

CASE STUDY:

GLOBAL ENERGY COMPANY SEEKS HELP WITH SOX COMPLIANCE

BACKGROUND

A global energy and inorganic chemical company deployed the Internet Security Systems (ISS) suite of products to assist in its compliance with Sarbanes-Oxley (SOX) regulations. The ISS suite of products is considered state-of-the-art in providing the security, privacy, and accountability of information that SOX compliance demands.

With locations spanning four continents and approximately \$14 billion in assets, this international company has built an IT infrastructure that is extensive and complex. The company uses ISS Internet Scanner to scan the network to discover what hosts exist on the network and to report on what vulnerabilities exist on those hosts. This solution runs more than 1500 checks on servers, desktops, and network devices against established security policies, performing an extremely comprehensive analysis of this global network. Additionally, the company uses Site Protector, which is part of the ISS management solution, as a repository database to capture all of the event information that it discovers.

PROBLEM

The sheer quantity of event information generated from regular scanning of this massive network was difficult to both interpret and disperse to the appropriate personnel. Company management realized they needed to be able to not only collect the information, but also analyze it and distribute it to the people who needed it. How could the appropriate employees - from analysts and executives to systems engineers - gain access to the information they needed more easily? How could they use the information more effectively to report on network conditions, to remediate problems, to be aware of how well the company was performing to comply with a wide range of regulations?

SOLUTION

The company engaged Accudata Systems to analyze how to access and appropriately utilize this information and implement a solution. The solution became to build a custom Web application designed to gather and analyze the data collected from the ISS suite of products and make it accessible throughout the company from executive management to systems engineer.

Accudata Systems created a solution that made this data comprehensible and accessible worldwide - the **Security Profile Reporting Application**. This application delivers real-time network reporting, corporate-wide, via a Web browser. The **Security Profile Reporting Application** was built on the Microsoft ASP .NET Web development platform using Microsoft SQL Server. This dynamic, Web-based application pulls the vulnerability data into its own database and extracts the data at different levels. This enables all management levels - from executive to IT personnel based on permissions - to drill down into the data by specified criteria and get the information they need to perform their jobs.

Upon accessing the **Security Profile Reporting Application**, a user can choose from three main 'dashboard' pages, each offering a different graphical presentation of data at a high level for the company as a whole. Click through capability allows the drill down into the information for finer detail. Built in a hierarchical design, all data is gathered from ISS SiteProtector and data from other applications.

For example, clicking on the 'desktop vulnerabilities' category on the first page presents information for the entire company. Drilling down shows statistics for each division, all division sites, and ultimately individual office locations.

Access to various types of information is based on permissions, limiting detailed data access to only IT management and staff for example. At the site level, detailed data is presented in a grid display. Clicking on a particular machine presents information on its IP address, location, the problem that was found, and how to fix the problem. So although the global network infrastructure is scanned from corporate headquarters, the people who locally 'touch the box' can use the **Security Profile Reporting Application** to drill down and gain access to the information they need to 'fix the box' at their location.

Using his permissions, an IT manager can access the data collected to trend the scenario of his organization. He can determine if an administrator ID and password is present on every desktop in his office. He can drill down into the data via the **Security Profile Reporting Application**, determine how well his site is doing in terms of how many vulnerabilities exist in his location, and prioritize with his staff the actions they need to take to remediate their situation.

RESULTS

The overall impact of the **Security Profile Reporting Application** has been powerful at this global corporation. Senior management now has access to a real time 'snapshot' of the company's IT security posture. The application brings a high level of manageability and accessibility to formerly disjointed, unmanageable data.

From a strategic level, when corporate executives want to know how well the company is doing as a whole - in terms of managing the global network, assessing its vulnerabilities, or maintaining compliance with a variety of regulations, including Sarbanes-Oxley - they now have access to that data and its analysis. They can say, with a great degree of certainty, how well they are performing due diligence in regard to established policies and conventions.

The Security Profile offers a solution that is:

- **Collecting data in real time** - see exactly what's going on in the current environment
- **Easy to use and customize** - target a variety of levels of management and staff
- **Available globally** - manage security from a Web browser
- **Accessible by all levels** - from executive to IT staff
- **Highly functional** - drill down into the data to gain complete information, locate and remediate issues

Real-time statistics regarding vulnerabilities, spam and content filtering, viruses deleted or quarantined are all readily available, as well as the drill down information needed to manage and mitigate these issues. Senior management can now examine network activity from a high level, measuring it against productivity expectations, legal policy, or bandwidth consumption, for example.

The **Security Profile Reporting Application** enables the company now to perform baselining and trend analysis, analyzing network vulnerability historical data from month to month, helping it comply with the requirements of SOX as well as prove due diligence. The management team can review up-to-date data and put some meaning behind the information, and help to ensure that remediation programs are working.

If information is power, then this global energy producer has a new weapon in its arsenal with the **Security Profile Reporting Application**.