A. Ruckelshausen et al. (Hrsg.): Intelligente Systeme Stand der Technik und neue Möglichkeiten,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 15

Datensicherheit: Die nächste große Herausforderung in der modernen Landtechnik?

Franz Kraatz[1], Frank Nordemann[1], Ralf Tönjes[1]

Abstract: Der wirtschaftliche Druck in der Landwirtschaft mit weniger Ressourcen höhere Erträge zu erwirtschaften hat zu einer zunehmenden Automatisierung und Industrialisierung agrartechnischer Prozesse geführt. Die Vernetzung von kooperativen Agrarprozessen verfügt über außerordentliches wirtschaftliches Potenzial, birgt aber auch große Gefahren für die Datensicherheit. Daten werden vielfach nicht durch den Dateneigentümer erfasst, sondern von beauftragten Dienstleistern (z.B. von Lohnunternehmen). Bei einer Datenerfassung durch Dienstleister sind Datenzugriffe nicht kontrollierbar und nachträgliche Datenmanipulationen nicht auszuschließen. Datensicherheitslösungen aus anderen Wirtschaftsbereiche lassen sich nur unzureichend auf die Landtechnik übertragen. Dieser Beitrag stellt ein Basiskonzept zur bereichsübergreifenden Datensicherheit in der Landtechnik vor. Das Ziel des Konzeptes ist, die Datenhoheit durch den Eigentümer zu jeder Zeit zu gewährleisten und ausgewählte Prozessdaten manipulationssicher zu dokumentieren.

Keywords: Kooperative Agrarprozesse, Datensicherheit, Privatsphäre

1 Daten in kooperativen Agrarprozessen

Während der Ausführung von Agrarprozessen nehmen Landmaschinen über den herstellerübergreifenden ISOBUS unterschiedlichste Daten in Form von Messwerten auf. Durch erfasste Daten zu Erträgen oder tatsächlichen Ausbringmengen können Prozesse optimiert und z.B. durch Applikationskarten mit teilflächenspezifischen Applizierungsangaben effizient gedüngt werden. Auch die Dokumentation zur Einhaltung von gesetzlichen Auflagen (z.B. Nährstoffbilanzen) erfolgt auf Basis der erfassten Daten, indem der applizierte Dünger ins Verhältnis zum Ertrag gesetzt wird. Eine Datenübertragung von Landmaschine zu Landwirt erfolgt meist ohne zwischengeschaltete Stationen. Allerdings erfahren Datendrehscheiben zum Datenaustausch zwischen Prozessakteuren eine steigende Verbreitung. Bislang finden bei der Übertragung und Verarbeitung dieser für den Landwirt sehr wichtigen Daten nur sehr geringe bis keine Datensicherheitsmechanismen Verwendung. Zudem werden Daten des Landwirts von unterschiedlichsten Systemen und Akteuren (Datendrehscheiben, Lohnunternehmen, Dienstleistern) erfasst und verarbeitet. Unberechtigte Datenzugriffe und Datenmanipulationen werden nicht ausgeschlossen. Es fehlt ein akteurübergreifendes, verteiltes Rechtemanagement, um den Datenzugriff in einer verteilten Umgebung mit unterbrechungsbehafteter Kommunikation zu sichern. Auch rechtliche Vorgaben zur lückenlosen Nachweispflicht werden eine manipulationssichere Datenerfassung erfordern.

[1] Hochschule Osnabrück, Fakultät Ingenieurwissenschaften und Informatik, Albrechtstr. 30, 49076 Osnabrück, Deutschland, f.kraatz;f.nordemann;r.toenjes@hs-osnabrueck.de

2 Datensicherheit in anderen Wirtschaftsbereichen

Die Grundlage für digitale Datensicherheit bilden *symmetrische und asymmetrische Verschlüsselungstechniken*. Der Unterschied beläuft sich auf die Verwendung eines Schlüssels bei symmetrischen Verfahren und dem Einsatz eines Schlüsselpaares bei asymmetrischen Verfahren. Beide Verfahren besitzen Vor- und Nachteile, weshalb sich z.B. für die sichere Datenkommunikation im Internet eine Mischform etabliert hat. Zur eindeutigen Zuordnung von öffentlichen Schlüsseln zu Kommunikationspartnern haben sich *digitale Signaturen* etabliert. Hier werden die Schlüsselpaare der asymmetrischen Verschlüsselung in umgekehrter Reihenfolge verwendet. Eine vertrauenswürdige Instanz signiert den öffentlichen Schlüssel des Kommunikationspartners. Das Verfahren wird bei Bankkarten eingesetzt, um Überweisungen digital zu unterschreiben. Ein zentrales Problem bei der Verteilung digitaler Daten ist die Gewährleistung der Datenhoheit. Die Medienindustrie realisiert Video- und Musikstreaming über gekapselte Softwareumgebungen, die mit *Digital Rights Management (DRM)* [Sta03] Datenzugriffe kontrollieren. Diese Mechanismen erlauben auch ohne stetige Kommunikationsverbindung den Datenzugriff *(Offline-Modus)*. Um Daten mit Gruppen zu teilen kann die *Attribute Based Encryption (ABE)* [LW11] eingesetzt werden. So können Ärzte oder Krankenschwestern je nach Gruppenzugehörigkeit auf die digitale Patientenakte zugreifen.

