

THE RISE OF SECURITY TESTING

Why comprehensive security testing is critical to proactive IT risk management

EXECUTIVE SUMMARY

This paper will outline the increasing recognition of comprehensive security testing as a best practice for addressing issues of organizational risk related to vulnerability assessment and remediation planning, identification and validation of exposure to data breaches, assessment of defense mechanisms and policies, and maintenance of regulatory compliance. It is meant to highlight the rapidly expanding scope of security and compliance issues facing organizations in today's computing environment -- and the ability of proactive security testing to address those challenges as the most important element of vulnerability assessment in meeting the shifting expectations of management, customers, business partners, shareholders and auditors.

IT SECURITY IN CRISIS

The emergence of more varied, targeted attack techniques from the malware and hacking communities, combined with growing regulation of organizational security standing -- from both government agencies and private industry watchdogs -- has resulted in a climate in which businesses are increasingly being required to assess their technological vulnerabilities and security defense mechanisms on an regular basis.

Despite many years and millions of dollars invested in the adoption of IT systems defenses, including a litany of technologies installed throughout network and endpoint infrastructure, it has become painfully clear that many organizations are still struggling to protect their assets and sufficiently lower the risk of external intrusion, business interruption and data loss.

In 2007, security researchers charted a record number of data breaches, with 443 major incidents reported in the U.S. alone,¹ along with a staggering number of new malware samples. For instance, anti-virus vendor Symantec recorded 711,912 unique threats during the course of the year, a 468 percent increase compared to 2006.²

And early indications are that 2008 will see even higher levels of malware proliferation.

Driving this staggering malware proliferation was the growing adoption among cyber-criminals of cutting-edge server-side polymorphism threat design methods meant specifically to defeat today's latest anti-virus technologies by creating nearly endless variants of themselves and using a wide range of other techniques to evade behavior-based monitoring systems.³

A growing percentage of the threats were crafted with specific groups of end users in mind, adopting sophisticated social engineering techniques such as "spear phishing" to go after smaller pools of targets, or even individuals, by luring those people to click on malware-infested attachments or Web links and subsequently infect their machines.⁴

At the same time, approximately 40 U.S. states⁵ have enacted data breach notification laws that require companies experiencing intrusions or accidents that lead to any exposure of sensitive information to disclose their incidents publicly.

As a result, regulators, both public and private, have increased scrutiny of organizations' IT security status, introducing new measures -- such as the Payment Card Industry's Data Security Standard (PCI DSS), backed by the world's largest credit card providers -- and tightening enforcement of existing laws -- including the Health Insurance Portability and Accountability Act (HIPAA), initially passed by the U.S. Congress in 1996 -- that compel organizations to proactively assess and test their systems defenses.

Yet, even the adoption of those stricter IT security standards has not prevented companies following the measures from being exploited or experiencing data loss.⁶

One could easily argue that organizations have never before faced a more diverse ecosystem of potential IT security, data protection and compliance risks.

¹ Identity Theft Resource Center (ITRC) Status Report, Dec. 2007

² Symantec "Internet Security Threat Report Volume XIII," April 2008

³ "Malware vs. anti-malware, 20 years into the fray," Computerworld, May 2008

⁴ "Spam more creative, better targeted," Government Computer News, May 2008

⁵ Consumers Union Status Report, August 2007

⁶ "New credit card breach will test PCI," InformationWeek, March 2008

THE MAJOR SHORTCOMINGS OF TRADITIONAL SECURITY MEASURES

Despite decades of investments made in security point products, from traditional endpoint and network anti-malware systems to emerging technologies including data loss prevention (DLP) tools, the reality is that many organizations are still woefully vulnerable to attacks and information leakage.

Research has proven, and even leading security vendors have recognized that most popular desktop and network anti-virus systems are being circumvented by a large percentage of these targeted, polymorphic attacks⁷ and that technologies such as DLP remain far too nascent to employ successfully on an enterprise scale.⁸

Organizations have installed layers of security infrastructure, but remain challenged to get disparate products to communicate with each other or provide staffers and managers with a structured, centralized method for reporting on the efficacy of network and endpoint defenses, and end-user training programs.

One of the most significant and widely-voiced challenges on today's IT security landscape is the seemingly insurmountable task of sorting through the vast amounts of data produced by traditional defense mechanisms, and even some newer security management and vulnerability scanning solutions.

Ubiquitous technologies including firewalls and intrusion detection/prevention systems (IDS/IPS), and newer security event/information management (SEM/SIM) systems provide organizations with volumes of information related to their security status and attempted hacks into their IT infrastructure.

Even with the continued advancement of those point products, most workers using the systems struggle to sift through the reams of data generated by the technologies to root-out false positives and isolate where their most significant strengths and weaknesses lie.

