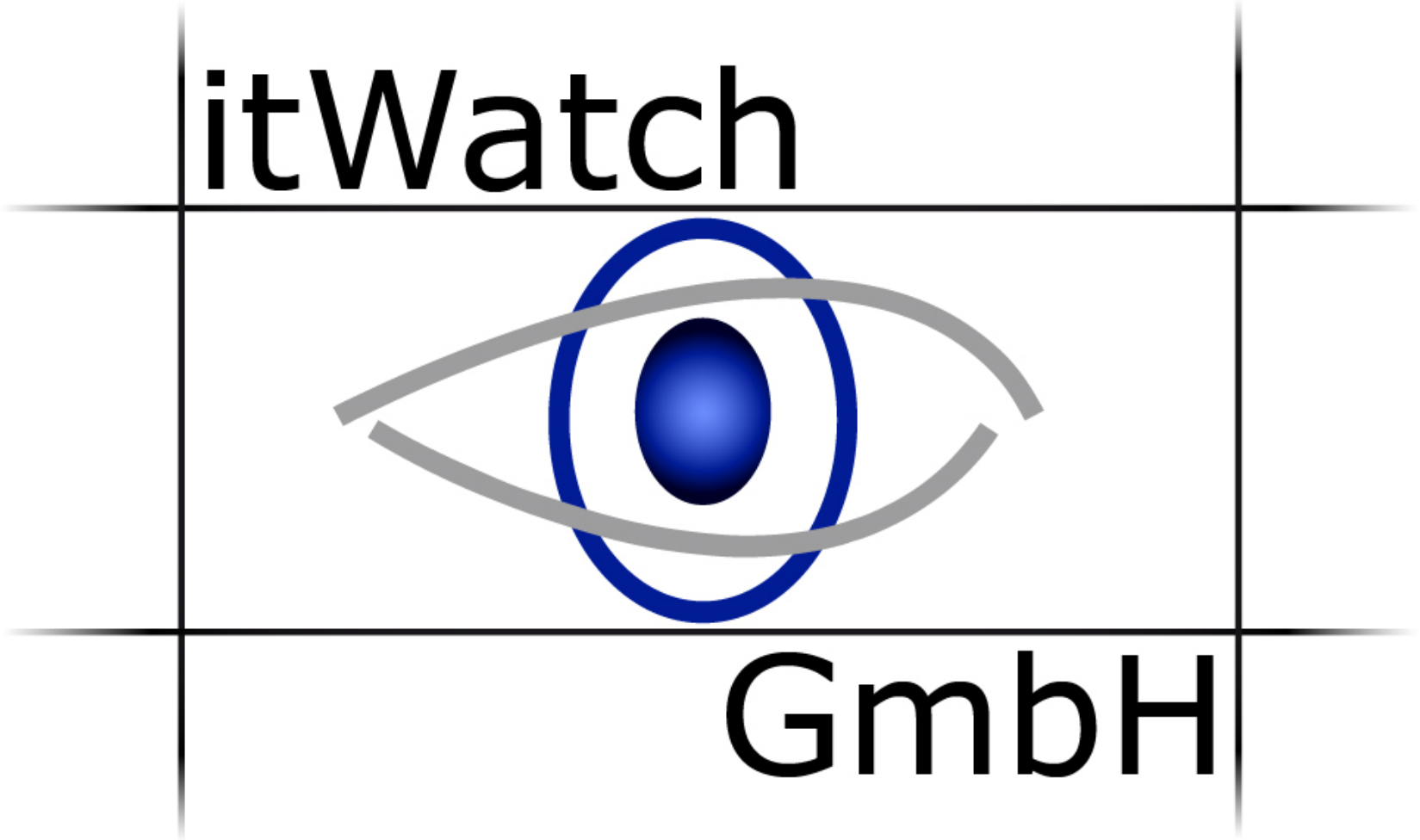
Ihre Sicherheit …
… unsere Mission



Digitale Souveränität und die Einschätzung der Sicherheit von Lieferketten – eine Managementdisziplin

Problembeschreibung und Lösungsansätze

Webinar-Reihe IT-Sicherheit 2. Staffel
Mittwoch, 22.03.2023
10.00 – 11.00 Uhr
Ramon Mörl | itWatch GmbH

IHK Industrie- und Handelskammer Nürnberg für Mittelfranken
VERANTWORTUNG SEIT 1843

Bayerisches Staatsministerium für Digitales

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

Ist ein Handy aus, wenn man es ausschaltet?

NACHRICHTEN ZUM THEMA
PEGASUS

Spähsoftware Predator

Griechenlands "Watergate"-Skandal

11.10.2022 - 11:36 Uhr

Ein griechischer Oppositionspolitiker und ein Journalist wurden mit einer Spionagesoftware abgehört. Die Regierung streitet jede Beteiligung ab - doch es gibt Verbindungen zwischen ihr und der Firma, die die Spähsoftware vertreibt. *Von Verena Schälter.*

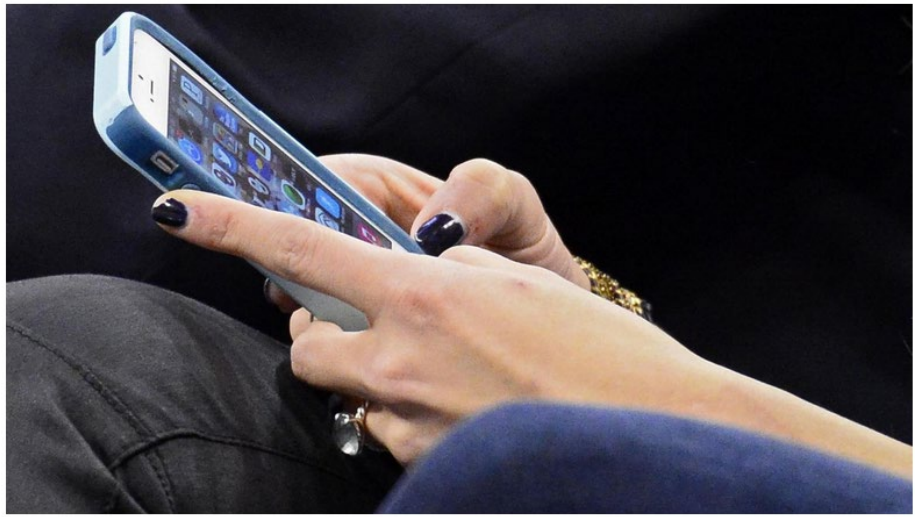
Spionage-Software

Alles Wissenswerte zum Pegasus-Trojaner

Der mexikanische Präsident, ungarische Investigativjournalisten, indische Oppositionelle – unter anderem ihre Smartphones sollen mit der Spionage-Software Pegasus überwacht worden sein. Weltweit sind mehrere tausend Personen betroffen. Ein Überblick.

