itWash

Netztrennende Datenschleuse
Datenwäsche
Workflow

Datenschleuse mit Datenwäsche

Warum Datenwäsche?

Daten aus unsicherer Herkunft können schädlichen Code enthalten. Potenziell schädliche Daten (Web, Download, E-Mail-Attachments, Links, mobile Datenträger, USB-Sticks, Tablets, Mobiltelefone, Anwendungen ftp, s-ftp) können Rechner oder das Netz mit (Schad)-Code infizieren.

So funktioniert's

Die ankommenden Daten werden zentral oder lokal sauber „gewaschen" und sicher zur Verwendung weitergeleitet. Als Ein- und Ausgabe definiert der Kunde, was zulässig ist: lokal z. B. CD, DVD, Blu-Ray, USB-Stick - auch „nur personalisiert", verschlüsselte E-Mail, FileShare wie Drop Box, Userverzeichnis, Mobiltelefone, Fachverfahren). Bei anwendergesteuerten Systemen wählt der Anwender zwischen den angebotenen, seiner Berechtigung entsprechenden Ein- und Ausgabekanälen. Zentral: unverschlüsselter Datenimport.

Die gewaschenen Daten werden automatisch an das gewählte oder nach Metadaten automatisch ermittelte Zielsystem geliefert. Die Daten werden hierzu auf einem vollständig isolierten Schleusensystem bearbeitet. Eine Integrität des Systems ist gewährleistet, das System selbst mehrschichtig gehärtet und durch eine Sicherheits-Policy der itWESS (Einsatz bis GEHEIM) und je nach Schutzbedarf durch vollständig entnetzte (air-gapped), separierte Hardware geschützt.

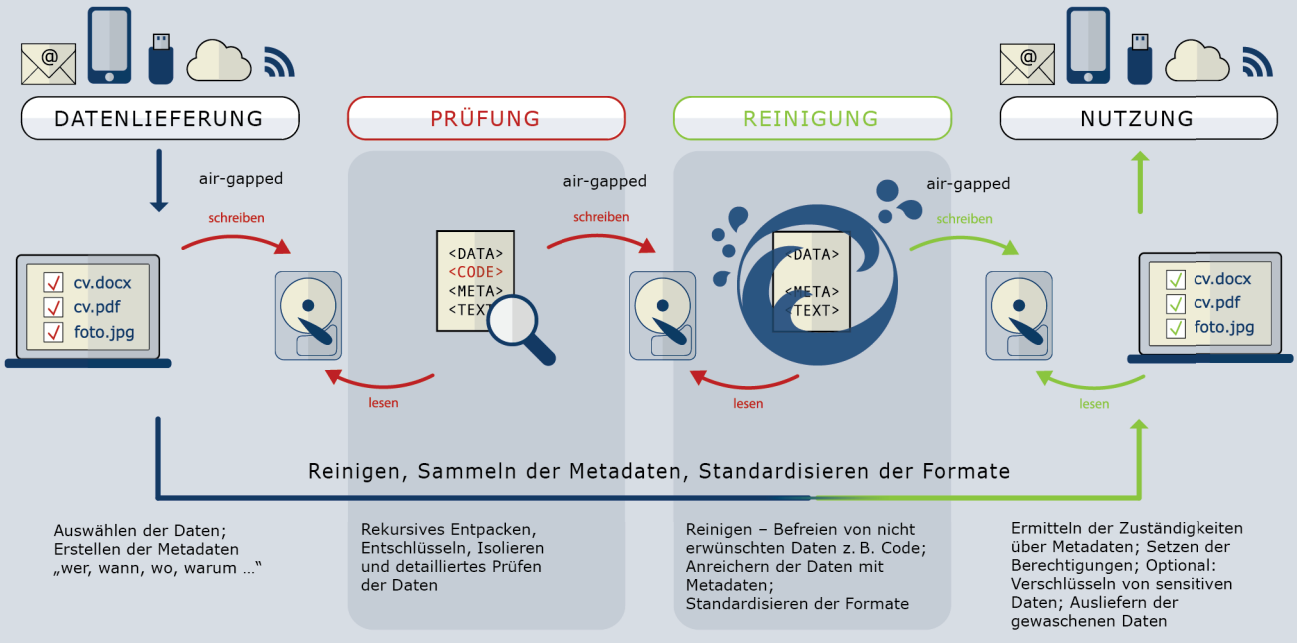
Potenziell schädliche Daten, das sind z. B. alle ausführbaren Datenelemente, werden durch die inhaltlichen Prüfungen sicher identifiziert, extrahiert und nach Richtlinie weiterverarbeitet. Verschlüsselte oder gepackte Daten werden in Klartext überführt, in alle einzelnen Elemente zerlegt und rekursiv an das „Reinigungssystem" weitergereicht und gereinigt. Algorithmische Prüfungen erlauben es, sicherheitsgeprüfte Code-Teile (bekannte / signierte Makros) in den Dateien zu erhalten.

