GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Patch Management

Deploying a process for

Patch Management

in relation to

Risk Management

© SANS Institute 2004, Author retains full rights.

Maik Medzich
GSEC Practical Assignment
Option 1
Version 1.4b

March 22, 2004

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Content

Table of Content 2
Table of Figures 3
Definitions 3
Glossary and List of Abbreviations 4
1 Abstract 5
2 Introduction 6
3 Process overview 7
4 IT Management Framework 8
4.1 Security Management 8
4.2 Operations Management 9
4.3 Configuration and Asset Management (CAM) 9
4.3.1 Classification of the CI's 9
4.3.2 Monetary valuation of the CI's 10
4.4 Change -/ Release Management (CM) 10
4.5 Problem-/ Incident Management (PM) 10
4.6 Control Boards 11
4.7 Conclusion 11
5 Risk Management 12
5.1 Risk Assessment 12
5.1.1 Threat Analysis 12
5.1.2 Vulnerability Assessment 13
5.1.3 Security Controls 13
5.2 Impact Analysis 14
5.2.1 Likelihood Severity 14
5.2.2 Quantitative vs. Qualitative Risk Assessment 14
5.2.3 Baseline protection level 15
5.3 Risk Level 16
5.4 Managing the risk 17
5.5 Conclusion 17
6 Patch Management 19
6.1 Patch Management Process 19
6.1.1 Event Monitoring 19
6.1.2 Event Assessment a nd classification 20
6.1.3 Testing & Documentation 20
6.1.4 Implementing the patch 21
6.2 Manual Patch Management 21
6.3 Automated Patch Man agement 21

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6.3.1 Thoughts of evaluating a Patch Management Tool 22
6.3.2 Integration of a Patch Management Tool in the Patch Management Process 22
6.4 Automated vs. Manual Patch Management - ROI & TCO 22
6.5 Side notes to patch management 23
7 Selling Information-Security to senior management 24
8 Summary 26
Annex A: Quantitative Risk Assessment – Example 28
Annex B: Security Intelligence Web Resources 29
Annex C: Advisory documentation template 30
References 31

Table of Figures

Table 2-1 Patch Management Process 7
Table 4-1 Baseline protection table 16
Table 4-2 Risk Level matrix 17

Definitions

	Definition
Vulnerability [1]	A "universal" vulnerability is one that is considered a vulnerability under any commonly used security policy which includes at least some requirements for minimizing the threat from an attacker. (This excludes entirely "open" security policies in which all users are trusted, or where there is no consideration of risk to the system.) The following guidelines, while imprecise, provide the basis of a "universal vulnerability" definition. A universal vulnerability is a state in a computing system (or set of systems) which either: • allows an attacker to execute commands as another user • allows an attacker to access data that is contrary to the specified access restrictions for that data • allows an attacker to pose as another entity • allows an attacker to conduct a denial of service
Exposure [1]	The following guidelines provide the basis for a definition of an "exposure." An exposure is a state in a computing system (or set of systems) which is not a universal vulnerability, but either: • allows an attacker to conduct information gathering activities • allows an attacker to hide activities • includes a capability that behaves as expected, but can be easily compromised

[1] According to CVE Definition [CVE-Def]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	• is a primary point of entry that an attacker may attempt to use to gain access to the system or data • is considered a problem according to some reasonable security policy
Common Vulnerabilities and Exposures (CVE)	A list of standardized names for vulnerabilities and other information security exposures - CVE aims to standardize the names for all publicly known vulnerabilities and security exposures. [

Glossary and List of Abbreviations

	Definition
CAM	Configuration and Asset Management
CM	Change -/ Release Management
PM	Problem-/ Incident Management
CI	Configuration Item
ITIL	Information Technology Infrastructure Library
ISS	Internet Security Systems
IRIS	Internet Risk Impact Summary (Report)
CVE	Common Vulner ability and Exposures, according CVE
IDS	Intrusion Detection System
ROSI	Return on Investment for Infor mation Security Guideline
SLA	Service Level Agreement
ROI	Return On Investment
OICT	The New South Wales Office of Information and Communications Tec hnology (OICT) is an agency of the NSW Government
NIST	National Institute of Standards a nd Technology
CRSC	Computer Security Resource Center as part of NIST

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1 Abstract

Today, the value and importance of data and information of an enterprise has much more increased than it's ever been expected to be. Growing usage of the internet seems to be essential for technology oriented enterprises, but also the increasing amount of client systems which has to be managed and secured are becoming more and more important. Even thinking about the several different ways employees can access to the corporate network (and therefore to data and information) will cause sleepless nights at the designated administrators. The enterprises most valuable but sometimes intangible assets, the data and information, are exposed to a high amount of potential threats and risks. Hackers, cyber-terrorists, viruses or even destructive employees are more or less invited to exploit the known and unknown vulnerabilities [2] and exposures [3]. This all could lead an enterprise into the total loss of business and the operational staff is daily faced with the challenge to counter such threats.

By implementing an effective security management framework, organizations will achieve a lot of business benefits and an overall increase of the protection of the company's assets. Reduced downtime, less data-loss and cost-effective IT management are perfect pros for deploying it. Compilations of security management processes are widely available, e.g. the ITIL[4] or Cobit[5] Framework. However, this paper focuses on the most important security maintaining process: The patch management process and it's relation to risk management.

Thus, the paper will focus on developing an applicable guideline on implementing a patch management process. The reader will be introduced in the main steps for risk management and patch management as well as the paper will outline the relations to an IT management framework.

The paper will neither focus on evaluating security policies nor will it focus on complete guidance to an IT management framework.

© SANS Institute 2004, Author retains full rights.

[2] According to the CVE definition; further referred as "Event" [CVE-Def]
[3] According to the CVE definition; further referred as "Event" [CVE-Def]
[4] ITL – IT Infrastructure Library for IT Service Management issued by Office of Government and Commerce; [ITIL-OGC]
5 Control Objectives for Information and related Technobgy, IT business process and control framework issued by IT Governance Institute; [ITGI]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2 Introduction

"Atlanta – Nov. 18, 2003 – Internet Security Systems, Inc. (ISS), today released its Internet Risk Impact Summary Report (IRIS) for the third quarter of 2003, which reveals a 15 percent increase in the number of security incidents over the second quarter of 2003… …725 new vulnerabilities,..., and 823 new viruses and worms…" [6]

As you might imagine, this little example is only one of hundreds that can be found during a quick research on the web. So, this should encourage you as a diligent system administrator to apply all patches as soon as possible. And, as it is in the perfect environment, you will always have enough people to do the job and have the full commitment of the senior management in place, haven't it? No, you haven't! But, how to master this challenge? Yes, you're right, implement a patch management process for all and every security related patch (with regard to the respective systems)!

What do you think now, is patch management important to maintain an IT environment? Well, yes it is! But do you really want to implement all, I mean very all patches? No, you don't, that would be a hell of a job! Take a few minutes and consider from your own experience. What did you done, if a new vulnerability arose which had affected your systems? You decide whether or not to apply the patch by take a look on the severity, affected OS and so on. But about what else you should think? What risk do you be exposed to by not applying the patch! Here is the point where the risk management process will take a part.

Implementing these processes within an IT-Infrastructure will help you to manage the challenge of an increasing insecure internet and/or intranet.

