IT-Monitoring

Wozu ist das gut?

Ob in der Cloud oder vor Ort, der kontinuierliche Blick in das Innenleben von IT-Services und -Infrastrukturen ist ein wesentlicher Bestandteil jedes gut funktionierenden IT-Systems.

Das Streben nach digitaler Transformation als zentralem strategischen Ziel für die meisten modernen Unternehmen hat dazu geführt, dass es ein entscheidender Teil jeder IT-Strategie sein muss, sicherzustellen, dass die IT-Systeme eines Unternehmens gut funktionieren, sicher sind und ein gutes Preis-Leistungs-Verhältnis bieten. Unabhängig der Unternehmensgröße.

Die Überwachung des IT-Status und der IT-Leistung ist entscheidend für:

- Kundenzufriedenheit
- Einhaltung von Gesetzen und Richtlinien (intern & extern)

Die jährliche Ausfallanalyse des Uptime Institute zeigt, dass zwei Drittel (67 %) aller Ausfälle Unternehmen mehr als 100.000 US-Dollar kosten.

Die Erkenntnis?

Die Fähigkeit, Systemanomalien schnell zu erkennen und zu beheben, ist eine Fähigkeit, die Sie benötigen.

Zur Erlangung der grundsätzlichen Fähigkeiten zur Systemüberwachung schauen wir uns in den nächsten Stunden an

- Was überwacht wird
- Den Prozess der Überwachung
- Zukünftige Trends

Was ist IT-Systemüberwachung grundsätzlich?

Einfach ausgedrückt bezieht sich der Begriff "IT-Überwachung" auf alle Prozesse und Tools, mit denen Sie feststellen, ob die IT-Geräte und digitalen Dienste Ihres Unternehmens ordnungsgemäß funktionieren. Die Überwachung hilft, Probleme zu erkennen und zu beheben – alle Arten von Problemen.

Heutzutage ist die Überwachung kompliziert. Das liegt daran, dass unsere Systeme und unsere Architektur kompliziert sind – die IT-Systeme, die wir verwenden, sind verteilt. (Genauso wie die Menschen, mit denen wir arbeiten, es auch sind.)

Schauen wir uns ein paar offizielle Definitionen an.

Hartenfelser IT Consulting
Gartenweg 19
2444 Seibersdorf

+43 2255 62080
office@hit-consulting.at

Das SRE-Buch von Google definiert Monitoring als "Sammeln, Verarbeiten, Aggregieren und Anzeigen quantitativer Echtzeitdaten über Ihr System". Diese Daten können die Anzahl und Typen von Abfragen, die Anzahl und Typen von Fehlern, die Verarbeitungszeiten und die Lebensdauer des Servers umfassen.

In *ITIL® 4* fallen Informationen über den Dienststatus und die Leistung unter die Praxis "Überwachung und Ereignisverwaltung". Sie definieren Monitoring als eine Funktion, die es Unternehmen ermöglicht:

- Angemessene Reaktionen auf vergangene Ereignisse
- Planung und Umsetzung proaktiver Maßnahmen, um zukünftige unerwünschte Ereignisse zu verhindern

Die Überwachung ist eng mit vielen der IT-Service-Management-Praktiken (ITSM) verknüpft, darunter Incident Management, Problemmanagement, Verfügbarkeitsmanagement, Kapazitäts- und Performance-Management, Informationssicherheitsmanagement, Service-Continuity-Management, Konfigurationsmanagement, Deployment-Management und Change Enablement.

Monitoring kann verschiedene Stoßrichtungen haben. Obwohl es in diesem Block um die Überwachung von IT-Systemen im Großen und Ganzen geht, können wir auch einige spezifischere Untergruppen der Überwachung kategorisieren, wie zum Beispiel:

- **Infrastruktur Monitoring**

  Uptime, Verfügbarkeit, Auslastung, Performance, Sicherheit
- **Netzwerk Monitoring**

  Performance, Verfügbarkeit, Konfiguration, Cloud (!)
- **Applikations Monitoring (APM)**

  Anzahl User Interaktionen, Ladezeiten, Transaktionswege
- **Multi-Cloud Monitoring**

  Verfügbarkeit, Sicherheit, Performance,
- **Daten Monitoring & Datenbank Monitoring**

  Fehleranzahl, Datenkonsistenz, Regulatorien & Gesetze, Verfügbarkeit
- **Synthetisches Monitoring & Real-User Monitoring (RUM)**

  Webseitenanalyse, Optimierungspotenziale, Protokolle
- **Security Monitoring**

  Zugriffe, Erkennung v. Bedrohungen, Datensammlung & Analyse

Hartenfelser IT Consulting
Gartenweg 19
2444 Seibersdorf

+43 2255 62080
office@hit-consulting.at

Was sollte in IT-Systemen überwacht werden?

