The Days of Feeling Vulnerable Are Over: Best Practices in Vulnerability Management

An EiQ Networks White Paper
The Need for Vulnerability Management

Vulnerabilities are potential holes introduced by flaws in software code or system configurations that may enable hackers to compromise your network or systems. Errors introduced during programming often result in inadvertent vulnerabilities that enable hackers a means of ingress to your systems. Other vulnerabilities may not be a result of software bugs at all, but rather incorrect configurations, such as failure to close appropriate ports on a firewall. Hackers constantly look for the open doors and windows left by vulnerabilities in software and system configurations and seek to exploit these openings to gain access and bypass your security controls.

Vulnerabilities come in many forms. For example, items such as open ports and protocols may leave unintended access to key areas of a system. Memory management issues may create other avenues for attackers to exploit and gain control over your systems. Because so many devices are connected together in modern businesses, once control of one system is gained, it is often easier for an attacker to gain control of additional systems within your network.

Once a vulnerability is identified by the community, software vendors often release patches that address the vulnerability and correct the code that caused the vulnerability. However, patches themselves may contain errors, and may have unintended impacts on other areas of your systems, particularly if you have extensive customization. Therefore, thorough review and testing of patches before deploying to production systems is often recommended.

To pinpoint which systems are subject to known vulnerabilities, regular monitoring of systems is required. Rather than simply trying to keep track of the latest patches that apply to each system, it is often easier to run automated assessments against known vulnerabilities to identify if these the vulnerabilities are present on a particular system in your network.

Vulnerability scans provide automation to help identify which systems are subject to which vulnerabilities. By checking ports and protocols as well as installed software and OS versions, a scan of your network can yield a list of systems and the vulnerabilities each system suffers. These can then be prioritized based on risk levels, with plans for remediation put into action.

Vulnerability management encompasses not just one-time scans, but also the process of managing these scans and the related remediation of the identified vulnerabilities in a systematic approach. Managing vulnerabilities can be a time-consuming and complex task, particular for mid-market organizations that don’t always have the time and necessary staff to investigate. Software flaws or misconfigurations could allow cyber-attackers to gain access to your IT systems. These vulnerabilities need to be quickly detected and remediated before they can be exploited.
Organizations often find challenges when attempting to implement vulnerability management on their own, without the support of a services organization, including:

- Scanning technology that requires too much time and effort to deploy and manage
- IT personnel who do not have the bandwidth to regularly scan and analyze the results
- The time and effort it takes to prioritize and follow up on vulnerability remediation

If you are responsible for your company’s information security program, you no doubt find that managing security flaws on your network devices, operating systems, and applications is both time-consuming and complicated. It’s hard to keep up with the ever-expanding amount of flaws that are exploited by attackers; for example: SYN Flood (DDoS), as well as Heartbleed (Open SSL), Shellshock (UNIX), and Poodle (SSL 3.0).

Every day, it seems like there is another update to install. Prioritizing necessary patches and performing the related testing prior to deployment can be a daunting task, particularly for smaller organizations. That’s not surprising, given the more than 7,000 vulnerabilities added to the National Vulnerability Database in 2014 alone.

How Vulnerability Management Fits into a Security and Compliance Program

The top five critical security controls, according to SANS/CIS, include 1) inventory of authorized and unauthorized devices, 2) inventory of authorized and unauthorized software, 3) secure configurations for software and hardware, 4) checking to see if vendors have left any flaws in the hardware or software that attackers can exploit (continuous vulnerability assessment and remediation). And after you have done all that, 5) you want to actively monitor your security to defend against malware and exploits. Vulnerability management is specifically focused on step four.

Many compliance regulations require similar measures, including PCI DSS Requirement 6.1, where the organization must establish a process to identify security vulnerabilities using reputable outside sources for security vulnerability information and then assign a risk ranking to newly discovered vulnerabilities, and PCI DSS Requirement 11.2, where the organization must run internal and external network vulnerability scans at least quarterly and also after any significant change in the network. This external scan must be done by an approved scanning vendor and no vulnerabilities ranked CVSS 4.0 or higher can be left unresolved.

