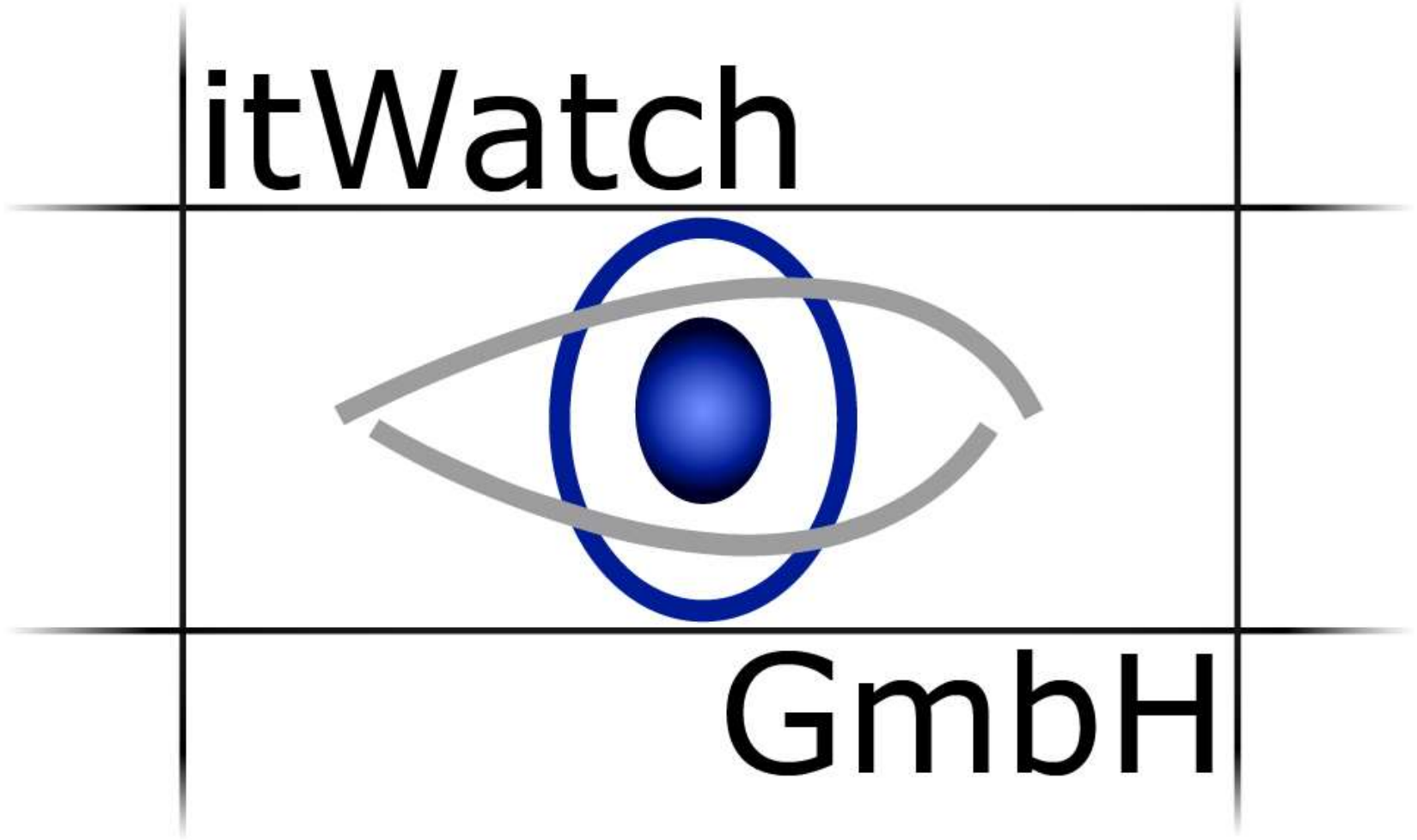
Ihre Sicherheit …
… unsere Mission



Ihre Cybersicherheitsstrategie – Wie können Sie Ihr Unternehmen verteidigen?

Wer hilft wie?

Mittwoch, 11.10.2023
10:45 – 11:00 Uhr
Knowledge Forum E

Die IT-Security Messe und Kongress
The IT Security Expo and Congress

Kurzvorstellung Ramon Mörl

- Über 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

Nationale Sicherheitsstrategie

Zitat:

Cybersicherheit ist

- eine gemeinsame Aufgabe von Staat, Wirtschaft, Wissenschaft und Gesellschaft …
- essenzieller Teil von integrierter Sicherheit

Cyber Security ist auf allen Ebenen gefordert

Im Unternehmen

der Anwender/Stakeholder erhält
geeignete „Awareness“
CEO, Admin, HR, R&D ...

