itWash

Netztrennende Datenschleuse Datenwäsche Workflow

Datenschleuse mit Datenwäsche

So funktioniert’s

Potentiell schädliche Daten von extern (Web, Download, E-Mail Attachment und Links, mobile Datenträger USB-Stick, iPhone/ Mobiles, etc., Kommunikation über Anwendungen ftp, s-ftp u.v.m.) werden inhaltlich geprüft, ohne dass der Rechner oder das Netz mit (Schad-) Code infiltriert werden kann.

Die ankommenden Daten werden zentral oder lokal sauber „gewaschen” und sicher zur Ausgabe weitergeleitet. Als Ein- und Ausgabe definiert der Kunde, was zulässig ist (z. B. CD, DVD, Blue-Ray, USB-Stick - auch „nur personalisiert”, E-Mail, Netzwerk-Share, User-Verzeichnis, Handy, Anwendung, Fachverfahren ...). Bei anwendergesteuerten Systemen wählt der Anwender zwischen den angebotenen, seiner Berechtigung entsprechenden Ein- und Ausgabekanälen.

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. Die 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, separierte Hardware geschützt.

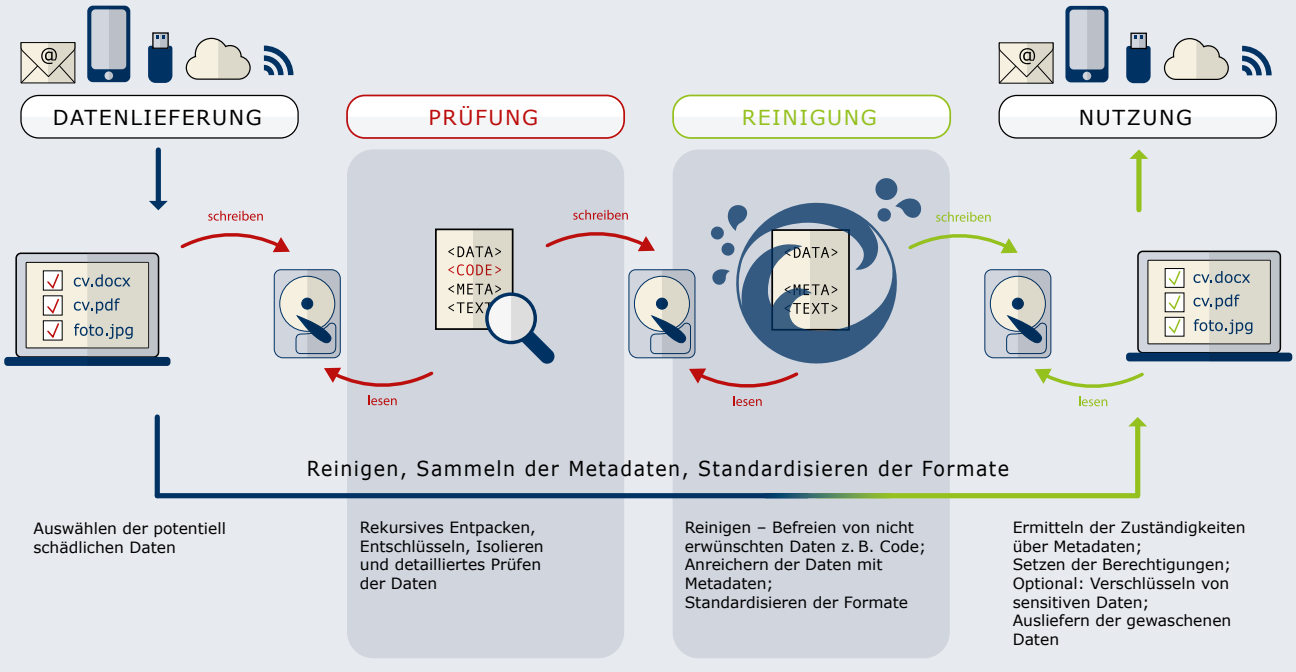
Potentiell schädliche Daten, das sind z. B. alle ausführbaren Datenelemente, werden durch die inhaltlichen Prüfungen sicher identifiziert, extrahiert und nach Richtlinie weiterverarbeitet. Verschlüsselte oder gepackte Daten werden im Klartext erstellt, in alle einzelnen Elemente zerlegt und rekursiv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

Einsatzszenarien

Daten unsicherer Herkunft gibt es an vielen Stellen in den Organisationen

- Mailattachments
- Downloads
- 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)
- Drehstuhl-Turnschuhschnittstellen für entnetzte Systeme
- Übergabe großer Datenmengen z.B. auf Baustellen oder als Produktdaten über Fachverfahren