Einsatzszenarien

Daten unsicherer Herkunft gibt es an vielen Stellen in den Organisationen

- Mailattachments
- Downloads
- FileShare-Plattformen
- Mobile Datenträger
- Personalabteilung
- Marketing
- Pressestelle
- Schadenbearbeitung und Meldestellen
- Vorträge und zugelieferte Inhalte von Partnern und Lieferanten
- IoT-Devices, Smart Home Devices, Überwachungskameras
- Fernwartung
- OT und Übergang zur IT
- Remote Patching
- Behörden – Bürgerdaten – E-Government – OZG
- Patientendaten auf CD/DVD und Wearables
- Digitale Archive – digitale Asservaten
- Unsichere Devices (BadUSB)
- Manuelle Schnittstelle für entnetzte Systeme
- Übergabe großer Datenmengen z.B. auf Baustellen oder als Produktdaten über Fachverfahren

Von der Datenlieferung zur gefahrlosen Nutzung



Mehr als Virenschutz

- Rekursives Entschlüsseln und Entpacken der Daten vor der Inhaltskontrolle
- Datenflusskontrolle zwischen Annahmestation, Schleuse und produktivem System – inkl. Monitoring, Protokollierung und Report
- Ent- und Verschlüsselung von vertraulichen Inhalten; DSGVO-Konformität
- Optional automatisierte/zwangsweise Wandlung auf gewünschte Ziel-Formate wie z.B. mp4, mp3, PDF/A-1a
- Schutz des produktiven Systems vor Zero-Day-Exploits, denn jeder Angriff braucht ein Stückchen Code
- Schutz vor allen contentbasierten Angriffen
- Keine IP-basierten Angriffstunnel möglich
- Integritätsschutz der Schleuse
- Beliebig komplexe, rekursive Inhaltsprüfungen mittels itWash-eigener Algorithmen zur sicheren Identifikation unerwünschter eingebetteter Inhalte
- Einbindung von beliebig vielen Anti-Viren-Systemen und beliebigen Drittsystemen für weitere Fähigkeiten (inkl. deren Protokollierung)
- Trennung aller Prozesse durch prozessspezifische Rechteräume und/oder durch entnetzte Hardware
- Sammlung aller Metadaten aus dem gewaschenen Objekt durch Analyse und KI mit offenen Übergabeschnittstellen in Datei und/oder Datenbank
- itWash ist kompatibel mit 3rd Party Services wie z.B. Labelling Services

	itWash	Anti Virus	AV basierte Schleuse
Reinigung – Veränderung des Dokuments	✓	✗	✗
Herauswaschen aller ausführbaren eingebetteten Objekte	✓	✗	✗
Blocken von identifizierbaren bereits bekannten Pattern von Schadcode	✓	✓	✓
Archivbomben entdecken und davor schützen	✓	✗	✗
Rollenbasierte Verarbeitungstemplates	✓	✗	✗
Erkennung und Entschlüsselung von verschlüsselten Inhalten vor Prüfung	✓	✗	✗
BadUSB verhindern	✓	✗	✗
Virenbefallene Informationen lesbar verändern	✓	✗	✗
Workflow rollen- und inhaltsbasiert	✓	✗	✗
Archiv vor Verarbeitung rekursiv entpacken	✓	✗	✗
Metadaten extrahieren und archivieren	✓	✗	✗
(Zwangs)Verschlüsselung/Signatur nach Verarbeitung	✓	✗	✗

