TrustedDesktop

Umfassende Client-Sicherheit und effizientes Desktop-Management

Auch der aktuellsten Informationstechnik mangelt es nach wie vor an einem effektiven Schutz gegen Bedrohungen von außen wie aber auch von Insidern. Gezielte Malware-Attacken und unerwünschte Datenverluste sind nur die sichtbarsten Beispiele für diese wachsenden Gefahren. Die Zeit ist gekommen, einen umfassenderen Ansatz zur Sicherung von Clientsystemen zu verfolgen. Heutige IT-Infrastrukturen sind verteilt und heterogen. Sie weiten sich aus in Richtung Cloud Computing. 360° Grad Sicherheitskonzepte werden essentiell, sie sollten aber keine zusätzliche Komplexität oder Funk-tionseinschränkungen nach sich ziehen. TrustedDesktop hebt den Schutz gegen Attacken von Internetbasierten Angreifern sowie gegen von Insidern - versehentlich oder beabsichtigt - verursachte Datenverluste auf einen ganz neuen Level. Rohde & Schwarz Cybersecurity ist das erste Unternehmen, das die Konzeption von „vertrauenswürdigen Systemen“ als ein Fundament für IT-Infrastrukturen umfassend implementiert hat.

Die Lösung

TrustedDesktop ist eine sichere virtuelle Desktop-Lösung für eine praktikable Informationsflusskontrolle. Sein Prinzip beruht auf der strikten Isolation kritischer Anwendungen und unternehmensweiter Workflows und auf der verlässlichen Durchsetzung von Sicherheitsrichtlinien.

Seine innovative Technologie ermöglicht einen umfassenden und reviewfähigen Schutz des Lebenszyklus aller Unternehmensdaten. Damit wird ein versehentlicher oder böswilliger Datenabfluss an unberechtigte Dritte effizient verhindert. Der TrustedObjects Manager stellt ein systemweites Management von Sicherheitsrichtlinien bereit und ist gleichzeitig ein sehr einfach nutzbares Installations-, Konfigurations- und Provisioning-System für die gesamte Infrastruktur unter Einschluss von Netzen, Usern und Desktop Images.

Die Architektur

Die Kernkomponente von TrustedDesktop ist der SecurityKernel. Dieser Sicherheitskern isoliert mehrere Betriebssysteme (Compartments) in einzelne Sicherheitszonen, die virtuell auf demselben Clientsystem ausgeführt werden. Jedes Compartment kann bei einer Trusted Virtual Domain (TVD) zugeordnet werden. Jede TVD umspannt eine auf viele Rechner verteilte, in sich geschlossene virtuelle Sicherheitszone. Wenn Daten ein Compartment verlassen, werden sie transparent verschlüsselt und können daher nur von lokalen oder entfernten Compartments, die zur selben TVD gehören, weiter verarbeitet werden. Dieses revolutionäre Konzept ermöglicht zum ersten Mal eine effektive unternehmensweite Informationsflusskontrolle für herkömmliche Betriebssysteme. Die Basis dieses Vorgehensmodells stellt die Security-Kernel-Architektur und die Integration von Trusted Computing Technologie bereit.

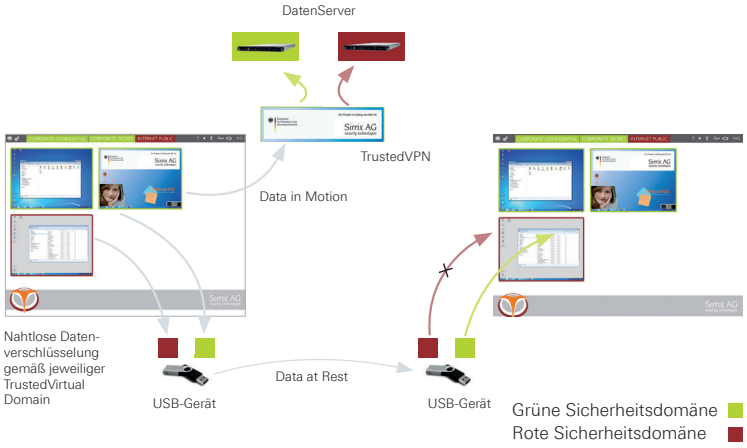
TrustedDesktop

TrustedDesktop bietet die folgenden Sicherheitsfeatures:

Umfassende Datenverlustabwehr durch transparente Dateiverschlüsselung. Daten werden beim Verlassen eines gesicherten Compartments transparent verschlüsselt, sobald ein Schreibzugriff auf mobile Datenträger (USB, HDD) oder entfernte Server (NFS, SMB) erfolgt. Damit wird auch ein sicherer Offline-Transport von Daten unterstützt. Ein Transfer unverschlüsselter Daten zwischen TVDs wird nur ermöglicht, falls und soweit die zentralen Sicherheitsrichtlinien dies ausdrücklich zulassen.

Ein intelligenter VPN-Client sorgt vollautomatisch für sichere Verbindungen zwischen den Compartments ein und derselben TVD und zu dedizierten besonders gesicherten Netzen.

Vollständige Festplatten-Verschlüsselung gestützt auf den TPM-Sicherheitschip: Im Gegensatz zu anderen Systemen ist der Verschlüsselungs-Schlüssel für das Betriebssystem niemals sichtbar und somit durch Viren oder Trojaner nicht angreifbar.



Features

TrustedInfrastructure

- Unternehmensweite Datensicherheit basierend auf Trusted Virtual Domains (TVDs)
- Cross-Plattform Informationsflusskontrolle
- Unterstützt Clients (TrustedDesktop), Server (TrustedServer) und Netze (TrustedVPN)

TrustedDesktop Client

- Unterstützt mehrere, strikt isolierte, zu unterschiedlichen TVDs zugeordnete virtuelle Maschinen. Basiert auf dem TURAYA™ SecurityKernel
- Gesichertes Booten und Systemintegrität basierend auf TPM-Chip
- Trusted GUI mit gesichertem Clipboard für die lokale Richtliniendurchsetzung
- Transparente Dateiverschlüsselung für lokale und entfernte Speichermedien
- Integrierter VPN Client für eine gesicherte Intra-TVD Kommunikation
- Smartcard-basierte Benutzer-Authentifizierung
- Zugriff auf Peripherie-Geräte (z.B. Kamera, Mikrofon)
- gesteuert über TVD-Richtlinien

TrustedObjects Manager

- Zentrales Infrastruktur- und Richtlinienmanagement für Clients, Netze, Server und virtuelle Maschinen (Trusted Objects)
- Zentrales Infrastrukturmanagement
  Registrierung und Authentifikation aller Trusted Objects
  Remote Attestation der Integrität aller Trusted Objects
  Verteilung zertifizierter Compartment Images
- Systemweites Sicherheitsrichtlinienmanagement auf TVD-Basis
  Definition erlaubter Informationsflüsse zwischen TVDs
  Netzzugangskontrolle und Firewallregeln innerhalb TVDs
  Nutzer- und rollenbasierte Richtlinien
- Webbasierte GUI für autorisierte Administratoren
- Voll integrierte PKI-Lösung
- Ready-to-run Appliance mit integriertem Sicherheitsmodul

Rohde&Schwarz Cybersecurity GmbH
Mühldorfstraße 15 | 81671 München
Info: +49 89 4129-206 000
cybersecurity@rohde-schwarz.com
www.cybersecurity.rohde-schwarz.com

3607577731

3607.5777.31 01.00 PDP 1 de.July 2016