WHITE PAPER: ENTERPRISE SECURITY

Threat and Vulnerability Management Plan

Volker Rath
Technical Lead, Consulting Services, EMEA
Symantec Security Services

December 2006

White Paper: Enterprise Security

Threat and Vulnerability Management Plan

Contents

Threat and vulnerability management today

Dealing with threats (viruses, worms, DoS attacks, etc.), vulnerabilities, exploits, and patches is a part of the daily business of every company today. Everyone, from the average user to C-Level management, knows that Internet threats can become a serious problem when they pass through perimeter protection (firewalls, AV scanners) and have the chance to infect the internal network, which typically has few barriers. The result is often the loss of availability, integrity, and confidentiality, which results in downtime. This translates into business disruption in the form of money and productivity loss. And if customer data is affected, it can also mean a loss of confidence by customers.

To keep the business up and running and to comply with industry and government regulations, companies try to do everything they can to protect against threats and attacks that target vulnerable points in their technology. The aim is the reduction of risk to an acceptable level while understanding that it is impossible to be 100% "bulletproof."

Because of the complexity and the number of different technologies that are used in the IT environment, each network or system administrator is responsible for rating threats and vulnerabilities, making appropriate decisions, and implementing remediation plans.

As a result of this localized defense strategy, stakeholders in the organization have the freedom to react to threats as they see fit. The outcome is often an inconsistent level of protection that can't be supervised or measured from a central point. Risk reduction cannot be measured because it is impossible for the CIO to know if all remediation efforts are sufficient, complete, and have been implemented in a timely fashion.

In day-to-day business, it is hard to find the right balance between availability and security. Security intelligence systems such as Symantec DeepSight™ help customers focus on the most important threats. These systems provide customers with in-depth information on threats and vulnerabilities with optional filters for the appropriate technologies. Nevertheless, the sheer mass of newly issued and updated vulnerabilities and threat information can overwhelm administrators and keep them from reacting effectively, especially if there are no repeatable processes and workflows built in to help prioritize remediation efforts.

Protection is a speed game

The undifferentiated mass of security information is just one problem. Another is the speed of the lifecycle of threats. The following graph shows an example of a typical threat lifecycle:

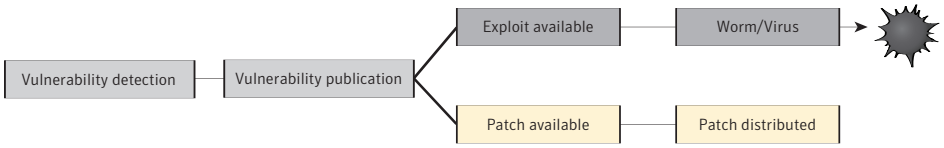

Figure 1. As exploits are disseminated sooner and sooner after a vulnerability is announced, it becomes more and more important for organizations to roll out patches quickly.

The critical time windows that can be influenced are the following:

1. Time between the patch issue date and knowledge that a patch is available
2. Spread of knowledge to all responsible people
3. Test of the patch
4. Rollout of the patch

The main challenge is the speed factor. Average exploit development time today is approximately 6.8 days after the published date of the vulnerability. Furthermore, in many cases, vulnerabilities are published by vendors only after a virus or worm is detected in the wild.

During the second half of 2005, 49 days elapsed on average between the publication of a vulnerability and the release of an associated patch. Most of the time, very critical patches were available much faster because of the potential risk or the existence of an exploit code. Most real harmful threats, critical patches, and remediation tactics are distributed within a very short time frame.

For example, the Zotob worm is based on one vulnerability that was published on August 9, 2005. The first exploit code was published three days later, and Zotob was discovered two days after that with backdoor and worm characteristics. Many people were not aware that Zotob changed subtly over its life span. After 15 mutations, the worm mutated again on January 20, 2006, into a second vulnerability with new functionality that allowed for the download of malicious code.