Die itWash-Elemente

itWash-Mail

Zentral: Unerwünschter Code in Anhängen und maliziöse Links in Mails sind die meistgenutzten Angriffsmethoden.

Zentrale Mailwäsche: Mit der zentralen Mailwäsche von itWash werden die Anhänge aller eingehenden Mails direkt gewaschen und an den Empfänger ausgeliefert.

Mail Client: itWash-Mail Client bietet dem sensibilisierten Anwender die Möglichkeit, Mails von unsicheren Absendern vor dem Öffnen völlig barrierefrei zu waschen, um Risiken zu vermeiden, und erlaubt eine Zwangsentschlüsselung mit Wäsche vor der Nutzung.

itWash-z

itWash als zentrale Einheit ist aufgeteilt in verschiedene Komponenten: Annahme bzw. Datenanlieferung, Prüfung und rekursive Analyse, Datenwäsche und Verteil- bzw. Übergabeeinheit zur nutzenden Stelle. In der Datenanlieferung können Daten unterschiedlicher Quellen ankommen, die dann, mit verschiedenen, diesen Quellen zugeordneten Waschprogrammen, gesäubert werden: z. B. Internetdownloads, Kommunikation mit Dritten wie Partnern auch über Bulktransfer-Schnittstellen, s-ftp oder Clouddienste, Bürgerdaten (OZG), Kundenportale, Schadensmeldungen etc. Die zentralen Waschkomponenten werden als 19”-Einheiten in verschiedenen Netzsegmenten (Extranet, DMZ, Backbone, separierte Netzeinheit) installiert. Die gereinigten Daten werden automatisiert weiterverteilt und mit den geeigneten Zugriffsrechten (Nutzer, Gruppe) bei Bedarf verschlüsselt abgelegt.

itWash-A

Annahmestation dient der manuellen, kabelgebundenen oder kabellosen Einlieferung von Datenmaterial, das dann an eine itWash-z on-premise oder in der Cloud weitergeleitet wird. Parameter über den Einlieferer und seinen gewünschten Rückkanal werden lokal an der Annahmestation erhoben und als Metadaten transportiert.

itWash-iz

Die Datenannahme findet an dem Standardarbeitsplatz der Mitarbeitenden statt. Potenziell schmutzige, oder abgelehnte Daten von USB, Mobiltelefone, Download, Mail-Anhang etc. werden zwangsweise an eine itWash-z gesendet, welche die gewaschenen Daten automatisch zurück liefert. Bei Doppelklick auf die einzuliefernde Datei kann eingestellt werden, dass die gewaschene Datei auch sofort nach Rücklieferung geöffnet wird.

itWash-d

itWash als dedizierter Kiosk für die Annahme von z. B. Kunden- oder Bürgerdaten in einem Self-Service. Als Ziele können z. B. die Besprechungsräume für Vortragdaten oder Fachverfahren definiert werden.

Erweiterung durch Add-In

Bestandslösungen und beliebige Drittprodukte wie z.B. KI zur Ermittlung von Metadaten mit Bilderkennung, Voice-to-Text werden einfach durch offene Schnittstellen eingebunden.

CleanFile

CleanFile realisiert die durchgehende Vertrauenskette von der Anlieferung bis zur Nutzung. Es markiert fertig gewaschene Datenpakete, sodass an einem Arbeitsplatz garantiert nur, vom eigenen Unternehmen gewaschene Daten, eingelesen werden können.

