How Secure is Secure Enough for Your Network?

Did you Know...

Having a security assessment done can find weak spots on your network. If there are any vulnerabilities within the network, they will be found so that the discussion for an effective solution can begin. Doing these assessments on a regular basis helps to decrease the chances of a data breach. For any company handling private personal info, credit card info, eCommerce, or need to meet some type of compliance level, this is a highly recommended proactive step to take.

Why should your business be preventative with your network?

If your business has a network or cyber security concerns, this assessment will make sure that your security needs are met. Even if your organization does not have any compliance standards out of the ordinary, this is still highly recommended. What if you could decrease downtime and emergency maintenance costs? This assessment will be able to guide your organization to the best solutions for your network and to keep viruses, disgruntled employees, and hackers out of your network!

Software Only

Software + Applicance

262.522.8560
sales@ontech.com

Ontech systems, inc.

Ontech Systems, Inc.
N85W16186 Appleton Ave., Suite A
Menomonee Falls, WI 53051

What is Found in a Security Assessment?

Network Security Risk Review: This report includes a proprietary Security Risk Score and chart showing the relative health (on a scale of 1 to 10) of the network security, along with a summary of the number of computers with issues. This powerful tool also reports on outbound protocols, System Control protocols, User Access Controls, as well as an external vulnerabilities summary list.

Network Security Management Plan: This report will help prioritize issues based on the issue's risk score. A listing of all security related risks are provided along with recommended actions.

External Vulnerabilities Scan Detail Report: A comprehensive output including security holes and warnings. Informational items that can help make better network security decisions, plus a full Port Scan which checks all 65,535 ports and reports which are open. This is an essential item for many standard security compliance reports.

Outbound Security Report: Highlights deviation from industry standards compared to outbound port and protocol accessibility, lists available wireless networks as part of a wireless security survey, and provides information on Internet content accessibility.

Physical Security: Ontech will review the physical environment for your IT assets, and make recommendations for improvements that can increase the security of your network infrastructure.

Login History by Computer Report: Same data as User Behavior but inverted to show you by computer. Quite useful, in particular, for looking at a commonly accessed machines (file server, domain controller, etc.) - or a particularly sensitive machine for failed login attempts. An example would be CEO's laptop - or the accounting computer where you want to be extra diligent in checking for users trying to get in.*This will vary depending on the security logs on your domain controller. *This will be a limited report if you have customized permissions

Login Failures by Computer Report: Report identifies users who have succeeded in logging in to another machine. Great for auditing/logging purposes to know of all attempts.

Advantages to Completing a Software + Device Scan!

The Inspector Device includes special deep-dive network and security bonus reports. You'll get a set of super useful Layer 2/3 diagrams and reports that provide both logical and physical device discovery. You'll also get internal vulnerability scan reports for identifying risks behind the firewall where most security breaches occur.

Internal Vulnerabilities Scan- Open Ports and Protocol Vulnerability that would be exploited ONCE a hacker is on your network - or by employees. INSIDE attacking INSIDE. This complements the external vulnerability scan performed with our Security Assessment module, which finds weaknesses at the network "edge" that could be exploited by external sources.

This security analysis is not all encompassing, however, the results of this analysis may prompt additional recommendations that are more focused on specific aspects of your environment.
EX: PCI & HIPAA audits, in-depth anti-virus testing, firewall/router audit, etc.