

Haushalt unter die Hände greifen können. Aber auch Robobots stehen bereits in den Startlöchern einiger Labs (und Militärs). Diese Roboterfamilien können zB in Situationen zum Einsatz kommen, die für Menschen gefährlich bzw unzugänglich sind (zB zur Brandbekämpfung, im Nachtbau, der Raumfahrt etc). Mehrere kleinere (und günstigere) Roboter könnten in der Gruppe zusammenarbeiten (zB Daten übertragen, Kommandos austauschen etc), und es würde auch keinen großen Unterschied machen, wenn ein paar der Gruppe defekt ausfallen würden (die Idee baut am Beispiel von Ameisen oder Bienenvölkern auf).

In Zukunft wird es immer mehr Computertechnologie in heutzutage noch unintelligenten Geräten geben, und die meisten dieser Geräte werden vernetzt sein. Für diese Aufrüstung kommen alle Haushaltsgeräte wie Kühlschränke, Fernseher etc in Frage. Durch den Preisverfall wird die Technologie aber schlussendlich überall einsetzbar sein. Der Kühlschrank, der über Computernetze mit seinem Inhalt kommuniziert und selbstständig zwei Liter Milch bestellt, sobald keine Milchpackung auf seine Anfrage antwortet, ist zwar noch Vision, technisch aber ohne größere Probleme umsetzbar. Eine Schlüsseltechnologie dafür wird RFID<sup>1</sup> (Radio Frequency Identification, englisch für Funkerkennung) sein. Diese Technologie ist billig und ermöglicht die Integration von „Geräten“ ohne eigene Stromversorgung (Kostenfrage) in ein Computernetz. Wenn man diese Teile zu einem Ganzen zusammenfügt, ergibt sich ein Bild, das nicht mehr einen Computer pro Person oder drei pro Haushalt, sondern 100 bis 1000 Computer pro Haushalt zeigt. Firmennetzwerke werden

dann nicht mehr Hunderte bis Tausende Computer, sondern einige 10.000 Geräte umfassen. Computer werden allgegenwärtig sein, man spricht in Fachkreisen daher auch vom „ubiquitären“<sup>2</sup> Computerzeitalter oder „Ubicomp“, und sie werden oft auf den ersten Blick nicht als Computer im heutigen Sinn erkennbar sein (Handy, digitales Papier etc).

Wenn auch viele Konzepte noch nicht spruchreif sind und manches wahrscheinlich nie die Laboratorien verlassen wird, so lassen sich doch mit gewisser Sicherheit folgende sicherheitsrelevanten Problemfelder von Ubicomp skizzieren, die der Bearbeitung harren.

#### Zugriffskontrolle

Zukünftige Geräte werden in aller Regel nicht durch das Abziehen eines Kabels vor unstatthaftem Zugriff geschützt werden können, sie werden nämlich kabellos erreichbar sein. Dies ermöglicht mehr Mobilität und ist billiger. Erste Erfahrungen in diese Richtung konnten mit den beliebten WLANs (Funknetzwerke) gemacht werden. Diese waren in der Grundeinstellung gegen fremden Zugriff ungeschützt, das Absichern ist nicht wirklich trivial, und unerwünschter Gebrauch durch Fremde ist schwer festzustellen, es sei denn, die Rechnung vom Internetprovider schnell in die Höhe, oder Sie finden Ihnen unerklärliche Ausdrücke im Ausgabeschacht Ihres Druckers. Zugriffskontrolle muss also ein fix integrierter Bestandteil der nächsten Generation von Geräten sein, wobei der PIN-Code des Mobiltelefons nicht geeignet scheint. In unserem Szenario müssten Sie sich nämlich die Pin-codes für Kühlschrank, Fernseher, Videorecorder etc merken. Sinnvoller ist eine Lösung, bei der das Gerät er-

## Mit Antares NetlogiX ISO & BSI konform

**Angesichts der steigenden Zahl der Einbrüche in IT-Systeme und der permanenten Angriffe durch Würmer und Viren sind die verantwortlichen Sicherheitsadministratoren oft damit beschäftigt, auf die Attacken zu reagieren und Löcher zu stopfen.**

**D**ies liegt zum Teil daran, dass viele Unternehmen die unterschiedlichen Schwachstellen mit entsprechenden Teillösungen, wie dem Patch-Management, erst bei Bedarf beseitigen.

In zunehmenden Masse werden Security Projekte jedoch in Prozesse umgewandelt und als nachhaltige IT Vorgänge institutionalisiert. Zunehmender Druck wird auch durch internationale Vorgaben wie ISO 17799, den Sarbanes-Oxley-Act und BSI Empfehlungen aufgebaut. Umfassende IT Sicherheit als Management Prozess (z.B. nach ITIL) geht natürlich weit über die Themen Anti-Virus und Firewallschutz hinaus.

#### Best Practises: Nicht das Rad neu erfinden

Bestehende Best-Practise Modelle und Templates, bereits integriert in führende Sicherheitsmanagement Lösungen wie den NetIQ Vulnerability Manager, erleichtern die Einführung und Umsetzung wesentlich. Schwachstellen-Analyse, Konfigurations- und Patch Management sowie konforme Auditierung sollten die Schwerpunkte eines funktionierenden IT Prozesses abdecken. Weitere Themen wie Gruppenrichtlinien Management, Log Konsolidierung und IT-Workflows sind ebenso integrativ abzudecken. Im Idealfall werden diese Themen zusammengeführt und laufend betreut – von der Planung bis zum deutschsprachigen Support durch Antares NetlogiX.

#### NetIQ überwacht den „kleinen Dienstweg“

Neben der technischen Konformität ist vor allem der weiche Faktor „Mitarbeiterverhalten“ entscheidend. Die Möglichkeit der technischen Durchsetzbarkeit von Policies sowie die Nachweisbarkeit - dass diese Vorgaben gelesen, verstanden und akzeptiert werden – sind sicherzustellen.

Sicherheitskonzepte sollten eine abschreckende Wirkung für unliebsame Eindringlinge und „flexible Mitarbeiter“ darstellen und bei IT Managern für ein gutes Gefühl sorgen. Am „1. Antares Technology Forum“ am 22. September in den Twintowers erfahren Sie mehr, wie Kunden derartige Projekte erfolgreich umsetzen. Anmelde-möglichkeiten unter

[www.netlogix.ws](http://www.netlogix.ws)