IAITested

Institut zur Analyse von IT-Komponenten
Rotdornstr. 2

41532 Korschenbroich

Im Test: Stormshield Endpoint Security 7.212

Sichere Clients ohne Pattern-Updates

Autor: Dr. Götz Güttich

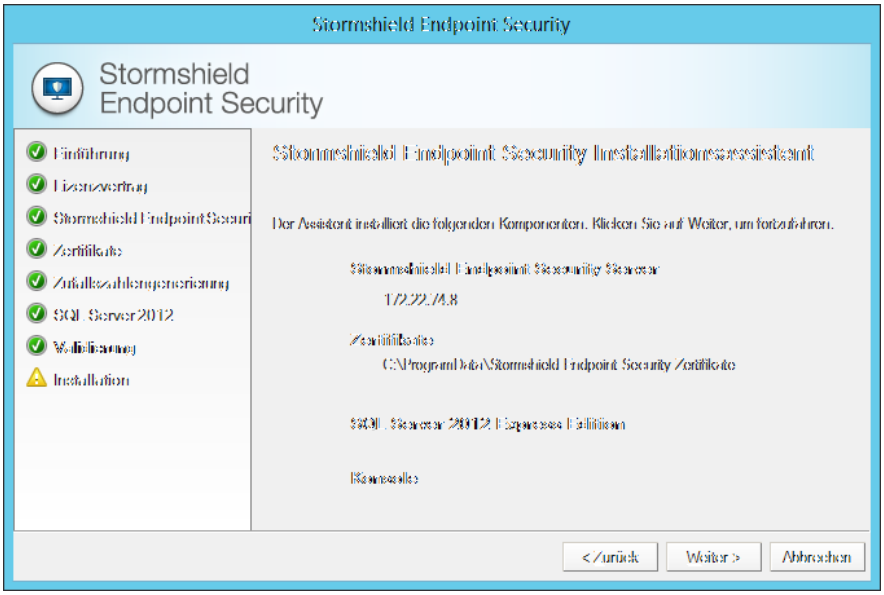
Mit der Endpoint Security 7.212 bietet Stormshield eine Sicherheitslösung für Windows-Systeme, die sämtliche auf den zu schützenden Rechnern stattfindenden Aktionen überwacht und potentiell gefährliche Aktivitäten unterbindet. Dabei verwendet das Produkt keine Pattern, um Viren, Würmer und Vergleichbares 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.

Die Angriffe auf IT-Umgebungen wurden in den letzten Jahren immer ausgefeilter gestaltet und besser an die jeweiligen Ziele angepasst. Auf diese Weise konnten Angreifer konventionelle Schutzsysteme mit stetig wachsendem Erfolg aushebeln. Mit der Endpoint Security 7.212 möchte Stormshield Schutz gegen einen Großteil dieser Attacken bieten. Das System verwendet eine proaktiv arbeitende, signaturlose Technologie, die sowohl gegen ausgefeilte Angriffe als auch unbekannte Angriffsmethoden schützt. Dabei ist der Schutz nicht nur gegen Attacken auf Schwachstellen des Betriebssystems, sondern auch gegen Angriffe auf Third-Party-Applikationen wie Java oder Flash wirksam. Darüber hinaus überwacht die Sicherheitslösung auch die Integrität des Systemspeichers. Die Erkennung der Schadprogramme erfolgt im Betrieb über Verhaltensanalysen (Behaviour Monitoring) und die Absicherung des Betriebssystems. Das System erkennt also keine Viren

anhand ihres Codes, sondern wehrt Angriffe gegen das Betriebssystem ab beziehungsweise blockt sie. So schützt es die Interprozesskommunikation im Speicher und verhindert, dass Malware durch Overflows an höhere Privilegien gelangt. Die Verwaltung des Security Tools läuft dabei über eine zentrale Management-Konsole ab, die dazu dient, Verhaltensregeln für die auf den Clients laufenden Agenten festzulegen und die Agenten während der täglichen Arbeit zu überwachen. Die Verhaltensregeln legen beispielsweise fest, welche Anwendungen laufen dürfen, welche nicht und welche eingeschränkt werden (Black-, White- und Gray-Listing). Darüber hinaus regeln sie auch, welche Dateitypen bestimmte Applikationen öffnen dürfen und vieles mehr. So lassen sich über die Policies unter anderem auch Benutzerprivilegien und Datenübertragungen genau steuern und der Einsatz von Peripheriegeräten wie USB-Sticks, Modems und ähnlichem erlauben oder untersagen. Ein Intrusion Prevention System und eine Firewall gehören ebenfalls zum Leistungsumfang der Endpoint Security, genau wie eine Honeypot-Protection. Das Stormshield-Produkt kann im Betrieb parallel zu klassischen Antivirus-Lösungen arbeiten, es stellt also eine zusätzliche Schutzebene für eine 0-Day Protection dar. Das ist auch erforderlich, da das Produkt zwar Angriffe erkennt und unterbindet, aber keine Malware entfernt. Auf Wunsch verschiebt die Endpoint Security infizierte Computer aber in eine Quarantäne, in der sie keinen Schaden mehr anrichten können.

