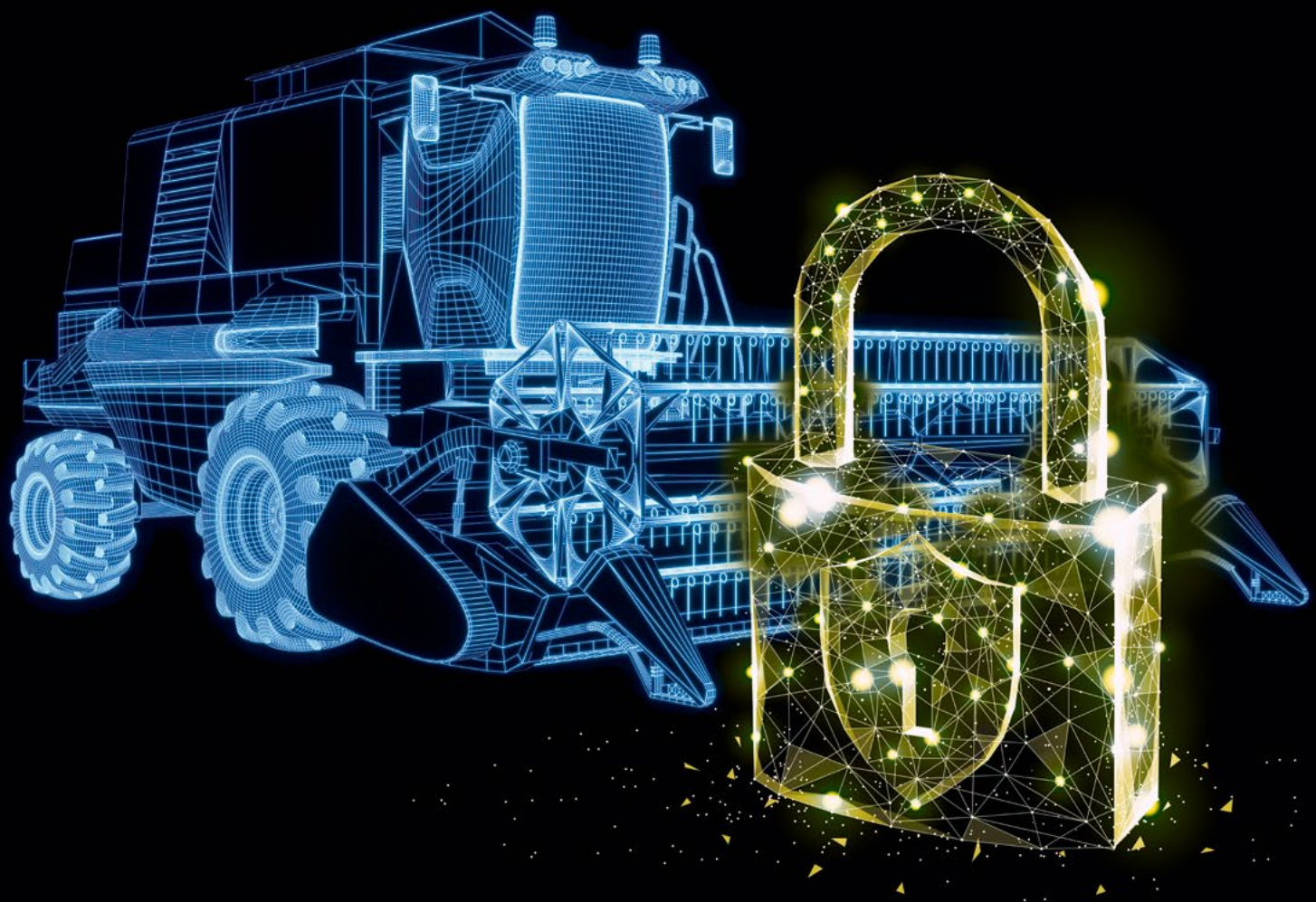
Springer Vieweg

ATZ extra



SECURITY

Herausforderungen ganzheitlich begegnen

itk ENGINEERING

/// INTERVIEW Jens Köhler, Daniel Steinmetzer [ITK]

