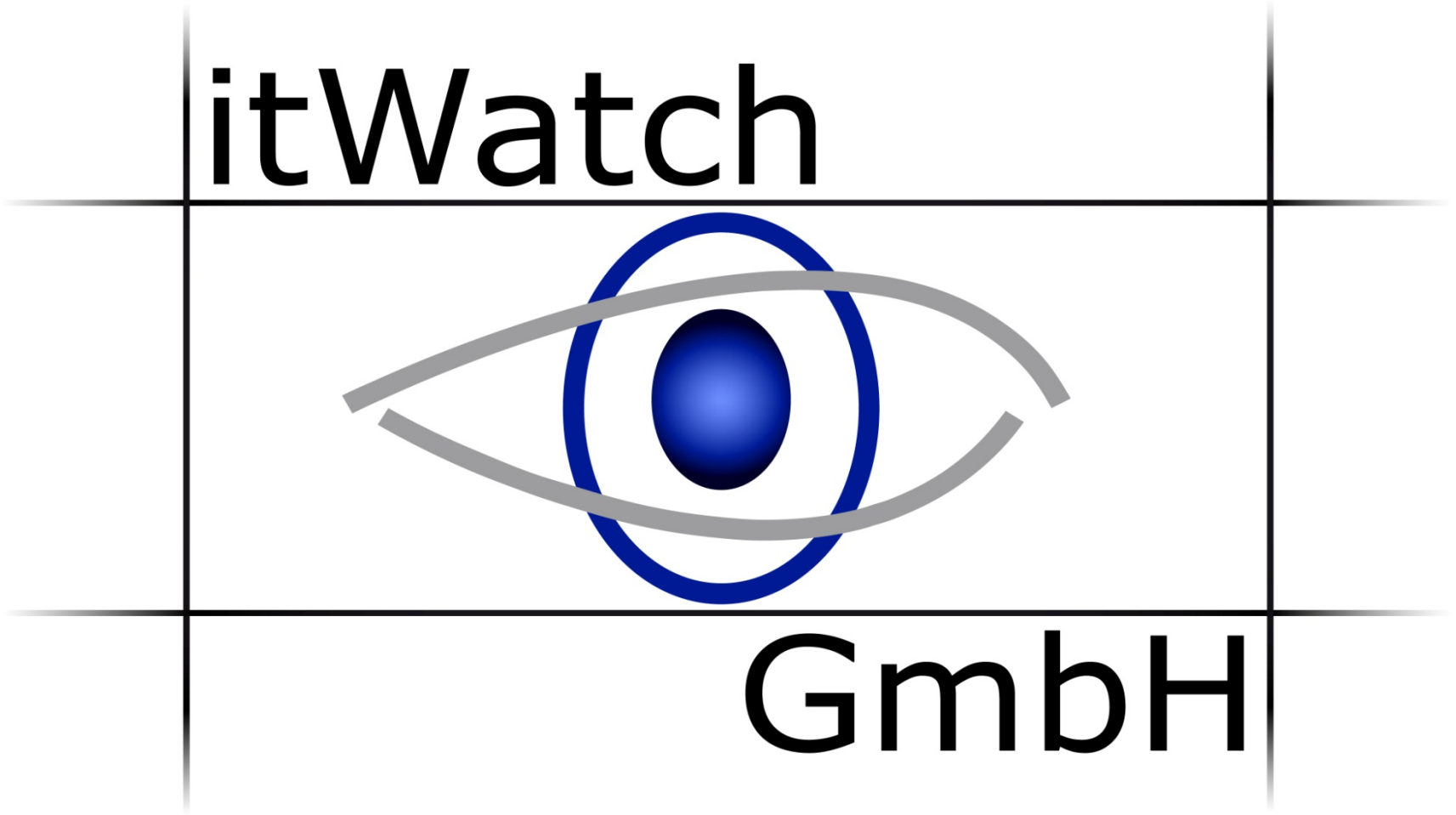
Ihre Sicherheit …
… unsere Mission



Adäquate Cyber Sicherheit für Industrie 4.0 – wie geht das?

