Kreis Mainz-Bingen

IT ist doppelt geschützt

[19.08.2019] Da eine Cloud-Lösung zum Schutz der IT-Systeme nicht infrage kam, wappnet sich der Kreis Mainz-Bingen mit einem lokalen Metro-Cluster gegen Ausfälle durch Elementarschäden oder Computer-Sabotage. In Rheinland-Pfalz gehört die Verwaltung damit zu den Vorreitern.

Computer-Sabotage und IT-Ausfälle sind für Privatwirtschaft und staatliche Stellen keine abstrakte, sondern eine sehr reale und alltägliche Gefahr. Nach dem Stand der Technik sollte eine IT-Infrastruktur daher heute möglichst hochverfügbar, also ausfallsicher sein. Dabei bezieht der Begriff der Ausfallsicherheit oder des Failover IT-Systeme, Netzwerke, Speichersysteme, Dienste und Programme ein. Zwar versprechen auch viele Cloud-Anbieter und Betreiber von Rechenzentren eine Hochverfügbarkeit von bis zu 99,99 Prozent, dennoch beträgt die durchschnittliche Cloud-Ausfallzeit in Deutschland 20 Minuten pro Monat, was sich entsprechend negativ auf den Betrieb einer Behörde oder staatlichen Einrichtung auswirken kann.
Darauf weist ein Manager des IT-Anbieters Veritas Technologies auf dem Online-Portal Security-Insider hin. Denn Cloud-Provider würden nach dem Shared-Responsibility-Modell handeln, so der Autor in seinem am 28. Februar dieses Jahres veröffentlichten Gastbeitrag „Cloud-Ausfälle: Katastrophenalarm für Behörden“. „Das bedeutet: Je komplexer der Dienst, desto mehr Verantwortung hat der Dienstleister. Jedoch bleibt der Kunde immer für seine Daten und deren Compliance verantwortlich. Treten Datenlecks oder Ausfälle auf, liegt die Verantwortung nicht beim Cloud Provider“, warnt der Experte.

Cloud-Lösung kam nicht infrage

Für den rheinland-pfälzischen Kreis Mainz-Bingen kam eine Cloud-Lösung aus verschiedenen Gründen nicht infrage. „Neben dem Datenschutz sprachen auch die steigende Abhängigkeit von Netz-Providern und Cloud-Anbietern sowie fehlende Fallback-Szenarien gegen die Nutzung einer solchen Lösung“, erläutert Kai Ruland, Fachbereichsleiter Datenverarbeitung bei der Kreisverwaltung Mainz-Bingen. „Denn was ist, wenn die Verwaltung zu einem anderen Cloud-Anbieter wechseln wollte oder müsste oder aber gezwungen wäre, Dienste wieder selbst lokal zu betreiben? Auf diese wichtigen Fragen haben wir derzeit noch keine befriedigenden Antworten gefunden. Um IT-Anwendungen, die in einem Cloud-Rechenzentrum gehostet werden, möglichst ausfallsicher und schnell genug anbieten zu können, müsste man außerdem entsprechende Bandbreiten mieten, was die Abhängigkeit von Dienstleistern zusätzlich erhöht. Darum kommen für uns zurzeit Cloud-Dienste nur für solche Applikationen infrage, die nicht systemkritisch sind.“
Der Kreis hat sich zum Schutz seiner IT-Infrastruktur daher für den Aufbau und Betrieb eines so genannten Metro- oder Failover-Clusters entschieden und zählt damit in Rheinland-Pfalz zu den Vorreitern. Geliefert und installiert wurde die Lösung von Christian Ruppert IT-Consulting aus Ingelheim am Rhein, das vor allem für mittelständische Unternehmen und regionale staatliche Auftraggeber arbeitet. Insgesamt hatte der Auftrag ein Volumen von rund 340.000 Euro.

