20 Dec 2022 |Dexter McGriff - President & CEO

Why Your Government Agency Needs Vulnerability Assessments

Unforeseen vulnerabilities can derail your agency and result in a variety of problems. Sometimes these issues are minor, while others are much more severe, such as ransomware or malware infecting your devices. Taking a proactive approach to identifying and taking care of these vulnerabilities is essential for Government Agencies. A managed service provider can give your company much-needed protection by offering vulnerability assessments. **What is a Vulnerability Assessment?** Vulnerability testing involves a detailed assessment of any security weaknesses within your IT infrastructure. These weaknesses can be wide-ranging, whether it's weak passwords, outdated software, or poor firewall configuration. A managed service provider will conduct these assessments on an ongoing basis to ensure your agency is well-prepared for resolving any issues or preventing the chance of a successful cyber-attack. **What are the Different Types of Vulnerability Assessments?** A managed service provider can perform different vulnerability assessments to best meet your needs. These assessments can focus on many different areas of your company, whether it's your network, workstations, applications, or database. Typically, it's a good idea to schedule vulnerability testing on a quarterly basis. However, a managed IT service provider can evaluate the needs of your agency to determine how often you should schedule vulnerability testing. Here are a few reasons to schedule vulnerability testing for your agency. **Cost-Effective Option** Keeping operating costs to a minimum is often a priority for government agencies. One of the reasons to schedule vulnerability testing is that it can help you identify and resolve any technical issues before they turn into major problems. An IT service provider can work closely with your team to develop a plan to resolve any issues, which is much more cost-effective than waiting to respond to an incident. **Stay Proactive Against Threats** Another reason to consider vulnerability testing is that it helps you stay proactive against all types of cyber threats. These tests can identify any potential problems, whether it's outdated software, network problems, or any other issues. Identifying and taking care of these issues now can help keep your agency safe and avoid downtime or a data breach. **Meet Compliance Requirements** Meeting different requirements for managing data is essential for many agencies. Failure to stay in compliance with these laws can result in substantial fines against your company. These violations can even damage your trust with customers. Vulnerability testing is a great way to identify any issues to help you take care of them now before it results in a compliance violation. **Final Thoughts** Vulnerability testing is a key aspect of keeping your agency safe. A managed service provider can perform vulnerability testing on a regular basis to help identify any problems ahead of time. Vulnerability assessments also offer a wide range of benefits, whether it's saving you money, reducing the threat of cyber-attacks, and helping you meet compliance requirements for your industry. Staying proactive by scheduling vulnerability testing with a managed IT service provider will give your agency much-needed protection in today's digital workspace.