Kundengesteuerte Produktionsgröße 1 und ungefährdete Produktion - ein lösbares Spannungsfeld

02. April 2019

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**

itWatch GmbH

Adäquate Cyber Sicherheit für Industrie 4.0 – welche Rolle spielt die Verlässlichkeit / Sicherheit der IT?

Bedrohungen in Industrie 4.0 Szenarien – was ist anders?

Wo stehen wir?

Strategien zur Verteidigung – Angriffs-robuste Architekturen – Betrachtung vollständiger Vertrauensketten

IoT Devices

Meine IoT Devices

Sind sehr teuer!

Termingerechte Nutzung lebenswichtig.

Dazu wird benötigt:

Cybersicherheit über den gesamten Entwicklungsprozess und Lifecycle

Klage wegen mangelhafter Security

Drohen Haftungsansprüche gegenüber allen Herstellern vernetzter IoT-Devices?

„Mangelhafte Security“: US FTC verklagt D-Link

US FTC = US Handelsmission (Federal Trade Commission)

Die US-Handelskommission FTC hat den taiwanischen Hersteller D-Link verklagt, weil das Unternehmen seine Kunden abstrakt einer Gefahr durch Hacker ausgesetzt habe. Sollte die FTC obsiegen, wären umfassende Haftungsansprüche und Class-Action-Lawsuits gegen alle IoT-Firmen mit Sicherheitsproblemen denkbar.

Router und IP-Kameras sind notorisch unsicher, ihre Hersteller zeigen bei der Schließung von Sicherheitslücken traditionell keine Eile. Als aber 2016 die Mirai-Malware bevorzugt Router und Online-Kameras befiel, aus diesen ein Botnetz bildete und mit DDoS-Attacken (Distributed Denial of Service) mehrmals Teile des Internets angriff und lahmlegte (darunter Twitter, den DNS Provider Dyn und Hunderttausende Arcadyan-Router der Telekom), muss es der US-Handelskommission (US Federal Trade Commission – FTC) gereicht haben: Sie statuierte unlängst ein Exempel und reichte Klage gegen den taiwanesischen Hersteller von Netzwerkequipment D-Link und seine US-Tochter D-Link Systems ein. Seite 3

Die Klage wirft dem Unternehmen vor, sich nicht um einen ausreichenden Schutz seiner Router und IP-Kameras gekümmert und seine Kunden damit Gefahren ausgesetzt zu haben. So habe es D-Link unterlassen, seine Geräte von Sicherheits-Fehlern zu befreien, die das Open Web Application Security Project (OWASP) wenigstens seit 2007 zu den kritischsten und verbreitetsten Verwundbarkeiten von Web-Anwendungen zähle.

D-Link habe wiederholt darin versagt, durch vernünftige Tests Router und IP-Kameras von leicht abzustellenden Sicherheits-Mängeln wie hartcodierten Nutzer-Berechtigungsdaten und anderen Backdoors zu befreien, die es Angreifern erlauben, Kontrolle über die Geräte zu erlangen.

D-Link habe ferner wiederholt dabei versagt, die Vertraulichkeit des privaten Schlüssels zu gewährleisten, den es benutzt, um seine Software zu signieren. Dieser Schlüssel war ca. ein halbes Jahr frei auf einer Webseite zugänglich. Außerdem habe D-Link nicht eine seit mindestens 2008 verfügbare freie Software genutzt, um die Sicherheit von Nutzer-Berechtigungsdaten in mobilen Apps zu sichern, die stattdessen in Klartext auf Mobilgeräten gespeichert würden.

