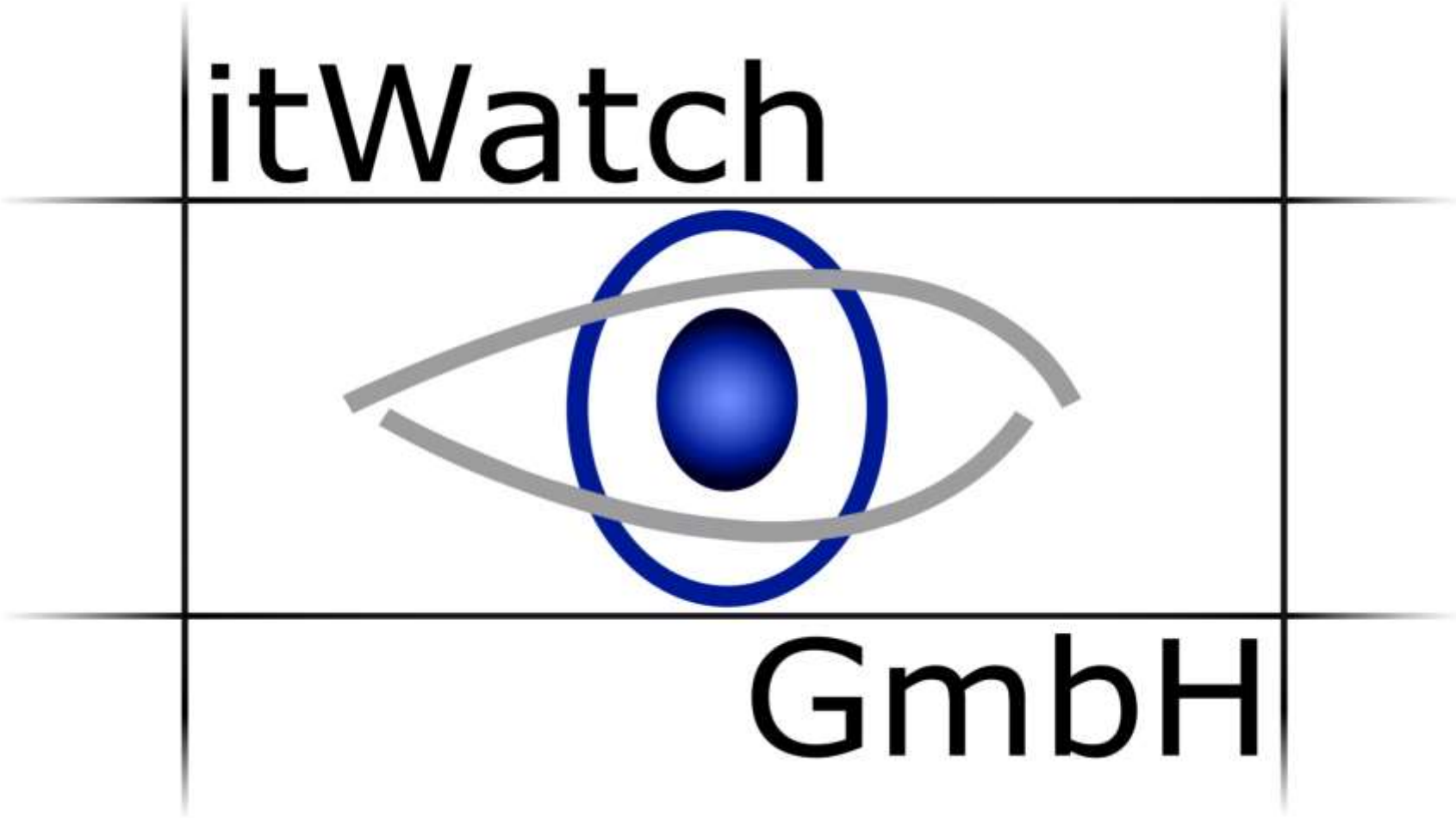
Ihre Sicherheit …
… unsere Mission



it-sa 2024

"Zero Trust als Idee und Digitale Souveränität als Ziel - reale Lösungen für die echten Herausforderungen“

23.10.2024 13 Uhr

Ramon Mörl, CEO itWatch GmbH

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

Über itWatch - Zahlen und Fakten

- Erste Produkte in 1997
- Produktherstellung in Deutschland ohne Zukauf
- Viele Millionen Lizenzen im Einsatz in allen KRITIS-Umgebungen – der Inneren und Äußeren Sicherheit
- Shareholder sind nur die verantwortlichen Geschäftsführer in Form von deutschen, juristischen und natürlichen Personen – kein Venture Kapital
- Vertrieb und Mehrwerte sowie Präsenz weltweit über Partner
- Produkte wurden vom BSI und anderen Sicherheitsorganisationen bis GEHEIM geprüft

Zero Trust – was bedeutet das?

