Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Patch Management and the Need for Metrics

The principle objective of `Patch Management and the Need for Metrics' is to demonstrate that organisations cannot meaningfully assess their security posture; with reference to their patch status, without the use of appropriate metrics.

Copyright SANS Institute
Author Retains Full Rights

AD

Patch Management and the Need for Metrics

Kenneth J. MacLeod

14th July 2004

SANS Security Essentials GSEC Practical Assignment
Version 1.4b
(Option 1)

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Abstract

The principle objective of '*Patch Management and the Need for Metrics*' is to demonstrate that organisations cannot meaningfully assess their security posture; with reference to their patch status, without the use of appropriate metrics.

This paper gives a detailed overview about what patch management is, why it is performed, the pro's and con's of patching, the risks a business is exposed to by security vulnerabilities and the associated costs of security breaches against unpatched systems. Finally, the paper goes on to suggest several patch metrics that can be applied to provide organisations with a quantitative view of their patch status.

© SANS Institute 2004, Author retains full rights.

Table of Contents

The need for Patch Management 1
Patch Management and Risk 1
Building the case for a Patch Management Process 2
Why software contains vulnerabilities 3
Patch Management in the context of Defence-in-Depth 3
Traditional Perimeter around digital assets is changing 4
An explanation of Malware – Worms, Viruses, Trojans 4
Firewall and Anti-Virus products no longer offer enough protection ... 5
Understanding Risk with reference to Vulnerability and Threat 6
Malware – now surfaces more quickly after patch release 7
Pro's and Con's of Patch Management 8
The Potential Costs of failing to patch 9
Making the case for Metrics 10
Patch Management Metrics 11
Proposed Patch Management Metrics 12
Metric-1 Percentage Patch Coverage for IP Subnet 13
Metric-2 Percentage Critical Patch Coverage per IP Subnet 14
Interpreting the different Patch Metrics 14
Metric-3 Percentage Patch Coverage for Latest Critical Patch 15
Metric-4 Patches missing per device 15
Metric-5 No. of Devices having problems after patching 15
Metric-6 No. of Applications with problems after patching 15
Benefits derived from using Patch Metrics 15
Time Based Metrics 16
Potential Conflict of Security Metrics with other Metrics 17
Security and Corporate Governance 17
Management Reporting of Security Metrics 18
The Future -- can the new Intrusion Prevention technology help 19
Conclusions 20
References i

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The need for Patch Management

Patch Management is one element of a change-management process that allows us to install vendor supplied software *'patches'* to correct deficiencies that exist in the vendor's software product. It is only one of several layers that should form part of an organisations *'Defence-in-Depth'* strategy.

Patch Management is now a major component in any organisations security programme, as Chan [1] cites:

> *The rise of widespread worms and malicious code targeting known vulnerabilities on unpatched systems, and the resultant downtime and expense they bring, is probably the biggest reason so many organizations are focusing on patch management.*

To emphasise the need for Patch Management the paper by McGhie [2] references a statement **…** *"Gartner reports that over 90% of the security exploits are carried out through vulnerabilities for which there are known patches".*

This highlights the fact that any organisation implementing a well thought out patch management process is on the right track in reducing its exposure and risk to published security vulnerabilities.

Patch Management and Risk

Your patch management policy should be designed to mitigate against the risks to the business presented by computing devices that are missing patch updates for known published vulnerabilities.

Also, when discussing patching within the context of risk management it is important to understand that with Risk Reduction [3] *"You cannot eliminate risk … as the number of vulnerabilities is infinite".*

Vulnerabilities appear within software over time, usually after the software vendor has released the software product to market. These vulnerabilities can be exploited by various forms of '*Malware*' (i.e. Viruses, Worms, Trojans and combinations of these, sometimes referred to as blended threats).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Building the case for a Patch Management Process

The fundamental patch management objective for most organisations is to ensure that published vulnerabilities are patched with the software provided by the vendor before any '*Malware*' is released into the public domain.

It is important that patch management processes and procedures are developed and maintained to keep the Networking Devices, Servers, PCs, Operating Systems and Applications protected by the latest security patches.

In order to implement our patch management process, we may be using particular point solutions (e.g. automated tools like vulnerability scanners and patch deployment software). However, any tool used is not an adequate solution in itself, unless it is used effectively within a well thought out process.

