A Global Company Balances the Priorities of IT Security, Compliance and International Law.

Do you find security demands, audit requirements and legal deadlines giving you the squeeze?

Accenture, one of the largest management consulting, technology services and outsourcing companies in the world gets everything done on time using AVDS.

Introduction

Maintaining an effective network security posture internationally is a constant exercise in adaptation. Because threats are constantly evolving and budgets are finite, 100% regulatory compliance is extremely challenging.

The task of assessing, understanding and managing the overall security posture in near real time — and doing so in relation to evolving compliance requirements and threats — can be time consuming, expensive and complicated.

The Challenge

A real-time understanding of client's security posture is the goal for Chris Lewis. At any given time, Lewis is juggling two or three audits as part of his role as a Technical Security Manager for Accenture. In this role, he manages security, compliance and Federal, state and internal audits for clients in the healthcare and other fields.

The networks he manages are very large, containing thousands of end-points including servers, workstations, network devices and IP phones.

"We now have the ability to scan at any time. Regular vulnerability assessments scans are like having sonar on our own network. We always know what is going on around us."
–Mike Gutknecht
Network Engineer
Rayovac Corporation

AVDS graphically, unobtrusively and with great detail demonstrated to me the situation of our network/firewall and web server after scanning our system with a huge range of tests. Reports were sent to me that were concise and clear and then the technical staff of Beyond Security talked me through the results of the scans, interpreting areas with which I was unfamiliar and suggesting simple and precise fixes. From the moment of my first contact with Beyond Security, I have been impressed and enjoyed their friendliness, clear talking, approach to confidentiality and technical knowledge."
–Paul Sheriff
IT Manager
City of Geraldton

As a technical security manager, Chris Lewis anticipates security issues that may disrupt client business operations by:

- Prioritizing corrective action depending on the seriousness of the threat and the importance of the asset threatened.
- Establishing and reporting on compliance with internal policies and external regulations.
- Managing the often conflicting priorities of IT security, compliance, and legal departments.
- Remediating security incidents and events quickly and accurately with policies that ensure policy compliance while minimizing business disruptions.

Identifying, monitoring, and understanding security alerts, and taking the time to manually audit security and configuration settings, can be time consuming and difficult in large, distributed deployments.

The Solution

By installing the AVDS appliance-based solution, Accenture got a real-time view of the network security topography of each client and can clearly demonstrate compliance with emerging global IT security standards and integrity legislation.

AVDS conducts automated vulnerability scans on periodic basis according to a pre-set schedule or on ad-hoc basis. From these reports, vulnerability trends can be identified for entire organizations, local networks or down to the level of single IP address.

AVDS also reports contain simple and applicable solutions to problems found. This in depth information shows how to fix and improve the security of your network, both as whole and for each of the devices in it. The solutions can be used globally and will prevent future vulnerabilities from occurring. The recommended solutions include device specific information as well as custom tailored solutions for your environment.

The information provided in the reports is very clear and concise. It explains to engineers what the problem is, where to look for more information, and how to fix it.
"With these reports we can be sure after every change to the network if we are making the right change in terms of our security requirements.
"We tried the free services. But when we piloted AVDS, we saw zero false positives and the differential reports make Management Reporting easy. These features are huge. They allow us to focus on delivering ICT services instead of chasing down vulnerabilities."
–Cody Phang
Head of IT for the Australian Government National Capital Authority (NCA)

By deplying AVDS, Accenture was able to:

- Strengthen current network security processes and procedures to protect against attacks from both external and internal threats.
- Deploy new security solutions that go beyond core-level technology to span the entire network.
- Respond more rapidly to changing client requirements driven by organizational changes, access, permissions and constantly changing operational procedures.
- Comply with new security policies that mandate IT upgrades.
- Perform routine vulnerability assessments of their network, not relying upon once-a-year penetration tests.

The objective is solid information - a regular scan of network vulnerabilities with a method for prioritizing alarms, automating security auditing, and consolidating the information required to meet reporting and regulatory requirements.

The Story
"Because of the complexity and volume of all the audits our client undergoes, we needed a way be proactive and stay one step ahead of the game, to regularly scan their network in advance of the external auditors," said Lewis. "There are plenty of tools out there that will provide a scan of vulnerabilities. What we needed was a tool that could prioritize alarms, automate security auditing, and consolidate the information required to meet reporting and regulatory requirements."

About AVDS
Beyond Security's AVDS performs a security mapping of each client's network and simulates attacks originating from both inside and outside the network. Once mapping of all devices, ports and services is complete, AVDS generates a detailed vulnerability report specifying any security weaknesses, along with detailing the best practice solutions to those vulnerabilities.

The engine is updated on a regular basis to stay abreast with the most recent security vulnerabilities. The updates include security vulnerabilities that were discovered by the company's own research and development team, as well as those discovered elsewhere.

Contact Information

USA

1616 Anderson Road   +1 800 801 2821
McLean, VA 22102   aviram@beyondsecurity.com

19925 Stevens Creek Blvd.   +1 408 329-6041
Cupertino, CA 95014   donw@beyondsecurity.com

EMEA

105 London St. Suite 609   +44 203 006 3022
Reading   RG1 4QD   zvim@beyondsecurity.com
UK

Asia Pacific

Post Office Box 4   +61 401 778 124
Mount Colah NSW 2079   steveh@beyondscurity.com
Australia

China

5/F South Block Tower C,   +86 10 598 22211
Rathcom Info Tech Park,   thomasz@beyondsecurity.com
No 2 Kexueyuan South Rd.
Haidian District Beijing 100190