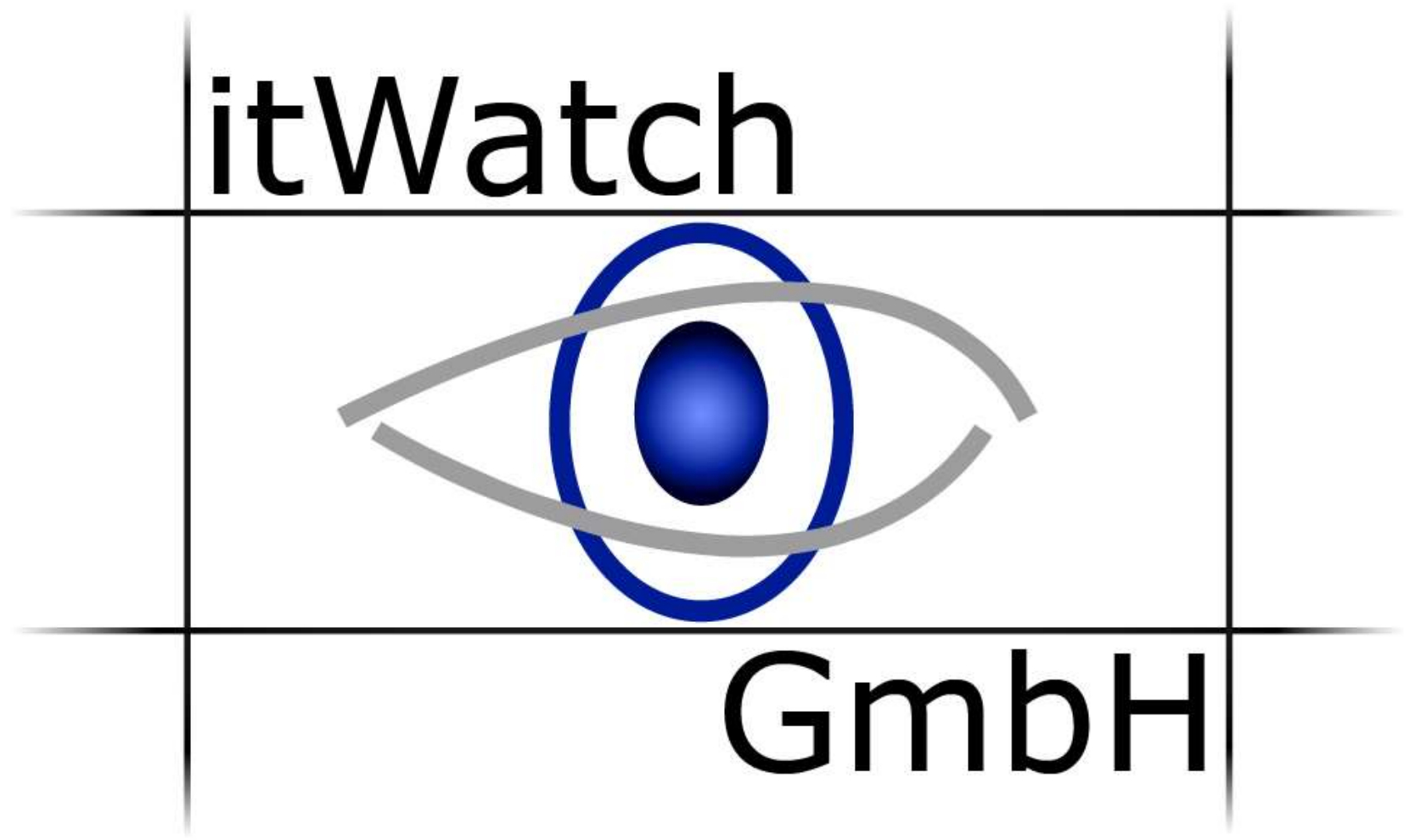
Ihre Sicherheit …
… unsere Mission



Datenwäsche gegen Cyberangriffe und Ransomware einsetzen

26. Oktober 2022 | 11:15 - 11:30 Uhr
Forum E – Halle 7A

Agenda

Kurzvorstellung

Die Herausforderung – wie kommt Ransomware ins Unternehmen?

Was tun mit Daten aus unsicherer Herkunft?