Statt diese Mängel zu beheben habe D-Link durch Werbe-Aussagen den Eindruck erweckt, seine Produkte seien sicher, und es würde alles getan, um sie nach Sicherheits-Problemen wieder sicher zu machen. Dies stelle eine Verletzung des US-FTC-Gesetzes im Sinne von Section 5(a), 15 U.S.C. § 45(a) dar, das »unfaire oder täuschende Handlungen oder Praktiken, die den Handelsverkehr beeinträchtigen«, verbietet. Die FTC ersucht das Gericht um ein Unterlassungsurteil, das D-Link künftige Verstöße gegen das FTC-Gesetz verbietet.

D-Link bestreitet die Vorwürfe als »unberechtigt« und »grundlos«, die FTC habe lediglich »vage und unsubstantiierte Behauptungen hinsichtlich Routern und IP-Kameras gemacht«, behaupte gar kein tatsächliches Eindringen in D-Link-Produkte, die D-Link Systems in den USA verkaufe, und spekuliere lediglich, »dass Kunden, der Gefahr ausgesetzt wurden, gehackt zu werden«. »D-Link wird sich energisch gegen die unberechtigten und grundlosen Vorwürfe der FTC verteidigen«, verkündet das Unternehmen auf seiner Fragen-und-Antworten-Seite zum Thema.

Zur Verteidigung bedient sich D-Link der Vereinigung „Cause of Action Institute“ (CoA), die Gerichtsverfahren übernimmt, bei denen die US-Regierung vermutlich ihre Kompetenzen überschreitet. Das sei hier der Fall, sagt CoA über das Gerichtsverfahren: »Dies ist ein gefährlicher Präzedenzfall für die Bundesregierung, eine gute Firma zu verfolgen und US-Jobs zu gefährden, ohne einen einzigen Fall tatsächlichen oder wahrscheinlichen Schadens für Konsumenten. (...) Wenn die FTC ein Gerichtsverfahren wegen der bloßen Möglichkeit von Datensicherheitsverletzungen anstrengen kann, wird praktisch jede Firma einer unbeschränkten und unerforschten Datensicherheits-Haftung unterworfen.«

Die Tatsache, dass die FTC keinen konkreten Schaden in den USA als Begründung für ihre Klageerhebung anführt, sollte aufhorchen lassen. Hier sind Ansätze der Entwicklung einer umfassenden Produkthaftung sichtbar, die, sollte die Klage „FTC vs. D-Link“ Erfolg haben, umfangreichen Haftungsansprüchen der US-Regierung und Kunden gegenüber allen Herstellern von vernetzten IoT-Devices Tür und Tor öffnet.

Die Stellung der Regierung Trump zum Fall ist noch nicht bekannt. Nimmt man Donald Trumps Devise „America first“ als Richtschnur, ist eine Bestrafung der taiwanischen D-Link durchaus vorstellbar. (hl)

6/2017 www.markt-technik.de
Offizieller Medienpart
Markt&Technik
DIE UNABHÄNGIGE WOCHENZEITUNG FÜR ELEKTRONIK

Quelle: Markt & Technik – Die unabhängige Wochenzeitung für Elektronik, 03.02.2017, Heft 3, S. 1 & 3

Kaspersky-Verbot für alle US-Bundesbehörden

ANTIVIRUS

US-Bundesbehörden bekommen Kaspersky-Verbot

Protektionismus? Die USA verbieten den Einsatz von Kaspersky-Produkten auf allen Computern von Bundesbehörden. Aus Gründen der *"nationalen Sicherheit"*, wie Trumps Heimatschutzministerin Elaine Duke sagt.

Die US-Regierung verbietet ab sofort den Einsatz von Kaspersky-Software auf Rechnern der Bundesverwaltung. Das ordnete die Heimatschutzministerin Elaine Duke an. Zur Begründung verwies sie auf angebliche Geheimdienst- und Regierungskontakte der russischen Softwarefirma.

Produkte von Kaspersky Labs würden demnach die nationale Sicherheit der USA gefährden, weil russische Regierungsbehörden angeblich vorhandene Backdoors nutzen könnten, um vertrauliche Informationen zu kopieren und für Spionagezwecke zu nutzen. Nachdem bereits Neuanschaffungen für bestimmte Ministerien verboten waren, sollen nach dem Beschluss alle Versionen von Kaspersky von den Rechnern der Verwaltung entfernt werden.