- Niemandem vertrauen
- Ist das realistisch?
- Was muss man dafür tun, wenn man das ernst meint?

Stabile Vertrauensketten bilden

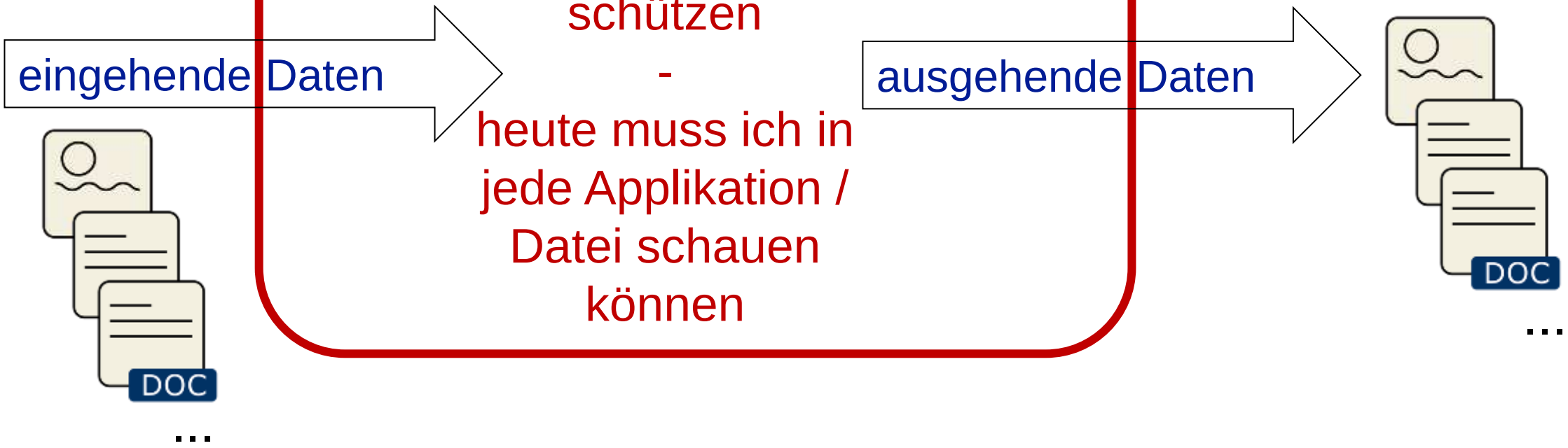
- Welches Vertrauen genießt mein Personal, die gekaufte Hardware, die genutzte Software, die Daten, die KI …
- Was ist eigentlich wichtig …

Vertrauensketten bewerten und bilden

- Personal – vertragliche Einbindung, ggf. mit Führungszeugnissen und Haftung unterlegen
- Partner und Lieferanten – vertragliche Einbindung mit Haftung unterlegen. Das gilt auch für Soft- und Hardware-Lieferanten – aber der Nachweis der Falschleistung ist nicht immer so einfach wie bei Crowdstrike.
- Unterscheidung der Vertrauensstellung
  - Direkte Netzeinbindung
- Datenlieferung / -austausch
  - Standardverfahren oder
    - Internetdownload
      - Verschlüsselt?
    - Mail, FTP, SFTP
    - Mobile Datenträger
  - Spezialverfahren – selbst implementierte / proprietäre Verfahren
  - Schutzversprechen auf der „anderen Seite“?

Richtungen des Datenaustauschs

Schadcode ist potentiell in jeder Datei, auch in **verschlüsselten**



Schutz vor Datenverlust (DLP)

Was brauchen die Nutzer?

