a seasoned cyber-security professional with 17 years' experience of delivering highly advanced technical security solutions into enterprises and government. Having published a series of cyber-security management guides geared towards educating the C suite in cyber-risk, his recent focus is researching the evolving risks in cyber and industrial control systems. The research is aimed at raising awareness at a senior level to ensure that the constant cyber- and ICS risk is approached in an informed and pragmatic way.

References

1. 'December 2015 Ukraine power grid cyber-attack'. Wikipedia. Accessed Feb 2017. https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyber_attack.
2. 'Steinitz: Israel's Electric Authority hit by 'severe' cyber-attack'. Times of Israel, 26 Jan 2016. Accessed Feb 2017. http://timesofisrael.com/steinitz-israels-electric-authority-hit-by-severe-cyber-attack/.

Software vulnerability management: how intelligence helps reduce the risk

Vincent Smyth

Vincent Smyth, Flexera Software

Recently, a widely publicised news report revealed that tens of thousands of computers could have been exposed to hacker threats due to malicious online advertisements that ran on major media companies' websites, including the BBC.[1] These incidents are becoming increasingly commonplace and serve as a chilling reminder of how exposed we all are to the threats caused by software vulnerabilities that are exploited by malicious hackers.

Every year, thousands of software vulnerabilities are discovered in thousands of products. Exploitation of vulnerabilities can cause extensive damage. Chief security officers probably don't need to be reminded of the high stakes surrounding software vulnerability management. The numbers speak for themselves. For instance, in 2015 there were 16,081 vulnerabilities discovered in 2,484 vulnerable products.

The cost is enormous for organisations that must deal with a successful vulnerability exploit by a hacker. According to PwC, the average financial loss attributed to cyber-security incidents was $2.5m in 2015.[2] And that cost does not take into account the brand and reputational damage caused by a successful hack.

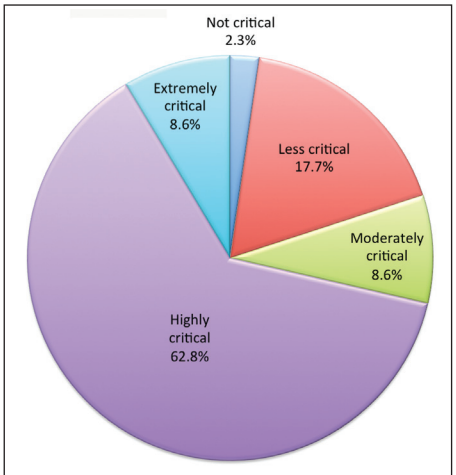
The good news is that 84% of all registered vulnerabilities had patches available on the day of disclosure.[3] Consequently, organisations can have the greatest impact on reducing their risk profile by proactively patching known vulnerabilities before they are exploited and, in the process, minimising the attack surface. But what is the fastest and most cost effective way of doing so? It starts with vulnerability intelligence.

Relevant threats

With an overwhelming number of software vulnerabilities reported every day, security departments can easily become overwhelmed with even the most basic aspects of addressing the problem, such as answering the question, 'Which vulnerabilities apply to us?'.

Companies need to filter out the known vulnerabilities and concentrate only on those impacting the organisation. That entails comprehensive asset discovery and inventory to determine which systems are potentially threatened by the known vulnerabilities. Once the universe of known vulnerabilities is winnowed down to only the subset impacting the enterprise, then teams can focus their attention.

Getting an accurate picture of IT assets in inventory is easier said than done. Most companies cannot accomplish this without implementing software asset management (SAM) processes



Criticality of software vulnerability advisories. Source: Flexera Software.

and technology. Fortunately, SAM has emerged in recent years as a bulwark against wasteful software spend – and many leading organisations around the world either have already implemented SAM or are in the process of doing so. Among other things, SAM solutions enable organisations to automate the process of discovering and inventorying their software (and hardware) assets – wherever they reside.