[6] Source: Internet Security Systems' X-Force Internet Risk Impact Summary Report for Q3 2003 (Press Release); [ISS-IRIS]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3 Process overview

First, the reader needs to get introduced to the main purpose of the paper, deploying a patch management process and it's relation to risk management embedded in an IT management framework. The following picture shows the patch management process and their relations within the IT management framework :

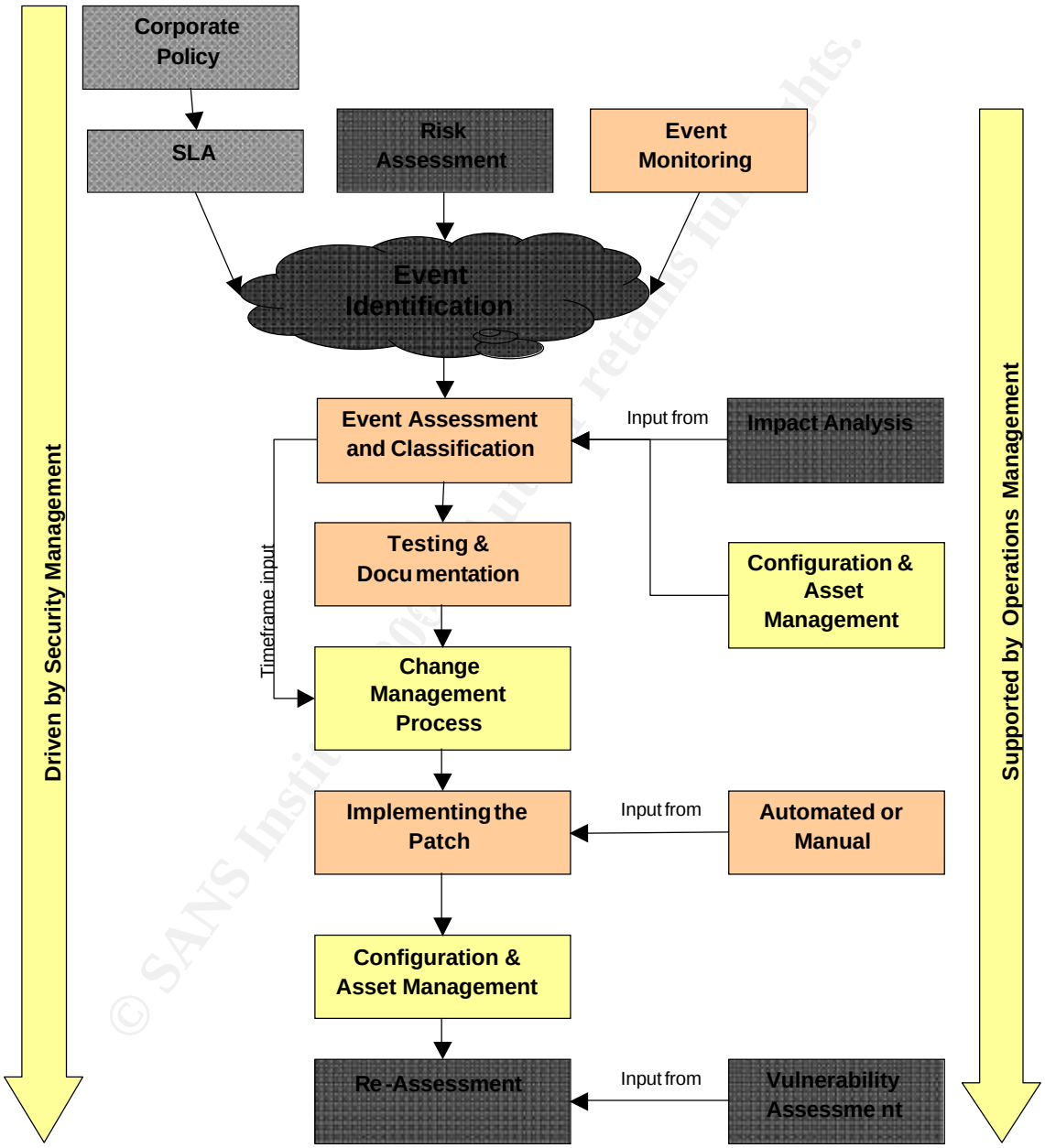


Table 3-1 Patch Management Process

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

How to read this:

Related to steps taken from the IT management framework

Related to steps taken from the patch management

Related to steps taken from the risk management

Related to steps which are not covered, but mentioned because of completeness

The next chapters are focusing on developing the process steps (outlined above) and gives you an understanding and guiding on how to implement them in an enterprise.

In the summary section you will find a checklist which enumerate all important steps and issues to built in a good patch management process.

4 IT Management Framework

Within the evaluation of a patch management process you have to set up some side processes as a prerequisite to manage this task. Because these processes are not the main scope of this document, the paper will only cover some principles regarding these ones. For this paper I had chosen the framework of the ITIL, a precise description can be found in the ITIL Framework for IT Service Management [7] from the Office of Government and Commerce and in "The ITIL and ITSM Directory" [8].

A good briefly overview and comparison of other standards and IT management frameworks (like COBIT, ITIL, ISO17799 and others) can be found at a guideline from the IT Governance Institute [9]

4.1 Security Management

One of the most important processes in this framework is the security management process which has side-channels to each other IT management process and is considered to be the overall control authority with respect to IT security relevant issues. Furthermore, in strictly speaking, this isn't really a process; this is more a comprehensive role with an intervening mandate and the following key responsibilities:

- Monitoring of all relevant Security Intelligence Web-Resources for security events
- Risk and impact assessment for all new and known vulnerabilities and exposures
- Managing documentation, e.g. of all published events (with regard to the specific environment)
- Deployment of guidelines, processes and policies which have security concern
- Escalation authority for reported security events

[7] ITIL – IT Infrastructure Library;[ITIL-OGC]
[8] Directory of ITIL and ITSM services & software;[ITIL-ITSM]
[9] Cobit Mapping – Overview of international IT guidance, ITGI; [COBIT]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Management authority for co ordinating the event analysis, testing of patches and implementation tasks.
- Test result evaluation
- Approval of the deployed workaround, patch or any other countermeasure which will mitigate or eliminate the security event.

4.2 Operations Management

Another, so metimes, underestimated process, is the operations management process, which is almost the single point of contact of the operation and should be established as a n overall control authority with respect to IT operational relevant issues.

- Assist the securit y management during the risk and impact assessment
- Allocate a team of specialists for the diffe rent systems and application, e.g. Unix -, Windows-, SQL- and web server analysts.
- Management authority for developing and testing of security measures within the ir group of specialists.
- Assistance in the evaluation of the test results
- Managing workarounds, especially if no appropriate patch is ava ilable
- Assistance during development of the implementation - guideline/ timeframe
- Managing the deployment of the approve d countermeasures

4.3 Configuration and Asset Management (CAM)

This part of an IT management framework ensures yo u to define all relevant configuration items (the inventory) and to store them in an appropriate database. CAM also supports yo u in tracking change s within the IT environment, because each change must be recorded in a CAM database. This has a high priority, because this is part of your baseline whether to implement a patch or not. This is also the first time when you can make a Vulnerability Assessment with regard to the configuration baseline, to be aware of the “built -in” threats!

Example configuration items (CI) are software versions (OS and a pplication), patch-level, release-version and hardware confi guration as well as documentation, procedures and system (business process -) owners . Other topics may be added with regard to the specific environment.