© ITK Engineering GmbH

„Es ist essenziell, komplexe Angriffspfade holistisch abzusichern“

Durch den hohen Kostendruck in der Landwirtschaft besteht die Notwendigkeit zu einem möglichst optimalen Einsatz der teuren Maschinen und Anlagen. Daher sind die Digitalisierung und Automatisierung bis hin zum autonomen Fahren in der Landwirtschaft weiter als im Pkw-Sektor. Welche Herausforderungen dies für die Entwicklerinnen und Entwickler bei OEMs und Zulieferern im Bereich Cybersecurity mit sich bringt, erklären Dr. Jens Köhler und Dr. Daniel Steinmetzer im Interview mit ATZelektronik.

ATZelektronik _ Die Digitalisierung nimmt in der Landwirtschaft einen immer höheren Stellenwert ein. Damit steigt auch die Relevanz von Cybersecurity. Welche Bedrohungen gibt es in der Landwirtschaft, sind das eher Hackerangriffe im Sinn von Ransomware oder auch in Richtung Sabotage?

KÖHLER _ Es gibt tatsächlich nicht den einen Angreifer, sondern mehrere Angreifertypen. Ein möglicher Angreifer, der einem nicht sofort in den Sinn kommt, ist der Nutzer selbst: Besonders bei Geschäftsmodellen, bei denen Zusatzfeatures bezahlt und dann freigeschaltet werden, hat er eine gewisse Motivation, dies zu umgehen. Es sollte also gut geprüft werden, ob diese Kundenoptionen Einfallstore für Manipulation oder Hacker sein könnten. Die Motivation externer Angreifer ist sehr unterschiedlich: White-Hat-Hacker wollen ihren Ruf in der Szene aufbauen, terroristische Angreifer haben das Ziel, wich-

tige Infrastrukturen lahmzulegen, wie zum Beispiel eine Flotte von Erntemaschinen. Kommerziell motivierte Angreifer sind auf Profit aus. Gerade die letztgenannte Gruppe gewinnt zunehmend an Bedeutung durch Ransomware-Angriffe. Zur Einordnung: Die Marktforscher von Vanson Bourne schätzen den weltweiten Umsatz mit Cyberkriminalität auf rund 600 Milliarden US-Dollar.

Was können Landtechnikhersteller durch die genannten Angriffe verlieren?
KÖHLER _ Das ist sehr unterschiedlich. In unseren Risikoanalysen ziehen wir häufig fünf Schadenskategorien heran: Rufschädigung, denn niemand möchte mit einem Traktor unterwegs sein, der von Unbekannten ferngesteuert oder lahmgelegt werden kann. Intellectual Property, da Informationen auf den Zielgerätschaften nicht in die Hände der Konkurrenz fallen sollen. Safety, um den Schutz von Leib und Leben der mit dem System interagierenden Personen sicherzustellen. Außerdem sind noch Aspekte zu berücksichtigen wie etwa rechtliche Schäden, also beispielsweise Schadensersatzforderungen aufgrund unsicherer Produkte, sowie finanzielle Schäden etwa durch Rückrufaktionen oder das Einspielen nötiger Aktualisierungen zum Beheben der Schwachstellen oder entgangene Gewinne durch Produktpiraterie.

Wo sind die Schwachstellen, wo kann angegriffen werden?
KÖHLER _ Naheliegend sind Schnittstellen des Systems, beispielsweise WLAN, Bluetooth, CAN, NFC, USB, GPS oder die Cloudanbindung. Physikalische Schnittstellen sind insbesondere beim Schutz gegen den Nutzer selbst relevant. Bei mit einem Backend vernetzten System ist auch das Backend selbst ein gern genutztes Einfallstor. Das haben die Hacks von zahlreichen Automotive-OEMs Anfang 2023 gezeigt. Aber auch losgelöst vom System lauern Gefahren. Hierunter fallen Supply-Chain-Angriffe, also Angriffe auf das Zielsystem, schon während es entwickelt wird, indem beispielsweise Entwickler selbst Schadcode einschleusen oder indirekt über kompromittierte Zulieferer.

