WHITE PAPER: SECURITY MANAGEMENT

Best Practices for Implementing a Security Process

Symantec.cloud

White Paper: Security Management

Best Practices for Implementing a Security Process

Contents

Introduction

There is no doubt that the cyber security threats facing organizations today are enormous. At the same time, many organizations believe that improving security technology is the answer to solving the complex security challenges of today. Security technology has evolved from static firewalls and anti-virus products to full suites of tools that are building up, layering on and overlapping security measures that are very effective in protecting against the modern threat. Unfortunately, without a solid process backing up the implementation of technology, organizations will still find themselves susceptible to emerging threats. This paper will look at aligning security processes, the human element of security, with the latest security technologies – creating a secure barrier against today's most insidious threats.

Technology without Process Equals Insecurity

Criminals are more sophisticated than ever before. Shortened URLs, targeted Trojans, and viruses embedded in common documents make protecting businesses from these modern threats extremely difficult. In 2009, 90.6% of spam contained a URL, or hyperlink, driven predominately by an upsurge in the second half of the year of using shortened URLs in spam campaigns. These shortened URLs helped disguise the true website that the user would be visiting and made it harder for traditional anti-spam filters to identify the messages as spam. URL-shortening is frequently used on social networking and micro-blogging sites and is popular among online criminals because of the inherent trust relationships that exist between users of these sites.[1]

Attackers have used everything from news events such as Michael Jackson's death to the recession to the World Cup to entice end users to click on malicious links posted on forums or in blogs.[2] By acting as legitimate commenters or posters on blog sites, criminals are finding it easier to lure unsuspecting users to malicious websites.

In addition to malicious websites, the malicious software infecting end users is very dangerous. The most common spyware on the Internet is generic software that captures everything typed into a computer. This puts banking information and passwords at risk. Unfortunately, that is not the only risk to users. Instead of just stealing money from compromised banking account logins, criminals are able to sell email accounts and social networking credentials. The login credentials for social networking sites and email accounts are sold to cyber criminals who use them to distribute spam and other malware. Twitter accounts are now being sold for $1,000 USD.[3]

The amount of malicious content coming in through an organization's gateway is staggering. In 2009 there were 107 billion spam emails sent on a daily basis.[4] Those spam emails, paired with a growing number of targeted Trojans, significantly increase the risks to businesses. In the first 5 months of 2010, malware levels never rose above 3 percent of all spam, even on days when malware spam increased. In June 2010, however, malware spam made up almost 12 percent of all spam.[5]

Surprisingly, simple spam techniques are still effective. Three of the most common subject lines used by spammers include a blank subject line, "Outlook Setup Notification" and "Reset your Facebook Password." It only takes one employee visiting a site hosting malware or opening a single infected document to open up the entire organization to attackers.

1-MessageLabs Intelligence: 2009 Annual Security Report
2-MessageLabs Intelligence: 2010 Predictions
3-http://www.thenewnewinternet.com/2010/06/23/twitter-accounts-hacked/
4-MessageLabs Intelligence: 2009 Annual Security Report
5-Symantec's State of Spam & Phishing Report, June 2010

Given the dynamic threat landscape, it is no wonder that desktops, laptops and servers are vulnerable to attacks from the web and through email. But that is not where the threat ends. Here are just a few examples illustrating the extent to which criminals are going to steal information.

In June 2010 a variety of new mobile viruses was discovered by researchers. These viruses carried subject names like "Free World Cup VOD" and leveraged other hot topics to sound convincing. These viruses were embedded in mini mobile games to lure users to download. Once downloaded, the virus originator had complete control of the device.[6]

Federal prosecutors that have filed a case against 5 individuals who are accused of trying to steal over $450,000 from the city of Carson's bank account. The criminals used stolen login credentials to attempt to transfer the money from the city's accounts to unnamed co-conspirators. The cyber criminals were able to steal the login information through a key logger program that was installed on the laptop of a city official. Officials still do not know how the malware was installed and who downloaded it. The city was able to recover all but $44,000 of the stolen funds.[7]

Just recently, Olympus Japan has issued an apology for distributing digital cameras with malware-infected internal memory cards. An estimated 1,700 Stylus Tough 6010 digital compact cameras were shipped with pre-infected memory cards. The malware does not pose any problems for the camera itself but instead uses the USB connection to infect computers when the camera is hooked up. In other words, users are at risk of infecting their Windows computers with the auto run worm when they plug the device into their USB drive.[8]