20.07.2021

Hören 05:06 | Audio herunterladen



Ein Schutz vor der Spionage-Software Pegasus ist kaum möglich (dpa/picture alliance/Larry W. Smith)

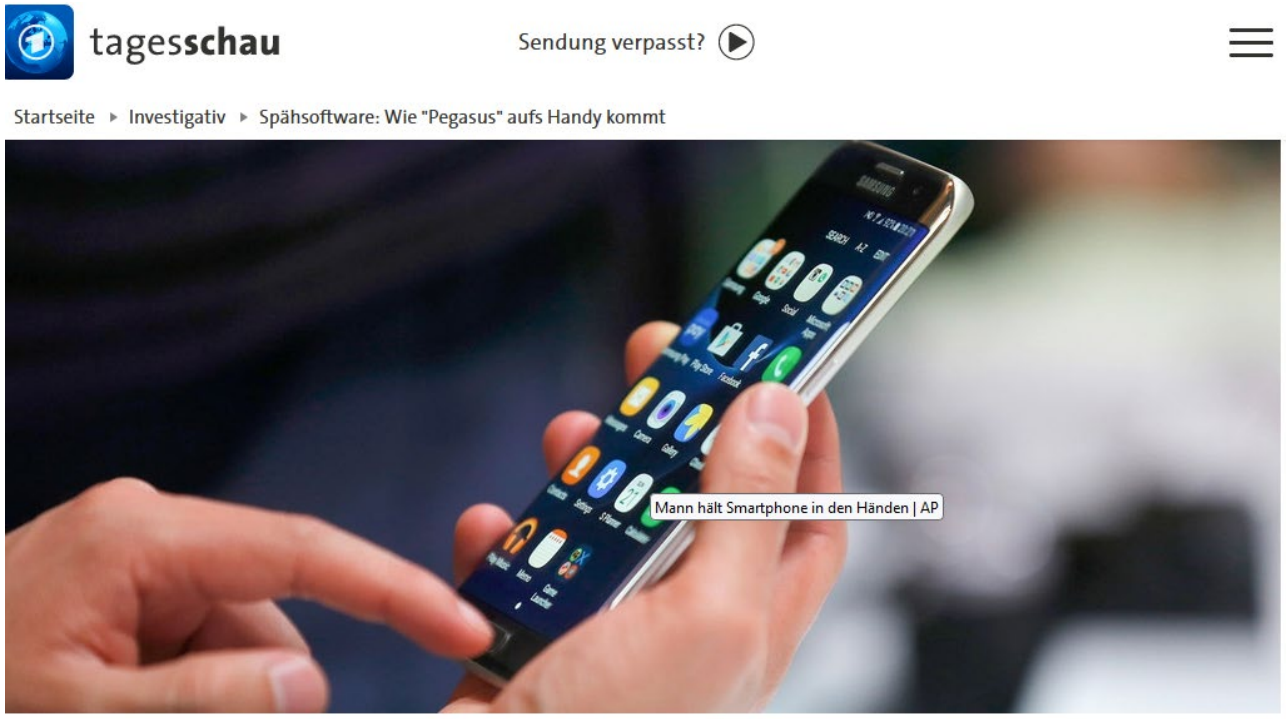
https://www.tagesschau.de/investigativ/ndr-wdr/spaeh-software-pegasus-smartphone-101.html
https://www.deutschlandfunk.de/spionage-software-alles-wissenswerte-zum-pegasus-trojaner-100.html

Was ist digitale Souveränität?

Man kann mit ausgeschaltetem Handy abgehört werden!
Die Software dazu 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



Sicherheitsfeatures verhindern polizeilichen Einsatz

Elektrofahrzeug wurde für polizeilichen Einsatz gekauft:

Quelle: de .motor1.com

- Geliefert
- AGB gehen an legal zur Freigabe
- Legal sagt:
  In den AGB steht, dass die Mikrofone im Fahrzeug durch den Hersteller aktiviert werden können, ohne dass die Insassen informiert werden
- Fahrzeug bleibt in der Garage
- **… weil die Vertraulichkeit der Kommunikation im Fahrzeug nicht souverän / selbstentschieden zu steuern ist**

Vertrauensketten und Fachkräftemangel

Cyber Security im Auto der Zukunft:

- Viele einzelne Sicherheitselemente sind im Auto der Zukunft nötig

- Frage an einen Hersteller:
  - Wie geht Ihr Haus mit der Entscheidung zu „make or buy“ um?
- Antwort:
  - Wir machen alles selbst sonst wäre es nicht sicher

- Unterschiedliche Verständniswelt zu „sicher“ – die souveräne Entscheidung wird höher priorisiert als die Nutzung der globalen Community

Ursula von der Leyen 2017

Meine IoT Devices

Die Fähigkeiten der Bundeswehr und das dazu benötigte Material kosten viele Milliarden Euro.

Die Nutzung dieser Fähigkeiten sind fast vollständig von der in den Systemen integrierten IT abhängig.

Dazu wird benötigt:
Souveränität über alle (wesentlichen) IT-Komponenten während des gesamten Nutzungsprozesses

IT-Komplexität in der Autoindustrie beherrschbar?

Quelle: Tesla: Sicherheitslücke entdeckt - 19-jähriger Bayer hackt sich in über 20 E-Autos (merkur.de)

Startseite › Wirtschaft

Tesla: Gefährliche Sicherheitslücke - 19-jähriger Bayer hackt sich in über 20 E-Autos

Erstellt: 26.01.2022, 21:58 Uhr
Von: Patricia Huber

So gefährlich war diese Lücke nicht, aber:

- Entertainment
- Fahrzeugsteuerung
- Monitoringdaten
- Predictive Maintenance
- Car2Car
- Softwareupdates over Air
- … alles auf einem Kabelbaum

Sinnhafte Regulierung hatte 100 Jahre Zeit

Autofahren 1917

Kein Führerschein, aber eigene Tankstelle

… und vorsicht der Daumen

James Dean – „East of Eden“ (1955)

Autofahren 2007

Start des Autos remote für Notfälle als Service des Herstellers

Bruce Willis – „ Stirb langsam 4.0“ (2007)

Autofahren 1917

Kein Führerschein, aber eigene Tankstelle

James Dean – „East of Eden“ (1955)

”East of Eden (1955) . Google Play . Abgerufen am 23.11.2016. CREDITS: TM & © Warner Bros. (1955).

