CASE STUDY

NESSUS USER PROFILES

THE SMB SECURITY ADMIN

In years past, small and medium-sized businesses might have considered themselves effectively immune to cyberattacks – inasmuch as thinking that they didn't represent targets big enough to interest profit-seeking hackers. If that was ever true, **it certainly isn't now.**

The rise of ransomware and other major trends have driven SMB Security Admins and their leaders to shore up their cybersecurity. For these organizations, the vulnerability scanning and assessment capabilities of Nessus can be critical to their protective efforts.

Key responsibilities

SMB Security Admins are generally privately owned corporations, partnerships or sole proprietorships. The individual responsible for vulnerability assessment in a small and medium-sized business may be a part-time employee, or could also be a security person in a team of one (or a few) who wears a number of different security hats.

Whatever the specific circumstances, job title or team size may be, SMB Security Admin personnel who handle cybersecurity are responsible for the following:

- Ensuring that the organization is reasonably and properly safeguarded against risk and security threats
- Identifying weak spots and addressing them before a vulnerability is exploited
- Providing regular matrixed reports that demonstrate security and compliance
- Being the go-to person for security/vuln needs

Common challenges

Without question, the biggest obstacle that SMB Security Admins aim to overcome in terms of cybersecurity is a relative lack of resources.

The typical SMB Security Admin faces many of the same security challenges as a large organization. The only real difference is capacity.

Resource limitations, however, mean that SMB cybersecurity efforts may have to be more like firefighting than a comprehensive plan. This, however, can be addressed by automating certain VA tasks so that personnel responsible for cybersecurity are free to focus on the most pressing issues that require human intervention. This can only be accomplished by utilizing the right tools.

Without question, the biggest obstacle that SMB Security Admins aim to overcome in terms of cybersecurity is a relative lack of resources.

How Nessus helps

Leveraging Nessus for identifying and assessing vulnerabilities can significantly empower and improve even a one- or two-person IT security department. As the world's No. 1 vulnerability assessment solution, Nessus can positively impact SMB Security Admin cybersecurity from the second it's implemented.

Prefigured templates make it simple to conduct "point-in-time" assessments across an unlimited number of IT assets. Nessus enables SMB Security Admins to run custom scans that can meet the organization's unique needs, and achieve full visibility of their network like never before.

Nessus' customization features don't end with scan policies: Reports can be modeled as users see fit to focus on vulnerability type, host, asset or plugin. This capability is ideal for SMB Security Admins that know they have specific vulnerabilities in legacy systems, or expect a particular type of cyberattack. The Automated Live Results interface ensures that offline vulnerability assessments take place every time a plugin is updated, which can help alert SMB Security Admins to the possibility of weaknesses before they conduct their next scan.

Ready to get started?

TRY NESSUS FREE FOR 7 DAYS

tenable®