4.3.1 Classification of the C I’s

At this point, it’s a pretty good idea to classify all recorded CI’s regardi ng the three main security needs, confidentiality, integrity and availability. Unfortunately, this is one of the most important and diffic ult parts of the CAM. The dependencies here are very abstru se. The classification should be derived from the security requirements within your security policy and sho uld be considered with respect to the importance within your business processes. An overall classification of each CI with reliance on there security needs is might be helpful in the later shown classificatio n within the patch management process. However,

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

in generally you should try to set up a classification for each CI in relation to the security triad CIA (Confidentiality, Integrity, Availability) and with the priority levels high, medium and low. A more detailed explanation of how to evaluate the priority levels I will give in the section Baseline protection level .

4.3.2 Monetary valuation of the CI's

Calculation based on ROI (Return on Investment) analysis becomes more and more important for security professionals, therefore it's essential to understand the terms of business valuation with respect to security. To calculate ROI on any security countermeasure you should assign a monetary value to your CI's (assets) .

Assigning a monetary value to an asset is quite more difficult due to the fact, that for some assets (usually for intellectual property) assigning such a value becomes a challenge. Be insured to have the senior management attendance in that discussion, otherwise, you will always be questioned about the reliability. However, some clues to think about, but not limited to that, are given here: [10]

- The original, replacement and/or re-creation cost of the asset (e.g. data)
- Penalties and/or damages arising from violation of legislation and/or regulation
- Potential revenue loss
- Potential loss from damage arising from disclosure, modification, destruction and/or misuse of information
- Advantages to have these intellectual asset (in comparison to your competitors)

4.4 Change-/ Release Management (CM)

This process as part of the IT management framework is needed to track changes, or even new releases within your environment as well as to prevent unauthorized changes which may have a security concern or harm your environment . Actually, the CM is the mechanism to implement your patches. With regard to the CAM , all approved changes must be recorded in the CAM database. Therefore a proper recording mechanism (i.e. the CAM database) for all changes needs to be established. There should be a single point of contact for the CM and an interface to the security management. Main tasks of the responsible Change -/ Release Manager are to categorize and prioritize changes according their severity as well as to schedule and monitor the implementation of changes and releases.

4.5 Problem-/ Incident Management (PM)

Here we talk about the main conjunction between a problem/incident and the security management. Within the PM process all upcoming threats, problems, incidents, for shorten all events will be collected, triggered and recorded. Because of your close interface to the respective process manager you will be able to collect all upcoming events and classify them whether there is a security breach or not. As well as the CM process you should

[10] Adoption from "Information Security Guideline for NSW Government – Part 1 Information Security Risk Management" (page39/40);[OICT-RM]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

establish this process within your management framework. An accurate implementation should also have a single point of contact and a well defined recording of the problems/incidents with at least the following information [11]:

- Date and time
- Affected system(s)
- Brief description
- Priority
- Solution (if available)
- Any other environmental dependent topic

4.6 Control Boards

In large organizations or even in high sensibility environments it's recommended to implement a Control-Board within your management framework. In this control board the respective managers from CM, PM and security management should participate. Here, the security management will be able to receive the information regarding changes, problems and incidents which have security concern and may have to result into a patch or other corrective measures!

4.7 Conclusion

As you could see an implementation of such processes will improve your IT management in a positive manner. The above described processes are necessary to set up an appropriate patch management process. The configuration and asset management with its database is the baseline for the evaluation criterion, the problem-/ incident management is might be a source for new discovered vulnerabilities or exposures. The change-/ release management is needed during the patch deployment, as part of the CAM. And the security- and operations management are both acting as overall control authorities, one from the security point of view and the other from the operational point of view.

Keep in mind, security is not limited to perimeter defense but there's a stringent necessity to implement security controls based on policies, processes and procedures.

[11] Adoption from Security Management, IT Infrastructure Library (OGC); [ITILBOOK]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

5 Risk Management

Starting with the risk management process will help us to understand the main goal of security management processes, protecting the value of an asset. The purpose and often unheeded advantage of risk management is to be conscious of the risks your business is bare to and the ability to manage and mitigate such risks to an acceptable level. This is a great opportunity for IT leaders and business process owners to maintain the balances between the risks to your assets and the mitigating controls in an economic and cost-effective manner, 100% mitigation is quite impossible or even to expensive!

A complete essay about risk management will probably exceed 100 pages or more, however, because of this I will focus only on the, from my point of view, most important principles to achieve the purpose of this paper. For further reading you are advised to study the NIST publication, „Risk Management Guide for Information Technology Systems – Recommendations of the National Institute of Standards and Technology“.[12] – Where this section is mainly based on but not limited to. Hence, the following is more a general view of the process itself and is usually performed before a new system is launched, a major change or improvement was done, or in any case a new assessment becomes necessary.

5.1 Risk Assessment

The main part in the risk management methodology, risk assessment, is essential to identify the monetary or qualitative value of your assets, the threats your assets are exposed to, existing vulnerabilities and adequate mitigating measures (technical or organizational). Input for this process is the corporate security policy, which defines the high-level security requirements and identifies the business areas with the highest security concern.

5.1.1 Threat Analysis

According to the NIST guideline (mentioned above), one step in the risk assessment process will be the identification of risks. Therefore, of course, you need to have an idea about the assets you have. Take a look at section Configuration and Asset Management (CAM); hereby you already have your instance to do so.

To identify the threats you can adopt the NIST' table[13] for common threat sources:

- Natural threats: Floods, earthquakes, tornados, avalanches, electrical storms, etc
- Human threats: Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions like network based attacks, malicious software upload, unauthorized access, disclosure, theft and/or sabotage of confidential information.
- Environmental threats: Long-term power failure, pollution, chemicals, liquid leakage, etc.

With respect to the original purpose of this paper (deploying a patch management process), I would like to leave this section as it is and stay focused on the human threat source, because I think it's something like a crazy idea to assign a patch to an earthquake or a flood.

[12] NIST Risk Management Guide for IT Systems; [NIST-800-30]
[13] NIST Risk Management Guide for IT Systems (page 14); [NIST-800-30]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Nonetheless, during your own risk assessment you need to be aware of the threats your systems are exposed to. But I think there's no doubt about the fact that an open and unprotected port on a public web server will be threatened by a huge amount of individuals. According to the "2003 Survey of Top Security Threats and Management Issues Facing Corporate America" [14] from Pinkerton Consulting & Investigations Inc., Internet/Intranet Security is still be ranked at the 3rd place, right after "Workplace Violence" and "Business Interruption/ Continuity Planning", the last issue, of course, could also be a result of an internet/intranet security breach. Significantly, this issue, in this rating, is positioned before terrorism.

5.1.2 Vulnerability Assessment

Identification of known (or sometimes unknown) vulnerabilities is far more a challenge within the risk assessment methodology. The vulnerability identification is necessary to provide an overview of currently existing vulnerabilities and exposures.

Recommended actions to identify the vulnerabilities and exposures are on the one hand side to map all your configuration items to an existing listing of vulnerabilities, i.e. determine, for example, if your implemented web server is known for any vulnerabilities. Therefore you need to consolidate the different sources, like vendor advisories, previous audits or other security related sources (see also: Event Monitoring).