Autofahren 2007 teil-digitalisiert

Bruce Willis – „ Stirb langsam 4.0“ (2007)

(2007): *Stirb langsam 4.0*. USA: Michael Fottrell.

Autofahren 2007 teil-digitalisiert

Bruce Willis – „ Stirb langsam 4.0“ (2007)

(2007): *Stirb langsam 4.0*. USA: Michael Fottrell.

Angriff auf die Lieferkette

SUCHE Spektrum.de MAGAZINE | ARCHIV | ABO/SHOP | SERVICE |

ASTRONOMIE | BIOLOGIE | CHEMIE | ERDE/UMWELT | IT/TECH | KULTUR | MATHEMATIK | MEDIZIN | PHYSIK | PSYCHOLOGIE/HIRNFORSCHUNG

Startseite » IT/Tech » SolarWinds: Ein Hackerangriff, der um die Welt geht

Um sich diesen Artikel anzuhören, melden Sie sich bitte an.

Hintergrund
15.01.2021
Lesedauer ca. 7 Minuten
Drucken
Teilen

SOLARWINDS-HACK

Ein Hackerangriff, der um die Welt geht

Der Angriff auf das Unternehmen SolarWinds gilt als größter Hack seit Jahren. Zehntausende Firmen könnten betroffen sein. Um was geht es, wie gefährlich ist es und wie kann man sich schützen? Antworten auf die wichtigsten Fragen.

von Eike Kühl

SolarWinds: Ein Hackerangriff, der um die Welt geht - Spektrum der Wissenschaft

- Alle Opfer nutzten die gleiche Softwareplattform
- Über ein kompromittierendes Update konnten die Angreifer eine Hintertür nutzen und Schadsoftware einschleusen
- Jemand hatte sich in der Lieferkette eingeschlichen und schädlichen Code ohne Wissen des Unternehmens eingebracht.

https://www.spiegel.de/netzwelt/netzpolitik/solarwinds-hack-der-spionagefall-des-jahres-a-0b728cc4-d375-4cb9-9450-3635ca8172a0

Andere Fälle betreffen Open Source

- Heartbleed
  - Ein Problem in einer sehr häufig genutzten Implementierung des SSL Stacks ermöglichte es unberechtigten Dritten die Session zu übernehmen
  - Das Problem: niemand wusste in welchen zugelieferten Produkten diese Open Source Lösung in welcher Version verbaut war
- Log4j
  - Ein Problem in einer sehr häufig genutzten Open Source Monitoring Lösung ermöglichte es unberechtigten Dritten von außen einzudringen
  - Das Problem: niemand wusste in welchen zugelieferten Produkten diese Open Source Lösung in welcher Version verbaut war
- Die offene Frage: wer kann beurteilen ob in einem IT-Element Hintertüren eingebaut sind?

versteckter Schadcode – Bsp.: JPG

Im Kommentarfeld kann exe-Datei enthalten sein!

Metadaten:

Canon EOS

2020:05:20 14:26:22

.....

...

.

Ja

Wo ist der Angriff versteckt?

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
- Plug-In in Anwendungen
- (Automatisch geladene) Patches
- Controller und Firmware (z.B. BadUSB)
- …

Wer kann gut und böse unterscheiden?

itWatch GmbH

Die Problematik

Man weiß nie, wo sich Angreifer verstecken!

Souverän über den ganzen Lebenszyklus

Lifecycle von Sicherheitseigenschaften digitaler Produkte

Entwickler

Schutz der Entwicklungsumgebung

Security by Design
Privacy by Design

itWatch GmbH

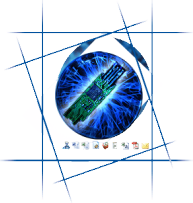
Sichere digitale Transformation

PD Watch - Verschlüsselung

Sicherheit der Produktionsumgebung

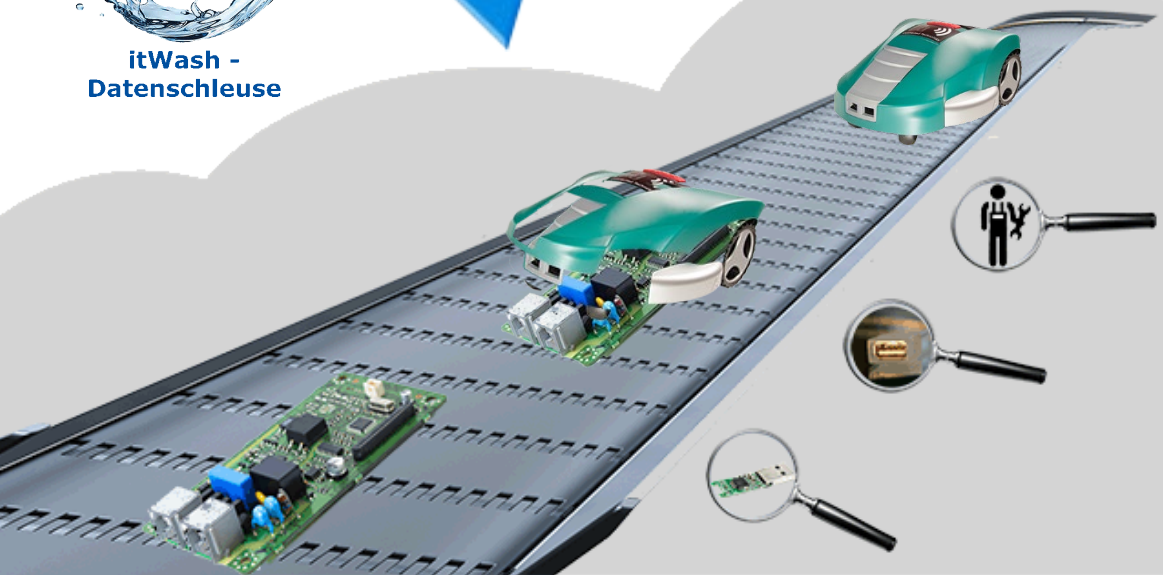
Security as Infrastructure

ApplicationWatch - Applikationskontrolle



XRayWatch - Contentkontrolle

itWash - Datenschleuse



Sicherheitszone Produktion

Sicherheitszone Produkt im Betrieb

Warum ist die Lieferkette so wichtig?