Anwender

„IT-Abteilung schützt den Anwender“
Angebot zur sicheren Nutzbarkeit

Außerhalb des eigenen Unternehmens

Schutzversprechen des Staates im Cyberraum
Regulierung, Legislative, Exekutive...

Cyber Security Anbieter
Hersteller von Produkten
Integratoren
Pentesting
C-SOC & Managed Service
Lieferketten
...

IT-Sicherheit – Komplexität in vielen Dimensionen

- Schnelle Weiterentwicklung der Technologie
- Komplexität der Systeme
- Konvergenz
- Vielfalt der Bedrohungen
- Fachkräftemangel
- Awareness beim Anwender
- rechtliche Rahmenbedingungen
- Keine Wertschöpfung
- Viele Meinungen – keine Vertrauenskette

Verfügbare Technologien / Themen

- Backup / Recovery, Anti Virus, Archivierung,TR-ESOR, ersetzendes Scannen
- Firewall, VPN, Mehrfaktor Authentifizierung, EDR, NDR, XDR, Device / Port / Schnittstellenkontrolle, Applikationskontrolle, Datendiode, Web Application Firewall, NAC
- SIEM, Email Security Gateway, Intrusion Detection System, IPS
- Verschlüsselung Layer 1, 2 und 3, Schlüsselspeicher- und Verteilkomponente, Key-Management-Software, Verschlüsselungsgeräte für spezielle Anwendungsfälle (Funk, Satellit, Telefon, E-Mail, Messenger, Datei, Festplatten, mobiler Datenträger,Fax)
- Schadsoftwareerkennung, DDoS-Schutz Layer 3, 4, 7,
- Datenschleuse, Datenwäsche, Labelling
- ISMS, SBOM, HBOM, Digitale Signaturen, CA, RA,
- ???Mobile Device Management, Netzwerkmanagement

- Separation Kernel, Applikationsvirtualisierung, Sandboxing
- Zero Trust, DLP, UTM, APT- Abwehr, CTI, …
- CSS …

- … und vieles mehr

Beispiele von Technologien und ihren Limitationen

- Sind wir sicher, dass das alle (gleich) verstehen?

- Anti Virus findet bekannte Viren in Klartextdaten – nicht aber in tief verschachtelten oder verschlüsselten Strukturen
- Backup hilft nicht, wenn der Schadcode schon im Backup ist
- Firewall schützt an der Netzwerkgrenze (Perimeter – aber wo ist der heute schon) lässt oft http-s in allen Richtungen durch – irgendwo wird das TLS schon terminieren
- VPN schafft Ende zu Ende Verschlüsselung – Schadcode fühlt sich verschlüsselt sehr wohl, weil ihn niemand entdecken kann
- Mehrfaktor Authentifizierung: die positive Authentisierung kann Faktoren haben so viele sie will – am Ende gibt es ein Token, wenn man das Token stehlen und duplizieren kann …
- SIEM damit Sie wissen was schon passiert ist
- Verschlüsselung schützt die Vertraulichkeit – wer die Schlüssel hat, hat Zugriff, die Schlüssel sind natürlich separat geschützt (müssen aber häufig verwendet werden)

Die großen Themen

- Separation Kernel: trotzdem sollen Daten von der unsicheren in die sichere Umgebung kommen
- Applikationsvirtualisierung: trotzdem werden die Daten auch vom Betriebssystem und im Dateisystem für Standardfunktionen verarbeitet und an Dritte weiter gegeben
- Sandboxing: saubere Daten will man aber in seinem datalake und nicht in einer Box haben
- Zero Trust: zuerst braucht man eine Vertrauenskette, denn die Hardware auf der alles läuft, das Betriebssystem, das gekaufte Verschlüsselungsprogramm … alles ohne Vertrauen?
- CTI (Cyber Threat Intelligence) – irgendwo ist alles was böse ist exemplarisch gespeichert und jede der Milliarden Aktionen, die pro Sekunde stattfinden, werden mit den Mustern dort abgeglichen

Microsoft: Gestohlener Cloud-Master-Key

- Hacker haben einen Master-Signatur-Schlüssel von Microsoft erbeutet
- Diese konnten dadurch auf Kundendaten in Azure, Outlook.com und Microsoft 365 zugreifen
- Das müssen Unternehmen jetzt wissen, um festzustellen, ob ihre Daten kompromittiert sein könnten.

