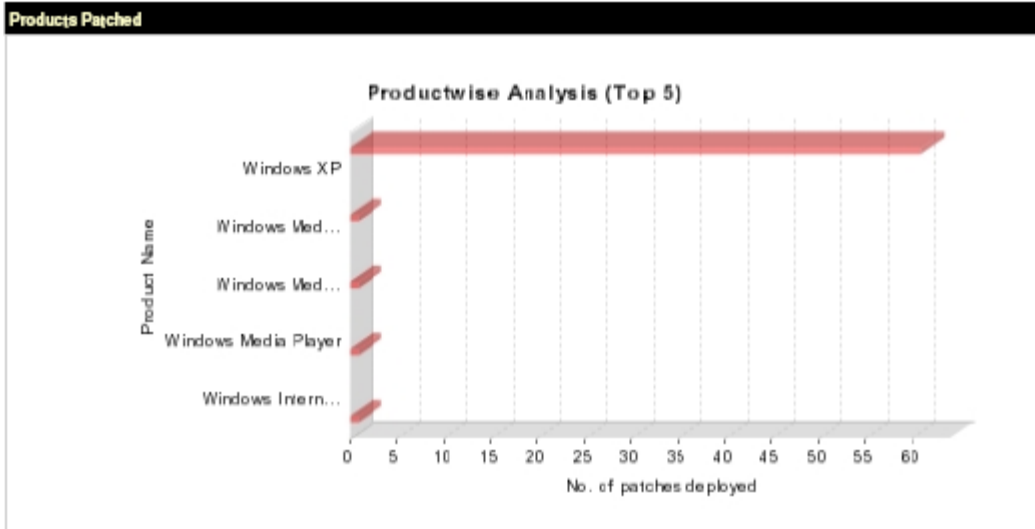


Bild: Darstellung der gepatchten Produkte

**Overview**

**Backup Servers**

**MARJAN** ■ - Success ■ - Failed ■ - No data

**Job Status for the Month of March 2007**

Job Name	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
Backup 00002	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Backup 00003	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

**Failure Job Details**

**MARJAN**

**Unique errors for jobs for the Month of March 2007**

Job Name	Error Description
Backup 00003	The job has completed with an error. The directory is invalid.

**Time Analysis**

**MARJAN**

Job Name	Avg Time Taken	Min Time Taken	Max Time Taken
Backup 00002	00:00:20	00:00:20	00:00:20
Backup 00003	00:00:07	00:00:07	00:00:08

Bild: Übersicht der durchgeführten Sicherungen des Servers MARJAN

# Lösungsvorschlag Sherlock Holmes – präventive Wartung



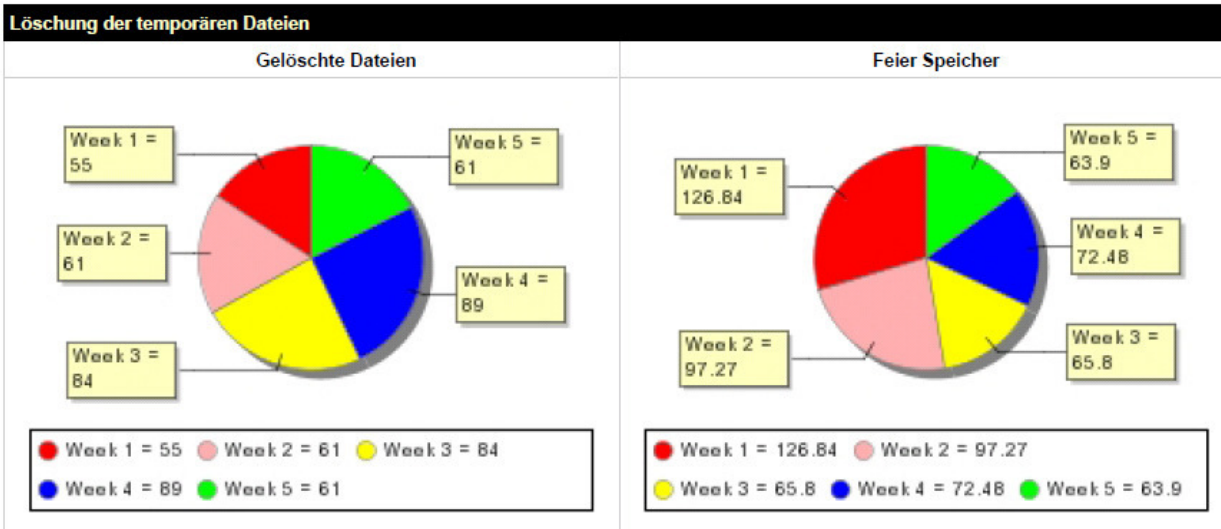
Asset [Total Number of Machine]	
Total Machine Scanned	2