CleanFile besteht aus zwei Komponenten: dem itWash-CleanFile-Client mit Funktionalitäten der itWESS (itWatch Enterprise Security Suite), der sicherstellt, dass nur gewaschene Daten in Nutzung gehen, und der Datenwäsche in itWash. CleanFile stellt die Compliance zur DSGVO her.

CodeWash

In CodeWash sind die Werkzeuge zur Code-Herstellung, dem Lifecycle Management und der Versionierung enthalten. Modelle, Code, Trainingsdaten, Rohmanuale und Installationswerkzeuge werden eingeliefert. Sie treffen innerhalb der „Waschstraße" auf Compiler, Source Code Prüfungen, Eskalationen für Fehler, Warnings und Manualkonverter. Ausgeliefert wird ein signiertes, versioniertes, beweisgesichertes Paket.

CodeIntegrity

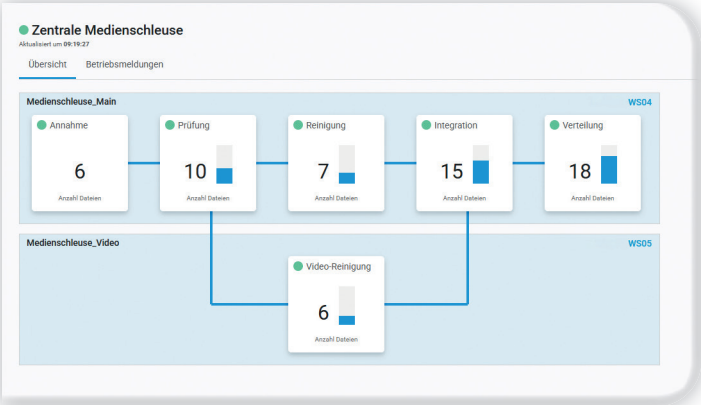
CodeIntegrity überprüft den eingelieferten Code auf Authentizität und Integrität und verifiziert Signaturen. Bei Bedarf können CVE (Common Vulnerabilities and Exposures), geprüft und SBOMs (Software Bill of Materials) hergestellt werden. Die Security-Lösung eignet sich optimal für automatisiertes oder air-gapped Patch-Management. Eine Übergabe und Freigabe der geprüften Software kann direkt an ApplicationWatch aus der itWESS Suite erfolgen. Das „Gedächtnis" sorgt dafür, dass später erkannte CVE zum Alert oder sogar zur sofortigen Sperrung der betroffenen Anwendung führen.

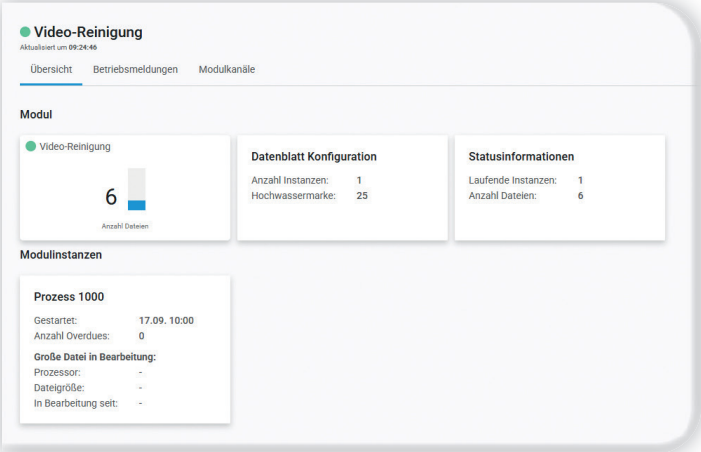
Anders als die itWash-Elemente, die Code aus den gelieferten Daten herausfiltern, sorgen CodeWash und CodeIntegrity für ein sicheres Life Cycle Management und die vollständige Beweissicherung – mit „Gedächtnis".

