Die „Polizei-Cloud“

Matthias Bongarth, Geschäftsführer des Landesbetriebes Daten und Information Rheinland-Pfalz und Dr. Torsten Neu, Mitarbeiter im CERT-rlp im Landesbetrieb Daten und Information Rheinland-Pfalz

Der in Mainz und Bad Ems ansässige Landesbetrieb Daten und Information (LDI) ist der zentrale IT-Dienstleister für die öffentliche Verwaltung des Landes Rheinland-Pfalz. In dieser Funktion betreibt der LDI eine Reihe von Fachverfahren für die rheinland-pfälzische Polizei. Um den Sparauflagen der Landesregierung gerecht zu werden und trotzdem die Leistung im Umfeld des Betriebs der polizeilichen Fachverfahren beizubehalten – ja, sogar zu verbessern -setzt der LDI konsequent auf Virtualisierung und Cloud-Computing. Eine wesentliche Rahmenbedingung dabei ist die Einhaltung der hohen Sicherheitsanforderungen im Polizeibereich. Die Umsetzung des Projektes „Polizei-Cloud“, einer Private-Cloud für die rheinland-pfälzische Polizei, wurde nun durch die Verleihung einer ISO 27001 Zertifizierung auf der Basis von IT-Grundschutz durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) belohnt.

Die Ausgangssituation

Dabei dürfen aber weder bei der Sicherheit noch bei der Verfügbarkeit der Systeme Abstriche gemachte werden. Weder Bürger noch Politiker hätten Verständnis für Misserfolge bei Einsatzlagen durch verlangsamten Informationsfluss wegen überlasteter Serversysteme oder Datenlecks, über die vertrauliche Informationen an die Öffentlichkeit gelangen.

Ein weiteres Problem bei auf physikalischer Hardware betriebenen Verfahren ist der Speicherplatz. Einige polizeiliche Verfahren benötigen nur vergleichsweise geringen Festplattenspeicher. Werden jedoch beispielsweise, wie bei Täterlichtbildsystemen, Fotos in Datenbanken gespeichert, kann sich der Speicherbedarf schnell erhöhen. Die stetig wachsende Dateigröße der Bilder durch permanent verbessertes Auflösungsvermögen moderner digitaler Kameras macht eine zukunftssichere Planung des Speicherbedarfs für ein Verfahren sehr schwer. Spätestens, wenn alle Festplatteneinschübe eines Servers gefüllt sind und die gespeicherten Daten langfristig vorgehalten werden sollen, muss eine alternative Lösung zur Datenspeicherung gefunden werden.

Das Projekt „Polizei-Cloud“

Cloud-Computing bietet die Möglichkeit auf einer Hardware mehrere virtuelle Server zu betreiben. Unter der Voraussetzung, dass auch zu Spitzenlast-Zeiten nicht alle Verfahren gleichzeitig unter Volllast laufen – so werden von einem Kollegen zu jeder Zeit nur ein und nicht tatsächlich zehn Verfahren wirklich gleichzeitig bedient werden –, können sich die virtuellen Server ohne Performance-Einbußen die Ressourcen der gemeinsamen Hardware teilen. Dies bedeutet, dass der Endanwender im Optimalfall keinen Unterschied zwischen einem auf virtueller oder auf physikalischer Hardware betriebenem Verfahren feststellen kann.

Das ambitionierte Projekt „Polizei-Cloud“ wurde Ende 2011 ins Leben gerufen. Zum damaligen Zeitpunkt wurden 30 Verfahren der rheinland-pfälzischen Polizei für das Projekt ausgewählt, die auf 339 (208 physikalische und 131 virtuelle), ausschließlich für die Polizei zur Verfügung gestellten, Servern betrieben wurden.

Das Thema „Hohe Sicherheit“ hatte im gesamten Projektverlauf durch die betroffenen Verfahren: Fahndungssysteme, Antiterrorsystem und Vorgangsbearbeitung der rheinland-pfälzischen Polizei hohe Priorität. Zur externen Überprüfung und Bestätigung des Sicherheitsstatus wurde schon in der Anfangsphase des Projekts die BSI-Zertifizierung der Cloud-Umgebung (entsprechend ISO 27001 auf Basis des BSI-Standards 100-2 (IT-Grundschutz)) angestrebt. Unter diesen Voraussetzungen war die Polizeiabteilung des Innenministeriums bereit den LDI mit der Umsetzung dieses innovativen Projektes zu beauftragen.