Asset [Desktop / Server]	
Operating System	No. Of Machines
Windows XP Professional	2

Top 10 Software Installed [10 Softwares Found]	
Software	Total
AddressBook	2
Address Book 6	2
Advanced Authoring	2
.NET Framework	2
Active Directory Service Interface	2
AmdoSoft/OCT Agent 4.5	2
Branding	2
Browser Customizations	2
Browsing Enhancements	2
Connection Manager	2

Service Pack Installed	
Service Pack	Total
Windows XP Professional Service Pack 2	2

Bild: Übersicht der durchgeführten Scanns der installierten Software





# Lösungsvorschlag Sherlock Holmes – präventive Wartung

---



## B. Server Zustand

Dieser Bericht gibt Ihnen Auskunft darüber, in welchem Zustand Ihr Server ist. Ziel dieses Monitorings ist es Bedingungen zu entdecken und entfernen, die die Produktivität Ihres Servers beeinträchtigen könnten. Der Bericht dokumentiert die den Zustand des Servers knapp und präzise ohne tief in technische Details zu gehen.

Notizen und Anmerkungen für ein besseres Verständnis des Berichts aus Endnutzer Sicht:

- Mein Server ist sehr wichtig für meine IT Umgebung. Ich möchte die Verfügbarkeit und Schnelligkeit kennen. Dadurch kann ich besser erkennen ob meine Geschäftsanwendungen verfügbar waren und zufrieden stellend auf Kundenanfragen reagiert haben.
- Wie ausgelastet ist der Server? Ein zu stark ausgelasteter Server kann nicht mehr schnell genug auf Kundenanfragen reagieren. Hieraus ergeben sich unzufriedene Nutzer, und einer der Hauptaspekte unseres Job als Administrator ist es schließlich die Nutzer, die wir unterstützen, zufrieden zu stellen.
- Gibt es genug Hauptspeicherplatz? Es ist sehr wichtig die Auslastung dieser äußerst relevanten Quelle zu kennen.
- Wie arbeiten die Server Festplatten? Ein Engpass bei einer Festplatte kann die Antwortzeit für auf dem Server laufende Anwendungen verringern, was wiederum zu unzufriedenen Nutzern führt.

## C. Hotfix Management

Es gab bisher schon mehrere weit verbreitete Angriffe und Schwachstellen auf Microsoft Software. Viele Unternehmen, die ein proaktives Sicherheits Patch Management eingesetzt haben, wurden hiervon nicht betroffen, weil sie auf Informationen reagiert haben, die Microsoft bereits vor diesen Angriffen zur Verfügung gestellt hatte. Dieser Bericht liefert Informationen zum Patch Management, welches bei Ihnen zusammen mit dem Sicherheits Hotfix durchgeführt wurde.

## D. Backup Handhabung

Die Komplexibilität und Flüchtigkeit von Backup Handlungen machen es schwer für Unternehmen, die tatsächliche Backup Rate und, was noch wichtiger ist, die Wiederverwendbarkeit der Daten nachzuvollziehen. Unternehmen sind durch Datenverluste erheblichen Geschäftsrisiken ausgesetzt. Ihre IT Abteilungen müssen vor dem nächsten Backup Zeitfenster Fehlerquellen herausfinden und beheben. Dieser Berichts stellt Ihnen ein knappes und präzises Dokument über die Backup Vorgänge und -Fehler, Grundursachen und Performance zur Verfügung.

## E. Information über Ihre IT-Umgebung

Dies ist eine Übersicht über Ihre IT Umgebung, speziell für interne Besprechungen gedacht.