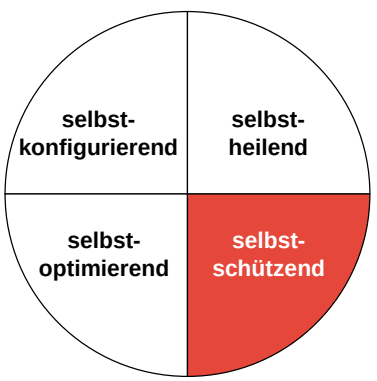
Tivoli software

Autonomic Computing: Die Fähigkeit zum Selbstschutz

Benutzerspezifische, bedarfsgerechte, pünktliche Bereitstellung von Informationen



Warum brauchen wir ‚Autonomic Computing'?

Warum ist ‚Autonomic Computing' heute so wichtig? Zwar sinken die Technologie-Anschaffungskosten, doch die IT-Ausgaben von Unternehmen steigen weiter. Angesichts der allgemeinen Kostensituation in der Wirtschaft suchen IT-Manager nach Möglichkeiten, ihre Investitionsrenditen zu steigern, indem sie die Gesamtkosten ("Total Cost of Ownership", TCO) reduzieren, die Dienstqualität verbessern, die Wertschöpfung beschleunigen und die Komplexität der IT-Umgebungen verringern. e-business ist eine Realität, und Ausfälle sind stets teuer und peinlich.

Was die Situation zusätzlich kompliziert, ist die zunehmende Heterogenität der Umgebungen im Hinblick auf Lösungsanbieter und Technologien. Lösungskomponenten müssen integriert und an die unternehmensspezifischen Geschäftsprozesse angepasst werden. Immer mehr Unternehmen sind darauf angewiesen, Daten, Anwendungen und Systemressourcen über Landes- und Unternehmensgrenzen hinweg austauschen zu können. Auch das trägt zur Komplexität von IT-Umgebungen bei. Die Verwaltung (Implementierung, Einstellung, Wartung und Sicherung) komplexer Umgebungen aber ist teuer.

Diese Tendenzen veranlassten IBM und andere, die Möglichkeiten einer autonomen Selbstverwaltung von Umgebungen (‚Autonomic Computing') zu erforschen. 2001 veröffentlichte IBM sein "Autonomic Computing Manifesto" und verteilte 75.000 Exemplare an die Fachöffentlichkeit. Damit wurde ein Prozess ins Rollen gebracht, der diese Ziele unter der Bezeichnung ‚Autonomic Computing' weiterverfolgt.

Was ist ‚Autonomic Computing'?

Autonomic Computing ist ein technologisches Konzept, das IT-Umgebungen zur Selbstverwaltung und zur dynamischen Anpassung an Veränderungen befähigt, wobei Entscheidungen automatisch auf der Grundlage vorgegebener Geschäftsregeln und -ziele gefällt werden. Ein System kann nur autonom handeln, wenn es "sich selbst kennt" und aus Komponenten besteht, die jeweils eine definierte Identität innerhalb des Systems haben. Da ein System verschiedene Ebenen umfassen kann, muss es alle seine Komponenten, deren aktuelle Zustände, ihre Kapazitäten und alle Verbindungen zu anderen Systemen genau kennen, um sich als autonomes System selbst steuern zu können. Es muss nicht nur über die Grenzen seiner eigenen Ressourcen informiert sein, sondern auch über Kapazitäten von Ressourcen, die gemeinsam genutzt werden können oder nicht allgemein zugänglich sein dürfen.

"Autonomic Computing" ist das Eigenmanagement von e-business-Infrastrukturen. Das System übernimmt einen großen Teil der Managementaufgaben selbst. Dadurch erreicht e-business eine neue Entwicklungsstufe

Worin besteht der besondere Vorteil des Autonomic Computing?
Das Konzept des Autonomic Computing beruht auf vier Grundprinzipien: Selbstkonfiguration, Selbstheilung, Selbstoptimierung und Selbstschutz.

- *Eine selbstkonfigurierende IT-Infrastruktur ist in der Lage, sich dynamisch im laufenden Betrieb selbst zu konfigurieren und sich – bei nur minimalen menschlichen Eingriffen – sofort selbständig auf die Integration neuer Komponenten oder auf sonstige Veränderungen in der IT-Umgebung einzustellen.*
- *Eine "selbstheilende" IT-Infrastruktur kann Abweichungen vom Normalbetrieb der Systeme, Transaktionen und Geschäftsprozesse erkennen und ohne Benutzerintervention Korrekturmaßnahmen auslösen*
- *Selbstoptimierung betrifft zunächst vorwiegend die Komplexität des Systemleistungsmanagements. Langfristig sollen selbstoptimierende Softwareprodukte "aus Erfahrungen lernen" und sich selbst vorausschauend auf die Geschäftsziele abstimmen können.*
- *Eine sich selbst schützende IT-Umgebung gewährleistet die effektive Verwaltung von Zugriffsrechten und kann automatisch geeignete Maßnahmen zur Reduzierung seiner Verwundbarkeit bei Angriffen auf die Laufzeit-Infrastruktur und die Geschäftsdaten treffen.*