Quelle Text: https://www.golem.de/news/antivirus-us-bundesbehoerden-bekommen-kaspersky-verbot-1709-130041.html
Quelle Kaspersky: http://www.t-online.de/digital/sicherheit/id_82168100/behoerden-in-den-usa-bekommen-kaspersky-verbot.html QuelleFlaggen: https://www.heise.de/newsticker/meldung/USA-verbieten-Behoerden-Nutzung-von-russischer-Kaspersky-Software-3831122.html (Bild: kremlin.ru CC BY 4.0 (Ausschnitt))

Priorisierung der Themen

Allen ist klar, dass ein AKW nicht einfach mit seinen produktiven Elementen an das Internet angeschlossen werden sollte.

?

Wo liegt aber nun die Grenze zwischen einem AKW und einen privaten internetfähigen Kühlschrank?

Priorisierung der Themen

Eine Priorisierung der Themen ist zwingend notwendig, um der Komplexität der IT-Security gerecht zu werden:

- Überlässt man die Antwort nur den klassischen markt-regulierenden Faktoren, werden aus Kostengründen Risiken für Leib und Leben im Risikomanagement nicht adäquat berücksichtigt und durch Haftungsübergänge und organisatorische Hinweise abgewälzt.

- Die neue Doktrin muss heißen, dass die Einsparungspotentiale durch Vernetzung, und den Einsatz von COTS (Commercial off the shelf) Produkten erst realisiert werden können, wenn die Safety in allen Eventualitäten dadurch nicht schlechter ist als vorher.

Schadcode in Bilddateien

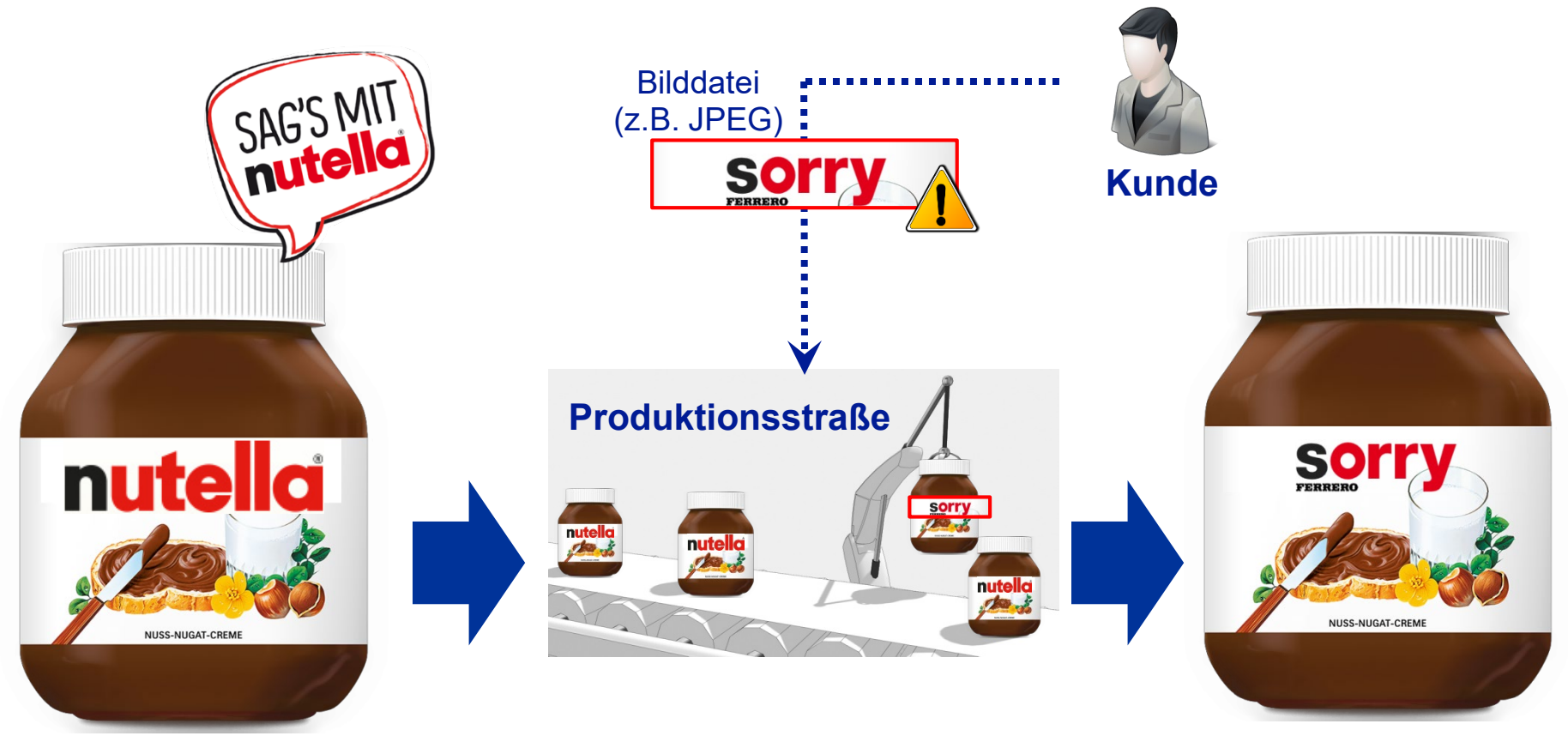
Auf der Sicherheitskonferenz RSA Security 2015 in San Francisco stellte Marcus Murray eine einfache Methode vor, wie Angreifer in Bilddateien Schadcode versteckten und ganze Webserver übernehmen können.

