

Neues Paradigma im IT-Betrieb

Probleme lösen, bevor sie entstehen

IT-Systeme, die sich selbst heilen, wenn sie sich unwohl fühlen und dazu noch melden, dass die Medizin gewirkt hat, wenn sie wieder gesund sind: Was wie Zukunftsmusik klingt, hat Siemens Business Services bereits in einer visionären Lösungsarchitektur konkretisiert. Das Heilmittel heißt Auto Immune Systems. Zentrale Komponenten der Lösung sind die Selbstheilung und aktive Immunisierung durch selbstlernende Prozesse.

Wie Strom aus der Steckdose oder Wasser aus dem Wasserhahn, so soll die IT jederzeit verfügbar sein. Welchen Kunden interessiert es, ob beim Anbieter ein bestimmter Server gerade läuft oder steht? Geht es nicht vielmehr darum, dass die Geschäftsprozesse verfügbar sind, statt der blanken Technik? Hier liegt die Diskrepanz zwischen dem herkömmlichen IT-Betrieb und einer neuen Sichtweise auf die IT-Infrastruktur. Die IT ist kein Selbstzweck mehr – sie bezieht ihre Daseinsberechtigung nur noch aus dem Kontext von Geschäftsprozessen. Zudem sollen sich Nutzer nicht im Detail um Sicherheit oder Fehler kümmern müssen, sondern die IT-Infrastruktur benutzen können wie elektrisches Licht.

Leider sieht die Realität heute anders aus. Auf der einen Seite steigt die Qualität der Software und Hardware. Andererseits tritt aber die von den Kunden gewünschte deutliche Verbesserung der Verfügbarkeit und Sicherheit der Geschäftsprozesse nicht ein. Im Gegenteil: Viele IT-Anwender klagen sogar über eine gesunkene End-to-End-Verfügbarkeit. Als einer der Gründe werden immer häufigere Betriebsunterbrechungen genannt – etwa durch die Installation von dringenden Security Patches. Hinzu kommen viele neue Bedrohungen durch Viren beispielsweise, die sich innerhalb von Minuten weltweit verbreiten und Reaktionszeiten fordern, die der Mensch nicht mehr erfüllen kann.

Probleme lösen, bevor sie entstehen

Um Systeme gegen Ausfälle und Angriffe zu schützen, sind deshalb innovative und automatisierte Services gefordert, die sichere und hochverfügbare Geschäftsprozesse "von innen heraus" gewährleisten. "Ebenso wie das biologische Vorbild des Immunsystems sollen sie Bedrohungen zielgerichtet, lernend und automatisch abwehren. Da die heutige Arbeitswelt mit ihren komplexen IT-Systemen Reaktionen innerhalb kürzester Zeit erfordert, muss das System in Echtzeit reagieren", so Christoph König, Projektleiter Auto Immune Systems bei Siemens Business Services. Gleichzeitig sind die gesamtwirtschaftlichen Aspekte des Unternehmens im Auge zu behalten.

Diese Anforderungen hat Siemens Business Services in der visionären Lösungsarchitektur Auto Immune Systems zusammengeführt. Der IT-Dienstleister vollzieht damit einen Paradigmenwechsel vom Heilen zur aktiven Immunisierung. Im Kern geht es darum, zu verhindern, dass überhaupt Probleme sichtbar werden. Fehler und Angriffe auf die IT-Infrastruktur werden so schnell beseitigt, dass der Anwender nicht in seiner Arbeit behindert wird. Dabei steht nicht der Schutz einzelner IT-Systeme, sondern die Gesamtsicht auf alle IT-Risiken für einen Geschäftsprozess im Vordergrund. Es geht also nicht nur um

die Verfügbarkeit von einzelnen technischen Komponenten. Was zählt, ist das wirtschaftliche Ergebnis eines Geschäftsprozesses.

Eine der zentralen Komponenten von Auto Immune Systems ist die Selbstheilung. In der Praxis leitet das System innerhalb von Sekunden nach Auftreten eines Fehlers Heilungsprozesse ein – und zwar möglichst ohne Betriebsunterbrechung. Reagiert beispielsweise der Browser nicht mehr, da eine Spyware die Applikation lahm gelegt hat, leitet das System sofort Patching-Prozesse ein, um das Problem schnellstmöglich zu beheben. Das Besondere daran: Der Anwender bekommt von dem ganzen überhaupt nichts mit. Damit die Heilungsprozesse hundertprozentig automatisiert und ohne notwendiges Eingreifen des Menschen erfolgen, ist eine Kontrolle über geeignete Regelwerke – die Policies – erforderlich. In den Policies ist genau festgelegt, welche Lösungsprozesse bei bestimmten Fehlerfällen zum Tragen kommen.