Architektur

Die Stormshield Endpoint Security (SES) besteht aus vier unterschiedlichen Komponenten: dem Server, der Datenbank, der Verwaltungskonsole und dem Agenten. Der Server setzt für den Betrieb mindestens einen Dual-Core-Prozessor mit 2 GHz Taktfrequenz und 2 GByte RAM voraus. Die Festplatte sollte 3 GByte freien Speicherplatz haben und als Betriebssystem kann entweder Windows Server 2008 R2 oder Windows Server 2012 R2 zum Einsatz kommen. Der Agent darf auf keinen Fall auf dem gleichen System wie der Server eingespielt werden, da sich die beiden Komponenten sonst bei der Nutzung der Ports in die Quere kommen.



Der Installationsassistent der Stormshield Endpoint Security 7

Als Datenbank muss ein Microsoft SQL Server verwendet werden. Die Express-Version dieses Servers kommt mit der Setup-Routine und lässt sich während der Installation automatisch mit einspielen. Sie reicht für kleine und Testumgebungen völlig aus. Was die Hardware angeht, benötigt der Datenbankserver ebenfalls mindestens 2 GByte RAM und mindestens 10 MByte Speicherplatz für die Datenbank.

Die Verwaltungskonsole lässt sich auf jedem Rechner mit mindestens einem 2-GHz-Prozessor, 75 MByte Festplattenplatz und 512 MByte RAM einspielen. Als Betriebssysteme können dabei alle Windows Versionen seit Windows XP mit Service Pack 3 zum Einsatz kommen.

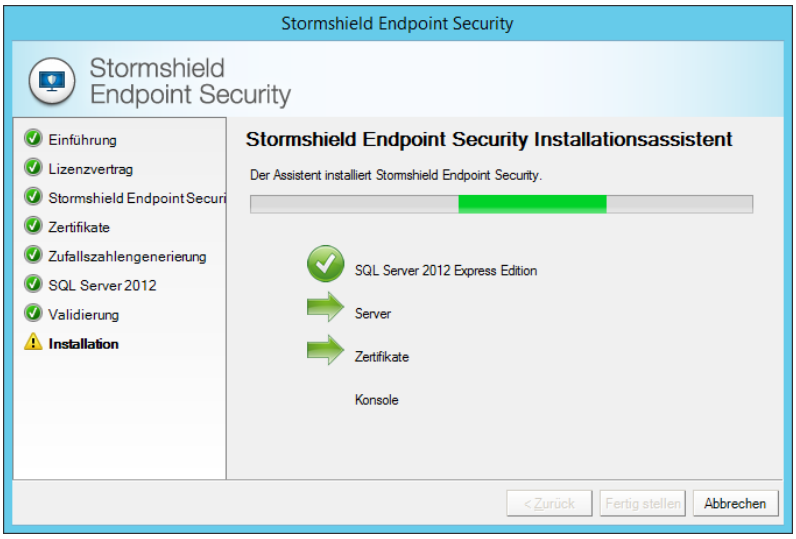
Der Agent benötigt schließlich ebenfalls eine 2-GHz-CPU und 512 MByte RAM, er kommt aber in der kleinsten Version ohne Antivirus mit 30 MByte Festplattenplatz aus. Die Hardwareanforderungen an das System sind folglich äußerst gering.

Der Test

Im Test spielten wir die Stormshield Endpoint Security (Server, Datenbank und Konsole) auf einem Windows System unter Windows Server 2012 R2 mit 8 GByte RAM, einer Quad-Core-CPU mit 2,6 GHz Taktfrequenz und 75 GByte freiem Festplattenplatz ein. Danach verteilten wir den Agenten auf die Clients im Netz, nahmen den Funktionsumfang der Management-Konsole unter die Lupe, erstellten Policies, um unser Netz abzusichern und gaben diese anschließend an unsere Agenten weiter. Zum Schluss griffen wir die Systeme mit Malware, Ransomware, Viren und ähnlichem an, um festzustellen, ob die Sicherheitslösung ihre Aufgabe zuverlässig versah.

Installation

Um die Stormshield Endpoint Security zu installieren, müssen die zuständigen Mitarbeiter insgesamt drei unterschiedliche Wizards abarbeiten. Da diese Wizards automatisch nacheinander gestartet werden, sollten in der Praxis dabei keine Probleme auftreten. Zunächst einmal geht es an das Entpacken der von der Herstellerwebseite heruntergeladenen Installationsdatei. Danach sind die zuständigen Mitarbeiter dazu in der Lage, das Setup aufzurufen. Anschließend müssen sie die Sprache auswählen, in der die Installation erfolgt. Hierfür stehen Deutsch, Englisch, Französisch, Spanisch und Portugiesisch zur Verfügung. Nach der Selektion der Sprache bietet der Wizard an, sich für einen bestimmten Installationstyp zu entscheiden. Die komplette Installation spielt alle Komponenten außer den Agenten auf einem Server ein. Alternativ gibt es auch die Option, nur den Server oder nur die Konsole zu installieren. Bei Bedarf lassen sich die einzuspielenden Komponenten auch frei auswählen. Im Test entschieden wir uns für die komplette Installation, woraufhin der eigentliche Setup-Assistent hochkam.



