business.technology.strategy

23. Oktober 2020
€ 12,00
10
20

funkschau

CLOUD Der Dynamik gewachsen sein

CRM Mindset und Technik für 360°-Kommunikation

NETZE FMC im Wandel

DATACENTER SPEZIAL

INFRASTRUKTUR IM BLICK BEHALTEN

Bild: Gorodenkoff / Adobe Stock

Viele IT-Abteilungen haben ihre Rechenzentren nicht so gut im Auge wie sie es gerne hätten. Ihnen fehlt oftmals die Möglichkeit, Gefahren früh genug zu erkennen und schnell zu reagieren. Eine Lösung dafür bieten gesamtheitliche Monitoring-Tools, die das System als Ganzes überwachen. In Kombination mit Drittwartung kann eine Entlastung der IT-Abteilung entstehen.

Autor: Klaus Stöckert ***Redaktion: Lukas Steiglechner***

➤ Das Rechenzentrum ist heute mehr denn je das digitale Gehirn eines Unternehmens. Dieses Kernstück der IT-Infrastruktur ist dafür verantwortlich, dass geschäftskritische Anwendungen funktionieren und relevante Daten jederzeit zur Verfügung stehen. Dabei entwickelt es sich im Zuge der fortscheitenden Digitalisierung ständig weiter, wächst, erhält neue Komponenten, neue Verbindungen und wird immer komplexer. Dennoch betreiben viele Unternehmen ihre Rechenzentren großteils im Blindflug.

Jedes Rechenzentrum ist technischen Gefahren ausgesetzt. Fehler in der Software, Schäden an der Hardware oder falsche Bedienung können einen kleinen Geräteausfall verursachen, der eine Kettenreaktion auslöst. Das kann bis zum teilweisen oder kompletten Ausfall des Rechenzentrums führen. Daten sind nicht mehr abrufbar, Aufträge nicht erfüllbar – ein geschäftsschädigendes Szenario. Ein Back-up-System kann hier zwar Hilfe leisten, jedoch ist die nötige Performance nicht gewährleistet. Denn: Software und Dienste stehen damit nur noch eingeschränkt zur Verfügung, wodurch Reputationsschäden entstehen. Weil die IT für jeden Geschäftsprozess ein elementarer Bestandteil ist, muss die interne IT-Abteilung stets alle Systeme am Laufen halten. Manche Abteilung hat sich zu einem Dienstleister oder dem One-Stop-Shop für Probleme mit digitalen Arbeitsmitteln gewandelt und arbeitet zwischen Rechenzentrum und Client an allen Fronten. Eine Überwachung der laufenden Systeme und vorausschauende Wartung fallen da schnell aufgrund von Überlastung unter den Tisch.

Prozesse holistisch optimieren

Die wenigsten Log-Dateien von Servern, Switches und Storage werden tatsächlich ausgewertet und überprüft. Seltener ist eine Monitoring-Software, die Probleme frühzeitig erkennt und meldet. So bemerken IT-Teams kritische Hardware-Zustände häufig zu spät, weshalb unerwartete Ausfälle entstehen können und die IT-Abteilung oft erst beim Problemfall reagiert. Die Wartung erfolgt also längere Zeit nachdem der Ausfall eingetreten ist, sei es durch die IT-Abteilung selbst oder über einen Servicevertrag mit dem entsprechenden Hersteller.

Dabei entscheidet das Service Level Agreement (SLA), wie schnell der Hersteller zur Fehlerbehebung anrückt. Allerdings müssen die Mitarbeiter zunächst identifizieren, welche Komponente von welchem Hersteller die Probleme verursacht. Bei komplexen Strukturen

EOL, EOD, EOSL – LEBENS(AB)LAUF VON IT-KOMPONENTEN

➤ IT-Geräte werden von Herstellern oftmals mit einem End of Life (EOL) versehen. Jedoch markiert dieses nicht das Ende der Funktionalität der Geräte, sondern vielmehr das Ende der Vermarktung, des Verkaufs und der Bereitstellung von Updates. Deswegen wird bei EOL auch oftmals von EOS gesprochen – End of Sale. Dieser Punkt wird durchschnittlich nach drei bis sechs Jahren erreicht, nachdem ein Produkt auf dem Markt erschienen ist. Nach sechs bis zwölf oder mehr Jahren setzt der nächste Schritt im Geräte-Support ein: Das End of Development (EOD) signalisiert den Zeitpunkt, wenn Anbieter die Entwicklung des Betriebssystems, und damit Software-Updates und Patches, einstellen. In derselben Zeitspanne setzt meist ebenfalls das End of Service Life (EOSL), auch End of Support Life genannt, ein. Damit beenden Hersteller Dienste und Updates beispielsweise für Server, Speicher und Netzwerkausrüstung. Der Support durch den Hersteller wird somit eingestellt und Unternehmen müssen entweder ihre Geräte durch neue ersetzen oder eine Third Party Maintenance einsetzen. *(LS)*