- Murray versteckte bei seinem Versuch schadhaften Code als Kommentar innerhalb der EXIF-Informationen von Bilddateien (z.B. „.jpg“, „.tiff“). Eine serverseitige automatische Bildvorschau führte den entsprechenden Schadcode dann aus, ohne dass ein Anwender starten muss.

- Unternehmen überprüfen zwar häufig die Endungen ankommender und ausgehender Dateien, weniger Häufig deren Authentizität, fast nie deren weitere Inhalte, die einfach abgetrennt werden können.

- Ausführbare Programme können jedoch z.B. wie durch Marcus Murray auf der RSA 2015 bewiesen **in Bilddateien (z.B. JPEG)** versteckt sein - und damit unbemerkt Schaden anrichten.

Problem Individualisierung 4.0



- Kunde möchte individualisiertes Produkt
- Kunde liefert die passende Bilddatei inklusive Schadcode zur Individualisierung (z.B. JPEG)
- Die Bilddatei wird in der Produktionsstraße direkt verarbeitet.

itWatch GmbH

Safety - Konvergenz Shop & Office-Floor – welche Rolle spielt die Verlässlichkeit / Sicherheit der IT?

Bedrohungen in Industrie 4.0 Szenarien – was ist anders?

Wo stehen wir?

Strategien zur Verteidigung – Angriffs-robuste Architekturen – Betrachtung vollständiger Vertrauensketten

Furby

Seit 2016 gibt es das Kinderspielzeug *Furby Connect* des japanischen Herstellers Hasbro auf dem Markt, der sich per Bluetooth mit dem Smartphone oder Tablet verbinden lässt.

Welche Gefahren diese neue Funktion birgt, zeigt ein Experiment des Kompetenz-zentrums IT-Sicherheit, dem es gelungen ist, den Furby so zu modifizieren, dass er dem Sprachassistenten Amazon Echo Befehle erteilen kann, die dieser bereitwillig ausführt.

Furby Connect hat eine ungesicherte Funkschnittstelle, über die man ihn alles sagen lassen kann, was man möchte.

