RESTECH
SOLUTIONS

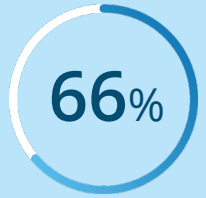
VULNERABILITY MANAGEMENT

THE NEXT LEVEL OF IT SECURITY SERVICE

A typical visit to the dentist includes a dental X-ray. Why? Because it identifies underlying issues that can't be seen. Those issues can lead to pain, costly dental work and a loss of productivity during the healing process. Vulnerability scans are no different. Vulnerability scans identify underlying network issues that you wouldn't otherwise notice. However, when these issues are identified and exploited by a cybercriminal, they result in organizational distress, loss and disruption in productivity.

Cybercriminals scan your computer systems from the outside for vulnerabilities in your firewall (if you have one). Once breached, hackers use automation to quickly probe every single device connected to your network, looking for an opening to gain administrative access to take over a computer or even the entire network. For cybercriminals, it's not the size of the business that matters, it's the ease of access.

Although many small and midsize businesses (SMBs) think they're too insignificant to draw the attention of hackers, breach reports prove otherwise with 66% of SMBs experiencing a cyberattack in the past 12 months. Most of those attacks (70%) were executed via web applications and miscellaneous errors, aka internal vulnerabilities.



66% of SMBs experienced a cyberattack in the past 12 months.

CAN YOU AFFORD AN ATTACK?

IBM's most recent Cost of a Data Breach report puts the average cost of a data breach at $4.24 million when you add up all the direct and indirect costs, including downtime, fines, lawsuits, notifications and identity protection, for individuals who were compromised.

The National Institute of Standards and Technology (NIST) recommends vulnerability scans to be run at least quarterly, regardless of network size or type. However, for any organization that relies on the continuous availability of its computer network for regular operations, a vulnerability scan should be run at least monthly, and even more frequently for organizations that collect and/or process personal, financial or sensitive data.

Even with this information, many companies aren't willing to invest in cybersecurity to properly protect the lifeblood of their organization. It goes without saying that the cost of a data breach can inflict far greater damage than just financial ramifications. Loss of customers and their trust are incalculable repercussions that could completely sink any organization.

IT CAN HAPPEN TO YOU!

- **57% of data breaches** that SMBs **suffered** involved external threat actors.
- **$2.98 million** is the average cost of a data breach for SMBs with <500 workforce.
- **Only 47% of SMBs** are identifying breaches within days.
- **43% of SMBs** do not have any cybersecurity defense plans in place.
- **1 in 5 SMBs** do not have any endpoint security protections.

WHAT ARE NETWORK VULNERABILITY SCANS?

Network vulnerability scans play a crucial role in safeguarding networks. The process involves both external vulnerability scanning — a scan from the outside to check your network's firewall and other "perimeter" defenses — and internal vulnerability scanning — a scan that tests every device on your network. Internal vulnerability scans not only look at your servers and workstations but also check laptops, mobile devices, printers, network phones and anything else internally networked.

The scanning process is identical to what hackers do when they search for weaknesses on a targeted network. The scans detect any known vulnerability and send an alert after each scan with details on the vulnerable devices and nature of the weaknesses. This is critically important because unless you find and fix the root cause of the problem, it leaves your systems inside the network vulnerable to attack.

New bugs and vulnerabilities are identified daily and can exist on any device on your network — both public-facing computers and systems inside the network. Vulnerabilities often remain unchecked for weeks, months or even longer, increasing the likelihood that a random check of your system by hackers will yield a payday for them and a nightmare for you.

PATCHES AREN'T PERFECT

Simply staying current on security patches isn't enough. That approach poses a two-pronged problem:

1

First, a vulnerability must become known before a patch can be developed. What if cybercriminals discover the weakness before the software vendor? What if the software vendor knows about the weakness, but fixing it requires a major development effort that could take weeks or months?