This point is well illustrated by Bruce Schneier [4] where he states **…** *"If you think technology can solve your problems, you don't understand technology and you don't understand your problems".*

Also, Chan [5] states in his conclusion that *"While the issue of patch management has technology at its core, it's clear that focusing only on technology to solve the problem is not the answer".*

Chan goes on to highlight that*, "Installing patch management software or vulnerability assessment tools without supporting guidelines, requirements, and oversight will be a wasted effort that will further complicate the situation."*

Fontana [6] highlights**:**

> *Companies need to have several pieces in place before a patch management process can be installed: network inventory, change management, configuration management, asset management, formalized record keeping, an understanding of costs, prioritization guidelines, and maintenance and communications plans.*

It is sometimes useful to appreciate that any unpatched device within your network is essentially the hackers' *'Man-In-Your-Camp'*.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Why software contains vulnerabilities

The question as to why these vulnerabilities come to exist within software in the first instance is a large subject in itself, usually covered in software engineering texts and papers under the headings of software reliability.

However, in dealing with this inherent malaise with software in general, Schneier [7] suggests that software vendors should be made more accountable for the quality of their products in line with manufacturers of non-software products.

In his article he states that **…** *"Real security improvement will only come through liability—holding software manufacturers accountable for the security and, more generally, the quality of their products".*

Patch Management in the context of Defence-in-Depth

In reference to Lindquist [8] we can appreciate that whereas the corporate perimeter was once protected by firewalls we now rely on more of a '*Defence-in-Depth*' approach where patching only represents one layer of a multi-layer portfolio of security countermeasures.

Some of the security layers that may form part of an organisations '*Defence-in-Depth*' strategy at the present time are as follows**:**

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Encryption
- Anti-Virus Systems
- Hardened Systems and
- Patch Management Processes and Procedures

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Traditional Perimeter around digital assets is changing

It is now generally accepted that the traditional perimeter surrounding the digital assets of a business is beginning to erode. This has largely been attributed to the advent of the Internet, Mobile Devices, Remote-Working and the introduction of wireless technologies.

Over time, the threats are constantly evolving, therefore the countermeasures also need to be evolving. The '*Defence-in-Depth*' approach is a realisation of the fact that no single product, be it firewalls or anti-virus, is enough to counter most current security threats.

Also, we must recognise that the products of today are unlikely to be appropriate for tomorrow's threats.

As Lindquist [8] indicates, *"we need to think beyond perfecting the digging of moats around the corporate castle only to find that we are now living in a world of bomber planes and guided missiles."*

It is also important to appreciate that any viruses or worms resident on one of your PCs, that is physically outside of the corporate network, can come up through your VPN and get onto your network.

This point is well illustrated in Steinberg [9] where he points out that **…** *"Worms and Viruses may utilise the SSL VPN to tunnel into the corporate network."*

An explanation of Malware – Worms, Viruses, Trojans

It is important to understand the different forms of *'Malware'* and how they can affect systems.

The 2003 Attacks Summary [10] provides details on the main *'Malware'* of 2003. An additional source explaining the various classifications of *'Malware'* can be found in [11] '*Viruses are from Venus Worms are from Mars*'.

These known published pieces of *'Malware'* represent some of the major threats to current vulnerable systems.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Firewall and Anti-Virus products no longer offer enough protection

The ongoing patching of systems is now a requirement because Firewalls and Anti-Virus products do not have sufficient capabilities on their own to prevent security breaches.

The fundamental principle behind '*Defence-in-Depth*' is that no single security product is full-proof and that you are required to have several layers of security products in place.

The weaknesses in Anti-Virus products is highlighted by Skoudis [12] *"Desktop AV may be leaving you wide open to attack … too many of us put unwavering trust in these applications to stop malware attacks".*

Weaknesses in Firewall products are well illustrated in [13] '*Analysis of Vulnerabilities in Internet Firewalls*'.

Continuing with this theme, Hill [14] discusses how easy it is to fool a Firewall either by changing the port numbers associated with a protocol or by using a protocol tunnel.

Van Hauser [15] discusses possible backdoors through different firewall architectures.

Software versions of firewall products have been found to be vulnerable to buffer overflows. In particular, the Witty Worm of 2004 [17] specifically targeted a published vulnerability in the [**] BlackICE ™ firewall product.

[**] BlackICE ™ is a trademark product of ISS Internet Security Systems http://www.iss.net/

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Understanding Risk with reference to Vulnerability and Threat

It is important to understand the relationship between Risk, Vulnerability and Threat in the context of patching and patch management.

Patch Management is performed because vulnerabilities exist in software. When a credible threat can target a vulnerability, then you have an identifiable risk that will remain as long as the threat exists.

However, once the vulnerability has been successfully patched, then the risk has been removed for that patched device even though the threat remains in place.

The relationship between Risk, Threat, Vulnerability and Cost (*Impact*) is well illustrated in the equations referenced in [16].

Risk = Threat x Vulnerability

This first equation is sometimes refined to take the associated Cost (Impact) into account.

Risk $_{\text{(due to a threat)}}$ = Threat x Vulnerability $_{\text{(to that threat)}}$ x Impact

You need to experience a level of threat to a vulnerability and a significant impact (Cost) for the vulnerability to present a significant risk to the business.