itWash Control Center

itWash-Dashboard

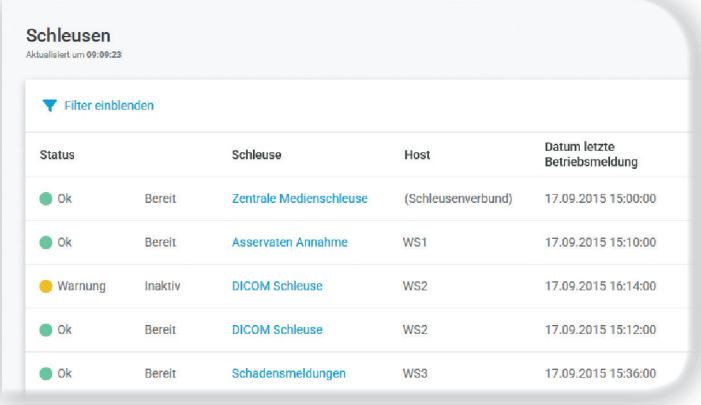
itWash-Dashboard visualisiert die Systemzustände, Incidents und Events, sodass ein Überblick über Auslastungen, mögliche Engpässe, Quarantänefälle in Echtzeit zur Verfügung steht.





itWash-FlowControl

itWash-FlowControl ermöglicht ein Auftragsverarbeitungs-, Datenvolumen- und Datenträgermanagement aller „Waschaufträge". Die sendende und empfangende Organisation kann unterschiedlich sein, und trotzdem wird keine Netzkopplung benötigt. Quelle, Ziel, Priorität, Geheimhaltungsstufen und Rechte sind konfiguriert und eine automatisierte Benachrichtigungsanforderung hinterlegt. Das Schleusen und Waschen großer Datenmengen (Petabyte) kann an Fachverfahren flexibel eingebunden werden.

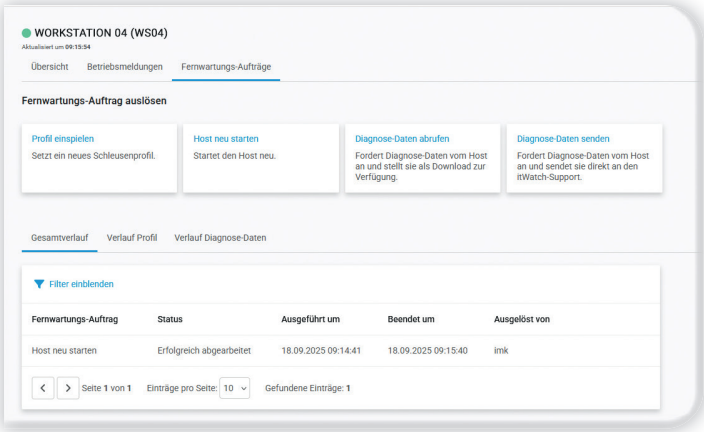


Monitoring und Verwaltung von itWash-Datenschleusen

Mit dem ICC (itWash Control Center) lassen sich mittels einer webbasierten Anwendung alle itWash-Instanzen zentral überwachen, steuern und verwalten.

Als integraler Bestandteil der itWash-Architektur ermöglicht es den permanenten Überblick, eine schnelle Reaktion auf sicherheitsrelevante Ereignisse und eine einfache Unterstützung der Anwender.

- Kontinuierliches und transparentes Live-Monitoring aller Schleusenaktivitäten über EIN Werkzeug
- Status- und Performancemonitoring der einzelnen Instanzen innerhalb einer Schleuse
- Anbindung an SIEM-Systeme und weitere Sicherheitsfeatures wie Alerting
- Visualisierung des Systemstatus über ein Ampelsystem
- Zentrale Verwaltung verschiedener Schleusentypen (zentrale und dezentrale)
- Vergabe und Übertragung von Sicherheitsprofilen
- Änderung von Schleusen-Konfigurationen auch während des Betriebs
- Echtzeit-Meldung von Status und Betriebsmeldungen
- Sichere on-premise-Nutzung ohne Cloudanbindung
- Fernwartung der Schleusenrechner