ist das alles andere als trivial. Hat die IT-Abteilung das Problem erkannt, muss sie sich mit dem Hersteller in Verbindung setzen, damit dieser den Service-Prozess startet. Unternehmen können aber an vier Punkten ansetzen, um Ausfallzeiten zu verhindern und zu verkürzen: Fehlererkennung, Fehleranalyse, Kommunikation und SLAs. Einen Ansatz, um die Fehlererkennung und -analyse zu optimieren, bietet dabei ein Monitoring-Tool. Eine vorrangige Herausforderung hierbei ist, dass das Tool die IT-Komponenten so gesammelt wie möglich überwacht. Die IT-Infrastruktur besteht dabei in der Regel aus Hardware verschiedener Hersteller, weshalb ein herstellerübergreifendes Monitoring-Tool hilfreich sein kann. Die IT-Abteilung erhält so die passende Übersicht, um das System als Gesamtkonstrukt zu überwachen. An einer solchen gesammelten Stelle sehen IT-Teams auch die Verfügbarkeit und den Durchsatz der Server. In kritischen Situationen werden ihnen auch die Fehler und die verantwortliche Komponente angezeigt. Das reduziert sowohl die Dauer als auch Mühe bei der Fehlererkennung und -suche.

Fehlerbehebung: Wettlauf gegen die Zeit

Wurde ein Fehler erkannt, kümmert sich entweder die IT-Abteilung selbst um das Problem oder sie kontaktiert den Hersteller der jeweili-

OEM VERSUS TPM-ANBIETER

➤ Bei der Frage nach dem passenden Wartungsservice haben sowohl der Support durch den Original Equipment Manufacturer (OEM) als auch der durch einen Third Party Maintenance (TPM)-Anbieter ihre jeweiligen Schwerpunkte. So bieten OEMs beispielsweise den Vorteil, dass die Hersteller ihre Produkte am besten kennen und somit die Geräte am effizientesten warten können. Das bedeutet jedoch gleichzeitig, dass sich jeder Hersteller nur um die eigenen Produkte kümmert. Bei einer Drittwartung können wiederum Produkte mehrerer Hersteller über einen zentralen Ansprechpartner abgedeckt werden.

Beim Vergleich von OEM und TPM stechen auch die unterschiedlichen Preisklassen heraus. So sind die Kosten bei OEM-Support in vielen Fällen höher als bei einer Drittwartung. Auch spielt das Geschäftsmodell der Hersteller eine Rolle. Denn: Diese geben ihren Geräten nur eine begrenzte Service-Lebensdauer, bis der Support eingestellt wird, nicht zuletzt, um auch den Verkauf von neuen Produkten zu fördern. Drittwartungsanbieter setzen stattdessen in vielen Fällen auf „lebensverlängernde" Maßnahmen für IT-Komponenten. Allerdings gibt Martin Epping, Business Director bei HPEs Service-Bereich Pointnext Services, zu bedenken: „Drittanbieter verwenden bei der Hardware-Wartung oft gebrauchte und nicht qualitätsgeprüfte Ersatzteile – erhöhte Ausfallraten dieser Komponenten können die Folge sein."

Aber nicht nur die Hardware, auch die Software spielt eine wichtige Rolle. So erklären die Analysten von Gartner, dass Aspekte wie Lizenzen und Updates als Teil der Wartung in der Regel den OEMs vorbehalten sind. Epping sagt hierzu: „Bei IT-Infrastruktur können Drittanbieter nur die Wartung der Hardware übernehmen, die Pflege und Aktualisierung der Systemsoftware kann in der Regel nur vom Hersteller kommen." Wer auf Drittanbieter-Support setzt, müsse also auf Weiterentwicklungen und Fehlerbehebungen in der Software gegebenenfalls verzichten.