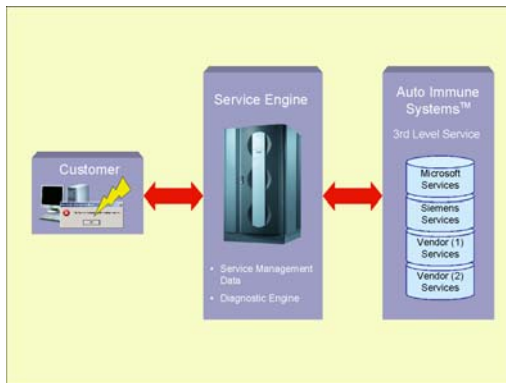
Selbstlernendes System verhindert Ausfallzeiten

Die Zahl der Betriebsunterbrechungen nimmt derzeit zu – sei es beispielsweise durch Softwarefehler oder Security-Patches. Deshalb sind Technologien notwendig, mit denen sich Aktualisierungen der Systeme ohne Störung des laufenden Betriebs durchführen lassen. Um solche Ausfallzeiten zu verhindern, setzt der Münchner IT-Dienstleister auf proaktive Instandhaltung. Selbstlernende Prozesse sind deshalb eine wichtige Komponente von Auto Immune Systems. Sie treiben die Immunisierung durch proaktive Maßnahmen voran.

Das System lernt fortwährend automatisch hinzu, wenn Fehlerfälle auftreten und welche Lösungen am besten helfen. Daraus resultiert eine ständige Qualitätsverbesserung. Die Auto-Immune-Systems-Datenbank ist durch den IT-Betrieb und die Security-Betreuung von rund 460.000 Siemens-Mitarbeitern weltweit bereits mit umfassendem Wissen gefüttert. Durch die Vernetzung der Wissensbasis mit den Datenbanken führender Software-Anbieter steht ein großer Wissenspool zur Verfügung.

Für das Filtern der auftretenden Fehlermeldungen und die Duplizitätserkennung der Diagnose ist die so genannte Service Engine zuständig. Dieses Herzstück der Lösung überprüft, ob das gleiche Problem in der Vergangenheit bereits aufgetreten ist und welcher Heilungsprozess damals eingesetzt wurde. Ähnlich gelagerte Fehlerfälle registriert die Service Engine automatisch, wodurch Fehlerarten nach Häufigkeiten gruppiert und sortiert werden können.

Die Service Engine sorgt zudem für das automatisierte Lernen, betreibt das Policy-Management ebenso wie das SLA-Monitoring. Auf Problemmeldungen reagiert die Service Engine nicht nur innerhalb weniger Sekunden, sondern fragt gleichzeitig die Qualität der Lösungsvorschläge ab.



BU: Das Herzstück der AIS-Lösung, die Service Engine, steht in ständigem Austausch mit den Datenbanken führender Software-Anbieter. (Quelle: Siemens Business Services, 2005)

Für den berüchtigten Zero-Day-Attack gewappnet

Den Unternehmen bleibt heutzutage immer weniger Zeit, auf aktuelle Bedrohungen zu reagieren. Dabei fürchtet sich die IT-Branche vor allem vor dem so genannten "Zero-Day-Attack" – dem Moment, wo der erste massive Angriff zu dem Zeitpunkt startet, an dem die Korrektur noch nicht verbreitet ist: am Tag Null.

Diesen Herausforderungen begegnet Auto Immune Systems mit dem so genannten Cybernetic Defense System, an dessen Umsetzung derzeit Siemens Business Services und die TU München arbeiten. Die Idee hierfür stammt aus der Praxis, und zwar von der US-Marine. Dort werden kybernetische Systeme zur systemgestützten und automatischen Abwehr von Angriffen eingesetzt. Analog hierzu soll ein System entstehen, das auch unbekannte Bedrohungen sofort erkennt und schnell genug mit der richtigen Abwehrmaßnahme reagiert. Dabei werden die Abwehrmaßnahmen und die daraus resultierenden Konsequenzen im laufenden Betrieb wirtschaftlich bewertet und den Risiken gegenübergestellt. Daraus ergeben sich dann dynamische Regelkreise. Falls die Abwehrmaßnahmen mehr Kosten verursachen als durch das Risiko überhaupt in Kauf genommen würden, entscheidet sich das System automatisch für das Risiko.

