Ihre IT Zukunft

Wissen, dass **alles läuft:**

Mit MCS und **Checkmk**

Die Unterbrechung wichtiger IT-Services für wenige Stunden kann heute bereits geschäftskritisch sein.

Die Ursachen für Störungen und Ausfälle in IT-Systemen sind vielfältig: von Hardware-Ausfällen bis zu gezielten Angriffen durch Kriminelle. Um drohende Probleme frühzeitig zu erkennen, ist die lückenlose Überwachung, das Monitoring der gesamten IT-Architektur eines Unternehmens notwendig. Eine Aufgabe, die immer anspruchsvoller wird, da die Zahl der zu überwachenden Geräte (z. B. IoT) und Dienste (z. B. Mikroservices) rasant wächst und die Komplexität der Architekturen zunimmt, etwa durch Virtualisierung und Multi-Clouds.

Dieses Whitepaper stellt mit Checkmk eine Lösung für die Herausforderungen vor.

Die **Komplexität der IT-Welt** wächst

Neue Geschäftsmodelle, neue Möglichkeiten, neue Technologien:

Das Wirtschaftsleben verwandelt sich gerade tiefgreifend. Was unter dem Begriff Digitalisierung zusammengefasst wird, verändert

- **Lieferketten**,
- die **Kommunikation** mit Kund:innen und Interessent:innen,
- die Art und Weise, wie Menschen und Unternehmen **einkaufen** und auch
- die **Arbeit in Unternehmen** an sich.

// Seit 30 Jahren sind wir **Lösungspartner** für komplexe Unternehmens-IT. //

Michael Rademacher _ Ihr MCS-Experte

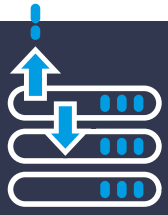
Immer neue technologische Möglichkeiten schaffen eine zunehmend komplexere und kleinteiligere IT-Welt.

- **Sensoren des Internet of Things** (IoT) überwachen auf dem Transportweg die Temperatur von Produkten, schaffen in Echtzeit mehr Transparenz in der Logistik oder liefern via Blockchain einen lückenlosen Herkunftsnachweis.
- **Intelligente Stores** kombinieren verschiedene Technologien (Gewichtssensoren, Kameras usw.), um den Warenbestand in Echtzeit zu überwachen. Mittels KI werden schrumpfende Lagermengen und Regallücken erkannt und eine Nachbestellung ausgelöst. Gleichzeitig erlauben sie es den Kunden einzukaufen, ohne sich an einer Kasse anstellen zu müssen.
- Versicherungsunternehmen arbeiten an **Verbrauchstarifen**, die auf die in Fahrzeugen ohnehin eingebauten Sensoren zugreifen, um das Fahrverhalten und die Nutzungsdauer zu ermitteln.
- In der Industrie 4.0 kümmern sich Produktionsanlagen selbstständig um die Beschaffung von Verbrauchsmaterial und Rohstoffen. Erste Ansätze eines **Machine-to-Machine-Payments** befinden sich bereits in der Entwicklung.

Die Zahl an IT-Systemen und Bausteinen wächst. Im Jahr 2019 waren bereits 27 Mrd. vernetzte Geräte im Einsatz, bis zum Jahr **2025 soll die Zahl auf 75 Mrd.** IoT-Devices wachsen.[1]

Vernetzte Geräte im Jahr 2019

27 Mrd.



Parallel zu dieser Entwicklung hat ein **Umdenken bei Design und Entwicklung von IT-Systemen** eingesetzt. Mikroservices lösen verstärkt monolithische Architekturen ab und kommunizieren via API miteinander. Dieser Ansatz stärkt agile Methoden, reduziert Kosten und vereinfacht die Weiterentwicklung von Systemen.

Beispiele dafür sind:

- **Kernfunktionen** können in anderen Services und Anwendungen einfacher genutzt werden: Eine Warenkorb-Funktionalität benötigt nicht nur der Webshop, sondern auch eine mobile App.
- Die **Validierung von Benutzer:inneneingaben** kann durch die Einbindung eines externen Mikroservice schnell umgesetzt werden.

MCS _ INFO

Eines der wichtigsten Bindeglieder im Zusammenspiel von API und Mikroservices ist die Cloud.