„Die Landtechnikbranche ist in der günstigen Position, Fast Follower zu sein“

Welche Normen, Standards und Prozesse sind im Hinblick auf Security bereits etabliert, und worauf müssen sich Landmaschinenhersteller und -zulieferer zukünftig einstellen?
KÖHLER _ Das ist eine spannende Frage. Der Gültigkeitsbereich der typenzulassungsrelevanten UNECE-R155-Regulierung gilt für Straßenfahrzeuge. In einer Vorabversion waren landwirtschaftliche Zugmaschinen eingeschlossen, wurden dann aber wieder gestrichen. Die UNECE R156 regelt dagegen den Umgang mit Softwareaktualisierungen und ist für die Landtechnik schon heute anzuwenden. Der EU Cyber Resilience Act (CRA) hat „products with digital elements“ im Fokus. Darunter fallen auch Traktoren und mobile Maschinen. Die CRA-Regulierung ist noch nicht final beschlossen. Falls der aktuelle Vorschlag von der Gesetzgebung verabschiedet wird, ist damit zu rechnen, dass Cybersecurity nachweislich im Entwicklungsprozess

Dr.-Ing. Jens Köhler ist Fachreferent für Cybersecurity bei der ITK Engineering GmbH. Er betreut seit sieben Jahren Kunden in verschiedenen Domänen bei der Ermittlung, Umsetzung und dem Testing von angemessenen Cybersecurity-Maßnahmen sowie bei der Etablierung von Cybersecurity-Engineering-Prozessen und -Methoden in den Unternehmen. Er hat am Fachbereich Informatik des Karlsruhe Institute of Technology (KIT) im Bereich Cloud Security promoviert.

Dr.-Ing. Daniel Steinmetzer ist Lead Expert für Cybersecurity bei der ITK Engineering GmbH. Er ist dort seit 2019 als Projektleiter, Trainer und Berater tätig und unterstützt diverse Kunden bei der Einführung und Umsetzung von Cybersecurity- Engineering-Maßnahmen und -Prozessen. Er hat am Fachbereich Informatik der TU Darmstadt im Bereich der sicheren drahtlosen Kommunikation promoviert.

und Lebenszyklus der Systeme oder Teilsysteme berücksichtigt werden muss. Passiert das nicht, drohen Strafen bis zu 15 Millionen Euro oder 2,5 % des weltweiten Jahresumsatzes. Sobald der CRA in Kraft tritt, bleiben den Herstellern und Zulieferern 24 Monate Zeit, die Vorgaben umzusetzen. Dieser Zeitraum ist gerade für Produkte, die über reine Software hinausgehen, äußerst ambitioniert. Die CEMA hat bereits Bedenken geäußert und drängt auf eine Erweiterung der Frist bis 2030. Auf Seite der Standardisierung ist die naheliegendste existierende Norm derzeit die ISO/SAE 21434 und die hat Einfluss auf den vorherrschenden Stand der Technik. Ein Landtechnik-spezifischer Standard ist durch ISO/TC23/SC19 für 2026 in Planung – kann jedoch gegebenenfalls nicht vor Inkrafttreten des CRA finalisiert werden.

