Why Every Digital Businesses Needs a
Mature Patching Process – and How to Achieve One

CYBER ATTACKS – IS THE RISE A SURPRISE?

> "Adversaries take the easiest path available when determining how and where their exploits will succeed. They choose products that present more attack surface opportunities; those opportunities are generally created by the use of unpatched or outdated software." – ***Cisco 2015 Annual Security Report***

Contents

Executive Summary

Cyber attacks are on the rise, costing companies an average of $7.6m. And yet, the vast majority of these attacks could be prevented by implementing best practices in systems management and creating better managed, more secure systems.

One of the key areas to concentrate on is patching, a practice that is highly recommended by the SANS institute, among others. Unfortunately, the vast majority of companies do not have a mature patching process – if, indeed, they have one at all.

There is now renewed pressure on software vendors to patch their vulnerabilities quickly, with Google recently announcing Project Zero, which will give vendors 90 days to patch vulnerabilities before making source code demonstrating how to exploit them publicly available. The fact that vulnerabilities are being made public in this way puts organizations under increased pressure, too. Most attacks are carried out using known public vulnerabilities, which means that organizations must update their systems as soon as a patch is available or face a heightened risk of attack.

Understanding these risks is the first step to removing vulnerabilities. One common misconception in addressing such risks is the idea that simply having an automated process is enough. The fact is, a business may already have an automated system but this doesn't necessarily mean that patches are applied with sufficient regularity or that the environment is as secure as it should be. This is where endpoint automation technologies from 1E can help: not only by making it easier to understand patching levels, but also by accelerating remediation.

Introduction

Cyber-attacks cost companies a great deal of money – the 2014 Global Report on the cost of Cyber Crime[1] produced by the Ponemon institute claims that after interviewing 257 companies across 7 countries, the average cost of cyber attacks over 2014 was $7.6m. Some higher profile attacks have reported costs reaching the tens of millions. According to an article by ABC News Australia, the EU Law Enforcement Agency has estimated that victims lose more than 250 billion euros each year worldwide, with cyber crime netting more income for criminals than the global trade in marijuana, cocaine and heroin combined[2].

What's more, these attacks are becoming increasingly common. The Global state of Information Security Survey 2015[3] commissioned by PwC claims that according to the survey's respondents, the number of reported cyber attack incidents in 2014 was 48% higher than the previous year. Of course, this statistic relates to the number of attacks that were reported, and it is very likely that the vast majority of cyber attacks pass not only unreported, but quite possibly undetected too.

It's hardly a surprise that cyber attacks are on the increase when, if done correctly the crime may not even be discovered. Given the insidious nature of this threat, what are companies already doing to protect themselves, and what should they do to protect themselves further?

For many companies, what they are doing at present amounts to avoiding the issue – and this is frequently due to lack of information and a poor understanding of the nature of security threats. When most think of security, they think of high cost, complexity and specialist knowledge. According the Centre for Strategic and International Studies (CSIS) in their Raising the Bar for Cybersecurity[4] white paper, only 3% of cyber attacks would have required difficult and expensive prevention techniques. The vast majority of attacks are carried out by opportunists taking advantage of poor systems management practices and known public vulnerabilities within software.

Secure environments are well managed and have robust processes in place to ensure there is very little room for attack by any external parties that wish to do harm. Achieving this boils down to managing the environment more effectively. In so doing, the security of the environment is automatically increased without actually thinking about – or investing in – security itself.

[1] Ponemon institute, Sponsored by HP Enterprise Security, October 2014, 2014 Global Report on the cost of Cyber Crime
http://h20195.www2.hp.com/v2/getpdf.aspx/4AA5-5207ENW.pdf?ver=1.0

[2] Emily Stewart, for abc.net.au, April 23 2015, Cyber attacks on Australian businesses rose 20 pc last year
http://www.abc.net.au/news/2015-04-23/cyber-attacks-on-australian-businesses-rise-20-per-cent/6415026

[3] Pricewaterhousecoopers, September 2014, The Global state of Information Security Survey 2015,
http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

[4] Centre for Strategic & international studies, February 2013, Raising the Bar for Cybersecurity,
http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf

This viewpoint is backed up by information published by a branch of the Australian government called the Defense Signal Directorate (DSD). Following a full and thorough analysis of the breaches they had been subjected to, the DSD discovered four critical controls that, where configured properly, offer the greatest benefit in terms of preventing breaches of security with minimal effort. These critical controls are:

- Application patching
- Operating system patching
- Application whitelisting
- Removal of unneeded administrative rights

By configuring these items effectively, at least 85% of vulnerabilities can be mitigated and are backed by the SANS Institute, CSIS in the United States and the Centre for the Protection of National Infrastructure (CPNI) in the United Kingdom.