On the other hand it is very important to assess your systems on a regular basis with automated vulnerability scanning tools like nessus [15], nmap [16] and Internet Scanner [17], at least in the initial phase or in combination with a penetration testing[18]. Pen-Testing is very useful to identify application related and environmental specific vulnerabilities. For automated tools it is very difficult to combine a "race condition" [19] with an "input validation failure"[20] to upload malicious software to your web server, but be sure, the hackers will!

5.1.3 Security Controls

Coming back to risk assessment, at this stage ones should be able to get aware of know vulnerabilities and to proceed in continuing of threat and vulnerability analysis. Regardless at which point you are, provide yourself and your senior management with a list of the threats and vulnerabilities every time. Documentation is essential!

The next step will be to weigh all the documented vulnerabilities against your existing security controls (for a more generally approach it's necessary to take also planned security controls into considerations) and see if these will mitigate or neutralize them.

Security controls can be either technical or non-technical and are either be preventive or detective controls. Technical controls are usually hard- or software based controls or even physical security measures, e.g. firewalls (preventive control), routers, IDS' (detective control) or even door-locks. Non-technical controls are generally summarized under the key words security policy, processes and procedures.

[14] Pinkerton Consulting & Investigations Inc; [Pinkerton]
[15] free available at: http://www.nessus.org
[16] free available at: http://www.insecure.org
[17] available after purchase at: http://www.iss.net
[18] A complete guideline to "Network Security Testing Overview" is available from NIST (800-42); [NIST-800-42]
[19] "Anomalous behavior due to unexpected critical dependence on the relative timing of events", definition according Hyper Dictionary; [HypDic]
[20] Failure in recognizing invalid user input.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

5.2 Impact Analysis

The previous sections illustrated to you how to get noticed about threats and there dependent vulnerabilities. In the next major step within the risk management methodology we will talk about the impact a vulnerability, exploited by a threat may have to your assets.

5.2.1 Likelihood Severity

Before evaluating the overall impact, let's take a couple minutes and discuss about the likelihood of a vulnerability. Not even if a vulnerability exist means that the vulnerability will be or can be exploited. The mitigating factors given in the released advisories are a good point to start this specific mitigating assessment.

The motivation and capability of one who tries to exploit a vulnerability, (e.g. attack from the web, or internally) has to be considered as well as which threat source underlies (e.g. authenticated user or not)! Additionally the characteristic of the vulnerability is essential to determine either if the vulnerability is easily exploitable with a given script or if a fundamental knowledge of system internals is needed. Finally, existing security controls should be examined in effectiveness against the vulnerability. Classification of the likelihood level can be done in four stages: [21][22]

- **VERY HIGH**, if an exploitation of the event of a direct accessible configuration item (CI) from external of the environment is almost certain. The threat source is exceedingly motivated and well skilled. Security controls aren't available or ineffective. Frequency of occurrence is estimated as *very high* (once or more a year)

- **HIGH**, if an exploitation of the event of a direct accessible CI from external of the environment is almost certain. The threat source is exceedingly motivated and well skilled, security controls are in place, but have a leak to mitigate, but are at least available in order to detect the violation. Frequency of occurrence is estimated as *high* (once a year).

- **MEDIUM**, if an exploitation of the event from external of the environment to an indirect accessible (via the DMZ[23]) CI in the MZ[24] becomes possible or from internal of the environment to a direct accessible CI. Security controls are in place to mitigate the exploitation significantly. Frequency of occurrence is estimated as medium (once in two years)

- **LOW**, if classification from VERY-High to MEDIUM not applies, but if the event is also considered to be relevant, especially if a combination of some LOW events might be exploited in future attacks.

5.2.2 Quantitative vs. Qualitative Risk Assessment [25]

Measuring the impact of an event goes hand in hand with the quantitative or qualitative risk assessment process. In some cases you feel inclined to use a mix of both to accomplish your goal. Both techniques have some advantages and some disadvantages, the right

[21] cf.: CRSC-NIST: Risk Management Guide for Information Technology Systems (page 27); [NIST-800-30]
[22] cf.: "Information Security Guideline for NSW Government – Part 1 Information Security Risk Management" (page 37); [OICT-RM]
[23] **D**e-**M**ilitarized-**Z**one, referred to as external zone for IT environments
[24] **M**ilitarized-**Z**one, referred to as internal zone for IT environments
[25] cf. SANS Security Essentials Cookbook (page 828 ff) [SANS-CBK]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

choice of which method will be appropriate to your requirements is one of the abilities a security manager should have.

In generally, by **quantitative risk assessment** ones mean the adverse monetary value of a risk to an asset, i.e. how much money you will loss, in case the event becomes exploited by a given threat source. This is a much more difficult approach to define impacts to an asset. However, in opposition to this, this is the best method to assign a very transparent value to an asset, so this is used to make the security management more aware to the board and to calculate the Return On Investment (ROI) for the countermeasures. You can use two different formulas to achieve this goal. (Please move to annex Quantitative Risk Assessment for an example)

Nevertheless, far more common in the industry is the **qualitative risk assessment**, since on the one hand side quantitative risk assessment is very difficult to calculate and on the other hand assigning values isn't applicable to customer confidence or loss of company intellectual properties (like the new marketing strategy or similar). That's the reason, why qualitative risk assessment is commonly used and is focused in this paper. Accomplish this means to assign more subjective values to an asset, as you will be introduced below.

5.2.3 Baseline protection level

Coming back to the Configuration and Asset Management (CAM), there, I already had mentioned the importance of the classification within the three main security categories, confidentiality, integrity and availability and their corresponding priorities. Talking about impact analysis always ends up or is referred to the adverse impact an event could have on a configuration item (asset). The adverse impact can be described in terms of loss or alteration of one or more of the three main security categories, confidentiality, integrity and availability.

This is very important to proceed in the overall risk determination; you need to apply the baseline protection level of each configuration item (asset). Take a look back, I already stated, that you should apply a protection level from low to high for each CI with regard to the security sensitivity. Therefore assess each CI and apply the appropriate protection level with regard to the three main categories.

In order to have sufficient guidance to evaluate the risk level from the security needs you can follow the adoption of the "Information Security Guideline for NSW Government – Part 1 Information Security Risk Management:" [26]

- **HIGH**, if the information asset is classified as strictly confidential, the confidentiality of the information asset must be guaranteed and comply with strict secrecy requirements. The information must be correct at all times. Unavailability of the information is not acceptable.

- **MEDIUM**, if the information asset is classified as confidential, the confidentiality of the information asset must be guaranteed. The information must be correct and any errors must be detectable and avoidable. A short period of unavailability is acceptable.

- **LOW**, if the confidentiality must be guaranteed for internal use only. The information must be correct and any errors must be detectable and avoidable but minor errors can be accepted. Moderate unavailability is acceptable.

[26] Information Security Guideline for NSW Government – Part 1 Information Security Risk Management (page 35 ff.); [OCT-RM]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

How to apply this:

Assign a level from LOW to HIGH for each category from the security triad according the guideline given above. The decision on which level you need is dependent on the business needs. Next step will be to estimate and merge the single protection levels into one baseline protection (result) level for each asset. Therefore business needs should take into consideration and comparison to the security is necessary to fulfill the business and security expectations.