Da die Bluetooth-Verbindung eine Reichweite von rund zehn Metern hat, wäre es denkbar, dass ein Hacker vor der Haustür steht und von dort aus auf den Furby zugreift.

Quelle: https://www.fzi.de/aktuelles/news/detail/artikel/fzi-blog-furby-allein-zu-haus-gefaehrliche-funktionen-eines-spielzeugs/

KI, Big Data - Missionskritisch

- KI ist digitales Lernen – nach mehreren Tagen „des Lernens“ könnte man die Frage haben „was hat das System gelernt“ – die Frage kann nicht direkt sondern nur durch Tests „heuristisch“ beantwortet werden.
- Wie kann man gegen falsche Empfehlungen „testen“ – wie löscht man „Fehler im Erlernten“
- Wem gehört das antrainierte „Wissen“ und wie kann man es mit anderen teilen ohne dass es den Dritten „gehört“
- Wie stellt man dem System seine Fragen und bekommt sie beantwortet.

Wo fehlt es an Know-how?

- Viele IT-Sicherheitsprodukte greifen auf „irgendetwas aus dem Internet“ zurück > Schwachstelle Drittprodukte
- Hersteller von „Non-IT-Security“-Produkten haben sich in den IT-Security-Markt bewegt - „*das ist ja auch nur IT– und so schwer kann das nicht sein*“ – bis zur Vernetzung
- Bei Entscheidungsverfahren um „make or buy“ stellt die Robustheit der Lösungen kein wesentliches Ziel dar.
- …
- D.h. auch in Produkten auf denen steht „IT-Sicherheit“ ist nicht immer das gleiche Maß an Schutz drin.
- Eine Metrik wäre gut, so dass der Konsument ohne eigenes Know-how verlässlich entscheiden kann
- => Vertrauenswürdige Handlungsketten sind sinnhaft

itWatch GmbH

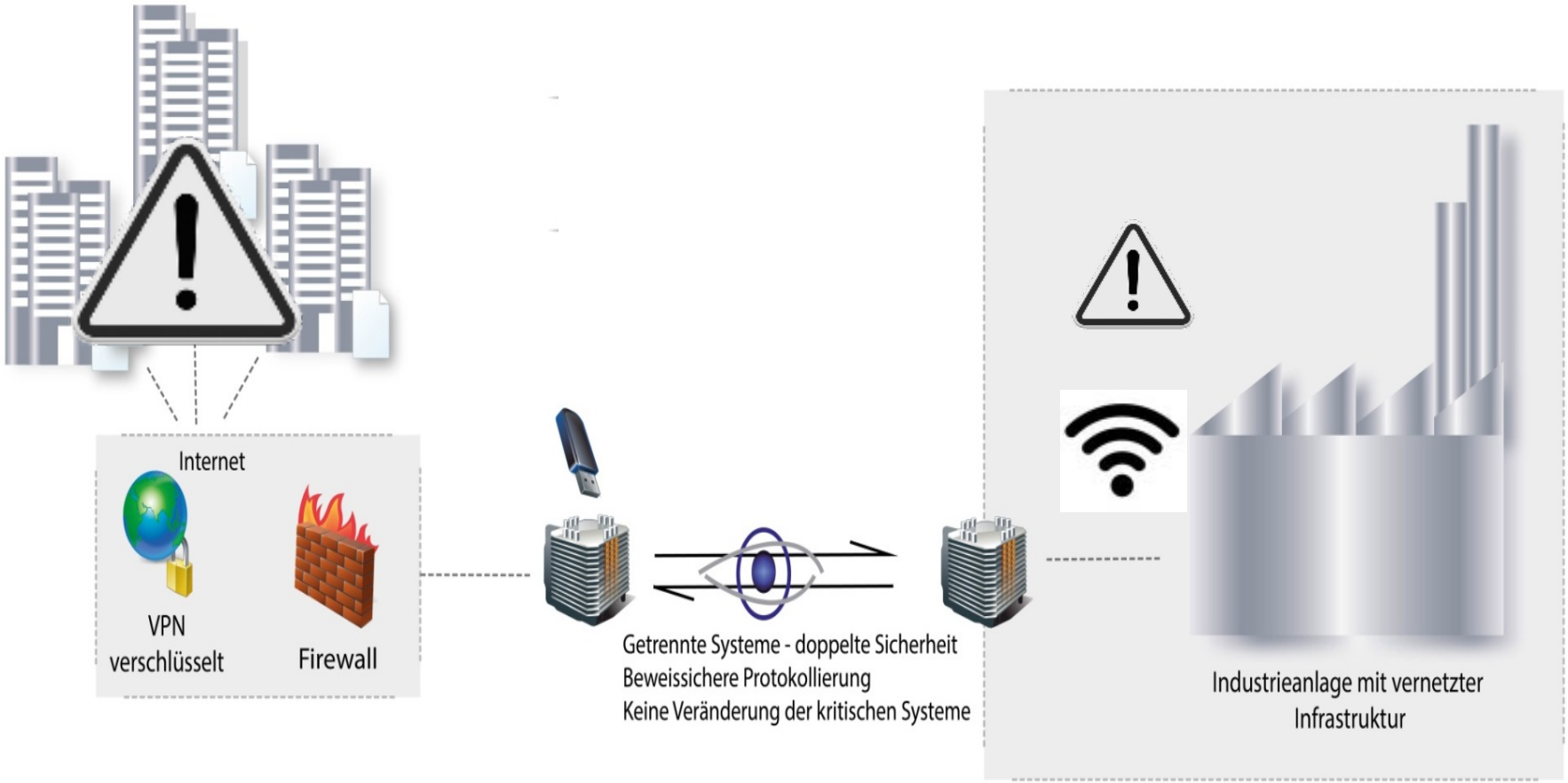
Safety - Konvergenz Shop & Office-Floor – welche Rolle spielt die Verlässlichkeit / Sicherheit der IT?