Drei von vier Unternehmen ab 20 Mitarbeiter:innen setzen inzwischen auf Cloud-Computing.[2]
Jedes dritte Unternehmen (32 Prozent) betrieb bereits Multi-Cloud-Computing.[3]

IT-Monitoring steigert **Resilienz** eines jeden Unternehmens

Die **wachsende Vernetzung und die fortlaufende Optimierung** von Prozessen schaffen Abhängigkeiten, in denen die Zeit ein kritischer Faktor wird. Je nach Branche kann ein Ausfall einer Kernkomponente bereits nach wenigen Stunden eine geschäftskritische Bedrohung sein. So bedeutet eine Fehlfunktion in einem Webshop für Retailer, die stark auf das Onlinegeschäft setzen, empfindliche Umsatzeinbußen. Dazu kommt auch noch der nicht direkt messbare Verlust der Reputation bei Kunden.

Bedrohungen für den Geschäftsbetrieb erwachsen auch noch aus einer anderen Richtung, denn die **Gefahr durch Kriminelle** nimmt ständig zu.[4] Potenziell kann jedes Unternehmen Opfer von Attacken aus dem Netz werden: direkt und indirekt. Denn selbst wenn die Firma nicht das eigentliche Angriffsziel ist, könnten die Angreifer:innen IT-Systeme (z. B. IoT-Devices) gekapert haben, um sie im Verbund mit anderen unter Kontrolle gebrachten Systemen zu einem konzertierten Angriff in Form einer DDoS-Attacke zu verwenden.

Eine Herausforderung, die sich aus der verstärkten Nutzung von kleinteiligen Architekturen ergibt, liegt in der **frühzeitigen Erkennung von Fehlfunktionen** oder sich schleichend entwickelnden Problemen. Ein System wirkt vordergründig funktionsfähig, doch im Hintergrund ist ein wichtiger Prozess zum Stillstand gekommen. Auch Angriffe durch Kriminelle kündigen sich häufig durch langsam wachsende Leistungseinbußen eines Systems an.

Zur **Steigerung der Resilienz** der IT eines Unternehmens ist die Überwachung wenigstens aller geschäftskritischen IT-Prozesse unbedingt notwendig. Ein aktives Business-Continuity-Management braucht Systeme, die frühzeitig auf mögliche Probleme hinweisen und beim Eintritt eines Risikos rechtzeitig und kurzfristig warnen.

[1] https://blog.wiwo.de/look-at-it/2019/09/09/internet-of-things-knapp-27-milliarden-vernetzte-geraete-oder-3-iot-gadgets-je-mensch/

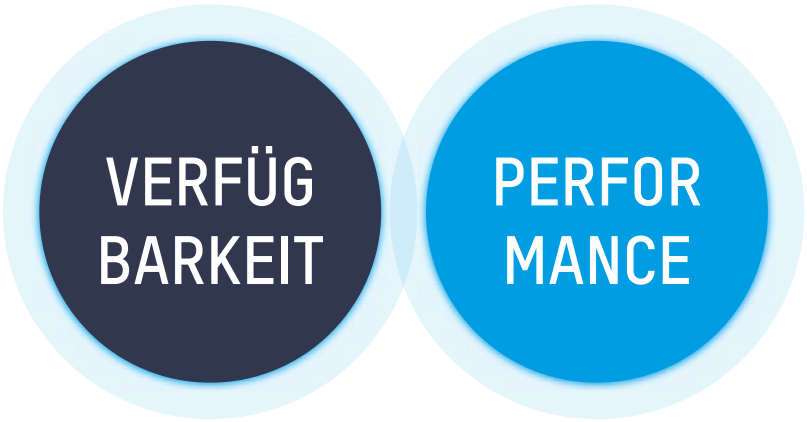
[2] https://home.kpmg/de/de/home/themen/uebersicht/cloud-computing.html

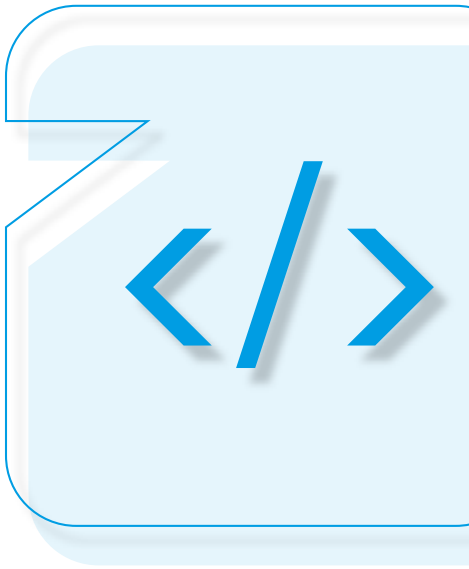
[3] https://www.bitkom.org/Presse/Presseinformation/Drei-von-vier-Unternehmen-nutzen-Cloud-Computing

[4] https://www.tagesspiegel.de/wirtschaft/ddos-angriffe-zahl-der-hacker-attacken-nimmt-waehrend-coronakrise-zu/25742728.html

