STORMSHIELD

STORMSHIELD NETWORK VULNERABILITY MANAGER

NEUEN BEDROHUNGEN EINEN SCHRITT VORAUS

OPTION

Vorteile für den Kunden

- Anwendungsinventar
- Schwachstellenermittlung in Echtzeit
- Empfehlungen zur Schwachstellenbeseitigung
- Anpassung an betriebliche Vorgaben
- Verfügbarkeit der IT-Umgebung und sensibler Bestände

Angesichts der modernen Angriffe auf Unternehmen jeder Größe sind traditionelle Schutzsysteme längst nicht mehr ausreichend. Eine effiziente und kontinuierliche Verwaltung von Schwachstellen ist unerlässlich.

Entscheiden Sie sich für ein einfaches und dabei leistungsfähiges Tool zur Erkennung von Sicherheitslücken, das sich nahtlos in Ihre vorhandene IT-Umgebung einfügt.

ENTWICKLUNG DER BEDROHUNGEN

Das explosionsartige Wachstum sozialer Netzwerke, die Verbreitung von Web-2.0-Inhalten durch Internetnutzer und der Einsatz von mobilen Endgeräten haben ganz neue Möglichkeiten für Internetkriminalität geschaffen. Bei der Entwicklung von schädlichen Inhalten mangelt es den Betrügern nicht an Einfallsreichtum, um an ihre Ziele zu gelangen.

Bösartige Codes sind für traditionelle Schutzsysteme immer seltener aufspürbar. Sie stützen sich auf Anwendungsschwachstellen beim Endnutzer, um immer mehr Geräte zu beschädigen.

ALLE SIND BETROFFEN

Internetkriminalität hat vor allem finanzielle Ziele (Lösegeld, Datendiebstahl und Weiterverkauf, Angriffe nach Auftrag) oder ist aktivistisch (politisch, ideologisch) motiviert. Die Entwicklung von Botnetzen, Rebound gegen ein anderes Unternehmen desselben IT-Ökosystems, kostengünstige Angriffe durch die Banalisierung von Internetpiraterie-Diensten – all das sind Bedrohungen, die jedes Unternehmen unabhängig von seiner Größe oder seiner Bekanntheit betreffen.

Täglich werden neue Websites attackiert, darunter selbst die von großen Unternehmen oder eigentlich "vertrauenswürdige" Websites, mit dem Ziel, schädliche Programmcodes einzuschleusen. Diese Codes nutzen die zahlreichen Schwachstellen in Webbrowsern und ihren Komponenten, wie Flash oder Java, um die Rechner von Besuchern zu infizieren. Mehr als 30% der webbasierten Angriffe machen sich Schwachstellen in Java-Plugins zunutze.

ÜBRIGENS

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).

WWW.STORMSHIELD.EU

Telefon
+33 9 69 32 96 29

ECHTZEITERKENNUNG

Der erste Schritt zum Schutz vor diesen modernen Angriffen ist die Erkennung und Behandlung der Schwachstellen, auf die diese Angriffe abzielen.

Die Zeit, die ein Angreifer zum Finden einer Sicherheitslücke benötigt, ist in den letzten Jahren enorm gesunken. Im Wettlauf gegen die Bedrohungen bietet eine geplante Analyse, wie sie von sogenannten "Aktiv-Schwachstellen-Scannern" durchgeführt wird, nicht die notwendige Reaktionsfähigkeit. Besser ist eine Lösung mit kontinuierlicher Schwachstellenanalyse in Echtzeit.

EIN TOOL FÜR TEAMS

Der Stormshield Network Vulnerability Manager ist nativ in den Angriffsschutz aller Stormshield Network Security-Anwendungen integriert. Seine einzigartige und patentierte Technologie gibt Ihnen in Echtzeit die Sicherheit, dass es in Ihren Beständen keine bekannten Sicherheitslücken gibt.

Basierend auf der Datenübertragung durch die Anwendung inventarisiert der Stormshield Network Vulnerability Manager die Betriebssysteme, die verwendeten Anwendungen sowie deren Sicherheitsrisiken. Diese Zuordnung liefert einen kontinuierlichen Überblick über Ihren IT-Bestand. Bei Erkennen einer Sicherheitsgefährdung in Ihrem Netzwerk wird umgehend eine Warnmeldung ausgegeben..

GESCHÄFTSKONTINUITÄT

Um den Bedürfnissen der Branche und der Nutzer gerecht zu werden, müssen Unternehmensnetzwerke immer funktionieren. Die Ermittlung von Sicherheitslücken erfolgt häufig durch sogenannte "aktive" Scans, die für jedes geprüfte Gerät mehrere hundert Verbindungen erzeugen. Diese Scans führen häufig zu Hardwareausfällen und/oder Netzwerkstörungen.

Dank seines Systems zur Erkennung von Sicherheitslücken direkt im Datenstrom ist der Stormshield Network Vulnerability Manager nicht intrusiv. Da die Schwachstellenerkennung auf der Verbindungsanalyse basiert, hat sie keine Auswirkungen auf die Verfügbarkeit von Servern oder sensiblen Geräten.

WEITERES VORGEHEN

Der Stormshield Network Vulnerability Manager bietet Ihnen eine Reihe von speziellen Berichten sowie ein Echtzeit-Dashboard, wodurch Sie die Kontrolle über Ihren IT-Bestand behalten.

So können Sie gefährdete Anwendungen, Betriebssysteme und Geräte leicht identifizieren. Ermittelte Schwachstellen werden nach Schadhaftigkeitsgrad und Exploit-Form (lokal oder remote) klassifiziert.

Die angebotenen Berichte schlagen intuitiv angebrachte Korrekturmaßnahmen vor. Wenn es für eine Schwachstelle keine Korrektur gibt, kann leicht eine Filterregel erstellt werden, um das Risiko zu senken, da sie aus der gleichen GUI heraus angelegt wird. Diese Unterstützung bei der Beseitigung von Schwachstellen bringt eine erhebliche Zeitersparnis bei der Verwaltung Ihrer IT-Umgebung mit sich.

Mit dem Stormshield Network Vulnerability Manager können Sie besser auf interne Anforderungen hinsichtlich der Konformität Ihrer IT-Umgebung reagieren. Sie können Audits vorgreifen und auf diese Weise den Mehrwert Ihrer Maßnahmen unter Beweis stellen.

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