Bei der Überwachung von IT-Systemen geht es darum, zwei grundlegende Fragen zu beantworten:

- Was passiert?
- Warum passiert es?

Um diese Fragen beantworten zu können, müssen kritische Elemente in ihren Systemen kontinuierlich auf Anomalien, Probleme oder Warnungen für Wartungsaktivitäten überwacht werden. Damit können sie sicherstellen, dass die Dienste funktionieren und gemäß den vereinbarten Leistungsstufen (Service Level Agreements) genutzt werden können.

Dazu dienen Metriken. Diese sind die Quellen von Rohmessdaten, die von Überwachungssystemen gesammelt, aggregiert und analysiert werden. IT-System Metriken erstrecken sich über mehrere Ebenen, darunter:

- Infrastrukturmetriken: Diese werden auf der Ebene von Host, Server, Netzwerk und Einrichtungen gemessen und umfassen unter anderem CPU, Speicherplatz, Stromversorgung und Schnittstellenstatus
- Anwendungsmetriken: Diese werden auf Softwareebene gemessen und umfassen unter anderem die Reaktionszeit, die Fehlerrate und die Ressourcennutzung
- Service-Level-Metriken: Hierbei handelt es sich gegebenenfalls um Infrastruktur-, Konnektivitäts-, Anwendungs- und Dienstebasierte Metriken

Die Überwachung auf der Grundlage von Low-Level-Infrastrukturmetriken wird als "Black-Box-Monitoring" bezeichnet. Dies ist in der Regel Systemadministratoren und DevOps-Ingenieuren vorbehalten. Auf Anwendungsebene gilt der Begriff "White-Box-Überwachung" und ist in der Regel die Arbeit von Entwicklern und Anwendungssupporttechnikern.

- Black Box Monitoring
    - Konzentriert sich auf rein auf Systeminputs und -outputs. Typische Merkmale sind der Fokus auf Ergebnisse, Einfache Anwendung, Nutzerperspektive
    - Wird verwendet bei Softwaretests, Netzwerküberwachung, Performance-Monitoring
    - Vorteile sind die Einfachheit, Flexibilität und der benutzerzentrierte Ansatz
    - Nachteile sind die begrenzte Einsicht und fehlende Diagnosemöglichkeiten
- White Box Monitoring
    - Bezieht den Aufbau, die Abläufe und Implementierungsdetails von Systemen mit ein und berücksichtigt Funktionsweisen auf Maschinenebene
    - Wird für detaillierte Analysen in der Softwareentwicklung oder auch für tiefergehende Performanceüberwachung eingesetzt. Unterstützt Fehlerdiagnosen

Hartenfelser IT Consulting
Gartenweg 19
2444 Seibersdorf

+43 2255 62080
office@hit-consulting.at

- Vorteile sind tiefgehende Einsichten, effiziente Fehlerbehebung, Aufzeigen von Optimierungsmöglichkeiten
- Nachteile sind die teilweise hohe Komplexität und aufwändige Implementierung sowie Code-Abhängigkeit durch Änderungsauswirkungen

Hartenfelser IT Consulting
Gartenweg 19
2444 Seibersdorf

+43 2255 62080
office@hit-consulting.at

Metriken zur Überwachung von IT-Systemen stammen in der Regel aus nativen Überwachungsfunktionen, die in den zu beobachtenden IT-Komponenten zumeist standardmäßig implementiert sind.

Darüber hinaus verwenden einige IT-Überwachungssysteme die Verwendung von benutzerdefinierten Instrumenten (z. B. schlanke Software-Agenten), mit denen erweiterte Service-Level-Metriken extrahiert werden können.

„Vier goldene Signale“

Laut Google gibt es vier goldene Signale, die bei der Überwachung von IT-Systemen im Mittelpunkt stehen sollten:

- **Latenz**

  Die Zeit, die benötigt wird, um eine Anfrage zu bearbeiten, d. h. die Round-Trip-Zeit in der Regel in Millisekunden. Je höher die Latenz, desto schlechter das Serviceniveau – Benutzer beschweren sich über Langsamkeit und mangelnde Reaktionsfähigkeit.
- **Verkehr**

  Ein Maß dafür, wie viel Bedarf auf Ihr System ausgeübt wird, d. h. die bearbeiteten Anfragen oder die Anzahl der Sitzungen innerhalb eines Zeitraums, die die konfigurierte Kapazität beanspruchen. Mit zunehmendem Datenverkehr steigt auch die Belastung der IT-Systeme und das Potenzial, das Kundenerlebnis zu beeinträchtigen.
- **Irrtümer**

  Die Rate der Anforderungen, die entweder explizit, implizit oder nach Richtlinie fehlschlagen. Fehler weisen auf Konfigurationsprobleme oder Fehler von Elementen innerhalb des Dienstmodells hin.
- **Auslastung**

  Ein Maß für den Systemanteil, das die Ressourcen hervorhebt, die am stärksten eingeschränkt sind, d. h. wie "voll" der Service ist. Das Überschreiten der festgelegten Auslastungsstufen würde wahrscheinlich zu Leistungsproblemen führen.

