Vulnerablity Management:

Common Concerns Addressed

But I am already protected.

"90% of CISOs are confident of their security policies, procedures and processes... However 60% are not patching their systems with 48% agreeing that security processes are not well understood..."

CISCO Annual Security Report, 2015.

secpod

> *“90% of CISOs are confident of their security policies, procedures and processes… However **60%** are not patching their systems with **48%** agreeing that security processes are not well understood...”*
>
> ***CISCO Annual Security Report, 2015.***

Introduction:

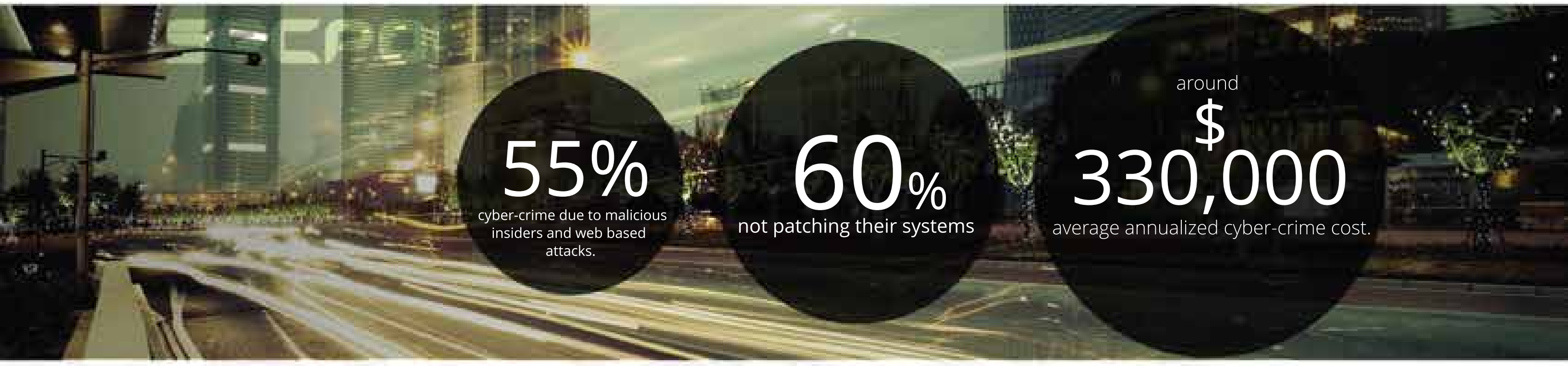
The above statements accurately summarize the contradiction between CISO’s perception of vulnerability management and the reality of its implementation. Undoubtedly vulnerability management is important. CISOs agree that there needs to be processes and resources in place to ensure the same. However, with **60%** not patching their systems, the approach to vulnerability management seems to be more of a chore that needs to be performed rather than a well thought out strategy as it should be.

In this document we take a look at the common concerns and misconceptions that CISOs have regarding vulnerability management and address the same.

➤ I have never been attacked, why should I worry now?

Thinking that you are not susceptible to an attack, because you have never been attacked or have never detected an attack before, is a flawed approach to organization security. The truth is, most organizations do not even realize they have been attacked before it is too late and the damage is already done. It is important to note that cyber- attacks makes use of vulnerabilities. So if you have a vulnerable system, you are prone to an attack.

Another disturbing trend observed is that about **55%** of all cyber-crimes are because of malicious insiders and web based attacks[1]. These two types of attacks have cost around **$330,000** in terms of average annualized cyber-crime cost[2]. The fact that a disgruntled employee, ex-employee, customer or vendor can make use of existing vulnerabilities to cause damage to your organization in terms of data theft, data loss, credibility loss and disruption of business is a compelling reason for you to have a proactive approach to security.


55%
cyber-crime due to malicious insiders and web based attacks.
60%
not patching their systems
around
$
330,000
average annualized cyber-crime cost.

I am protected by Anti-virus

Anti-virus provides a false sense of security to many organizations. They feel having an anti – virus is all that is needed to ensure device and data security. On the contrary, anti – virus does not ensure security. In fact studies have shown that the detection rate of anti – virus is less than **5%**[3] for a newly created virus. While this rate may increase over time, the inherent flaw is that anti-virus works on signature detection mechanism. By the time a virus's signature is detected and added to the anti-virus check list, it might be too late.

At its best anti-virus may help in detecting and, to some extent, stopping an ongoing attack but not in preventing an attack. In fact, **14** of the **17** major anti – viruses are known to have exploitable local and remote flaws[4] which makes them as vulnerable as the applications they are trying to protect. Also anti – virus does not offer protection from advanced hacking methods and viruses which are polymorphic in nature.

While it is not recommended to eliminate anti-virus completely, you cannot solely rely on it to provide the best line of defence either. The need is to have a reliable solution that detects and fixes vulnerabilities to prevent an attack from taking place.

Why do I need to scan regularly? I am fine with weekly/monthly scans.

This approach might have worked in the past where fewer vulnerabilities were detected. According to **NIST 7,903** vulnerabilities were discovered in 2014 alone[5]. That is a staggering 22 vulnerabilities per day or 152 vulnerabilities per week. Out of these vulnerabilities, 22% were rated as severe[6] and caused the maximum damage.