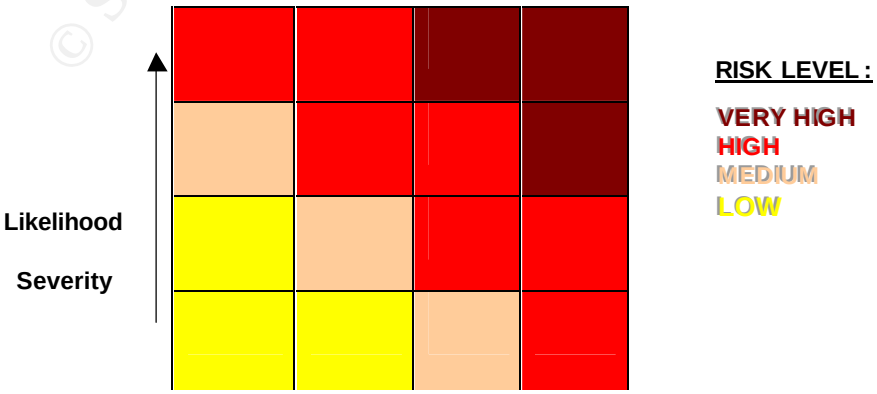
Security Category	Protection level Assign: low, medium, high
Integrity	Low to High
Availability	Low to High
Confidentiality	Low to High
Result	LOW; MEDIUM; HIGH; VERY-HIGH

Table 5-1 Baseline protection table

The result should end up with four different levels to accomplish are more granular classification. Keep in mind that we had merged three categories into one level of protection. For example, if you have assigned to all categories a "high" the result should be "Very-High", or if you have at least one "high" your result should be "high"

5.3 Risk Level

Merging the likelihood severity and baseline protection level into one matrix is the last step within the risk assessment. As you might believe, this is quite a roughly matrix and should be adjusted for better guidance in determining the overall risk with respect to your specific business needs. For some reason it's might be also a good idea to add a value for the liability that your business will probably have to its customers or government.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Table 5-2 Risk Level matrix

Having this rating means having a basis to form a judgment for the necessary countermeasures for remedy or to mitigate the risk.

- **VERY HIGH**, immediate action is unavoidable to prevent against serious loss or damage of monetary assets or trustworthiness. This may be has to result into shut down or forgo of some services or functions (e.g. in case of zero-day virus/worm attacks). A workaround to mitigate the event to risk *HIGH* must be implemented before re-launching the service. Senior management needs to be involved.

- **HIGH**, mitigating actions are required within an appropriate timeframe (SLA dependent). Countermeasures are required to avoid future exploitation of the event. Senior management needs to be informed about the occurrence.

- **MEDIUM**, immediate actions aren't required, but countermeasures need to be implemented for remedy or to mitigate the likelihood and exploitation of the event. An appropriate timeframe should be derived from the SLA.

- **LOW**, no actions during the normal maintenance process are necessary, but countermeasures or mitigating factors should be implemented during the next release or soft-/hardware upgrade.

5.4 Managing the risk

Managing the risk is a must for every organization to protect their assets. Here, it's independent whether a risk management process took place, in the initial phase of a project or during the operation of the project. Some central ideas that you may think about are contained by the risk treatment: [27]

- *Risk avoidance* – by deciding to stop the risk generating activity.

- *Reduce the likelihood or impact* – by implementing countermeasures to reduce the risk to an acceptable level.

- *Risk transference* – by transferring the risk to, e.g. an insurer.

- *Risk acceptance* – senior management decides to bears all risk.

5.5 Conclusion

Managing the risk is not only limited to this given, rarely more theoretical, guideline. Sometimes it will be happen that this general guideline will not fulfill the expectations or requirements of your business especially when undesired but unavoidable events will

[27] Adoption from "Information Security Guideline for NSW Government – Part 1 Information Security Risk Management" (page 43); [OICT-RM]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

threaten your assets. Therefore, by applying this process you need a lot of security instinct. Managing the risk means to understand the importance of your business processes and the value of your assets, monetary or qualitative value doesn't make any difference. To achieve this goal the risk management process should be driven by excellent skilled security managers with a high level of management experience and must be supported by the senior management and business process owners.

Remember that there is might be the need to derive some monetary evaluations or even to calculate some ROI. Be prepared in doing this, further reading can be done at: http://www.oit.nsw.gov.au/Guidelines/4.3.37.a.ROSI.htm , "Return on Investment for Information Security Guideline" [OICT-ROSI]

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6 Patch Management

There are two main ways to set up a patch management process. Either you decide to patch manually all upcoming patches with respect to your systems, or you decide to do the job with the support of appropriate tools.

But first of all I will introduce you in what to consider for both ways. What has to be done to build up a patch management process, or easier, what has to be done to keep your systems up to date and secure!

Throughout the patch management section you will be provided with some evaluating criteria for applying security patches in an economic sense with respect to the exposed risk.

6.1 Patch Management Process

The patch management process should be derived from your organizational security policy and all measurements and steps should be documented and agreed within the SLA, especially the Event Assessment and classification and the Implementing Timeframe for implementing the measurements.

In generally the process consists of the following main parts: Event monitoring (for new arisen vulnerabilities), event assessment and classification, testing & documentation, implementation in the operational environment and update of the CAM database.

6.1.1 Event Monitoring

The need to start the Patch Management Process is initiated by an event. Such an event could be:

- A released patch from your specific software vendor (or your own development)
- A Security Advisory from different sources (i.e. CERT [28], bugtraq [29], SANS [30], X-Force [31], SOPHOS [32], SecurityFocus [33], Microsoft [34] etc)
- An event from then PM/CM control board or from your organization's help desk
- An identified vulnerability or exposure (during the risk assessment)
- Any other trusted source

In order to be aware of every new disclosed vulnerability and exposure it's highly recommended to you to monitor all for your business relevant sources. Therefore you can subscribe for the different mailing lists, which can be reached from the different security homepages given in the annex Security Intelligence Web Resources.

The summary of all relevant events, incident reports, etc is recommended to be documented in an appropriate way to build up a database for the security management.

[28] www.cert.org
[29] www.bugtraq.org
[30] http://isc.sans.org (Internet Storm Center)
[31] http://xforce.iss.net/xforce/alerts
[32] http://www.sophos.com
[33] http://www.securityfocus.com
[34] http://www.microsoft.com/security/security_bulletins/

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

This database will be helpful within the security risk assessment for future releases or events. In annex C Advisory documentation template you will get assistance what records are needed or recommended.

6.1.2 Event Assessment and classification

Once, an event had occurred there is the need to assess and classify this new discovered vulnerability or exposure. Map the event to the CAM and determine if and what is affected! If one of the CI's is considered to be affected the next step is the classification or impact analysis. At this point the Risk Management will take a part in the patch management process.

Review the risk assessment section especially for the Impact Analysis to assess your event and classify it according to the given guideline. Having the overall risk rating, you can proceed with the implementation.

6.1.2.1 Implementing Timeframe

As soon as the assessment is done you need to follow the process by implementing the appropriate measures to mitigate or to get rid of the vulnerability or exposure. The implementing timeframe depends strong on the given environment in your organization. But however I will give some guidance from my own experience in implementing patches.

- For **VERY-HIGH Events** it is unavoidable to implement a mitigating workaround as soon as you had been made aware of the event. In very critical situations that might has to be result into network disconnection or similar! That seems very rigorously, but decide by yourself, which is the worse event, a temporally unavailability of your web-server or a full compromise without even knowing it!