Hartenfelser IT Consulting
Gartenweg 19
2444 Seibersdorf

+43 2255 62080
office@hit-consulting.at

Best Practices für Alarmmüdigkeit

Wenn Systemadministratoren Überwachungssysteme einrichten, um Daten zu erfassen, laufen sie Gefahr, von Folgendem überwältigt zu werden:

- Die Anzahl der ausgelösten Warnungen
- Die Komplexität bei der Verknüpfung von Warnungen, Fehlern und Protokollen

Es empfiehlt sich, einfache, vorhersehbare und zuverlässige Regeln aufzustellen, die in den meisten Fällen echte Probleme aufdecken.

Darüber hinaus sollten die Ergebnisse von Monitoring-Maßnahmen regelmäßig überprüft, und die Schwellenwerteinstellungen (Information, Warnung, Fehler) sowie die effektive Konfiguration automatisierter Hintergrundtasks angepasst werden.

Tätigkeiten im Bereich IT-Systemüberwachung

Werfen wir nun einen Blick auf die sechs Hauptaktivitäten bei der Überwachung von IT-Systemen:

1. Phase - Planung

Bei der Auswahl eines zu überwachenden IT-Systems müssen Sie mehrere Planungsaktivitäten durchführen. Die wichtigsten sind

- Definieren der Priorität
- Auswählen der zu überwachenden Funktionen
- Festlegen von Metriken und Schwellenwerten für die Ereignisklassifizierung
- Definieren eines Dienstintegritätsmodells (End-to-End-Ereignisse)
- Definieren von Ereigniskorrelationen und Regelsätzen
- Zuordnen von Ereignissen zu den zuständigen Aktionsplänen und Teams.
- Auswahl der Kommunikationskanäle

Zu den wichtigsten Ergebnissen der Planung gehören

- Ein Monitoring Plan für jedes IT-System
- Ein Dienstintegritätsmodell
- Definierte Arten von Ereignissen
- Kriterien für die Ereigniserkennung
- Priorität und Reaktion auf die Ereignisse
- Eine Verantwortungsmatrix für das Operations-Team

Hartenfelser IT Consulting
Gartenweg 19
2444 Seibersdorf

+43 2255 62080
office@hit-consulting.at

2. Phase - Erkennung und Protokollierung

Dies ist die erste Phase der Ereignisbehandlung. Hier werden die Warnungen der IT-Systeme erkannt, wenn die festgelegten Schwellenwerte und Kriterien überschritten werden.

Warnungen werden von einem IT-Überwachungssystem erfasst, wo sie angezeigt, aggregiert und analysiert werden können.

3. Phase - Filterung und Korrelation

Basierend auf den festgelegten Regeln filtert das Überwachungssystem die empfangenen Meldungen und setzt sie gegebenenfalls in Verbindung (Korrelation) zu anderen Systemkomponenten. Die Filterung kann auf folgenden Kriterien basieren:

- Quelle
- Zeitpunkt des Auftretens
- Level (Kritikalität)

Bei der Korrelationsprüfung werden Muster und andere Warnungen überprüft, um Anomalie Quellen und potenzielle Auswirkungen zu ermitteln.

4. Phase – Klassifizierung

In dieser Phase wird das Ereignis nach festgelegten Kriterien (z. B. Typ und Priorität) gruppiert, um die richtige Antwort zu erhalten. Zum Beispiel würden Warnungen im Zusammenhang mit Eindringlingen oder Ransomware als Sicherheitsereignisse klassifiziert – und dies informiert ein SOC-Team, um darauf zu reagieren.

5. Phase – Ereignis Behandlung

Basierend auf dem zuvor definierten Aktionsplan und der Verantwortungsmatrix wird das entsprechende Team per E-Mail, SMS, Online-Kollaborationssystemen oder anderen vereinbarten Kanälen kontaktiert.

In einigen IT-Umgebungen kann die Ereignisreaktion automatisiert werden, was bedeutet, dass Maßnahmen unabhängig von menschlichen Eingriffen ergriffen werden, wie z. B. das Neustarten von Instanzen oder das Failover des Datenverkehrs.