This problem also poses a secondary business challenge to IT security managers who must explain to their CEOs, CIOs and other executives why the investments that their organizations have already made in security technologies have not served to adequately address all their risks.

Perhaps even more frustrating, this scenario often makes it harder for IT security managers to defend future spending on additional tools meant to augment their existing defenses, based on the perception that the products they have in place aren't doing the job, or even based on a level of overconfidence related to the capabilities of those mechanisms.

With a robust, diversified ecosystem of defensive technologies already in place, organizations are still fighting to ward off attacks, meet the requirements of individual regulations, and most importantly, gain a clear level of visibility into their overall security posture.

It is increasingly evident that what has been missing from this picture is a method for assessing vulnerabilities, measuring the efficacy of security systems and validating related investments.

THE SCOPE OF SECURITY TESTING

All of these aforementioned problems play directly to the strengths of integrated testing technologies that aim to provide security and compliance management professionals with a more comprehensive view into an organization's overall security standing.

Just as civil engineers are required to conduct regular inspections to ensure that time and the elements have not eroded the stability of their constructions, architects of IT infrastructure are

⁷ Yankee Group report "Herd Intelligence Will Reshape the Anti-Malware Landscape," Dec. 2007

⁸ "Data-leak security proves to be too hard to use," InfoWorld, March 2008

increasingly being ordered to conduct more frequent reviews of the networks, devices and users for whom they are responsible to protect against the existence of potential security gaps.

In direct response to this challenge, a wider variety of commercial-grade security measurement technologies have been introduced to help organizations assess their IT systems and policies on an ongoing basis to determine where their strengths and weaknesses lie.

The promise of these IT security assessment platforms is roughly the same as the manual processes employed by construction engineers to validate the reliability of their physical structures. Some of these testing technologies can be used to search for a broad range of potential issues across variety of different assets, while others are targeted in nature and focus on addressing specific aspects of individual systems.

Many IT product vendors have also begun building onboard diagnostic capabilities into their products to help customers ensure that their security systems are functioning properly. But this model has fundamental shortcomings, as these testing capabilities are typically designed to ensure that the products they live in operate smoothly -- and perform only the most rudimentary of status checks, rather than aggressively seeking out a full range of potential security risks.

As such, experts have recognized the need for testing capabilities delivered independently of other technologies to provide the most comprehensive and objective view into potential risks.

Three different types of independent vulnerability assessment systems in particular are being adopted by large numbers of organizations to help address the need for more frequent, repeatable self-inspection:

- **Source code analysis** systems aim to help developers locate vulnerabilities in the underlying code of software programs and applications before they are put into production.
- **Vulnerability scanners** are used to find and report flaws in networking infrastructure, as well as both live and pre-production applications, to identify potential weak points or improper configurations.
- **Security testing** systems emulate real-world threats to help organizations safely expose vulnerabilities and assess the efficacy of security infrastructure and policies to mitigate operational risk by prioritizing response efforts.

IT industry analysts, compliance auditors and adopters of all these technologies have recognized publicly that the vulnerability assessment and testing capabilities that they offer provide real-time metrics that offer true visibility into different elements of organizational security posture.

For example, as part of the PCI DSS standard -- which requires that all businesses processing credit or debit card transactions provide acceptable levels of electronic data security -- payment card industry regulators have required that such companies engage in active systems and application testing⁹ -- including all three flavors of assessment listed above -- to help lower the risk of information exposure.

In recently published reports, industry analysts¹⁰ have predicted that significant numbers of organizations will begin conducting more aggressive assessment, specifically vulnerability testing, on an ongoing basis, to help gain the information needed to prioritize and mitigate risks, gain visibility into the performance of IT security systems, and meet the requirements of external assessors.

The many proponents of IT security testing systems, including many large organizations operating in highly-regulated vertical segments, have reported that ongoing use of the technologies has markedly

⁹ PCI Data Security Standard v1.1, Sept. 2006

¹⁰ Gartner Case Study: "Penetration Testing Tool Use," April 2008

improved their ability to garner actionable data critical to address their security issues, and identify and prioritize risks.¹¹

Organizations that do not engage in proactive security testing are increasingly being viewed as laggards who have failed to adopt a critical IT best practice by everyone from industry watchers to business partners and customers.

And though many organizations have traditionally hired external consultants to come in on annual, or bi-annual engagements to conduct their security testing, more experts than ever are viewing ongoing, automated assessment as the best manner of supplementing that work and providing organizations with a way to gauge their defenses on a more frequent basis.¹²

Testing systems can also provide consultants with a tangible baseline from which to launch their own assessments, with many professional services companies using the products to do so themselves.

The technologies are being cast by a broad range of experts as the most effective way to monitor vulnerabilities on a regular, repeatable basis to gain an understanding of whether security efforts are meeting their goals.