- For **HIGH Events** it is recommended to implement the patch or other appropriate measures within a timeframe of 10 business days. Again, this is only my personal suggestion to do so!

- For **MEDIUM Events** it is recommended to implement the patch or take appropriate measures within 10-20 business days.

- For **LOW Events** it is recommended to collect such events and bundle them up into a security release which can be deployed for example 3-4 times a year or with respect to its needs.

6.1.3 Testing & Documentation

In order to reach the best results while implementing the measurements you should develop a test guideline and perform a test cycle on a production similar environment. This is necessary to avoid unexpected behavior as a result from the taken measures and also to be sure that the measures will work like you expect. Be very smart while implement patches or other measures in your environment (especially in a clustered environment), don't start with a full upgrade of the whole platform! Start with a less important server and evaluate the result before you deploy the patch throughout the complete test environment. Another reasonable way could be to rely on professional vendors. But be careful by relying only on them, like Joe Wang, CEO of South Jordan, Utah based LANDesk stated in a posting on the CIO.com website at December 23, 2003: "Some Patch Management vendors offer tested and validated patches, but you still need to consider what you have in your

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

environment and make sure that testing has been done that accurately reflects your environment and what you have in it." [35]

However you decide to test your patches, after a successful test cycle you should write an approval report and document all findings during the testing. Don't forget to build in some test steps to take care that you didn't open some new or old and still fixed vulnerabilities during the implementation, e.g. run a vulnerability scanner after implementing a patch and double-check the applied policies for the server. Occasionally, it's may reasonable to complete a full Vulnerability Assessment, which should take place after major changes.

Another very important issue is that you have a proper backup - and recovery processes in place. Remember, before you implement a patch make sure a backup has run successfully and is restorable in a reasonable manner. This is valid for both instances, the test environment and operational environment.

6.1.4 Implementing the patch

After you have successfully ran through a test cycle and were able to write an approval to the related patch it's the time to start the implementation on the operational environment. Here is the point where the Change Management (CM) will take a part in the whole process. The CM will now set up all necessary steps for implementing the measure (Patch, Release or similar), e.g. inform the dedicated administrators, announce the Implementing Timeframe (usually out of business hours), inform the user help-desk and so on. But the more important part of the CM is the cross-link to the Configuration and Asset Management (CAM), starting the CM should automatically force an entry into the CAM to keep the CAM-Database up to date!

Beside this, you should consider which is the best way to implement the measure as well as you had done this for the test environment. This is very dependent on the given environment and must be decided one by one for each individual environment.

6.2 Manual Patch Management

The steps taken in the section above (Patch Management Process) are fully applyable to a manual patch management process!

6.3 Automated Patch Management

Daily new arising vulnerabilities and exposures, and sometimes more than once a day released advisories from different vendors makes it more and more important to establish an automated patch management. "…the struggle can be akin to being trapped in a horror movie – something like "A Nightmare on Patch Street" [36], said Rutrell Yasin in the article "In need of a quick fix" published on www.fcw.com at December 1, 2003.

Whereas this section will not cover an evaluation of a specific Patch Management Tool, but will give you some general guidance to evaluate your own tool with respect to your specific environmental needs. However, to have an idea how much tools are widely available you should enter "Patch Management" into your favorite search engine and view the results… take your time!

[35] [CIO], http://www2.cio.com/ask%5Cexpert/2003/questions/question1847.html
[36] [FCW], http://www.fcw.com/fcw/articles/2003/1201/cov-patch-12-01-03.asp

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6.3.1 Thoughts of evaluating a Patch Management Tool

Implementing an automated patch management tool is a helpful idea regarding the increasing amount of patches administrators were faced to in today's businesses. But nevertheless patch management tools aren't the panacea in the IT world and evaluating such a tool will require suitable skills and knowledge about what is needed in your environment. Abilities which are necessary to consider and which the tool should comply with are:

- Automatic deployment of the patch immediately after the release. An additional recommendation here is the ability to have the prerequisite to let each individual patch be approved by an authorized administrator. This is to prevent automatic deployment of unapproved patches which are might harm the systems.

- Applying patches at a basis of the single server, i.e. each patch can be applied for each individual server. Think about the possible necessity to have a 99% high-availability SLA and you need to update your clustered network in two steps (each step with one part of the cluster).

- Monitoring of the patch-level from the release through the installation, i.e. reporting of the current patch-level, notification in case of missing patches, selection and coordination controlled by an administrator, logging and reporting of the whole installation process and alarming in case of errors.

- A standardized (e.g. a Web-) administration interface should be available and easy to use

- A categorization of the patches according their priority (according to the Risk Level) should be possible and an exact timeframe must be able to be administering for the rollout.

- Consider which software products and applications you want to update with the tool and map this to the abilities of the tool

- Be sure that there is the possibility to reinstall the patch as well as a fall-back opportunity in case of any unforeseeable event. At least your environment should have a suitable integrated backup and recovery processes.

6.3.2 Integration of a Patch Management Tool in the Patch Management Process

This is quite easier than it might look like. Implement the tool in the process at the time of Implementing the patch, here you will have the best time- and cost-effective result. And, of course it's still necessary to test patches before deploying them into the operational environment. In some bigger environments, with some dependencies to the used software and applications, it's might be reasonable to implement such a tool in the test environment as well. Another plus for this is that you should in generally test all new software in a test environment, thus also the Patch Management Tool.

6.4 Automated vs. Manual Patch Management - ROI & TCO

It always comes back to money if ones be asked for the best choice. Same in here, manual patching is, in relation to automated patching very expensive and uneconomical, due to the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

fact, that the administrators often have to perfo rm similar steps for each patch which can be easy automated.

Following above chapters, once you have decided which tool you prefer, try to make an analysis on ROI (Return on Investment) and TCO (Total Cost of Ownership) . Some available tools are free of charge, some aren't, but in any case I predict that the investment in an autom ated patch management tool will return to you after several month by saving money during patching and in parallel improving quality and security of the environment.

6.5 Side notes to patch management

During the research for this paper, I became aware of another very interesting point, patching a compromised server! This is a very tricky and difficult approach and should be done very carefully, because in the main cases the patch w ouldn't behave like expected and not even patch the vulnerability. For the paranoi d, once a server has been compromised, it is best to re -install the OS. However, from my point of view, this is mo re an incident response issue and therefore only noted shortly. For deeper insights, please ref er to NIST' guide "Procedures for handling secu rity patches", Sep. 2002[37].

Another interesting and very important thing is, to sec ure your mobile computers which are often abroad and hardly to maintain but still come back and access your network. Establish dedicated access zones for them and scan these devices for missing patches and virus -scanner-updates before you accept them to access yo ur internal network, data and information.

[37] CRSC-NIST: P rocedures for Handling Security Patches ; [NIST-800-40]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

7 Selling Information-Security to senior management

Along the research and from personal experiences I would like to drop a few words on how to sell your Info-Sec (Information Security) program (in our special case the patch management process) to your senior management. This is a tough issue and hardly to examine, but on the other side it's the only way to get the commitment from them.

Senior management is often very busy and involved in many concerns from the company's businesses. Having chances to present your Info-Sec affairs are rarely to get. If you want their attention be well prepared and do your job.

