Olympus Europa Holding GmbH hält die IT-Infrastruktur mit Qualys regelkonform und sicher

Ein Unternehmen wie die Olympus Europa Holding GmbH kann die Sicherheitsvorgaben für seine IT-Infrastruktur nur dann effizient überwachen, wenn die Prüfmechanismen hochgradig automatisiert und in den Unternehmens-Workflow eingebunden sind. Mit der QualysGuard Suite hat das Unternehmen zentrale Überwachungsprozesse etabliert, welche auch die Datenbasis für die Kommunikation mit der Geschäftsleitung bilden.

"QualysGuard ist die zentrale Basis zur Kommunikation mit der Geschäftsleitung."

Matthias-Marc Gsuck
IT Audit Manager IT Security,
Olympus Europa

Olympus wurde 1919 unter dem Namen Takachiho Seisakusho in Japan gegründet und ist einer der weltweit führenden Hersteller von optischen Produkten. 1949 wurde das Unternehmen in Olympus Optical Co, Ltd umbenannt. Das Produktspektrum umfasst neben den digitalen Kameras für den Consumermarkt vor allem Mikroskope und Endoskope für medizinische und industrielle Anwendungen.

Die 47 europäischen Tochtergesellschaften von Olympus sind in der Olympus Europa Holding GmbH mit Sitz in Hamburg zusammengefasst. Die Holding bietet den Tochtergesellschaften umfangreiche Services in den Bereichen Finanzen, Personalwesen, IT, Logistik, Marketing und Unternehmenskommunikation. Neben der Corporate Division zählen die Consumer Product Division und die Medical Systems and Micro-Imaging Solutions Group zur Olympus Europa Holding.

Die Olympus Europa Holding GmbH beschäftigt 4.700 Mitarbeiter. Der Umsatz lag im Geschäftsjahr 2009/10 bei 1.383,712 Millionen Euro.

Die IT-Infrastruktur basiert auf Windows Servern und Clients sowie verschiedenen Hostsystemen (Datenbanken und Citrix-Terminal-Systemen). Im Netzwerkbereich setzt Olympus Europa auf Cisco. Das Unternehmen orientiert sich an den Vorgaben des Standards 27001 für Informationssicherheitsmanagement (ISMS) und ist gemäß Standard zertifiziert.

Automatisierung der Scans war unausweichlich

Besonders sensible IT-Bereiche im Intranet und Extranet, E-Commerce und CRM wurden schon immer regelmäßig auf Schwachstellen untersucht. „Wir haben hier am Standort Hamburg ein Prüfungsschema aufgebaut, das den Anforderungen von Sarbanes-Oxley (SOX) beziehungsweise seiner japanischen Ausprägung JSOX sowie den COSO- und CObIT-Frameworks genügt“, sagt Matthias-Marc Gsuck, IT Audit Manager IT Security bei Olympus Europa.

Ursprünglich ging man dabei manuell vor und verwendete beispielsweise Nessus und andere Opensource-Systeme. Die Ergebnisse waren durchaus gut, allerdings stieß man angesichts der umfangreichen IT-Infrastruktur bei der manuellen Handhabung schnell an Grenzen. Eigenständige Systeme für die Durchführung der Prüfungen waren zwar vorhanden, aber sie hätten ständig aktualisiert werden müssen. “Bei diesen Aktualisierungen mussten wegen der Orientierung der Prüfungsschemata an den geschäftlichen Abläufen zudem ständig die entsprechenden Fachabteilungen einbezogen werden. Das war ein immenser Arbeitsaufwand, so dass eine Automatisierung des Scan-Prozesses unausweichlich war”, so Matthias-Marc Gsuck.

Auch die Clients werden künftig auf Regelkonformität geprüft

Die IT-Verantwortlichen bei Olympus Europa suchten deshalb eine Scan-Lösung, mit der die Schwachstellenanalyse über alle IT-Bereiche hinweg vereinheitlicht und zentral gesteuert werden kann. Es sollten keinerlei lokale Installationen an den jeweiligen Rechnern und Geräten notwendig sein.

Olympus Europa Holding GmbH hält die IT-Infrastruktur mit Qualys regelkonform und sicher

Die QualysGuard Suite mit ihrem Software-as-a-Service-Ansatz (SaaS) war deshalb für Olympus Europa genau die richtige Lösung. Nach einer längeren Testphase wird mittlerweile das Modul QualysGuard Vulnerability Management (VM) im Produktivbetrieb eingesetzt. Die beiden Module Policy Compliance und Web Application Scan von Qualys sind im Pilotbetrieb.

Durch das SaaS-Konzept kann die Schwachstellenanalyse in den verschiedenen Unternehmenseinheiten von Olympus Europa einheitlich genutzt werden, wobei sich die Scan-Parameter an die Notwendigkeiten der jeweiligen Aufgabe individuell anpassen lassen, ohne dass vor Ort Software oder Hardware installiert werden müssen.

Mit QualysGuard wurde der gesamte Workflow bei Olympus Europa automatisiert. „Patchprozesse im Stil der Feuerwehr eignen sich nicht für den Grad von Sicherheit, wie wir ihn benötigen“, sagt Matthias-Marc Gsuck, deshalb würden in Zukunft nicht nur die oben erwähnten exponierten Systeme automatisiert gescannt, sondern mit Modulen wie Policy Compliance vor allem auch die Clients.