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

Ein Arbeitsplatz in der Personalabteilung

- Da kommt eine Bewerbung: Putzpersonal
- E-Mail-Adresse ist „komisch“
- Text ist schlechtes Deutsch
- Bewerber sagt, er kommt aus der Ukraine
- Firmenrichtlinie sagt „nicht klicken“
- Das Unternehmensinteresse ist „Details ansehen“
- Die Lösung wäre „sicher klicken“ – wie geht das?

Wo verstecken sich Angriffe?

Jeder Angriff braucht etwas eingeschleusten Code.
Ausführbarer Code kann sich in unterschiedlicher Form an verschiedenen Orten verstecken:

- Eingebettete Objekte an beliebigen Stellen im Objekt
- Makros
- Nachladbare Objekte in Mails oder Browserinhalten
- Automatisch vom Betriebssystem (nach-)geladene Objekte
  z.B. lnk-Angriff
- Plugins in Anwendungen
- (Automatisch geladene) Patches
- Controller und Firmware (z.B. BadUSB)
- …

Vertrauen in Daten und ITK-Nutzung?

Man weiß nie, wo sich Angriffe verstecken!

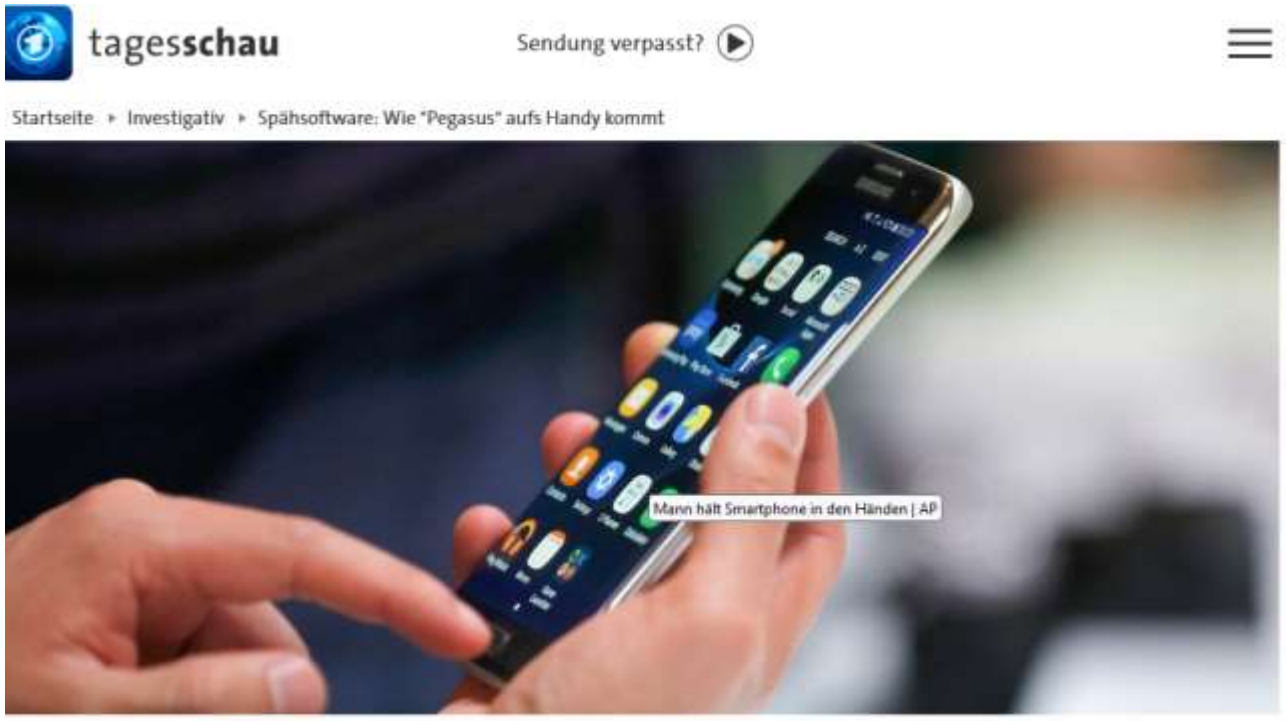
Cyberkriminelle nutzen KI und verstecken professionell!

Deshalb ist Digitale Souveränität das Ziel

Man kann mit ausgeschaltetem Handy abgehört werden!
Die Software dazu wird installiert ohne Kenntnis des Handybesitzers.