- Ist das Auto der Zukunft
  Software auf Rädern
  oder
  ein traditionelles **Auto mit immer mehr Software**

- In einem modernen Auto sind über 100 CPUs verbaut, intern vernetzt und z.T. über verschiedene Kommunikationswege mit der Außenwelt in Echtzeit verbunden.

- Hintertüren – mögliche Angriffe schlagen schnell auf alle Komponenten und das ganze Fahrzeug durch

Wenn der Hersteller des KFZ nicht alle Bauteile kennt, kann er das Risiko für den Käufer und Fahrer nicht einschätzen.

Die Konsequenzen

- Um die Risiken erkennen und vermeiden zu können, die durch Lieferketten entstehen, muss man verstehen
  - welche IT-Komponenten enthalten sind
  - wie diese aktualisiert oder durch andere Mechanismen verändert werden können,
  - sei es geplant, durch Angriff oder Fehlverhalten
- Ziel
  - Bekannt gewordene Risiken transparent kommunizieren
  - die Risiken muss man nicht nur für sich selbst, sondern auch für die Nutzer der Endprodukte und die eventuell in der Lieferkette nachfolgenden Organisationen einschätzen können bzw. das Risiko transparent machen

Vollständige Komponentenliste über die Lieferkette

- Am einfachsten ist das natürlich über Regulierung und Verträge zu gewährleisten. Die Fleischskandale der Vergangenheit haben ja auch dazu geführt, dass alle Bestandteile, Herkunft und Werdegang jeder Currywurst nachvollzogen werden kann – weil es deutlich sichtbar um die Gesundheit von Menschen ging.

- Die Ziele der Beteiligten in allen Unternehmen in der Lieferkette und der Nutzer beim Umgang mit den technischen Geräten und dem Verständnis was „Cyber Security“ ist, sind divergent und stehen sich teilweise entgegen.

- Die Diskussion „ob“, „wie“ „wo ja“ „wo nein“ „wie richtig“ wird emotional und an einzelnen meist statischen Themen z.T. sehr technisch geführt – und endet oft in Frustration.

- Sinnvoll wäre es, die Interessen aller Beteiligten, benötigte Vorgehensmodelle und Werkzeuge zur Umsetzung des erwünschten Schutzes und den Wille zur Kooperation in das allgemeine Bewusstsein zu bringen und dann gemeinsam danach zu handeln.

Das Ziel: Einen Beitrag zum kooperativen Umgang zu leisten.

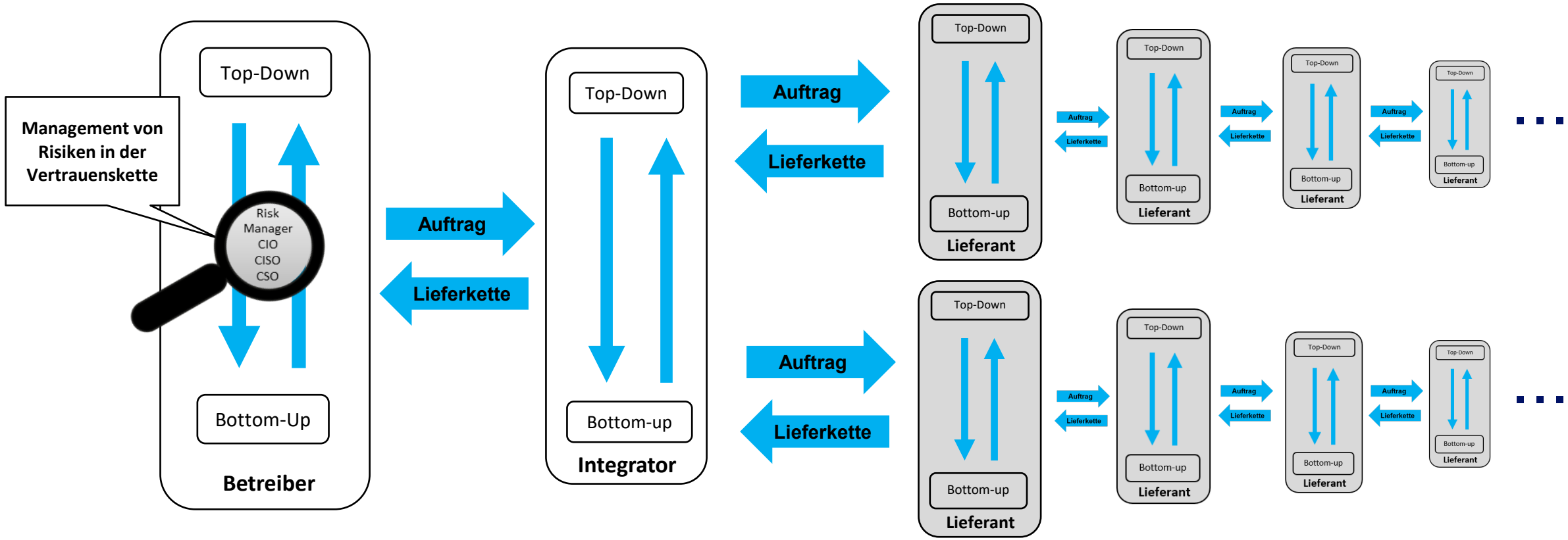
Die Probleme in der Herstellung

- Time to market
- Verfügbarkeit steht orthogonal auf den Zielen Vertraulichkeit und Integrität
  - Bsp: 2 Firewalls
  - Parallel erhöhen sie die Verfügbarkeit verringern aber Vertraulichkeit und Integrität
  - In Serie verringern sie die Verfügbarkeit erhöhen aber Vertraulichkeit und Integrität
- Vertraulichkeit durch Verschlüsselung
  - Wer hat den Schlüssel?
  - Wer kann ihn wie bekommen?
- Betriebssysteme haben meistens nicht das Hauptziel „Security“. Embedded ist das Hauptziel meist Verfügbarkeit.
- Nutzung: wie genau kann der Hersteller eines Chips und der Programmierer des Controllers auf dem Chip verstehen wofür der Chip genau verwendet wird
  - Insulinpumpe
  - Nicht vernetzte Kaffeemaschine