Zero Tolerance

Patience for software companies releasing software with exploits has worn thin enough for someone to take action. Google decided in mid-2014 that enough was enough and decided to set up Project Zero[5]. This team, headed up by former Google Chrome Security head Chris Evans, has the sole focus of finding zero-day exploits in software and reporting them back to the vendor concerned. After 90 days, the finding is made public (along with source code to unearth the vulnerability in question) or the information is released to the public earlier, should a fix be made available by the relevant vendor. It is likely that other vendors will follow suit with their own teams focused on the same thing in competition with Google, however the result will be good for the overall security of applications and data worldwide.

What this means is that vulnerabilities are being actively, perhaps aggressively searched for and made public with the intent of uplifting the security of our data across the board. Vendors are being put under massive pressure to fix issues that are found as quickly as possible and because vulnerabilities located are being made public there is a huge pressure on companies to install fixes or suffer the consequences of having vulnerable software with known exploits.

In this white paper, we will focus on improving patching effectiveness and the overall security of your environment. We will also touch on how 1E technologies can provide awareness of areas that require patching and help to rectify this where needed.

[5] Google online security blog, Chris Evans, July 2014, Announcing Project Zero, http://googleonlinesecurity.blogspot.co.uk/2014/07/announcing-project-zero.html

Patching makes perfect

Patching the environment and application set is a key element of cyber attack reduction. According to the paper Raising the Bar for Cybersecurity[6] , 75% of attacks use techniques that could have been prevented by regular patching. However according to an article by CSO[7] online.com , 58% of companies do not have a mature patching process and 12% of companies have no patching process at all. Patching the environment is probably the easiest aspect to solve, since in the vast majority of cases, the fix for the vulnerability is free, widely available and can be deployed and installed by your existing management infrastructure, such as Microsoft System Center Configuration Manager (SCCM).

As these statistics show, not all organizations patch effectively if at all. There are typically two reasons for this:

- Lack of awareness of the risks arising from not patching
- A belief that an existing automated solution is effective, resulting in patching being taken for granted

[6] Centre for Strategic & international studies, February 2013, Raising the Bar for Cybersecurity, http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf

[7] Maria Korolov, csoonline.com, December 2014, Report: Most companies fail at keeping track of patches, sensitive data, http://www.csoonline.com/article/2857012/disaster-recovery/report-most-companies-fail-at-keeping-track-of-patches-sensitive-data.html

Education, Education, Education

As the examples above demonstrate, educating your organization on the benefits of patching is a critical part of ensuring that your patching process is successful. There is plenty of material available to help achieve this. The 2015 Annual Security Report from Cisco[8] goes into detail about the importance of educating users and how tools that can protect from breaches such as patching are overlooked by almost 50% of respondents.

According to Cisco, "Adversaries take the easiest path available when determining how and where their exploits will succeed. They choose products that present more attack surface opportunities; those opportunities are generally created by the use of unpatched or outdated software."

Closing vulnerabilities is one aspect of security, but if a company handles personal data, there are also legal requirements to look after that data and secure it from unauthorized access. In the United Kingdom, there is the Data Protection Act, and in Europe there is the Data Protection Directive. The United States doesn't have a single law covering the same elements, but has many covering different aspects, all of which are governed by various regulatory bodies. Regardless of a given country's legislation, they all agree there is a responsibility to keep personal data secure. Interestingly, only South Africa's Protection of Personal Information Act includes an explicit mention of updating applications.

Regardless of whether or not keeping applications updated is explicitly stated, the legislations are clear on one thing: each company or organization is responsible for keeping the information it collects secure. Closing vulnerabilities via patching of operating systems and applications is a key method for effectively attending to this responsibility.

[8]Cisco, January 2015, 2015 Annual Security Report,
http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html

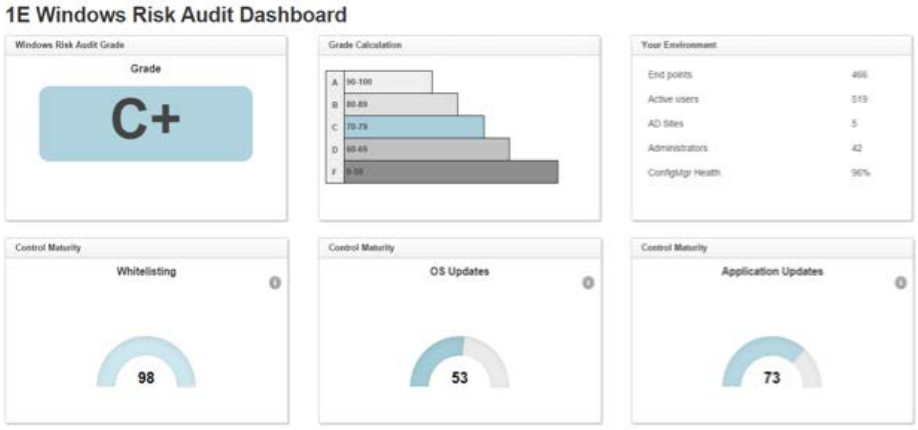
Automatic patching, problem solved?