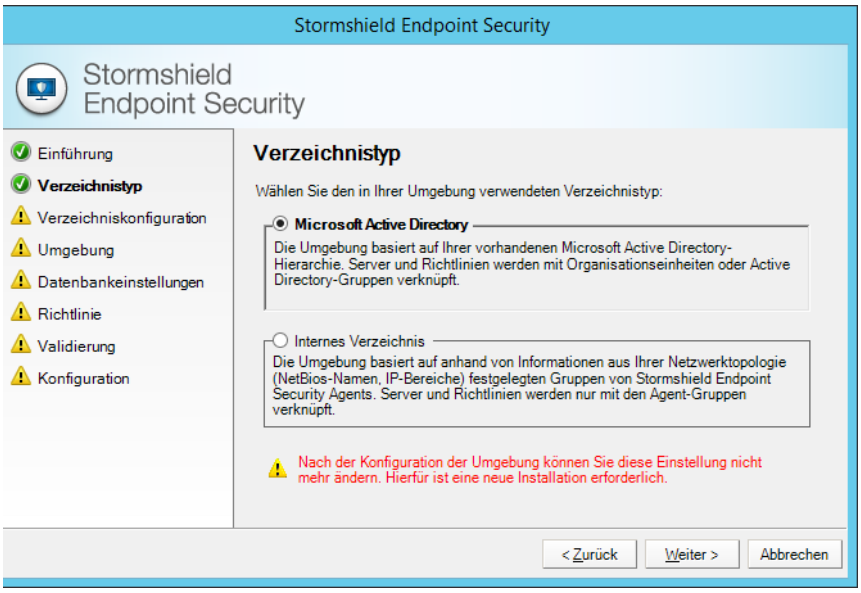
Das Setup der SQL Server Express Datenbank erfolgt auf Wunsch während der Installation automatisch

Dieser Assistent zeigt zunächst einmal eine Einführung und diverse Lizenzinformationen an. Danach möchte er wissen, welche IP-Adresse der Server hat und welche Ports für den Webdownload (über diesen können sich bei Bedarf später im Betrieb die Clients die Installationsdatei des Agenten vom Server laden), die Antiviruslösung und den Download der Agentenzertifikate zum Einsatz kommen sollen. Im Test beließen wir sämtliche Portangaben auf ihren Default-Werten, da in unserer Umgebung keine anderen Applikationen die entsprechenden Ports belegten.

Sobald das erledigt war, ging es daran, eine Passphrase für die Zertifikate einzugeben, Zufallszahlen mit Hilfe von Mausbewegungen zu erzeugen und die SQL-Server-Authentifizierung festzulegen (wir entschieden uns an dieser Stelle für die Windows Authentifizierung). Zum Schluss zeigte uns der Assistent eine Übersicht der durchzuführenden Schritte an und führte die Installation durch. Dabei wurde auch automatisch die SQL Server Express-Datenbank eingerichtet, die zum Lieferumfang gehört, da diese für unsere Testumgebung vollkommen ausreichte. Die Administratoren müssen während der Installation lediglich darauf achten, dass sie für jedes einzelne aufgerufene Setup-Programm (SQL-Server, Stormshield Server und Konsole) jeweils bestätigen, dass es auf dem Rechner ausgeführt werden darf, da die Installation sonst hängenbleibt.

Das Einrichten der Datenbank

Nach dem Abschluss des Installationswizards startet automatisch der Setup-Assistent für die Datenbank. Auch dieser präsentiert zunächst eine Einführung und möchte dann wissen, auf welche Weise sich der Super Admin einloggen soll. In unserem Fall war hier die Windows Authentifizierung die richtige Wahl. Der Name der Instanz, mit der die Verbindung hergestellt werden sollte ({IP-Adresse des Servers\SES}) war bereits ausgefüllt.



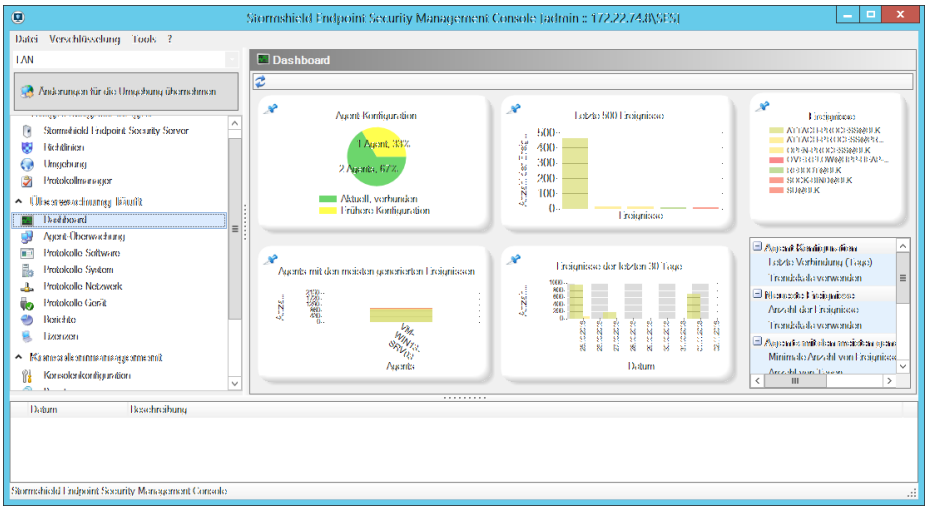
Neben dem Active Directory kann bei Bedarf auch ein internes Verzeichnis mit der Stormshield Endpoint Security zum Einsatz kommen

Im nächsten Schritt ging es daran, die Stormshield Endpoint Security Hauptdatenbank zu erstellen und die Zugangsdaten für diese Datenbank festzulegen. Anschließend fragte der Wizard die gleichen Informationen für die Protokoll- und Überwachungsdatenbank und die Schlüsseldatenbank ab. Bei der Schlüsseldatenbank entschieden wir uns – wie vom Assistenten angeboten – dazu, die selben Credentials wie bei der Protokolldatenbank zu verwenden. Zum Schluss fragt der Wizard noch, ob und wie eine automatische Datenbanksicherung erfolgen soll (in unserem Testszenario konnten wir diese Funktion nicht nutzen, da sie mit der Express-Version des Microsoft SQL-Servers nicht funktioniert) und zeigt dann eine Übersicht der durchzuführenden Schritte an. Danach läuft die Installation durch.

