LAPTOP SECURITY CHECK
FOR A
SECURE IT
IN A
BUSINESS ENVIRONMENT

Mag. Walter Sedlacek, MSc MBA

CIO, General Motors Powertrain Austria

Abstract

In today’s business laptops are state-of-the-art. Often there is a need to connect a laptop belonging to an employee of company A to a network of company B, e.g., during a business-visit or during some maintenance activities in a manufacturing plant. Because the laptop could be infected with a virus and thus could harm the IT environment of the company B, this connectivity is sometimes forbidden by the corporate IT security policy of company B. This paper describes various solutions on the market, which overcome this situation and ensure the IT security that customers need.

Content

1 Problems with External Laptops

Most laptops run *Microsoft Windows* as an operating system, which has a high connectivity. Not only network support via TCP/IP over Ethernet is part of this operating system but many alternatives like Wireless Networks or USB also help the system to connect to various sources.

Running this multi-connection operating system without a proper security management is a high risk. Every month three million *Microsoft Windows* operating systems get infected by viruses, worms or other malicious code. The attacks are not only based on email attachments, simple network connections can also lead to unwanted effects.

In corporations IT security policies drive the IT protection for the internal PCs and laptops and enable to manage the risk of IT security issues.

Often there is a need to connect an external laptop, belonging to an employee of a different company to the corporate network, e.g., during a business-visit or during some maintenance activities in a manufacturing plant. This would disrupt the internal IT security policy and increase the risk of a vulnerability attack tremendously. On the other hand not connecting this external laptop might harm business relations or lead to higher maintenance costs.

2 Specification of a IT Security Check tool

To reduce the risk of potential IT vulnerability the following prerequisites must be met for *Microsoft Windows* based systems:

- An Anti Virus System must be installed
- The latest Anti Virus Patterns must be loaded
- The latest Service Pack from *Microsoft* must be installed
- The latest Hotfixes from *Microsoft* must be installed

These prerequisites, which can be seen as the IT security policy, are agreed between all major software companies and independent IT security organizations like BSI[1], HEISEC[2] or CERT[3].

The prerequisites should be audited on the laptop by an application within less than one second in order to avoid to high impact for the to the laptop owner.

The application needs to be loaded with the latest security information regarding Anti-Virus-Patterns and *Microsoft* Hotfixes. The IT security policy, which drives the behavior of the application, should be adjustable regarding the dates of the required latest Hotfixes or Anti-Virus-Patterns.

If the IT security policy is not met, e.g. the Anti Virus Patterns are older than required by the IT security policy; the application should indicate this in a simple, easy-to-understand way.

[1] http://www.bsi.de

[2] http://www.heise.de/security/

[3] http://www.cert.org

3 Solutions on the Market

There are many solutions on the market which meet the requirements mentioned above. Some are very highly sophisticated and need a special network architecture from a specific vendor. Others are simple and easy to use. Between these two extremes all kinds of solutions are available. The following sub-chapters give an overview of some representatives of the various solutions. The list is, of course, not complete.

3.1 *Cisco* Clean Access (NAC Appliance)

Description from vendor[4]

Cisco Clean Access (NAC Appliance) is an easily deployed Network Admission Control (NAC) product that allows network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto the network. It identifies whether machines are compliant with security policies and repairs these vulnerabilities before permitting access to the network. *Cisco* NAC Appliance integrates the tasks of authentication, posture assessment, and remediation into one package, making it suitable for organizations that prefer a comprehensive turnkey solution over an infrastructure-based solution.

Interpretation

This solution provides a very good interface to *Microsoft* products (all relevant operating systems are supported), but a 100% *Cisco* based environment is a prerequisite. If a company does not have a 100% *Cisco* based environment, this solution is not applicable.

[4] http://www.cisco.com/en/US/products/ps6128/index.html

3.2 *Microsoft* Network Access Protection (NAP)

Description from vendor[5]

The Network Access Protection (NAP) platform is a computer health policy enforcement technology that provides system health validated access to private networks. The NAP platform provides an integrated way of detecting the health state of a network client that is attempting to connect to or communicate on a network and optionally isolating that network client until the health requirements have been met. To protect access to a network, a network infrastructure needs to provide the following areas of functionality: policy validation, ongoing compliance, network restriction, and remediation. The NAP platform provides enforcement for DHCP address configuration, VPN-based network connections, 802.1X authenticated connections, and IPSec-based communication. The NAP platform is an architecture through which policy validation, ongoing compliance, network restriction, and remediation can occur via additional components supplied by third-party software vendors or Microsoft.

Interpretation

This solution is not 100% ready and supports only *Microsoft* Windows XP SP2. Therefore it is of very limited use for grown and legacy environments.

3.3 *Shavlik's* PatchPush Tracker

Description from vendor[6]

Intuitive Patch Management interface allow to control which groups will be scanned, by what criteria and when, how patches are deployed and more. In minutes instant validation of patches can be received. Shavlik HFNetChkPro™ allow to work with patches in a variety of ways, including criticality, patch grouping, type of patch, annotation, machine grouping, machine and deployment templates and more. Pushing patches to clients is possible also. Supported platforms and products including Windows

[5] http://www.microsoft.com/technet/itsolutions/network/nap/naparch.mspx

[6] http://www.shavlik.com/hfnetchkpro.aspx

NT, XP, 2000, Windows Server 2003, Exchange, SQL Server, Outlook, Microsoft Office, Java Virtual Machine, non-Microsoft product support such as WinZip, Apache and more.

Interpretation

This product shows a very high performance and enables patching of the investigated system. On the other hand, Anti Virus Systems can not be checked.

3.4 *WEL-Service* SecurityPolicyCheck

Description from vendor[7]

The SecurityPolicyCheck tool is loaded with the latest security information regarding Anti Virus Patterns and *Microsoft* Hotfixes. The IT security policy, which drives the behavior of the SecurityPolicyCheck tool, is fully customize-able, meaning the date of the required latest *Microsoft* Hotfix or Anti Virus Pattern is adjustable.

It is possible to implement the application, which audits the laptop, on an USB stick, a CD-ROM or a floppy disk. The application is start-able from the laptop, while being loaded on the external stick/CD/floppy. If the IT security policy is not met then the SecurityPolicyCheck tool will visually indicate this with a red banner in the application. A command-line version can be used in e.g. log-on scripts or as ActiveX within websites.

Interpretation:

This is a very small application, which consists of only one executable with less than 800 Kbytes. It meets all requirements and it is a low-cost solution to minimize IT security risks. For heterogeneous environments it is a very good solution, because it is inexpensive and simple to use.

[7] From an interview with the owner of the company in June 2006.

4 Conclusion

IT Security is more and more important for companies and due to budget cuts and business demands a cost-effective and easy to use solution is required. *WEL-Service*[8] Security-Policy-Check is one product that meets all these requirements.

For 100% *Cisco* based network environments the *Cisco* Clean Access (NAC Appliance) might be an alternative.

Mag. Walter Sedlacek, MSc MBA
CIO, General Motors Powertrain Austria
Information Systems & Services
Grossenzersdorferstrasse 59
A-1220 Vienna / Austria
Phone: + 43 1 28899 4605
Mobile: + 43 664 3423011
E-mail: walter.sedlacek@at.gm.com

[8] http://www.welservice.com/en/