NEWSLETTER WHITEPAPER WEBINARE PODCAST STELLENMARKT

SECURITY INSIDER

Start IT-Awards Bedrohungen Netzwerke Plattformen Applikationen Identity- und Access-Management Security-Management

Bedrohungen - Sicherheitslücken - Gestohlener Master-Key von Microsoft

So ist der Hack von Storm-0558 passiert, das müssen Sie wissen!

Gestohlener Master-Key von Microsoft

18.09.2023 | Von Thomas Joos | Lesedauer: 2 min

Hacker haben einen Master-Signatur-Schlüssel von Microsoft erbeutet und konnten dadurch auf Kundendaten in Azure, Outlook.com und Microsoft 365 zugreifen. Das müssen Unternehmen jetzt wissen, um festzustellen, ob ihre Daten kompromittiert sein könnten.

Durch einen kompromittierten Microsoft-Account und einen ungeschützten Crash-Dump konnte die Hackergruppe Storm-0558 einen Master-Signatur-Schlüssel von Microsoft stehlen. Die Folgen sind gravierend.
(Bild: Skórzewiak - stock.adobe.com)

Quelle:
https://www.security-insider.de/gestohlener-master-key-von-microsoft-a-e13eabefaeb7354292ddd63dfae063d0/?cmp=nl-36&uuid=688db3470408ab81388e4848a6cc9aa2

Hardware und IT-Sicherheit

- Wissen Sie, welches Motherboard auf Ihren Systemen im Einsatz ist?
- Welche Information nehmen Sie mit, wenn es heißt: „das sollten Sie jetzt wissen“?
- Die Hintertüre erlaubt es, beliebige Firmware aufzuspielen!
- Die Hintertüre kann von staatlichen Stellen, genauso wie von beliebigen Hackern genutzt werden!
- Welche Reaktion schützt?

PCWELT

NEWS

Viele Gigabyte-Mainboards enthalten eine Firmware-Backdoor – das sollten Besitzer jetzt wissen

Ein Sicherheitsunternehmen hat eine gravierende Lücke in Mainboards von Gigabyte entdeckt. Über eine Hintertür werden Software-Updates von ungesicherten Webservern installiert.

Die Sicherheitsexperten von Eclysium haben entdeckt, dass Gigabyte in der UEFI-Firmware hunderter seiner Mainboards eine Backdoor installiert hat. Laut Eclysium wird der Code von Gigabyte dafür genutzt, um Firmware-Updates entweder über das Internet oder über einen angeschlossenen Speicher in einem lokalen Netzwerk zu installieren. Den Forschern zufolge ist das Tool jedoch größtenteils ungesichert, was bedeutet, dass jeder böswillige Akteur, der davon weiß, potenziell seinen eigenen Code auf das PC-Mainboard installieren kann.

Quelle:https://www.pcwelt.de/article/1937813/viele-gigabyte-motherboards-enthalten-eine-versteckte-firmware-hintertur.html

Barracuda Email Security Gateway – sofort ersetzen

- Hat der Kommunikationspartner – der Email Empfänger alles richtig gemacht – oder hat er das ESG im Betrieb und noch nicht ersetzt.
- Wie betrifft mich das als Sender einer Nachricht?
- Bei wem kann ich nachfragen ob bei meinem Mailprovider das ESG im Einsatz ist?
- Ist die Sicherheit in diesem Fall eine Hol- oder Bringschuld? … von wem?

heise online

IT Wissen Mobiles Security Developer Entertainment Netzpolitik

Cyber-Attacken: Admins müssen attackierte Barracuda ESG sofort ersetzen

Der Hersteller von Email Security Gateway Appliances (ESG) Barracuda appelliert an Admins, angegriffene Geräte auszutauschen. Sie sollten umgehend handeln.

Derzeit haben Angreifer Barracudas Email Security Gateway Appliances (ESG) im Visier und machen sich durch Hintertüren auf Geräten breit. Der Hersteller hat zwar bereits automatisch ein Sicherheitsupdate verteilt. Das funktioniert aber offensichtlich nicht wie gewünscht und der Hersteller rät nun dringend zum Austausch von attackierten Geräten.

Jetzt handeln!