The vulnerability in itself only represents a piece of information. When a credible threat exists which can exploit this vulnerability and the associated Cost (Impact) is significant, then your risk is real.

For example, the specific vulnerability presented by the RPC-DCOM flaw identified in July 2003 represented a piece of information or *'intelligence'* to I.T. Security personnel.

When a credible threat, in the form of the *'exploit-code'* was known to exist, then your risk assessment process would possibly have directed that applying the critical patch (MS03-026) should commence immediately.

When the MS-Blast worm finally appeared, the threat was concrete and the risk of a security breach occurring on unpatched systems was extremely high.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Malware – now surfaces more quickly after patch release

Although the vast majority of exploits are targeted at Microsoft software, the recent '*Witty*' worm established that no vendor's product is safe from exploit. This worm also demonstrated the new trend of worms appearing very quickly after a patch is released.

Shannon and Moore [17] give a thorough analysis of '*The Spread of the Witty Worm*'. In their conclusion they present a disturbing view of reality of the new trend in security breaches. **…**

> *The Witty worm incorporates a number of dangerous characteristics. … The practical implications of this are staggering; with minimal skill, a malevolent individual could break into thousands of machines and use them for almost any purpose with little evidence of the perpetrator left on most of the compromised hosts.*

This report goes on to highlight that '*Witty*' was the first widespread Internet worm to actually direct an attack at a security product and the authors suggest that the model in which we apply patches to plug '*security-holes*' is no longer viable.

Lemos [18] highlights the very short time available between the patch release and the exploit worm surfacing **…**

> *"The Witty worm first hit computers known to be vulnerable and emerged so quickly that most companies had no time to apply a patch",* according to an analysis of the program.
>
> *"The worm started spreading around the Internet in less than 48 hours after the first public description of the flaw was released."*

Brenner [19] reports that *"security experts said, malicious code writers will continue to find speedier ways to exploit weaknesses. That's why the IT security community needs to find a better way to respond."*

His report goes on to mention that **…** *"Looking at the most recent cycle between vulnerability, and attack and the impact rapid patching has had on an organization, it becomes apparent we'll need additional approaches to protect systems other than installing patches."*

In addition, Foundstone [20] and Bennet and Thomson [21] provide further support to illustrate this shrinking window of opportunity in which to patch.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Pro's and Con's of Patch Management

It is important to appreciate that there are both Pro's and Con's of applying patches to systems. This is the constant dilemma faced by security professionals.

As Thomson [22] implies, *'If you patch your system and something breaks, you are damned. If you don't patch and vulnerable systems are breached by Malware, you are damned.'*

On the surface, from an ideal world perspective, it may appear that every patch should be applied as soon as it is published. Unfortunately, things are rarely that simple. There are many documented cases where patches have corrupted systems and caused failures.

In one example, *'Patch & Pray'* [23], a performance improvement patch was released, but this build contained an older version of the software module that fixed the SQL Slammer flaw. So organisations that applied this performance improvement patch, made their systems vulnerable to SQL Slammer again.

It is because of these types of issues that I.T. professionals are wary of applying patches immediately and try to wait a reasonable period of time to establish if any undesirable *'side-effects'* are reported on internet news-groups etc. Sufficient time is also required to test the new patch on test systems before hand-over to User Acceptance Testing.

If a new patch is seriously flawed, the details tend to be reported in news-groups, the failed patch is usually pulled and a new patch released. However, as discussed earlier, with the time-frame for patching constantly shrinking, this approach may no longer be advised.

'Patch & Pray' [23] states some advantages and disadvantages of the current patch dilemma and identifies that *"there are simply too many vulnerabilities requiring too many combinations of patches coming too fast".*

The author also illustrates the paradox of the vendor that creates the original vulnerability being the same body that produces the patch in the '*Swimmers story*' analogy.

The author builds the case for not applying patches because of the sheer number of patches that cause more problems than they set out to solve, in conjunction with the relatively low number of vulnerabilities that are actually successfully exploited.

However, this is very much a *'Bean-Counter'* view of risk management and may not be appropriate for your environment, as the potential costs associated with security breaches can be substantial.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The Potential Costs of failing to patch

When an organisation does not actively perform patch management or does not perform patching within the available time-frame before the '*Malware*' strikes, then the organisation is exposed to unnecessary risk and subsequent loss.

Some of the risks presented are both the direct and indirect costs sustained by the business when '*Malware*' causes disclosure of data, corruption of data, or data loss (Kaplan [24]).

Some of the costs involved when a rogue program hits the business are**:**

- the cost of clean-up and post-incident recovery,
- the loss of production,
- the loss of sales,
- the cost of overtime for catch-up,
- the potential loss of customers and
- any consequential damage to the reputation of your organisations brand.