Figure out the are as of the bigges t concerns and translate this into monetary values. Senior management always open up their eyes when it comes to keywords like ALE (Annual Loss Expectancy), TCO and ROI. Easiest way for it, show them how much money they either loss or save by either implementing or not implementing your proposed security countermeasures. Show them, e.g. in an example from the past, how much money they have lost by wiping your servers from the last virus. On the other hand show them the cost you estimate for implementing an appropriate Anti-Virus solution (Invest & TCO).

Coming back to patch management, take the advantage that you know how to calculate an ALE and ROI on Info-Sec. Take a look at the annex Quantitative Risk Assessment and show them the example of applying a patch or not. Take a simple example, e.g. patching 100 servers with a "high-risk" level patch, which inherit that the likelihood of the exploitation seems to be very high:

Manual Patching:

1 FTE[38] X 5 hrs to patch X 100 server X $100 per hr = **$50.000 per patch**

Note: The 5 hours includes the administrator and the affected employees as well as the evaluation, testing and down-time of the server.

Security Incident (compromise due code execution):

Estimated temporary downtime until recognition:	2 hrs
Estimated downtime due analysis:	8 hrs per server
Re-Installing of OS and application:	12 hrs per server
Estimated Exposure Factor:	75%

= (8 hrs downtime + 12 hrs reinstalling) X 75% + 2 hrs recognition time

= 20 hrs X 75 + 2hrs = 1502 hrs X $100 per hr = **$150.200 per incident**

Note: The estimated costs doesn't includes the cost of losing intangible assets like the disclosed information and secrets as well as it doesn't includes the loss of

[38] FTE – Full Time Employee

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

revenue, customer confidence and consequences from legal liabilities or shareholders!

As you can see in this little calculation, patching isn't that expensive in comparison to server compromise. Well, while this is a very rough and high level calculation, it will open the eyes from senior management. Nevertheless, try to estimate your own business case, based on your specific environment and needs.

Underpin your research with open available surveys from official accepted institutes like Gartner[39], Pinkerton[40], McKinsey[41] or similar, regarding threats and their likelihood, especially for your specific business.

Give examples (if aware of some) where your Info-Sec program works well and had improved security, quality and therefore the business case. On the other hand, give also examples where thinks weren't went well due to a missing Info-Sec program.

Find out, if your business must follow legal liabilities. Giving them impressions on how they get blamed or get in trouble with legislation by not applying best practices, might be helpful to open their eyes. But be careful with to offrankly speaking, senior mgmt. often tends to overreact if they are confronted with a punch in their face.

Show them how an Info-Sec program can improve the overall *Quality of Service*, by increasing availability and decreasing major downtime due security incidents.

© SANS Institute 2004, Author retains full rights.

[39] www.gartner.com
[40] www.ci-pinkerton.com
[41] www.mckinsey.com

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

8 Summary

Wrap-up what we got, we have learned a lot of IT management processes, their related roles within the IT management framework. We have covered the principles about risk management and patch management . Let's take a short look back to summarize the main steps:

- ✓ IT Management Framework
  - Start your Info-Sec (Information Security) program by implementing one of the available IT management frameworks or standards .
  - Establish at least Security-, Operations-, Configurations-, Incident-, Problem- and Change-Management and their associated control boards.
  - Classify your assets with respect to the security triad (CIA – Confidentiality, Integrity, Availability)
  - Establish a security relevant reporting (analyze IDS-, Firewall-, Web-Logs, Virus-Report, etc; Be involved in incident- and change management)
- ✓ Risk Management
  - Assess your environment regarding risks, threats and vulnerabilities ; Evaluate the risk exposed to your assets
  - Perform an impact analysis based on the risk assessment; Evaluate an overall risk level
  - Manage the risk by *Avoiding*, *Mitigating*, *Transferring* or *Accepting* the risk
- ✓ Patch Management
  - Maintain security, at least, by implementing a patch management process (automated or manual)
  - Monitor security intelligence resources to become aware of vulnerabilities and exposures.
  - Classify the patches according their severity.
  - Test the patches on a production similar environment and document the findings; Develop a "how to" guideline for implementation.
- ✓ Side Notes
  - Re-Assess (audit) your environment on a regular basis (e.g. once a year)
  - Scan your perimeters on a regular base, at least after each change in the environment
  - Get the commitment from the senior management (and therefore also the money and resources)
  - Plan your IT budget to have the resources for security maintenance.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Allocate recourses and responsibilities within all involved departments

✓ Document, document, document… Be smart and document all steps you have done or you plan to do as well as you write down all policies, procedures, findings, vulnerabilities, exposures, released advisories and whatever else is considered to be important to do your job.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Annex A: Quantitative Risk Assessment [42] – Example

In order to get the attention from your senior management the quantitative risk assessment is might be the best choice to do so. As it is the real world, senior management is always very busy and you need to get their attention for your affairs.

Methods for assigning monetary value to an asset:

SLE (Single Loss Expectancy) **= AV** (Asset Value) **x EF** (Exposure Factor)

Asset Value (AV) is the monetary value of an asset

Exposure Factor (EF) is the percentage of loss an event would have on an asset

Example: Assume that an e-commerce website will have revenue of $1 M per day due to 100% availability of the web servers. If an successful attack shuts down the server for 6 hours means, that the exposure factor is 25% (100% X 6h / 24h). The asset value is $1M, therefore your SLE is:

$1M x 25% = $250.000 SLE loss in revenue

ALE (Annual Loss Expectancy) **= SLE x ARO** (Annualized Rate Occurrence)

Annualized rate occurrence (ARO) is the estimated amount of times at which an event occurs.

Taking the example from above, i.e. if you expecting that your web servers will be attacked once each month you should exceed your calculation by the ARO of 12 (once each month – 12 a year):

SLE ($250.000) x 12 = $3M ALE loss in revenue

[42] cf. SANS Security Essentials Cookbook (page 828 ff) [SANS-CBK]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Annex B: Security Intelligence Web Resources [43]

Description	Link
CERT® Coordination Center Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213 -3890, U.S.A.	www.cert.org
bugtraq.org mailing list; security t hreat posting list	www.bugtraq.org
Internet Storm Center , operated by SANS.org	http://isc.sans.org
SANS (SysAdmin, Audit, Network, Security) Institute	http://sans.org
Homepage of the "N *map Security Scanner* "	http://www.insecure.org
Homepage of *INFOSYSSEC* - The Security Portal for Information System Security Pr ofessionals	http://www.infosyssec.net/
Homepage of *Center for Internet Secur ity*	http://www.cisecurity.org/index.html
Homepage of the *Computer Security Resource Center* (CSRC) as part of the National Institute of Standards and Technology	http://csrc.nist.gov/
Homepage of the *National Institute of Standards and Technology (NIST)*	http://www.nist.gov/
Homepage of the " *Nessus Vulnerability Scanner* "	http://www.nessus.or g
SecurityFocus , security resources website, vendor independent, lot of security mailing lists available	http://www.securityfocus.c om
Microsoft " *Trustworthy Computer Security* " homepage	http://www.microsoft.com/security/
Microsoft TechNet " *IT Pro Security Zone* "	http://www.microsoft.com/technet/secu rity/community/defaul t.mspx
Homepage of the *CVE* initiative "Common Vulnerabilities and Exposures (CVE ®) is: A list of standardized names for vulnerabilities and o ther information security exposures"	http://www.cve.mitre.org/
Homepage of *ISS' X-Force* research	http://xforce.iss.net/xforce/alerts
Homepage of *SOPHOS* , an anti -virus solution vendor, free mailing list available	http://www.sophos.com
Homep age of *Trend Micro* , an anti -virus solution vendor	http://trendmicro.com
IT Baseline Protection Manual from the German " Bundesamt für S icherheit in der Informationstechnik"	http://www.bsi.bund.de/gshb/engli sh/m enue.htm
Security book is intended as a 'self help' guide to computer & network security	http://www.boran.com/security/

[43] Please note: This list doesn't claim to be complete!

