



CUSTOMER CASE STUDY

Vulnerability Management assists with compliance for Hillsborough County

Hillsborough County, situated midway along the west coast of Florida, includes the city of Tampa as its county seat. The County's IT Services (ITS) department provides technology integration and support services to approximately 4,200 clients at over 100 administrative sites. To improve manageability of this large network infrastructure the Hillsborough County ITS team identified five key security and administrative initiatives for 2005. This project encompassed selecting a set of security technologies to ensure compliance with HIPAA regulations, security policies and standards based on ISO17799, and audit findings. Technology implemented in 2005 included network intrusion prevention, patch management, security information management, policy compliance and vulnerability assessment. Facilitating network security and complying with HIPAA regulations lead the County's Information Security team to Rapid7 and NeXpose.

Situation

Before Hillsborough County acquired a vulnerability management solution, ensuring that their over 250 servers were secure and compliant proved difficult for ITS' team of three security engineers. The County's process was to contract with outside vendors to run periodic vulnerability assessment scans. With new security requirements increasing the need for more frequent auditing, they needed an in-house solution. The team identified products that would enable a more proactive process for scanning new and existing systems. The County's security engineers required detailed reports that identified vulnerabilities to be remedied before they could pose substantial risk to the network environment.

To evaluate vulnerability management solutions, ITS defined a set of technical requirements against which to measure selected vulnerability assessment scanners. The desired solution would need the ability to:

- Perform stealth scans
- Support multiple platforms including Windows and Linux
- Schedule routine scans
- Scan multiple platforms, applications and devices
- Support unauthenticated and authenticated scans
- Scan all systems without installing an agent
- Store the reports in a repository
- Perform incremental scans
- Provide future support for wireless protocols

Solution

After testing several vulnerability assessment products, Hillsborough County selected NeXpose, an Enterprise Vulnerability Management solution from Rapid7. David Rippel, a senior security engineer for Hillsborough County ITS, led the process for selecting the software. He states, “Our customers ultimately are the taxpayers of Hillsborough County. Any tool that assists us in better protecting our information assets and frees up available staff hours helps us to keep operating costs low and ensures that we are providing quality service to the citizens.”

After a thorough evaluation and selection process, the County purchased Rapid7’s system stating that NeXpose:

- Is the most accurate at operating system detection. NeXpose is able to enumerate exact software revisions and minor version numbers. This is critical to reducing the number of false positives in a penetration test.
- Provides comprehensive reporting. Scan results are organized for the types of reports and analysis customers need, including a management summary, trend analysis and detailed remediation reports. The Remediation Report has step-by-step directions that provide system administrators information on how to resolve a specific security issue and an estimated duration of how long the work will take.
- Is intuitive and easy to use such that our security engineers were immediately productive with the NeXpose web-based user interface. It's a more natural end-user experience compared to other products and has clearly defined steps for setting up and running a scan.
- Offers flexible licensing based on IP address and supports both the Windows and Linux platforms. Clients are not bound to using unfamiliar hardware found in similar appliance-based products.

Hillsborough County currently uses NeXpose to audit 254 hosts from three scan engines.. “Installing the product is a snap,” said David. “Deployment options are flexible including support for multiple operating systems and distributed scan engines. The web based user interface makes it easy to support scanning from a remote office. NeXpose has given us the foundation we needed to build a strong vulnerability assessment practice.”

Benefits

Although many great features made NeXpose stand out from the competition, Rippel identified four key benefits that made NeXpose the leader:

- NeXpose is very cost-effective. Not only is NeXpose the least expensive product of those which the County evaluated based on a per-node price, it also provides an immediate ROI as it is useful ‘out of the box’ without any customization or intensive training.
- NeXpose saves security and network administrators’ time. More precise vulnerability detection and more accurate reports due to testing for the exposure versus just checking patch levels, reduces the time it takes us to find and fix issues. The software will not only list potential threats and fixes more accurately, but also identify which of the devices are most vulnerable to the threat before the hosts are compromised.
- NeXpose is simple to use. The Security Administrators are able to work with NeXpose without having to constantly refer to user documentation. Configuring and running a scan is straightforward and it has a very instinctive user interface. Thanks to the built-in ticketing and workflow controls, security staff can stay on the same page from initial vulnerability identification until an issue is resolved, streamlining the

remediation environment.

- Rapid7 offers high quality technical support that exceeds client expectations. All requests are taken seriously, acted upon promptly, and the development team will do what it takes to make the product work better for their customers when appropriate.

“Simply put – Rapid7 rocks!” said David. “It’s exactly what we were looking for in our initial evaluation and has not disappointed us. None of the features we wanted in the product had to be customized – they all are available in the standard product.”

NeXpose has already shown a return on Hillsborough County’s initial investment. According to David, “Being proactive about identifying vulnerabilities in our computing infrastructure equates to reduced potential downtime of mission-critical services that we provide for the public. Not having to commit countless staff hours to penetration testing enables us to employ a smaller staff than our peers, based on an administrator to server ratio, which helps to keep operating costs low.”

About Rapid 7

Rapid7 is a leader in vulnerability management and compliance, delivering a single unified solution across an organization’s entire infrastructure. Rapid7 NeXpose helps securities professionals to reduce their attack surface by providing actionable insights into the real threats from vulnerabilities across their entire IT infrastructure. Rapid7 NeXpose is the only solution that provides in-depth coverage of vital Web and database systems in addition to networked devices, servers, and operating systems. The NeXpose A.I. and Reporting Engines synthesize large quantities of raw data to provide direct insight into the vulnerabilities that represent the most risk to the business. From this insight the product delivers a set of prioritized remediation recommendations that help security professionals get protection fast. Organizations, including Black & Decker, Trader Joe’s, Florida State University, the New York Times, and the City of Philadelphia, continually rely on Rapid7 products and services to mitigate risk and remain compliant. For more information, go to www.Rapid7.com.