Kaplan [25] '*Determining the Cost of a Breach*' and D'Amico [26] in section '*How Cost is Measured*' both provide an insight into some of the costs you should take into consideration in calculating any loss. These lists are by no means complete and organisations should assess the unique cost factors that directly affect them.

Bloor [27] in the section '*Cost to the Business'* details the hard dollar damage done by the Code Red worm as being in excess of $2.6 billion with 359,000 computers infected in less than 14 hours of the worm's release.

According to Luo and Warkentin [28] *"the recent MS Blaster worm cost approximately $475,000 (includes hard, soft, and productivity costs) per company to remediate wounds and that some large companies reported losses as high as $4,228,000 from this worm breach."*

A very recent paper by Weaver and Paxson [29] puts forward a disturbing case estimating the possible costs to the USA of a malicious worm at $50 Billion.

These security breaches can represent significant costs to organisations and as demonstrated via the world media are occurring on an ongoing and frequent basis.

In calculating the costs of not patching versus cost of patching within your environment, you must determine which is worse**;** a patch causing an application or server failure**,** versus a full system breach by a worm.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Making the case for Metrics

The need for measurement within any field is best reasoned by this quote from Lord Kelvin [30] **…**

> *When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge of it is of a meager and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced it to the stage of science.*
>
> **Sir William Thompson, Lord Kelvin (1824-1907)**

Without having available metrics to measure specific aspects of your patch management programme, it is difficult to establish or set appropriate patching targets and objectives.

This in turn makes it impossible to measure deviation from targets and if these deviations are within acceptable tolerance limits.

Metrics can help to demonstrate that your patching efforts are effective and offer the security management team solid information that allow them to communicate security posture to the business stakeholders in a meaningful way.

In *'The ABC's of New Security Leadership'* [31], the authors express the view that - *"Eventually, security will be almost completely metrics-driven. A reliance on metrics is, after all, the mark of a mature corporate function."*

As referenced in NIST [32] '*IT security metrics must be based on IT security performance goals and objectives*.'

Within this paper I will build upon the idea of the metric suggested in NIST [33] in '*Percentage of systems with the latest approved patches installed*'.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Patch Management Metrics

There are currently very few metrics available today in the field of Patch Management.

How can an organisation determine how effective it is in performing patch management, if it cannot provide a quantitative breakdown of its achievements over a period of time?

By asking itself what it can measure, a business learns something valuable, such as the quality and consistency of its existing information security process and policy. In '*Why the Future belongs to the Quants'* [34], the document refers to a suggested metric of *'Patch Coverage'*, which again, I will build upon.

In *'A Guide to Security Metrics'* Payne [35], we see reference to the fact that metrics are generated from analysis and that good metrics are SMART, i.e. Specific, Measurable, Attainable, Repeatable, Time-Dependent.

Some suggested areas for measurement are as follows**:**

(i) The need for Physical Equipment Audits
You should document all appropriate equipment in your organisation to ensure that you have a complete record of what devices should appear on scans.

(ii) Where possible, you should make use of Automated Patch Management Software to Scan, Deploy and Report on Patches

(iii) Extraction of Raw-Data from Automated Patch Management Software Scans, to construct *'Metrics'* that will demonstrate the effectiveness of your Patch Management programme.

(iv) As part of your change management processes you may wish to use Change Control Logs for Critical Infrastructure.

Foundstone [36] states that security metrics essentially change in 3 ways**:**
(i) Over Time, (ii) By Industry and (iii) by Action.

In final support of the case for metrics, Drew [37] states in a recent study that only 45% of information security programs within the financial sector have *" performance goals and metrics to measure [the] program",* and that as a comparison to other disciplines that use metrics the author cites the case that **…**
"This stands in direct contrast to the initiatives around quality that have evolved over the past decades; significant amounts of research show that driving projects and initiatives around quantitative data is a key indicator of success."

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Proposed Patch Management Metrics

Here, I will refer to the collection and reporting of specific patch metrics relating to Microsoft patches.

The following suggested metrics are based on the collection of data captured by the Shavlik HFNetChkPro 4.0 [38] Patch Management software package.

However, the same data could be obtained via other Patch Management software.

NB: It would not be practical to collect this data without the use of automated tools.

Regardless of type of scan you perform you should record the following data**:**

1. Number of Machines Scanned
2. Number of Machines **Not** Scanned
3. Number of Patches Found
4. Number of Patches **Missing**

If you use the Shavlik patch management product to scan an IP range, it will automatically return a summary screen detailing the 4 data elements above. Once you have this information you can then use it to calculate your metrics.

© SANS Institute 2004, Author retains full rights.