Ziel des Projektes war es die Zahl der Server deutlich zu reduzieren, Kosten zu sparen und gleichzeitig die Effektivität der Systeme zu erhöhen. Zur Umsetzung des Plans wurde von Anfang an auf eine konsequente und echte Virtualisierung durch eine optimierte und automatisierte Cloud-Umgebung gesetzt. Die Unternehmen Avanade und Microsoft haben gemeinsam mit dem LDI eine auf Microsoft Hyper-V R2 basierende Lösung konzeptioniert, die sämtliche Anforderungen des LDI und seiner Kunden abdeckt (technische Details: siehe Infokasten).

TECHNISCHE DETAILS DER „POLIZEI-CLOUD“ (STAND: NOVEMBER 2013)

- Als Basis der „Polizei-Cloud“ dient Microsoft Hyper-V R2 mit den System Center Produkten:
  - Virtual Machine Manager 2008 R2,
  - Virtual Machine Manager Self Service Portal 2.0
  - Operations Manager 2007 R2
  - Configuration Manager 2007 R3
  - Data Protection Manager 2010
  - Opalis (Prozessautomatisierung)
- Die Integration der System Center Monitoring- und Management-Lösung sorgt für eine optimale Auslastung der physischen Ressourcen. Die Cloud-Umgebung verfügt über eine integrierte Backup-Funktionalität, sowie Software- und Patchverteilungsmechanismen für die Host- und Gastsysteme.
- Eine maximale Skalierbarkeit der Cloud wird durch die modulare Architektur sowohl horizontal, durch mehrere Server, als auch vertikal durch das Hinzufügen von Ressourcen, wie zum Beispiel Prozessoren, Hauptspeicher und Storage über das Self-Service-Portal gewährleistet.
- Das Zusammenspiel von Opalis- und den System Center Produkten erlaubt eine Automatisierung von Betriebsprozessen mit geringem Aufwand. Bei der Aktualisierung der Host-Systeme beispielsweise im Rahmen des Patchmanagements können so die Gast-Systeme immer auf andere Hosts verschoben werden, um Ausfallzeiten zu vermeiden. Wartungen können also ohne Beeinträchtigung der Funktionalität im laufenden Betrieb vorgenommen werden, so die Anwendung dafür geeignet ist.

Nach einer dreimonatigen Design- und Implementierungsphase konnte die zentrale, hochverfügbare und hochsichere Plattform in Betrieb genommen werden. Die Cloud-Umgebung des LDI erfüllt alle Kriterien einer echten Cloud gemäß den Kriterien der BITKOM und bietet das Servicemodell „Platform as a Service“ (PaaS) als „Private Cloud“ nach NIST-Definition.

Positive Effekte für Umwelt und Finanzen

Bei der Migration der polizeilichen Fachverfahren in die „Polizei-Cloud“ wurde die Auslastung der Hardwareressourcen optimiert (siehe Infokasten Auslastung). Dabei wurden die Gast-Systeme auf möglichst wenigen physischen Hosts verteilt. So konnte die Gesamtzahl der Server (physisch und virtuell) um 34% reduziert und somit die Kosten für 115 Windowslizenzen gespart werden. Gleichzeitig wurde die durchschnittliche Auslastung der Serversysteme unter Normallast von etwa fünf auf 30 Prozent angehoben.

Durch Reduktion der physischen Server um 39% wurde der jährliche Stromverbrauch um ca. 547.000 kWh gesenkt und die CO2–Emission um 275 Tonnen p. a. reduziert – ein großer Schritt in Richtung „Green-IT“!

MEHRWERTE DER CLOUD

AUSLASTUNG DER IT-SYSTEME DEUTLICH VERBESSERT

Durch Integration polizeilicher Verfahren in die „Polizei-Cloud“ konnten Ressourcen optimal verteilt werden. So liegt beispielsweise die CPU-Auslastung einiger Verfahren nun bei etwa 30%, während der Betrieb der Verfahren auf rein physikalischer Hardware, wegen eingeplanter Sicherheitsreserven, teilweise bei unter 5% lag.

