NopSec vulnerability risk management separates the wheat from the chaff

Analyst: Javvad Malik

16 Oct, 2013

An asset management firm with operations in 16 countries faced the challenge of assessing and prioritizing its IT security for sizeable infrastructure and applications with constrained security staff and resources. Therefore, to separate the wheat from the chaff, the firm reached out to NopSec for help. NopSec's Unified VRM SaaS provided a combination of aggregation, prioritization and decision insights in order to expedite remediation of the vulnerabilities that matter most.

Company name:
Asset management firm (not disclosed)

Activities:
Financial services provider, asset management

Head office:
New York

Number of employees:
2,000

Key suppliers:
NopSec

Early Adopter Snapshot

The well-established institute has been through several transformations throughout its history. As a result, many of the security products in place were handed down from a legacy environment or as part of a tactical fix. For its vulnerability scanning, the firm used Tenable Nessus, with which the security team was very satisfied. However, as IT infrastructure and applications ramped up over the years, two issues emerged. First, the IT security team did not scale up at the same rate the IT infrastructure grew. Furthermore, and more importantly, as Nessus was scaled up to scan roughly 7,000 nodes, the security team found that although Nessus was really good at scanning and generating custom reports, it wasn't really helping the business in remediating vulnerabilities.

The issue was compounded over time because there was minimal cooperation from management or other IT departments. The IT security team would spend considerable time prioritizing vulnerabilities and going through numerous dashboard innovations. However, no matter what view they presented, management was only able to see a bleak picture that painted an insurmountable number of vulnerabilities within IT.

In order to reverse the situation, the IT security department chose to adapt its tactics and pursue a risk-based approach whereby instead of identifying individual vulnerabilities, the department would highlight the overall risk to the business over time. The company chose NopSec to assist in meeting this objective based on its strong record of performance with financial services companies.

Deployment summary

The IT security department started the NopSec Unified VRM deployment on Web applications, and it was immediately favored by the firm's Web developers. The new product allowed them to test and see the results very quickly. Once developers fixed an issue, the tool allowed them to retest and after confirming that the issue was fixed, they could simply mark the ticket as completed within the tool. In essence, the process became much more streamlined and, hence, was adopted across the development teams.

Initially, the firm was able to leverage its existing technology investment by running both products simultaneously. NopSec Unified VRM added to Nessus by providing a view of the data in a more meaningful and productive way. Some education was needed here to illustrate that NopSec Unified VRM was not a vulnerability scanner like Tenable Nessus but, rather, more of a tool with governance, risk and compliance-style capabilities that can take the results of a scan and boil it down into meaningful risk data that businesses could understand. However, when the firm saw that NopSec could do what Nessus had done plus had more capabilities on top of that, it decided to replace Nessus completely.

Because NopSec is priced by subscription instead of by IP addresses scanned, it was attractive and easy to scale up the scanning, and today, Unified VRM undertakes continuous monitoring on 7,000 nodes internally and 30 externally facing Web applications. The firm believes Unified VRM's application logic 'Intelligent Algorithm' works extremely well. It is supplemented with manual checking by NopSec engineers, so the number of false positives is near zero.

Another aspect the company states has been refreshing is that NopSec is extremely responsive to any queries and is open to discussing feature requests. As a result, the asset management firm believes that the capabilities Unified VRM offers is pertinent to organizational needs. An example is the ability to extract reports for audit that can highlight the relevant data.

The firm's security team had always tried to gain stakeholder acceptance to the fact that in order to address the mountain of vulnerabilities, the root causes needed to be fixed, such as securing standard server builds. That point, it says, could never be illustrated with Nessus; however, with Unified VRM, the story is very clear.

Challenges and obstacles

The biggest challenge from a technological perspective was adopting a new approach, which extended beyond pure vulnerability scanning. There was a learning curve for all parties involved, as well as some prep work that was required to discover assets and work out which assets are supported by which processes. Aside from this, the only other challenge was getting stakeholder buy-in and acceptance to replace Tenable, which had been in place for a number of years and, despite some of its drawbacks, was well liked and understood.

Innovation and roadmap

Over the coming months, the asset management firm is looking to expand the use of the Web application module and embed it into the process whenever new Web applications are deployed online to ensure they are all tied together into the vulnerability management process.