There are many methods for automatically applying patches, however the most common method in use today is Microsoft's System Center Configuration Manager. If the business is applying patches automatically via such a system, then there my be a general belief that the systems are effectively patched. However, while patches can be downloaded directly from the Microsoft update server, there are situations that prevent patches being deployed. The three most common are:

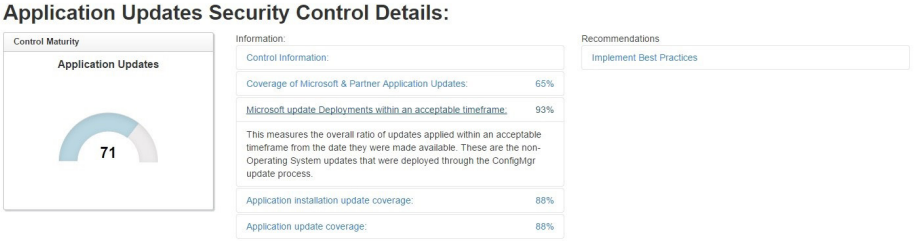
- Machines may be powered off when patch installation is attempted, preventing the update
- Machines are not rebooted after patches are applied, preventing the patch from being fully installed and therefore active
- Network bandwidth may be a problem for remote offices and therefore those machines are not patched

How to help solve the patching problem

The first step with any problem is to recognize that a problem exists and to measure its extent. However, understanding your current patching levels is not an easy task to undertake and this is where technologies from 1E can help you. The Windows Risk Audit from 1E takes all the update information that is available within Configuration Manager and compares the patches installed on your endpoints with what's available on your Microsoft update server.



Once the information is gathered, the Windows Risk Audit works out the percentage of coverage your environment has for critical and security-related updates, coverage of all updates and whether deployments of patches were performed in an acceptable timeframe.



Once you know the percentage of the environment that is patched effectively, it immediately becomes clear what needs work. Resolving this issue involves locating the machines that require patching. 1E provides a comprehensive set of reports that can be used in conjunction with the Windows Risk Audit to not only pinpoint any unpatched machines, but also identify which patches have been installed.

Having this information on hand allows questions to be asked as to why patches are not being installed on the machines in question.

AD Sites

AD Site	Machines	Weighted AVG	Critical OS Coverage	OS Coverage	NonOS Coverage	Days To Install OS	Days To Install NonOS
IN-Office	66	74.5	81.5	81.5	39.9	19	6
WindowsAzure	119	77.9	81.1	81.9	60.0	0	0
	12	79.2	81.2	88.7	54.5	7	0
CP-House	240	79.3	82.6	83.5	60.8	10	2
US-Office	42	83.8	90.3	91.1	49.9	25	5

Domains

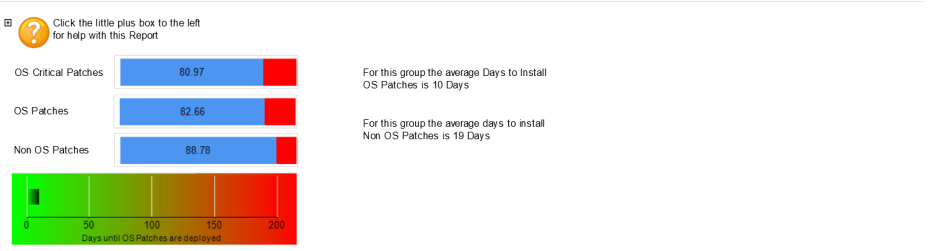
Domain	Machines	Weighted AVG	Critical OS Coverage	OS Coverage	NonOS Coverage	Days To Install OS	Days To Install NonOS
1E	478	78.4	82.7	83.6	55.3	10	3

OU

OU	Machines	Weighted AVG	Critical OS Coverage	OS Coverage	NonOS Coverage	Days To Install OS	Days To Install NonOS
1E.LOCAL/SERVERS/PRODUCTION SERVERS	9	34.6	31.9	39.3	33.3	14.8	0.0
	155	76.4	79.3	81.0	58.5	16.2	2.4
1E.LOCAL/1EWORKSPACE/ROAMINGPROFILETEST	182	78.4	81.7	82.5	60.0	0.3	0.5
1E.LOCAL/CMCOMPUTERS	133	85.0	91.6	91.2	53.1	16.2	3.1