Von der Datenlieferung zur gefahrlosen Nutzung



Mehr als Virenschutz

- Schutz des produktiven Systems vor Zero Day Exploits, denn jeder Angriff braucht ein Stückchen Code
- Schutz vor allen Content-basierten Angriffen
- Keine IP-basierten Angriffstunnel möglich
- Integritätsschutz der Schleuse
- Datenflusskontrolle zwischen Annahmestation, Schleuse und produktivem System – inkl. Monitoring, Protokollierung und Report
- Ent- und Verschlüsselung von vertraulichen Inhalten; DSGVO-Konformität
- Rekursives Entschlüsseln und Entpacken der Daten vor der Inhaltskontrolle
- 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
- Zwangsweise Wandlung auf sichere Formate wie z. B. PDF/A-1a möglich
- 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 Labelling Services, Security Labels, die sich ggf. in den angelieferten Daten befinden, werden von itWash in allen internen Prozessen berücksichtigt. Labels werden durch itWash weder entfernt noch manipuliert, die Klassifizierung bleibt somit erhalten.

	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 Inhalts-basiert	✓	✗	✗
Archiv vor Verarbeitung rekursiv entpacken	✓	✗	✗
Metadaten extrahieren und archivieren	✓	✗	✗
(Zwangs)Verschlüsselung/Signatur nach Verarbeitung	✓	✗	✗

itWash Mail

Schadcode in Anhängen oder Links in Mails ist die meistgenutzte Angriffsmethode.
Mail Client: itWash-Mail Client bietet dem sensibilisierten Anwender die Möglichkeit, Mails von unsicheren Absendern vor dem Öffnen zu waschen und damit die Risiken zu vermeiden.
Zentrale Mailwäsche: Mit der zentralen Mailwäsche von itWash werden die Anhänge aller eingehenden Mails direkt gewaschen und an den Empfänger ausgeliefert.

Die Schleusen Varianten

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 Partner 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 weiter verteilt und mit den geeigneten Zugriffsrechten (Nutzer, Gruppen…) bei Bedarf verschlüsselt abgelegt.

itWash-A

itWash 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 der gewaschenen Daten werden lokal an der Annahmestation erhoben und als Metadaten über den gesamten Waschvorgang transportiert.

itWash-iz

Die Datenannahme findet an dem Standardarbeitsplatz der Mitarbeitenden statt. Potentiell schmutzige Daten von USB, Mobile, 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 werden einfach durch offene Schnittstellen eingebunden.

Archivierung und Beweissicherung

- Als „unerwünscht” erkannte Dateien können:
  - in sichere Datenformate konvertiert werden
  - gelöscht / sicher gelöscht werden
  - separiert und verschlüsselt in einem Quarantänebereich 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 Metadaten (Zeit, Ursprung …) mit juristischer Beweiskraft durch Signaturen und Echtzeitstempel möglich.

itWash-Dashboard

itWash-Dashboard visualisiert die Systemzustände, Incidents und Events, so dass ein Überblick über Auslastungen, mögliche Engpässe, Quarantänefälle etc. in Echtzeit zur Verfügung steht, der es ermöglicht, geeignete Maßnahmen einzuleiten.

itWash-FlowControl

itWash-FlowControl ermöglicht das Schleusen und Waschen großer Datenmengen (Petabyte), ein flexibles, an Fachverfahren angebundenes Auftragsverarbeitungs-, Datenvolumen- und Datenträgermanagement aller „Waschaufträge”, wobei die sendende und empfangende Organisation unterschiedlich sein können und trotzdem keine Netzkopplung entsteht. Quelle, Ziel, Priorität, Geheimhaltungsstufen und Rechte werden konfiguriert, eine Benachrichtigungsanforderung hinterlegt.

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 sicher keine Angriffe im 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.

Systemmanagement

itWash Managementserver decken mehrere Funktionsbereiche ab. Bei Bedarf und nach Nutzungsart, Servicelevel, Mandantenfähigkeit etc. stehen unterschiedliche Funktionsbereiche auf unterschiedlichen Hardware-Komponenten in unterschiedlichen Netzen zur Verfügung.
Die Komponenten können virtualisiert betrieben werden.
Die Definitionen der Zugriffsregelungen sind Bestandteil eines umfassenden Sicherheitskonzeptes.

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

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

itWash-MS/DC (zentrales Reporting)

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

itWash-MS/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-MS/Health Status

Überwachung der Auslastung der verfügbaren Schleusenmodule

Wir sind für Sie erreichbar

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

itWatch GmbH
Aschauer Str. 30
81549 München

itWatch.de
itWash.de
itWESS.de

V1/05-2025