Vulnerability Management – an approach to a cost-benefit analysis

Introduction

Businesses and Governments around the globe have to deal with the ever increasing amount of software flaws, configuration weaknesses, and similar issues piling up behind their next-generation firewalls while using Information Technology to improve their efficiency. Adding to that, compliance regulations have to be fulfilled to gain or maintain a required status.

When considering implementing Vulnerability Management, an IT security professional will be asked the same question again. Business owners and other stake holders want an answer to: "what is good for, what's the value it will bring in?"

Addressing the costs and benefits of an IT security solution in a white paper has its challenges and the pros and cons of such an attempt have been widely discussed by well-respected experts[1][2] in the past.

Our approach is to use the various steps in the Vulnerability Management process cycle as depicted below and to associate cost (time and effort) and benefits (security posture improvements) to them.

Our scenario uses an average enterprise infrastructure with 500 assets or IP-enabled devices. Assuming 65% of those are Microsoft Windows systems (desktops and laptops, a few servers), 15% are Linux devices (servers for web, email, file share, ..), and 20% are other IP-based devices (printers, VOIP phones, ..) with other aspects of an infrastructure omitted in the considerations below.

1Bruce Schneier on ROI: https://www.schneier.com/blog/archives/2008/09/security_roi_1.html

2Dr. Lawrence Gordon and Dr. Martin Loeb: Managing Cyber Security Resources: A Cost-Benefit Analysis.

Cost and Benefit

Prepare

Preparation is about defining secure configurations, white-listing systems and applications, and mapping out related security controls. That can be in conjunction with compliance regulations in place.

The effort needed for this step is similar in either way, using or not using Vulnerability Management.

Identify

Identifying assets and vulnerabilities is – when done manually per asset – taking a substantial amount of time. Other tools might be in place to help with this, which could then require individual verification for some systems.

Effort w/o Vulnerability Management	**Effort when using Vulnerability Management**	**Benefits**
5 minutes as an average for each asset, mounting to 2500 minutes for all 500 assets. Requires access to a Vulnerability Database.	SCAP[3]-based scan of assets in the network, done in 240 minutes on average including setup (but depending on network responses).	Comparing various scans allows to identify changes over time, provide for trends, and to support forensics with historic data about the infrastructure.
5+ working days (41 hours)	**4 hours**	

Classify

Classification means to sort the information discovered and add asset criticality details to it. Security information from CERTs and other sources can be added automatically.

Adding asset critically to the data requires similar amount of effort in both ways.

Effort w/o Vulnerability Management	**Effort when using Vulnerability Management**	**Benefits**
Using a spreadsheet program to enter and sort the discovered data from the various sources, correlate the data: 300 minutes	As the data is already available in structured format, sorting is straight forward: 20 minutes	Having it in structured format enables automated updating of the data, in a cyclical process.
5 hours	**20 minutes**	

3SCAP: Secure Content Automation Protocol family. CVE, CPE, and CVSS are part of it.

Prioritize

Prioritizing identified vulnerabilities and other weakness (like aged/weak passwords or unauthorized applications) is a usual process when dealing with security issues. To decide about which one to tackle first can be challenging when handling a massive amount of data sets. With asset criticality being part of data, another selection criterion is available.

Effort w/o Vulnerability Management	**Effort when using Vulnerability Management**	**Benefits**
After sorting the data, various views are generated to allow judgement about the vulnerabilities which need to be tackled first: 30 minutes	Using (pre-)defined selections, priority is given to the most critical vulnerabilities: 10 minutes	Priorities are re-evaluated, due to changes in the criticality of assets or the severity of vulnerabilities. Vulnerability Management makes it easy to re-assess.
30 minutes	**10 minutes**	

Assign

Assigning the task to the right person within the organization needs attention, as it is necessary to match the experience of the security team members with the required knowledge for a specific vulnerability. The number of discovered vulnerabilities has an impact to the time and effort needed.

Effort w/o Vulnerability Management	**Effort when using Vulnerability Management**	**Benefits**
Manually grouping the discovered vulnerabilities and assign them to the correct person in a workflow or ticket system: 180 minutes	Interfacing both the Vulnerability Management and the ticket systems (including initial setup): 30 minutes	Automation greatly reduces human error in the process.
3 hours	**30 minutes**	

Mitigate & remediate

Mitigating or remediating the discovered weaknesses takes the same effort for both described ways. Being able to annotate vulnerability information or to add overrides is an advantage of Vulnerability Management solutions. Necessary mitigation and remediation information is part of the details being provided by a Vulnerability Management solution, easing patching a system or implementing a work around.

Store & repeat

Repeating the process is necessary as every week about 120 new software vulnerabilities are published, and about 40 of these are categorized as high or critical. That means going through the cycle depicted in this document again. Storing scan data to make them available for comparison, like mentioned above, allows for trending and prognosis of impact for newly discovered vulnerabilities.

Effort w/o Vulnerability Management	**Effort when using Vulnerability Management**	**Benefits**
Repeating the complete cycle will surely be more efficient but still labor-intense: 1500 minutes	Scheduled tasks are started automatically, generating detailed reports based on daily updated security feeds, required is system management: 120 minutes	Vulnerability Management is about repeating a cyclical process. Comparing cycles discovers changes, which would have otherwise gone unnoticed.
3 working days	**2 hours**	

Improve

Achieving improvements to the security posture is the real intent behind Vulnerability Management. This can be supported by providing KPIs. Manually calculating KPIs might be impossible due to the lack of tracking capabilities.

Summary

A first cycle of manually handling vulnerabilities in the depicted setup sums up to 2,840 minutes of effort with every repeat being estimated at 1,400 minutes compared to 280 minutes for the initial cycle with Vulnerability Management in place plus 120 minutes for each additional one.

The number of process cycles an enterprise or government entity does is the final piece to a cost-benefit analysis. Assuming a monthly routine, the total figures for the 500 assets are:

Minutes needed	**Manual handling**	**Vulnerability Management**
Initial run	50 hours (3,010 min)	5 hours (300 min)
11 cycles	275 hours (16,500 min)	22 hours (1,320 min)
Total	**40 working days (325 hours)**	**3 working days (27 hours)**

So the manual approach requires an effort of 40 working days where the Vulnerability Management just needs 3 working days. Doing things right means that an organization can free resources of almost 2 months working time to other topics while decreasing the organization's attack surface by 99.9%.

Whether or not Vulnerability Management (manual or automated) is considered in first place as a viable way of reducing an organisation's attack surface (doing the right things) and is a topic discussed in another white paper of Greenbone Networks.

Final notes

The effort estimates for the manual process are rather optimistic while those for using Vulnerability Management aren't. We refrained from assigning a cost figure to the effort given in minutes as that is misleading by itself.

The assumptions for efforts per each step and the number of assets to look after can be different in a specific setup and infrastructure as well as the number of cycles.