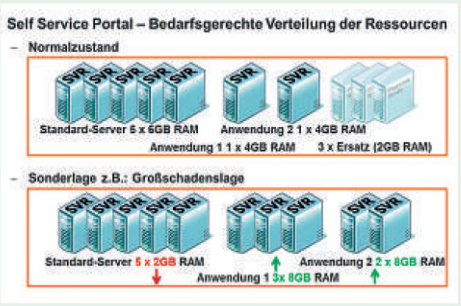
Durch die einfachere Verwaltung, die Automatisierung von Prozessen und geringere Lizenzgebühren konnte eine erhebliche Kosteneinsparung erzielt werden. Addiert man nur die gesparten Kosten für Betriebssystem-Lizenzen, Hardware, Strom und Personal, kommt man auf die beachtliche Summe von 215T€ Einsparungen bereits im ersten Jahr. Diese Kosteneinsparung wurde direkt an die Polizei weitergegeben. Ein derartiger Betrag ist bei der angespannten Finanzlage der Länder und dem daraus resultierenden Kostendruck ein Faktor, der richtungsweisend für die Weiterführung der Virtualisierungsbestrebungen des Landes Rheinland-Pfalz ist.

Taktische Vorteile

Die Einsparungen, die durch die „Polizei-Cloud“ erreicht werden konnten, sind nur eine Seite der Medaille. Es muss natürlich auch der praktische Nutzen, also die Brauchbarkeit der Systeme, im reellen Einsatz betrachtet werden. Auch hier bietet die „Polizei-Cloud“ taktische Vorteile. Im Normalbetrieb muss nicht für jedes der 30 bisher in der Cloud betriebenen Verfahren eine überdimensionierte Reserve vorgehalten werden. Durch „Resource Pooling“ werden die notwendigen Ressourcen wie Rechenzeit, Haupt- oder Festplattenspeicher in physischer oder virtueller Form zentral vorgehalten (siehe Infokasten: Taktische Vorteile). Die Ressourcen werden bei Bedarf dynamisch zugewiesen bzw. wieder freigegeben, sind also nicht an eine Anwendung gebunden („Rapid Elasticity“). Ein intelligentes Managementsystem optimiert die Ressourcenzuweisung und erstellt Serviceberichte („Measured Service“) für die Polizei. Diese Proaktive Überwachung führt letztendlich zu einer Erhöhung der Verfügbarkeit der polizeilichen Fachverfahren.

Im Falle einer Großschadenslage kann der Polizeiführer die Prioritäten der polizeilichen Verfahren neu festlegen. Über ein Self-Service-Portal werden dann einzelne Verfahren, wie beispielsweise das Fahndungssystem, mit mehr Speicher und Rechenkapazität versorgt, um auf die Situation effektiv reagieren zu können (siehe Infokasten: Taktische Vorteile). Zusätzliche virtuelle Maschinen können mit kurzen Provisionierungszeiten erstellt und verwaltet werden. Abhängig von einer Situation kann es vorkommen, dass nur wenige Beamte auf ein einzelnes Verfahren zugreifen müssen. Dessen freie Ressourcen, wie zum Beispiel ein Teil des Hauptspeichers, können dann vorübergehend einem verstärkt frequentierten Verfahren zugewiesen werden. Nach Beendigung der Großschadenslage wird dann wieder zum Normalbetrieb zurückgekehrt. Die Abrechnung der zusätzlich zur Verfügung gestellten Leistungen erfolgt nachträglich. So kann die Polizei ohne formelle Anträge, Telefonate und Wartezeiten direkt auf Situationen reagieren und alle Verfahren innerhalb der „Polizei-Cloud“ effektiv dem Ressourcenbedarf anpassen. Während vorher die Bereitstellung eines zusätzlichen Servers – insbesondere dann, wenn neue Hardware beschafft werden musste – Wochen dauerte, können heute zusätzliche Ressourcen mit wenigen Mausklicks zugeordnet werden.

TAKTISCHE VORTEILE DURCH HOHE FLEXIBILITÄT (RAPID ELASTICITY)



Bei einer Großschadenslage (GSL) können schnell und flexibel die Hardwareressourcen angepasst werden. Beispielsweise kann der Hauptspeicher vorrübergehend weniger beanspruchter Verfahren (zum Beispiel das Zeiterfassungssystem TEMPUS) zugunsten anderer Anwendungen reduziert werden. Stark beanspruchte Verfahren (z.B. BAO-E, das Verfahren für Besondere Aufbauorganisationen) erhalten mehr Ressourcen. Ggf. können weitere virtuelle Server schnell zur Verfügung gestellt werden. Diese Flexibilität ermöglicht eine effektive Reaktion auf Sonderlagen, ohne dass im Normalzustand für alle Verfahren maximale Hardwareressourcen vorgehalten werden müssen. Die Verfahren in der „Polizei-Cloud“ erhalten die Ressourcen, die sie benötigen – schnell und flexibel.