Because of USB drives and other portable storage, organizations are still not safe from accidental or intentional internal infection. Common documents have become the vehicle of choice for malware, as seen with the malware-laden PDF documents. Additionally, a single infected USB stick could infect an entire organization, stealing data, passwords and account information and sending it to a malicious attacker in another country.[9]

The growing mobile workforce has employees working not just from home, but from coffee shops and on other insecure public networks. Mobile devices can be infected in many ways including email, MMS, external memory cards, PC synchronization, unsecure VPN and even via Bluetooth. With an increased uptake of mobile devices, the risks to business reputation, communication and continuity are becoming more serious and the need for good processes is required.

Key Areas for Security Process Evaluation

Getting started on security process evaluation is a major challenge for many organizations. There seems to be an overwhelming number of areas to look at and some organizations may not have the experience or expertise to know where to begin. In order to help address this challenge, the following is a list of the most critical areas that organizations should begin evaluating for formal processes.

Information Security Governance

According to the Information Systems Audit and Control Association (ISACA), the goal of Information Security Governance is to "Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations."[10] In other words, is information security a part of

6-http://www.telegraph.co.uk/technology/apple/7872836/Hackers-target-Apple-iTunes-App-Store.html
7-http://www.thenewnewinternet.com/2010/06/01/bank-robbing-for-the-21st-century/
8-http://www.thenewnewinternet.com/2010/06/09/company-distributes-malware-infected-cameras/
9-Radcliff, Deb "Slurping the USB Port" SC Magazine September 1, 2008
10-http://www.isaca.org

the daily operations of the organization? Processes related to information security governance include access control, regulatory compliance, and communication with upper management on security issues.

The organizations listed below provide valuable information on specific standards or examples of security governance standards:

International Organization for Standardization (ISO): This is a consortium of national standards institutes from 157 countries. The ISO is the world's largest developer of standards.

The USA National Institute of Standards and Technology (NIST): This is a non-regulatory federal agency within the U.S. Department of Commerce. The NIST Computer Security Division develops standards, metrics, tests and validation programs as well as publishes standards and guidelines to increase secure IT planning, implementation, management and operation. NIST is also the custodian of the USA Federal Information Processing Standard publications (FIPS).

The Internet Society: This is a professional membership society with more than 100 organizations and over 20,000 individual members in over 180 countries. It provides leadership in addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). The ISOC hosts the Requests for Comments (RFCs) which include the Official Internet Protocol Standards and the RFC-2196 Site Security Handbook.

The Information Security Forum: This is a global nonprofit organization of several hundred leading organizations in financial services, manufacturing, telecommunications, consumer goods, government, and other areas. It provides research into best practice and practice advice summarized in its biannual Standard of Good Practice, incorporating detailed specifications across many areas.

Change Management

Change management is the process around how changes are made in an organization. Without a formal change management process in place, an organization is at the mercy of anyone who has the rights to make a change. By putting a formal process in place, an organization ensures that changes are only made with appropriate sign off. This helps ensure that multiple parties are aware of any changes being made to the organization's infrastructure.

Any change to the information processing environment introduces an element of risk. Even simple changes can have unexpected effects. In the most extreme cases an organization could be held hostage by a single individual. This scenario occurred in San Francisco when a disgruntled administrator changed and subsequently refused to divulge the administrator password to city computers.[11]

Change management is a tool for managing the risks introduced by changes to the information processing environment. Part of the change management process ensures that changes are not implemented at inopportune times when they may disrupt critical business processes or interfere with other changes being implemented.

Not every change needs to be managed. Some kinds of changes are a part of the everyday routine of information processing and adhere to a predefined procedure, which reduces the overall level of risk to the processing environment. Creating a new user account or deploying a new desktop computer are examples of changes that do not generally require change management. However, relocating user file shares, or upgrading the Email server pose a much higher level of risk

11-http://www.wired.com/threatlevel/2008/07/insider-tech-at/

to the processing environment and are not a normal everyday activity. The critical first steps in change management are defining change (and communicating that definition) and defining the scope of the change system.