The challenge, then, is for the security and IT operations teams within organisations to recognise their mutual need for asset discovery and inventory and work together (and not in silos) to collect this data. If an organisation already has a SAM implementation in-house, security teams should be aware of this and utilise the discovery and inventory data as the common 'version of the truth' for determining which vulnerabilities apply to them. Moving forward, as SAM and security continue to converge, SAM tools are increasingly integrating capabilities with software vulnerability management tools – which, ultimately will help siloed security and IT operations teams work better together.

Refining security efforts

Picture this: a company's IT environment holds thousands of different applications and systems, all interconnected. Every year, as thousands of vulnerabilities are discovered in thousands of products – some are extremely critical and their exploitation can cause extensive damage – these need to be dealt with straight away. Others are not very critical and can be dealt with in due course. Security teams need to match their own environment with the vulnerabilities that are discovered, assess the risk the vulnerabilities pose and then prioritise mitigation of the vulnerabilities.

This in itself is a daunting task. Add to it that every day, some 300 new vulnerability alerts are reported globally. But in fact, on average, only about 8% of these 'reported' vulnerabilities turn out to be real. To know which threats to take seriously, it is necessary to thoroughly investigate them. This is highly skilled work that must be performed by experts in their field.

If curating vulnerability information is not a main line of business, companies most likely will not have the resources or the motivation to employ a full team of people whose only purpose is to monitor and curate vulnerability information. Instead, organisations must find a trusted software vulnerability management resource whose function is to perform this work, providing vulnerability *intelligence* – not just information.

"With limited time and resources available to patch the hundreds – or even thousands – of vulnerabilities that may impact an organisation, how are security teams to know which are the most important?"

Vulnerability intelligence means that reported vulnerabilities are actually verified, with additional intelligence, delivered in a format that security teams can use and act upon, which explains how to handle the issue. Moreover, it means that the intelligence has been tested, vetted and is relevant – so that the information delivered pertains only to vulnerabilities in products relevant to the specific environment. For instance, beyond verification of a vulnerability's existence, vulnerability intelligence should detail what IT security teams need to know to mitigate the risk to the organisation by the vulnerability.

Good vulnerability intelligence will not only verify the existence of a vulnerability, but will also rate the vulnerability's criticality. This is important because, as noted, not all vulnerabilities are created equally. And with limited time and resources available to patch the hundreds – or even thousands – of vulnerabilities that may impact an organisation, how are security teams to know which are the most important?

As this sounds very theoretical, it may be helpful to provide an example. The Secunia Research team provides vulnerability advisories in this manner. Beyond verifying and detailing the vulnerability, these advisories assign to it a criticality rating of 1 to 5 – with 1 representing the least critical and 5 representing the most critical.

The criticality of a vulnerability is based on the assessment of the vulnerability's potential impact on a system, the attack vector, mitigating factors and whether an exploit exists for the vulnerability and is being actively exploited prior to the release of a patch. The vulnerability ratings are as follows:

- **Extremely critical (5):** typically used for remotely exploitable vulnerabilities that can lead to system compromise. Successful exploitation does not normally require any interaction and exploits are in the wild. These vulnerabilities can exist in services like FTP, HTTP and SMTP or in certain client systems such as email applications or browsers.
- **Highly critical (4):** typically used for remotely exploitable vulnerabilities that can lead to system compromise. Successful exploitation does not normally require any interaction but there are no known exploits available at the time of disclosure. Such vulnerabilities can exist in services like FTP, HTTP and SMTP or in client systems like email applications or browsers.
- **Moderately critical (3):** this rating is also used for vulnerabilities allowing system compromise on LANs in services such as SMB, RPC, NFS, LPD and similar services that are not intended for use over the Internet. Typically used for remotely exploitable denial of service vulnerabilities against services such as FTP, HTTP and SMTP and for vulnerabilities that allow system compromises but require user interaction.
- **Less critical (2):** typically used for cross-site scripting vulnerabilities and privilege escalation vulnerabilities. This rating is also used for vulnerabilities allowing exposure of sensitive data to local users.
- **Not critical (1):** typically used for very limited privilege escalation vulnerabilities and locally exploitable Denial of Service vulnerabilities. This

rating is also used for non-sensitive system information disclosure vulnerabilities (eg, remote disclosure of installation path of applications).