How Vulnerability Management Works

Let’s take a closer look at the steps involved in a typical Vulnerability Management process:

1) Discovery
2) Prioritization of Assets
3) Assessment
4) Reporting
5) Remediation
6) Verification that remediation actually worked
The first step to discover and prioritize assets when looking for vulnerabilities is to inventory and map all of your assets on the network and build a network map to see what’s connected to what; after all, you cannot secure what you cannot see. Understanding all these different connections will help you understand how valuable something is. You might think a certain server is no big deal until you find it’s connected to something that if someone got access to it, it would be a big problem.

Next, you assign a business value of each asset, for example, high, medium, and low, based on whether it’s external or internal-facing, and what data it holds, to will help you understand what the damage would be if it were breached.

It’s important to realize that vulnerability and risk are not the same thing. Risk is the probability of the vulnerability being exploited multiplied by the cost of damage it will cause. This is required for risk evaluation and will help you prioritize your remediation efforts as well as define compliance boundaries.

Once assets are inventoried and assigned values, vulnerability assessment is then performed via vulnerability scanning, which is dedicated technology that scans the IP addresses both inside the network as well as outside the network blocked by a firewall, so you are able to identify potential vulnerabilities accessible both inside and outside your internal network. Scans can take hours to a day and should be scheduled for a time that won’t disrupt the network, usually on a monthly or bi-monthly basis.

Once you do the assessment, you will receive a report with a description of the vulnerability, a CVE #, which stands for Common Vulnerabilities and Exposures (a database run by Mitre that collects common vulnerabilities from around the world) and a CVSS score, which stands for Common Vulnerability Scoring System, between 1-10 based on severity, 10 being the most severe. The report also typically details the threat, its impact, solution, and reference link.

Before performing remediation, you will need to prioritize which vulnerabilities are most significant and should be handled first based on the risk to your organization. Remediation itself typically involves finding, testing, and installing a patch or changing configuration settings. If no patch is available, you will need to find alternate ways to mitigate the risk, for example by disabling the system. Either way, a ticketing system should be used to track and document the remediation. This can be difficult for smaller teams who are constantly challenged to put out fires and prove to auditors that systems are compliant.
The final step is to verify the fix and scan the asset again after remediation to ensure the fix is applied. Be sure to document all steps.

Performing all of these steps can be time-consuming. Typically, organizations will scan the network once or twice a month and teams will spend between 20 minutes and 3 hours a day reviewing the reports. You will need to understand how severe your organization’s vulnerabilities are and which systems are affected. You then must cross-reference the exploit database, document the security and business case for a patch, convince your systems administrator to install patches, and then verify the fix.

Approaches to Vulnerability Management

Many of EiQ’s customers have tried to deploy Vulnerability Management software on their own, but found that the total cost of ownership (software license, staffing, consulting and maintenance fees, for example) dwarfs the value received. Vulnerability assessment technology is widely available and can be used to scan for vulnerabilities, but without investing in the right people and processes, the data does not provide much value. A typical vulnerability report consists of page-after-page of detail, but that is just the beginning of the vulnerability management process. A trained analyst needs to research and prioritize the vulnerabilities based on factors including:

- The business value of the IT asset
- The criticality of the IT asset within the network security design
- The availability of exploits targeting the vulnerability
- The exposure time of the system

To make matters worse, the process is an infinitely repeating loop that constantly re-evaluates the security posture of the organization.