Durch die Kosteneinsparungen, die durch die „Polizei-Cloud“ erreicht werden konnten, wurden neue Möglichkeiten geschaffen, ohne dass bei den polizeilichen Verfahren auf Funktionalitäten verzichtet werden muss. Der Polizist im Einsatz spürt also keinerlei Nachteile. Im Gegenteil – durch schnelle und flexible Anpassung der Rechnerressourcen können Wartezeiten auch in Großschadenslagen minimiert werden. Hinzu kommt, dass sich z. B. bei den Großverfahren im Bereich der Vorgangsbearbeitung und der Fahndung eine deutliche Verbesserung der Antwortzeiten ergeben hat. Insbesondere die Zeiten bei komplexen Suchen konnten halbiert werden.

Allgemeine Vorteile für die Polizeiarbeit

Durch Entlastung der Mitarbeiter der Polizei von der Basisadministration werden Kapazitäten für die eigentliche Polizeiarbeit freigesetzt. Die Polizei kann sich dadurch auf ihre Kernkompetenzen, beispielsweise auf die Fachverfahren konzentrieren. Die Basisadministration erfolgt durch Spezialisten in den zertifizierten Rechenzentren des LDI. Die Rechenleistung der Cloud kann also von den Fachanwendern wie „Strom aus der Steckdose“ bezogen werden.

Ein weiterer Vorzug der standardisierten Technologie offenbart sich, wenn man die von der Polizei Rheinland-Pfalz verwendeten „Mobile Devices“ betrachtet. Es kommen sehr heterogene Endgeräte wie Smartphones, Tablets, Notebooks oder PCs zum Einsatz. Damit alle Polizisten mit den von ihnen verwendeten Geräten auf die von ihnen benötigten polizeilichen Verfahren zugreifen können, werden die Ressourcen der „Polizei-Cloud“ über das IP-basierte Netzwerk mittels Standardmechanismen zur Verfügung gestellt („Broad Network Access“). Auf diese Weise kommen die Funktionalitäten der in der Cloud betriebenen Verfahren bis zum Einsatzort der Polizei. Dies ermöglicht zeitnahe Zugriffe auf wichtige Informationen und kann entscheidende Ermittlungsvorteile bewirken. Lösungen dazu werden bereits pilotiert.

Big Data

Der Begriff Big Data ist derzeit in aller Munde. Er beschreibt die Bearbeitung, Auswertung und Visualisierung großer Datenmengen aus vielfältigen Quellen. Die Politik fordert seit Jahren die Einführung eines polizeilichen Informations- und Analyseverbundes (PIAV).

Die flexiblen Rechnerzeiten und Skalierbarkeit der „Polizei-Cloud“ eröffnen auch im Umgang mit Big Data neue Möglichkeiten. Polizeiliche Verfahren, die an dem Informationsmodell Polizei (IMP) orientiert sind, lassen sich relativ leicht in Beziehung setzen, so können beispielsweise Daten zu einer Person innerhalb eines Verfahrens mit anderen Verfahren abgeglichen werden. Dies

ermöglicht eine verfahrensübergreifende Recherche. Durch die theoretisch verfügbare Rechenpower der virtualisierten Verfahren könnten somit auch statistische Auswertungen und Lageberichte generiert werden, die als Basis für strategische Entscheidungen dienen können.

