STORMSHIELD

ULTIMATIVER SCHUTZ GEGEN UNBEKANNTE UND KOMPLEXE ANGRIFFE

ENDPOINT SECURITY

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY

Stormshield

Endpoint Security

DIESE SICHERHEITSLÖSUNG BLOCKIERT BISHER UNBEKANNTE ODER BESONDERS RAFFINIERTE ANGRIFFE, DIE VON IHREN HERKÖMMLICHEN SICHERHEITSMECHANISMEN NICHT ERKANNT WERDEN.

ENDPOINT SECURITY

Cyber-Angriffe werden immer zielgerichteter und ausgefeilter programmiert, um herkömmliche Schutzsysteme zu umgehen. Dabei werden hochentwickelte Infektionstechniken eingesetzt, beispielsweise durch Exploits, die auf unbekannte Sicherheitslücken setzen. Zur Verschleierung vor dem Betriebssystem werden hochintelligente Mechanismen verwendet. Die Bedrohungen sind nicht auf Netzwerke beschränkt, sondern erstrecken sich jetzt auch auf sensible oder industrielle Umgebungen, bei denen die Auswirkungen deutlich größer sind (Risiko physischer Angriffe, Unterbrechung von Produktionsanlagen usw.).

Einzigartiger Schutz

Stormshield Endpoint Security basiert auf einer einzigartigen Analyse der Interaktionen zwischen den Prozessen und dem System an einem Arbeitsplatz oder Server. **Das System bietet daher einen umfassenden Schutz gegen komplexe und umfassende** Angriffe und ergänzt damit Ihre herkömmlichen Schutzprogramme.

Auf mehreren Ebenen werden effiziente Verteidigungsmechanismen gegen Angriffe auf das System eingerichtet, die seine Integrität garantieren: Blockierung der Exploits von Schwachstellen (beispielsweise die Provokation eines Fehlverhaltens im Arbeitsspeicher, um bösartigen Code auszuführen), Erkennung der Installation eines Virus auf dem Endgerät, insbesondere Ransomware, Erkennung von bösartigen Verhalten usw.

Proaktive und Offline-Technologie

Stormshield Endpoint Security ist das Ergebnis von jahrelanger Forschung und Entwicklung. Das System ermöglicht die Erkennung von unbekannten und ausgereiften Angriffen ohne Aktualisierung des Produkts oder Verbindung mit einem externen System. Die Lösung stellt damit eine hervorragende Antwort auf die Schutzbedürfnisse von Offline-Umgebungen dar und ist für den Schutz von veralteten Umgebungen (beispielsweise Windows XP, für das keine Sicherheitspatches mehr ausgeliefert werden) geeignet.

Diese Technologie wird weltweit von zahlreichen Kunden eingesetzt, die sensible Infrastrukturen (Militär, kritische Infrastrukturen usw.) schützen müssen oder bei denen strenge betriebliche und rechtliche Vorgaben vorherrschen (Industrie, Energie, POS usw.).

Vollständiges Angebot für die Kontrolle von Arbeitsplatzrechnern

Stormshield Endpoint Security ermöglicht die Kontrolle verschiedener Verhaltensweisen des Arbeitsplatzrechners und die Definition jener Verhaltensweisen, die zulässig oder unzulässig sind.

Unsere Lösung ist eine wesentliche Voraussetzung für wirksame Maßnahmen gegen Datenlecks und Datenverluste, gegen Infektionen von außen und Fehlfunktionen durch absichtliche Fehlverwendung der IT-Systeme des Unternehmens.

Diese Kontrolle des Arbeitsplatzrechners umfasst auch die Nutzung von externen Kommunikationsgeräten (WLAN, Bluetooth) sowie von Peripheriegeräten (USB-Datenträger) und stellt die Konformität der Workstations (neueste Windows-Patches, virusfreies Gerät, usw.) sicher.

SCHUTZ IM KONTEXT

Stormshield Endpoint Security kann je nach seiner Umgebung automatisch reagieren. Diese einzigartige Anpassungsfähigkeit ermöglicht eine sofortige Anwendung von Maßnahmen bei Veränderungen des Kontextes, egal ob der Arbeitsplatzrechner mit dem Internet verbunden ist oder nicht.

Als Schutz gegen Sicherheitslecks ermöglicht Stormshield Endpoint Security beispielsweise:

- Versetzen eines Arbeitsplatzes in Quarantäne, wenn die Sicherheitskorrekturprogramme nicht angewendet wurden
- Konfiguration strengerer Sicherheitsrichtlinien, wenn sich der Arbeitsplatz außerhalb der Infrastruktur befindet

AUTONOMER SCHUTZ

Stormshield Endpoint Security ist ein autonomer Schutz, der für seine Aktualisierung keine Verbindung mit dem Internet benötigt. Seine proaktiven und generischen Sicherheitsmechanismen ermöglichen das Blockieren der Zero-Day-Bedrohungen, ohne eine Aktualisierung oder neue Version der Software einspielen zu müssen.

BEGRENZTE BELASTUNG DES SYSTEMS

Der Vorteil einer proaktiven Technologie besteht darin, dass eine begrenzte Belastung des Systems erfolgt. Die herkömmlichen Schutzsysteme erfordern, dass jeder Teil der Prozesse mit Signaturdatenbanken verglichen wird, die Millionen von Einträgen enthalten. Das beeinträchtigt die Systemleistung. Die Technologie von Stormshield Endpoint Security überwacht die sensiblen Zonen des Betriebssystems, um darin anomale Verhaltensweisen zu entdecken.

