

Qualitätssicherung laufend prüfen

## Transparenz für Security-Dienstleistungen

**Unternehmen können Aufgaben der IT-Security an externe Anbieter auslagern – doch die Verantwortung und Haftung können sie nicht abgeben. Für die Durchsetzung einer optimalen Sicherheitsqualität muss Transparenz über das aktuelle Schutzniveau im Netzwerk herrschen. Unabhängige Monitoring-Lösungen ermöglichen eine Qualitätssicherung und minimieren das Restrisiko. So werden die Verantwortlichen in ihrer Sorgfaltspflicht unterstützt.**

Kostendruck und die Verschlangung der IT sind die Hauptgründe, weswegen immer mehr Unternehmen die Verteidigung ihrer Systeme in professionelle Hände geben und an Managed-Security-Anbieter auslagern. Die Experton Group berichtet von einem aktuellen Marktvolumen für IT-Sicherheits-Dienstleistungen von 2,1 Milliarden Euro. Im Zusammenhang mit Berichten über das Outsourcing von IT-Sicherheit ist immer wieder davon zu lesen, dass die Unternehmen „die Verantwortung externen Dienstleistern übertragen“. Doch davon kann keine Rede sein. Die letzte Instanz für den Schutz der eigenen Daten ist und bleibt das Management des Unternehmens.

### Früherkennung gefordert

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) definiert die Pflichten der Unternehmensleitung bezüglich des Risikomanagements und der Risikosteuerung. Dort formuliert der Gesetzgeber die Anforderung an den Vorstand in Paragraph 91 Absatz 2 AktG – im Wortlaut: „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“. In Paragraph 93 Absatz 2 AktG wird dann besonders deutlich, warum es im ureigensten Interesse des Managements ist, immer selber kontrollieren zu können, wie es um das aktuelle Schutzniveau in der eigenen IT-Sicherheit bestellt ist: „Vorstandsmitglieder, die ihre Pflichten verletzen, sind der Gesellschaft zum Ersatz des daraus entstehenden Schadens als Gesamtschuldner verpflichtet. Ist streitig, ob sie die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt haben, so trifft sie die Beweislast.“ „Ein Service Level Agreement (SLA), welches beispielsweise festlegt, dass der Virenschutz gemäß dem aktuellen

Stand der technischen Möglichkeiten betrieben werden soll, reicht nicht mehr aus“, sagt Peter Graf, Geschäftsführer des IT-Security-Dienstleisters AMPEG.

### Transparenz einfordern

Sicherheitsverantwortliche müssen selbst über den Zugriff auf entsprechende Überwachungssysteme im Unternehmen verfügen. Ungeachtet vom gewählten MSS-Modell muss das Management immer über den aktuellen Sicherheitsstatus im Netzwerk informiert sein. Dabei darf es keine Rolle spielen, ob die IT-Sicherheit bei einem externen Anbieter gehostet wird oder ein externer Mitarbeiter die Systeme im eige-



„Ein Service Level Agreement (SLA), welches beispielsweise festlegt, dass der Virenschutz gemäß dem aktuellen Stand der technischen Möglichkeiten betrieben werden soll, reicht nicht mehr aus“, sagt Peter Graf, Geschäftsführer des IT-Security-Dienstleisters AMPEG. Foto: AMPEG