In der aktualisierten Warnmeldung schreibt Barracuda, dass Admins alle

Quelle:https://www.heise.de/news/Cyberattacken-Admins-muessen-Barracuda-ESG-sofort-ersetzten-9181326.html

Applikationen und IT-Sicherheit

- Security by Design
- Privacy by Design

- Hr. Schaar – ehemaliger Bundesdatenschutz-beauftragter – sagte:
  „Eine Anwendung kann nur so sicher sein, wie das darunter liegende Betriebssystem“

- Das gilt für den ganzen „Stack“ – also alle beteiligten IT-Elemente

scinexx das wissensmaga

Home Geowissen Biowissen Medizin Energie Technik Physik Kosmos Arch

Earthview Medien-Tipps Galerie Lernwelten Schlagzeilen BusinessNews Videos Jobs

Sicherheitslücke in Microsoft Office entdeckt

Schwachstellen in der digitalen Signatur erlauben Manipulation vermeintlich geschützter Dokumente

Vorlesen

Nicht sicher: IT-Forscher haben eine erhebliche Sicherheitslücke in Microsoft Office entdeckt. Dadurch lassen sich vermeintlich geschützte Dokumente unerkannt manipulieren – trotz digitaler Signatur. Denn die in Office-Anwendungen verwendeten Signatur-Methoden haben gleich fünf Schwachstellen, durch die eine Signatur gefälscht oder umgangen werden kann, wie das Team berichtet. Microsoft hat zwar vier dieser Sicherheitslücken in der neueste Retail-Version des Office-Pakets behoben, in der vor allem in Unternehmen eingesetzten LTSC-Version von 2021 bestehen sie aber weiterhin.

Quelle:https://www.scinexx.de/news/technik/sicherheitsluecke-in-microsoft-office-entdeckt/

