TESTBERICHT
Reddfort App-Protect

CSPi Technology Solutions, ist einer der führenden IT-Security Integratoren in Deutschland. Im Rahmen einer Security-Überprüfung wurde die Software-Lösung **„App-Protect“ von dem Unternehmen ReddFort** auf Herz und Nieren geprüft. Um eine praxisnahe Beurteilung der Produktqualität abgeben zu können, wurden verschiedene Kompromittierungsfälle simuliert, von einfachen Binary-Droppern, bis hin zu fortgeschrittenen Technologien, die sich einzig und allein auf Powershell stützen und somit von vielen Antivirusprogrammen nicht erkannt werden.

GETESTETE KERNFUNKTIONALITÄTEN:

- **SCHUTZ vor aktueller Schadsoftware**
- **ABSICHERUNG gegen Keylogger-Angriffe**
- **ISOLIERUNG der Anwendungen durch GuardedDesktop**
- **SCHUTZ vor Library Injections**

CSPi testete die oben genannten Punkte in einem Security Assessment und bewertete die Sicherheits-Mechanismen als ausgereift und effektiv im Schutz vor aktueller Schadsoftware. Auch der Schutz des isolierten Desktops stellt aktuelle Malware vor neue Hindernisse.

SCHUTZZIEL VON **APP-PROTECT**

Risikoreduzierung bei Schadsoftware auf dem Rechner
Ist Schadsoftware von Firewall unbemerkt auf den Rechner gelangt und wurde diese vom Virenscanner nicht erkannt, beginnt die Schutzwirkung von **App-Protect.**

CSPi
SICHERE IT

SCHUTZFUNKTIONEN IM DETAIL

Schutz vor aktueller und unbekannter Schadsoftware

App-Protect durchläuft in der ersten Phase nach der Installation einen Scan des gesamten Datenträgers. Dabei erstellt die Software für jede Binary-Datei, also für jede ausführbare Datei oder Bibliothek, eine eindeutige Signatur. Nach dieser Phase wird das System in einen Zustand versetzt, in dem alle unbekannten ausführbaren Dateien nicht mehr gestartet werden können. Dadurch wird sichergestellt, dass selbst unbekannte Schadsoftware nicht auf diesen Systemen ausgeführt werden kann. Im Test zeigte sich diese Sicherheitsfunktionalität als ausgereift und ließ sich nicht durch gleiche Dateinamen oder Dateigröße überlisten.

Absicherung gegen Keylogger-Angriffe und Isolierung der Anwendungen durch GuardedDesktop

Verschiedene Keylogger wurden zuerst zu den erlaubten Anwendungen hinzugefügt, um eine Umgehung des Ausführungs-Schutzes zu simulieren. Anschließend wurde eine Anwendung in der GuardedDesktop-Umgebung ausgeführt und es wurde getestet, ob ein Keylogger Zugriff zu den Tastatureingaben innerhalb der isolierten Umgebung hatte. Dies war nicht möglich, da die App hinreichend durch **App-Protect** isoliert wurde. Durch die Implementierung kann der Anwender gleichzeitigallerdings wie gewohnt von dem GuardedDesktop auf alle seine Dateien zugreifen und Notizen oder ähnliches lesen. Er kann also weiterhin den vollen Funktionsumfang der eingesetzten Software nutzen.

Wirksamer Schutz vor Library Injections

Es wurde ebenfalls überprüft, ob Anwendungen, die anfällig für Third Party Library Injections sind, unerlaubt abgelegte Dateien im Anwendungsverzeichnis nachladen können. Dies war ebenfalls nicht möglich und wurde durch Testbericht **Reddfort App-Protect** erfolgreich unterbunden. Die Engine erkennt in diesem Fall den Nachladevorgang der DLL und prüft die Checksumme. Ist diese nicht in der White-List, kann eine Ausführung nicht stattfinden.

UNSER FAZIT:

App-Protect ist ein sehr guter Schutz vor aktueller und unbekannter Schad-Software sowie vor Llibrary iInjections; **App-Protect** sichert zudem Anwendungen wirksam gegen Key-Logger-Angriffe. **App-Protect** kann problemlos neben „normalen“ Viren-Scannern eingesetzt werden und erweitert den Schutz von Applikationen deutlich. Zu **App-Protect** vergleichbare White-Listing-Programme haben im Unterschied zu **App-Protect** keinen GuardedDesktop und schützen deshalb nicht gegen Key-Logger und ähnliche Angriffe.

STANDORTE EUROPA

Deutschland
Oskar-Jäger-Str. 173 / K4
D-50825 Köln, Deutschland
Telefon: 49 (0) 221.954466.0
www.cspi.com/de

United Kingdom
12A Oaklands Business Centre
Oaklands Park Wokingham,
Berkshire RG41 2FD, Großbritannien
Telefon: 44 (0) 118.989.3843