Threat and Vulnerability Management Program—the Symantec approach

Neither a bundle of tools nor a static predefined process is able to provide the reaction time that is necessary to reach the highest possible level of protection and an acceptable level of risk. Symantec has developed its Threat and Vulnerability Management Program (TVMP) to provide customers with a customized framework built on people, process, and technology. TVMP helps organizations collect, process, and prioritize security intelligence and assess it against the assets in their environment and their unique risk posture. This allows customers to proactively combat threats and vulnerabilities before they become incidents. The service helps minimize the business impact of potential incidents while strengthening an organization's security posture and supporting its compliance goals

The TVMP framework covers all steps of a professional threat and vulnerability management plan. Although this basic structure applies to all organizations regardless of company, industry, or technology that is used, the framework itself is flexible enough to be adapted to individual needs.

The aim of TVMP is to design and implement a best-of-breed framework optimized to customer needs and individual requirements. Symantec's consultants can play a major role in the following project phases:

- Analyzing the individual IT environment
- Analyzing existing processes and experiences
- Setting up the Threat and Vulnerability Management Team
- Designing the framework
- Implementing the framework
- Customizing tools and solutions
- Training
- Building awareness
- Advising on risk estimations for threats and vulnerabilities onsite

The project phases

Assessment phase

Symantec Threat and Vulnerability Management Program begins with an assessment of the customer's environment. If necessary, Symantec consultants first begin with an assessment of the assets that require protection. Once the assets are identified, they can be evaluated for vulnerabilities. The assets are then prioritized based on criticality to allow for a customized response to threat and vulnerability intelligence.

After assessing and prioritizing the assets to be protected, Symantec consultants then assess the organization's existing threat and vulnerability framework. They evaluate what intelligence data is collected, how remediation is performed, what resources are involved, escalation paths, metrics, reporting, trending, and benchmarking, if any. Symantec consultants do this by interviewing key staff on the customer's security and operational teams. Symantec consultants then investigate the customer's existing threat and vulnerability management mitigation and remediation process and review design documents associated with the process as well as any technologies used. Symantec further reviews the customer's business requirements to identify the business drivers, service capabilities, and specific areas of security concern.

Upon completion of this phase, Symantec will deliver a Threat and Vulnerability Management Program Assessment Report, which contains the following modules:

- An Executive Summary, including a high level summary of the analysis and findings and a prioritized action plan for remediation
- A Management Summary, including objectives and process information
- An assessment of the threat and vulnerability management program currently in place compared with best security practices
- An analysis of process issues found and their implications for the customer's overall security posture, with recommendations for remediation
- A prioritized list of recommendations intended to enhance security and reduce risk

Design phase

Armed with Symantec Threat and Vulnerability Management Program Assessment Report, Symantec consultants leverage best practices gained through numerous security engagements performed on behalf of customers ranging from small enterprises to Fortune 100 clients. Symantec consultants work closely with the customer to design a Symantec TVMP Framework customized to their organization.

Symantec consultants will design a process that offers an optimum level of protection to meet the customer's business needs, balanced with the customer's budget and risk tolerance. At the end of the design stage, the customer is presented with a Threat and Vulnerability Management Program Design Document.

The major principle of the program design is to make sure that all activities are a part of the security lifecycle that assures a constant level of protection to keep the risk level low.

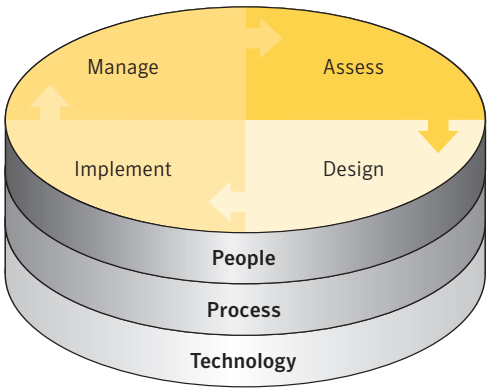

Figure 2. Proactively protecting systems and data requires a multidimensional, multistage approach such as that provided by Symantec Threat and Vulnerability Management Program.