Die Konfiguration der Umgebung

Sobald der Datenbank-Assistent abgeschlossen ist, kommt automatisch der Wizard zum Konfigurieren der Umgebung hoch. Auch dieser präsentiert zunächst einmal eine Einführung und möchte dann wissen, ob als Verzeichnis ein Active Directory oder ein internes Verzeichnis zum Einsatz kommen soll. In unserer Umgebung entschieden wir uns an dieser Stelle für unser Active Directory.

Sobald wir das erledigt hatten, fragte uns der Assistent nach der Domäne oder dem Forest für die Konsolenumgebung und den dazugehörigen Zugangsdaten. Nachdem die Software die Verbindung erfolgreich getestet hatte, ging es daran, die Umgebung zu benennen, die Lizenzdatei auszuwählen und der Konfigurations-Policy einen Namen zu geben. Danach wollte der Assistent noch wissen, auf welchem SES-Server die Policy eingerichtet werden sollte und in welchem Verzeichnis die Zertifikatsdateien für die Konsole landen. Zusätzlich benötigt der Wizard an dieser Stelle auch noch die Passphrase für die genannten Zertifikate. Die letztgenannten Informationen sind in der Dialogmaske bereits ausgefüllt und lassen sich einfach übernehmen. Das gleiche gilt für die Datenbankeinstellungen, die anschließend an die Reihe kommen. Auch hier hat der Assistent die SQL-Server-Instanz bereits eingetragen, so dass die zuständigen Mitarbeiter sie in den meisten Fällen einfach übernehmen können.



Das Dashboard informiert über den Systemstatus und die aktuellen Ereignisse

Zum Schluss fragt der Wizard noch nach der zu implementierenden Richtlinie. An dieser Stelle stehen "Leer", "Standard" und "Erweitert" zur Auswahl. "Leer" bedeutet, dass überhaupt keine Regeln eingetragen werden. Diese Option eignet sich besonders für erfahrene Administratoren, die alle Settings im Betrieb selbst vornehmen möchten. "Standard" umfasst Sicherheitsregeln für das Basis System und den Netzwerkschutz und "Erweitert" sichert zusätzlich noch diverse Applikationsgruppen ab. Im Test entschieden wir uns zu diesem Zeitpunkt für die Standard-Policy. Danach präsentierte der Assistent wieder die übliche Zusammenfassung und führte anschließend die Konfiguration durch. Im Test kamen wir zu dem Ergebnis, dass die SES-Inbetriebnahme zwar verhältnismäßig viele Schritte erfordert und einige Zeit dauert, aber keinen Administratoren vor irgendwelche Schwierigkeiten stellen wird.

Die Verwaltungs-Konsole

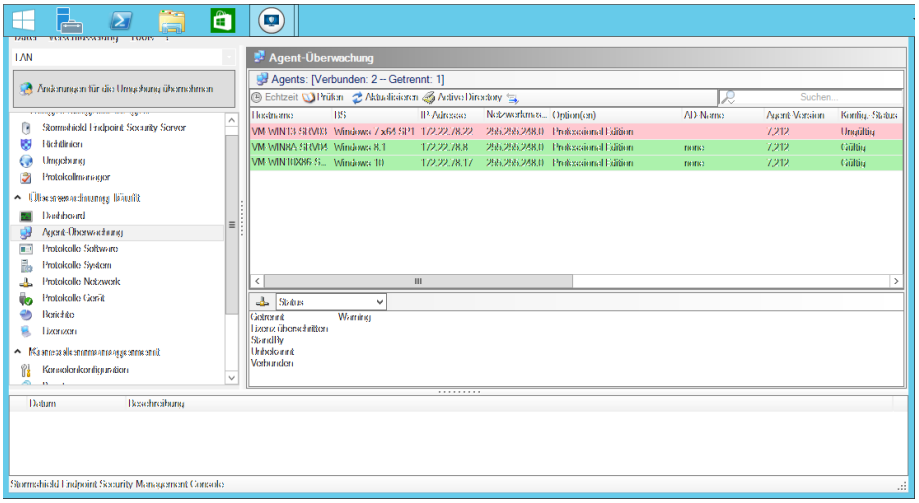
Nach dem Abschluss der Installation meldeten wir uns zunächst einmal bei der Management-Konsole des Systems an. Nach dem Login landet der Administrator in einer Dashboard-Übersicht, die ihm zeigt, welche Agenten verbunden sind und ob ihre Konfiguration aktuell ist. Darüber hinaus informiert das Dashboard über die 500 letzten Events, die Agenten, die die meisten Events generiert haben und die Events der letzten 30 Tage. Zu diesem Zeitpunkt verfügten wir noch über keine Agenten, deswegen konnte es auch keine Ereigniseinträge geben. Wir machten uns folglich daran, den Funktionsumfang der Software zu erforschen und eine an unsere Anforderungen angepasste Konfiguration zu erstellen, um diese dann zusammen mit dem Agenten an den ersten Testclient auszurollen.