Machen die vergleichsweise geringen Stückzahlen in der Landwirtschaft das Thema Digitalisierung/Cybersecurity schwieriger als beispielsweise im Pkw-Sektor?
KÖHLER _ Ja, definitiv. Durch geringere Stückzahlen schlagen Entwicklungskosten viel stärker auf den Stückpreis durch. Da auch Landtechnikkunden preissensitiv sind, bedeutet das, dass weniger Geld für die Entwicklung von Software und nicht funktionaler Aspekte wie Cybersecurity vorhanden ist, als in anderen Branchen. Was deutlich anders ist: Es müssen häufig viel pragmatischere Wege gefunden werden als im Automobilsektor, in dem viel abgesichert wird über Prozesse, Qualitätssicherungsverfahren für Entwicklungsartefakte wie Security-Risikoanalysen/-konzepte und komplexe Zuliefererstrukturen.

In der Entwicklung herrschen meist knappe Zeitpläne und Ressourcen. Kann die Landtechnik von anderen Branchen profitieren, die vor der gleichen Herausforderung stehen?
KÖHLER _ Die Landtechnikbranche ist in der günstigen Position, Fast Follower zu sein. Im Automobilbereich hat in den letzten Jahren eine ähnliche Umstellung bereits stattfinden müssen: Sicherlich kann nicht alles 1:1 übernommen werden, es gibt aber durchaus vergleichbare Herausforderungen. Grundlegende Konzepte aus dem Nutzfahrzeugbereich wie die Absicherung von Updates, Secure-Boot, Secure Onboard-Communication, Absicherungsverfahren für Diagnose und Debug-Schnittstellen können ohne weiteres auch für Landtechnikprodukte integriert werden. Auch bestehende Produkte, die nötig sind, um diese Konzepte umzusetzen, wie zum Beispiel Softwarelösungen oder Hardware-Security-Module, können übernommen werden.

Wo sollte man Ihrer Meinung nach anfangen?
KÖHLER _ Unsere Erfahrungen aus der Automobilbranche haben gezeigt: Pragmatische Ansätze für Cybersecurity führen zu den besten Ergebnissen – frühzeitig klein anfangen und das Thema iterativ aufbauen. Da produktbezogene Risikoanalysen ohnehin gefordert werden, ist es extrem sinnvoll, dort anzusetzen. Die Ergebnisse der Risikoanalyse sind auch Grundlage für weitere Entscheidungen über Maßnahmen und fördern das Verständnis und die Akzeptanz bei Mitarbeitern und Managern für die Erweiterung der Entwicklungsprozesse um Security.

© IITK Engineering GmbH

Je später Cybersecurity im Engineering-Prozess berücksichtigt werde, desto teurer und aufwendiger seien nötige Änderungen, meint Köhler

„Es müssen häufig viel pragmatischere Wege gefunden werden als im Automobilsektor“

Welche technischen Maßnahmen kann man nutzen, um landwirtschaftliche Geräte gegen Manipulation zu schützen?
STEINMETZER _ Man muss sich beispielsweise gegen eine manipulierte Firmware im Speicher oder ein manipuliertes Update schützen. Zur Absicherung der drahtlosen Kommunikation mit anderen Maschinen oder der On-Board-Kommunikation zwischen Steuergeräten im Fahrzeug können kryptografische Protokolle eingesetzt werden. In bestimmten Szenarien macht auch ein Intrusion-Detection-and-Prevention-System Sinn, um Angriffe und Schadcode zur Laufzeit erkennen und im Idealfall sogar unterbinden zu können. Außerdem sollte bei Entwicklung und Produktion darauf geachtet werden, dass alle nicht notwendigen Anschlüsse und Debugging-Schnittstellen wie die JTAG-Schnittstelle geschlossen oder deaktiviert werden. Sie fungieren oft als Hintertür, um andere Security-Maßnahmen zu umgehen. Da diese Mechanismen meist mit Entwicklungs-, Integrations- und Betriebsaufwand einhergehen, macht es Sinn, vorab zu prüfen, ob diese wirklich notwendig sind. Ein effektiver Schutz ist anschließend durch eine auf das Gerät zuge-

© ITK Engineering GmbH

Ein effektiver Schutz sei durch eine auf das Gerät zugeschnittene, individuelle Kombination von Security-Maßnahmen möglich, sind sich Köhler und Steinmetzer einig

schnittene, individuelle Kombination an Security-Maßnahmen möglich.