ULTIMATIVE LÖSUNG

Unser Schutz umfasst eine Gruppe von Sicherheitsbarrieren (Firewall, Netzwerkschutz, Anwendungssteuerung), die den durchgehenden Schutz der Server, der Arbeitsplatzrechner oder der Terminals ohne Softwareaktualisierung garantiert. Stormshield Endpoint Security ist eine Ergänzung der herkömmlichen Schutzsysteme (Antivirus), womit eine zusätzliche Schutzschicht eingezogen wird.

VOLLSTÄNDIGE INTEGRATION

Die Sicherheitsrichtlinien können mithilfe verschiedener Methoden an Benutzergruppen angepasst werden: IP-Adresse, MAC-Adresse, Name der Geräte, aber auch Heranziehung des Active Directory der Organisation, um Zeit und Kosten für die Administration zu verringern. Das Produkt kann in die marktgängigen SIEM-Produkte integriert werden, damit Sie von der Korrelation von Ereignissen mit anderen Sicherheitslösungen profitieren.

TRANSPARENTER SCHUTZ

Die Lösung ermöglicht den Schutz in Echtzeit ohne Beeinträchtigung der Leistung am Arbeitsplatz. Stormshield Endpoint Security verständigt den Benutzer bei einem Angriff und leitet die Information über die zentrale Konsole sofort an den Administrator weiter.

GRANULARITÄT DER KONFIGURATION

Das Produkt bietet umfassende Flexibilität der Konfiguration im Bereich der Sicherheitsrichtlinien zur Anpassung an die Besonderheiten von Unternehmen. Der Schutz wird daher so nah wie möglich an den Bedarf der Unternehmen angepasst.

SCHUTZ IM MOBILEN UMFELD

Mobile Arbeitsplätze sind oft völlig ohne Schutz und Kontrolle, wenn sie sich nicht im Unternehmen befinden. Sie verfügen nicht über die verschiedenen Schutzbarrieren (Firewall, Netzwerkschutz usw.). Stormshield Endpoint Security sorgt für die Sicherheit von mobilen Arbeitsplätzen innerhalb oder außerhalb der eigenen Infrastruktur.

REDUKTION DER BETRIEBSKOSTEN

Unser proaktiver Schutz ermöglicht die drastische Reduktion der Kosten für die Anwendung von Sicherheitskorrekturen: Mit unserem Produkt, das proaktiv (Zero-Day) gegen die Ausnutzung von Schwachstellen schützt, bleibt der Zustand Ihrer Sicherheit erhalten.

Zero-Day-Schutz gegen unbekannte Bedrohungen

Schutz gegen die Ausnutzung von Schwachstellen im Betriebssystem, Schutz gegen die Ausnutzung von Schwachstellen in Drittanwendungen, Kontrolle der Integrität des Systemarbeitsspeichers, Schutz gegen Virenstämme, die im Arbeitsspeicher arbeiten (Fileless Malware)

Schutz von Arbeitsplatz und Server

Erkennung von böswilliger Software durch Verhaltensanalyse, Hardening des Betriebssystems, Anwendungskontrolle (durch Positivliste und schwarze Liste), Schutz gegen Berechtigungserweiterungen und Identitätsdiebstahl, Granulare Kontrolle der Benutzerrechte, Granulare Kontrolle und Auslesen von sensiblen Daten

Schutz gegen Eindringlinge

Firewall Erkennung von Eindringversuchen im Netzwerk

Kontrolle des Netzwerkzugriffs

Erstellen von kontextabhängigen Richtlinien auf der Basis von Benutzern, Maschinen, Verbindungen und der Konformität der Maschine, Überprüfung des Zustands und der Konformität der Richtlinien unabhängig vom Standort des Arbeitsplatzes, Vollständig automatisierte Säuberung

Anpassbarer Schutz

Dynamische Anpassung der Verbindungsrechte der Benutzer nach Ort oder Kontext, Positivliste der WLAN-Zugriffspunkte Ihres Unternehmens, Erzwingung der WPA/WPA2-Sicherheitsnormen, Verpflichtung zur Verwendung eines VPN bei öffentlichen Zugriffspunkten, Kontrolle der Nutzung des HSDPA/3G-Modems

Kontrolle der Peripheriegeräte

Autorisierung oder Sperre von Peripheriegeräten nach Typ oder Seriennummer, Blockierung oder Einschränkung diverser Nutzungsvorgänge des Peripheriegeräts, Verschlüsselung von tragbaren Peripheriegeräten, Schutz gegen Infektionen, Sperre oder granulare Kontrolle der Peripheriegeräte: USB, CD/DVD/BR-Brenner, Netzwerkkarten, serielle/parallele Schnittstelle, Firewire usw., Beurteilung (geeignet oder nicht) und Prüfung der Dateiübertragungen

Technische Daten

SOFTWAREKOMPONENTEN

Agent
Server
Verwaltungskonsole

EMPFOHLENE SYSTEMVORAUSSETZUNGEN

FÜR DEN AGENTEN

Pentium IV 3 Ghz

Arbeitsspeicher
512 MB (Minimum) / 1 GB (empfohlen)

Festplattenspeicher
250 MB (90 MB mit der Agentensoftware)

Betriebssysteme
Windows XP SP3 (32 Bit)
Windows 7 SP1 (32 und 64 Bit)
Windows 8.1 Update 1 (32 und 64 Bit)
Windows 10 (32 und 64 Bit)
Windows Server 2008 SP2 (32 Bit)
Windows Server 2008 R2 (64 Bit)
Windows Server 2012 R2 (64 Bit)

FÜR DEN ADMINISTRATIONSSERVER

Mindestens 1 GHz getakteter Prozessor

Arbeitsspeicher
Mindestens 1 GB

Betriebssysteme
Windows Server 2008 SP2 (32 Bit und 64 Bit)
Windows Server 2012 R2 (64 Bit)

STORMSHIELD

WWW.STORMSHIELD.EU

Contact
dach@stormshield.eu