IT-Sicherheit

Die hohen Sicherheitsanforderungen der polizeilichen Verfahren, machten es notwendig, das IT-Sicherheitsmanagement durch externe Auditoren verifizieren zu lassen. Der Antrag auf Erteilung eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde im Juli 2012 gestellt. In den vorausgegangenen und folgenden Monaten sind die damit verbundenen Dokumente erstellt und in einem Präsenz-Audit durch ein BSI-Grundschutz-Auditoren-Team geprüft worden.
Alle Anstrengungen wurden im Mai 2013 durch die Erteilung des ISO 27001-Zertifikats auf der Basis von IT-Grundschutz (BSI-IGZ-0128-2013) für den Betrieb der Cloud-Umgebung belohnt. Rheinland-Pfalz ist das erste Bundesland, das über eine BSI-zertifizierte Virtualisierungsinfrastruktur („Polizei-Cloud“) verfügt.
Da die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit der Daten von Anfang an im Fokus des Projekts standen, kam ausschließlich kundenexklusive Hardware innerhalb der Cloud-Umgebung zum Einsatz. Die zugehörigen Management- und Storage-Netze sind in eigenen Sicherheitszonen realisiert. Ein wesentlicher Sicherheitsaspekt in einer Cloud-Struktur.
Der Zugriff auf die in der „Polizei-Cloud“ betriebenen polizeilichen Verfahren ist ausschließlich über das interne rheinland-pfälzische Polizeinetz, das in diesem Zusammenhang ebenfalls sicherheitszertifiziert wurde, möglich, somit können Störungen und Datenabfluss über das Internet sicher ausgeschlossen werden. Durch ein differenziertes Administrationskonzept, bei dem der Landesbetrieb Daten und Information (LDI) die Basisinfrastruktur zur Verfügung stellt sowie administriert und die Zentralstelle für Polizeitechnik (ZPT) die Fachadministration verantwortet, wird sichergestellt, dass Kompetenz und Know-How aller Beteiligten optimal zur Anwendung kommen.
Die „Polizei-Cloud“ ist Teil des ebenfalls zertifizierten Informationsverbunds „Betrieb des rlp-Netzes“ (BSI-IGZ-0127-2013). Modernste Hardware- und Sicherheitstechnologien in Rechenzentrum und Ausweichrechenzentrum bieten somit ein sicheres Gesamtpaket – auch für die hochkritischen polizeilichen Verfahren. Diese zertifizierte Sicherheit nützt nicht nur dem Landesbetrieb Daten und Information, auch für die Kunden des LDI sind die Zertifikate sehr nützlich. So konnte im Sommer 2013 ein länderübergreifendes Audit (KommSi) bei der rheinlandpfälzischen Polizei sehr erfolgreich abgeschlossen werden. Sämtliche bei der BSI-Zertifizierung auditierten Systeme und die entsprechende Dokumentation wurden von den Auditoren anerkannt, was zu einer erheblichen Reduktion des zeitlichen Aufwands bei der Vorbereitung und Durchführung des Audits führte. Da dieses Audit das erste war, bei dem BSI-zertifizierte Systeme untersucht wurden und ein Zertifikat vollumfänglich anerkannt wurde, dürfte dies für künftige Audits richtungsweisend sein.

Ausblick

Die Migration der polizeilichen Verfahren in eine Cloud-Umgebung ist nur der erste, vielversprechende Schritt bei der Modernisierung der IT-Infrastruktur der Landesverwaltung von Rheinland-Pfalz. Die rheinland-pfälzische „Polizei-Cloud“ ist schon jetzt ein Erfolgsmodell, das sicherlich in Zukunft noch weiter ausgebaut werden wird. Für Bund und Länder ergeben sich nun neue Möglichkeiten der länderübergreifenden Zusammenarbeit. So konnte eine Sicherheitspartnerschaft zwischen dem Landesbetrieb Daten und Information und der rheinland-pfälzischen Polizei vereinbart werden.
Inzwischen wurde ein solcher Vertrag auch mit dem Innenministerium und der Polizei des Saarlandes abgeschlossen. Auf Basis dieses Vertrages ist es nun möglich, die Verfahren der saarländischen Polizei in die bestehende „Polizei-Cloud“ zu integrieren, wo sie einerseits von der zertifizierten Sicherheit der etablierten Infrastruktur profitieren, andererseits aber weiterhin durch Firewall- und VLAN-Trennung unabhängig von den Verfahren der Polizei Rheinland-Pfalz betrieben werden. Die Cloud-Struktur ist auch mit dem rheinland-pfälzischen Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) abgestimmt.
Die vertrauensvolle Zusammenarbeit zwischen der Polizei und dem LDI, für die wir uns an dieser Stelle noch einmal ausdrücklich beim Innenministerium und der Zentralstelle für Polizeitechnik bedanken möchten, ermöglicht die synergetische Nutzung modernster Technologien. Insbesondere aber durch die klar vereinbarte Aufgabenverteilung werden Doppeltarbeiten vermieden und Kosten eingespart. Weil der LDI zahlreiche Infrastrukturen bereits zertifiziert hat, brauchen die Polizeien hier keinen Aufwand mehr zu betreiben und können sich verstärkt um polizeiliche Ermittlungsarbeit oder die Fachverfahren kümmern.Die Integration weiterer polizeilicher Verfahren, auch von anderen Länder- oder Bundespolizeien, in die bestehende Infrastruktur der „Polizei-Cloud“ ermöglicht allen Beteiligten die Ausnutzung von Synergien und somit in der

Summe die Reduktion der betrieblichen Kosten. Mit den Einsparungen, die, wie dieses Beispiel zeigt, mal nicht zu Lasten der Qualität oder des Personals gehen, lässt sich an anderer Stelle im Polizeibereich sicher etwas Sinnvolles anfangen.

© Verlag Deutsche Polizeiliteratur