Implementation phase

Once a design has been agreed upon, Symantec works closely with the customer to implement the TVMP Framework, making every effort to maximize the customer's existing resources. During this phase, Symantec customizes the included toolset to the customer's specific needs. The deliverable for this stage is a Threat and Vulnerability Management Program Project Plan.

Monitor phase: security intelligence, analysis, and reporting

Symantec Threat and Vulnerability Management Program includes security intelligence drawn from Symantec's Global Intelligence Network, the same intelligence used by award-winning Symantec DeepSight Alert Services. This security intelligence provides early warning of potential security threats and the latest information on vulnerabilities and malicious code.

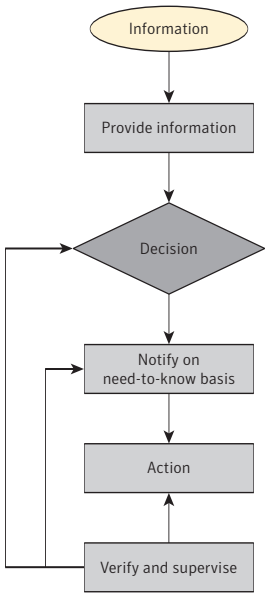

Figure 3. The monitoring phase combines solid security intelligence and information intelligence tools with proven decision-making processes.

To be able to analyze and prioritize the security intelligence, Symantec TVMP comes with a powerful tool—the Threat and Vulnerability Management System (TVMS). TVMS, a tool developed by Symantec Consulting experts, is adapted to each customer's individual environment. The technology is open source and allows the building of connections to other technology (e.g., ticketing systems).

Threat and Vulnerability Management Program Framework

Once the consulting engagement is complete, Symantec will have developed a customized Threat and Vulnerability Management Program Framework tailored to each customer's environment and needs. This framework will allow customers to find, capture, and process all the critical information necessary to mitigate threats and vulnerabilities.

Information gathering

The initiation of the remediation process always relies on the security intelligence. To manage information means having the information in a structured format, which allows modification and the addition of comments and individual ratings. To enable that ability in the TVMP framework, the intelligence data comes in the form of an XML data feed.

Decision-making

One of the weakest points in most threat and vulnerability management processes today is the decentralized decision model. The basic theory behind this model is that implementing security measurements is a part of the job of people whose primary responsibility is providing and guaranteeing the availability of IT systems and infrastructures. The net result of that approach is that it gives rise to a conflict of interests. Do resources invest time in security or in availability? When manpower is limited, security is often a "pain in the neck" for administrators because of its complexity and the necessity to invest a lot of time to stay up-to-date every day.

For example, a worldwide operating company with sites in America, Europe, and Asia is running Windows® systems in each location. A critical Windows core system vulnerability affects all systems: workstations, notebooks, and servers. Each site has different administrators for the different types of systems, and each administrator is responsible for deploying all necessary security patches in his area. Although all administrators have a subscription to a security intelligence service like Symantec DeepSight, the individual risk estimations and reaction times are very different. Because of the worldwide-connected network, each vulnerable system has the ability to harm the rest of the company's systems. Unprotected systems can be infected and damaged by others abroad, and network traffic caused by infected machines can potentially bring the network down.

A much better way to manage the decision-making process company-wide is the implementation of a group that defines proper risk estimation for each vulnerability and threat: a Threat and Vulnerability Management Team. This team is responsible for defining adequate risk ratings and their corresponding measurements. One enterprise can have several local teams, but all of them

have a strong relationship to other teams in each technical department (e.g., client/server administration, network administration, firewall administration, etc.). This is necessary to ensure that all decisions are made by people with the best possible competence in each of the critical areas.

Because risk estimations and classifications with associated actions are made from a central place, network and system administrators can rely on a small number of advisories with high impact. They don't have to comb through a morass of security-related messages and emails looking for the information that is pertinent to them, and they don't have to make decisions about appropriate actions and reaction times. Centralized decision-making also has the added benefit of making the process transparent and auditable.