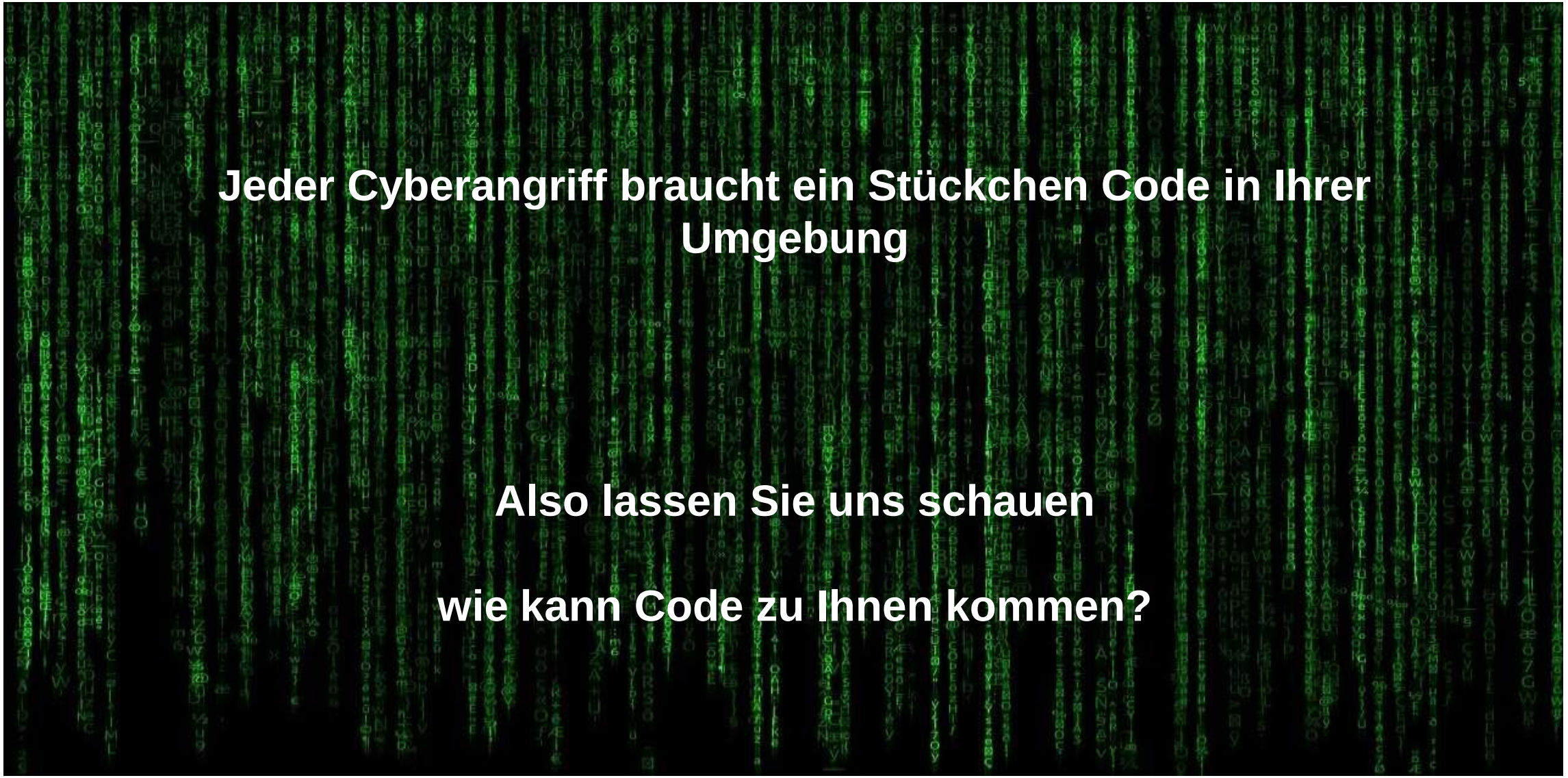
Das Ergebnis

Welche der vorgestellten Schutzmechanismen hätten bei welchem Problemen geholfen?

- Backup / Recovery, Anti Virus, Archivierung,TR-ESOR, ersetzendes Scannen
- Firewall, VPN, Mehrfaktor Authentifizierung, EDR, NDR, XDR, Device / Port / Schnittstellenkontrolle, Applikationskontrolle, Datendiode, Web Application Firewall, NAC
- SIEM, Email Security Gateway, Intrusion Detection System, IPS
- Verschlüsselung Layer 1, 2 und 3, Schlüsselspeicher- und Verteilkomponente, Key-Management-Software, Verschlüsselungsgeräte für spezielle Anwendungsfälle (Funk, Satellit, Telefon, E-Mail, Messenger, Datei, Festplatten, mobiler Datenträger,Fax)
- Schadsoftwareerkennung, DDoS-Schutz Layer 3, 4, 7,
- Datenschleuse, Datenwäsche, Labelling
- ISMS, SBOM, HBOM, Digitale Signaturen, CA, RA,
- ???Mobile Device Management, Netzwerkmanagement

- Separation Kernel, Applikationsvirtualisierung, Sandboxing
- Zero Trust, DLP, UTM, APT- Abwehr, CTI, …
- CSS …

- … und vieles mehr


Jeder Cyberangriff braucht ein Stückchen Code in Ihrer Umgebung
Also lassen Sie uns schauen
wie kann Code zu Ihnen kommen?

Der Nutzen nur auf Klartextdaten

Schadcode ist potentiell in jeder Information

eingehende Daten

heute reicht es nicht mehr, das Netz zu schützen

-

heute muss ich in jede Applikation / Datei schauen können auch wenn sie verschlüsselt oder komprimiert ist

ausgehende Daten

Schutz vor Datenverlust (DLP)

Wo ist der Angriff versteckt?

Wo kommen die Daten „von außen“ herein:

- Internet - Downloads
- E-Mails
- Mobile Datenträger
- (Private) Devices – BYOD
- IoT im Haus – Kamera, Rauchmelder
- OT / IT
- Kommunikationssoftware
  - ftp, s-ftp
  - Kalendersynchronisation
  - …
- Anwendungen und ihre (automatisch geladenen) Patches
- Remote Control Schnittstellen
- …

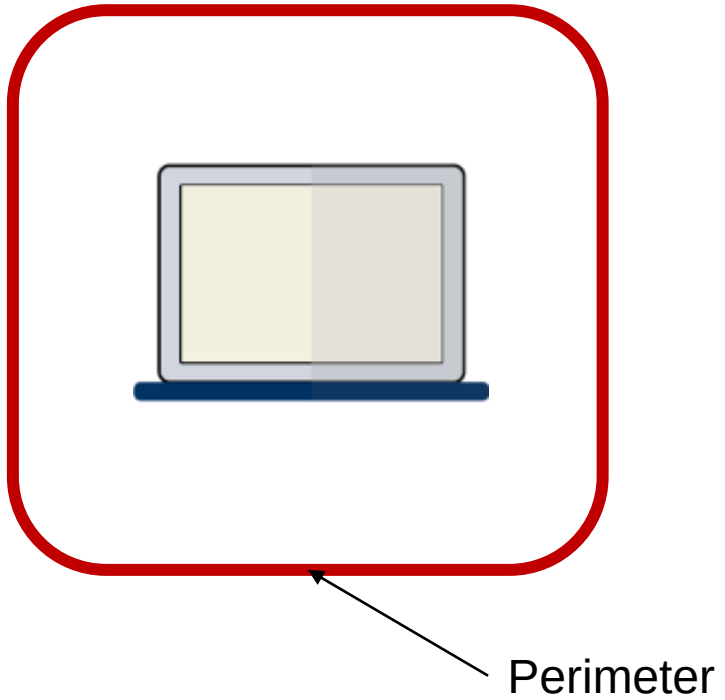
Ausführbarer Code kann sich in unterschiedlicher Form an verschiedenen Orten verstecken

