SECURING YOUR DESKTOP

In today's computing environment, the security of all computing resources, from network infrastructure devices to users' desktop computers, is essential. There are many threats to users computers, ranging from remotely launched network attack to malware and viruses that are spread through e-mails, websites, and files. Increasing the security of individual desktop protects them from these threats and reduces the chances to be compromised.

The main objective of this article is to formulate a security configuration policy for Microsoft Windows Operating Systems called as Baselines. These baselines can be adapted to any organization running any versions of Windows Operating Systems. Apart from these baselines, Anti-Virus and Windows Updates are mandatory to ensure System Security.

Dr. SHUBHAG CHAND
Technical Director
shubhag@nic.in

VINOD KUMAR J
Scientific Officer SB
nj.vinod@nic.in

Group Policy is a feature of the Microsoft Windows Operating systems that controls behaviour of the operating system. Group Policy provides the way of configuring of operating systems policy, applications behaviour with operating system, and user settings. Group Policy primarily decides what users can and cannot do on a computer system.

GROUP POLICY OBJECT (GPO)

Group Policy Object is a group of configuration policies that configures a group policy. Our primary objective is to formulate a Group Policy Object that enhances the security configuration of the system without affecting its working. Some standards and list of security steps should be decided to make the group policy object effective. Available standard has been adopted as reference and new GPO is prepared. This GPO Object is applied to the individual systems to enhance the security.

SECURITY BASELINES

Security baseline is a collection of Group Policy Objects grouped on the basis of features. New baselines can be created by adding or removing the Group Policy Object from the available Baselines. Microsoft and other Security Agencies provide several baselines for Windows Operating Systems Security. Each baseline specifies the basic change that has to be made in the policy.

The commonly used baselines provided by the Microsoft are Specialized Security Limited Functionality (SSLF) and Enterprise Client (EC).

Specialized Security Limited Functionality (SSLF) Baselines are used in environment, which has a high risk of attack. Enterprise Client (EC) Baselines are used in enterprise environment, which is usually comprised of a server and client system that need to be protected from threats on the Internet.

These two baselines i.e. EC and SSLF can be combined to create a new baseline as per the organization requirement. Microsoft has published their baselines for all available versions of Windows Operating Systems.

Another baseline commonly used was evolved from the Federal Desktop Core Configuration Mandate defined by the United States Government & named as United States Government Configuration Baseline (USGCB). The purpose of the USGCB is to create security configuration baselines for systems deployed in Federal Agencies of United States. USGCB has published their baselines for Windows 7, Windows Vista, Windows XP, Internet Explorer and Red Hat Enterprise Linux. These baselines are published by National Institute of Standards and Technology (NIST).

To strengthen the desktop security further, new baseline can be created by combining the Microsoft baselines and USGCB baseline depending upon the organization need.

SECURITY COMPLIANCE MANAGER

To create Group Policy Object for the prepared baseline, a Security Compliance Manager provided by the Microsoft is used. This tool helps in creating a GPO by importing the available GPO and modifying it as per the organisation requirements, merging two or more different baselines to create a new baseline etc.

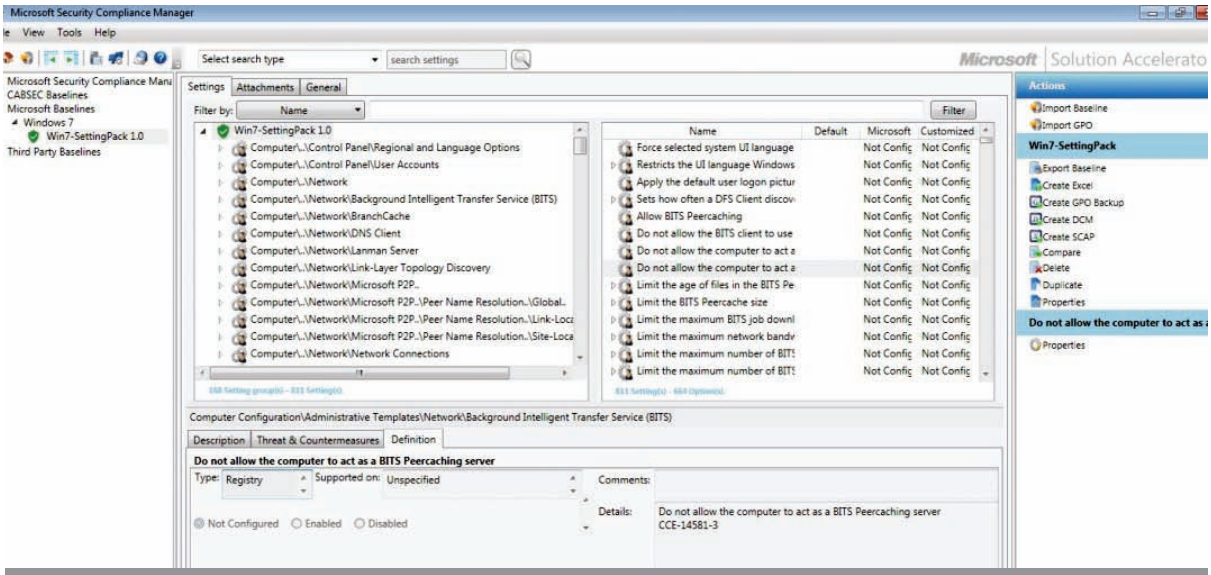

Figure: Screnshot of Microsoft Security Compliance Manager

APPLYING BASELINES

Once the baseline and the Group Policy Object are ready, we need to deploy these policies in the client machine. If the machine is available in the domain, we would simply update the GPO in the Active Directory Server and push it to all the clients. But if the machine is not available in the domain, we need to have a special software issued by Microsoft called Local GPO.

This Local GPO has built-in script that has the ability to read the GPO object and apply it to the desktop.

HOW TO IMPLEMENT?

Initially, one has to prepare a list of security configurations from the baselines, which are essential for the concerned organisation. Then, prepare a Group Policy Object, and implement this GPO in all the desktops of your organisation. If there is any performance or work related issue with the implemented baseline, issues have to be identified and new baseline have to be prepared moderating the security settings. Each time whenever you change or add to the security settings, you have to follow all the above steps. Once the perfect GPO is ready, the batch file so created will get the GPO object location and implements the complete security baselines on the client system, which would internally implement more than 450 security settings for Windows 7 Operating System, depending upon the baselines one has adopted for the concerned organisation, which is not feasible when done manually.

SECURITY AUDIT

To check whether the baseline is implemented properly, one can use any auditing tools available in the open market. For example, Belarc Advisor is one tool which can audit the client security policy and provides the rating based on USGCB baselines. Similarly, there are many tools available which can benchmark the system based on the commonly used baselines like USGCB or Microsoft baselines and provide the rating for the system.

CONCLUSION

Implementing either the USGCB Baselines or Microsoft SSLF Baselines directly ensures that that system security rating is more than 80% in most of the commonly available third party security auditing tools.

To achieve higher security ratings, one has to add more security steps in the USGCB or SSLF baselines.

Sustainable efforts can be made to maintain constant vigil regarding computer security by implementing a strong baseline and computer security audit. They should be carried at regular intervals as per concerned organization needs.

Apart from implementing a strong baseline, Anti-Virus software should be regularly updated.

FOR FURTHER INFORMATION:
Dr. Shubhag Chand
HOD, Cabinet Secretariat
Rashtrapati Bhawan
New Delhi.
E-mail: shubhag@gmail.com