Agenda

Kurzvorstellung

Die Herausforderung – wie kommt Ransomware ins Unternehmen?

Was tun mit Daten aus unsicherer Herkunft?

Kurzvorstellung Ramon Mörl

- 30 Jahre Erfahrung als Berater in der IT-Sicherheit
- Leitende Tätigkeiten in Projekten für Firmen wie HP, IBM, Siemens, ICL und Bull in Belgien, Deutschland, Frankreich, Italien, Österreich, Schweiz und USA
- Als unabhängiger Evaluator und Berater der Europäischen Union vor allem im Bereich der ECMA und ISO-Standards für die IT-Sicherheit tätig
- Seit 2002 Geschäftsführer der itWatch GmbH

Agenda

Kurzvorstellung

Die Herausforderung – wie kommt Ransomware ins Unternehmen?

Was tun mit Daten aus unsicherer Herkunft?

Wie kommt Ransomware ins Unternehmen?

Wozu sind Links in Mails in Dokumenten im Internet … da?

… um den Anwendern zu sagen:

NICHT Klicken – gefährlich

Wozu sind USB Sticks da?

… um den Anwendern zu sagen:

NICHT Einstecken – gefährlich

Wozu sind Mail-Attachments da?

… um den Anwendern zu sagen:

NICHT Öffnen – gefährlich

Bruce Schneier auf der mcsc

Die Problematik

Man weiß nie, wo sich Angreifer verstecken!

Kann der Anwender gut & böse erkennen?

Schadcode in Bildern

RSA Security 2015 in San Francisco:

Marcus Murray zeigt eine einfache Methode, um Schadcode in Bilddateien zu verstecken – und einen Webserver zu übernehmen

- Murray verbirgt Schadcode als Kommentar in der EXIF-Information von Bilddateien.
- Der Schadcode wird im Rechteraum des Anwenders ausgeführt, ohne dass ein Nutzer das merkt.
- Ähnliche Verstecke für Schadcode gibt es in allen Dateiformaten, Video, Office-Dokumente, pdf etc.
- Risiken sind in allen ausführbaren Elementen – Makros etc. enthalten.
- **Wie können potentiell risikobehaftete Dateien importiert, bearbeitet, archiviert und auf jedem Rechner weiter bearbeitet werden?**

Datenschleuse: Reinigen – Bsp.: JPG

Im Kommentarfeld kann eine exe-Datei enthalten sein!

Canon EOS

2020:05:20 14:26:22

…..

…

.

Die praktischen Notwendigkeiten

Die Schattenseite der Digitalisierung: Daten können nicht abgelehnt werden, nur weil der Datenlieferant z.B. einen Virus auf seinem Handy hat.

Aktuelle Lagen – verlangen nach

- Mehr Detail-Information in kürzerer Zeit
- Anreicherung der Metadaten um manuell erfasste Daten
- Schnellere und vor allem filigranere Reaktionsmöglichkeit auf Inhalte
- Bei Schadcodebefall ist Ablehnen keine Option: es gilt das sichere Arbeiten zu ermöglichen

Immer mehr Flexibilität und Mobilität wird in den Businessprozessen benötigt – das Einbinden

- neuer Geräte der Informationslieferanten
- Unbekannter Informationen
- spontaner Kommunikationsbeziehungen
- Workflows, Priorisierung und automatische Zuordnung, um der Menge an Information Herr zu werden

Gesetzliche Vorschriften

- Das Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG) verpflichtet Bund, Länder und Kommunen, bis Ende 2022 ihre Verwaltungsleistungen über Verwaltungsportale auch digital anzubieten.

Agenda

Kurzvorstellung

Die Herausforderung – wie kommt Ransomware ins Unternehmen?

Was tun mit Daten aus unsicherer Herkunft?