Bedrohungen in Industrie 4.0 Szenarien – was ist anders

Wo stehen wir?

Strategien zur Verteidigung – Angriffs-robuste Architekturen – Betrachtung vollständiger Vertrauensketten

Lösung - Produktion



Lösung – zusätzlich zu den bekannten

- Gehärteter Client unter Kontrolle des Systembetreibers mit folgendem Ziel
  - Beweissicherung bereits am Point of Action
  - Schutz vor Infiltration durch unsichere Netze des Partners
  - Schutz vor MAC-Spoofing und vielen anderen Angriffen zur Übernahme von authentisierten Sessions
- Netztrennung durch Virtualisierung
- Einfügen einer virtuellen Schleuse vor sicherheitskritischen Netzteilen:
  - Inhaltlicher Kontrolle
  - Protokollierung
  - Vertraulichkeit
  - Integrität
- USB und physikalische Schnittstellen absichern
- Funksteuerung schützen gegen Jammer und dedizierte Angriffe

Lösung - beispielhaft

Fernzugriff (Remote Admin)

- gehärteter Client mit VPN, keine DMA, BadUSB … Angriffe
- itWESS (itWatch Enterprise Security Policy) mit
  - geeigneter Schutz Policy und
  - Monitoring
- wird als bootfähiges Device mit Sicherheitsmerkmalen zur Authentisierung an den Remote Admin verteilt.
- Viele Sicherheitsfeatures:
  - Handshake gegenseitig authentisiert
  - beim booten werden alle "überflüssigen" Devices geblockt, der VPN Tunnel im Systemmodus aufgebaut, ohne dass der Anwender sie verändern kann
  - Datenaustausch über protokollierte und inhaltskontrollierte Schleusenfunktion
- zulässig sind Datentransfers der definierten Fachanwendungsdaten in verschlüsselter Form auf definierte oder beliebige Memorysticks (contentabhängig)
- Zur Bearbeitung der Daten stehen definierte Geräte (Drucker, Scanner, Biometrie) zur Verfügung, nicht gelistete Geräte sind nicht erlaubt

