j.a.m. GmbH

Wartung

Ein Leitfaden zur Wartung von EDV-Anlagen

Virenschutz | Hardware | Backup | Netzwerk | Datenbanken

Die Einrichtung und Ausführung einer regelmäßigen Wartung dient in erster Linie der Vorbeugung von Ausfällen der EDV-Anlage. Leider wird des öfteren genau dieser Grundsatz vernachlässigt – sei es aus Unwissenheit oder um vermeintliche Kosten zu sparen. Das Ergebnis sieht unserer Erfahrung nach immer gleich aus: Kommt es zum Schadensfall, entstehen oftmals deutlich höhere Kosten und längere Ausfallzeiten, als bei einer konsequent gepflegten Hard- und Softwareplattform.

Vorteile

Die Vorteile einer regelmäßigen und gewissenhaften Wartung liegen auf der Hand:

- viele Wartungsaufgaben lassen sich von Ihnen selbst durchführen, darüber hinausgehende Tätigkeiten werden von j.a.m. erledigt
- die Spezialisten der j.a.m. GmbH bieten „Rundumwissen" – ein Einzelner kann heutzutage nicht mehr in allen Fragen rund um die EDV Wissen besitzen
- feste Wartungsintervalle für festgelegte Aufgaben – vergessen zählt nicht
- fixe Kosten, mit denen Sie kalkulieren können
- sicherer, störungsfreier und nahezu ausfallsicherer Betrieb
- klar definierte und geplante Wartungsfenster können zu „ruhigen" Arbeitszeiten oder sogar außerhalb der Kernarbeitszeiten angesetzt werden – Ihr Vorteil ist die geringere Behinderung der eigentlichen Arbeit (im Gegensatz zur panikartigen Problembehebung)

Wir erarbeiten gerne mit Ihnen einen detaillierten Wartungsplan. Sie werden feststellen, dass einige, vielleicht sogar der Großteil der Arbeiten durch Sie selbst durchgeführt werden können. Dieser Leitfaden soll Ihnen hierzu eine Hilfe sein.

Allgemeines

Einige Grundsätze erscheinen zwar selbstverständlich, sollen hier aber trotzdem Erwähnung finden, denn sie bilden die Grundlage einer erfolgreichen Systemwartung.

- Erstellen Sie, falls nicht vorhanden, eine Auflistung aller verwendeten Hard- und Softwareprodukte. Aktualisieren Sie die Liste bei Neuanschaffungen, dem Ersetzen oder Entfernen von Produkten. So lässt sich bei einem Ausfall von Hardware schnell Ersatz beschaffen.
- Überlegen Sie sich, mit welchen Ausfallzeiten Ihrer Gesamt-EDV bzw. Teilen davon Sie „leben" können. Die meisten erkennen diese Fragen erst in dem Moment als lebenswichtig, wenn die EDV bereits nicht mehr verfügbar ist. Denken Sie auch an Ausfallzeiten durch Vandalismus, Diebstahl, Unwetterschäden und ähnliches.
- Prüfen Sie von Zeit zu Zeit die Unterlagen und auch die an die EDV gestellten Anforderungen hinsichtlich der in sie gesetzten Ziele. Haben sich Anforderungen geändert, sind mehr Mitarbeiter oder umfangreichere Projekte in Ihr Unternehmen gekommen, wächst natürlich auch die EDV. Stimmen die Backupstrategien, sind Ressourcen überlastet?
- In Zeiten der globalen Vernetzung ist theoretisch der Zugriff auf jeden einzelnen vernetzten PC von jedem Punkt der Welt aus möglich. Die daraus erwachsenden Vorteile ziehen natürlich auch Probleme nach sich. Ein gesundes Misstrauen dem Internet gegenüber sollte selbstverständlich sein. Können Außenstehende oder Besucher aber auch Mitarbeiter Zugriff auf Informationen erlangen, die ihnen nicht zur Verfügung stehen sollten? Gerade die immer mehr in Mode kommenden Funknetzwerke können zu ernsthaften Sicherheitsproblemen führen.
- Wie wird mit Passwörtern umgegangen? Müssen die Passwörter regelmäßig geändert werden? Kennen mehrere Benutzer die Kennwörter von Kollegen?
- Dokumentieren Sie Ihre EDV. Erstellen Sie Dokumente für Neuinstallationen bzw. lassen Sie diese erstellen.