Ziel und Umsetzung einer Datenwäsche

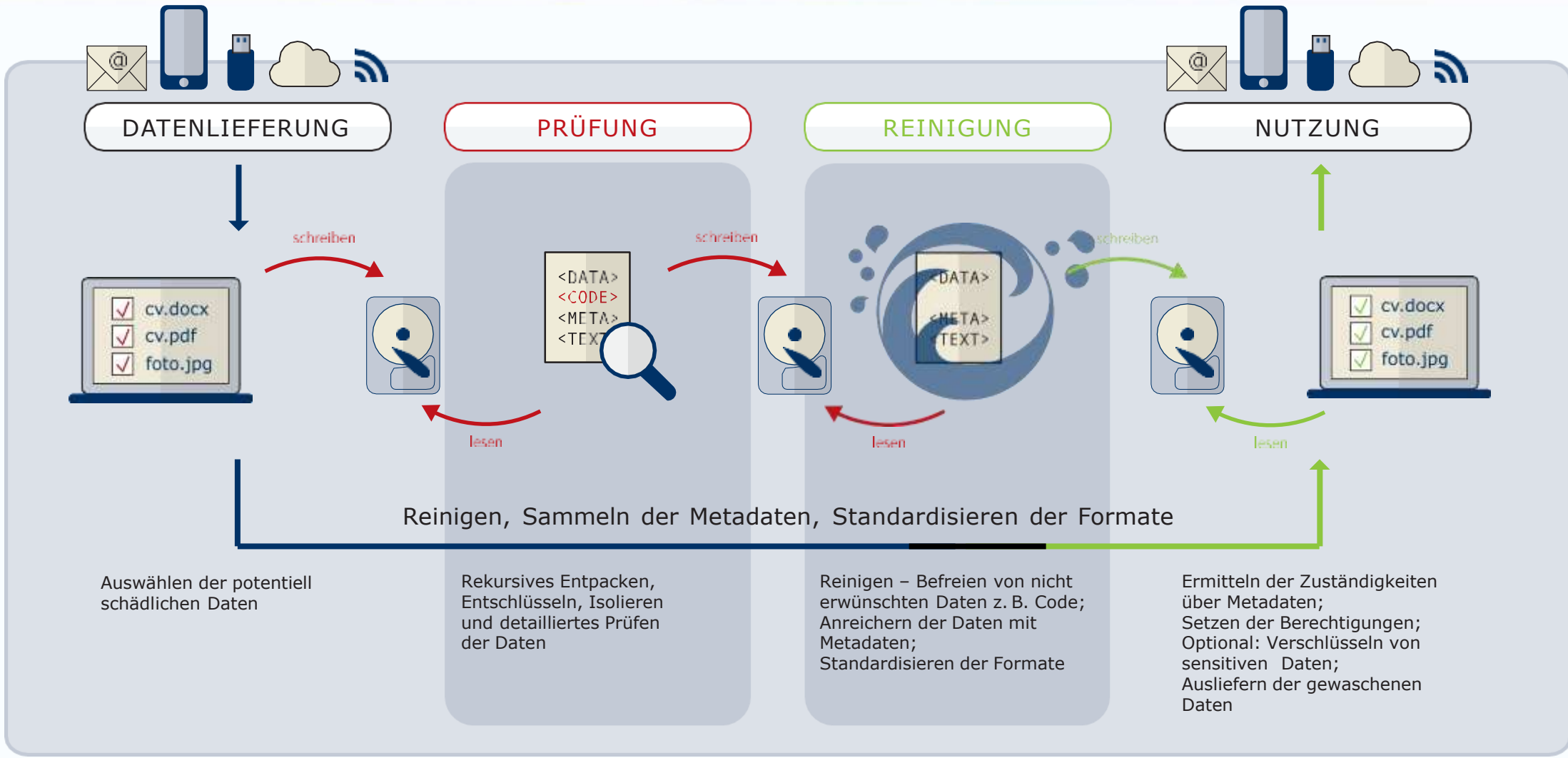
- Potentiell **schädliche Daten** von extern (Web, E-Mail, USB-Stick, I-Phone / Mobiles, eigene Anwendungen …) werden **sicher** in das **innere Netz geschleust**, in einem definierten Workflow mit weiteren Daten (z.B. **Metadaten**) angereichert, das Format **standardisiert** und im inneren Netz weiter verarbeitet.

- Die Daten werden auf einem isolierten, teilweise als **Opfersystem** ausgeprägten System von **Schleusenrechnern** erfasst. Die Integrität wird nach jedem Boot wieder hergestellt und jedes System selbst wird durch geeignete **Härtungsmaßnahmen** unter anderem einer Sicherheitspolicy der itWESS geschützt.

- Potentiell schädliche Daten werden gereinigt.

