ALERT LOGIC®

CRITICAL WATCH™ REPORT

SMB THREATSCAPE 2019

Small to mid-sized businesses (SMBs) are under greater pressure than ever to address threats. Cybercriminals are increasingly targeting smaller businesses in addition to larger entepises. The principal challenge for SMBs is that they must face these threats with fewer security resources than large enterprises. Limited budgets and staff constraints are causing many organizations to make inadequate cybersecurity investment decisions that continue to put them at risk, but forward-looking SMB leaders are seeking new ways to be 'security smart' as they address cyber risks and respond to attacks.

Over a period of six months, Alert Logic researched the vulnerabilities present in SMBs.

Here are some highlights from our Critical Watch Report: SMB Threatscape 2019:

42%

of top SMB security issues are related to encryption

ENCRYPTION-RELATED MISCONFIGURATIONS ARE THE LARGEST GROUP OF SMB SECURITY ISSUES

Automated patching has made inroads in the fight to eliminate vulnerabilities in the SMB space. Patches are often distributed and can be done automatically across ecosystems. What remains as an issue is misconfigurations which can require remediations ranging from manual reviews to complete architectural redesigns. In our analysis, we determined that 13 encryption-related configuration issues account for 42% of all security issues found.

WEAK ENCRYPTION IS A TOP SMB WORKLOAD CONFIGURATION CONCERN

When we examined the top workload configuration issues, we discovered that 66% of the issues were related to weak encryption. This indicates that many organizations just implement the default encryption associated with an application. This presents a security challenge as many of these defaults were defined when older encryption protocols were still considered safe.

66%

of top SMB workload configuration issues involve weak encryption

65%

of port vulnerabilities appear on three ports: SSH (22/TCP), HTTPS (443/TCP) and HTTP (80/TCP)

THE THREE MOST POPULAR TCP PORTS ACCOUNT FOR 65% OF SMB PORT VULNERABILITIES

In examining ports, given that these ports are the ones that are exposed to the internet it is no surprise that SSH (22/TCP), HTTPS (443/TCP) and HTTP (80/TCP) made the top three with 65 percent of the vulnerabilities. It is, however, interesting to note that the recent MS RDP BlueKeep attack targets the fourth most popular port, RDP/TCP.

UNSUPPORTED WINDOWS VERSIONS ARE RAMPANT IN MID-SIZED BUSINESSES

More than 66 percent of scanned devices are running Microsoft OS versions that will be out of support by January 2020. The current Windows Server release – 2019 – is almost undetectable while the majority of devices scanned during the period analyzed are running Windows versions that are more than 10 years old.

66%

of SMB devices run Microsoft OS versions that are expired or about to expire

50%

the approximate amount of SMB Linux kernels that are among the 'working dead'

OUTDATED LINUX KERNELS PRESENT IN NEARLY HALF OF ALL SMB SYSTEMS

About half the systems we identified are still running a version 2.6 kernel, which has been out of support for more than 3 years. There are at least 69 known vulnerabilities for this kernel level, with many of them relatively easy to exploit and with 24 of the Common Vulnerabilities and Exposures (CVEs) scoring 7 or above on the severity scale.

SMB EMAIL SERVERS ARE OLD AND VULNERABLE

Almost a third of the top email servers detected were running on Exchange 2000, which has been unsupported for almost 10 years (since July 2010). Despite being the life blood of organizations, SMBs are running the risk of email failures resulting from newly identified vulnerabilities for which patches will not be made available.

>30%

of SMB email servers operate on unsupported software

GET THE COMPLETE SET OF INSIGHTS FROM ALERT LOGIC

DOWNLOAD THE FULL REPORT

ALERT LOGIC®