Metric-1 Percentage Patch Coverage for IP Subnet

Measures the percentage of all patches found on all scanned devices.

Percentage Patch Coverage per IP Subnet =

[Patches_Found / (Patches_Found + Patches_Missing) **]** * 100

Example:
If there are 40 Patches available for a Windows XP PC and you have 100 PCs in your subnet and each PC had all the possible patches installed, then the scan would return 4000 patches found.

If your scan uncovered total of 3000 patches found across the 100 PCs, (i.e. 1000 patches missing) then this metric would reveal a result of**:**

à [3000 / (3000 + 1000)] * 100
à (3000/4000) * 100
à 75%

i.e. Patch Coverage for Windows XP PCs on this IP Subnet = 75%

It is important you understand that this metric could account for 10 patches missing per individual PC or for all patches missing for 25 PCs. You would need to use the patch management tool to find the specific details.

© SANS Institute 2004, Author retains full rights.

Metric-2 Percentage Critical Patch Coverage per IP Subnet

Measures percentage of critical-patches found on all scanned devices.

Percentage Critical Patch Coverage per IP Subnet =

[CriticalPatches_Found / (CriticalPatches_Found + Patches_Missing) **]** * 100

This depends on you creating and maintaining a "Patch-Group" called Critical Patches that contains all the patches that your organisation have deemed to be critical.

You would then perform the scan for your IP Subnet Range with this "Critical Patch Group".

Example:
If there are 40 Patches available for a Windows XP PC it may be the case that only 20 of these patches are critical. These 20 Critical Patches would be added into a Critical-Patch-Group and this group would form the basis of the scan.

If you have 100 PCs in the scan and each PC had all the possible *'Critical Patches'* installed, then this would account for 2000 *'Critical Patches'* found.

However, if your scan uncovered total of 1800 patches found across 100 PCs, (i.e. 200 patches missing) then this metric would reveal a result of**:**

à [1800 / (1800 + 200)] * 100
à (1800/2000) * 100
à 90%

i.e. Critical Patch Coverage for Windows XP PCs on this Subnet = 90%.

Interpreting the different Patch Metrics

On the surface Metric-1 states that you are only 75% covered for all patches, but using Metric-2 provides more information by demonstrating that you are 90% covered for all *'Critical Patches'*.

Various different metrics can be used together to build an overall picture of your patch-status. You may wish to record these two metrics on a daily basis to track the *'Percentage of devices patched'* before**:**

(*Time-E*) - time that any exploit-code was released
(*Time-W*) - time when the actual worm was released

This could provide useful feedback information for management.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Metric-3 Percentage Patch Coverage for Latest Critical Patch

If Metric-2 were modified slightly for the *'Latest Critical Patch'* and you recorded this metric each day, you would then be in a position to state, for example, that before (*Time-E*) you were 65% covered for the *'Latest Critical Patch'* and before (*Time-W*) you were 85% covered.

Metric-4 Patches missing per device

Use your patch management tool to record total number of devices with**:**

- 0 missing patches
- 1 missing patch
- 2 or more missing patches (i.e. defined to the levels that you require)

Metric-5 No. of Devices having problems after patching

Metric-6 No. of Applications with problems after patching

With Metric-5 and Metric-6, you would likely require the support of your service desk team to provide accurate feedback as to any problems being reported with specific devices or applications after patches had been applied.

Benefits derived from using Patch Metrics

The fact that these types of measurements are actually being recorded at all, should demonstrate due diligence to senior management and auditors that there is a measurable patch management process in place.

Trends can be monitored over time and management can have some visibility as to how effectively their Security Policies are being implemented and as a result, improvement plans can be developed for under-performing areas.

You should also be in a position to tie your patch metrics directly to your Security Policies and Procedures. For example, if your Security Policy states that all patches deemed critical by Microsoft will be applied to the affected platforms within 7 working days, subject to local testing, then your metric can help to ensure that your policy is being adhered too.

Finally, you need to balance the patching requirements against the risks. Your metrics should reflect your specific environment. There is no point in measuring a metric for all security patches when you are only ever going to apply the *'Critical Security Patches'* that your risk assessment have deemed appropriate.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Time Based Metrics

Developing time-based patching metrics allows us to track how effective our patching efforts are before a worm is released. For example, if you can state to management that 90% of your devices were patched prior to the worm being released you have quantitative data.

Foundstone [20] references the fact that *"the cycle from vulnerability to worm is shortening dramatically – putting increasing pressure on IT departments to remediate vulnerabilities faster than ever."*

Two of the most publicised worm based exploits of the Windows platform were the MSBlast/Lovesan Worm of August 2003 and the more recent Sasser Worm of May 2004. There is a timeline that exists for all worms.