- Verschiedene Archivierungs- und Beweissicherungsauflagen werden automatisch erfüllt

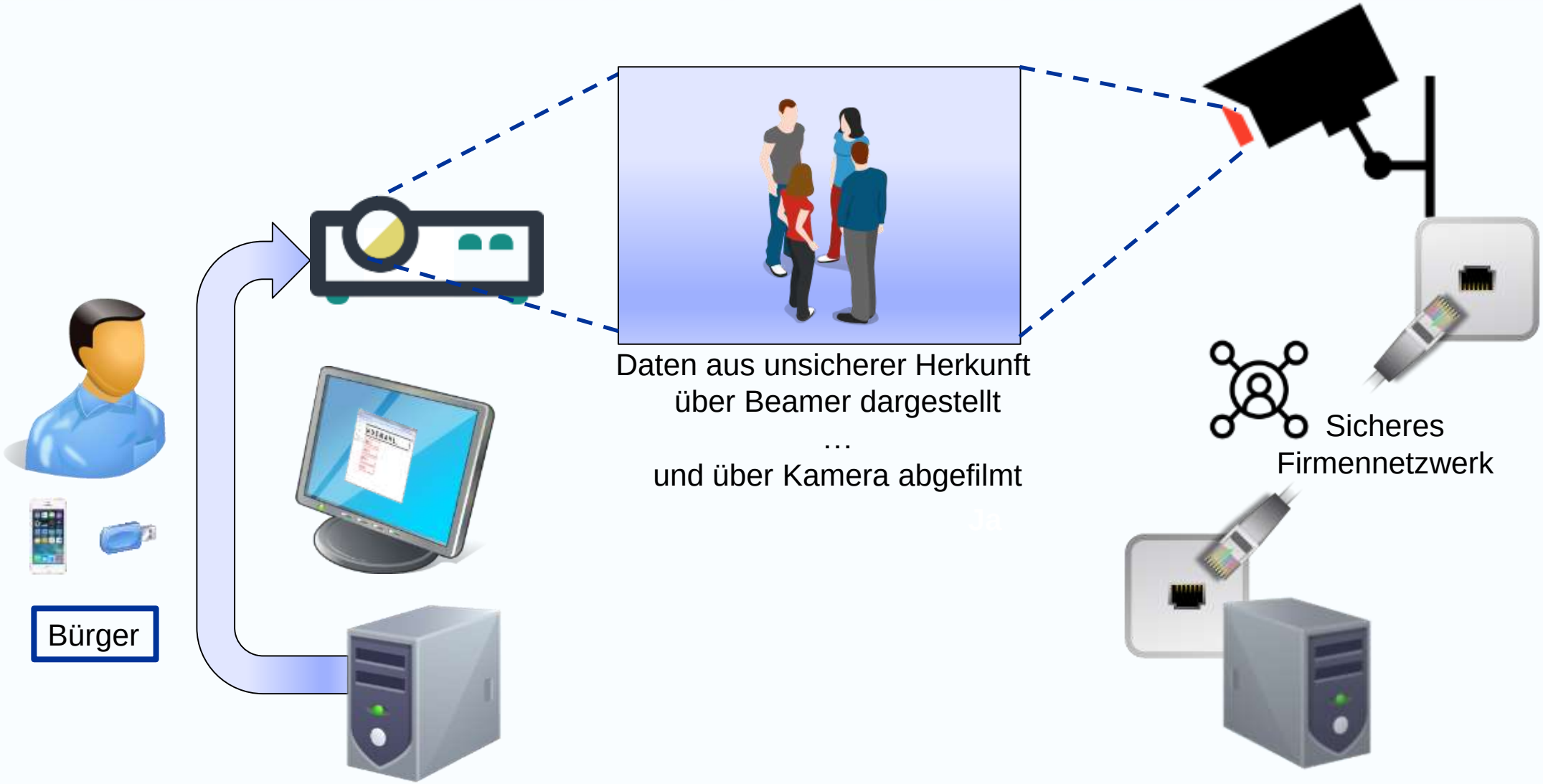
Von der Datenlieferung zur gefahrlosen Nutzung



Wo braucht man eine Datenwäsche

- Mailattachments
- Downloads
- Mobile Datenträger
- Personalabteilung
- Marketing
- Pressestelle
- Schadenbearbeitung und Meldestellen
- Vorträge und 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- bzw. Turnschuh-schnittstellen für entnetzte Systeme