- Eingebettete Objekte an beliebigen Stellen in Dateien
- Makros
- Nachladbare Objekte in Mails oder Browserinhalten
- Automatisch vom Betriebssystem (nach-) geladene Objekte z.B. lnk Angriff
- Plug-In in Anwendungen
- Controller und Firmware (z.B. BadUSB – Motherboard von GigaByte)
- …

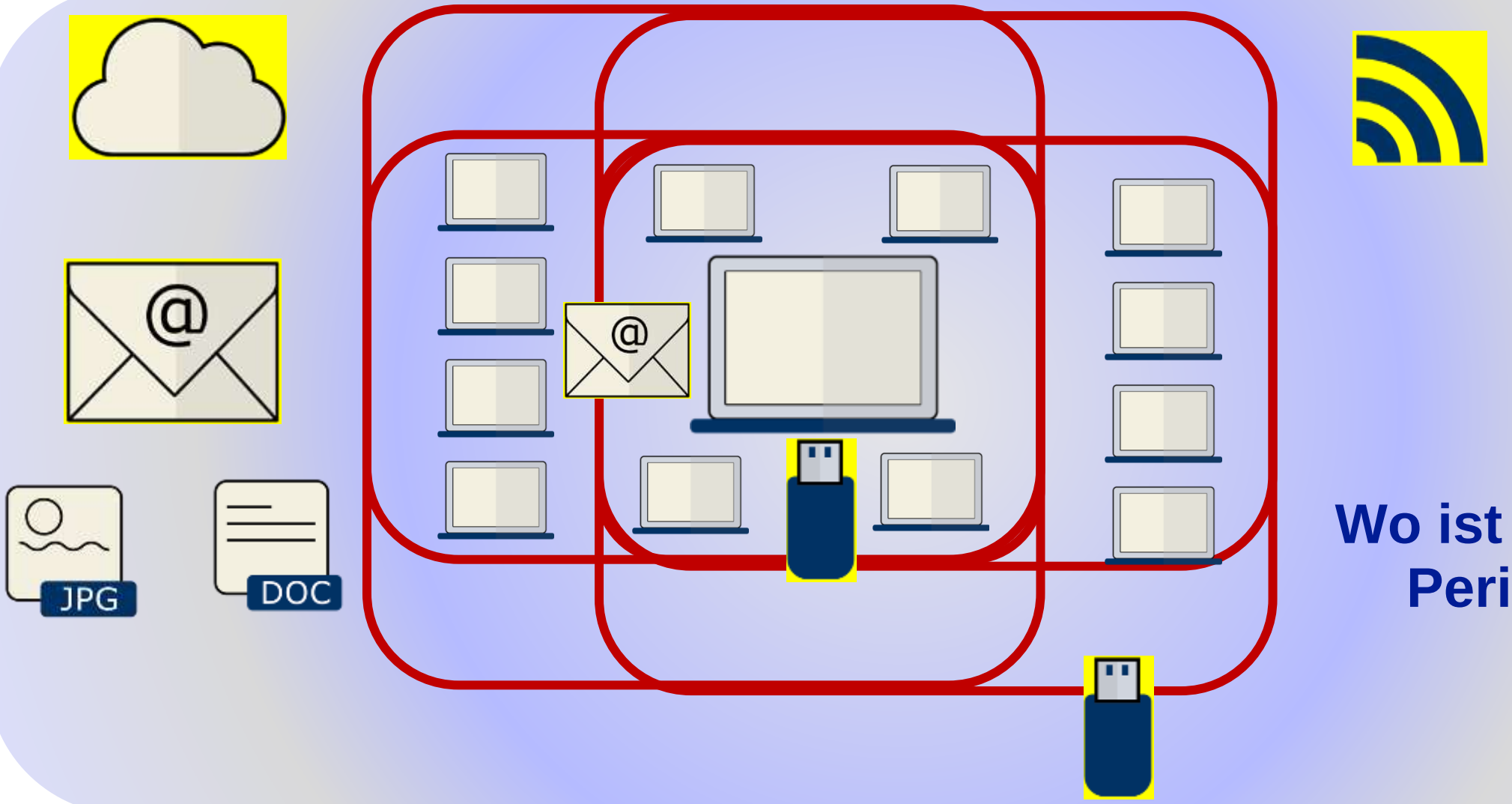
Wer kann gut und böse unterscheiden?