1. Information about the vulnerability is released to the software vendor
2. The software vendor takes the decision to fix the vulnerability
3. The vendor releases a software patch to fix the vulnerability
4. Individuals or Groups set about producing credible "Exploit-Code"
5. A worm is released to exploit the published vulnerability

Here are the specific timelines for MSBlast and Sasser worms:

Patch Released	*Exploit-Code Released*	*Worm Released*
16th Jul 2003	29th Jul 2003[(a)]	(MSBlast) 11th Aug 2003
13th Apr 2004	17th Apr 2004[(b)]	(Sasser) 1st May 2004

[(a)] http://www.computerworld.com/securitytopics/security/story/0,10801,83525,00.html
[(b)] http://www.arnnet.com.au/index.php?id=277437400&fp=4&fpid=1382389953

For DCOM-RPC Vulnerability exploited by MSBlast
(i) 13 Days between patch release and initial 'Exploit-Code'.
(ii) 13 Days between "Exploit-Code" and final 'MSBlast Worm'.
(iii) 26 Days between patch release and final 'MSBlast Worm'.

For LSASS Vulnerability exploited by Sasser
(i) 4 Days between patch release and initial 'Exploit-Code'.
(ii) 14 Days between "Exploit-Code" and final 'Sasser Worm'.
(iii) 18 Days between patch release and final 'Sasser Worm'.

In producing time based patch objectives and metrics you can attempt to make your patching efforts fit the time available and measure your effectiveness in doing so.

For example, your security goal might be to achieve 50% coverage between patch release and exploit-code release, with the remaining 50% of devices being patched immediately after the release of the exploit-code.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Potential Conflict of Security Metrics with other Metrics

It is likely that in achieving patch targets, your system uptime or availability may be compromised. This potential conflict must be managed at the appropriate level.

Security Teams and System Administrators should not be working at crossed purposes and their specific targets and metrics should be designed to work together to avoid potential tension and conflict.

If applying the latest critical patch to servers causes 20 minutes downtime per server, this must be factored into the system availability metrics that may be used by system administrators and the operations support team.

Accurate records should be maintained to demonstrate how effective the patch management programme is, when rolling out a new patch.

Security and Corporate Governance

Security Teams are responsible to their senior management and stakeholders within the organisation to ensure that security policies are matched to appropriate corporate governance guidelines.

As Swindle [39] states **…** *"Information security, though often viewed as a set of technical issues, must be embraced as a corporate governance responsibility that involves risk management, reporting controls, testing and training, and executive accountability."*

In the second page of this report, the author makes reference to the USA Sarbanes-Oxley Act and the fact that legislators in California have established regulatory regimes that determine how organisations must secure consumer information if they want to avoid severe civil penalties and potential class-action litigation.

Similar types of legislation are being developed within Europe and the UK.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Management Reporting of Security Metrics

When Senior Management ask '*What is the current security patch status within our organisation*', it will not be satisfactory to respond with statements of excellent, good, fair or poor without hard data to back up your position.

This is where metrics can help.

If you can state categorically that for 1000 devices on your network that there are 8000 patches found, 35 patches missing and all service packs are in place, then you are in a position to convey solid information.

Your organisation can then devise reports based on targets that allow you to communicate your patch status based on the well publicised '*Traffic Light*' indicator system. For example, you could communicate a high level view of your Global Critical Patch Status based on arbitrary guideline of **:**

- *'Green'* for 'Critical Patch Coverage' of 95% and above
- *'Amber'* for 'Critical Patch Coverage' of 85% - 94%
- *'Red'* for 'Critical Patch Coverage' of below 84%

For example, this could result in a high-level patch summary report as follows:-

Region	*%age Critical Patch Coverage*	*Status*
Country-A	95	
Country-B	90	
Country-C	96	
Country-D	80	

Traffic-Lights taken from Clip-Art Gallery.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The Future -- can the new Intrusion Prevention technology help

As discussed in this paper, there is a shrinking window of opportunity in which to apply security patches to vulnerable devices. As a consequence, security products are evolving to counter these threats.

The vast majority of security vendors are now including Intrusion Prevention technologies into their product offerings.

As there are so many products available I have confined my reference to the McAfee product. McAfee have evolved their security product offering into McAfee VirusScan Enterprise 8.0i as referenced in *'Mena Report'* [40] and by Jaques [41].

This new class of product should provide organisations with sufficient protection to perform their patching processes on their own timescales rather than being forced to patch before the next worm surfaces.

© SANS Institute 2004, Author retains full rights.

Conclusions

It is important to remember that *'Patch Management'* is only one critical element of an organisations *'Defence-in-Depth'* strategy. Organisations must consider developing security metrics similar to those discussed in this paper to measure the effectiveness of their patch management efforts.