The sheer volume of vulnerabilities being detected – which runs into hundreds per week highlights the need and urgency for regular scanning. Monthly/ quarterly scans are performed more from an auditory standpoint to ensure that systems meet the set benchmark. These scans are not the right means to detect vulnerabilities. Ideally all vulnerabilities need to be fixed before an auditory scan to show compliance to the benchmark.

I am a mid-size organization, this is an additional expense for me.

You will be surprised to know that according to reports, there is an inverse correlation between the organizational size and annualized loss. Because a large number of small and mid-sized organizations do not perform regular vulnerability management they incur a significantly higher per capita cost than large organizations. Small organizations incur a loss of **$1,601** per seat. Enterprises on the other hand have infrastructure and means in place for vulnerability management and incur a loss of **$437** per seat[7].

The loss incurred by not performing vulnerability management outweighs the cost of implementing a vulnerability management solution in place.

My IT team deals with vulnerability management internally. I do not need a tool for this.

With the ever increasing number of vulnerabilities as stated above, it is hard for any IT team to stay on top of all vulnerabilities. The manual process of vulnerability management is prone to error, time delay and often leads to incorrect patch management.

It is not a financially viable option either. On an average IT professionals spend **63%** of their total time[8] on vulnerability management in the current scenario. This number will only increase going forward. Simply put- organizations cannot afford to not automate vulnerability management.

Also, organizations that take necessary steps to ensure security by investing in the required resources and tools have cyber cost crimes that are lower than companies that have not implemented these measures. These cost savings vary from **$1.1** million to **$1.3** million[9].

I use a vulnerability scanner and my IT team fixes vulnerabilities. This seems like a repetition.

Contrary to this belief, it is the combination of automated scanning and manual patching that is repetitive, time consuming and error prone. It involves integrating the results of an automated process with manual IT ticketing system. With more vulnerabilities being detected by scanners, IT teams are hard pressed to patch these vulnerabilities and in the process of trying to stay on top of every vulnerability that has been reported, some vulnerabilities evade being patched and continue to exist.

Another problem of this approach is the IT team may not be equipped to patch lesser known vulnerabilities and might implement an untested patch which can make matters worse.

Why agent based Vulnerability Management?

So far organizations have been exposed to and to a certain extent have become comfortable with network based vulnerability scanners. These scanners utilize organizations network bandwidth to ping each system and determine its security state. The drawbacks of this approach is that it consumes enormous network bandwidth and time to perform these scans. To avoid this overhead organizations usually perform a partial scan, scans during the 'off time' or even schedule scans on a weekly/monthly/ quarterly basis. This defeats the purpose of vulnerability management which is to proactively detect vulnerabilities and fix them immediately.

On the contrary agent based vulnerability management is independent of network bandwidth to perform a scan. Agents are installed on each endpoint and it scans that particular endpoint for vulnerabilities. These scans happen in parallel across all endpoints and the time taken to scan N endpoints is the same as the time taken to scan one endpoint. Thus it enables daily, automated scans while making minimal use of network bandwidth. This in turn reduces the Total Cost of Ownership (TCO)

With an agent based solution like Saner Business, you get a real time, holistic view of enterprise wide endpoint security state while offsetting the disadvantages of typical network based scanner.

I am not comfortable installing agents on my systems. It seems intrusive.

Although the concern is understandable, an agent based architecture facilitates accurate information collection for evaluating and remediating vulnerabilities. This can be achieved only if the agents reside on the endpoints. To offset any concerns regarding data collection, with Saner Business IT admin have access to a centralized monitoring console that allows the viewing of data collected from each endpoint.

Conclusion:

Keeping organization's security and business continuity in mind, it is necessary to have a vulnerability management solution in place that is proactive and offers real-time protection. While there are many products in the market that offers some of the features, it is essential for organizations to choose a single, reliable solution that offers integrated vulnerability detection and remediation along with real-time visibility. Focusing on these features will assure comprehensive vulnerability management while offering financial benefits.

Reference:

[1] 2014 Global Report on the Cost of Cyber Crime

[2] 2014 Global Report on the Cost of Cyber Crime

[3] Hacker Intelligence Initiative, Monthly Trend Report #14

[4] SC Magazine: Security researcher finds exploitable flaws in 14 antivirus engines

[5] NVD 2014 Vulnerability database

[6] NVD 2014 vulnerability severity rating

[7] 2014 Global Report on the Cost of Cyber Crime

[8] CISCO Annual Security Report 2015

[9] 2014 Global Report on the Cost of Cyber Crime

About us:

Founded in 2008 and headquartered in Bangalore with operations in USA, SecPod Technologies creates cutting edge products to ensure endpoint security. We strongly believe in the principle '**Strong Defense, Not a Weak Cure'**, and our product Saner Business reflects this ideology by proactively detecting and eliminating vulnerabilities before they can be exploited. We have been entrusted by Enterprise and mid level organizations in various verticals including Government, Healthcare and IT/ITES .

Contact us:

Web: www.secpod.com

Email: info@secpod.com

Tel: +91-80-4121 4020

+1-918-625-3023