Leistungsumfang des Konfigurationsinterfaces

Das Verwaltungswerkzeug arbeitet auf der linken Seite mit einer Baumstruktur, die in verschiedene Bereiche unterteilt wurde und die es den Administratoren ermöglicht, die einzelnen Funktionen der Software aufzurufen. Der erste Bereich, ist der so genannte Umgebungsmanager. Hier sind die zuständigen Mitarbeiter dazu in der Lage, die im Netz vorhandenen Stormshield Endpoint Security-Server zu verwalten und die Policies, die in ihren Netzen zum Einsatz kommen sollen, an ihre Anforderungen anzupassen.

Die Verwaltung der Regeln

Möchte ein IT-Mitarbeiter eine Regel erstellen, so kann er entweder eine bereits bestehende Policy duplizieren und anpassen oder eine komplett neue Regel einfügen. Alle Policies erhalten zunächst einmal einen Namen. Im Betrieb stehen für die Regeln mehrere unterschiedliche Typen zur Verfügung. Der erste nennt sich "Server Configuration". Eine Server Configuration-Policy kommt auf den Endpoint Security Servern zum Einsatz und legen die Serverrollen (Security-Server und Antivirus-Server) genauso fest wie die Syslog- und die SMTP-Konfiguration, das Log Monitoring und die Netzwerkeinstellungen mit der Zahl der maximal erlaubten gleichzeitigen Verbindungen.



Über die Agentenüberwachung erhalten die zuständigen Mitarbeiter Informationen zu den im Netz vorhandenen Agenten, den dazugehörigen Clients und dem aktuellen Verbindungsstatus

Die "Dynamic Agent Configuration" befasst sich im Gegensatz dazu mit den Agenten, die auf Workstations laufen. Diese lassen sich drei unterschiedlichen Schutzmodi betreiben: Im Standby-Modus bleibt der Agent passiv, im Warning-Modus schreibt er nur seine Erkenntnisse in die Log-Dateien und ergreift keine Schutzmaßnahmen. Dieser Modus ist während der Implementierung sinnvoll, da er den Administratoren dabei hilft, herauszufinden, welche Aktionen im Netz alltäglich sind und welche nicht. Der normale Modus kommt schließlich im Betrieb zum Einsatz, hier ergreift der Agent beim Auffinden von problematischen Aktionen Maßnahmen zum Schutz des Clients. Die dynamische Agentenkonfiguration
legt zudem die Sprache fest, mit der sich die Benutzerinterfaces der Agenten auf den Clients melden. Das gleiche gilt für die Benachrichtigungen und den "Temporären Webzugriff". Letzterer erlaubt es dem Anwender, unabhängig von der Firewall auf die Dienste HTTP und HTTPS zuzugreifen. Auf diese Weise ist es zum Beispiel in einem Hotel möglich, über den temporären Webzugriff das Captive Portal des Hotel-WLANs aufzurufen und die Internet-Verbindung herzustellen. Anschließend werden dann das VPN aktiviert und der temporäre Webzugriff abgeschaltet, um verschlüsselt weiter zu arbeiten. Es handelt sich beim temporären Webzugriff um ein sehr nützliches Feature.

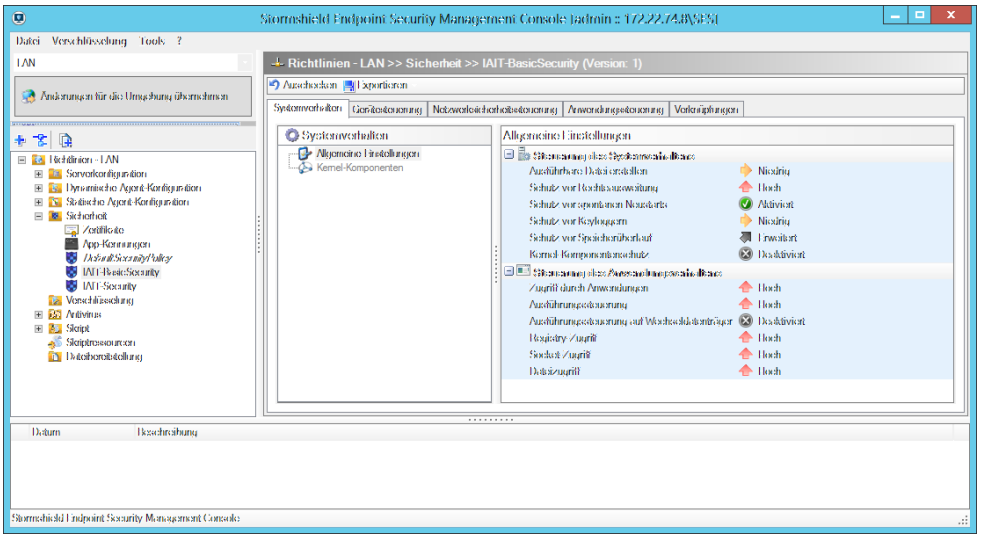
Die Antivirus-Settings gehören ebenfalls mit zur dynamischen Agent-Konfiguration. Stormshield liefert auf Wunsch als Antivirus-Lösung Aviras Enterprise Management Server mit, es lassen sich aber auch die Produkte anderer Hersteller, wie

beispielsweise F-Secure, McAfee, Symantec oder auch Trend Micro in das System einbinden.