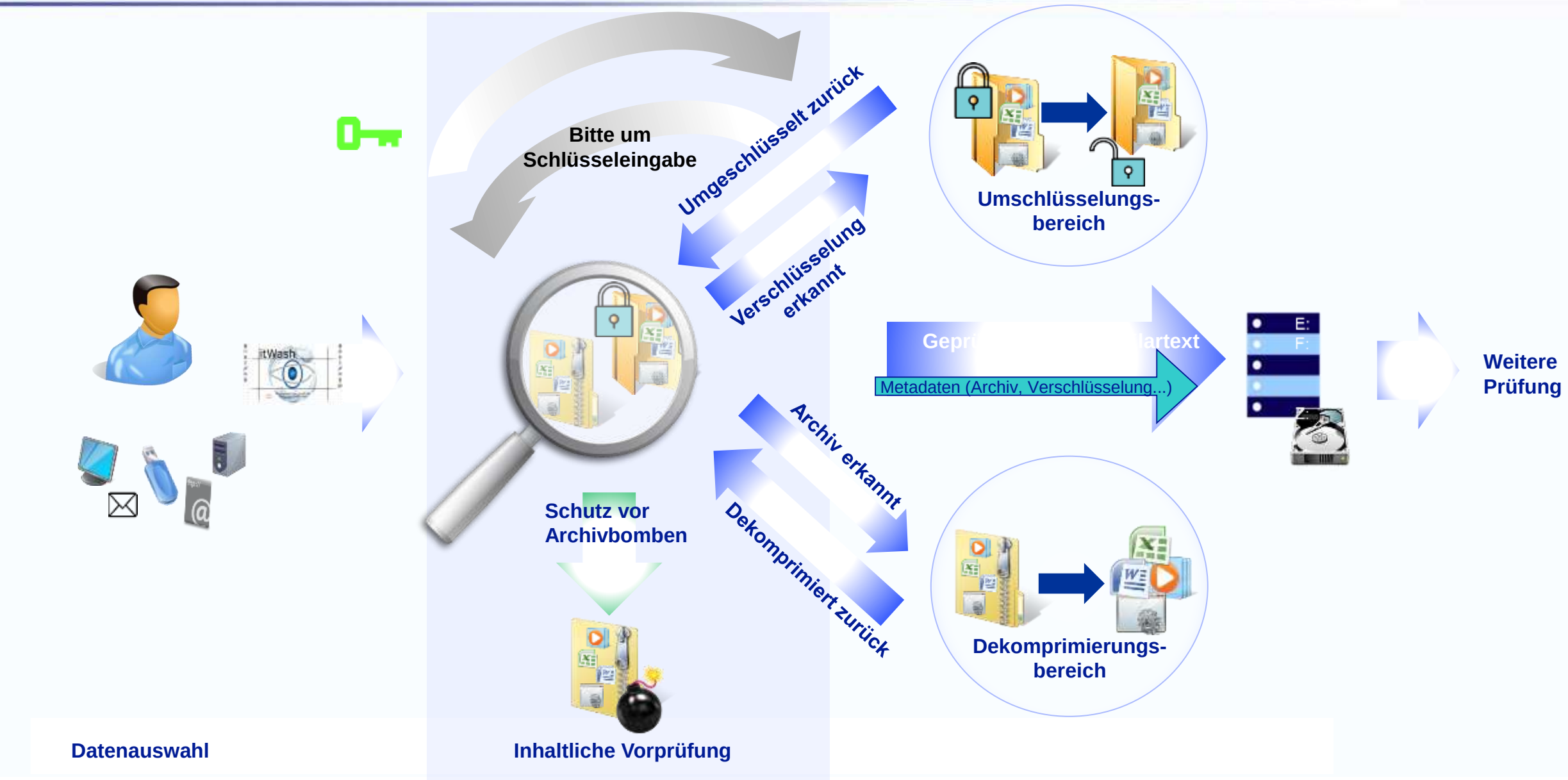
Wie geht 100% sichere Wäsche



Vergleich itWash – AntiVirus Lösungen

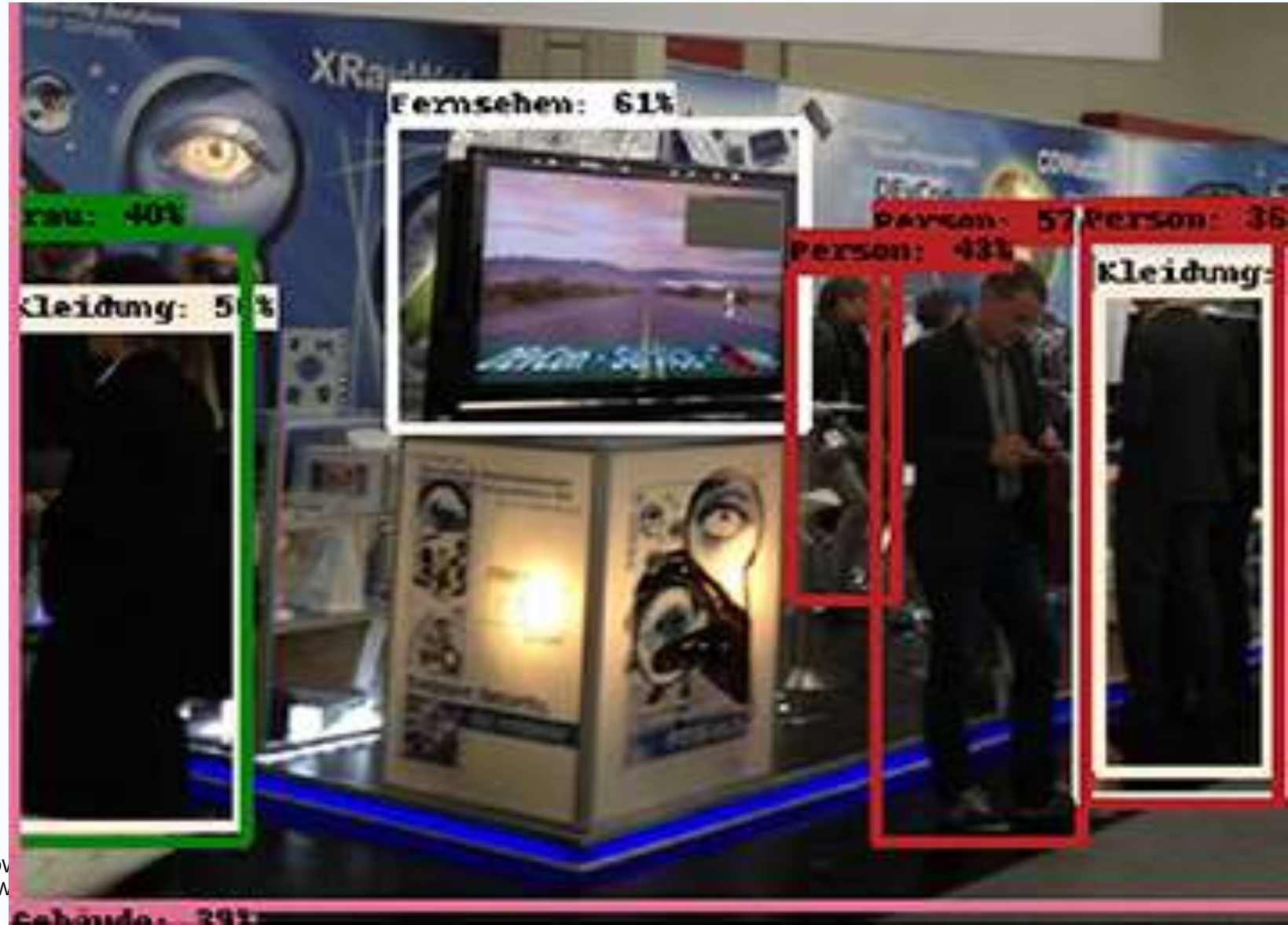
	itWash	Anti Virus	AV basierte Schleuse
Reinigung – Veränderung des Dokuments	✓	✗	✗
Herauswaschen aller ausführbaren eingebetteten Objekte	✓	✗	✗
Blocken von identifizierbaren bereits bekannten Pattern von Schadcode	✓	✓	✓
Archivbomben entdecken und davor schützen	✓	✗	?
Rollenbasierte Verarbeitungstemplates	✓	✗	✗
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	✓	✗	?