Introducing EiQ Networks’ SOCVue® Vulnerability Management Service

The SOCVue Vulnerability Management service from EiQ provides vulnerability assessment, analysis, and remediation guidance to mid-market organizations (those with fewer than 5,000 employees) at a fraction of the cost of alternate solutions. It is a subscription service that combines people, process, and technology to deliver an effective vulnerability management program. This means that customers gain the use of cutting-edge vulnerability assessment technology, along with an extended security team, to effectively analyze vulnerabilities and track the remediation process. The service can save an IT team hundreds of hours every year, while providing the vulnerability management necessary to meet compliance mandates and reduce information security risk.

EiQ partners with the leading vulnerability scanning technologies (such as Qualys) to ensure that scans are comprehensive and that the vulnerability database is up-to-date with the latest zero-day threats. The results can be integrated with the SOCVue Security Monitoring service so that vulnerabilities are correlated with other security event data.
Benefits of Using SOCVue Vulnerability Management Service:

<table>
<thead>
<tr>
<th>Improve Your Security</th>
<th>Improve Your Compliance</th>
<th>Save You Time</th>
<th>Save You Money</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Provide visibility into security posture</td>
<td>• Deliver PCI ASV scans</td>
<td>• Manage deployment and scans</td>
<td>• No upfront software cost</td>
</tr>
<tr>
<td>• Remove easily exploited vulnerabilities</td>
<td>• Scan frequency set to meet requirements</td>
<td>• Analyze and prioritize</td>
<td>• Better value than one-time assessments</td>
</tr>
<tr>
<td>• Implement structured remediation process</td>
<td>• Measurable results to track progress</td>
<td>• Provide actionable guidance</td>
<td>• Reduce personnel costs</td>
</tr>
</tbody>
</table>

SOCVue Vulnerability Management helps reduce your attack surface, while saving time and reducing your operational costs. The service includes:

- Fully managed vulnerability assessment software-as-a-service
- Regular and unlimited scanning of critical internal and external-facing IT systems for known vulnerabilities
- Risk-based prioritization of vulnerabilities based on your unique business and security needs
- Summary data to stakeholders with easy-to-read executive reports
- Help meeting compliance requirements for vulnerability management
- Targeted scans for new or modified systems upon request
- Regular consultation with EiQ Security Analysts to discuss risk assessment and vulnerability trends
- Correlation of vulnerability results with active attacks by combining this service with SOCVue Security Monitoring
- Remediation guidance

© 2015 EiQ Networks, Inc. All Rights Reserved. EiQ, the EiQ logo, the SOCVue logo, SecureVue, ThreatVue, SOCVue, ComplianceVue, ForensicVue, and Continuous Security Intelligence are trademarks or registered trademarks of EiQ Networks, Inc. in the US and/or other countries. All other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies. All information presented here is subject to change and intended for general information.
Next Steps

Want to speak with a security expert? Schedule a demo with one of our Solutions Engineers to learn more about how SOCVue hybrid SaaS security services from EiQ can help you identify, analyze, and remediate the growing number of advanced cyber attacks and vulnerabilities and ensure compliance at a fraction of the cost of alternate solutions.

Or, attend one of our already scheduled weekly product briefings, held every Thursday at 1:00 p.m. Eastern.
About SOCVue

SOCVue® is the only subscription SaaS security offering that combines people, process, and technology to deliver an effective information security program, including:

- Proactive and Continuous Critical Security Controls Auditing
- Co-managed SIEM & Log Management
- Continuous Vulnerability Management
- 24x7 Security Monitoring by Trained EiQ SOC Security Analysts
- Incident Analysis, Notification, and Remediation Guidance
- Compliance Reporting

About EiQ Networks

EiQ, a pioneer in hybrid SaaS security services, is transforming how mid-market organizations build enterprise-class security programs. Acting as an extension of our customers’ IT teams, EiQ provides continuous security operations based on best-of-breed technology at a fraction of the cost of alternative solutions. EiQ is a trusted advisor to organizations that need to improve their IT security and compliance posture and protect against cyber threats and vulnerabilities. For more information, visit: www.eiqnetworks.com