Security-Insider.de – Sichere Clients ohne Pattern-Updates

Zusätzlich zu seinen in die Tiefe gehenden Tests der Stormshield Endpoint Security (SES), wird Dr. Götz Güttich, Leiter des Instituts zur Analyse von IT-Komponenten (IAIT), Sie durch die unterschiedlichen Funktionen des Produktes führen und das detaillierte Ergebnis des Test genauer erläutern (veröffentlicht auf der Webseite www.security-inside.de). Für die ungekürzte Version des Tests folgen Sie bitte dem folgenden Link: http://www.security-insider.de/sichere-clients-ohne-pattern-updates-a-569497/.

Einführung

Mit der Endpoint Security 7.212 bietet Stormshield eine Sicherheitslösung für Windows-Systeme, die sämtliche auf den zu schützenden Rechnern stattfindenden Aktionen überwacht und potentiell gefährliche Aktivitäten unterbindet. Dabei verwendet das Produkt keine Pattern, um Viren, Würmer und Vergleichbares zu erkennen, sondern nimmt ausschließlich die Aktivitäten der laufenden Programme unter die Lupe und analysiert diese auf Gefahren hin. Damit ist die Lösung dazu in der Lage, alle möglichen Angriffe zu unterbinden, egal ob durch Keylogger, Ransomware, unbekannte Viren oder ähnliches, ohne dabei auf ständige Aktualisierungen angewiesen zu sein. Wir haben das Sicherheitswerkzeug im Testlabor unter die Lupe genommen.

Absicherung des Systemverhaltens

Werden die Parameter des Systemverhaltens richtig konfiguriert, so blockt die Stormshield Endpoint Security nach Herstellerangaben ohne sonstige Konfigurationsmaßnahmen bereits 95 Prozent aller Angriffe ab. Im Test verwendeten wir eine Konfiguration, die uns vom Hersteller empfohlen worden war und die nur das Systemverhalten im Blick behielt. Es gab also keine Regeln in Bezug auf einzelne Anwendungen und ähnliches. Diese Konfiguration war demzufolge sehr schnell erstellt. Auf ihre Wirksamkeit gehen wir später noch genauer ein.

Ebenfalls im Bereich "Sicherheit" findet sich die so genannte Gerätesteuerung. Hier legen die Verantwortlichen fest, ob der Einsatz von Modems, Bluetooth-Komponenten, IrDA, LPT, Disketten, diversen USB-Devices und vielem mehr zulässig ist. Die Administratoren können an dieser Stelle bei Bedarf mit Gruppenrechten arbeiten, loggen, welche Datei wann auf welchen USB-Stick kopiert wurde und diese –falls erforderlich – automatisch verschlüsseln.

Die Anwendungsregeln kommen zum Einsatz, um Black-, White- und Gray-Lists zu erstellen. Sie legen für jede definierte Anwendung fest, was sie im Dateisystem, auf den Netzwerk-Sockets, beim Registry-Zugriff und so weiter darf. Die Regeln lassen sich vor der Inbetriebnahme testen und können auch jederzeit aktiviert und deaktiviert werden. Im Test ergaben sich dabei keine Probleme.

Die Erweiterungsregeln legen im Gegensatz dazu fest, welche Programme welche Dateitypen verwenden dürfen. Hier sorgen die Administratoren zum Beispiel dafür, dass Outlook nur PST-Files öffnen darf, was die Sicherheit in vielen Umgebungen deutlich erhöhen kann. Die Sicherheitspolicies sind folglich extrem leistungsfähig und bringen eine sehr große Zahl an Funktionen mit.

Über "Skripts" sind die IT-Verantwortlichen dazu in der Lage, anhand von Bedingungen genau festzulegen, was wann passieren soll. Die Skripts kommen beispielsweise zum Einsatz, um Aktionen zu definieren, die nur aktiviert werden, wenn Kondition eins "wahr" und

Kondition zwei "falsch" ist. So besteht beispielsweise die Option, einem Benutzer aus Gruppe eins andere Policies zuzuweisen, als einen User aus Gruppe zwei. Die genannten Skripts sind in vielen Umgebungen zweifellos von großem Nutzen. Wenn die Policies fertig definiert wurden, lassen sie sich über den Punkt "Umgebung" mit den Zielsystemen verknüpfen.

