Uncovering Network Vulnerabilities: RedSeal Systems Vulnerability Management Tool

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Keeping track of the changing threat and vulnerability picture is a challenge for any security or network administration team. Threats change because of the constant efforts of Bad Actors who actively seek to exploit known vulnerabilities and to discover new ones. Vulnerabilities change because of changes in software versions, installation of new hardware or new firmware, installation of new software patches, and changes in network topology.

RedSeal Systems (<http://www.redseal.net/>) recently published a short White Paper entitled “Does the pace of business change create ‘holes’ in your security?” (<http://www.redseal.net/landing/WP_PaceofChange.pdf>) which, refreshingly, is available without registration. The authors discuss three major categories that can affect security:

- “Business drivers: Mergers & Acquisition, Business Project Pilots, Project & Service Outsourcing
- Regulatory/Compliance Mandates: Payment Card Industry Data Security Standards (PCI DSS) Sarbanes Oxley, HIPPA and other industry mandates
- New emerging technology adoption: Wireless services (e.g. WiFi), Virtualization, Hosted Applications, Cloud computing”

The authors continue, “Typically these changes also involve organizational changes. It is inevitable that change in the business and organization drive networks to constantly adapt. While being bombarded with competing demands, most organizations are in reactive fire fighting mode. With limited available resources, most businesses fail to integrate a security risk management process when making changes to the network. The disparate nature of various teams managing different aspects of the network aggravates this security risk environment across the enterprise. This often translates into unintentional security holes, defects and vulnerabilities, exposing the entire business and key stakeholders to high risk and in many instances, gross violation of compliance mandates.”

Readers may find the “short product tour” (<http://www.redseal.net/flash/srm_prod_overview.shtml>) interesting; in about seven minutes, the well-modulated voice of the speaker discusses the functionality of the RedSeal Security Risk Manager (RedSeal SRM).

RedSeal SRM has three major components: map, measure and mitigate.

- The map function audits the network infrastructure, including configuration and topology for all firewalls, servers, routers and other components; configurations can be imported manually or automatically. RedSeal SRM generates a network map that can be exported for further use. The vulnerability analysis at this phase produces reports on a wide range of violations of security best practices. The best practices standards “are compiled from
third-party vendors, security firms, and RedSeal security research team.” Reports can show the audit in a variety of ways, such as by device or by type of failure.

- The next function, “measure,” maps the original vulnerabilities to the as-configured topology, showing threat paths that represent the possible exploits to business assets within the network. Users can drill down to details of each vulnerability as reported by such organizations as the Computer Emergency Response Team Coordination Center (CERT/CC)< http://www.cert.org/ > and the MITRE’s Open Vulnerability and Assessment Language (OVAL) Repository < http://oval.mitre.org/repository/index.html >. These links usually provide links and instructions for patches.

- The mitigation function generates automatic reports recommending priority lists for corrections of the vulnerabilities that have been discovered. Each recommendation includes an estimate of how many devices can be attacked via the specific vulnerabilities and prioritizes according to the biggest payback per correction. This function also provides overall reports and trend analyses showing possible improvements in the security posture as a result of actual interventions.

The company offers 30-day trials.


[Note: I have never heard of RedSeal before I received a press release and have no financial relation with this company whatsoever. Their product just seems interesting to me.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at < http://www.mekabay.com/index.htm >.

Copyright © 2008 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.