6. Phase – Beurteilung/Planung

Basierend auf dem Umgang mit Ereignissen und den daraus resultierenden Auswirkungen auf die Qualität der IT-Systeme sollte eine regelmäßige Überprüfung der Monitoring-Planung erfolgen, um sicherzustellen, dass die gesetzten Metriken und Schwellenwerte weiterhin Ihren Anforderungen entsprechen. Im Zuge dieser Überprüfung sollten auch:

- Meldungskommunikation, Antwortverfahren und Zuständigkeiten aktualisiert werden
- Die Leistung von Metriken die mit dem Monitoring verknüpft sind, z. B. die Qualität der Daten und fehlgeschlagene Erkennungen, die zu Dienstausfällen führen überprüft werden

Hartenfelser IT Consulting
Gartenweg 19
2444 Seibersdorf

+43 2255 62080
office@hit-consulting.at

Zukunftstrends der IT-Systemüberwachung

Da IT-Systeme immer komplexer werden, müssen Unternehmen in Tools zur Überwachung von IT-Systemen investieren, die die erforderlichen Funktionen bieten, um mit der technologischen Entwicklung und dem Umfang der vorgenommenen Änderungen Schritt zu halten.

Eine Umfrage von 451 Research ergab, dass 39 % der Befragten in 11 bis 30 Überwachungstools für ihre Anwendungen, Infrastruktur und Cloud-Umgebungen investiert haben – wow! Diese Tool-Ausbreitung führt schnell zu Folgendem:

- Ineffizienzen
- Geldverschwendung
- Verpasste Chancen

Tools, die sich über die gesamte Technologielandschaft erstrecken und Ereignisse über unzählige Systeme und Umgebungen hinweg konsolidieren können, werden für Unternehmen, die ein gutes Preis-Leistungs-Verhältnis suchen, unweigerlich attraktiver sein.

In der Zusammenarbeit mit Kunden in den letzten Jahren und bei der jährlichen Forschung zeichnen sich zwei Haupttrends ab.

Auswirkungen von ML und KI

Der Einfluss von KI/ML auf die Überwachung von IT-Systemen wird weiter zunehmen, insbesondere angesichts der zunehmenden Leistungsfähigkeit großer Sprachmodelle (LLMs). Moderne Tools, die KI integriert haben, können nun den gesamten Prozesslebenszyklus von der Erkennung bis zur Reaktion abdecken, insbesondere bei der Analyse großer Ereignisdatenmengen sowie bei der Handhabung mühsamer Aktivitäten wie Ereigniskorrelation und Protokollanalyse in verteilten Systemen.

Mit entsprechender Schulung sind diese Tools perfekt geeignet, um Alarm-"Rauschen" und "Falsch Positives/Negatives" schneller und effektiver als jedes menschliche Team zu sortieren. Dies bedeutet jedoch nicht, dass Personen vollständig von der Überwachung der IT-Systeme ausgeschlossen werden müssen – stattdessen wird sich ihr Fokus auf die Entwicklung besserer Orchestrierungs- und Automatisierungstools verlagern, um auf Warnungen zu reagieren und diese zu beheben.

Einheitliche Beobachtbarkeit (observability)

Der andere Trend, der sich auf die Überwachung von IT-Systemen auswirkt, ist das Aufkommen der einheitlichen Beobachtbarkeit. Das Aufkommen von Plattformen, die durch die Analyse von Protokollen, Metriken und Traces eine zentrale Ansicht über Infrastruktur, Anwendungen und Benutzererfahrung bieten, bedeutet, dass Ihnen eine wertvolle Lupe zur Verfügung steht: eine gründlichere Analyse von Warnmeldungen, um die genauen Probleme zu ermitteln, mit denen Benutzer in komplexen Umgebungen konfrontiert sind.

Hartenfelser IT Consulting
Gartenweg 19
2444 Seibersdorf

+43 2255 62080
office@hit-consulting.at

Überwachen Sie den Zustand Ihres Unternehmens

Für Unternehmen jeder Größe ist die Überwachung von IT-Systemen ein wichtiger Weg, um die Funktionalität, Leistung und Sicherheit ihrer IT-Services zu gewährleisten. Der Bereich der IT-Systemüberwachung wird sich weiterentwickeln, um neuen Herausforderungen gerecht zu werden und mehr Vorteile zu bieten, solange die Technologie weiter wächst.

Die Bedeutung der kontinuierlichen Verbesserung kann nicht hoch genug eingeschätzt werden. Unternehmen können nur dann garantieren, dass ihre Dienste einen Mehrwert bieten, wenn sie einen proaktiven, datengesteuerten Ansatz für die Überwachung von IT-Systemen verfolgen.

Training:

Windows Client	https://learn.microsoft.com/de-de/training/modules/monitor-troubleshoot-windows-client-performance/
Windows Server	https://learn.microsoft.com/de-de/training/modules/monitor-windows-server-performance/
Azure	https://learn.microsoft.com/de-de/training/modules/configure-alerts-responses/