Jenseits der SLAs steckt enormes Optimierungspotenzial

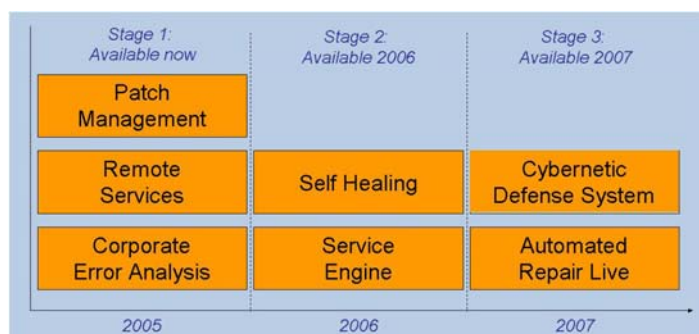
Die visionäre Lösung ermöglicht gleichzeitig die Einführung eines neuen Modells für die Leistungsverrechnung. Gemäß dem Motto "je besser die Geschäftsprozesse laufen, desto besser für alle Beteiligten", teilen sich die Partner beim so genannten Benefit Sharing Risiken und Vorteile. "Statt simpler SLAs schafft das neue Rechnungsmodell zwischen Kunden und Service-Anbieter eine Win-Win-Situation", erklärt Christoph König.

Bei diesem Modell geht es also darum, den wirtschaftlich sinnvollsten anstelle des höchstmöglichen Schutzes zu realisieren. Da die positiven Auswirkungen auf die gesamten Geschäftsprozesse dafür genau bekannt sein müssen, schließt das Benefit Sharing die Notwendigkeit eines Business-Performance-Monitoring-Systems mit ein. "Ohne genaue Erfassung der einzelnen Prozesse funktioniert das neue Geschäftsmodell nicht, weshalb wir bereits aktiv an der Umsetzung umfassender Überwachungstools arbeiten", so Christoph König. Hierzu definiert

Siemens Business Services gemeinsam mit dem Kunden Standard-Geschäftsprozesse, die beispielsweise regelmäßig von Messgeräten oder Testbenutzern durchlaufen werden.

Auto Immune Systems – eine Lösungsarchitektur aus intelligenten Komponenten

Auto Immune Systems besteht aus den Lösungskomponenten Advanced Patch Management, Automated Repair Live, Corporate Error Analysis, Cybernetic Defense System, Remote Services, Self Healing und Service Engine. Jede der intelligenten Komponenten kommt dem Ziel der automatisierten Immunisierung ein Stück näher. Auto Immune Systems ist heute schon Wirklichkeit, denn die ersten Lösungskomponenten sind bereits verfügbar.



BU: In drei Stufen zu Auto Immune Systems (Quelle: Siemens Business Services, 2005)

Das Modul Advanced Patch Management sorgt für maximale Sicherheit von Servern, PCs und Laptops gegen Angriffe von außen und verbessert deutlich die Produktivität der Mitarbeiter. Durch die Offenlegung möglicher Schwachstellen und Verteilung aller erforderlichen Patches und Updates bewirkt die Lösungskomponente eine höhere Effizienz der Sicherheitssysteme. Software-Fehler werden proaktiv beseitigt, damit die Arbeit der Mitarbeiter nicht unterbrochen wird, denn jede Änderung einer Konfiguration birgt ein Risiko, das bewertet und minimiert werden muss. Mussten Mitarbeiter bislang beim Aufspielen neuester Software auf ihren Rechner bis zu 30 Minuten pro Update untätig vor dem Rechner ausharren und anschließend noch einen Neustart des PCs durchführen, geht das Update künftig fast unmerklich vonstatten.

Mit Corporate Error Analysis bekommt der CIO einen vollständigen Überblick über die Lage: Sind seine IT-Systeme sicher? Welches Problem ist wie oft aufgetreten? Wo muss unbedingt nachgebessert werden? Eine Software auf Microsoft-Basis sammelt die notwendigen Informationen und gewichtet sie. Die daraus resultierenden Vorschläge zur Verbesserung kommen postwendend beim CIO auf den Tisch.

Bei Remote Services melden Server sich krank, wenn sie sich unwohl fühlen. Ist etwa die Temperatur zu hoch, kein ausreichender Speicherplatz vorhanden oder die Auslastung über einen längeren Zeitpunkt an der Obergrenze, setzt der Server automatisch eine Alarmmeldung an das Siemens-Service-Team ab: Der erste Schritt, um wieder gesund zu werden.

Siemens Business Services arbeitet kontinuierlich an der Entwicklung der Lösungskomponenten für die nächsten Stufen von Auto Immune Systems. Parallel wird das bestehende Service-Angebot an die visionäre Lösungsarchitektur angepasst.

Fazit

„Den Anforderungen eines Echtzeit-Unternehmens an Sicherheit und Verfügbarkeit von Geschäftsprozessen werden die heutigen Ansätze der IT-Industrie nicht gerecht. Wir brauchen daher ein neues Paradigma, das nicht nur die Verfügbarkeit einzelner Systeme betrachtet, sondern das Ergebnis des gesamten Geschäftsprozesses. Mit Auto Immune Systems bringen wir die Unternehmen auf diesem Weg zu immer zuverlässigeren und gleichzeitig wirtschaftlichen Geschäftsprozessen“, resümiert Christoph König.

Ansprechpartner:

Christoph König, Projektleiter Auto Immune Systems bei Siemens Business Services