



Security Vulnerability Scanning

Business Vitals' Security Vulnerability Scanning service looks at your network from the "INSIDE" as a Network Administrator or System Administrator would see it, to identify security vulnerabilities that may put your network at risk. This service may be engaged for a variety of reasons:

- You want the "peace of mind" that comes from having an objective 3rd party look at your network and confirm that your information security policy has been properly implemented.
- You had an internal accident where an employee made a mistake that resulted in a security breach.
- You have an upcoming regulatory compliance audit and you want to make certain you are prepared for it.

Many of our Clients use this service to audit the security profiles of their networks in the same way that they engage independent financial auditors to examine their financial auditors. The results of these audits can be used to confirm compliance with legal and financial regulations.

Engagement Objectives:

- Run network scanning tools from multiple remote locations to identify security vulnerabilities.
- Identify open ports on servers that could be exploited to attack your network.
- Identify servers running services that are not needed for specific business purposes.
- Identify website applications that could be attacked to compromise your network.
- Preparation of recommendations designed to eliminate or mitigate the risks posed by identified security vulnerabilities.

Benefits:

An objective, qualified and certified 3rd party examines your network from the "INSIDE" to identify security vulnerabilities posed by:

- Servers that are not up to date with software patches, security updates and service packs
- Improperly managed passwords
- Remote access services that are not properly secured
- Servers running questionable services
- Shared hard drives that are not properly secured

Recommendations are presented to eliminate or mitigate the identified security risks.

Most Frequently Asked Questions (FAQ):

1. How do I engage Business Vitals to help me with security vulnerability scanning?

When you contact Business Vitals about security vulnerability scanning, a security consultant will meet with you to identify and understand your requirements, and draft a statement of work that accurately describes the work to be done. The statement of work will include a time line and the cost for performing the work. The consultant will review the statement of work with you to confirm that it accurately describes the work to be done, and after it is signed by both parties, the work is scheduled.

2. How often should vulnerability scanning be done on my network?
Most corporate networks are constantly changing to keep up with the requirements of users in the business units who need the network to perform their jobs. To ensure that a high network security profile is maintained, security industry best practices suggest that vulnerability scanning should be performed at least annually or any time after a significant change is made to the network infrastructure.

3. How are the security vulnerability scans run?
An appliance (PC), configured with a collection of scanning tools, is delivered to your designated site, connected to your network and given appropriate access rights. The appliance is controlled remotely through an Internet connection and network scans are initiated through a remote console. Data collected by the scanning tools is encrypted and transmitted to a secure server in our data center. The data is held there for the duration of the assessment, then destroyed to ensure that it is not compromised.

4. How intrusive are the security vulnerability scans?
The scans are not intrusive at all. They can be run from a remote location so there is no need for our network engineers or security consultants to come to your site. Or, if you prefer, they can be run by

our professionals from your site. If your network is being monitored, your systems should alert you of our scanning activity.

5. Will the vulnerability scans disrupt the normal operation of my network?

We have never had a complaint that our vulnerability scans had a negative effect on a Client's network performance. If you are concerned about that, the scans can be scheduled to run after normal business hours.

6. What will the vulnerability scans tell me about my network?

The scans identify security vulnerabilities that could be exploited by a hacker or a person with malicious intent to attack your network. The scans also identify missing software patches, security updates and service packs. Security vulnerabilities are correlated with known security breaches and recommendations are presented to eliminate or mitigate them.



Outsource Your Technology Risk™

888.287.8483 ext. 102

www.businessvitals.com