Metro-Cluster mit NetApp-Systemen

Das Metro-Cluster besteht aus eigenen, redundant ausgelegten Back-up- und Speichersystemen des US-amerikanischen Herstellers NetApp, die räumlich vom Standort der Verwaltung sowie deren Außenstellen getrennt sind. „Bei einer Störung schaltet das Metro-Cluster automatisch – ohne Eingreifen eines

Administrators – auf die redundant gespiegelten Anwendungen um“, beschreibt Ruland, was er als größten Vorteil der Lösung empfindet. „Sollte eine der beiden Seiten des Metro-Clusters irreparabel geschädigt werden, kommt es bei dieser synchronen Spiegelung zu keinem oder nur zu einem sehr geringen Datenverlust.“ Darüber hinaus sind weder für Hard- noch für Software Ausfallzeiten etwa aufgrund von Updates zu befürchten, und durch das automatische Takeover kann die Verfügbarkeit von IT-Diensten und -Anwendungen erheblich gesteigert werden.
Als Standort des lokalen Metro-Clusters wurde ein Raum im Gebäude der Polizeiinspektion Ingelheim ausgewählt, für den bereits eine Notstromversorgung vorhanden war. Das stellt die Nutzung der IT-Systeme auch bei längeren Stromausfällen sicher. Zudem befindet sich unter dem Dach der Polizeiinspektion auch das Katastrophenschutzzentrum des Landkreises Mainz-Bingen. Bei Großschadenslagen wie Rhein-Hochwasser, Chemieunfällen oder Bombenentschärfungen werden von hier aus Polizei, Feuerwehr und Hilfsorganisationen geleitet. Zum Anschluss des Metro-Clusters an das Landratsamt Mainz-Bingen wurden im Stadtgebiet rund 1,2 Kilometer Glaserfaserkabel verlegt. Die Strecke des Kabels führt auch an der künftigen Feuerwehrwache vorbei, wodurch technisch eine standortübergreifende Datensicherung möglich ist.

Zuverlässige Back-up-Strategie dennoch notwendig

„Auf dem Metro-Cluster am Standort Ingelheim sind zwar nicht sämtliche Daten der Kreisverwaltung gespeichert, jedoch wird der Löwenanteil unserer IT-Anwendungen mithilfe dieses Systems betrieben“, erklärt Kai Ruland. „In den Außenstellen – dem Gesundheitsamt Mainz sowie den beiden Kfz-Zulassungsstellen Bingen und Oppenheim – sind zudem Systeme von NetApp installiert, die mehrmals täglich via SnapMirror auf ein Back-up-System gesichert werden, das sich ebenfalls in den Räumen der Polizeiinspektion befindet.“ Auch die Daten des Metro-Clusters werden in regelmäßigen Intervallen auf das Back-up-System gespeichert – denn die Lösung schützt nur gegen physikalische Schäden durch beispielsweise Brand, Wasser oder Unfall. Werden Daten jedoch durch eine Schad-Software oder versehentlich manuell von einem Mitarbeiter auf dem System gelöscht, sind diese verloren. „Auch beim Betrieb eines Metro-Clusters kommt man daher nicht um eine zuverlässige Back-up-Strategie herum“, so der Fachbereichsleiter weiter.

Mitnutzung perspektivisch möglich

Um sicherzugehen, dass das Metro-Cluster keine unerwarteten Fehlerquellen birgt, hat die Kreisverwaltung gemeinsam mit IT-Consultant Christian Ruppert nach der Einrichtung einige Failover-Szenarien durchgespielt und getestet, so beispielsweise das Ausfall- und Umschaltverhalten bei der Stromversorgung und im Netzwerk. „Für den Aufbau und die Tests des Metro-Clusters haben wir vier Tage benötigt“, berichtet Kai Ruland. „Die Datenmigration von den alten NetApp-Storage-Systemen auf das Metro-Cluster im Gesamtumfang von circa 17 Terabyte war im laufenden Betrieb nach einem weiteren Tag abgeschlossen. Zur Überwachung des laufenden Betriebs nutzen wir neben den integrierten Funktionen des NetApp-Speichersystems als weiteres Tool PRTG Network Monitor.“
Perspektivisch könnten nach Angaben von Kai Ruland auch die Stadtverwaltung Ingelheim oder andere Verbandsgemeinden des Kreises Mainz-Bingen das Metro-Cluster mitnutzen. Diese Idee sei bislang jedoch nur angedacht und werde noch nicht ernsthaft weiterverfolgt: „Hierfür müssten zunächst sowohl personelle als auch technische Fragen geklärt werden – etwa, ob dafür die Netzanbindungen von einem Mietgebäude zum anderen ausreichen würden. Das wäre eine ganz wesentliche technische Voraussetzung für die gemeinsame Nutzung des Metro-Clusters.“

()

Dieser Beitrag ist in der Ausgabe August 2019 von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Kreis Mainz-Bingen, Metro-Cluster, NetApp, IT-Infrastruktur, Christian Ruppert IT-Consulting