10 Vulnerability Management Myths

By Mark Stamford, OccamSec

Vulnerability Management (VM) continues to be a key part of many security programs; however, for those still considering doing it, or those bogged down with it, here are ten issues you may have come across and their surprising (?) answers.

The key with any VM program is to prepare your organization for three types of issues (to quote Donald Rumsfeld):

- Known knowns, threats and vulnerabilities we know about,

- Known unknowns, emerging threats in areas that we are aware of, but don`t know the specifics,

- Unknown unknowns, threat and vulnerabilities we have no idea about.

Approaching VM correctly will help your organization deal with these issues. It may not completely address the latest “unknown unknowns” but it will put you in a better position to respond to, and lessen the likely impact of, “unknown unknowns”.

1) Vulnerability management is easy

Well, no, unfortunately its not. Even if you’re a small organization there are still several pitfalls that can trip you up. Patches that address vulnerabilities sometimes have a nasty habit of preventing existing applications from running. Failure to properly test patches can result in downtime and lost productivity.

Remember, VM is not just about patch management and many different areas of security and technology management need to be combined if you are going to make it work.

2) Vulnerability management is just patch management

While a large chunk of a vulnerability management program is dealing with security patches, and the patching aspect is the piece that everyone tends to think of when discussing vulnerability management, VM is more than just applying a patch. It is important to think of a vulnerability as any weakness within your infrastructure that an attacker could exploit to their advantage. So when you think of a VM program you really need to be considering the following as well:

- Penetration testing: These tests find vulnerabilities, and demonstrate the impact of those findings, so you need to manage them. In many cases the issues found may not be “patchable” items but may be configuration or architecture issues.

- Vulnerability scanning: This is not the same as penetration testing, scans find the low hanging fruit that most attackers or worms could find, while penetration tests find the deeper issues that can lead to serious problems later.

- Network or Host configuration: Issues with network or host configurations can have a devastating effect on your network or system security and have nothing to do with patching.

- Access control issues: Poorly implemented access controls can lead to systems compromise without the need for any exploit (e.g. allowing blank passwords is never good). There are no “patches” for poor access controls.

3) Its purely a security function

If this were a true statement then far fewer organizations would have issues with VM. The reality is that to be successful a VM program is likely to have to include participants from across an organization. Risk management will need involvement since they are often involved in risk treatment, policy decisions, and can provide insight into the business impact of addressing or accepting certain risks associated with your VM program. Within IT groups like Development, Engineering, Deployment, and Operations (basically anyone who is designing, deploying, or supporting systems or applications you are finding issues with) should be given the opportunity to provide input on the process. Equally important is making sure that they assign resources to properly test and deploy fixes to vulnerabilities that are identified.

If your company has an internal audit group they should be involved, although this will typically only be in an oversight role. While internal audit may sometimes be viewed as having an adversarial relationship with IT, with the right dialogue, they can help with providing backing and support to getting vulnerabilities fixed and can sometimes cut through inter or intra-departmental politics that may be bogging the process down.

Finally, and often equally as important, the system owners are going to need some involvement in the VM process. In many organizations systems are owned by a business unit or division. Their view is that it’s their application, their system, so any fixes to be applied need to be approved by them.

4) if it’s not purely a security function then it’s purely a technical function right?

See no.3

5) *I have deployed security tools XXXX so I have no need for a robust VM program*

The principle of defense in depth continues to apply. While many good security tools do exist, there is no silver bullet that removes the need for mature security processes. What happens if that tool can be bypassed and you haven't properly managed the vulnerabilities on your systems? A good example is relying on anti-virus or Host Intrusion Prevention solutions. Both continue to improve; however, they also continue to be defeated by attackers and still do not detect all malware or host based attacks. Placing all our faith in a single technology or process will leave you unprepared to deal with the situation when those technologies or processes fail. Adding additional layers to your security posture allows you stand a much better chance of surviving the next outbreak relatively unscathed. If a worm or attacker was to gain access to your network, a robust VM program will cut down the access and impact to your systems.