With the potential high costs associated with security breaches and the decreasing window in which to apply security patches, security teams need to be constantly reviewing processes and technologies that can mitigate against the risks.

With constantly evolving corporate governance and security related legislation emerging within the USA and Europe, any appropriate methods that can provide quantitative results for patch management efforts, will help demonstrate due diligence to your senior management, stakeholders and auditors.

References have been presented in this paper identifying the fact that patching alone will not solve the problems of *'Malware'* based security breaches. Rather, we need to adopt complimentary approaches that will fit with the current patching paradigm.

The current releases of Intrusion Prevention System products are now more intelligent, in that they do not rely purely on pre-defined '*signatures*' to detect *'Malware'*. This will very likely diminish the requirement to perform patching on a reactive and knee-jerk basis.

However, as long as patching remains a business requirement, the case for using appropriate patch metrics will remain strong.

As a final point, for organisations that were infected by the *MSBlast* worm of August 2003, the associated clean-up cost was on average $475,000 per organisation. It is therefore reasonable to imply that every time a new worm fails to affect your organisation, because your systems were patched, you have achieved significant *'Cost Avoidance'* for your organisation.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References

1. Chan, Jason, "Patch Management Essentials", January 2004, PatchManagement.org, URL: http://www.patchmanagement.org/pmessentials.asp

2. McGhie, Lynda, "Software Patch Management – The New Frontier", SBQ – Secure Business Quarterly, Volume Three- Issue Two, URL: http://www.sbq.com/sbq/patch/sbq_patch_lmcghie.pdf

3. Kurtz, George, "Security Risk Management: Nine Required Steps to Successfully Implement Vulnerability Management", , URL: http://loop.interop-comdex.com/comments/172_0_1_0_C/

4. Schneier, Bruce, "Secrets & Lies: Digital Security in a Networked World". New York: John Wiley & Sons, Inc., 2000. (Preface Page xii)

5. Chan, Jason, "Essentials of Patch Management Policy and Practice", March 2004, @stake, URL: http://www.atstake.com/research/reports/acrobat/atstake_patch_mngmnt.pdf

6. Fontana, John, "How to Handle Patch Management", 12/01/03, NetworkWorldFusion, URL: http://www.nwfusion.com/research/2003/1201howtopatch.html

7. Schneier, Bruce, "Hacking the Business Climate for Network Security" April 2004, IEEE Computer, URL: http://www.schneier.com/essay-ieeecomputer.pdf

8. Lindquist, Christopher, "The World is Your Perimeter", February 2004 CSO Magazine, URL: http://www.csoonline.com/read/020104/perimeter.html

9. Steinberg, Joseph, "SSL VPN Security", 16 May 2003, URL: http://www.sans.org/rr/wp/SSL_VPN.pdf

10. "A Roundup of recent Worms, Trojans and Malicious Code", WholeSecurity – 2003 Summary of Attacks, URL: http://www.wholesecurity.com/news/media_kit_resources/2003_Attack_Summary.pdf

11. Cooper, Russ, "Viruses are from Venus and Worms are from Mars", October 2003, The Remediator – Security Digest, Shavlik, URL: http://www.internetviz-newsletters.com/shavlik/e_article000193116.cfm?x=%5B%5BIMN.LID%5D%5D,%5B%5BIMN.USER_ID%5D%5D

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

12. Skoudis, Ed, “Desktop AV may be leaving you wide open to attack”,
June 2004, Information Security Magazine, URL:
http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss407_art803,00.html

13. Kamara, Seny; Fahmy, Sonia; Schultz, Eugene; Kerschbaum, Florian;
Frantzen, Michael, “Analysis of Vulnerabilities in Internet Firewalls”,
12/01/03, (CERIAS) Purdue University, URL:
http://www.cs.jhu.edu/~seny/pubs/firewall-analysis.pdf

14. Hill, Jake, “Bypassing Firewalls: Tools and Techniques”,
March 2000, URL:
http://www.megasecurity.org/Firewalls/Bypassing_firewalls.pdf

15. van Hauser, “Placing Backdoors through Firewalls v1.5, URL:
http://www.itsecurity.com/papers/p37.htm

16. Cole, Eric; Fossen, Jason; Northcutt, Stephen; Pomeranz, Hal,
“SANS Institute: 1.2 Defense In-Depth”,
2004, (SANS Security Essentials and the CISSP 10 Domains), Chpt 7 p28 & 29

17. Shannon, Colleen & Moore, David, “The Spread of the Witty Worm”,
April 2004,CAIDA Analysis, URL:
http://www.caida.org/analysis/security/witty/

18. Lemos, Robert, “Witty Worm Frays Patch-Based Security”,
March 2004, CNET News.com, URL:
http://news.com.com/2100-7355_3-5180482.html

