Security-Insider.de - Protect Your Terminals With Signatureless Solutions

Further to his recent in-depth tests of the Stormshield Endpoint product SES, Dr. Götz Güttich, Head of the Test Laboratory within the Institute for the Analysis of IT Components, IAIT will talk you through the different functionalities of the product and the results obtained in the following article (published on the following site 'Security-inside.de'). To read the full version of his test results http://www.security-insider.de/sichere-clients-ohne-pattern-updates-a-569497/

Introduction

With Endpoint Security 7.212, Stormshield provides a security solution for Windows systems which monitors all actions taking place on the computers in question and prevents potentially dangerous activities. Rather than using signatures to detect viruses, worms, and similar malware, the product exclusively examines the activities of the running programs and analyzes them for dangers. This enables the solution to prevent all possible attacks, be it from keyloggers, ransomware, unknown viruses, or other malware, without having to rely on constant updates. The security tool underwent extensive testing in our test lab.

Safeguarding the System Behavior

Stormshield claims that, if the system behavior parameters are configured correctly, Stormshield Endpoint Security already blocks 95% of all attacks without any other configuration measures. During the test, we used a configuration that was recommended by the manufacturer, and which concentrated exclusively on the system behavior. There were therefore no rules with regard to individual applications and similar features. This configuration was therefore created very quickly.

The "Security" area also includes the device control, where the responsible persons specify whether the use of modems, Bluetooth components, IrDA, LPT, disks, various USB devices, and much more is authorized. If required, the administrators can work with group rights, log which file has been copied onto which USB stick when, and – if necessary – encrypt them automatically.

The application rules are used to create blacklists, whitelists, and greylists. These lists determine what each defined application is allowed to do in the file system, on the network sockets, during registry access, and so on. The rules can be tested before commissioning, and can also be activated and deactivated at any time. There were no problems concerning this aspect during the test.

By contrast, the extension rules specify which programs are authorized to use which types of file. For example, administrators can ensure that Outlook is only authorized to open PST files, which can significantly increase security in many environments. The security policies are therefore extremely efficient and provide a very large number of functions.

Using the "Scripts" area, IT administrators are able to determine exactly what should happen when certain conditions are met. For example, the scripts are used to define actions that are only activated when condition one is "true" and condition two is "false". There is, therefore, the option of assigning different policies to a user from group one than to a user from group two. These scripts are undoubtedly very useful in many environments. Once the policies have been defined, they can be linked to the target systems via the "Environment" point.

Testing the Agent

After we had configured our test policy to protect against ransomware and malicious code, we deployed the agent to our clients on Windows 7, Windows 8.1, and Windows 10, and distributed our configuration. After securing our clients, we first opened Thunderbird, the e-mail program which is installed on the test systems. We had previously created an e-mail account to collect all the spam with attachments or dubious links that we had received through our regular e-mail addresses in the past weeks. During the test, we started by opening all the attachments and running the files that they contained. At the same time, we visited the potentially dangerous websites that were advertised by the spam e-mails. We received many messages from the Stormshield solution, warning us about heap overflows, attempts to carry out dangerous actions and other similar dangers. We then tried to open various current viruses and ransomware programs directly on the test clients. Once again, the Stormshield agent reported that it had blocked numerous unwanted actions. In the end, we spent a while surfing the Internet with the test clients, focusing particularly on sites with a bad reputation from the erotic, keyz, and warez scene. On these pages, we clicked primarily on advertisements which could potentially force malware on visitors to the websites in question. Our system was not compromised during any of these actions. We verified this by performing complete virus scans on all clients with two different antivirus products (Avira and Windows Defender) after completing the test. When we examined the results in detail, it turned out that the RAM and registry had not been compromised at all, and that the antivirus solutions only found infected malware files on the hard drive.

Conclusion

On completing the test, we were completely convinced by the Stormshield Endpoint Security solution. The agent is extremely efficient and blocked all attempted attacks by our malware products. Web access was also protected so that there were no infections. However, due to the large number of available functions, the product is not self-explanatory. Administrators who wish to work with it must have time to familiarize themselves with the documentation and administration interface. However, they will then be rewarded in practice with a safety configuration that precisely meets the requirements of their environment and which significantly increases the level of protection in the company.

About the Author: Dr. Götz Güttich is Head of the Institut zur Analyse von IT-Komponenten (Institute for the Analysis of IT Components, IAIT) and has over fifteen years of industry experience as an IT consultant and specialist editor or editor-in-chief in the IT environment. Due to his many years of extensive testing work for leading German network magazines, his skills are not limited to the theory of IT business.