Über die statische Agentenkonfiguration sind die IT-Verantwortlichen dazu in der Lage, Skripts auf den Clients auszuführen. Die Skripts können auf Wunsch bestimmte Aktionen bei Einsätzen außerhalb des Unternehmens ermöglichen. Da sie frei wählbar sind, lassen sie sich für praktisch alle Aktionen nutzen, typische Einsatzgebiete sind beispielsweise das temporäre Freigeben des Internetzugangs, das Deaktivieren der Firewall, das Anstoßen von Viren-Scans oder auch das Aktivieren des Loggings.

Absicherung des Systemverhaltens

Die Sicherheitspolicies, die sich jederzeit Ex- und Importieren lassen, stellen das Herzstück der Lösung dar. Der wichtigste Punkt in diesem Zusammenhang ist der Bereich "Systemverhalten". Hier konfigurieren die Administratoren, was die Sicherheitslösung während des Betriebs macht, wenn versucht wird, ausführbare Dateien zu erstellen, Rechte auszuweiten und spontane Neustarts durchzuführen. Außerdem bietet die Lösung an dieser Stelle einen Schutz vor Keyloggern, Speicherüberläufen sowie einen Kernel-Komponentenschutz.

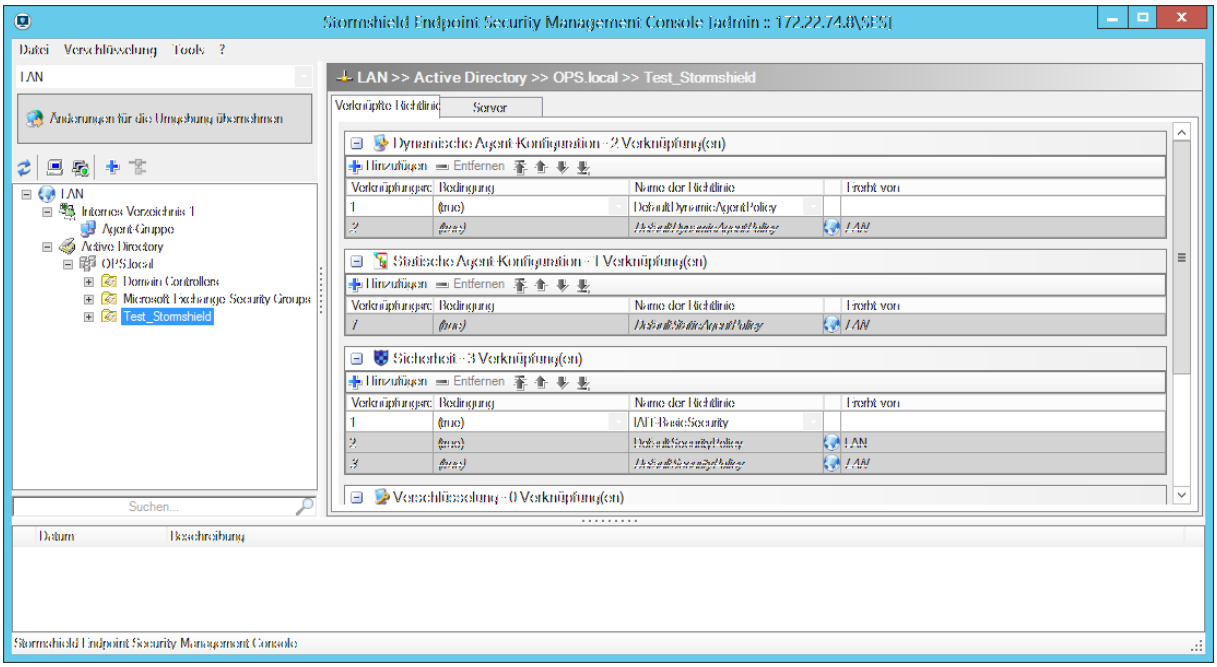


Eine Basic-Security-Policy wie diese schützt ohne weitere Konfiguration vor praktisch allen Angriffsversuchen

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.