Notification on a need-to-know-basis

Reliable notifications about threats and vulnerabilities are needed everywhere in an organization. But what is the value of actionable information if it is hidden in a flood of information that is not of any interest? The TVMS ensures that the information routed to stakeholders fits the technologies they are responsible for. With a risk rating and the defined action for each threat and vulnerability defined by the TVM team, information can be relied on.

Information management

To provide detailed and well-structured information to all people that are part of the information management process, the XML data feed is imported into an SQL database with a powerful and easy-to-use HTML front end: the TVMS. This solution is used to store and visualize all threat- and vulnerability-related data and is a management solution that reflects the individually defined process of each customer. Depending on the role of the user, the TVMS allows for powerful searches, adding information and individual risk ratings to each vulnerability, definition of technology lists to reduce the mass of information and a full set of reports and statistics.

One of the biggest advantages of the XML data feed compared with the email-based security intelligence delivery method of other intelligence feeds is that all threat- and vulnerability-related information is also available offline in the local TVMS database. Today there are more than 16,000 vulnerabilities and approximately 6,500 malicious code variants in the database—all with detailed in-depth information. The TVMS acts a knowledge-based system with very powerful search functions. For example, if a firewall administrator wants to know which threats are using port 6000 or a system administrator is looking for the latest security patches of a particular software, the TVMS database can quickly provide detailed and reliable information for all kind of vendors, products, and technology.

Threat and Vulnerability Management System

Extended view on the data

The TVMS provides a well-structured, in-depth view into threat- and vulnerability-related data. Flexible search functionality enables quick and easy access to all the important details needed. A list of exploits and fixes per software or vulnerability is simply one of many unique features.

Supporting the process

The TVMS is the first system that allows customers to download full security intelligence data from a security information provider and customize it for each organization by annotating it with information (ratings, comments, assignments). It is a management framework that supports most parts of the threat and management process and is open to the integration of many tools and solutions that are needed to support the full process—starting with incoming new information and ending with remediation.

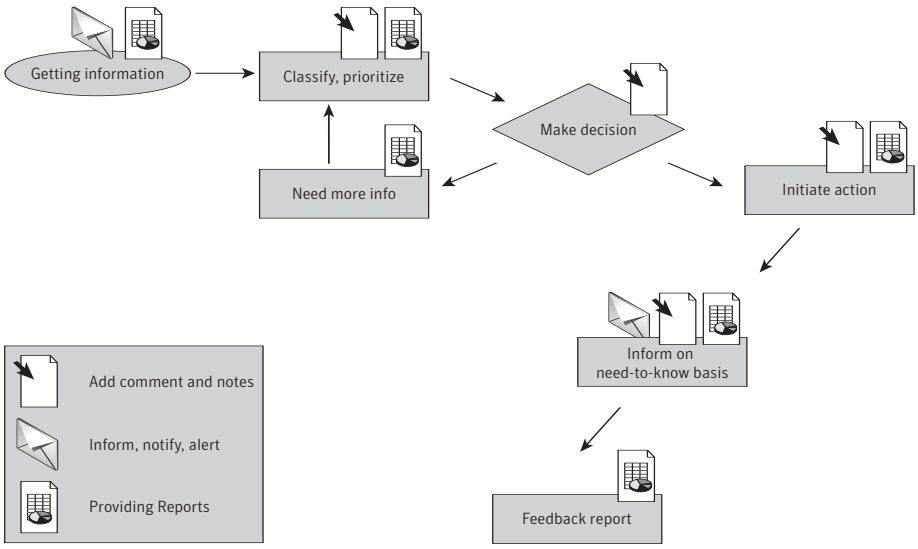

Figure 4. Symantec TVMP offers customizable options for annotating, distributing, and reporting on threats and vulnerabilities.

Role based model

The TVMS allows for different user roles:

- The TVM Officer, who has an eye on all technologies of the organization and performs the risk estimation together with experts for all vulnerabilities.
- The Service Provider, who has a filtered view adjusted to the technology she is responsible for. She also gets security advisories and remediation tasks from the TVM Officer and additional notifications from the system.
- The Manager, who is typically the CISO, gets valuable reports that make the process transparent. He can check that all remediation plans are consistent in all areas.
- The TVMS Administrator, who maintains the TVMS, adds and removes users and verifies the logs.