Eschersheimer Landstr. 471 · 60431 Frankfurt
Telefon: 0 69/4 60 98-800 · Fax: 0 69/4 60 98-878
E-Mail: info@jam-gmbh.de · Internet: www.jam-gmbh.de

Wartung

Ein Leitfaden zur Wartung von EDV-Anlagen

Virenschutz

Durch die Überwachung und regelmäßige Überprüfung des Virenschutzes sowohl auf Client- als auch auf Serverseite wird eine maximale Sicherheit gegenüber bestehenden und vor allem neuen Viren und Würmern erreicht. Dazu ist ein regelmäßiges Erneuern der sogenannten Virenpatterns erforderlich. Diese müssen natürlich auch auf dem Client bzw. Server aktiv werden.

Prüfpunkte

1. Virensignaturen der Clients überprüfen (Finden Updates statt? Wann fanden die letzten Updates statt?)
2. Virensignaturen der Server überprüfen (Finden Updates statt, werden die Signaturen an die Clients ausgeliefert?)
3. Strategie des Virenschutzes prüfen (Genügt das regelmäßig konfigurierte Update?)
4. Bei veralteten Virenscannern oder Befall gesamte Festplatte prüfen
5. Funktion des Virenscanners prüfen (Testmuster erkennen lassen! Ist der Virenscanner aktiv?)
6. Taskmanager auf ungewöhnliche Prozesse überprüfen

Spy-/Adware

Nicht erst seit gestern verseuchen so genannte Adwareprogramme das Internet. Einmal auf dem lokalen Rechner angekommen, beglücken sie den Benutzer durch von Zeit zu Zeit aufgehende Browserfenster mit Werbungsinhalten. Oder aber sie senden Informationen über das Verhalten des Benutzers an ihre zentrale Sammelstelle und sorgen so für die Durchleuchtung des PC-Benutzers. Umleitungen des verwendeten Browsers auf fremde Seiten sind ein typisches Zeichen für befallene Systeme.
Eine Spy- oder Adware von einem PC zu entfernen ist in den meisten Fällen eine zeitintensive Beschäftigung und sollte nach Möglichkeit vermieden werden.

Prüfpunkte

1. Ausführen und Aktualisieren von entsprechenden Scannern. Diese berichten und entfernen teilweise auch die gefundenen Adware-Softwarepakete.

Backup

Sind Daten verloren gegangen, kommt das oft vernachlässigte Backup ins Spiel. Ein unter „ferner liefen" betreutes Backup kann die hohen Ansprüche, die daran gestellt werden, nicht erfüllen. Daher gehört zu einem gepflegten EDV-System eine durchdachte Backupstrategie und vor allem eine regelmäßige Überprüfung und Überwachung des Backups. Das Feststellen eines Fehlers im Backup bei einer Wiederherstellung ist mit Sicherheit der ungünstigste Zeitpunkt...

Prüfpunkte

1. „Soll" bzw. Strategie überprüfen (Wird alles gesichert was gesichert werden muss?)
2. Backup Log überprüfen
   a. Fehler beim Backup
   b. Generationssicherheit
   c. Vollständigkeit
   d. Backupzeitpunkt
3. Backup Wiederherstellung prüfen
   a. Vollständige Wiederherstellung
   b. Stichprobenhafte Wiederherstellung
4. Backupmedienaufbewahrung prüfen
5. Backupzeitraum überprüfen

Windows-Clients

Eine kontinuierliche Betreuung der Windows-Clients sorgt für einen reibungslosen Alltag Ihrer Mitarbeiter. Dazu gehören in erster Linie das Einspielen von Sicherheitsupdates aber auch die Überwachung der durch Einschränkungen bestimmten Grenzen – sowohl hinsichtlich der Hardware des Systems als auch im Hinblick auf die Benutzung der Arbeitsplatzrechner durch die Mitarbeiter.

Prüfpunkte

1. Windows Update ausführen
2. Windows Patches einspielen
3. Taskmanager auf ungewöhnliche Prozesse überprüfen (siehe auch Virenbefall)
4. Festplattenplatz prüfen
5. Postfächer auf Größe prüfen
6. Portscan von außen durchführen
7. Installierte Software inventarisieren, Veränderungen feststellen und dokumentieren

Eschersheimer Landstr. 471 · 60431 Frankfurt
Telefon: 0 69/4 60 98-800 · Fax: 0 69/4 60 98-878
E-Mail: info@jam-gmbh.de · Internet: www.jam-gmbh.de

Hardware

Hardware unterliegt ständiger Belastung durch Umwelteinflüsse. Hiervon betroffen sind in erster Linie „bewegliche" bzw. durch Hitze beanspruchte Komponenten. Eine Vorsorge durch die frühzeitige Erkennung von Problemen kann schwerwiegende Folgen, wie beispielsweise Datenverlust, vermeiden. Eine Überprüfung wichtiger Komponenten ist für die Betriebssicherheit ausschlaggebend.

Prüfpunkte

1. Lüfter in PCs überprüfen
   a. Netzteil
   b. CPU
   c. Grafikkarte
   d. Gehäuselüfter
2. Staub aus Gehäuse entfernen
3. Maus/ Tastatur reinigen

Netzwerk

Netzwerke erlauben ein schnelles Austauschen von Daten – innerhalb eines Standortes, zwischen mehreren Standorten eines Unternehmens und natürlich auch weltweit über die Strukturen des Internets. Doch genau dies birgt natürlich auch Gefahren. Ein schlecht gewartetes Netzwerk kann fremde Teilnehmer beherbergen. Die Zugriffspunkte der einzelnen Rechner können vollkommen schutzfrei dem Internet ausgesetzt oder über eine Firewall geschützt sein. Ein WLAN dient nicht nur der maximalen Mobilität, sondern auch, im Falle eines mangelhaften Schutzes, dem einfachst denkbaren „Einbruch" in ein lokales Netzwerk.

Prüfpunkte

1. Firewall
   a. Log prüfen sofern vorhanden
   b. Updates einspielen
   c. Portscan gegen Firewall ausführen
   d. Einstellungen überprüfen
   e. Funktion prüfen
   f. VPN
      i. Policies prüfen
      ii. VPN Benutzer prüfen
2. Windows Clients im Netzwerk mit Sicherheitspaketen (Nessus, Microsoft Baseline Security Test, ...) prüfen
3. Bestandsabbild der Netzwerkclients, sowohl LAN als auch WLAN
4. WLAN Security prüfen

Windows-Server

Die Überwachung der Windows-Server erscheint auf den ersten Blick wesentlich einfacher als die der Clients: Eine eingeschränkte Benutzergruppe wartet den Server, führt Konfigurationsänderungen durch und sorgt vor allem durch die hohe Anforderung, die an einen Server gestellt wird, für ein größeres Bewusstsein der Notwendigkeit von regelmäßigen Wartungen. Auf der anderen Seite erfahren einmal konfigurierte Systeme selten notwendige Updates oder Überprüfungen: „Es läuft ja alles einwandfrei!" und leider hat auch diese Einstellung an mancher Stelle ihre Berechtigung.

Prüfpunkte

1. Windows Update ausführen
2. Windows Patches einspielen
3. Taskmanager auf ungewöhnliche Prozesse überprüfen (siehe auch Virenbefall)
4. Domäne prüfen
   a. Größe der Benutzerprofile
   b. „Leichen" in der Benutzerliste, Benutzerliste exportieren
   c. Festplattenplatz für Profile, Home-Laufwerke feststellen
   d. Postfachgrößen überprüfen
   e. Passwortchecker gegen Domäne/ evtl. Clients
5. Festplattenplatz prüfen
6. Zustand des Hardware-/ Software-RAIDs?

Linux-Server

Ihrem Ruf, Stabilität und Flexibilität in Form eines exzellenten Serversystems zu vereinigen, werden Linux-Systeme durchaus gerecht. Umfangreiche Logs zeigen detailliert Probleme an – gerade bevor aus kleineren Schwierigkeiten handfeste Probleme erwachsen. Doch auch ein stabiles Betriebssystem will gewartet, immer auf dem aktuellsten Stand gehalten sein und die Loginformationen ausgewertet wissen.

Eschersheimer Landstr. 471 · 60431 Frankfurt
Telefon: 0 69/4 60 98-800 · Fax: 0 69/4 60 98-878
E-Mail: info@jam-gmbh.de · Internet: www.jam-gmbh.de

Prüfpunkte

1. Server Log-Dateien
   a. auf Fehlermeldungen, Warnungen etc. prüfen
   b. werden die erforderlichen Logs geschrieben
   c. funktioniert das Logrotate
2. Test auf Rootkits durchführen
3. Passwortcheck gegen Authentifizierungsdateien, Warnungen aussprechen, Konten sperren
4. Online Updates durchführen
5. Patches einspielen
6. laufende Dienste prüfen, Snapshot erstellen
7. Festplattenplatz prüfen
8. Dienste prüfen (überflüssige entfernen, offene Ports usw.)

Datenbanken

Einmal optimal aufgesetzt, versieht ein Datenbanksystem in der Regel seinen Dienst klaglos. Oft wird von Wartungen abgesehen, da sich Fehler ja zunächst meist nur in „kleiner" Form äußern. Werden aus den anfänglichen Aussetzern allerdings handfeste Probleme, ist es meist schon zu spät – die mühsam erfassten Daten sind entweder schon verloren oder zumindest in Gefahr, Arbeitsprozesse können nicht mehr reibungslos ablaufen.

Prüfpunkte

1. Backup/ Export durchgeführt?
2. Status (Online, usw.)
3. Logs auf Fehler prüfen
4. Freien Speicher prüfen, Tablespaces prüfen
5. Performance der Datenbank feststellen, festhalten für spätere Vergleiche

Kontakt

Für Fragen und Anregungen stehen wir Ihnen gerne zur Verfügung. Gerne erstellen wir Ihnen einen detaillierten Wartungsplan und unterstützen Sie bei der Durchführung und Überwachung der einzelnen Arbeiten.

Sie erreichen uns telefonisch, per E-Mail oder Telefax. Gerne nehmen wir Ihre bestehende DV-Anlage unter die Lupe und überzeugen uns vor Ort von den Gegebenheiten.
Wir freuen uns auch über Ihren Besuch auf unseren Webseiten oder in unserem Haus.

Eschersheimer Landstr. 471 · 60431 Frankfurt
Telefon: 0 69/4 60 98-800 · Fax: 0 69/4 60 98-878
E-Mail: info@jam-gmbh.de · Internet: www.jam-gmbh.de

j.a.m. GmbH
Computer, Systemberatung, Softwareentwicklung, Webservices

Eschersheimer Landstr. 471
60431 Frankfurt

Telefon 0 69/4 60 98-800
TeleFax 0 69/4 60 98-878
E-Mail info@jam-gmbh.de
Internet http://www.jam-gmbh.de

Per Fax an 0 69/4 60 98-878

Mein Name: _____

Meine Adresse: _____

E-Mail: _____

Telefon: _____

☐ **Bitte schicken Sie mir weitere Informationen zu:** _____

_____

_____

☐ **Bitte erstellen Sie mir ein unverbindliches Angebot zu:** _____

_____

_____

Bemerkungen: _____

_____

_____

_____