Die Software kann unbemerkt auf sämtliche Daten zugreifen und sie über das Internet versenden.
Pegasus lässt sich auf den meisten Geräten mit Android oder iOS aus der Ferne über das Internet installieren, ohne dass es der Besitzer merkt.

Das ist NICHT digital souverän



Hardwaretausch als Risikoreduktion

Kostenloser Austausch von Barracuda

Letzte Woche appellierte der Hersteller sogar, dass Admins attackierte Barracuda ESG sofort ersetzen müssen. Das automatisch verteilte Sicherheitsupdate funktioniert offensichtlich nicht wie gewünscht und der Hersteller rät dringend zum Austausch der attackierten Geräte. Der Austausch sollte nicht aus Kostengründen abgelehnt werden, denn Barracuda verspricht, allen kompromittierten Kunden neue Geräte kostenlos zur Verfügung zu stellen. Zudem empfiehlt der Hersteller, die eigenen Netzwerke eingehend auf eine eventuelle Verbreitung der Malware zu prüfen.

Zero-Day-Lücke in Barracudas ESG: Die Spur führt nach China

Angreifer haben etwa hochrangige Stellen in Hongkong und Taiwan ausspionieren wollen. Auf die Patches haben sie umgehend mit eigenen Gegenmaßnahmen reagiert.

Lesezeit: 3 Min. In Pocket speichern 25

(Bild: Herr Loeffler/Shutterstock.com)

16.06.2023 04:34 Uhr | Security

Von Frank Schröer

https://www.heise.de/news/Zero-Day-Luecke-in-Barracudas-ESG-Die-Spur-fuehrt-nach-China-9189409.html

Digital souveräne Infrastruktur?

Spion in der Wohnung

Wenn der Saugroboter zum Sicherheitsrisiko wird

t-online, AV-Test

Aktualisiert am 30.01.2019
Lesedauer: 7 Min.

Saugroboter von iRobot auf der IFA 2018: Praktische Haushaltshelfer oder Spion? (Quelle: imago-images-bilder)

Quelle:
https://www.t-online.de/digital/id_85170130/viele-saugroboter-spionieren-ihre-besitzer-aus.html

WARNUNG DER BUNDESNETZAGENTUR

Rauchmelder hört mit

VON HELMUT BÜNDER, DÜSSELDORF - AKTUALISIERT AM 21.12.2021 - 14:00

Harmlos wirkende Spielzeuge und Haushaltsgeräte haben oft Hintertüren. Verbraucher sollten auf verborgene Kameras und Mikros achten. 4600 Produkte wurden dieses Jahr schon aus dem Verkehr gezogen.

https://www.faz.net/aktuell/wirtschaft/unternehmen/rauchmelder-hoert-mit-warnung-der-bundesnetzagentur-17693994.html

Szenar Staubsauger-Roboter

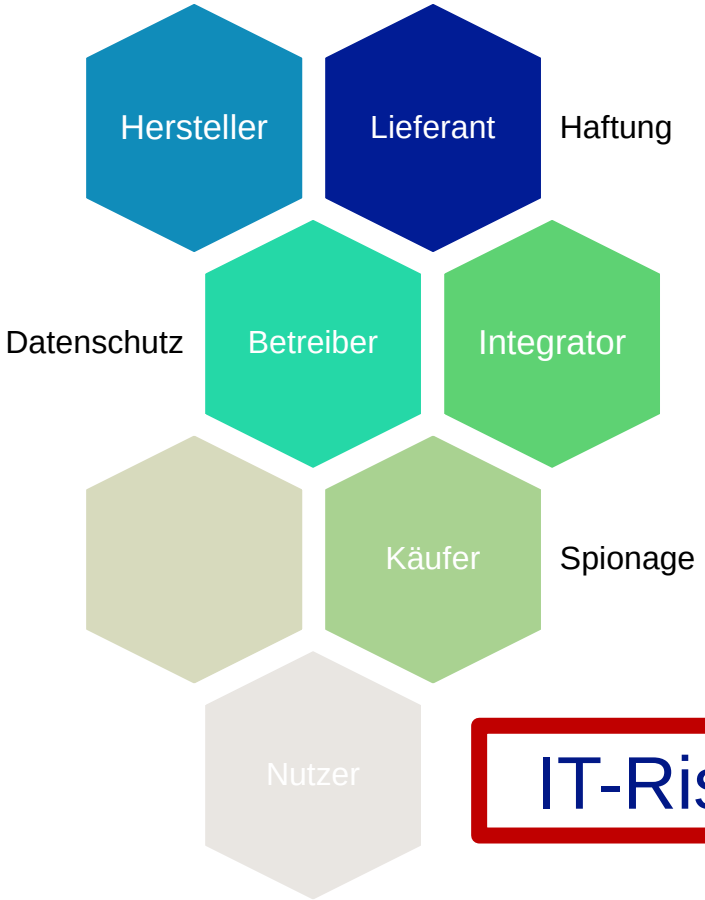
- Ein Hardwarelieferant kann also diese Audio- und Videofunktionen ohne Kenntnis des Herstellers in seine Hardware integrieren und die Kommunikationsinfrastruktur des Herstellers „nutzen“, um diese mit illegal gesammelten Daten im Zuge der wachsenden Datenökonomie gewinnbringend zu verkaufen.