Konfigurationen lassen sich über die Umgebungsseite bestimmten Systemen zuweisen

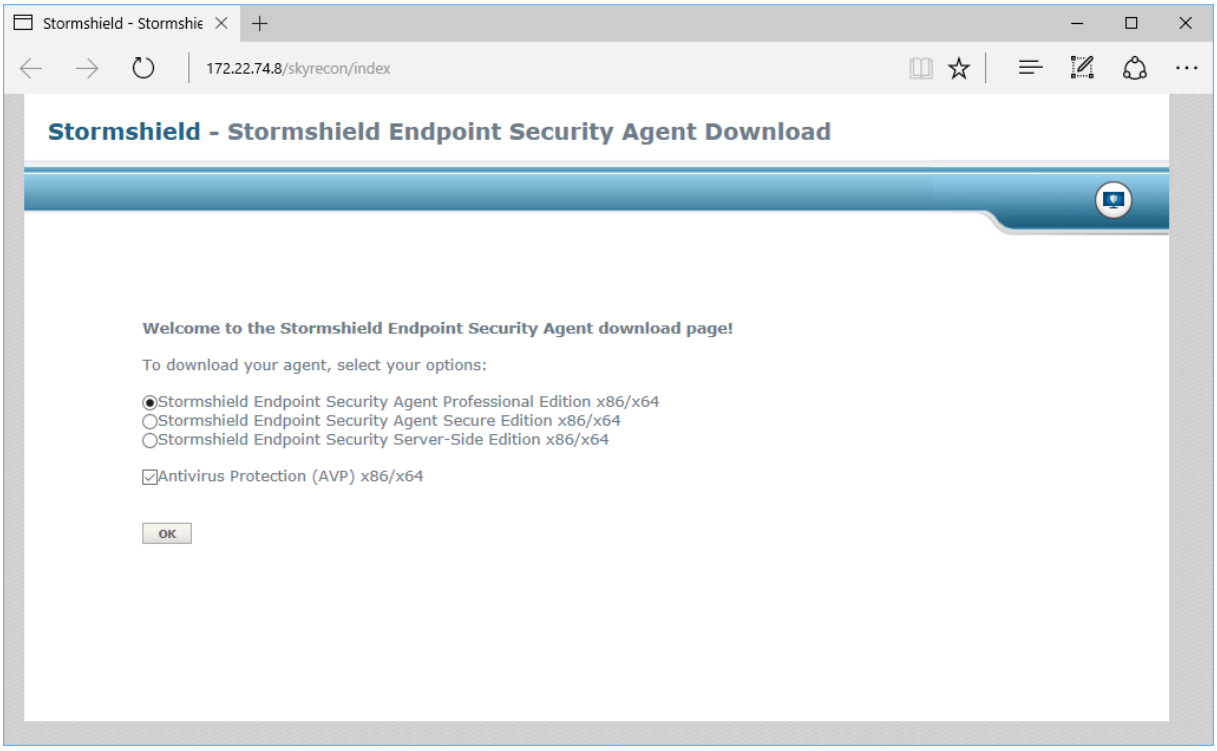
Punkte zur Konfiguration der Netzwerksicherheit und der Anwendungssteuerung schließen die Konfiguration der Sicherheitsrichtlinien ab. Die Netzwerksicherheit befasst sich mit der Steuerung der Netzwerkaktivitäten, wie dem Schutz vor Portscans, der TCP-Integritätsprüfung und vielem mehr. Außerdem kümmert sie sich um WLAN-Verschlüsselung und -Authentifizierung.

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. Umfangreiche Logging- und Protokoll-Funktionen sorgen gleichzeitig dafür, dass die zuständigen Mitarbeiter – etwa per E-Mail – jederzeit über die Aktivitäten in ihrem Netz auf dem Laufenden bleiben. Das Logging erfolgt bei Bedarf für jede einzelne Regel. Im Betrieb arbeitet das System die Anwendungsregeln genau wie eine Firewall von oben nach unten ab, es zählt also immer nur das erste Match. 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. Alternativ gibt es auch die Möglichkeit, eine bestimmte Aktion zu starten, wenn eine Datei ein bestimmtes Alter überschritten hat. Die durchzuführenden Aktionen lassen sich in diesem Zusammenhang beliebig definieren, das System kann sowohl einen Prozess starten oder ein weiteres Skript ausführen, als auch eine Datei löschen oder ähnliches. Die genannten Skripts sind in vielen Umgebungen zweifellos von großem Nutzen.



Die Webseite zum Download der Agenteninstallationsdatei über das Internet

Wenn die Policies fertig definiert wurden, lassen sie sich über den Punkt "Umgebung" mit den Zielsystemen verknüpfen. Auch hier kann es wieder Konditionen geben, wie "wenn verbunden", "wenn nicht verbunden", "immer" und ähnliches. Der Protokollmanager schließt die Umgebungsverwaltung ab. Er kommt zum Einsatz, um Log-Nachrichten anzupassen und die Benachrichtigungen des Agenten zu konfigurieren. Was die Logs angeht, so unterscheidet das System zwischen Software-, System-, Netzwerk- und Geräteprotokollen.

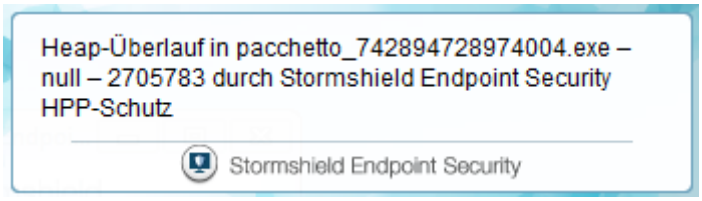
Während des täglichen Betriebs ist es übrigens möglich, aus einem Protokolleintrag heraus direkt zu der Regel zu wechseln, die den Eintrag ausgelöst hat. Das kann bei der Fehlersuche sehr hilfreich sein.

Das Überwachen der Endpoint Security-Lösung

Der zweite Hauptpunkt des Management-Werkzeugs nach dem Umgebungsmanager befasst sich mit dem Monitoring. Hier findet sich das bereits erwähnte Dashboard, außerdem bietet das System an dieser Stelle auch eine Agent Monitoring-Seite an, die alle im Netz vorhandenen Agenten in einer Liste anzeigt. Diese Liste umfasst Informationen über den Host, das ausgeführte Betriebssystem, die IP-Adresse, die Netzwerkmaske, die Agentenversion, die aktive Policy und vieles mehr. Abgesehen davon bietet die Monitoring-Übersicht auch noch diverse Option zum Einsehen der

Software-, System-, Netzwerk- und Device-Logs. Dabei stehen den zuständigen Mitarbeitern immer leistungsfähige Filterfunktionen zur Verfügung, die ihnen dabei helfen, die Informationen ausfindig zu machen, die sie gerade benötigen. Eine Reportfunktion, die Berichte über Server und Agenten, die Computerintegrität, die Systemsicherheit, den Agentenstatus und vieles mehr anbietet, schließt gleichzeitig mit einer Lizenz-Übersicht den Leistungsumfang des Monitorings ab.