Regulatorische Anforderungen werden durch QualysGuard gut abgedeckt

Die Qualys Scan Engine erhält laut Gsuck nicht zuletzt dadurch einen großen Mehrwert, dass durch sie auch die regulatorischen Anforderungen abgedeckt werden können. Die Anforderungen sind in den Workflow und das Ticketing-System eingebunden. „Wir haben mit einem Testaccount von Qualys angefangen und haben diesen immer noch - für Testzwecke. Mittlerweile aber auch eine auf IP-Adressen basierende Lizenz von QualysGuard”, erzählt Matthias-Marc Gsuck aus der Historie. Derzeit scannt man bei Olympus Europa rund 2000 IP-Adressen, will die Lösung aber auf allen Kernsystemen einsetzen. In den nächsten Jahren könnten laut Gsuck rund 6000 Systeme (Server, Clients und Netzkomponenten) dazukommen. „Qualys passt bezüglich der Prozesse und der Zuordnung der Systeme wie der Deckel auf den dazugehörigen Topf“, lobt der IT Audit-Verantwortliche und fährt fort: „Pro Host wird ein Systemeigner definiert und diese Information automatisch in das Ticketing-System übertragen, sodass alles transparent und nachvollziehbar und die jeweilige Verantwortlichkeit richtig zugewiesen ist.“ Damit können die Anforderungen von SOX ebenso nachgehalten werden wie die internen Kontrollsysteme, die bei Olympus gelten.

Wichtig bei der Entscheidung für QualysGuard war auch, dass Qualys eine gut handhabbare Anwendungsprogrammierschnittstelle (API) liefert, sodass die Ergebnisse der Schwachstellenanalyse gut in Systemmanagement- und Helpdesksysteme zu integrieren sind. „Unsere diesbezüglichen Systeme werden in den nächsten Jahren konsolidiert werden, der Schwachstellen-Scan sollte aber keine Vorentscheidung für ein bestimmtes Managementsystem mit sich bringen, wir wollten da ganz frei bleiben“, erläutert Gsuck.

Saas-Ansatz birgt immense Vorteile

Manche Unternehmen zeigen immer noch eine gewisse Reserve gegenüber SaaS-Lösungen im Security-Bereich, weil interne Daten in die Obhut eines externen Dienstleisters gegeben werden. Mattias-Marc Gsuck kann diese Bedenken nachvollziehen, teilt sie aber in diesem Fall nicht. Schließlich würden die Daten der Schwachstellenanalyse in der Datenbank von Qualys verschlüsselt und mandantensicher gespeichert. Vor allem sieht er aber die immensen Vorteile. Beispielsweise kann QualysGuard VM durch ausgereifte Korrelationsmechanismen eine Gewichtung von erkannten Schwachstellen festlegen.

Unschätzbare Vorteile bringt der SaaS-Ansatz dadurch, dass einerseits die Anforderungen einzelner Unternehmensteile schnell umgesetzt werden können und andererseits der Scan-Prozess zentral gesteuert werden kann, sowie ein zentrales Berichtswesen möglich ist. „Für mich ist die Qualys-Plattform gleichzeitig die zentrale Datenbasis für die Kommunikation mit dem Management. Die Berichte enthalten die wesentlichen Punkte, sind übersichtlich und stärken auf diese Weise das Engagement der Geschäftsführung für Fragen der IT-Sicherheit“, sagt der IT Audit-Verantwortliche bei Olympus Europa.

ÜBERBLICK

Unternehmen: Olympus Europa Holding GmbH
Branche: Optische Industrie (Digitalkameras, Endoskope und Mikroskope)
Firmenzentrale: Hamburg, Deutschland
Firmengröße: Umsatz 2009/2010: 1.383,712 Millionen Euro, 4.700 Mitarbeiter

ZIELE FÜR DIE IT-SICHERHEIT

Automatisierung und zentrale Steuerung der Schwachstellenanalyse

LÖSUNG

- QualysGuard Vulnerability Management (im Produktivbetrieb)
- QualysGuard Policy Compliance (im Pilotbetrieb)
- QualysGuard Web Application Scan (im Pilotbetrieb)

Warum hat sich die Qlympus Europa Holding GmbH für QualysGuard entschieden?

- Mit QualysGuard lassen sich die existierenden Prüfschemata von Olympus automatisieren und in den Workflow einbinden.
- Die API von QualysGuard lässt dem Anwender alle Freiheiten bei der Einbindung in andere Softwarelösungen.
- Das SaaS-Konzept macht eine einfache Nutzung des Scanners in den verschiedenen Unternehmenseinheiten von Olympus Europa möglich, ohne dass vor Ort Software oder Hardware installiert werden müssen.
- QualysGuard bildet eine ideale Basis für die Kommunikation über IT-Sicherheit zwischen IT-Verantwortlichen und Geschäftsleitung.
- Das Lizenzmodell auf der Basis gescannter IP-Adressen ist fair und leicht verständlich.

QUALYS®
www.qualys.com

USA – Qualys, Inc. • 1600 Bridge Parkway, Redwood Shores, CA 94065 • T: 1 (650) 801 6100 • sales@qualys.com
UK – Qualys, Ltd. • Beechwood House, 10 Windsor Road, Slough, Berkshire, SL1 2EJ • T: +44 (0) 1753 872101
Germany – Qualys GmbH • München Airport, Terminalstrasse Mitte 18, 85356 München • T: +49 (0) 89 97007 146
France – Qualys Technologies • Maison de la Défense, 7 Place de la Défense, 92400 Courbevoie • T: +33 (0) 1 41 97 35 70
Japan – Qualys Japan K.K. • Pacific Century Place 8F, 1-11-1 Marunouchi, Chiyoda-ku, 100-6208 Tokyo • T: +81 3 6860 8296
United Arab Emirates – Qualys FZE • P.O Box 10559, Ras Al Khaimah, United Arab Emirates • T: +971 7 204 1225
China – Qualys Hong Kong Ltd. • Suite 1901, Tower B, TYG Center, C2 North Rd, East Third Ring Rd, Chaoyang District, Beijing • T: +86 10 84417495

ON DEMAND SECURITY