- Durch diese Einnahmen kann der Hardwarehersteller besonders günstig – auch unter Herstellungspreis – anbieten.

Wie können der Hersteller des fertig integrierten Staubsaugerroboters, der Verkäufer, der Käufer, die Risiken des Produktes beurteilen?

Wer was warum wie beweisbar

Möglichkeit, Vorgaben an die Beteiligten zu stellen:



Wer bin ich?

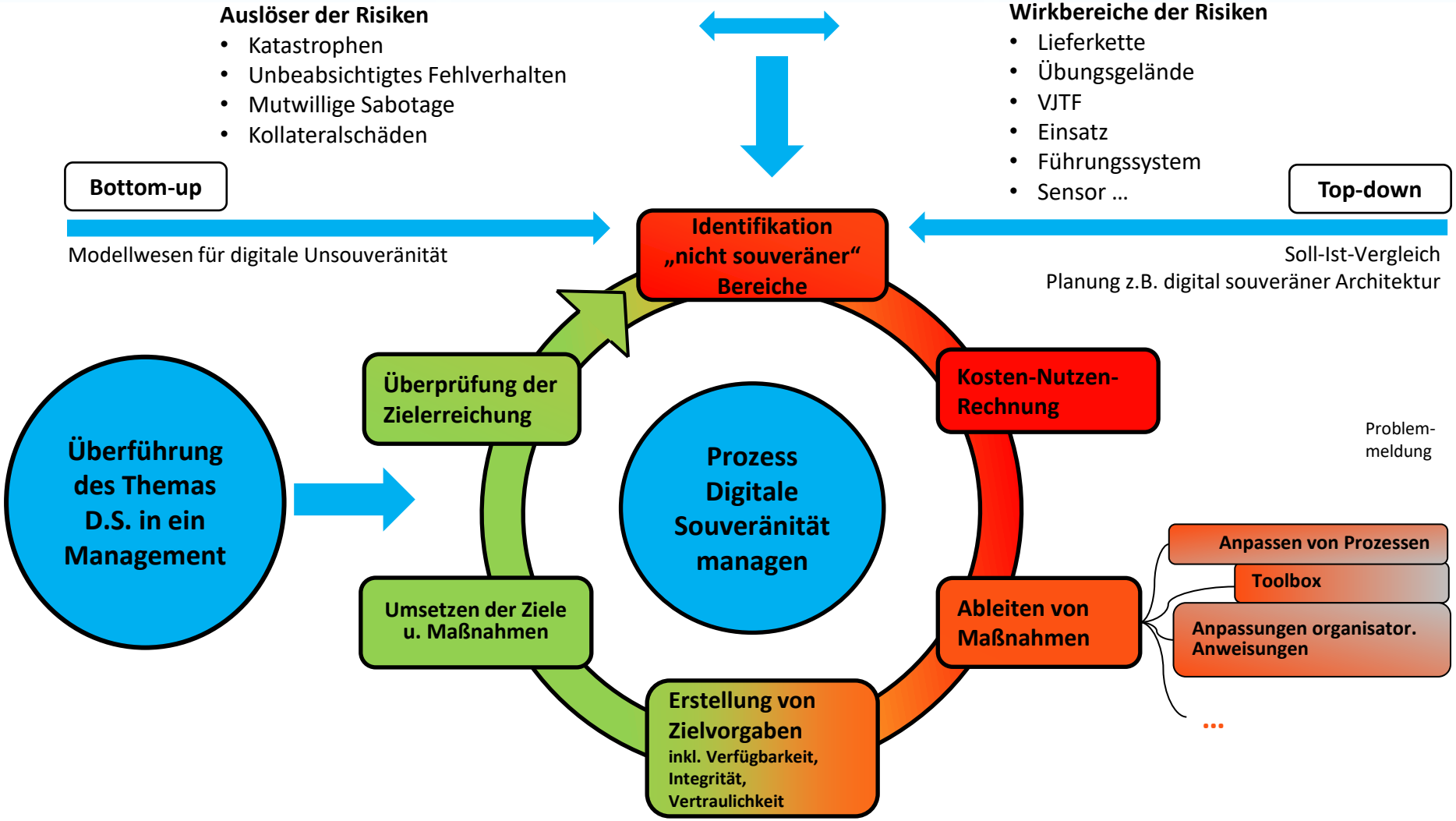
Welche IT-Risiken sind mit meinem Modul verbunden? Und wie habe ich diese mitigiert?