Based on those factors, all signs point to widespread adoption of IT security testing technologies today, and in the future, based on the reality that such work is rapidly becoming entrenched as a fundamental best practice and the most critical element of vulnerability assessment.

Even further, it would appear logical that integrated security testing systems that cover the widest possible range of assets, or that can be easily married with other similar technologies, represent the promise of a future where organizations are no longer left wondering where their most significant risks lie and will instead perform their own proactive analysis to understand where they stand at any given point in time.

COMPREHENSIVE TESTING WINS OUT

While all breeds of vulnerability assessment systems promise organizations the ability to gain a firmer grasp on their current weaknesses -- along with an opportunity to use results to defend staffing and monetary investments -- only integrated, multi-tiered testing across networks, endpoints, applications and end users provides companies with a comprehensive, centralized approach to IT systems defense and risk management.

Unlike source code analysis tools, which only address the software development process, or vulnerability scanners, which provide organizations with long lists of potential weak points, comprehensive security testing software solutions arm users with actionable data on their most significant risks, allowing them to address their most serious issues immediately.

Many assessment platforms allow organizations to explore and isolate potential weaknesses, as in the case of standalone Web application vulnerability inspection systems, but only integrated security testing offers organizations the ability to repeatedly gauge their real risks and target remediation efforts across the entire scope of IT operations, from hard assets to issues of end-user policy adherence.

Many vulnerability assessment technologies offer organizations an ability to meet specific elements of individual compliance mandates, but only a handful have been added to the explicit requirements of those measures, as in the case of security testing solutions in Section 11.3 of the PCI Data Security Standard.¹³

¹¹ Aberdeen Group "Application Security Report - User Survey," May 2008

¹² "Penetration Testing: Assessing your overall security before attackers do," SANS Institute, June 2006

¹³ Information Supplement: "Requirement 11.3 Penetration Testing," PCI Standards Board, April 2008

Beyond those specific requirements, testing systems also help organizations prove the viability of their broader compliance efforts across the entire range of defense mechanisms and policies, with auditors increasingly accepting use of the technologies as a form of proof of recommended practices.

And legal experts studying the impact of high-profile data breaches -- such as that experienced by TJX Companies, for which the retailer has already agreed to pay \$65 million¹⁴ in settlements while facing additional litigation -- have suggested that many courts may soon see comprehensive security testing as an admissible form of due diligence, even for businesses operating outside the scope of regulations that require them to do so.

The confluence of more complex threats, stricter compliance regulations and the information glut produced by traditional security systems has paralyzed many organizations and left their leaders conflicted about what their next investments should be, and how to defend the expense of such acquisitions to other executives.

IT security managers demand sources of more readily-available, high-quality information that allows them to stay ahead of potential problems and reduce the likelihood that they will need to launch painful, time-consuming investigative and remediation efforts after they have been exploited.

IT buyers are demanding technologies that address as much of their operations as possible and that can be rolled out quickly, versus those existing in "silos," or that take years to install, integrate and prove their value.

Moreover, security, compliance and line-of-business executives are looking for products that will help them reduce potential security, legal and regulatory risks both today and in the future, and help illustrate the veracity of their ongoing efforts to improve the state of their defenses.

As scrutiny of IT budgets and regulatory compliance continues to increase, along with third-party forensic investigations of major intrusions and data loss incidents, comprehensive, systems-independent testing will increasingly be seen as a requirement for all responsible organizations, and the best method for proving adherence to commonly accepted security practices.

Comprehensive, independent security testing software solutions offer organizations the most effective method of exposing their critical vulnerabilities, mitigating operational risk and assuring the effectiveness of their security efforts.

The era of proactive security testing is now.

CONCLUSION

Organizations that truly desire to do the best possible job of protecting their IT assets and sensitive data must ask themselves a battery of important questions, including:

- "Do we have a firm grasp on our most significant risks and vulnerabilities, and how frequently are we assessing these issues?"
- "If we were targeted with an attack, would we be able to prevent it, and could we even detect it?"
- "How do we know if our existing security systems are functioning effectively and delivering return on investment, and how do we gain better visibility into this?"
- "Are our employees following security policies and procedures, are those rules sufficient in their makeup, and how consistently do we enforce them?"

¹⁴ "TJX completes Mastercard breach settlement," Securityfocus.com, May 2008

- “Will industry or government regulations change the manner in which we protect our IT assets and electronic data, and how must we prepare for this likelihood?”

In consideration of all these critical questions, organizations that are truly committed to proactively meeting the changing dynamics of the security and compliance landscape must ask themselves how comprehensive, independent security testing will improve their overall standing and rapidly move to adopt such technologies.



For additional information on CORE IMPACT, please contact us at 617-399-6980 or via email at info@coresecurity.com. You can also visit our web site at www.coresecurity.com.