STORMSHIELD

FIREWALL

Funktionsumfang

IT-SICHERHEIT

Um sich weiter zu entwickeln und wettbewerbsfähig zu bleiben, ist es für heutige Unternehmen an der Tagesordnung, in immer größerem Umfang und immer direkter mit Kunden und Partnern zu kommunizieren und gar einen Teil ihrer IT-Systeme zugänglich zu machen.

Parallel dazu nimmt die Komplexität der Unternehmensnetze stetig zu: W-LAN-Verbindungen innerhalb lokaler Netzwerke, immer feinere Rechte- und Benutzersegmentierung sowie Konformitätsanforderungen (ISO270X, PCI-DSS,..).

Vor diesem Hintergrund stellen sich besondere Anforderungen an die IT-Sicherheit, beispielsweise die Einschränkung des eingehenden Netzwerkverkehrs und die Verwendung von leistungsfähigen Lösungen, die eine transparente und exakte Filterung der Benutzeridentitäten ermöglichen.

FIREWALL NEXT-GENERATION

Diese Segmentierung sowie die Kontrolle der Benutzerzugriffe auf die verschiedenen Ressourcen im Netzwerk schützen das Unternehmen vor Angriffen von außen. Darüber hinaus helfen diese Techniken, die interne Verbreitung von Viren in den verschiedenen Diensten des Unternehmens zu verhindern.

Wenn Ihr Unternehmen außerdem zur Einhaltung der Standards nach PCI-DSS verpflichtet ist, ist die Überwachung bestimmter Teile des Netzwerks unumgänglich. Dies setzt in der Regel die Installation einer Firewall voraus.

Wie in Studien herausgefunden wurde, finden Bedrohungen der IT-Sicherheit zum größten Teil im eigenen Unternehmensnetzwerk statt. Wenn Sie Ihr Netzwerk segmentieren, haben Sie mithilfe der Stormshield Network Security-Anwendung die Möglichkeit, den Verkehr sowie die berechtigten Benutzer zwischen den geschützten Bereichen zu definieren.

Zur Überprüfung des autorisierten Verkehrs und zur Erhöhung der Anwendungssicherheit kommen im integrierten Intrusion Prevention-System von Stormshield Network Security Verfahren wie Protokollanalyse, Anwendungsfilter oder Virenprüfung zum Einsatz. In der Anwendung Stormshield Network Security können Sie individuelle Sicherheitsrichtlinien definieren und so den Schutz der Netzwerkressourcen erhöhen, die für alle Benutzer zugänglich sind.

FILTERN VON WINDOWS-DIENSTEN

Mithilfe der Filterfunktionen der Windows-Dienste können Sie das Benutzerverhalten innerhalb Ihres Netzwerks detailliert verwalten (Speichern und Wiederherstellen von Active Directory, IIS-Dienste, Microsoft Messenger,…).

Durch die Überprüfung des Windows DCE-RPC-Protokolls können die zugänglichen Dienste identifiziert und entsprechend angepasste Filterregeln angewendet werden. Damit schützen Sie Ihre Infrastruktur sowohl gegen Malware als auch gegen Techniken zur Sicherheitsumgehung, die mögliche Schwachstellen dieser Dienste ausnutzen.

IPV6

Das IPv6-Protokoll ist in den Filterfunktionen der Stormshield Network Security-Anwendungen implementiert. Damit eignet sich Ihre Sicherheitslösung für einen transparenten Über-

gang zu den Netzwerken der neuen Generation.

FIREWALL-ANWENDUNG

Die Bedrohungen auf Unternehmensnetzwerke werden immer vielfältiger und zahlreicher, und gewöhnliche Firewalls reichen als Schutzmaßnahme nicht mehr aus. Es ist heute unumgänglich, die Netzwerke entsprechend den neuesten IT-Sicherheitstechniken anzupassen und zu modernisieren. Dabei reicht es nicht aus, nur die Netzwerkschicht zu schützen.

Neue Systeme reagieren nicht nur auf Bedrohungen des Netzwerks an sich, sondern auch auf Bedrohungen von Anwendungen und Diensten. Vielmehr geht es darum, Anwendungen, Benutzer sowie Übertragungsinhalte zu überwachen und einzuschränken. Herkömmliche Firewalls sind nicht mehr in der Lage, Bedrohungen wie die Verwendung nicht-standardmäßiger Ports oder verschlüsselte Angriffe abzuwenden.

Vorteile:

- Umfassender Schutz vor Sicherheitslücken in Anwendungen
- Fokus auf gesamtem Netzwerk
- Leistungsfähige, Port-unabhängige Filter

Die multifunktionalen Stormshield Network Security-Firewalls bieten mehrere proaktive Sicherheitsmodule. Diese lassen sich durch kontinuierliche Weiterentwicklung entsprechend den stetig wachsenden Anforderungen von Unternehmen skalieren. Das Intrusion Detection System (IPS) von Stormshield Network Security der auf IT-Sicherheit spezialisierten Hersteller Arkoon und Netasq ist das Produkt aus mehr als 10 Jahren Forschung und Erfahrungen in diesem Bereich und bietet als solches ein außergewöhnlich hohes Maß an Schutz.

Die in Stormshield Network Security enthaltene Firewall umfasst u. a. ein Echtzeit-Analysemodul. Stormshield Network Vulnerability Manager, ein Modul zur Verwaltung von Sicherheitsrisiken, ermöglicht die Kontrolle der Anwendungen, Dienste und sämtlicher Schwachstellen im Netzwerk. Das Modul bietet einen Überblick über das gesamte Netzwerk und ermöglicht so ein schnelles und effizientes Risikomanagement. Sie haben damit die volle Kontrolle über Ihre Infrastruktur.