Was geschieht beim Thema Entwicklung und Test der Systeme/Software, um sicher zu entwickeln?

STEINMETZER _ Grundsätzlich sollte die komplette Entwicklung des Systems oder der Software einem standardisierten Security-Engineering-Prozess unterliegen. Dieser startet mit einer Risikoanalyse zur Identifizierung von Schwachstellen und Risiken. Basierend darauf können im Rahmen eines Security-Konzepts Maßnahmen definiert werden, um potenzielle Angriffe zu erschweren und Risiken zu senken. Wichtig ist es, bei der Auswahl auf etablierte Maßnahmen und Algorithmen zu setzen. So kann das Risiko, neue Schwachstellen zu öffnen, minimal gehalten werden. Bei der Implementierung sollte neben der Codequalität ein Augenmerk auf Secure Coding Guidelines zur Vermeidung von Schwachstellen in der Softwareentwicklung gelegt werden. Beim abschließenden Testing wird geprüft, ob Maßnahmen passend sind und korrekt umgesetzt wurden – optimalerweise durch funktionale Tests der Security-Features und durch nichtfunktionale Penetration Tests. Letztere überprüfen das fertige System mit Methoden und Tools, die auch einem externen Angreifer zur Verfügung stehen würden.

Auch die Punkte Fernwartung sowie Over-the-Air-Updates sind ein Thema. Wie sichert man diese ab?

STEINMETZER _ Alle Updates sollten mit einer digitalen Signatur abgesichert werden. Für die Erstellung von Updates wird dann der digitale Schlüssel benötigt, den nur der Herausgeber hat. Insbesondere bei der Fernwartung sollte auf eine starke beidseitige Authentifizierung gesetzt werden, um sicherzustellen, dass ausschließlich autorisierte Benutzer Zugriff bekommen.

In landwirtschaftlichen Geräten kommt immer häufiger eine KI zum Einsatz. Wie kann man diese absichern?

STEINMETZER _ Eine Besonderheit bei der KI ist die Frage, wie und mit welchen Daten ein KI-Algorithmus trainiert wurde, um mögliche Adversarial Attacks vermeiden zu können. Bei solchen Adversarial Attacks werden der KI konstruierte Eingabewerte vorgelegt, die zu einer Fehlklassifizierung führen würden. Solche Angriffe können – je nach Anwendungsfall – zu schwerwiegenden Problemen führen. Das kann zum Beispiel schon anhand von leicht abgeänderten Straßenschildern demonstriert werden – der Mensch erkennt ein Stoppschild, die KI erkennt ein Schild mit Tempolimit 130. Da bei KI per Definition nicht klar vorgegeben wird, wie Entscheidungen zu treffen sind, ist es nicht trivial, sich gegen derartige Angriffe abzusichern. Tatsächlich ist das noch Gegenstand aktueller Forschung. Im Beispiel könnte die KI-basierte Straßenschildererkennung durch Kartenmaterial plausibilisiert werden. Reaktiv kann zusätzlich ein Security Operations Center eingesetzt werden, um mögliche Schwachstellen der KI während der gesamten Lebenszeit des Gerätes zu beobachten, zu bewerten und gegebenenfalls den KI-Algorithmus gegen neue Angriffe zu härten.

Die Kombination externer Daten und interner Sensorik kann auch ein Angriffspunkt sein, oder?

STEINMETZER _ Ja, das stimmt. Deshalb ist eine Absicherung externer und interner Sensoren sowie die Kommunikationsverbindung wichtig. Externe Daten werden häufig von Clouddiensten bezogen, die eine große Angriffsfläche bieten. Bei Manipulation oder Ausfall sollten interne Daten daher als Plausibilisierungs- und Fallbackoption dienen. In den meisten Anwendungsfällen werden die internen Sensordaten daher in der Regel höher priorisiert, sodass die lokalen Auswirkungen eines Angriffs auf die externe Datenquelle limitiert bleiben. Wichtig ist es, das Gerät zu ermächtigen, einen sicheren, aber gegebenenfalls eingeschränkten Betrieb auch bei kompromittierter externer Datenquelle zu gewährleisten.