Der Mensch im Mittelpunkt



Plug-In Fähigkeit

- Automatische Anreicherung von Metadaten
  - itWash angereichert durch Bild- und Videoerkennung mittels KI von Drittherstellern als plug-In
  - Bilder und Videos verschlagworten
  - Anreichern von Metadaten zur Suche in Datenbanken
  - Beweissicherung
  - Priorisierung
  - Standardisierung



DeviceWatch, ApplicationWatch, XRayWatch, PDV
RiskWatch, MalWareTrap, Sichere Tastatur, LogOnW

Drittprodukte einfach einbinden

- Beliebige Drittprodukte - auch eigene Lösungen wie Skripte – können als „sicherer Prozess“ eingebunden werden

- Eigener Rechteraum für jedes Drittprodukt
  - Metadatenermittlung mittels KI
  - Konvertierung von Daten von IoT-Geräten verschiedener Hersteller auf genutzten Standard
  - Konvertierung von Foto und Video Daten auf genutzten Standard, um ohne die mitgelieferten Viewer auszukommen
  - Viewer können in einer unsicheren Umgebung ausgeführt werden

- Durch diese Architektur werden die „blinden Flecken“ von Anti-Viren-Programmen behoben – Erkennungsraten nahe an 100% (aber nur für bekannte Viren)

Workflowkomponente

- Zentrale – also an Fachverfahren angebundene – Schleusensysteme arbeiten mit einem konfigurierbaren Workflow: Z.B. Dublettenprüfung, Priorisierung, automatische Ermittlung der Zuständigkeiten …
- Die Art der Wäsche ist bspw. beim gleichen Dateityp unterschiedlich, wenn dieser Dateityp von unterschiedlichen Quellen kommt.
- Der Output und der auf dem Zieldatenträger gültige Zugriffsschutz ist algorithmisch im Workflow wählbar
- … ebenso die Art und Notwendigkeit der Beweissicherung
- Die Eingabedateien werden automatisch so konvertiert, dass sie standardisiert sind, so dass im Verarbeitungsprozess nur ein vordefinierter Dateityp verwendet wird.

itWash-Mail

Mails können verschlüsselt sein – erst auf dem Client liegt der Klartext vor
Nach der Entschlüsselung auf dem Client erfolgt die Wäsche!

- Attachments in Mails werden beim Doppelklick auf dem Arbeitsplatz entschlüsselt, gelöst und an die Datenwaschmaschine itWash geschickt
- Der Transport ist natürlich verschlüsselt
- In der Datenwaschmaschine itWash werden die Daten gewaschen
- Zurück kommt ein sauberes Dokument, welches direkt geöffnet wird
- Zur Minimierung der Anzahl der Datenwäschen werden vertrauenswürdige Maildomänen konfiguriert - interne Mails werden nicht gewaschen.
- Unterschiedliche Waschprogramme sind möglich
- Über die erfolgten Waschvorgänge wird ein Report erstellt und je nach Konfiguration dem Anwender angezeigt.

Management und Reporting I

itWash Managementserver decken viele Funktionsbereiche ab.

- Nutzungsart, Servicelevel, Mandantenfähigkeit etc. können unterschiedliche Funktionsbereiche auch auf unterschiedlichen Hardware-Komponenten in unterschiedlichen Netzen zur Verfügung stehen.
- Die Komponenten können virtualisiert betrieben werden.
- Die Definitionen der Zugriffsregelungen sind Bestandteil eines umfassenden Sicherheitskonzeptes.

- itWash-MS/DC
  zentraler Überblick über alle Ereignisse, Statusmeldungen und statistischen Analysen aller im Einsatz befindlichen itWash

Management und Reporting II

- 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/VPN (Virtual Private Network)
  Die verschiedenen VPN Nutzungsszenarien von itWash werden zentral gemanagt
  - Einbindung von itWash in die kundenseitige Infrastruktur
  - ggf. für den itWatch Remote Wartungszugang (je nach SLA)

- itWash-MS/Health Status
  Überwachung der Auslastung der verfügbaren Schleusenmodule