Armed with reliable intelligence covering reported and verified vulnerabilities, which of those verified vulnerabilities apply to an organisation's own hardware, software and systems and – of those that apply – which are more critical and which less, security teams can then begin to establish an effective remediation plan.

The proactive nature of software vulnerability management presupposes that it is less costly to avoid successful attacks than to fix the problem after an attack has occurred. Therefore, organisations need to understand what IT assets exist within their environments that could be the target of attack. They need to have a complete picture of the vulnerability landscape – and, more importantly, a picture of which vulnerabilities apply to them. Then finally, organisations need an accurate and reliable assessment of the criticality of those vulnerabilities, so they can prioritise remediation. A thorough programme founded upon vulnerability intelligence will help minimise the attack surface, reducing the risk that a successful exploit can occur.

About the author

Vincent Smyth is senior vice-president EMEA at Flexera Software, responsible for driving revenue, market share and customer satisfaction in the independent software vendor, high-tech manufacturer and enterprise account domains. Prior to Flexera Software, he held several sales management responsibilities for Business Objects, PTC and Computer Associates. He has extensive experience of doing business across Europe and the Middle East.

References

1. Kirk, Jeremy. 'Large advertising-based cyber-attack hit BBC, New York Times, MSN'. Infoworld, 16 Mar 2016. Accessed Feb 2017. www.infoworld.com/article/3044880/security/large-advertising-based-cyber-attack-hit-bbc-new-york-times-msn.html.
2. 'The Global State of Information Security Survey 2017'. PwC. Accessed Feb 2017. www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.
3. 'Vulnerability Review 2016'. Flexera Software, 16 Mar 2016. Accessed Feb 2017. www.flexerasoftware.com/enterprise/resources/research/vulnerability-review/.

Why communication is vital during a cyber-attack

Nick Hawkins

Nick Hawkins, Everbridge

Cyber-attacks are a constant threat to organisations. However, cloud-based communications platforms can help an organisation improve emergency communications and more effectively recover from the effects of a attack.

In today's globalised business environment, organisations of all sizes face the prospect of falling victim to a cyber-attack or IT outage that could cause serious damage to their infrastructure and ability to operate. The need to combat cybercrime is rising up the UK Government's agenda with the opening of the National Cyber Security Centre (NCSC). According to its 2016-2021 report, the NCSC's role will be to manage national cyber-incidents, provide an authoritative voice and centre of expertise on cyber-security and deliver tailored support and advice to government departments, the devolved administrations, regulators and businesses.

Despite the improvement of cyber-security techniques, criminals have developed sophisticated ways to disrupt systems and steal data. The need to prepare for cyber-attacks is more important than ever.

True cost of cyber-attacks

According to Cisco's '2017 Annual Cyber Security Report', more than one-third of the organisations that experienced a cyber breach in 2016 reported a loss of customers, business opportunities and revenue.[1] The '2017 SonicWall Annual Threat Report' reported an increase from 3.8 million ransomware attacks in 2015 to 638 million in 2016.[2] In March 2016 alone, ransomware attack attempts rose from 282,000 to 30 million.

Cyber-attacks cost UK businesses a total of £34.1bn between summer 2015 and 2016, with each attack costing an average of £4.1m and taking 31 days to resolve.[3] While large corporations, which invest millions of pounds in cyber-security, have the potential to recover easily from such a crisis, for most Small/Medium Enterprises (SMEs) and Non-Governmental Organisations (NGOs) cyberbreaches can have more far-reaching and detrimental consequences.

No business is safe

Investing large sums of money into cyber-security is not a guarantee of success, as shown by a number of recent high-profile cyber-attacks against large corporations all over the world – including the BBC, Sony's PlayStation Network, HSBC and eBay.