Lösung - beispielhaft

Technologie der virtuellen Schleuse:

- Transparenter Datentransfer nach Erfüllung folgender Anforderungen:
  - Inhaltlicher Kontrolle
  - Protokollierung
  - Verschlüsselter Transport
  - Integritätsschutz
- schützt Systeme vor:
  - Schadcode
  - Angriffen aus anderen Netzsegmenten (u.a. Internet)
- Wird für ICS zwischen System und Wartungsrechner gebracht
  - Schleusensystem selektiert Inhalte für die ICS

Sichere digitale Transformation

itWatch GmbH

Lifecycle von Sicherheitseigenschaften digitaler Produkte

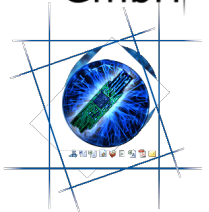
Entwickler

Security by Design
Privacy by Design

itWatch GmbH

Sichere digitale Transformation

ApplicationWatch - Applikationskontrolle



XRayWatch - Contentkontrolle

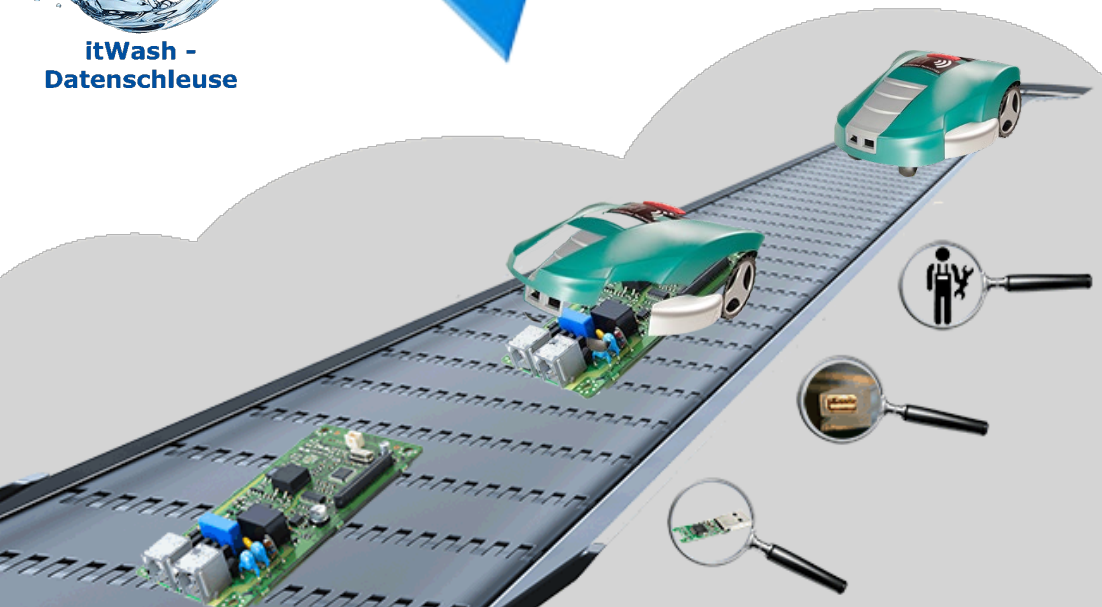
Schutz der Entwicklungsumgebung

PD Watch - Verschlüsselung

Sicherheit der Produktionsumgebung

Security as Infrastructure

itWash - Datenschleuse



Sicherheitszone Produkt im Betrieb

Sicherheitszone Produktion

WhiteIT und itWatch - Einladung am 2.4.

ab 19.00 Uhr heute Abend der Innenstadt von Hannover

itWESS itWatch Enterprise Security Suite

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!

itWash — Datenschleuse mit Datenwäsche

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

Fragen…

Treffen Sie uns in Halle 6 Stand C16