REBASOFT

Information on how to better reduce exposure to vulnerabilities

IN THIS PAPER

Rebasoft Ltd - Continuous Vulnerability Assessment

PUBLISHED

14 December 2021

WRITTEN FOR

All audiences

This paper shows that performing continuous vulnerability assessments as recommended by many security standard/frameworks can reduce cyber-security breachs

Continuous Vulnerability Assessment

Barely a month goes by without an app on our iPhones needing an update. App updates are automatically run, and we hardly notice. Operating system updates are less frequent but require our attention. Sometimes, after updating, old applications cease working or exhibit strange behaviour. Incompatibilities cause this and are one of the fiddlier aspects of vulnerability management; ensuring your security upgrade does not break your application.

Business systems are also affected by vulnerabilities and require updates just as our iPhones. The problem is that you can't just let users perform updates as they see fit. Many organisations like to have a standard desktop/laptop builds so that the environment is supportable and predictable.

Similarly, server changes need to be planned and tested, with regression options if something unforeseen is discovered. For this reason, many organisations do not use fully automated patching solutions.

> Some 15,000-20,000 are found each year and keeping on top of them can be a full-time job. Not every vulnerability is relevant or even exploitable. A fraction of those discovered (estimated around 2%) are "exploitable" and represent a threat to many organisations. The trick is knowing which ones to worry about.

WHAT IS VULNERABILITY MANAGEMENT?

Simply put, it is the exercise of ensuring operating systems and applications are patched to reduce their likelihood of being compromised. The latest vulnerabilities are published daily. The trick is keeping on top of those vulnerabilities that might be a problem for your organisation. This means you need to:

1. Have a complete, up-to-date inventory of all your systems
2. Ensure they are analysed on a regular basis for known vulnerabilities
3. Quickly build and execute a plan for patching or upgrading systems to close vulnerabilities

Simple?

HOW CAN YOU DO BETTER VULNERABILITY ASSESSMENTS?

There are many vulnerability scanning solutions on the market. They all use the daily feeds from the NIST National Vulnerability database as a core data feed. Each of your systems is scanned (often an agent needs to be installed to scan non-network visible components). The process of installing, often a dissolvable agent, scanning and processing the results for a large network can take a considerable time. This means that many organisations scan weekly, monthly or, in some cases, only once a year.

Key problems with traditional scheduled scans include:

- They are not responsive to new, critical vulnerabilities release between scheduled scans
- They are often run at quiet times to reduce the impact of scanning loads but may miss connected systems
- They are often disconnected from the discovery / asset management process, again, meaning humans need to input to ensure no systems are missed
- They often lack information so that a prioritised change plan can be quickly built, adding to workload, and adding delays to plugging vulnerability holes.

HOW CAN REBASOFT HELP?

Rebasoft's real-time asset discovery capability means you get the latest, detailed knowledge of every asset you need to protect. There are facilities for tagging the most important systems to help with remediation priorities in your change control processes.

Our vulnerability scanning capability means the system can be scheduled to scan every device it finds – without you needing to manually set each scan up. It means

- Regular scans will pick up relevant vulnerabilities automatically

- Cross-referencing with device importance, and current connection status, means assessing and building change requests to install the most critical updates can be done with less effort and more accuracy

WHAT THE SECURITY STANDARDS SAY

Vulnerability management is an important part of every cybersecurity standard. There are many security standards, the table below shows some of the standards and the relevant sections stating the need for a vulnerability management process.

Subcategory	Framework reference
ID.RA-1: Asset vulnerabilities are identified and documented	CIS CSC 4
	COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02
	ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12
	ISO/IEC 27001:2013 A.12.6.1, A.18.2.3
	NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5