WO **MONITORING** ANSETZT

Im Fokus der Überwachung von IT-Systemen geht es um zwei wesentliche Gesichtspunkte:





Zu den **grundlegenden Aufgaben** einer Lösung für das Monitoring gehört die Überprüfung, ob ein System, eine Komponente oder Prozesse (Applikationen, Dienste, Mikroservices) laufen, also überhaupt verfügbar sind. Kommt es zu einem (temporären) Ausfall, schlägt das System Alarm. Damit besteht die Chance, möglichst frühzeitig einzugreifen und Abhilfe zu schaffen. Die Palette potenzieller Störungen reicht von Hardwaredefekten (beispielsweise Ausfall eines Datenspeichers, Disk-Controllers, Netzwerkkarten usw.) bis zu Softwarestörungen (Stillstand eines Server-Dienstes, Ausfall der Erreichbarkeit einer API, Konnektivitätsausfälle).

Die zweite Kernaufgabe liegt in der **Überwachung der Leistung und anderer (vitaler) Parameter**. Hier kommt es also nicht darauf an, ob Systeme oder Komponenten überhaupt funktionieren, sondern unter welchen Voraussetzungen dies geschieht. Eine ständig über einem kritischen Wert liegende Temperatur kann einen sich entwickelnden Lüfterschaden andeuten, der zu einem großen Problem werden kann. Die wachsende Antwortzeit eines Datenbankservers deutet unter Umständen auf Probleme mit der Datenintegrität hin. Die Zunahme des Netzwerkverkehrs außerhalb sonstiger Erfahrungswerte könnte auf eine beginnende Attacke verweisen.

Die in Unternehmen erwähnte **Aufspaltung der IT-Landschaft in zusätzliche Systeme** und Prozesse führt in der Praxis trotz des Einsatzes von Überwachungssystemen immer wieder zu Unterbrechungen und Ausfällen wichtiger Prozesse. Schuld daran sind oft Lücken in der Überwachung, die wichtige Komponenten oder Ressourcen nicht einbezogen haben. Auf diesem Wege können eigentlich kleinere Störungen zu großen Problemen heranwachsen.

System-Monitoring ist indes nicht nur bei der Steigerung der Resilienz der IT-Systeme nützlich. Die gewonnenen Informationen können auch zur Kostensenkung beitragen. So ist es beispielsweise sinnvoll, die Auslastung von virtuellen Servern, die bei den großen Hyperscalern gebucht wurden, zu überwachen. Zeigen die gewonnenen Informationen etwa, dass selbst zu Spitzenzeiten die Auslastung von CPU oder Speicher regelmäßig unter 50 Prozent liegt, kann somit problemlos auf eine geringere Ausstattung und damit einen günstigeren Tarif gewechselt werden.

Umgekehrt kann die langfristige Auswertung der Auslastung und Antwortzeiten aufzeigen, dass gebuchte oder installierte Ressourcen an ihre Leistungsgrenze stoßen. **Damit trägt Monitoring auch direkt zur Skalierung des eigenen Geschäftsmodells bei,** da rechtzeitig weitere Ressourcen aufgebaut werden können, bevor Kund:innen oder Partner:innen beeinträchtigt werden.

Mit **Checkmk 2.0** alles im Blick

Checkmk 2.0 ist so vielseitig, dass tatsächlich ein umfassendes Monitoring aller wichtigen Ressourcen möglich ist.

Der Lösung gelingt es, die unterschiedlichen Datenquellen und Herausforderungen bei der (Server-) Überwachung unter einer Oberfläche zu bewältigen:

