SDoT
Malware Protection Service

In Kürze verfügbar!

Sichere Malware-Prüfung mit multiplen Scan-Engines

Grundlagen

Informationsmanagement und operative Datenverarbeitung sind wichtige Aufgaben von militärischen und behördlichen Einsatzkräften zur Erfüllung ihres Auftrages. Die jeweiligen Bereiche sind auf eine verzugslose Verfügbarkeit von relevanten Informationen aus vielfältigen Quellen angewiesen. Dies gilt insbesondere auch für die Anbindung von nicht-vertrauenswürdigen Datenquellen, beispielsweise dem Internet.
Bisher werden Daten, die in geschlossene IT-Netze eingebracht werden sollen, manuell oder automatisch auf Schadcode geprüft. Bei einer großen Anzahl an Dateien ist eine manuelle Prüfung nicht mehr praktikabel. Herkömmliche automatische Systeme haben jedoch Einschränkungen bezüglich der Tiefe der Prüfung und der Selbstsicherung.
Daher besteht die Anforderung, eine automatisierte, technische Lösung zu finden, welche eine sichere Prüfung ermöglicht und eine ausreichende Härtung und Selbstsicherung aufweist.

Produkt

Das Produkt SDoT Malware Protection Service (MPS) bietet hierfür eine passende Lösung. Es wird in die Eingangskontrolle der Daten integriert und wickelt die Virenprüfung für alle erlaubten Dateiformate ab.
Die Daten werden mithilfe von mehreren, voneinander unabhängigen Antivirenscannern (AV-Engines) untersucht. Dies erlaubt eine bessere Erkennung des Schadcodes. Der Befall der Daten wird zuverlässig entdeckt und falsch-positive Befunde vermieden. Die Ergebnisse der Prüfung werden in einem maschinenlesbaren Format erfasst und erlauben eine vollständige Automatisierung des Dateieinganges. Die höhere Bedrohungslage wird durch eine sichere Ablaufplattform und entsprechende Selbstschutzmechanismen beantwortet. Durch diese Eigenschaften wird die Kontaminierung innerhalb des SDoT Malware Protection Service erschwert und eventuelle Folgen der Kontaminierung minimalisiert.

Sicherheitsarchitektur

Die interne Sicherheitsarchitektur des SDoT MPS basiert auf dem mit dem SDoT Security Gateway 6.0 eingeführten und mehrfach vom BSI bis GEHEIM zugelassenen SDoT Security Framework.
Die Entwicklung der Hard- und Software der gesamten SDoT-Produktfamilie folgt strikt dem Grundsatz „Security by Design". Angriffe, falsche Benutzereingaben und technische Fehlfunktionen sind von Anfang an berücksichtigt und die Produkte sind so konzipiert und gehärtet, dass Sicherheitsfunktionen zu keinem Zeitpunkt außer Kraft gesetzt werden können.

Übersicht der Funktionen

- Mehrere AV-Engines prüfen die Dateien und erfassenden Befund in Metadaten
- Eine befallene Datei wird vom Schadcode bereinigt und einer Nachprüfung unterzogen
- Selbstüberwachung des Systems
- Herunterfahren der sicherheitskritischen Funktionen im Falle einer Kompromittierung
- Automatische Update-Funktionen für kurzlebige Daten wie Virendefinitionen

Zusammenfassung

INFODAS GmbH stellt mit dem SDoT Malware Protection Service eine sichere, flexible, robuste und leistungsfähige Lösung zur Prüfung von Daten aus nicht-vertrauenswürdigen Datenquellen für alle Anwendungsfälle vor.
Das Produkt befindet sich in der Entwicklung und wird in Kürze zur Verfügung stehen.

infodas
Gesellschaft für Systementwicklung und Informationsverarbeitung mbH
Rhonestraße 2
50765 Köln
T +49 221 70912-0
F +49 221 70912-86
vertrieb@infodas.de
www.infodas.de