Zusammenfassend: Was sind aus Ihrer Sicht die wichtigsten Dinge, die bei der Verankerung des Themas Security in der Landtechnik zu beachten sind?

© ITK Engineering GmbH

Zunehmend vernetzte Systeme bergen Gefahren und böten Angriffsflächen. Ein ausgefeiltes Security-Konzept sei daher essenziell, erläutert Steinmetzer

KÖHLER _ Zusammenfassend kann man sagen: Vergleichsweise geringere Stückzahlen sorgen in der Landtechnik für ein kleineres Budget für Cybersecurity-Maßnahmen als beispielsweise in der Automobilbranche. Daher ist ein pragmatischer Ansatz wichtig. Einige Vorgehensweisen können aus der Automobilbranche oder anderen Branchen übernommen werden. Die Grundlage ist immer die Risikoanalyse, nur so werden systematisch alle potenziellen Risiken erkannt. Gerade im Fachgebiet Cybersecurity steckt der Teufel oftmals im Detail. Expertise und Know-how sind daher gefragt: Es ist essenziell, komplexe Angriffspfade holistisch abzusichern. Cybersecurity in Unternehmen umzusetzen, ist ein langer Prozess, der nicht von heute auf morgen ausgerollt wird. Daher sollten Vorgehensweisen bei Security wie Risikoanalyse und Konzeption frühzeitig in ausgewählten Projekten pilotiert werden. Je später Cybersecurity im Engineering-Prozess berücksichtigt wird, desto aufwendiger sind nötige Änderungen.

Danke für das Interview, Dr. Steinmetzer und Dr. Köhler.

INTERVIEW: Robert Unseld

IMPRESSUM:
Sonderausgabe 2023 in Kooperation mit ITK Engineering GmbH, Bergfeldstraße 2, 83607 Holzkirchen; Springer Fachmedien Wiesbaden GmbH, Postfach 1546, 65173 Wiesbaden, Amtsgericht Wiesbaden, HRB 9754, USt-IdNr. DE81148419

GESCHÄFTSFÜHRER:
Stefanie Burgmaier I Andreas Funk I Joachim Krieger
PROJEKTMANAGEMENT: Anja Trabusch

TITELBILD: © [M] KengVit14 ICoreDESIGN I Stock.adobe.com

ITK Engineering

Seit der Firmengründung 1994 stehen wir für Stabilität, Sicherheit und Methodenexpertise. Damals wie heute bildet branchenübergreifendes Spezialwissen insbesondere im Bereich der Regelungstechnik und der modellbasierten Entwicklung die Basis, um unsere Kunden von der Idee bis zur Serienproduktion durchgängig und partnerschaftlich zu begleiten.

Unsere Kompetenzen umfassen u.a.:

- Softwareentwicklung
- Hardwareentwicklung
- Elektrik/Elektronik
- Systemintegration
- Software als Produkt
- Komplettlösungen
- Auftragsentwicklung
- Technische Beratung
- Schulungen
- Qualitätssicherung

Die Zufriedenheit all unserer Partner und ein respektvolles Miteinander prägen unsere Unternehmensphilosophie, in der vier Werte fest verankert sind: Lesen Sie gerne mehr darüber im Web.

V.1.0.0_d_2021

ITK Engineering GmbH
Hauptsitz Rülzheim
Im Speyerer Tal 6
76761 Rülzheim
Tel.: +49 (0)7272 7703-0
Fax: +49 (0)7272 7703-100
info@itk-engineering.de

www.itk-engineering.de
www.itk-karriere.de

Gegründet 1994 –
heute hat ITK deutschlandweit Niederlassungen und ist international vertreten.

Folgen Sie uns auch auf: