

Monitoring: 8 Dinge, die Sie in Ihrem Netzwerk überwachen sollten

cebra GmbH - new technologies

Sankt Martin Str. 9, 84539 Ampfing

Telefon: +49 8636 69 76 67

E-Mail: info@cebra.it

Webseite: <https://www.cebra.it>



Allgemeines

Autor:	Christian Sigl
Version:	3.0
Versionsdatum:	2022-08-02

Vorwort

Handeln Sie proaktiv und nicht reaktiv - ihr Geldbeutel wird es Ihnen früher oder später danken!

Eine konsequente Überwachung aller Server, Rechner und Netzwerkgeräte kann Ihnen enorm viel Zeit und vor allem Nerven sparen. Mit geeigneten Monitoring Tools können Sie mögliche Fehler frühzeitig erkennen und anschließend proaktiv beheben. Was man überprüfen sollte und wann ein Eingreifen erforderlich ist erfahren Sie im folgenden Artikel.



Designed by rawpixel.com from [Freepik](https://www.freepik.com)

1. Performance

Mithilfe geeigneter Tools können Sie prüfen, ob Ihre Systeme beeinträchtigt oder optimierbar sind. Es kann z.B. die Festplattenaktivität, Speicher- oder CPU-Auslastung in Echtzeit überwacht und so Rückschlüsse auf Performanceengpässe gemacht werden. Liegt die aktive Datenträgerauslastung für einen bestimmten Zeitraum (z.B. 10 Minuten) über einen definierten Schwellwert von z.B. 90%, sollte die Ursache geprüft werden.

2. Potentielle Festplattenfehler

Mithilfe der Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T) können Festplattenlaufwerke (HDD) und Solid-State-Drives (SSD) überwacht und so Vorhersagen eines möglichen Ausfalls getroffen werden. Verschlechtert sich zum Beispiel die Anzahl der brauchbaren Sektoren einer Festplatte, sollte man sich langsam Gedanken um einen Austausch der HDD machen, um einen Ausfall des Gesamtsystems zu vermeiden.

3. Kapazitätsgrenze Festplattenspeicher

Immer wieder kommt es vor, dass die internen Festplatten eines Systems durch Software, Logfiles, temporäre Updatedateien und Backupdaten vollgeschrieben werden. Erreicht der freie Speicherplatz einen kritischen Schwellwert von beispielsweise 10-15%, kann automatisiert eine Festplattenbereinigung mit dem Löschen temporärer Dateien gestartet werden.

4. Ausstehender Neustart von Geräten

Server, Workstations und Mobile Clients wie Notebooks sollten in regelmäßigen Abständen neu gestartet werden. Nach der Installation von Windows Updates oder wichtigen Sicherheitspatches erfordern die Systeme meist einen Neustart um die Installationen abschließen zu können.

5. Ausführung kritischer Anwendungen

Fallen kritische Anwendungen oder Dienste auf einem Server aus, können diese in Echtzeit identifiziert und unmittelbar neu gestartet werden. In den meisten Fällen ist die Ausfallzeit eines Dienstes mit einem geeigneten Monitoring-Tool so gering, dass die Mehrheit der Mitarbeiter den Ausfall gar nicht mitbekommt.

6. Netzwerküberwachung

Mit einer Monitoring-Software können Sie außerdem prüfen, ob alle notwendigen Netzwerkgeräte verfügbar sind sowie offene Ports oder die Verfügbarkeit von Kunden-Websites überwachen. Wird z.B. aus irgend einem Grund die Windows-Firewall deaktiviert (z.B. durch einen unerlaubten Zugriff), besteht die Möglichkeit sich automatisch benachrichtigen zu lassen und die Windows-Firewall wieder zu aktivieren.

7. Fehlerhafte Anmeldeversuche von Benutzern

Über einen Windows-Fehler im Ereignisprotokoll lässt sich nachvollziehen, ob ein Benutzer versucht hat, sich mit einem falschen Passwort anzumelden. Bei Überschreitung einer bestimmten Anzahl an Anmeldeversuchen können Sie sich umgehend benachrichtigen lassen und anschließend der Ursache auf den Grund gehen.

8. Fehlgeschlagene Backups

Eines der wichtigsten Themen ist wohl das Thema Datensicherung. Für nähere Informationen möchte ich Sie auf den Artikel [Das Gesetz || 3-2-1 Regel für Backups](#) verweisen. Hier finden Sie

alle wichtigen Informationen rund um das Thema Datensicherung.

Mithilfe einer Monitoring-Software können Sie sich natürlich auch im Falle von fehlerhaften Backups benachrichtigen lassen. So können Sie schnellstmöglich reagieren, sodass Sie im Worst-Case-Szenario alle Daten wiederherstellen können.

Fazit

Ein effektives Monitoring kann Ihnen unter Umständen enorm viel Zeit, Geld und Nerven sparen. Sie als Geschäftsführer(in) müssen letztendlich die Kosten für einen Ausfall der IT-Infrastruktur tragen. Aus diesem Grund sollten Sie unbedingt tätig werden und eine geeignete Monitoring-Lösung implementieren.

Mit diesen hilfreichen Tools können Sie nicht nur interne Hardwarekomponenten wie die CPU oder die Festplatten eines Systems überwachen, sondern auch die Systeme von temporären Altdaten bereinigen und automatisierte Neustarts durchführen.

Handeln Sie proaktiv und nicht reaktiv!

Revision #19

Created 2022-07-22 09:22:57 UTC by Christian Sigl

Updated 2022-08-25 14:58:02 UTC by Christian Sigl