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Annex C: Advisory documentation template

In this annex you'll provided with a template for advisory recording and tracking. This has to be seen as an example and is not limited to these points. Nevertheless, it's recommended to record the advisories in an appropriate manner, e.g. a database or excel-sheet to keep changes up to date:

Running Number:	*Internal reference within your recording*
Date of release:	*Date when the advisory was released*
Advisory number:	*Number given from the releasing institute*
Advisory Source:	*Releasing institute*
Brief description:	*Headline of the advisory*
Affected Operating System:	*Summarize all affected OS; if it is an update include the date of the update*
Affected Software:	*Summarize all affected SW/ Applications; if it's an update include the date of the update*
Enterprise system affected :	*Here you declare which of your systems seems to be affected*
Reference to CAM:	*Gives the reference to the CAM database*
Reference to Incident Management:	*Reference to your incident management (e.g. trouble-ticket tool) in case you are affected*
Likelihood Severity:	*Severity from LOW to VERY-HIGH*
Impact Severity:	*Severity from LOW to VERY-HIGH*
Overall severity:	*Overall risk level from LOW to VERY-HIGH*
Status:	*Examples: Open, under investigation, testing, pending, closed (or similar)*
Assignment:	*The group within your company which currently has the assignment, e.g. Sec-Mgmt., Develop-ment, Testing, Ops.-Mgmt., Administrators, etc.*
Patch available:	*Is a patch available? Note the source!*
Remarks:	*Any kind of comments!*

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

Internet Resources

[CVE-Def]
Dictionary of standarized names of information security Vulnerabilities and Exposures; **CVE** "*Common Vulnerabilities and Exposures* ", terminology of " *Vulnerability* " and " *Exposure* " ; Maintained by MITRE Corporation
www.cve.mitre.org/about/termi nology.html ; (03.10.2004)
http://www.mitre.org/ ; (03.10.2004)

[ITIL-OGC]
Website of **OGC, Office of G overnment Commerce** , "*Information Technology Infrastructure Library* ", (04. April 2002)
http://www.ogc.gov.uk/index.asp?id=2261 ; (03.10.2004)

[ITIL-ITSM]
Website of **ITIL & ITSM World, "** *Directory of ITIL and ITSM services & software. A launch pad for the IT infrastructure library (ITIL) & ITSM* "
http://www.itil-itsm-world.com/ ; (03.10.2004)

[ISS-IRIS]
ISS - *Internet Security Systems' X -Force Internet Risk Impact Summary Report for Q3 2003* , November 18, 2003
http://bvlive01.iss.net/issEn/deliv ery/prdetail.jsp?type=&oid=23118 ; (03.10.2004)

[NIST-800-30]
CRSC-NIST : *Risk Management Guide for Informa tion Technology Systems* , published January 2002
http://csrc.nist.gov/publications/nistpubs/800 -30/sp800-30.pdf ; (03.10.2004)

[NIST-800-40]
CRSC-NIST : *Procedures for Handling Security Patches* , published September 2002
http://csrc.nist.gov/publications/nistpubs/800 -40/sp800-40.pdf ; (03.10.2004)

[NIST-800-42]
CRSC-NIST : A complete guideline to *Network Secu rity Testing Overview* , published October 2003
http://csrc.nist.gov/publications/nistpubs/800 -42/NIST-SP800-42.pdf ; (03.10.2004)

[Pinkerton]
Pinkerton Consulting & Investigations Inc .: *2003 US Top Security Threats Survey - TOP SECURITY THREATS and MANAGEMENT ISSUES FACING CORPORATE AMERICA, 2003* ; **available after free registration**
http://www.ci-pinkerton.com/news/pdf/Pinker tonTopThreats2003.pdf ; (03.10.2004)
http://www.ci-pinkerton.com/news/confirmPa pers.html ; (03.10.2004)

[Gartner]
Gar tner, Inc ., research and advisory firm for technology, founded 1979
www.gartner.com ; (03.10.2004)

[McKinsey]
McKinsey&Company , management consulting firm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

www.mckinsey.com ; (03.10.2004)

[SRAD]
C&A Security Risk Analysis Group , *Security Risk Analysis Directory, Introduction to Security Risk Analysis*
http://security-risk-analysis.com/ ; (03.10.2004)

[HypDic]
Hyperdictionary – Online Dictionary
http://www.hyperdictionary.com ; (03.10.2004)

[OICT-RM]
NSW Office of Information and Communications Technology (OICT); *Information Security Guideline for NSW Government - Part 1 Information Security Risk Management* - Issue No: 3.2
First Published: Sept 1997
Current Version: Jun 2003
http://www.oit.nsw.gov.au/Guidelines/4.3.16.a.security.asp ; (03.20.2004)

[OICT-ROSI]
NSW Office of Information and Communications Technology (OICT) ;*Return on Investment for Information Security Guideline* - Issue No: 1.0
First Published: September 2003
Current Version: September 2003
http://www.oit.nsw.gov.au/Guidelines/4.3.37.a.ROSI.asp ; (03.10.2004)

[MS-Bulletins]
Microsoft Corporation Security Bulletins website
http://www.microsoft.com/security/security_bulletins/ ; (03.10.2004)

[CIO]
Joe Wang , *CEO and president of LANDesk, based in South Jordan, Utah, answers your questions about patch management* ; **CIO.com** website posting December 23, 2003
http://www2.cio.com/ask%5Cexpert/2003/questions/question1847.html ; (03.10.2004)

[COBIT]
IT Governance Institute , *Cobit Mapping - Overview of International IT Guidance* , 2004
http://www.isaca.org/Template.cfm?Section=About_Isaca&Template=/ContentManagement/ContentDisplay.cfm&ContentID=10016 ; (03.10.2004)

[ITGI]
IT Governance Institute, Issued *Cobit, Control Objectives for Information and related Technology* , IT business process and control framework
http://www.itgi.org/ ; (03.10.2004)

[ISACA]
Information System Audit and Control Association,
http://www.isaca.org/; (03.10.2004)

[FCW]
Rutrell Yasin , *In need of a quick fix* ; ***FCW.com*** website posting December 1, 2003
http://www.fcw.com/fcw/articles/2003/1201/cov-patch-12-01-03.asp ; (03.10.2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Books and Guidelines

[SANS-CBK]

SANS Security Essentials with CISSP CBK Volume One
Eric Cole, Jason Fossen, Stephen Northcutt & Hal Pomeranz , SANS Security Essentials with CISSP CBK Version 2.1 Volume One, published by SANS Press
First Printing February 2003
Second Printing April 2003
ISBN 0-9724273-6-8

[ITILBOOK]

Security Management, IT Infrastructure Library (OGC)
Office of Government Commerce, published by The Stationery Office
First published 199 9
Second Impression 2001
ISBN 0-11-330014-X

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.