Individual view of data

All views and reports are available in filtered and unfiltered formats. The filtered format only shows vulnerabilities, exploits, fixes, and other data that are pertinent to the role defined in the technology filter settings. Unfiltered views, with powerful search options, are available for all system users.

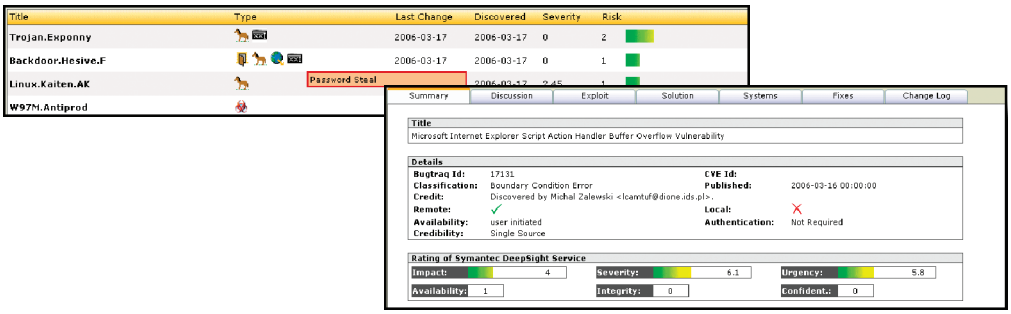

Figure 5. Views and reports can focus on the information required by certain people, or left unfiltered to provide comprehensive data.

Reports and statistics

Daily security reports, statistics about threat progression, and available fixes by product are just some of the reports available through the TVMS.

All notifications, reports, and statistics are always up-to-date owing to continuous updating of the TVMS database by the Symantec DeepSight data feed.

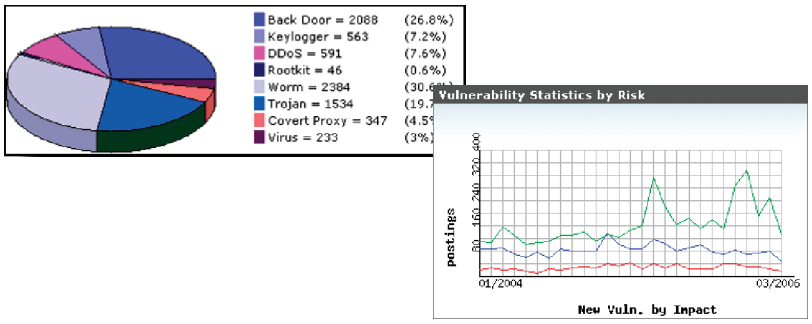

Figure 6. A wide range of graph and chart styles is available to make TVMP data easily understandable.

Symantec Threat and Vulnerability Management Program represents a best practice

The aim of Symantec TVMP is to help move organizations from a reactive to a proactive approach with respect to dealing with threats and vulnerabilities. Symantec's proposed workflow helps make the threat and vulnerability process more transparent, more reliable, more effective, and faster. Symantec TVMP helps to implement a constant high level of protection by ensuring that security measurements are consistent across departments, divisions, and sites.

TVMP helps organizations protect against threats based on intelligence gathered both internally and externally, then applying expert analysis and providing customized, prioritized actionable information available to people along the command chain. This proactive and preventive approach is increasingly important as both the number of vulnerabilities and industry-specific attacks are increasing year over year. In addition, TVMP, which could also be seen as an incident prevention program, helps to protect every part of a corporate infrastructure, regardless of technology deployed, ownership, or physical location.

About Symantec Consulting Services

Symantec Consulting Services has helped IT teams from over 95 percent of Fortune 500 companies enhance and maintain the security and availability of their information and infrastructures. With more than 900 consultants worldwide, we provide consulting services in 60 countries and participate in over 4,000 engagements per year. Our consultants possess an average of 15 years of experience in security, storage, and availability technologies across all major operating systems, storage hardware, and application environments.

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

12/06 10753677