REDDFORT APP-PROTECT

ReddFort App-Protect erzeugt mit Hilfe eines neuen Desktops einen geschützten Bereich. Innerhalb dieses Schutzsystems dürfen NUR die vorab registrierten Anwendungen ausgeführt werden.

ReddFort App-Protect beinhaltet einen „GuardedDesktop“ und dieser kann eine gesicherte Anwendungsumgebung in Form eines zweiten Desktops öffnen. Dabei wird eine isolierte –nicht virtuelle/sandbox– Umgebung erzeugt, innerhalb derer zuvor registrierte Anwendungen ausgeführt werden.

Zudem verfügt der „GuardedDesktop“ über eine wichtige Überwachungsfunktion: Während der Laufzeit wird sichergestellt, dass aktive Anwendungen nur auf zulässige und unverfälschte Systemkomponenten zurückgreifen. Jegliche Abweichung der Anwendungen wird bemerkt und kann analysiert werden.

ReddFort App-Protect besteht aus einem Verwaltungsmodul, einer Startkonsole und einem Laufzeitmonitor. Alle Anwendungen in Unternehmen, die unter besonderen Schutz gestellt werden sollen, werden zunächst in der Verwaltung registriert. Im Anschluss daran können alle registrierten Anwendungen über die Startkonsole gestartet werden.

Folgende Angriffsszenarien können mit App-Protect verhindert werden:

• System-wide Hooks (Beispiel: Vertauschung eingegebener Zeichen)
• Kopieren des Bildschirminhaltes über die DirectX-Schnittstelle
• Kopieren des Bildschirminhaltes über die Win32-API- Schnittstelle
• Kopieren des Inhaltes von Passworteingabefeldern
• Kopieren/Schreiben des Inhaltes beliebiger Felder
• Library Injection: Einbetten von DLLs in den virtuellen Speicher eines Prozesses
• Key-Logger: Aufzeichnung von Tastenanschlägen
• Message Corruption: Lesen/Schreiben von Daten in Handles
• Imulation von Eingaben und Kommandos an andere Fenster
• IAT-Hooking (Beispiel: Daten werden beim Speichern verschlüsselt)

Die Vorteile im Überblick:

• Kein Zugriff von außen auf sicherheitskritische Anwendungen und Prozesse
• Alle im „GuardedDesktop“ laufenden Anwendungen sind für mögliche Angreifer unsichtbar, Tastatur- und Mousebefehle können nicht mitgeschnitten werden
• Der bestehende Desktop und der „GuardedDesktop“ sind voneinander unabhängig und kommunizieren nicht miteinander. Mögliche Angriffe auf den „Client oder Server“ können also keinen Schaden verursachen.