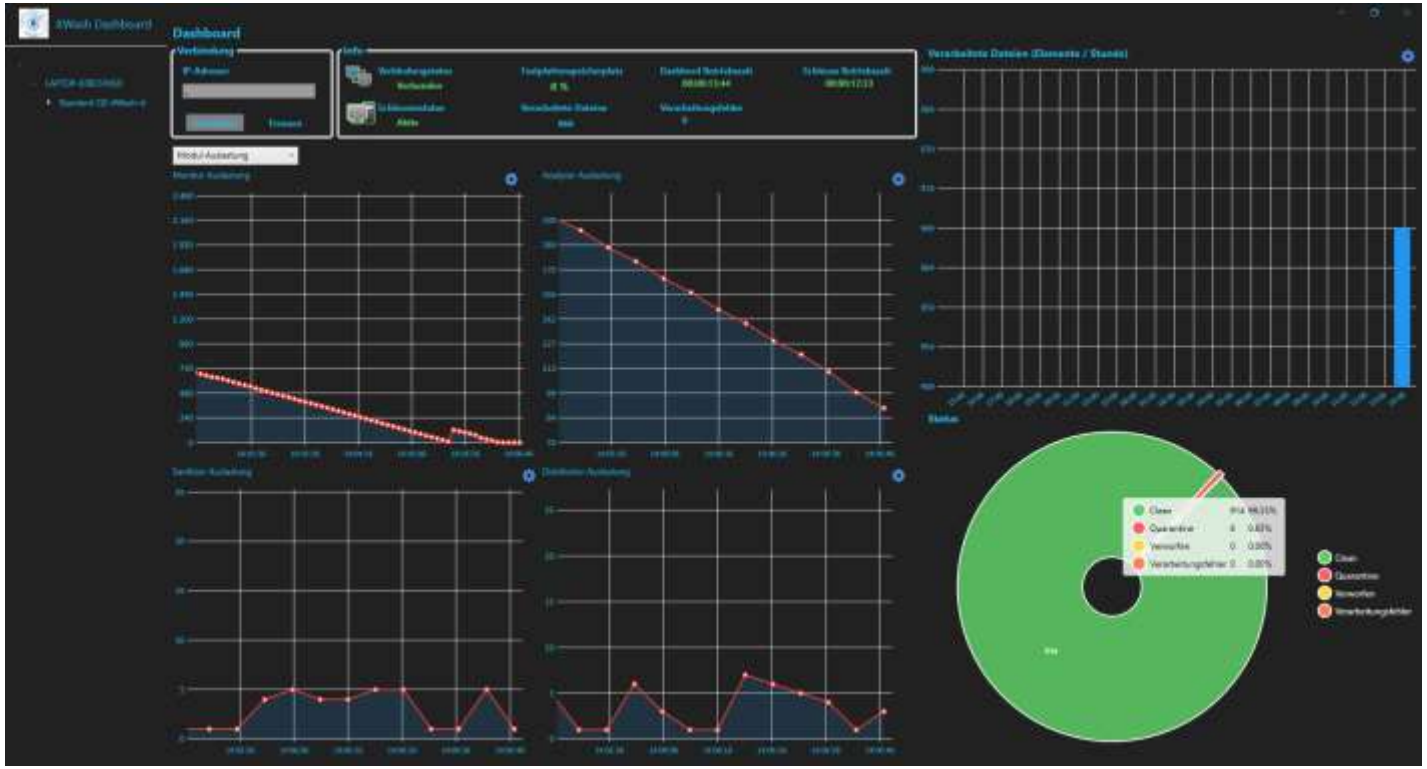
itWash FlowControl

FlowControl wurde insbesondere für das Schleusen und Waschen großer Datenmengen entwickelt

- ermöglicht flexibles, an Fachverfahren angebundenes Auftragsverarbeitungs-, Datenvolumen- und Datenträgermanagement aller „Waschaufträge“
- Quelle, Ziel, Priorität, Geheimhaltungsstufen und Rechte können konfiguriert werden
- Benachrichtigungsanforderungen können hinterlegt werden
- separierte Datenträgerverwaltung
- konfigurierbare Auftragserfassung
- Auftragsverwaltung zur Steuerung der Aufträge

itWash Dashboard

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



Fragen…

itWatch
Itsa 2022
Forum E – Halle 7A
Stand: 7A-108

Ramon.Moerl@itWatch.de