Der dritte Punkt des Verwaltungswerkzeugs nennt sich "Console Manager". Hier konfigurieren die Administratoren alles, was mit den Einstellungen zur Konsole selbst zu tun hat, wie beispielsweise Sprache, Layout, die Konsolenzertifikatsdatei und ähnliches. Über den "User Manager" lassen sich Benutzerkonten mit unterschiedlichen Rechten anlegen, die auf verschiedene Bereiche der Verwaltungslösung Zugriff erhalten. Es besteht also die Option, mehrere unterschiedliche Administratoren mit verschiedenen Aufgabengebieten im System abzubilden. Ein Event Viewer mit Suchfunktion und Filter gehört ebenfalls zum Console Manager. Er zeigt sämtliche vom Administratoren der Managementkonsole durchgeführten Aktionen.



Der Agent meldet auf einem Client einen Heap-Überlauf

Der letzte Punkt "Device Enrollment" dient zur Geräteregistrierung. Damit lassen sich beispielsweise Gefahren durch das Anstecken gefundener USB-Sticks unterbinden. Wenn die Administratoren an dieser Stelle die im Unternehmen vorhandenen und als sicher befundenen USB-Sticks erfassen und nur den Zugriff auf diese bekannten Speichermedien erlauben, so verhindern sie damit, dass die Rechner im Netz auf infizierte USB-Sticks zugreifen und verschließen damit diese häufig genutzte Infektionsmethode. Die Geräteregistrierung ist im Betrieb sogar dazu in der Lage, einzelnen Devices den "Trusted"-Status wieder zu entziehen. Steckt ein User zum Beispiel einen vertrauenswürdigen USB-Stick an einen nicht vertrauenswürdigen Rechner – etwa bei sich zu Hause – an, so verliert der Stick seine Einstufung als vertrauenswürdiges Gerät, wenn sich der Inhalt des Sticks ändert und kann erst dann wieder im Unternehmen zum Einsatz kommen, wenn die IT-Abteilung ihn vorher überprüft und anschließend wieder freigibt.

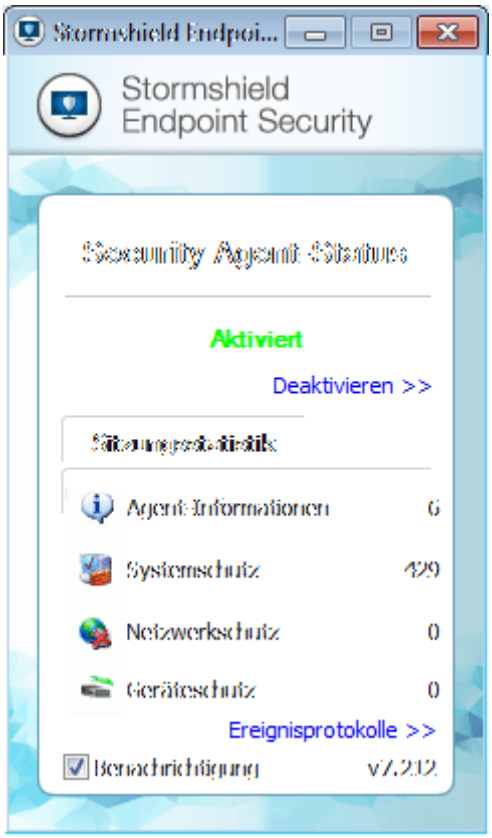
Das Ausbringen des Agenten

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. Das Ausbringen des Agenten ist über drei verschiedene Wege möglich. Der erste besteht darin, den dafür vorgesehenen Assistenten, der zum Lieferumfang der Stormshield Endpoint Security gehört, auszuführen und dabei die gewünschten Zielsysteme anzugeben. Der zweite Weg nutzt MSI-Dateien, die das Sicherheitsprodukt nach der Installation im Verzeichnis "\Programme (x86)\Stormshield\Stormshield Security Server\Files" bereitstellt. Im Test verwendeten wir unsere Active Directory-Umgebung, um diese im Netz zu verteilen. Die MSI-Files

enthalten bereits die Serveradresse, zu der sie ihre Verbindung aufbauen sollen, sie eignen sich also immer nur für die aktuelle Umgebung. Nach der Verteilung startet die Agenteninstallation auf den Clients, der Agent kommt hoch und baut eine Verbindung zum Server auf. Anschließend lädt er automatisch die ihm zugewiesene Konfiguration vom Server und aktiviert sie. Danach ist das System auch Client-seitig einsatzbereit. Der dritte Weg zum Verteilen das Agenten läuft schließlich über das oben erwähnte Web-Portal, das Download-Links für die Installationsdateien des Agenten bereitstellt. Diese Option bietet sich an, wenn Clients die Agenten über das Internet laden müssen.

Die Stormshield-Lösung in der Praxis

Nachdem wir unsere Clients gesichert hatten, öffneten wir zunächst einmal ein 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.



So sieht die Statusseite des Agenten aus, wenn man sie auf dem Client aufruft

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.