Als was handle ich?

Wie kann ich das „beweisen“

IT-Risiken Bottom-up aufsammeln

Selbstbestimmtes Handeln im Cyberraum



Vertrauen durch Sicherheitszonen

Anwender, HW, SW und Daten gleicher Sicherheits-klassen in die gleichen Zonen legen

Dann Daten unsicherer Herkunft bewerten

- **Mailattachments**
- **Downloads**
- **Mobile Datenträger**
- **Personalabteilung**
- Marketing
- Pressestelle
- Schadensbearbeitung und Meldestellen
- Vorträge und Inhalte von Partnern und Lieferanten
- IoT Devices, Smart Home Devices, Überwachungskameras
- Fernwartung
- OT und Übergang zu IT Remote Patching
- Behörden – Bürgerdaten – E-Government – OZG
- Patientendaten auf CD/DVD und Wearables
- Digitale Archive – digitale Asservate
- Unsichere Devices (BadUSB)
- Drehstuhl-Turnschuhschnittstellen für entnetzte Systeme
- ...

Und am Zonenübergang „Rauswaschen“

Im Kommentarfeld kann eine exe-Datei enthalten sein!

Canon EOS

2020:05:20 14:26:22

…..

…

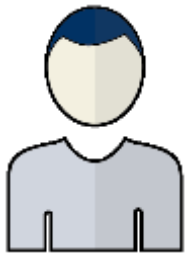
.