19. Brenner, Bill, “Sasser shows that there must be a better way”,
May 2004 SearchSecurity.com, URL:
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci963170,
00.html?track=NL-358&ad=482644

20. Computer Vulnerability-to-Worm Cycle Compressing Dramatically
May 2004, Foundstone website, URL:
http://www.foundstone.com/index.htm?subnav=company/navigation.htm&subco
ntent=/company/pressrelease_template.htm%3Findexid%3D132

21. Bennet, Madeline; Thomson, Iain, “Patching Gap gets Narrower”,
May 2004, IT Week, URL:
http://www.vnu.co.uk/news/1154925

22. Thomson, Iain, “Did Sasser leave you shamefaced”
12 May 2004, vnunet.com, URL:
http://www.vnu.co.uk/comment/1155099

23. Berinato, Scott, “Patch and Pray”,
August 2003 CSO Magazine, URL:
http://www.csoonline.com/read/080103/patch.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

24. Kaplan, Simone, “It’s not easy being breached”,
December 2002 CSO Magazine, URL:
http://www.csoonline.com/read/120902/cost.html

25. Kaplan, Simone, “Criteria for Determining the Cost of a Breach”,
December 2002 CSO Magazine, URL:
http://www.csoonline.com/read/120902/cost_sidebar_1_664.html

26. D’Amico, Anita D., “What does a computer security breach really cost”,
September 2000, SANS Institute Paper, URL:
http://www.avatier.com/products/PasswordBouncer/docs/CostsOfBreaches-SANSInstitute.pdf

27. “The Patch Problem – It’s costing your Business Real Dollars”,
Baroudi Bloor 2003, URL:
http://mithras.itworld.com/download/special_reports/smallbusiness/PatchProblemReport_BaroudiBloor.pdf

28. Luo, Xin and Warkentin, Merrill,
“Assessment of Information Security spending & costs of failure” , URL:
http://www.information-institute.org/security/3rdConf/Proceedings/96.pdf

29. Weaver, Nicholas; Paxson, Vern “A Worst-Case Worm”,
May 5, 2004, URL:
http://www.icir.org/vern/papers/worst-case-worm.WEIS04.pdf

30. Lord Kelvin, “Quote on Measurement”, URL:
http://www.quantum-earth.com/Anap/Lord%20Kelvin%20measurement%20quote.htm

31. Berinato, Scott; Daintry, Duffy; Scalet, Sarah; Wailgum, Tim; Wheatley, Malcolm, “The ABC’s of New Security Leadership”
February 2004, CSO Online, URL:
http://www.csoonline.com/fundamentals/abc_leadership.html

32. Swanson, Marianne; Bartol, Nadya; Sabato, John; Hash, Joan; Graffo, Laurie, “NIST Security Metrics Guide for Information Technology Systems”,
URL:
http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf,
Page vii - Executive Summary

33. Swanson, Marianne; Bartol, Nadya; Sabato, John; Hash, Joan; Graffo, Laurie, “NIST Security Metrics Guide for Information Technology Systems”,
URL:
http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf,
Section 10.3 Are Systems managed to reduce vulnerabilities (p73 A-37) from Appendix-A Sample IT Security Metrics

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

34. Greer, Daniel, Jr.; Soo Hoo, Kevin; Jaquith, Andrew,
"Information Security: Why the Future Belongs to the Quants",
July/August 2003, Published by IEEE Computer Society, @stake, URL:
http://www.atstake.com/research/reports/acrobat/ieee_quant.pdf

35. Payne, Shirley C., "A Guide to Security Metrics",
11 July 2001, SANS GSEC Practical Assignment, URL:
http://www.sans.org/rr/papers/5/55.pdf

36. "Foundstone Information Security Metrics", April 2003. , URL:
http://www.foundstone.com/resources/whitepapers/wp_securitymetrics.pdf

37. Drew, Steven, "The Evolution of Metrics in Threat Management",
On the Radar, Volume 4, , URL:
http://www.lurhq.com/vol4.html

38. "Shavlik Technologies", Home Page, URL:
http://www.shavlik.com

39. Swindle, Orson, "The Link between Information Security and Corporate Governance",
5th May 2004, ComputerWorld, URL:
http://www.computerworld.com/securitytopics/security/story/0,10801,92915,00.html

40. Mena Report, "Network Associates launches McAfee VirusScan Enterprise 8.0i", 16th June 2004, URL:
http://www.menareport.com/story/printArticle.php3?sid=279028&lang=e

41. Jaques, Robert, "McAfee combines anti-hacking tools",
7th June 2004, VNUnet.com, URL:
http://www.vnunet.com/news/1155686

© SANS Institute 2004, Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**