Selbstschutz
Eine selbstschützende Umgebung hat das Ziel, spezifische Informationen zu einer bestimmten Zeit an bestimmte Benutzer je nach deren Rolle und den geltenden Regeln bereitzustellen. Eine sich selbst schützende IT-Umgebung kann automatisch Maßnahmen einleiten, um ihre Anfälligkeit gegen Angriffe auf die Laufzeitinfrastruktur und die Geschäftsdaten zu verringern—Angriffe in Form unbefugter Zugriffe, unautorisierter Nutzung, als Virusattacken, die Festplatten formatieren und Geschäftsdaten zerstören, oder
als Denial-of-Service-Angriffe, die wichtige Geschäftsanwendungen lahm legen. Ein Beispiel: Ein e-business-Einzelhandelsunternehmen, das zu bestimmten Jahreszeiten, wie z. B. in der Vorweihnachtszeit, eine stark erhöhte Arbeitsbelastung zu bewältigen hat, wird das Opfer unbefugter Systemzugriffe. Für dieses Unternehmen empfiehlt sich die Implementierung einer selbstschützenden Infrastruktur mit Security- und Speichermanagement-Software, die solche Bedrohungen unmittelbar abwehrt, ohne den laufenden Betrieb zu stören.

IBM Tivoli® Security-Management-Software schafft die Voraussetzungen für eine konsequente Umsetzung von Sicherheits- und Datenschutzregeln; sie trägt zur Senkung der Administrationskosten im Security-Bereich bei, und sie steigert die Mitarbeiterproduktivität und die Kundenzufriedenheit. Schwerwiegende Konfigurationsänderungen sowie Änderungen der Zugangsverwaltung müssen eine entsprechende Autorisierung voraussetzen. Mit Speichermanagement-Tools von Tivoli Software können Unternehmen ihre Geschäftsdaten automatisch und effizient sichern und schützen. Autonome Sicherheits- und Speicher-Managementlösungen verschaffen Administratoren ein Instrumentarium zur Erstellung von Korrelations- und Automatisierungsregeln.

Wann empfiehlt sich die Implementierung einer selbstschützenden Umgebung?

- *Wie schützen Sie die Daten Ihres Unternehmens über heterogene Speicherumgebungen hinweg?*
- *Wie integrieren Sie die unterschiedlichen peripheren Security-Lösungen so, dass die Integrität Ihrer gesamten Infrastruktur gewährleistet ist?*
- *Wie verschaffen Sie sich die Gewissheit, dass Sicherheitsregeln in Ihren kundenseitigen Anwendungen konsistent umgesetzt werden?*

Deloitte & Touche, eine der führenden Steuer- und Unternehmensberatungsfirmen der USA, verfügt über Niederlassungen in mehr als 100 amerikanischen Städten und beschäftigt etwa 30.000 Mitarbeiter. Für Deloitte & Touche ergab sich die Notwendigkeit, den Kunden eine Lösung für komplexe Vertraulichkeits- und Datenschutzanforderungen anzubieten. Das Unternehmen entschied sich für den

IBM® Tivoli Privacy Manager, eine Lösung mit leistungsfähiger Selbstschutzfunktionalität. Jetzt kann Deloitte & Touche das Vertrauen der Kunden aktiv sichern, sich effizient an Veränderungen der Vertraulichkeitsanforderungen anpassen und anwenderdefinierte Regeln automatisch umsetzen, um die gewünschten Vertraulichkeitsstufen zu schützen und langfristig aufrechtzuerhalten.

"Dank Tivoli Privacy Manager und seiner Fähigkeit zum Selbstschutz können wir unseren Kunden eine Security-Lösung bieten, die ihre Vertraulichkeitsanforderungen innerhalb der jeweiligen Industriesparte erfüllt."

William Levant, Geschäftsführer, Deloitte & Touche LLP

Die folgenden Produkte eignen sich zur Implementierung einer selbstschützenden Umgebung:

IBM Tivoli Storage Manager
Der IBM Tivoli Storage Manager gewährt autonomen Schutz durch automatisierte Sicherung und Archivierung von Unternehmensdaten über heterogene Speicherumgebungen hinweg. Sein Schutz kann auf Tausende von Rechnern

mit einem Dutzend verschiedener Betriebssysteme ausgedehnt werden. Die intelligenten Datenverlagerungs- und Datenspeicherungsverfahren sowie umfassende Automatisierungsfunktionen reduzieren die Administrationskosten und erhöhen die Qualität der IT-Dienste.

IBM Tivoli Access Manager
Die Lösungen der Produktfamilie IBM Tivoli Access Manager sind selbstschützend, da sie unerlaubten Zugriff verhindern und über einen einzigen Security-Policy-Server Sicherheitsregeln auf unterschiedliche Dateitypen, Anwendungen, Geräte, Betriebssysteme und Protokolle anwenden. Alle diese Produkte unterstützen unterschiedliche Benutzerauthentifizierungsverfahren einschließlich der konsolidierten Anmeldung per Internet und der Steuern Zugriffs auf viele verschiedene Arten von Ressourcen.