6) *VM is really just something I need for compliance*

Many regulations require patches to be deployed in some kind of organized, managed, and measurable fashion. These regulations also typically have requirements around strong access control and periodic vulnerability assessments and penetration testing. However, it is always important to remember that compliance should really be seen as the minimum level of security required to protect your organization.

While meeting compliance requirements will give your organization a basic level of security, additional actions are typically required to lower the risk faced from many common attacks. In many ways it's similar to the safety features in a car. Seat belts are required by law, airbags, roll bars, and advanced safety systems are not; however, people will often purchase a car with these additional features in order to decrease the likelihood that they will suffer serious injury in a crash. Do you really want your most sensitive corporate systems and information protected by only a seat belt?

7) *We don't use Windows so I don`t need to patch anything*

Security patches are released for all major operating systems. The complexity of modern software makes it inevitable that bugs will exist and that some of these bugs will lead to security exposures. Windows is not alone in requiring security patches (see http://web.nvd.nist.gov/view/vuln/search to search for published vulnerabilities). As the growth of other platforms continues it's also likely that attackers will start to focus on them which likely means more vulnerabilities and exploits for those platforms.

Deploying a non-windows operating system in and of itself should not be seen as a security measure that negates the need for patching.

8) We can fix every security issue ASAP

A nice idea, but in reality once your environment becomes more then a handful of systems this may not be the case.

There are several reasons why this may not be possible (and why you probably don`t even need to).

i) You have many mobile users: Most patching systems try to deploy a patch when a system connects to the network, if a system is rarely plugged in then its not going to receive all the updates it needs in a timely manner.

ii) You have a small team to do the work: Dealing with vulnerabilities takes time, if a small team is assigned the task of remediating issues then they may well need some time to take care of everything, regardless of what technical solutions you have in place.

iii) Some systems are more at risk than others: Systems that are either exposed to the Internet, directly connected to those systems, or used by large numbers of users are more likely to be vulnerable to attack then isolated systems. You should therefore make it a priority to address these issues first. How can you figure out what systems are most at risk? The simplest way in a small environment is to look at everything in the DMZ and what they connect to. In larger environments a number of approaches can be taken including perceived asset criticality and the use of tools, which allow network configurations and vulnerabilities to be mapped so that high risk systems are identified.

9) For security patches and scan results, I can just go with the vendor ratings

Vendors usually rate the patches they release or the findings from their scans so you have some guidance as to the risk associated with the vulnerability. Unfortunately you cannot use these ratings or a “one size fits all” risk assessment approach. Consider the following scenarios:

i) A patch is released for operating system XYZ which is rated as ‘critical’. Organization ‘Company1’ has 4 servers running XYZ, all of these are located in a trusted network zone with restricted access controls. Company1’s security policy states that a patch rated critical must be deployed within 2 weeks.

ii) ‘Company2’ performs regular internal and external vulnerability scans of its environment. During the last round of scans the external scan picked up 2 critical rated vulnerabilities in an external facing web server, and the internal scan picked up some critical vulnerabilities on some internal systems.

In both of these cases it can be argued that a generic rating of ‘critical’ is not the most efficient way to handle these issues. Instead vulnerabilities may need to be rated entirely differently for your organization, or broken down into different ratings for different groups of systems (this is where a VM process would come in). The larger an organization is, the more applicable this issue becomes.

10) This is going to be expensive

It doesn`t have to be. Security patches are released freely, alert information is available to anyone, and there are a wide range of open source tools that can help your organization deal with many areas of vulnerability management. Scanning solutions are available, as are systems that provide issue-tracking capabilities.

They key to any successful program is going to be having the support of all stake holders. If vulnerability management is just seen as a purely technical function with no support from business users then in all likelihood it will fail. You’ll end up with system disruptions or nothing will ever get done. Drumming up this support within your organization really just takes time, but starting with the approach that it’s a business wide program and not just a technical project creates the foundation for success. Tools can be purchased but successful VM cannot. Successful VM requires buy in from stakeholders, not just buy-ing of technology.