Antivirus genügt nicht

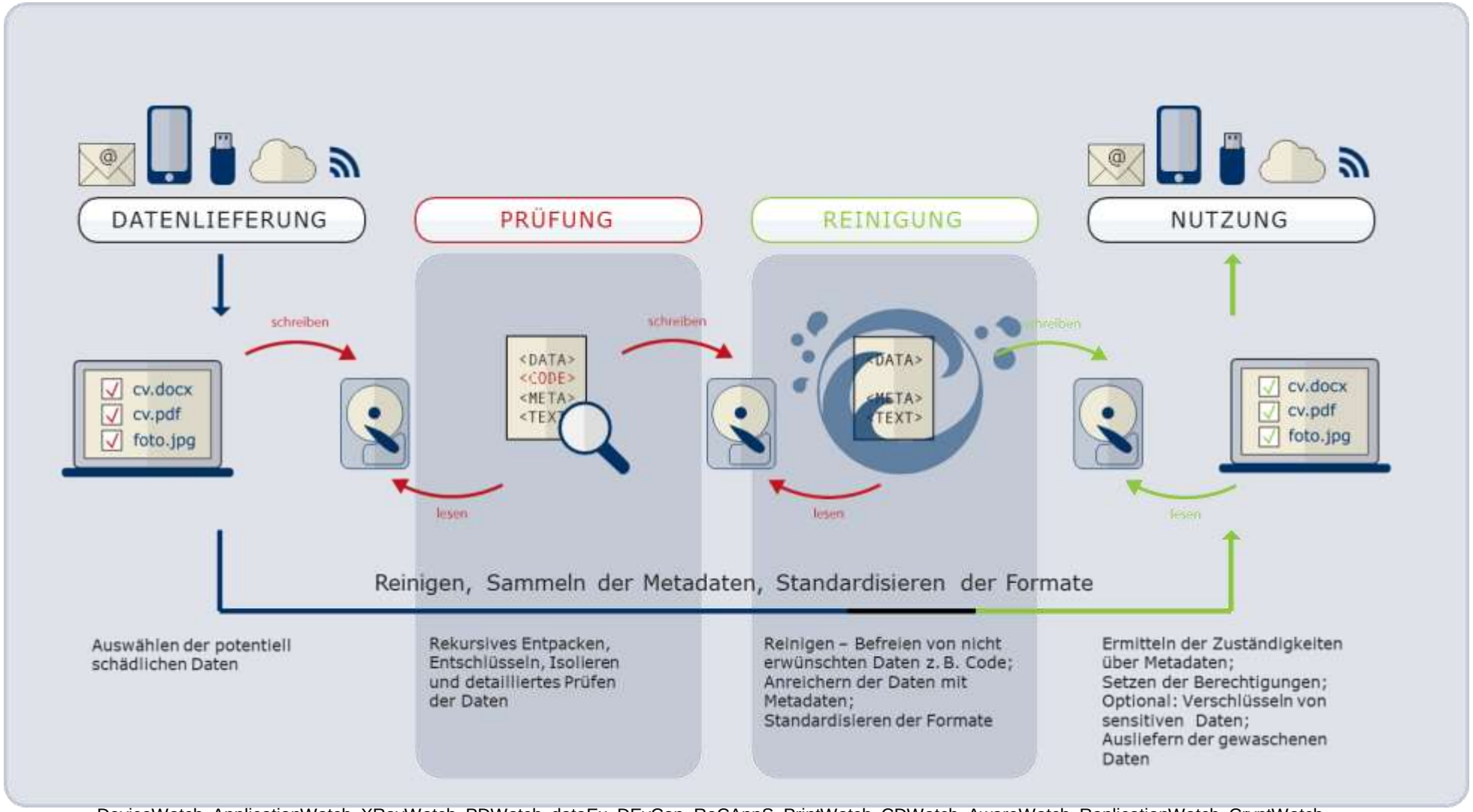
Unterschied zwischen Anti-Virus-Lösungen und itWash:

	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	✓	✗	?

Datenwäsche mit Netztrennung und Workflow



Lieferant



Nutzer

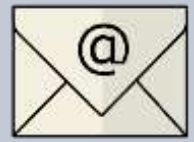
Nutzung von KI zur Fake-Erkennung

KI-basierte PRÜFUNG

Einlieferung der Inhalte (Bilder, Video, Voice, ...) z.B. aus OSINT, vom Bürger, der Kommune, dem XDR oder aus Fachverfahren

Inhaltliche Analyse, rekursives Entpacken und kontextabhängige Definition des Workflows