IBM Tivoli Identity Manager
Der IBM Tivoli Identity Manager realisiert das Konzept des Selbstschutzes durch zentralisiertes Identitätsmanagement, durch die Kopplung automatisierter Workflowprozesse mit Geschäftsprozessen und die Nutzung produktivitätssteigernder Selbstbedienungs-Benutzeroberflächen.

IBM Tivoli Risk Manager
Der IBM Tivoli Risk Manager sorgt für systemweiten Selbstschutz durch Auswerten möglicher Sicherheitsbedrohungen und automatisches Einleiten von Gegenmaßnahmen, z.B. durch Server-Umkonfiguration, Implementierung von Security-Patches und Sperrung von Zugangskonten. Er erfasst Sicherheitsinformationen von Firewalls, Intrusionssensoren, Vulnerability-Scannern und anderen Security-Instanzen. Er vereinfacht und korreliert die Vielzahl der Ereignismeldungen und Warnungen, die von diesen Tools generiert werden, und identifiziert rasch die tatsächlichen Sicherheitsbedrohungen, so dass Administratoren mit entsprechenden Gegenmaßnahmen reagieren können.

IBM Tivoli Privacy Manager for e-business
Der IBM Tivoli Privacy Manager for e-business wirkt selbstschützend, indem er viele mit der Security-Compliance verbundene Vorgänge automatisiert und die Kopplung

Was spricht für IBM Tivoli Software für Autonomic Computing?

- *IBM Tivoli Software stellt bereits heute autonome Funktionen bereit.*
- *IBM Tivoli Software erlaubt es dem Kunden, seine Aufmerksamkeit den geschäftlichen Aufgaben zu widmen, anstatt sich ständig mit der IT-Infrastruktur beschäftigen zu müssen.*
- *IBM Tivoli Software verbindet die Dynamik eines jungen Unternehmens mit der Erfahrung, der Qualität und den Ressourcen von IBM*
- *IBM Tivoli Software bietet schrittweise Implementierungsrichtlinien*
- *IBM Tivoli Software steht für Evolution, nicht Revolution*
- *Das IBM Tivoli Software-Team bietet jederzeit Unterstützung (IBM und IBM Business Partner)*

von Vertraulichkeitsregeln mit Geschäftsprozessen sowie ihre Überwachung und Umsetzung vereinfacht. Er registriert die Regelzustimmung bzw. -ablehnung der Endanwender, überwacht und erzwingt die Einhaltung von Vertraulichkeitsregeln für den Systemzugriff und erstellt Prüfprotokollberichte.

Fazit

IBM weiß, dass jedes Unternehmen ein Interesse daran hat, seine IT-Kosten zu senken, das Management seiner IT-Ressourcen zu vereinfachen, einen schnellen Return-on-Investment auf seine IT-Investitionen zu erzielen und ein hohes Maß an Verfügbarkeit, Leistung, Sicherheit und Auslastung zu gewährleisten. Dies lässt sich durch eine Kombination von Prozessänderungen, Mitarbeiterschulung, neue Technologien, eine entsprechende Architektur und offene Standards erreichen.

Zum Autonomic Computing führt ein schrittweiser Evolutionsprozess. IBM Tivoli Software und IBM entwickeln den Implementierungsplan und sorgen dafür, dass jede Implementierungsphase für den Kunden eine wertschöpfende Wirkung entfaltet. IBM ist bestens vertraut mit dem Wertschöpfungspotenzial des Autonomic Computing, den Entwicklungsstufen zu seiner Realisierung und der Notwendigkeit offener Standards und einer offenen Architektur für heterogene Betriebsumgebungen. IBM fördert die Idee des Autonomic Computing und unterstützt die Bemühungen von Tivoli Software, unsere Kunden zum Autonomic Computing hinzuführen.

Autonomic Computing ist mehr als eine neue Technologie – es ist eine fundamentale Neuorientierung im Management von IT-Systemen. Durch intelligente Technologien werden IT-Mitarbeiter von vielen Routinetätigkeiten im Systems-Management freigestellt und können sich dadurch wertschöpfenden Aufgaben widmen.

Weitere Informationen

Informationen zu IBM Tivoli Software und integrierten Lösungen von IBM erhalten Sie von Ihrem IBM Vertriebsbeauftragten oder im Internet unter: **ibm.com/tivoli**

IBM Deutschland GmbH
70548 Stuttgart
http://www.ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
http://www.ibm.com/at

IBM Schweiz
Bändliweg 21, Postfach
8010 Zürich
http://www.ibm.com/ch

Die IBM Homepage finden Sie unter:
http://www.ibm.com
http://www.ibm.com/services/de

10-02

Die Tivoli Homepage finden Sie im Internet unter **ibm.com/tivoli**

Die IBM Homepage finden Sie im Internet unter **ibm.com**