Change management is usually overseen by key business areas, security, networking, systems administrators, database administration, applications development, desktop support and the help desk. The tasks of these stakeholders can be facilitated with the use of automated work flow applications. The responsibility is to ensure the organization's documented change management procedures are followed. The typical change management process is as follows:

1. **Requested:** Anyone can request a change. When a request for change is received, it may undergo a preliminary review to determine if the requested change is compatible with the organization's business model and practices, and to determine the amount of resources needed to implement the change.

2. **Approved:** IT Management runs the business and controls the allocation of resources; therefore managers must approve requests for changes and assign a priority for every change. A change request could be rejected if the change is not compatible with the business model, industry standards or best practices. IT Management might also choose to reject a change request if the change requires more resources than can be allocated for the change.

3. **Planned:** Planning a change involves discovering the scope and impact of the proposed change; analyzing the complexity of the change; allocation of resources and developing, testing and documenting both implementation and back out plans. Need to define the criteria on which a decision to back out will be made.

4. **Tested:** Every change must be tested in a safe test environment, which closely reflects the actual production environment, before the change is applied to the production environment. The contingency plan must also be tested.

5. **Scheduled:** Part of the manager's responsibility is to assist in the scheduling of changes by reviewing the proposed implementation date for potential conflicts with other scheduled changes or critical business activities.

6. **Communicated:** Once a change has been scheduled, it must be communicated. The communication is to give others the opportunity to remind others about the changes or reduce conflicts of critical business activities that might have been overlooked when scheduling the change. The communication also serves to make the Help Desk and users aware that a change is about to occur. Another responsibility of the manager is to ensure that scheduled changes have been properly communicated to those who will be affected by the change or otherwise have an interest in the change.

7. **Implemented:** At the appointed date and time, the changes must be implemented. Part of the planning process is to develop an implementation plan, testing plan and contingency plan. If the implementation of the change should fail or the post implementation testing fails or other "drop dead" criteria have not been met, the back out plan should be implemented.

8. **Documented:** All changes must be documented. The documentation includes the initial request for change, its approval, the priority assigned to it, the implementation, testing and back out plans, the results of the change review board critique, the date/time the change was implemented, who implemented it, and whether the change was implemented successfully, failed or postponed.

9. **Post change review:** The IT Manager should hold a post implementation review of changes. It is particularly important to review failed and contingency changes. They should try to understand the problems that were encountered, and look for areas for improvement.

The above outlines a change management procedure. These procedures will greatly reduce the overall risks created when changes are made to the environment. Good change management procedures improve the overall quality and success of changes as they are implemented. This is accomplished through planning, peer review, documentation and communication as outlined above.

Disaster Recovery

As the name implies, an organization's disaster recovery process entails the steps to be followed in the case of a catastrophic disruption to the organization – man-made or natural, hardware or software. Disaster recovery processes should be tested on a regular basis as the organization will change in terms of personnel and makeup during the regular course of business.

Adhering to compliance can be a challenge in this part of the process as governmental laws and regulations will have a significant effect on data processing and information security. Important industry sector regulations have to be considered when they have a significant impact on information security. For example, Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act of 2002 (SOX), Payment Card Industry Data Security Standard (PCI DSS), and Security Breach Notification Laws in states like California, Nevada, Wisconsin and more.

Incident Response

Incident response is the process that an organization should follow in the wake of an attack. This attack can be physical or logical in nature and could originate from either inside or outside of the organization. The process around incident response should be structured so that all evidence is collected and law enforcement is involved if necessary.

Computer security incident management is an administrative function of managing and protecting computer assets, networks and information systems. These systems continue to become more critical to businesses. This responsibility extends to having a management program for "what to do, when things go wrong." Incident management is a program which defines and implements a process that an organization may adopt to promote and protect its information.

A typical incident response process will have the following elements:

1. **Event / Incident:** An incident is an event attributable to a human root cause. This distinction is particularly important when the event is the product of malicious intent to do harm. An event is an observable change to the normal behavior of a system, environment, process, workflow or person / components. There are three basic types of events:

    - Normal -- a normal event does not affect critical components or require change controls prior to the implementation of a resolution.
    - Escalation – an escalated event affects critical production systems or requires implementation of a resolution that must follow a change control process.
    - Emergency – an emergency is an event that may breach primary IT controls of critical systems and affect a component's performance. Preventing protective IT measures, like virus updates that guard information, also has a negative impact on system activities and can also be deemed an emergency. Computer security and information technology personnel must handle emergency events according to a well-defined computer security incident response plan.