2

Second, patches won't fix misconfigurations when a system is deployed in a misconfigured state. The system remains in that misconfigured state no matter how many patches are deployed until a vulnerability scan detects the issues or a cybercriminal exploits them.

SCANNING ALONE ISN'T ENOUGH

Simply scanning your network doesn't make your network any safer or less vulnerable to a data breach. It's like getting your teeth X-rayed. You need a professional to interpret the fuzzy gray image, determine what the actual decay is, and then address a small cavity before it worsens to the extent that the tooth cracks or needs to be removed.

A scan checks more than 65,000 ports on every device on your network, so you can imagine the amount of data it delivers. Not all discovered vulnerabilities present the same risk level, and it is virtually impossible to address every vulnerability on every device, every day.

A great number of network vulnerabilities are benign because they're on devices that don't contain important information worth stealing or they aren't connected to more important devices. Other vulnerabilities are benign because they have a very low likelihood of being exploited.

VULNERABILITY MANAGEMENT IS ESSENTIAL FOR YOUR IT SECURITY

Just like everyone needs to get periodic X-ray scans when they visit the dentist, every computer network needs periodic vulnerability scanning as part of good IT security hygiene. Sometimes, an X-ray will reveal hidden decay or other issues that need immediate attention. The same X-ray may also reveal minor problem areas that can wait until your next scheduled visit.

As with the analysis of fuzzy X-rays, you will want a qualified IT professional to review the results of each network vulnerability scan to determine what is a serious vulnerability that deserves immediate action and what vulnerabilities present a lower risk that can be addressed during a scheduled network cleanup session.

The frequency of scans and regularly scheduled network hygiene sessions depends on a lot of factors. Small organizations with just a few computers running in a workgroup may only need periodic scans when changes are made to the network. However, for most situations, a monthly scan with regularly scheduled quarterly security cleanup tasks is the minimum frequency. For any organization that collects, uses or stores sensitive data, a weekly scan with monthly network adjustments is recommended. Even more frequent scans may be needed for certain regulated industries and organizations that require the highest level of cybersecurity.

OUR VULNERABILITY MANAGEMENT SERVICE

Our enhanced IT security service involves setting up one or more dedicated security vulnerability scanners on your computer network. The scanner is designed to check every device on your network — including servers, desktop computers, mobile devices, printers, network phones, etc. — and look for known vulnerabilities. We can also use our external scanners to perform the same vulnerability tests on your firewall.

We will program it to run automatically at a specific time interval and set up a schedule for routine network adjustments based on the results of the scan data. The frequency of scans and scheduled security hygiene sessions will depend on your specific situation.

As soon as each network scan is complete, the system sends the results of the scan to our cloud-based vulnerability management platform along with alerts of any discovered issues. The alerts tell us the nature and location(s) of each discovered issue. This allows us to quickly address any high- risk vulnerabilities and creates a checklist of more routine items to take care of during our regularly scheduled network hygiene sessions.

ROOT CANAL OR CHECKUP?

Nobody LIKES going to the dentist, but an annual checkup is far less costly, painful and debilitating than ignoring routine inspections and ending up needing a root canal, crown or something worse. The same can be said about vulnerability scanning. Nobody is ever excited about an additional service or additional fee but ignoring vulnerabilities and pretending that they don't exist will eventually result in a cyberattack that could cost millions in extortion and remediation.

Don't put your business at risk by ignoring potential network vulnerabilities. The question is no longer "What if someone exploits a vulnerability on our network?" but rather "When will someone exploit a vulnerability on our network?" We can help eliminate the risks by identifying and remediating those vulnerabilities before someone else discovers them.

1. Ponemon Institute's state of the cybersecurity report
2. IBM and the Ponemon Institute's 2021 Cost of a Data Breach Report
3. Verizon's 2021 Data Breach Investigations Report (DBIR)

RESTECH SOLUTIONS

Please contact us today to get a professional assessment and customized vulnerability management plan.

713-936-6855
info@restech.solutions
https://restech.solutions/contact