Customer Success Story

The Company

e-Commerce

The profiled company is a rapidly growing provider of e-commerce platform, online marketplace and retail fulfillment services to thousands of motivated self-starters.

Using its’ online services, would-be entrepreneurs and fashion designers can upload their personalized designs for clothing and a wide range of other retail items and then create online stores where they market their products to potential buyers. Whenever someone buys a product from one of its’ users’ stores, the company goes about processing the transaction, putting together the order and shipping it to its final destination. The e-commerce specialist also provides store owners with customer support services for their transactions, as well as the opportunity to market their wares on its centralized consumer shopping portal.

The company’s IT director and information security officer is responsible for overseeing all of the company’s internal IT operations, including its security systems and processes. He’s also tasked with helping the company prepare for its mandated compliance audits, including those covering the PCI Data Security Standard. In addition, as part of the firm’s ongoing security efforts, the official is responsible for conducting the company’s vulnerability management operations, including penetration testing.

The Challenge

Like many other e-commerce businesses, the profiled organization has seen its IT security considerations broaden extensively over the past several years as its operations continue to grow and mature, cyber attacks continue to proliferate, and regulatory compliance requirements become more stringent. With fixed IT security staffing resources on hand, the company has found itself in the position of needing to strengthen its electronic defenses and extend its regulatory compliance efforts, without adding to its departmental headcount to do so.

By engaging in automated penetration testing, the e-commerce firm wanted to get a better handle on how all of its networks and applications inter-relate from a security standpoint. It also needed detailed vulnerability data that would allow its IT staff to address any weak points in a timelier, more strategic manner. In addition to lowering its exposure to external attacks and better protecting the sensitive information of its store owners and their customers, the company also sought to ease its regulatory compliance efforts without committing resources to added consulting engagements.

"It only takes one small issue to cause major problems, and often times you see the same configuration flaw or systems vulnerability repeated over and over again across servers and desktops, or even within a single application, creating a security predicament that reaches across the entire organization,” said the company’s IT Director. “Penetration testing using Impact Pro gives us an immediate view on how vulnerable our networks might be, especially when used in cooperation with scanning reports to rule out the false positives and false negatives that those tools produce.”

The Solution

To make the most of his security budget and better align its defenses to protect its customers’ data, while complying with the PCI data security standard (DSS), the profiled company’s IT department decided to move away from using open-source penetration testing frameworks and adopt an automated solution that could expedite the work and translate vulnerability scanner results into actionable remediation data. By running Impact Pro against its Nessus vulnerability scanner results, the organization could quickly move from reactive patching and updating to proactive risk mitigation and remediation.

"Using CORE Impact Pro has allowed us to reduce the amount of time it takes to sort through vulnerability scanner results by 80 percent, giving us the ability to throw out false positives and directly address high-priority exploitable issues. We’re using these results to rethink applications development and re-frame our entire security testing and remediation process.”

Solution Summary

<table>
<thead>
<tr>
<th>CUSTOMER TYPE</th>
<th>Online retail sales and e-commerce platform provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHALLENGE</td>
<td>Improving overall security standing and optimizing internal IT resources via automated penetration testing</td>
</tr>
<tr>
<td>SOLUTION</td>
<td>CORE Impact® Pro, the first comprehensive penetration testing software solution for assessing organizations’ most significant IT vulnerabilities and information security threats.</td>
</tr>
</tbody>
</table>
While the company’s major networks are under close monitoring at all times, using CORE Impact Pro has allowed the company to get a better fix on security issues resident in its many subnets by pushing its penetration tests far deeper into its infrastructure to root out potential problems.

In addition to improving matters of operational security, the IT Director said that Impact Pro has also served as a useful vehicle for illustrating security issues to non-security staff, including network administrators and senior leadership. “At the end of the day it gives you that crucial ability to step outside your network and see what others can see, to test what they can and will test,” he said. “And in terms of illustrating our current security needs to our administrators and executives at any given time, it’s helped provide them with a clearer picture of our overall security posture.”

The Result

Maximizing Internal Resources

Having to serve as both IT director and information security officer at the company forces the official to make the most of his time, especially when it comes to launching in-depth vulnerability assessments of the company’s sizeable network infrastructure. By adding Impact Pro to its collection of solutions, the company was immediately able to get a better fix on where its most significant issues reside to target remediation efforts and keep its staff focused on the most important security work at hand at any given time, without being forced to hire additional workers.

“Using Metasploit or other scripting tools took so much effort that I couldn’t do it all on my own anymore, it took too many hands to do all the work involved,” he said. “Of all the products that I’ve seen, Impact Pro covers by far the most in terms of processes that you want to automate.”

Streamlining Operational Security Processes

One of the major reasons the e-commerce specialist moved to adopt automated penetration testing was its desire to assure that proper security practices were being followed consistently across its operations, specifically within its network infrastructure. As network administrators place significant emphasis on providing uptime and availability of the assets they manage, the company wanted to avoid security becoming a secondary consideration.

Once the company brought in CORE Impact and began running tests against its assets, it became clear that the application of network systems security patches was frequently being delayed to focus on other responsibilities, largely because so many of the patches themselves create operational headaches. As a result of those findings, the e-commerce provider has been able to remind administrators to keep their patching practices up to date and ensure that critical updates are put into place as quickly as possible -- and tested to ensure that they've been applied and work properly.

Demonstrating Security Issues to Others

One of the biggest challenges in today’s enterprise computing environment is garnering continued support from senior executives who have signed off on layers of defensive security and compliance management technologies in the past, and are now being told that they still need to add new staffing and solutions to address their IT-driven risks. Using the results of Impact Pro tests to share findings regarding exploitable vulnerabilities with upper management – showing them exactly which problems could be attacked by outsiders and how – the IT Director said that he’s been able to maintain the attention of his non-technical colleagues, both to advance the cause of security across the organization and to justify continued spending on security solutions and expertise.

Easing PCI Compliance

Another primary reason that the company sought to adopt automated penetration testing was to maintain compliance with the PCI standard between consulting engagements and ease the process of preparing for both voluntary and required third-party security audits. Rather than calling in the consultants and scrambling to fix any problems that they might find several months ahead of an audit, the organization can now maintain a consistent approach year-round, while using the solution to meet the specific pen testing demands established in PCI requirement 11.3. Once the company has gained greater experience in using the technology, the IT Director said that the e-commerce company may decide to altogether replace some of its consulting work with more comprehensive use of CORE Impact Pro.

“Knowing where the economy is right now I’m sure that some people think that buying this type of a product might be unnecessary, but if you look at it from the perspective of cost savings down the road – from the time and money you’d need to test manually or hire PCI consultants – it pays for itself and it’s a no-brainer.”