Datenökonomie und Beschaffung

- Wir kaufen für verschiedene Geräte einen Bluetooth Chip – Stückzahl mehrere Millionen; Staubsaugerroboter, Kaffeemaschinen, Heizungen …
  Ziel: die Steuerung über Apps direkt über BT Kontakt
- Die Beschaffung findet standardmäßig über eine Ausschreibung statt in der bei den angefragten Funktionalitäten der beste Preis das Zuschlagskriterium bildet.
- Ein Hersteller verbaut in seinem BT Chip weitere nicht veröffentlichte Funktionen:
  - Sensoren, Audiofähigkeiten
  - Remote Updatefähigkeit, um neue Funktionen nachzuladen
  - Funktionen zum Ausleiten von lokalen Daten, die zur Fehler-Diagnose benötigt werden
- Der BT Chip ist über die lokal verfügbaren Stromzugänge „always on“
- Der Hersteller des BT Chips kann über den Verkauf der ausgeleiteten Daten mehr verdienen als mit dem eigentlichen Produkt

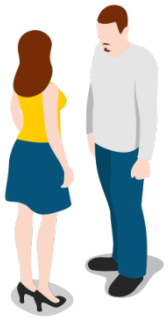
… und das über die ganze Lieferkette



V E R T R A U E N S K E T T E

Integrität – Verfügbarkeit – Vertraulichkeit – Robustheit der Schutzziele - Vertrauenswürdigkeit - Zukunftsfähigkeit

… und in jedem Unternehmen Silodenken vs. Querschnittlicher Notwendigkeit von Security



CEO

CSO

CIO

IoT Produktion

IoT Produkte

Werkschutz

CISO

CSO

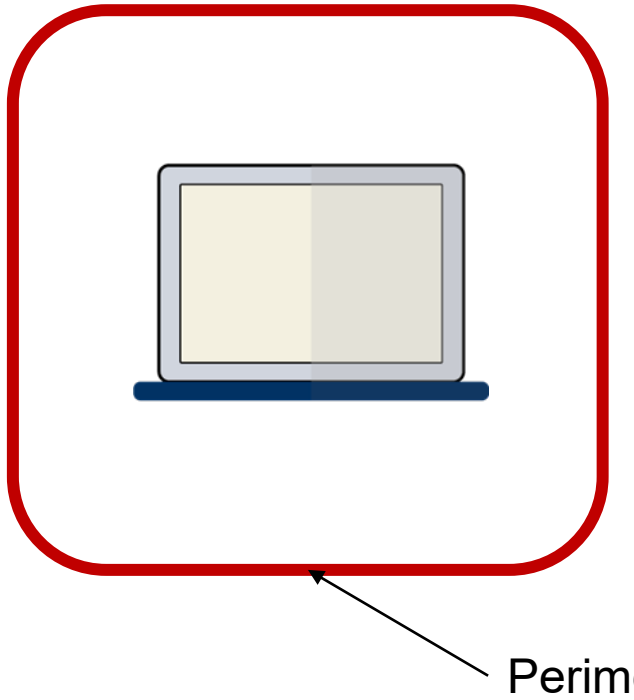
CSO

Zuerst: Jede Abteilung handelt für sich

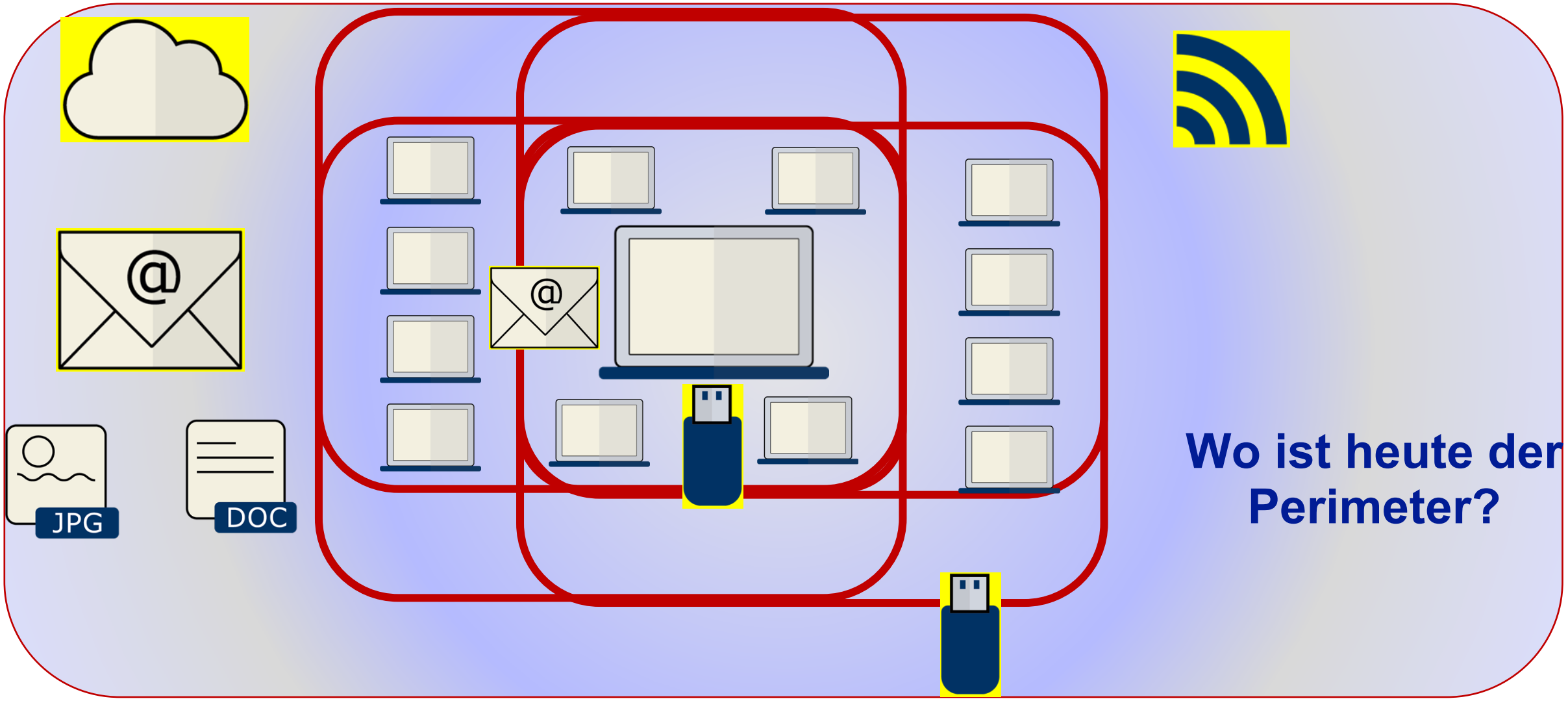
Vertrauenskette schaffen

Ist in dieser Struktur zielgerichtete fachübergreifende Zusammenarbeit für das querschnittliche Thema Cyber Security möglich?