# 7. FACHMESSE FÜR

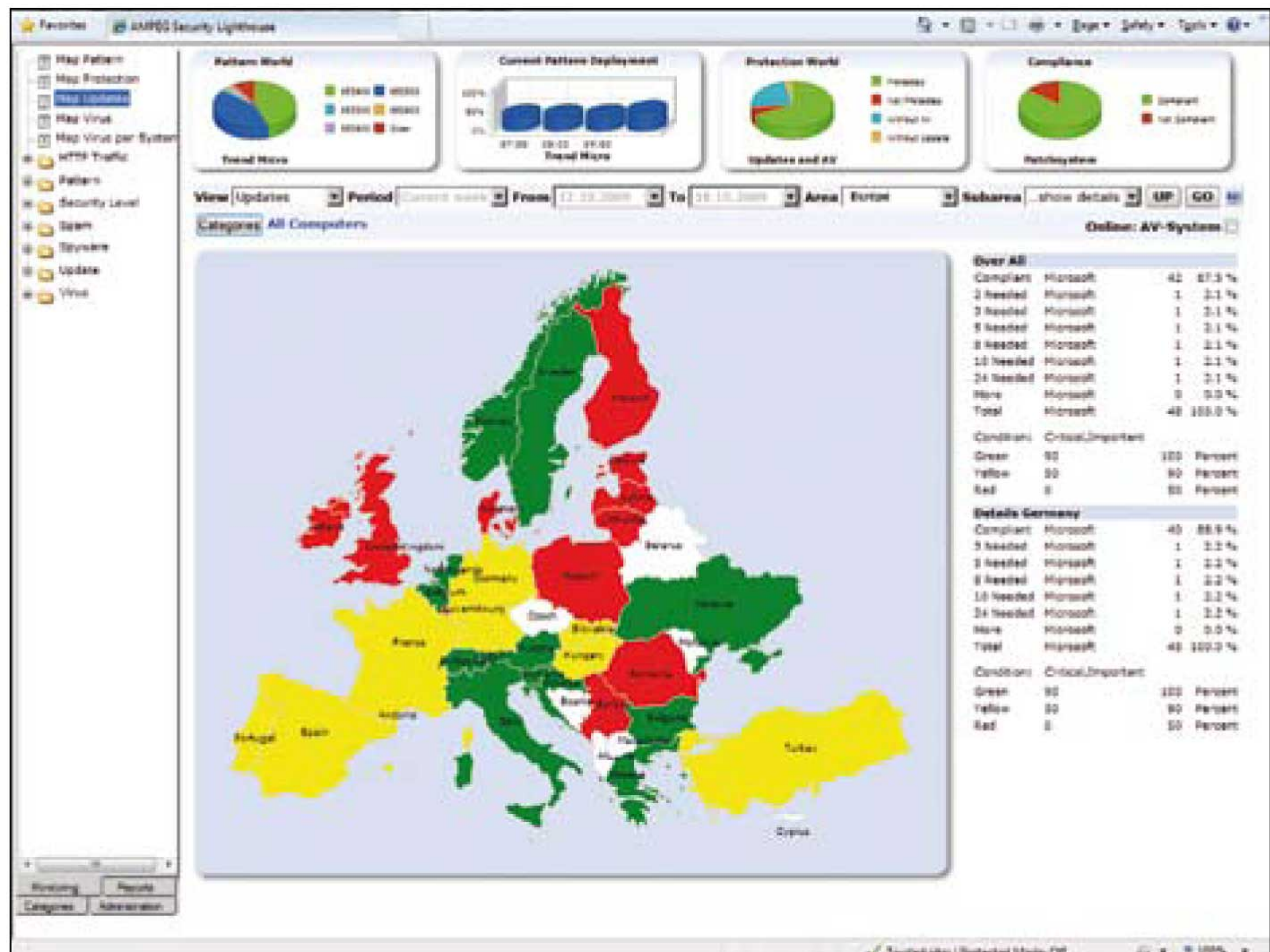
ZUTRITTSKONTROLLE  
VIDEOÜBERWACHUNG  
IT-SECURITY  
BRANDSCHUTZ

7. – 8. JULI 2010  
ICM MESSE MÜNCHEN

→ NETCOMM GmbH  
Tel. 089/88949370  
info@sicherheitsexpo.de  
WWW.SICHERHEITSEXPO.DE

SICHERHEITSEXPO  
07.-08. JULI 2010 MÜNCHEN

## MANAGED SECURITY SERVICES



Sicherheitsverantwortliche müssen jederzeit selbst in der Lage sein, sich einen Überblick über den unternehmensweiten Sicherheitsstatus zu verschaffen  
Grafik: AMPEG

nen Unternehmen betreibt. Mit herstellerübergreifend arbeitenden Monitoring- und Reporting-Systemen ist es möglich, die erforderliche Transparenz herzustellen. Diese Systeme sammeln Log-Daten aus allen Sicherheitslösungen und prüfen deren Leistung gegen vorher festgelegte Zielwerte. Als Ergebnis der Analyse wird das aktuelle Schutzniveau in möglichst aussagekräftigen Listen und Charts angezeigt oder mit Ampelfarben in einer Security-Information-Map visualisiert. Die Security-Verantwortlichen erhalten so einen permanent aktuellen Blick auf die Sicherheitslage. Das ist die Voraussetzung, um einen nachhaltigen Qualitätssicherungsprozess für die IT-Sicherheit einzurichten.

### Security Level Management reduziert Risiken

Der in § 91 Absatz 2 AktG geforderten Früherkennung können Sicherheitsverantwortliche durch die Einführung eines Security Level Managements (SLM) gerecht werden. Im Rahmen eines SLMs werden aus abstrakten Security Policies zunächst messbare Grenz- und Schwellenwerte für die einzelnen Sicherheitssysteme im Unternehmen abgeleitet. Dank der transparenten Sicht können dann die Ist-Werte erfasst und mit dem Soll abgeglichen werden. Durch die fortlaufende Beobachtung des Security Levels werden Schwachpunkte im

Netzwerk frühzeitig identifiziert und ein proaktives Handeln wird ermöglicht. Im Hinblick auf das gemeinsame Ziel von MSS-Anbieter und Unternehmen, IT-Sicherheit zu verbessern und das Restrisiko zu minimieren, ist es für beide gleichermaßen von Interesse, Transparenz herzustellen und eine Qualitätssicherung für die IT-Sicherheit mittels SLM zu etablieren.

In der Verantwortung steht am Ende jedoch der Auftraggeber, der die Leistungen so einkaufen und überwachen muss, dass seine Unternehmensprozesse nicht gefährdet werden.



Florian Hohenauer,  
talkabout communications