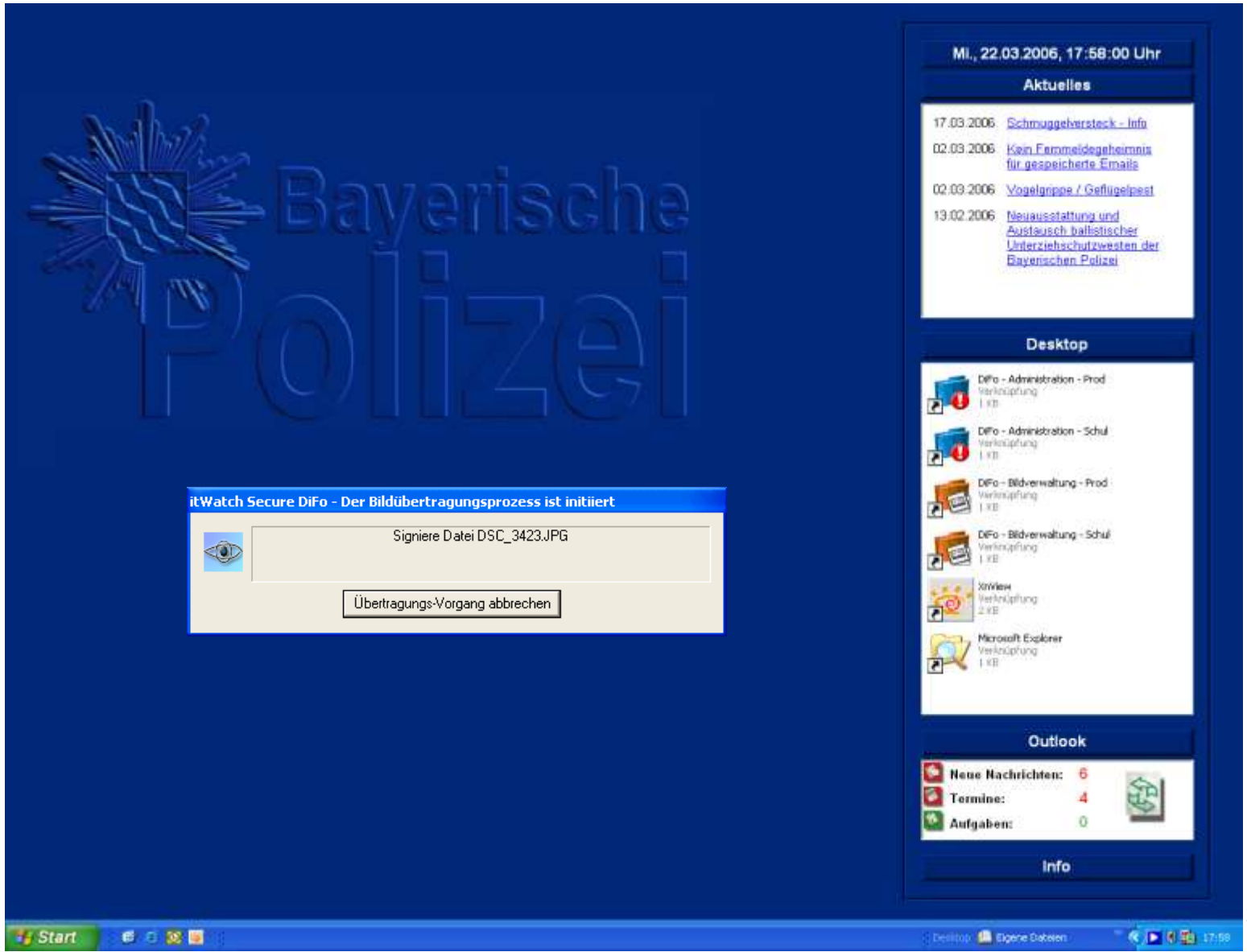
Verschlagwortung	Zuführen von	Vertextung von	Zuführen
und Anwendung	Bildern und Videos	Videos und	der
von KI	zur Analyse der Inhalte,	Sprachnachrichten,	Texte
zur Erkennung	zur Erkennung	OCR aus Bildern	zur
von	von Deep Fakes	und Verschlagwortung	Erkennung
Fakes	und Verschlagwortung	der Texte	von Fakes



Aufbereitung der Ergebnisse und Zustellung

Beispiel für eine Integration in Fachverfahren

Beispiel für eine Oberflächenintegration



itWatch-Produkte

DeviceWatch	Gerätekontrolle
ApplicationWatch	Applikationskontrolle
XRayWatch	Dateien, Inhalte blockieren & auditieren
PDWatch	Verschlüsselung mobil, lokal und zentral
CDWatch	Medienbasierter Schutz
DEvCon	Kaskadierende Device Event Konsole
ReCAppS	Virtuelle Schleuse
DataEx	Sicher löschen und formatieren

PrintWatch	DLP-Kontrolle über gedruckte Dokumente
AwareWatch	Security Awareness in Echtzeit
ReplicationWatch	Sichere Datenreplikation
RiskWatch	Risikoidentifikation auf Knopfdruck
LogOnWatch	Sicheres Microsoft Login – geschützt gegen Ausspähen
MalWareTrap	APT erkennen & isolieren

Die **itWESS** - ein einziger Cyber Defense Agent!

Datenschleuse mit Datenwäsche

www.itwash.de

CryptWatch	HW-Verschlüsselung
Sichere Tastatur	Vollständige Lösung BadUSB
Private Data Room	Geschützter Datenraum
itWESS2Go	Mobilitätslösung für alle Sicherheitsklassen

Produktübersicht zum Download

Fragen…

Besuchen Sie auch gerne unseren itWatch-Stand

Halle 9
Stand 247

Ramon.Moerl@itWatch.de