Früher, als alles noch gut war ... ;-)



Heute ist es etwas komplexer ...



Heute ist es etwas komplexer ...

- Perimeter:
  also der Ort wo sich fremde Information / Netzübergänge und eigene treffen
  wandert in modernen Umgebungen an die verschiedensten Orte …
  wobei „Orte“ im Cyber Raum nicht so genau definiert ist.

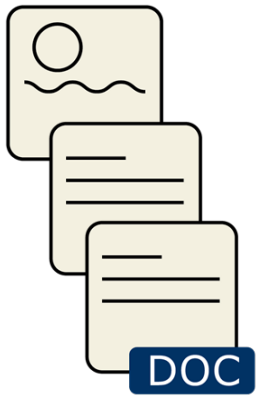
- Auf jeden Fall müssen verschlüsselte Daten immer im Klartext inspiziert werden – also liegt der Perimeter beim „Schreibvorgang“ der entschlüsselnden Anwendung

- Bei der technischen Umsetzung von IT Sicherheit geht es im Wesentlichen um zwei Themen
  - Was kommt rein (bitte kein Schadcode)
  - Was geht raus –
    - hoffentlich nicht meine Firmengeheimnisse
    - Und nichts was meine Partnerunternehmen mit Schadcode infiltriert

Die unterschiedlichen Dimensionen

Schadcode ist potentiell in jeder Datei

eingehende Daten



...

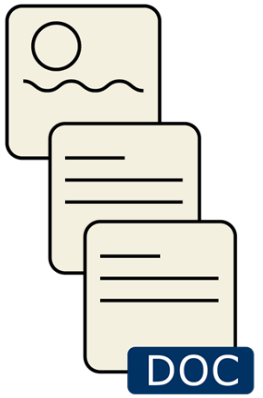
heute reicht es nicht mehr, das Netz zu schützen

-

heute muss ich in jede Applikation / Datei schauen können

ausgehende Daten

Schutz vor Datenverlust (DLP)



...

… und die Luftschnittstelle?

Was passiert, wenn eine Hintertür in einer Hardware eine nicht dokumentierte Luftschnittstelle anbietet

Sicherheit trotz Fachkräftemangel

- Der Fachkräftemangel führt dazu, dass für die Sicherstellung der IT-Security benötigtes Personal immer schwerer zu akquirieren ist.
- Auf der anderen Seite ist „hacken“ zu einem Geschäftsmodell geworden und zum größten Teil ökonomisch motiviert.
- Die Interessen der Beteiligten in der Verteidigung im Cyber Informationsraum sind divergent und stehen sich teilweise entgegen.

Security by Design
Privacy by Design
… ohne Fachkräfte?

Design against Crime

itWatch GmbH

Das Ziel

Mögliche Lösung: IT-Security als Infrastruktur

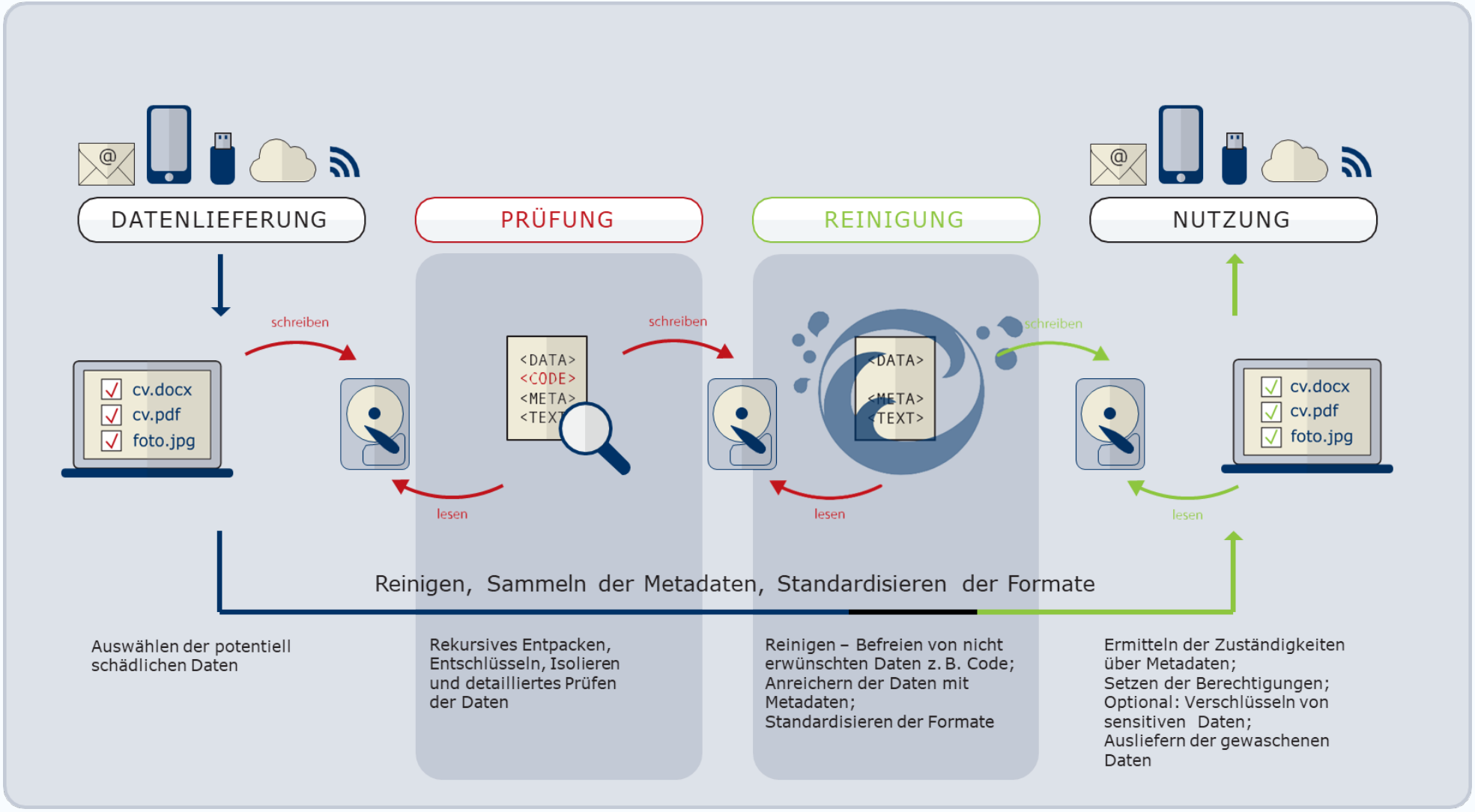
- Organisatorische Einbettung, juristische Unabhängigkeit technisch best of the breed
- Produkte
  - praktische Erfahrungen
  - Installation
  - Roll-out
  - Anfangskonfiguration
  - Betriebskonzept
- Integration mit verschiedenen sinnhafte Lösungen im partnerschaftlichen Modell
- Erfahrungsdatenbank über Querwirkungen mit branchentypischen Fachverfahren
- User Groups zum Austausch über Verbesserungsvorschläge

AntiVirus genügt nicht

Unterschied zwischen Anti Virus Lösungen und Datenwäsche:

	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	✓	✗	?