Doch vor allem der Kostenaspekt kann für die Drittwartung sprechen. Laut Gartner sind hier Einsparungen von bis zu 70 Prozent im Vergleich zum Service der Hersteller möglich. Auch kann TPM die Möglichkeit bieten, Komplexität zu reduzieren und die Wartung auf einen Ansprechpartner zu konzentrieren. Von Vorteil kann darüber hinaus sein, wenn die Anbieter selbst Partner der Hersteller sind und auf zertifizierte Spezialisten zugreifen können. Uwe Wiest, Regional Sales Director DACH OEM Solutions EMEA bei Dell, kommentiert „Wir arbeiten im OEM-Bereich eng mit dem Channel zusammen. Unsere Partner entwickeln hier eigene Lösungen auf der Basis von Dell Technologies – da fließt viel Intellectual Property ein, teilweise entwickeln sie auch eigene Hardware-Designs." Unternehmen sollten also genau abwägen, auf welche Ressourcen sie selbst Zugriff haben, welche Aspekte entscheidend sind und welches Wartungsmodell sich somit für den individuellen Fall eignet. *(LS)*

gen Komponente. Dafür müssen die Verantwortlichen Kontakt mit dem Original Equipment Manufacturer (OEM), also dem Erstausrüster, aufnehmen. Zusätzlich müssen Wartungsverträge überprüft werden, um die Kapazitäten der Wartung abzuklären. Diese Schritte können Ausfallzeiten, die durch Fehler entstehen, gegebenenfalls verlängern. Kombinieren Rechenzentrumsbetreiber das Monitoring hingegen mit einem Third Party Maintanence (TPM)-Anbieter, also einer Drittwartung, gestaltet sich der Prozess anders. Erscheint eine Fehler- oder Warnmeldung beim Monitoring-Tool der IT-Abteilung des Unternehmens, kann diese, wenn gewünscht, parallel bei dem Dienstleister für die Drittwartung angezeigt werden. Dabei lässt sich der Wartungsprozess automatisieren, indem auch ein Ticket für die Problembehebung erstellt wird. Dienstleister und Unternehmen sprechen sich ab und so kann der Dienstleister die Wartung der Komponenten und die Fehlerbehebung gegebenenfalls unabhängig von der internen IT-Abteilung durchführen.

Anbieter von Drittwartung können IT-Teams beispielsweise unterstützen, wenn diesen die Kapazitäten fehlen, um Monitoring und Wartung ohne Pause zu gewährleisten. Vor allem bei einer heterogenen IT-Landschaft brauchen die Mitarbeiter tiefgreifendes Wissen zu den Geräten unterschiedlicher Hersteller. Multi-Vendor-Dienstleister sind in in der Lage, Geräte verschiedener Hersteller gesammelt zu überwachen und zu warten. Durch die gesammelte Wartung entsteht im Idealfall ein Single Point of Contact, eine zentrale Anlaufstelle, wenn Probleme auftreten.

Über die Grenzen des End of Service Life hinaus

Geräte, die ihr End of Service Life (EOSL) erreicht haben, erhalten von ihren Herstellern keine Updates und keinen Support mehr. Das stellt jedoch nicht die Funktionalität der Geräte in Frage. Rechenzentrumsbetreiber müssen nicht unbedingt neue IT-Komponenten anschaffen, denn: Geräte können auch ohne Performance-Verlust im Einsatz sein, nachdem der OEM-Support eingestellt wurde. Sobald das EOSL erreicht ist, kann aber beispielsweise auch ein Drittwartungsanbieter den Support übernehmen.

Neben länger andauernder Support-Dauer bieten viele Drittwartungsdienstleister darüber hinaus auch „refurbished" Hardware an: Gebrauchte Hardware, die wiederaufbereitet wurde. Sie verfügt oftmals über die gleiche Funktionalität wie Neuware. Dies kann besonders wichtig für Unternehmen sein, die in ihrer IT-Landschaft gegebenenfalls auf bestimmte ältere Hardware-Bausteine angewiesen sind.

IT-Umgebungen in Rechenzentren sind komplex. Sie bestehen aus Geräten unterschiedlicher Hersteller oder Komponenten mit überschrittenem EOSL. Rechenzentrumsbetreiber stehen vor der Herausforderung, diese komplexe Infrastruktur effizient zu überwachen und zu warten. Dabei müssen sie abwägen, ob sie Monitoring und Wartung selbst übernehmen, auf OEMs vertrauen oder sich in die Hände eines TPM-Dienstleisters begeben. Wie sich ein Unternehmen auch entscheidet, ist das Ziel doch klar: Prozesse vereinfachen, Ausfälle reduzieren, IT-Abteilungen entlasten.

Klaus Stöckert, CEO der TechnoGroup IT Service