Das Testen des Agenten

Nachdem wir unsere Test-Policy so konfiguriert hatten, dass wir vor Ransomware und Malicious Code geschützt waren, gingen wir daran, den Agenten auf unsere Clients unter Windows 7, Windows 8.1 und Windows 10 auszubringen und unsere Konfiguration zu verteilen. Nachdem wir unsere Clients gesichert hatten, öffneten wir zunächst einmal das auf den Testsystemen installierte Mail-Programm Thunderbird. Wir haben uns zuvor einen Mail-Account angelegt, in den wir sämtlichen Spam gesammelt hatten, den wir über unsere regulären Mail-Adressen in den letzten Wochen erhalten hatten und der über einen Anhang verfügte oder zweifelhafte Links enthielt. Im Test öffneten wir zunächst einmal sämtliche Anhänge und führten die darin befindlichen Files aus. Gleichzeitig besuchten wir die potentiell gefährlichen Webseiten, auf die die Spam-Mails uns locken wollten. Dabei erhielten wir eine Vielzahl von Meldungen von der Stormshield-Lösung, die uns auf Heap-Überläufe, Versuche, gefährliche Aktionen durchzuführen und ähnliches aufmerksam machte. Anschließend versuchten wir, diverse aktuelle Viren und Ransomware-Programme direkt auf den Test-Clients zu starten. Auch hier meldete uns der Stormshield-Agent wieder, dass er etliche unerwünschte Aktionen blockiert habe. Zum Schluss surften wir noch eine Zeitlang mit den Test-Clients im Internet und konzentrierten uns dabei besonders auf Seiten mit schlechtem Leumund aus der Erotik-, Keyz- und Warez-Szene. Auf diesen Seiten klickten wir vor allem Advertisments an, über die den Besuchern der jeweiligen Webseiten möglicherweise Malware untergejubelt werden sollte. Unser System wurde bei all diesen Aktionen nicht beeinträchtigt, wie wir durch komplette Viren-Scans, die wir auf allen Clients nach dem Abschluss des Tests mit zwei unterschiedlichen Antivirus-Produkten (Avira und Windows Defender) durchführten, belegen konnten. Dabei stellte sich im Detail heraus, dass der Arbeitsspeicher und die Registry in keinem Fall kompromittiert wurden, die Antivirus-Lösungen fanden lediglich die infizierten Malware-Files auf der Festplatte.

Fazit

Im Test konnte uns die Stormshield Endpoint Security voll überzeugen. Der Agent ist extrem leistungsfähig und blockte alle Angriffsversuche unserer Malware-Produkte ab. Auch der Webzugriff wurde so abgesichert, dass es zu keinen Infektionen kommen konnte. Aufgrund der Vielzahl der verfügbaren Funktionen gilt das Produkt aber nicht als selbsterklärend. Administratoren, die damit arbeiten möchten, müssen schon ein wenig Zeit mitbringen, um sich mit der Dokumentation und dem Verwaltungsinterface vertraut zu machen. Dafür werden sie aber später im praktischen Einsatz mit einer Sicherheitskonfiguration belohnt, die exakt auf die Anforderungen ihrer Umgebung eingeht und die das Schutzniveau im Unternehmen deutlich erhöht.

Über den Autor: Dr. Götz Güttich ist Leiter des Institut zur Analyse von IT-Komponenten (IAIT) und verfügt über mehr als fünfzehn Jahre Branchenerfahrung als IT-Consultant und Fach- beziehungsweise Chefredakteur im IT-Umfeld. Aufgrund seiner langjährigen umfangreichen Testtätigkeit für führende deutsche Netzwerkmagazine beschränken sich seine Fähigkeiten nicht auf die Theorie des IT-Geschäfts.