Datenwäsche schützt vor unerwünschtem Code

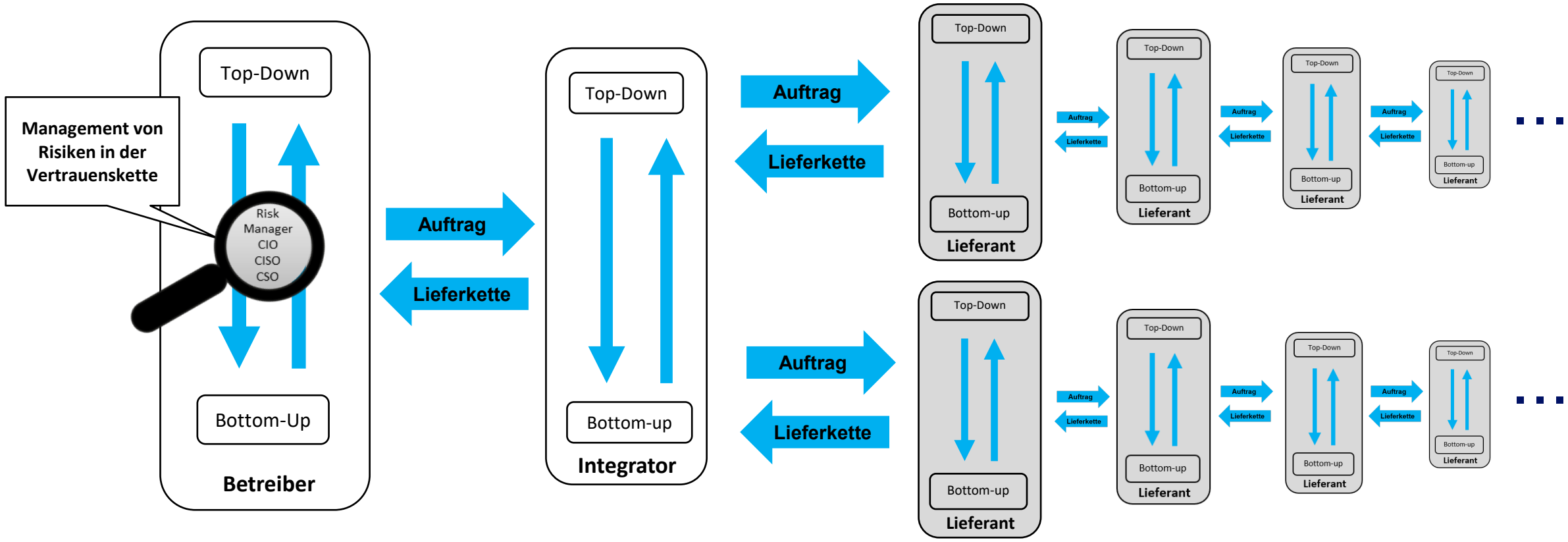


Aufgabe einer guten Sicherheitsarchitektur

Die beste Verteidigung ist eine gute IT-Sicherheitsarchitektur.
Diese ist lückenlos in mehreren Dimensionen:

	Durchgehende, lückenlose Vertrauenskette
Technik	Zusammenfügen der Sicherheitsprodukte zu einer sicheren, durchgehenden Vertrauenskette – von der Tastatur bis zu den Services und Daten
Organisation	Brückenschlag zwischen Security Awareness und Technischer Lösung
Rechtssicherheit	Verfolgen der Lieferkette unter Berücksichtigung von überlagernden Rechtsräumen (z.B. patriot act)
Haftung	Wenn die Haftung für erfolgreiche Angriffe nicht durchgesetzt werden kann, muss der proaktive Schutz erhöht werden
Lieferkette	Integritätskontrolle der fertig integrierten Produkte bis in ihren produktiven Einsatz hinein