- Hardwareproduzenten stellen in der Regel **eigene Monitoring-Tools** für ihre Server zur Verfügung. Mit Checkmk werden die darüber ermittelten Werte abgerufen.
- Checkmk **kann jeden Linux-Server überwachen**, unabhängig davon, ob er mit Red Hat Enterprise Linux, Fedora, CentOS, openSUSE, SLES, Debian oder Ubuntu läuft.
- Bei der Überwachung von Windows-Servern setzt Checkmk nicht auf "Windows Management Instrumentation" (WMI) von Microsoft, sondern liefert einen **eigenen Agenten in Form eines MSI-Pakets.** Die einfach ausführbare Datei verzichtet auf DLL-Abhängigkeiten, was zur Stabilität der Überwachung beiträgt.
- Checkmk kümmert sich bei Bedarf um die **Aktualisierung der Agenten**, der Plugins und deren zentraler Konfiguration.
- Die Plattformen für virtuelle Server (z.B. VMware vSphere, Citrix XenServer oder Microsoft Hyper-V) umfassen ebenfalls eigene Tools, die Informationen zu den virtuellen Maschinen liefern. Checkmk greift auf diese Daten **über entsprechende Schnittstellen** zu.
- Checkmk **erkennt Container** und kann unmittelbar nach deren Erstellung zur Überwachung genutzt werden, eignet sich somit auch für innovative Dienste wie Docker oder Kubernetes.
- Da in vielen Unternehmen der Einsatz von **Multi-Cloud-Diensten** an Bedeutung gewinnt, ist Checkmk in seiner aktuellen Version auch in der Lage, AWS-Services wie Glacier, DynamoDB, ELB, EC2 und RDS zu überwachen. Auch die Azure-Cloud wird unterstützt.
- **Bereits eingesetzte Lösungen** wie Grafana oder das Netzwerk-Performance-Monitoring-Werkzeug Ntop sind integrierbar.
- Checkmk bietet die **Inventarisierung** aller installierter Hard- und Software. Die Informationen werden nicht nur systematisch abgerufen, sondern können auch über individuelle Zeiträume abgeglichen werden. Damit lassen sich defekte oder veränderte Hardwarekomponenten leichter identifizieren. So können Veränderungen beim Datendurchsatz von Festplatten, die nicht durch mehr Last des Systems zu erklären sind, auf einen schleichenden Defekt hinweisen. Das Betriebssystem würde dagegen lediglich erkennen, dass die Platten vorhanden sind und arbeiten. Mit Checkmk werden dagegen **Anomalien leichter entdeckt.**
- Für die **Überwachung von Datenbanken** (bzw. Datenbankservern) gibt es zahlreiche Plugins, die das Monitoring von MySQL/MariaDB, MS SQL, PostgreSQL, Oracle, MongoDB, IBM DB2, SAP HANA oder Microsoft Azure SQL erlauben.
- Ein **anpassbares Reporting** liefert aussagekräftige Informationen für das Management in ansprechenden PDFs.

Um die **schnelle Reaktion auf Probleme und Anomalien** zur ermöglichen, laufen alle Informationen in zentralen Dashboards zusammen, die individuell an die eigenen Bedürfnisse angepasst werden können.

// Checkmk ist eine zuverlässige, benutzerfreundliche Plattform, die wir **aus Überzeugung** einsetzen. //

Michael Rademacher _ Ihr MCS-Experte

Unsere Expert:innen holen **für Sie alles aus Checkmk** heraus

Checkmk ist eine vielseitige und leistungsstarke Lösung für alle Monitoring-Aufgaben in Ihrer IT:

ob physische oder virtuelle Server, Konnektivität, Datenbanken oder (Multi-) Cloud. Dank seiner Plugin-Architektur gibt es (kaum) einen Aspekt, der sich nicht überwachen lässt. Und Checkmk kann mit bereits vorhandenen Monitoring-Tools verbunden werden.

Damit es keine Lücken und unliebsame Überraschungen in den Überwachungsprozessen Ihrer Systeme gibt, ist es ratsam, die Implementierung, das Testen und die Wartung von Checkmk in die Hände erfahrener Expert:innen zu übergeben.

Als **langjähriger Partner von Checkmk** bieten wir Ihnen alle Leistungen rund um Checkmk, damit Sie sich auf Ihr Kerngeschäft konzentrieren können. Um die komplexe, aber äußerst wichtige Aufgabe der Einrichtung des (Server-) Monitorings kümmert sich MCS!

Wir **bieten** Ihnen:

- Analyse des Überwachungsbedarfs
- Entwicklung einer lückenlosen Monitoring-Strategie
- Aufsetzen und Einrichtung von Checkmk inklusive der notwendigen Plugins
- Anbindung von Checkmk an Ihre bereits vorhandenen Monitoring-Tools
- Pflege und Wartung des Systems
- Die regelmäßige Anpassung an die Veränderungen in Ihrer Systemlandschaft, damit die Überwachung auch lückenlos bleibt

Damit bei Ihnen **auch in Zukunft** alles läuft

Sie wollen nicht nur darauf vertrauen, sondern wissen, dass alles in Ihrer IT rund läuft? Dann ist Checkmk die ideale Lösung dafür.

Als offizieller Partner von Checkmk sind wir für Sie da – heute und in der Zukunft!

Sie möchten die **Vorteile von Checkmk** kennenlernen und erfahren, wie das Monitoring Ihnen dabei hilft, Ihre Businessziele zu erreichen? **Dann freuen wir uns auf Ihre Anfrage.**

Michael Rademacher _ Ihre IT Zukunft

Essener Bogen 23
22419 Hamburg

T +49 40 53773-162
Michael.Rademacher@mcs.de

www.mcs.de