Das ICC deckt mehrere Funktionsbereiche ab. Bei Bedarf und nach Nutzungsart, Servicelevel, Mandantenfähigkeit stehen verschiedene Funktionsbereiche auf unterschiedlichen Hardware-Komponenten in diversen Netzen zur Verfügung.

itWash-ICC/SV+U (Softwareverteilung und Updates)

Die Softwareverteilungskomponente des ICC dient der Herstellung, der Aufrechterhaltung und Wiederherstellung der Betriebsbereitschaft der verschiedenen itWash-Komponenten. (Zertifikate, Signaturen, Patches, …)

itWash-ICC/DC (zentrales Reporting)

Zentraler Überblick über alle Ereignisse, Statusmeldungen und statistischen Analysen aller im Einsatz befindlichen itWash-Systeme.

itWash-ICC/VPN (Virtual Private Network)

Die verschiedenen VPN Nutzungsszenarien von itWash werden zentral gemanagt:

- Einbindung von itWash in die kundenseitige Infrastruktur
- zweites VPN optional für den Remote-Wartungszugang (je nach SLA auch von itWatch)

itWash-ICC/Health Status

Überwachung der Auslastung der verfügbaren Schleusenmodule

Die Komponenten können virtualisiert betrieben werden. Die Definitionen der Zugriffsregelungen sind Bestandteil eines umfassenden Sicherheitskonzeptes.

Skalierung

Das System skaliert in mehreren Dimensionen:

Kosten: Von einem kostengünstigen, dedizierten itWash-System (all-in-one), bis zu einem mehrstufigen serverbasierten System.

Sicherheit: Der Schutz kann so definiert werden, dass durch Daten von außen sicher keine Angriffe in das Zielnetz möglich sind.

Durchsatz: Die Performance des Gesamtsystems skaliert nach Durchsatz und Laufzeit der Einzelaufträge durch die aufeinander abgestimmten Komponenten und hohe Parallelität nach Kundenbedarf – auch im Cloudbetrieb. Komponenten können bedarfsgerecht in Echtzeit z. B. als fertiger Container zugeschaltet werden. Einzelne itWash-Komponenten können auf separate Hardware ausgelagert werden, z. B. um länger laufende Waschvorgänge zu separieren.

Archivierung und Beweissicherung

- Als „unerwünscht” erkannte Dateien können:
  - in sichere Datenformate konvertiert werden
  - gelöscht / sicher gelöscht werden
  - separiert und verschlüsselt in einem Quarantäne-bereich gelagert werden
- Jeweils mit oder ohne Hinweis an den Lieferanten
- Quarantäne hinter eigener Firewall
- Auf die Quarantäne kann von einzelnen Berechtigten, z. B. Forensik sicher zugegriffen werden
- Beweissicherung der Originaldaten inkl. der Meta-daten (Zeit, Ursprung) mit juristischer Beweiskraft durch Signaturen und Echtzeitstempel möglich.

Datenwäsche selber testen

Probieren Sie wie einfach und barrierefrei die Datenwäsche als Service aus der Cloud oder on-premise sein kann!

Senden Sie eine Mail mit Anhang an:

MyLaundry@DataWashing.de.

Anschließend erhalten Sie den gewaschenen Anhang als Mail umgehend zurück.
Oder Scannen Sie den QR-Code.

Wir sind für Sie erreichbar

Senden Sie gerne Ihre Fragen an **info@itWatch.de**. Zusätzlich steht unseren Kunden unser technischer Support jederzeit telefonisch oder unter der **hotline@itWatch.de** zur Verfügung.

Sie möchten lieber einen direkten Ansprechpartner?

Technische Hotline
+49 1805 999984 (0,14 €/Minute)
Kostenfreie 0800-Nummern sind bei geeigneten Wartungsverträgen verfügbar

Für weitere Fragen:
+49 89 62030100

Ihre Sicherheit. Unsere Mission.

itWatch GmbH
Aschauer Str. 30
81549 München

itWatch.de
itWash.de
itWESS.de

itWatch GmbH