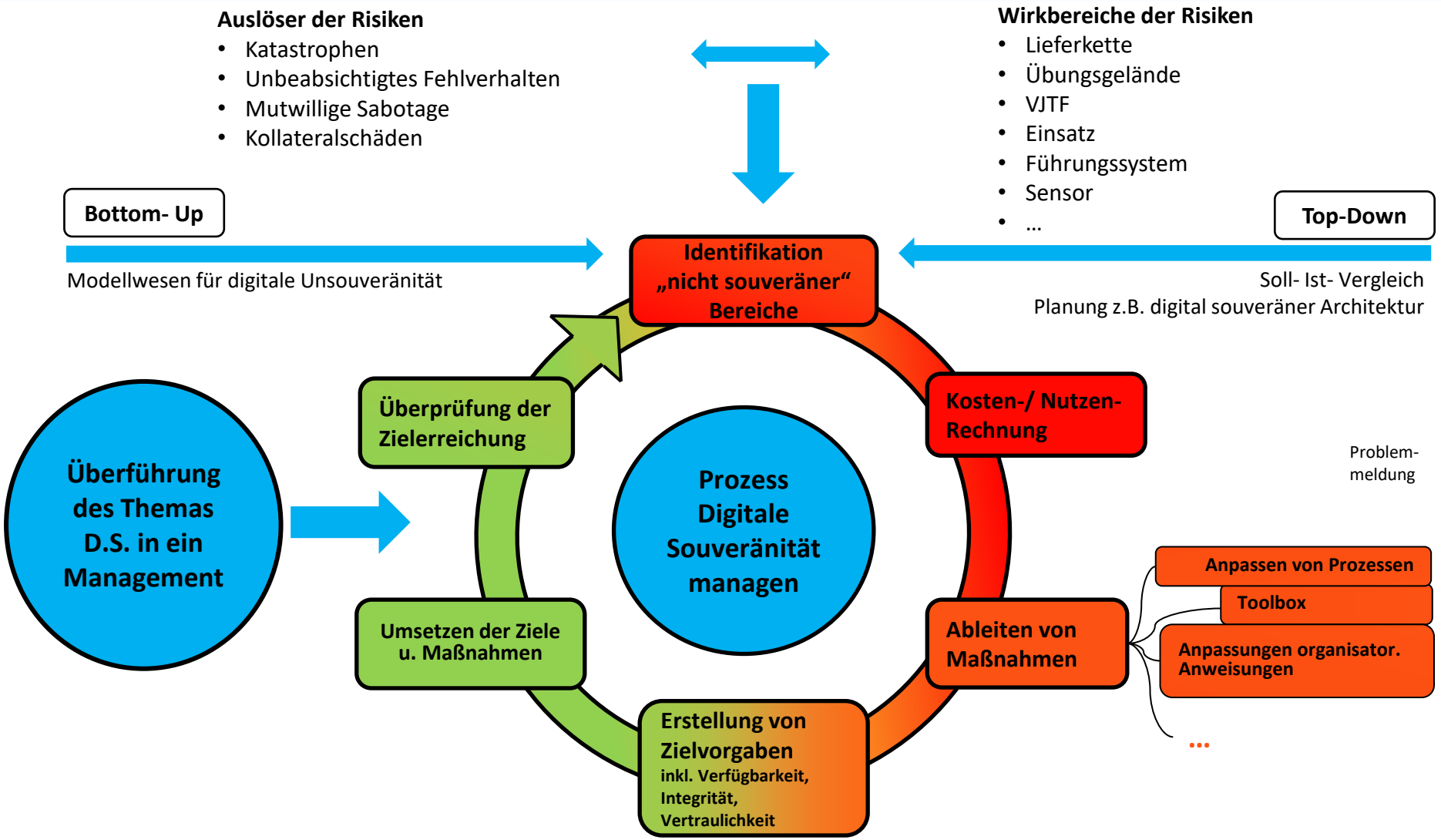
… das Aufsammeln der Risiken entlang der ganze Lieferkette



Risiken aufsammeln in das Endprodukt

Integrität – Verfügbarkeit – Vertraulichkeit – Robustheit der Schutzziele - Vertrauenswürdigkeit - Zukunftsfähigkeit…

Digitale Souveränität auf dem Endprodukt



Digitale Souveränität ist kein definierter, erreichbarer Endzustand sondern beschreibt den Wunsch nach einem selbstbestimmteren Handeln im Cyber- und Informationsraum.

FAZIT

Was wird technisch benötigt, um die Gefahren zu minimieren?

- Vollständige Software liste SBOM (Software Bill of Material)
- Vollständige Liste der Hardware und der darauf befindlichen Firmware, Patchmöglichkeiten der Firmware und Authentisierungsverfahren dafür
- Vollständige Liste aller Remote Zugänge inkl. Port, Kommunikationsstack, Protokoll, Requestor, Authentisierungsverfahren
- Hintertürfreiheit bestätigt
- und alles unter einklagbarer Haftung
- Darauf basierend ein Risikomanagement, welches es erlaubt die Risiken von unten aufzusammeln und für die verschiedenen Stakeholder zu bewerten (beim Auto z.B. Fahrzeugvermieter, Fahrer, Besitzer, Eigentümer, Fahrgäste, andere Verkehrsteilnehmer, Hilfskräfte wie z.B. Feuerwehr und Rettungskräfte, Passanten ...)

Demonstrator digitale Souveränität

- itWatch erstellt derzeit einen Demonstrator zur digitalen Souveränität von Lieferketten. Dieser Demonstrator wird Blockchain-Technologie für die Sicherheit von Informationen nutzen. Dazu gehören insbesondere sicherheitsrelevante Informationen der gesamten digitalen Supply Chain.

- Diese Informationen müssen mindestens in Teilen über regelbasierte Verfahren in Blockchain-spezifischen Smart Contracts hinterlegt werden.

- Der Demonstrator hilft dabei den Stand der Digitalen Resilienz eines Produktes zu veranschaulichen und erlaubt es die Bewertung bei veränderten Parametern zu erneuern.

- In einem geeigneten Szenar wird der Status der Digitalen Souveränität eines Cyberphysischen Produkts abgebildet und Auswirkungen von Veränderungen angezeigt.

- Anhand des Demonstrators wird aufgezeigt werden, welche Optionen, speziell von Sicherheitstechnologien bestehen, die Digitale Souveränität zu erhöhen.

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 und Workflow

www.itwash.de

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

Produktübersicht zum Download

Übersicht weiterführender Vorträge

- **„Digitale Souveränität und die Einschätzung der Sicherheit von Lieferketten – eine Managementdisziplin“** Problembeschreibung und Lösungsansätze“, Vortrag von Ramon Mörl am 01.02.2022 auf dem 18. Deutschen IT-Sicherheitskongress des BSI

- Vortrag von Ramon Mörl "Alle ausführbaren Objekte/Anwendungen überall erkennen, qualifizieren und sicher nutzen: wie geht das?"
  Vortrag von Ramon Mörl "Ohne ausführbares Objekt kein Angriff: alle Anwendungen sicher nutzen – was braucht man dazu?"
  Interview mit Ramon Mörl: Wie nutzt man fremde Daten in den eigenen Daten ohne Risiko? Schadcode, Makros, embedded Apps ... ob in Büro, Industrie, Leitstelle. (Alle Themen von der it-sa 365 2021).

- Unter dem Motto "Cyber Security - Rethinking Cyber Strategies in Tumultuous Times" fand im April 2021 die siebte mcsc des Sicherheitsnetzwerkes München e.V. statt. Ramon Mörl diskutierte in einem Panel mit dem Titel **„Corporate Cyber Risk Management – What Makes the Difference?“** (Munich Cyber Security Conference (mcsc) 2021)

- **„Data Centric Cyber Security – denn eigentlich geht es doch um Daten“**
  Vortrag von Ramon Mörl (it-sa 365 2020)

Fragen…

Ramon.Moerl@itWatch.de

itWatch Kontaktdaten

Bitte kontaktieren Sie uns für weitere Informationen:

itWatch GmbH
Aschauer Str. 30
81549 München
Tel.: +49 (0)89 6203 010 0
eMail: Vertrieb@itWatch.de
www.itWatch.de
www.itWash.de