OS

OS	Machines	Weighted AVG	Critical OS Coverage	OS Coverage	NonOS Coverage	Days To Install OS	Days To Install NonOS
Windows 2003	2	25.1	21.5	18.0	50.0	18	20
Windows XP	4	30.2	28.0	23.5	50.0	14	0
Windows 2008	6	56.7	61.0	62.0	33.3	15	0
Windows 2008 R2	57	65.0	66.4	72.2	46.0	17	2
Windows 7	27	79.9	81.9	83.1	67.3	19	4
Windows 8.1	370	81.5	86.4	86.7	56.4	8	2
Windows 8	13	83.7	87.0	86.0	69.4	16	13



Machine Name	Domain	User Name	AD Site	OU	OS	Machine Type	Critical OS Coverage	OS Coverage
1EPRDSCCMUK01	1E		CP-House	1E.LOCAL/SERVERS/PRODUCTION SERVERS	Windows 2008 R2	Desktop	33	41
1EPRDTST01	1E		CP-House	1E.LOCAL/SERVERS/PRODUCTION SERVERS	Windows 2008 R2	Generic	0	6
1EUKCOL1173	1E	Peter.Clark	CP-House		Windows 8.1	Generic	98	99
1EIE-HYPERV-1	1E				Windows 2008 R2	Generic	0	50
1EIRDEVWKS1347	1E	Neetha.Annayyagari	CP-House		Windows 8.1	Generic	84	85
1EVCOL103	1E	pmurray	CP-House	1E.LOCAL/CMCOMPUTERS	Windows 7	Laptop	90	91
1EUKCOL1215	1E	pmurray	CP-House		Windows 8.1	Generic	100	100
1EVWKSREFW81X64	WORKGROUP	Administrator			Windows 8.1	Generic	100	100
1EUKITW1054	1E	andrew.french	CP-House		Windows 8.1	Generic	98	99

Shutting off machines to save energy

As we have already discussed, one of the barriers to effective patching is the fact that machines are often switched off when patches are applied, or not rebooted after patches have been updated. 1E NightWatchman empowers the administrator to create policies to allow updates to run on machines that are switched off, effectively waking them up so that they can be patched as needed and on-demand. This can be accomplished in two ways:

The first is to use NightWatchman's integration with Microsoft's System Center Configuration Manager to apply a wake up command to the package(s) before they are sent to the machine. This means that in cases where the machine is in a low power state at the time of package deployment, the machine will be woken up, the package deployed and then the machine will be returned to the state it was in before the package was deployed. This is the best way to ensure that machines are specifically targeted to be patched as soon as a patch or update is made available. The value of this is that it minimizes the attack surface at the earliest possible convenience. This solution also ensures that all patching can take place when users least require the services of the machine – overnight – eliminating disruptions to user productivity.

Should the machine require a reboot following the installation of the patch or update, then the NightWatchman solution will ensure this has been carried out before the user needs to access their desktop again, ensuring the machine is protected. Any user data left unsaved by the user before they left their PC will be automatically saved and the user will be notified of their saved work the moment that they re-access their desktop.

The second method is to schedule a set maintenance window to wake machines up in order to conduct systems management tasks, such as patching operating systems and applications, updating antivirus and anti-malware signatures or configuration files, and performing the antivirus scans while the user is not physically present. The use of the maintenance window in this manner ensures the security of the machine is maximized while any impact on user productivity is minimized or removed entirely by performing all such tasks after hours

Limited bandwidth

Bandwidth can be a major factor in remote locations. As such, in many instances patching is sacrificed for the sake of the bandwidth. However a chain is only as strong as its weakest link, and any machines that are not patched represent a potential gateway into an organization's network.

Because SCCM uses Background Intelligent Transfer Service (BITS) as its package deployment mechanism, it doesn't cope well on lower bandwidths and in some instances requires a distribution point at every remote location in order to be effective. Deploying extra servers in order to make sure remote machines are patched may be prohibitive in most organizations, adding administrative overhead and cost.

Nomad replaces BITS as a bandwidth-friendly alternate content provider for SCCM, diligently backing off to other network traffic to ensure that business operations suffer no negative effect. It continually uses spare and available bandwidth to ensure that you get crucial updates to your branch sites as quickly as possible without any impact on the business.

Conclusion

In a world where cyber attacks are more prevalent than ever before and initiatives such as Google's Project Zero are making cyber crime accessible to even the novice hacker, patching is essential.

In the course of this paper, we have established that patching is a proven methodology to remove vulnerabilities within software – and yet most organizations don't know how well they are patched across their environment. The only way to fully appreciate this risk is to develop a complete understanding of the environment. This includes being fully appraised of patch levels across the estate with a view to taking corrective action as appropriate.

Technologies such as the Windows Risk Audit, Nomad and NightWatchman are designed by 1E to provide the business with such information so that the environment is fully understood, proactively monitoring and protecting itself.

Contact us
UK(HQ): +44 20 8326 3880
US: +1 866 592 4214
India: +91 120 402 4000
info@1e.com