Der integrierte Virenscanner untersucht auf Viren, Spyware sowie Phishing und bietet einen hochwirksamen Schutz gegen Schadsoftware. Der Virenscanner wird automatisch aktualisiert und ist damit stets auf dem neuesten Stand. Die Stormshield Network Security-Lösungen garantieren dauerhaft IT-Sicherheit auf höchstem Niveau.

BENUTZERZENTRIERTE IT-SICHERHEIT

Die Anwender werden immer mobiler und die Netzwerke immer komplexer. Es wird zunehmend schwieriger, die Netzwerksicherheit und den Zugriff auf Anwendungen nur auf Grundlage bekannter und bewährter Netzwerkarchitekturen zu verwalten. Der moderne Benutzer verfügt über verschiedenste Mittel, mit deren Hilfe der Zugriff auf Anwendungen möglich ist: Remote-Zugriff, portable PC, Tablets, Smartphones usw.

Daher ist es heutzutage notwendiger denn je, den Benutzer in den Fokus der IT-Sicherheitsmaßnahmen zu rücken. Moderne Sicherheitssysteme bewirken also ein Blockieren der Benutzer und nicht der Server bzw. Computer. Dafür ist es notwendig, auf die individuellen Bedürfnisse angepasste Sicherheitsregeln zu definieren.

Die multifunktionalen Stormshield-Firewalls ermöglichen die Definition von Sicherheitsregeln auf Grundlage der Benutzeridentität. Mit einem Computer als Gateway werden die Rechte für den Zugriff auf Ressourcen individuell anhand der Benutzeridentität verwaltet. Jedes neu an das Netzwerk angeschlossene Gerät wird automatisch mit den Sicherheitseinstellungen des jeweiligen Benutzers synchronisiert. Auf diese Weise ist es möglich, die Netzwerkressourcen schnell und effizient zu verwalten.

Sämtliche Produkte von Stormshield Network Security bieten die Möglichkeit zur modularen Definition von Sicherheitsrichtlinien. Auf diese Weise können Sie die ordnungsgemäße Nutzung der Netzwerkressourcen steuern. Weitere mögliche benutzerbasierte Funktionen sind Verbindungszeitfenster, Inhaltsfilter, VPN SSL sowie IPSec-Zugriff auf Remote-Ressourcen. Auf diese Weise kann die Anzahl der auf alle Ressourcen des Benutzers anwendbaren Regeln begrenzt werden, unabhängig davon, welche und wie viele Installationen bzw. Geräte zum Einsatz kommen.

Dank eines direkt beim Controler bzw. einem Domainrechner installierten SSO-Agent (Single-Sign-On; SSO) kann die Kontrolle der Benutzerzugriffe anhand Ihrer internen Verzeichnisse erfolgen (LDAP, Windows Active Directory) und vollständig transparent umgesetzt werden. Bei geöffneter Windows-Sitzung werden die Benutzer durch Stormshield Network Security automatisch authentifiziert. Dies ist auch dann der Fall, wenn die Verbindung über Mehrbenutzersysteme wie Citrix oder TSE erfolgt.

Die Stormshield Network Security-Anwendungen ermöglichen die simultane Anwendung unterschiedlicher Identifikationsmethoden, welche verschiedene Möglichkeiten zur Benutzeridentifizierung bieten (Zertifikate, Captive Portal zur Authentifizierung, transparente Windows-Authentifizierung, internes LDAP-Verzeichnis, Gastmodus…).

KONTROLLE VON MOBILEN GERÄTEN, ANFORDERUNGEN IM ZUSAMMENHANG MIT BYOD

Die zunehmende Nutzung von privaten mobilen Geräten wie Smartphones, Tablets oder Laptops am Arbeitsplatz sowie außerhalb des Unternehmens stellt IT-Sicherheitsbeauftragte vor immer größere Probleme. Kopfzerbrechen bereitet insbesondere die Frage, wie die Unternehmen mit der BYOD-Praxis (Bring Your Own Device; BYOD) Schritt halten und dabei den Schutz ihrer eigenen Infrastruktur gewährleisten können.

Vorteile:

- Benutzerzentrierte IT-Sicherheit
- Modulares Sicherheitskonzept
- Netzwerkänderungen ohne Auswirkungen auf vorhandene Regeln
- Keine Auswirkungen auf Benutzer dank transparenter Authentifizierung

Mit Stormshield Network Security ist es möglich, die an das IT-System angeschlossenen mobilen Geräte zu identifizieren und deren Nutzung zu überwachen. Zudem können Sie den Einsatz dieser Geräte autorisieren oder verbieten für bestimmte Zeiten, Benutzer oder Benutzergruppen odeer auch für den Zugriff auf einzelne Ressourcen. Ferner haben Sie die Möglichkeit, für bestimmte Anwendungsfälle erweiterte Sicherheitsprofile einzurichten.

Stormshield Network Security bietet sowohl für private als auch für Unternehmensgeräte eine in höchstem Maße flexible Benutzerauthentifizierung. Für die Überprüfung der Zugriffe von Geräten gleich welcher Art stehen alle bekannten Authentifizierungsmethoden zur Verfügung.

ÜBER STORMSHIELD

Arkoon und Netasq, 100%ige Töchter von Airbus Defence and Space CyberSecurity, vertreiben unter der Marke Stormshield innovative End-to-End-Sicherheitslösungen zum Schutz von Netzwerken (Stormshield Network Security), Arbeitsplatzgeräten (Stormshield Endpoint Security) sowie Daten (Stormshield Data Security).

STORMSHIELD

N°Cristal 09 69 32 96 29
APPEL NON SURTAXE

WWW.STORMSHIELD.EU

Netasq
Parc Scientifique Haute Borne - Parc Horizon, Bat 6, Avenue de l'Horizon 59650 Villeneuve d'Ascq