itWatch GmbH

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

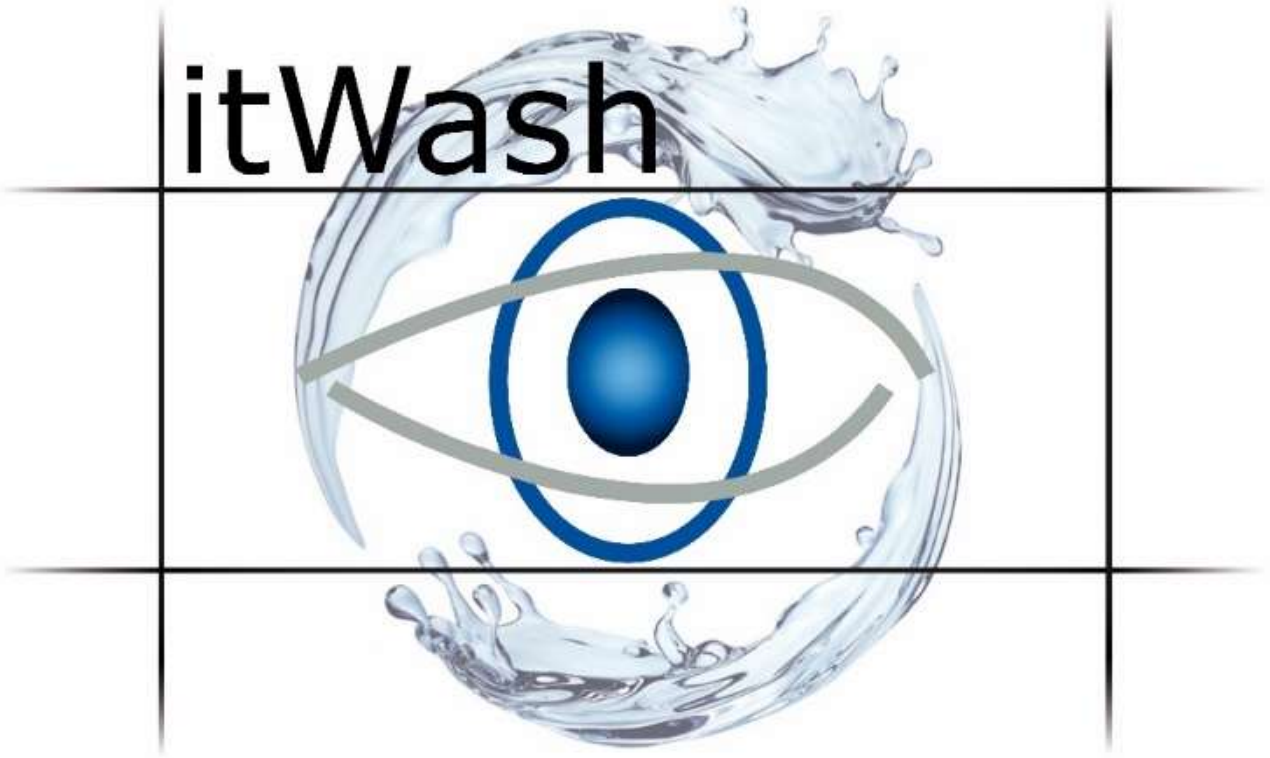


Heute ist es etwas komplexer ...



Wo ist heute der Perimeter?

itWash – Datenschleuse mit Datenwäsche



itWash
Datenschleuse
Datenwäsche
Workflow

- Entschlüsselt und Entpackt rekursiv bis alle Details im Klartext vorliegen
- Wäscht dann die Daten nach Unternehmensvorgaben (Waschmittel)

- Am Standardarbeitsplatz
- An den Netzübergängen
- In allen Mails
- In Fachverfahren
- In Kiosksystemen
- Zwischen getrennten Netzen
- … überall wo es notwendig ist