2. **Tracking:** Employee, vendor, customer, partner, device or sensor reports event to Help Desk or IT Manager. Prior to creating the ticket, the Help Desk may filter the event as a false positive. Otherwise, the help desk system creates a ticket that captures the event, event source, initial event severity and event priority. The ticket system creates a unique ID for the event. IT Personnel must use the ticket to capture email, IM and other informal communication. Subsequent activities like change control, incident management reports and compliance reports must reference the ticket number.

3. **Responders:** The First Level Responder captures additional event data and performs preliminary analysis. The First Responder determines criticality of the event. Events that affect critical production systems or require change controls must be escalated to IT Management. Organization management may request an immediate escalation without first level review.

4. **Resolution:** The event is ready to resolve. The resource enters the resolution and the problem category into the ticket and submits the ticket for closure. The ticket owner (employee, vendor, customer or partner) receives the resolution. They determine that the problem is resolved to their satisfaction or escalate the ticket.

5. **Reporting:** The escalation report is updated to show this event and the ticket is assigned a Second Tier resource to investigate and respond to the event. The Second Tier resource performs additional analysis and re-evaluates the criticality of the ticket. When necessary, the Second Tier resource is responsible for implementing a change control and notifying IT Management of the event.

Emergency Response:

Events may follow the escalation chain until it is determined that an emergency response is necessary. Top-level organization management may determine that an emergency response is necessary and invoke this process or additional processes directly.

Best Practices for Aligning Process and Technology

Security is an ever changing, ever evolving field. As described above, the threat is constantly increasing and becoming more nefarious as the criminals get better. There are a wide variety of management styles and it is very difficult for organizations to even begin to implement the right processes for their organization.

There are numerous questions that should be asked as an organization is evaluating current processes that are in place or processes that it wishes to implement. Some questions that should be asked are:

- *Does your organization have written policies in place around the appropriate use of email, Internet, and Instant Message?*
- *How frequently does your organization provide threat awareness training/campaigns for employees?*
- *Does your organization have an alert in place to ensure that endpoint security products are active and updated?*
- *Does your organization currently archive spam, viruses or other malware?*
- *How often does your organization change employees' passwords and privilege levels?*
- *Does your organization have a process for handling changes and is someone in the organization responsible for these changes?*
- *Does your organization have a formal risk mitigation process for new devices and equipment?*
- *Have we defined everyone's role and the process itself?*
- *Can the team implement these procedures? Have we trained them in this process?*

The answers to these questions will help an organization begin to think about their daily operations and the processes that will enable success in the event of an incident. Organizations who do not know the answers to these questions run the risk of being blindsided by any of the current attack methodologies and/or blindsided by the lack of process for dealing with these attacks.

Understanding what data is accessed on a daily basis by employees will help organizations understand what processes are needed to ensure secure handling of that data. Some organizations need very specific processes around daily operations, in order to allow smooth transition during times of turnover. Some organizations may only detail processes in place around specific events – like a malware attack, an act of nature, or some other disruptive event. Other organizations may require specific human resource processes and policies to ensure compliance with security initiatives. Whatever the ultimate solution is, it varies from organization to organization, but is only effective if the organization understands the most dangerous threats to itself.

Best Practices for Implementing Security Processes

After determining the best technology solutions and choosing a vendor, the deployment of security technologies into the organization begins. This is not a trivial exercise and – if done without both upper management support and end user understanding – one that will fail.

Some best practices around security process deployment include:

1. **Practice** – It is imperative that any solution be tested before implementation. Every environment is different and some solutions may interfere with business critical processes. It is important to understand the unintended results of implementing a security process before making it required.

2. **Upper Management Approval –** Upper management should not only be aware of upcoming security initiatives, but should support them wholeheartedly. This is critical when human resource policies come into play that could affect personnel. Upper management support will be necessary to enforce process that may be time-consuming or require additional resources.

3. **End User Awareness –** End users should be made aware of upcoming changes to security processes. Surprising end users by changing a process causes fear, confusion and legitimate frustration. Users should receive awareness as to what is changing and the policies put in place to ensure that business continues.

4. **Human Resource Policies –** Ultimately, human resource policies have to be applied to ensure compliance with security policies. Security processes are often seen as obstructive and employees may try to avoid or circumvent technological solutions. It is imperative that human resource policies are in place to discipline these actions.

