itWash

Die Schleuse mit Datenwäsche

itWatch

itWatch GmbH

Aschauer Str. 30
D-81549 München

Tel.: +49 (0) 89 62 03 01 00
Fax: +49 (0) 89 62 03 01 069

www.itWatch.de
info@itWatch.de

itWash - die Schleuse mit Datenwäsche

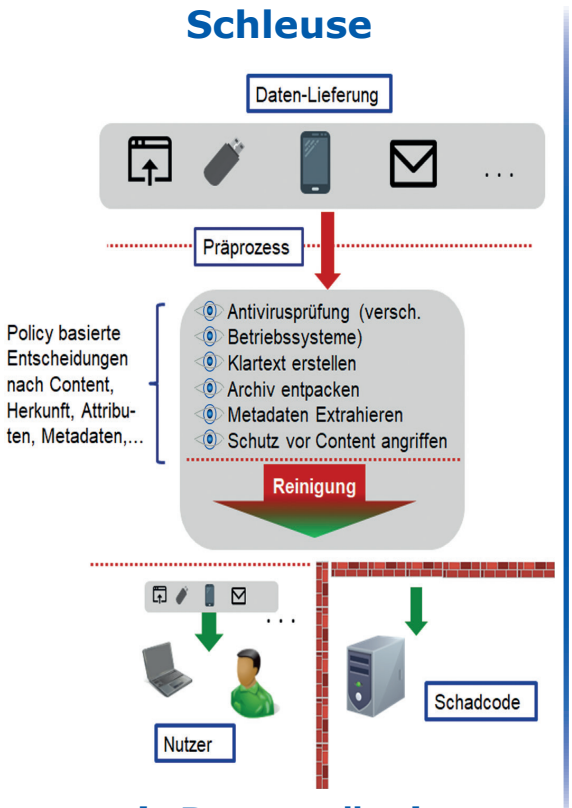
So funktioniert`s

Potentiell schädliche Daten von extern (Web, E-Mail, USB-Stick, I-Phone / Mobiles …) werden inhaltlich geprüft, ohne dass der Rechner oder das Netz mit Schadcode infiltriert werden kann. Die ankommenden Daten werden sauber „gewaschen" und sicher zur Ausgabe weitergeleitet. Als Ausgabe definiert der Kunde einen mobilen Datenträger oder eine Datenempfangsstation auf dem Fileserver im inneren Netz, so dass die gewaschenen Daten an den gewünschten Endgeräten weiterverarbeitet werden können. Die Daten werden hierzu auf einem isolierten, als Opfersystem ausgeprägten Schleusenrechner gebracht. Die Integrität des Systems wird nach jedem Boot wiederhergestellt und das System selbst wird durch eine Sicherheitspolicy der itWESS geschützt. Potentiell schädliche Daten werden durch die Prüfungen der itWESS identifiziert und an das „Reinigungssystem" weitergereicht und gereinigt.

Architektur

Das System skaliert in mehreren Dimensionen:

- **Sicherheit:** der Schutz kann so weit nach oben „reguliert" werden, dass sicher keine Angriffe über die importierten Daten möglich sind
  Kosten: angefangen von einem kostengünstigen dedizierten Wasch-PC, der alle Komponenten integriert bis zu einem mehrstufigen Server-basierten System skaliert das System nach Kosten und Durchsatz
- **Durchsatz:** je nach erwarteten Datenvolumina skaliert die Performance des Gesamtsystems durch die aufeinander abgestimmten Hardewarekomponenten nach Kundenbedarf



itWash Varianten

- **Dedizierte Schleuse:** Einzelplatzsystem mit allen Funktionen integriert
  - Mit Trennung der Hardware (eigene CPU je Prozess) itWash-d-HW
  - Mit Trennung der Prozesse durch prozessspezifische Rechte itWash-d-SW
- **Zentrale Schleuse: itWash-z**
  Die Waschkomponenten werden auf einer oder mehreren zentralen Instanzen installiert
- **Weitere Spezialkonfigurationen** z.B. für Boston Infrastructure in Software oder Hardware

Sicherheit

- Schutz des produktiven Systems (PS) vor allen Angriffen
- Integritätsschutz der Schleuse
- Datenflusskontrolle zwischen Schleuse und PS
- Entschlüsselung der Daten vor Inhaltskontrolle
- Anwendungen von beliebig vielen Anti Viren Sytemen und Einbindung von beliebigen Drittsystemen für weitere Prüfungen
- Anwendungen von beliebig komplexen rekursiven Inhaltsprüfungen mittels XRayWatch gegen eingebettete ausführbare Inhalte wie Executables, Makros, Java Skript etc.
- Trennung von Benutzer und Systemprozessen mit itWESS Mitteln durch vordefinierte Rechte der einzelnen Anwendungen

Archivierung Schlechtdateien

- Als „schlecht" erkannte Dateien können:
  - in sichere Datenformate konvertiert werden
  - gelöscht werden
  - sicher gelöscht werden
  - separiert und in einem Opferbereich gelagert werden
- jeweils mit oder ohne Hinweis an den Lieferanten
- Opferbereich hinter Firewall-System
- Opferbereich kann von einzelnen Berechtigten über rdp oder Standalone zugegriffen werden
- Opferbereich kann für Forensik etc. weitere Dienste leisten

Automatisierung

- Automatische Aktivierung standardisierter Aktionen z.B. Dialoge
- Automatischer Datentransport und Konvertierung
- Und viele weitere Automatisierungen