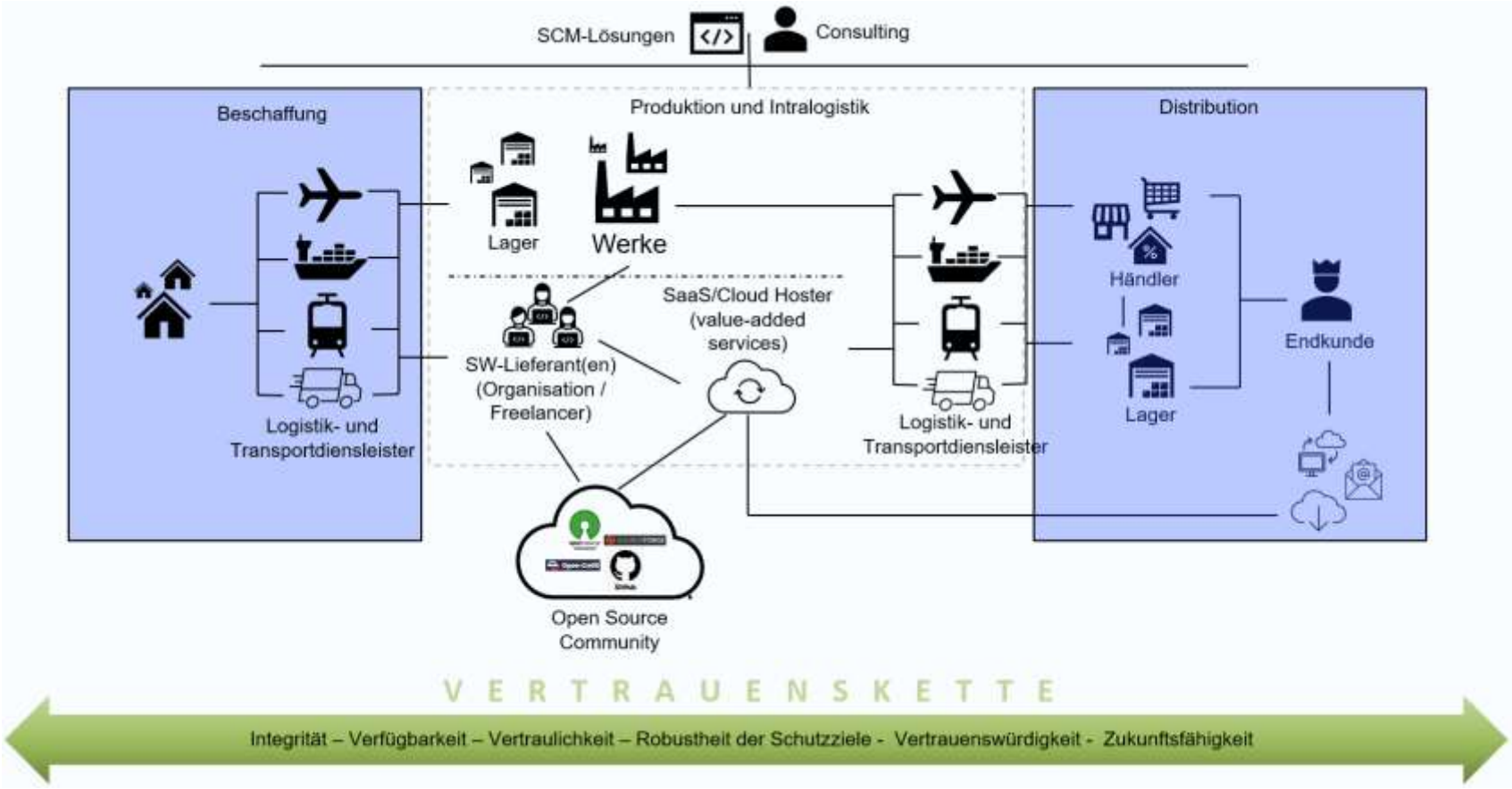
Finanziert von der Europäischen Union
NextGenerationEU

Demonstrator „Digitale Souveränität von Supply Chains“

DIGITALE SOUVERÄNITÄT IN DER PRAXIS MANAGEN

Lieferkette cyberphysischer Produkte

Ziel des Demonstrators ist es, darzustellen, wie die Digitale Souveränität und Resilienz der Lieferkette cyberphysischer Produkte durch die Verwendung von Distributed-Ledger-Technologie erhöht werden kann.



Schutz im Cyberraum …

Lassen Sie uns Ihre Visitenkarte/ Kontaktdaten zukommen und wir senden Ihnen gerne ein Freiexemplar der aktuellen Ausgabe in physischer Form oder online zu.

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

Fragen…

Besuchen sie uns
am Stand!
Halle 7A
Stand 108

Ramon.Moerl@itWatch.de