Conclusion

Defending the modern organization is a daunting task. An increasingly mobile workforce, increased regulatory compliance pressures, and more sophisticated attacks are forcing organizations to take a hard look at the security around their data. It is imperative that organizations look at the wide variety of business transactions they are performing on a daily basis and implement effective security processes to protect those vectors. Without well defined security processes, critical client data and intellectual property could be lost or the organization could fall hostage to a single disgruntled employee.

Security processes are not implemented by a single person or department. Upper management, end users, vendors, human resources, and legal department must all come to the table ahead of a crisis situation in order to build the foundation that will ultimately serve to protect the organization. Data is valuable to criminals and technology solutions will always leave gaps in protection across the organization. By implementing secure processes across the organization that are consistently re-evaluated and tested, an organization will find itself both resilient to the latest threats and even more agile in the adoption of new technologies. With a secure foundation in place, businesses can focus on profitability and other corporate goals, knowing that security is woven into the daily activities of the business. This provides a much more flexible and safe environment from which to operate.

More Information

AMERICAS

UNITED STATES
512 Seventh Avenue
6th Floor
New York, NY 10018
USA
Toll-free +1 866 460 0000

CANADA
170 University Avenue
Toronto, ON M5H 3B3
Canada
Toll-free :1 866 460 0000

EUROPE

HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
Tel +44 (0) 1452 627 627
Fax +44 (0) 1452 627 628
Freephone 0800 917 7733

LONDON
3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom
Tel +44 (0) 203 009 6500
Fax +44 (0) 203 009 6552
Support +44 (0) 1452 627 766

NETHERLANDS
WTC Amsterdam
Zuidplein 36/H-Tower
NL-1077 XV
Amsterdam
Netherlands
Tel +31 (0) 20 799 7929
Fax +31 (0) 20 799 7801

BELGIUM/LUXEMBOURG
Symantec Belgium
Astrid Business Center
Is. Meyskensstraat 224
1780 Wemmel,
Belgium
Tel: +32 2 531 11 40
Fax: +32 531 11 41

DACH
Humboldtstrasse 6
Gewerbegebiet Dornach
85609 Aschheim
Deutschland
Tel +49 (0) 89 94320 120
Support :+44 (0)870 850 3014

NORDICS
St. Kongensgade 128
1264 Copenhagen K
Danmark
Tel +45 33 32 37 18
Fax +45 33 32 37 06
Support +44 (0)870 850 3014

ASIA PACIFIC

HONG KONG
Room 3006, Central Plaza
18 Harbour Road
Tower II
Wanchai
Hong Kong
Main: +852 2528 6206
Fax: +852 2526 2646
Support: + 852 6902 1130

AUSTRALIA
Level 13
207 Kent Street,
Sydney NSW 2000
Main: +61 2 8220 7000
Fax: +61 2 8220 7075
Support: 1 800 088 099

SINGAPORE
6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
Main: +65 6333 6366
Fax: +65 6235 8885
Support: 800 120 4415

JAPAN
Akasaka Intercity
1-11-44 Akasaka
Minato-ku, Tokyo 107-0052
Main: + 81 3 5114 4540
Fax: + 81 3 5114 4020
Support: + 852 6902 1130

About Symantec.cloud

Symantec.cloud uses the power of cloud computing to secure and manage information stored on endpoints and delivered via email, Web, and instant messaging. Building on the foundation of MessageLabs market leading software-as-a-service (SaaS) offerings and proven Symantec technologies, Symantec.cloud provides essential protection while virtually eliminating the need to manage hardware and software on site.

More than ten million end users at more than 31,000 organizations ranging from small businesses to the Fortune 500 use Symantec.cloud to secure and manage information stored on endpoints and delivered via email, Web, and instant messaging.

Symantec.cloud helps IT executives to protect information more completely, manage technology more effectively, and rapidly respond to the needs of their business.

For specific country offices and contact numbers, please visit our website.

Symantec.cloud North America
512 7th Ave.
6th Floor
New York, NY 10018 USA
1 (646) 519 8100
1 (866) 460 0000
www.MessageLabs.com

Symantec helps organizations secure and manage their information-driven world with **security management**, **endpoint security**, **messaging security**, and **application security** solutions.

1/2011 21169184