In zur Landtechnik verwandten Wirtschaftsbereichen ist ein deutlich gestiegenes Bewusstsein für Datensicherheit zu erkennen. *Stuxnet* hat verdeutlicht, dass auch Industrieanlagen durch Cyberangriffe bedroht werden. Mit *Industrie 4.0* wird die Automatisierung industrieller Prozesse gesteigert. Dabei rückt das Thema Datensicherheit in den Fokus, weshalb das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Reihe von Anforderungen und Testempfehlungen für Hersteller erarbeitet hat [BSI14]. In der Automobilindustrie werden unter dem Begriff *Car-to-X* Verkehrsinformationen ausgetauscht und Autos vermehrt direkt oder über Smartphones an das Internet angebunden. Damit ist das Fahrzeug kein geschlossenes Kommunikationssystem mehr und Sicherheitslücken können für Cyberangriffe [Sch15] missbraucht werden. Eine Übertragung bestehender Datensicherheitskonzepte aus anderen Bereichen (Bank- / Gesundheitswesen, Industrie 4.0) ist durch die Charakteristika der Landtechnik nicht ohne Einschränkung möglich. Agrarprozesse verfügen über heterogene und dynamisch ändernde Akteure und Komponenten, die in einer örtlich verteilten und mit Kommunikationsunterbrechungen versehenen Umgebung einen Auftrag bearbeiten. Dennoch soll die Datenhoheit über erfasste Daten zu jedem Zeitpunkt beim Auftraggeber liegen. Auch rechtliche Dokumentationsvorgaben müssen mit beschränkter Hardware eingehalten werden.

3 Basiskonzept zur Datensicherheit in der Landtechnik

Das entwickelte Basiskonzept zur Datensicherheit in Abb. 1 wird anhand des Agrarprozesses Flüssigmistausbringung erläutert. Dieser Anwendungsfall beinhaltet neben einer bedarfsgerechten Düngeverteilung auf einem Schlag auch die manipulationssichere

Dokumentation der Ausbringmengen, die an zuständige Behörden gemeldet werden. Der Agrarprozess wird zudem nicht durch den eigentlichen Landwirt, sondern durch einen beauftragten Lohnunternehmer bearbeitet und über eine Datendrehscheibe zugestellt.

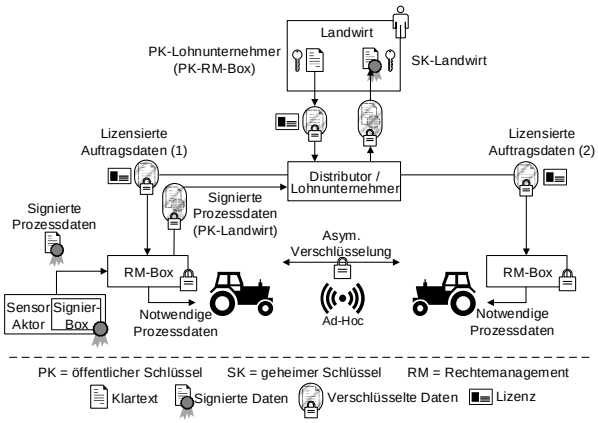

Abb. 1: Basiskonzept zur Datensicherheit in der Landtechnik

Zur Wahrung der Datenhoheit durch den Dateneigentümer ist die Nutzung von *digitalen Lizenzen* für den **Zugriff auf Daten** vorgesehen. Der Eigentümer beschreibt in einer Lizenz, welchen Akteuren er für einen bestimmten Zeitraum ein Nutzungsrecht auf eine definierte Datenmenge einräumt. Auf diesem Weg kann ein Landwirt z.B. einen Datensatz über den Auftrag Flüssigmistdüngung einem Lohnunternehmer zukommen lassen und den Datenzugriff auf den Ausführungszeitraum begrenzen. Die Datensicherheit kann bei Bedarf durch Mechanismen der *Attribute Based Encryption (ABE)* weiter gesteigert werden, in dem für den Datenzugriff Attribute erfüllt sein müssen (z.B. Zugriffsort, Zugriffskomponente, etc.). Die Einhaltung der Nutzungslizenzen wird durch eine manipulationssichere Software zum **Datenzugriffsmanagement** gewährleistet. Sie ist auf prozessteilnehmenden Geräten (PCs, mobile Geräte, Landmaschinenterminals) installiert oder kann als Hardwarebaustein (*RechteManagement-Box [RM-Box]*) realisiert werden. Die Software kapselt Datensätze auf den Geräten und regelt Zugriffe über Nutzungslizenzen. Der Zugriff auf Prozessdaten kann zur Laufzeit konfiguriert werden, um die Datenhoheit des Landwirts bei der Datenaufnahme durch einen Lohnunternehmer zu sichern. Die weitläufigen Umgebungen im Agrarbereich verlangen zudem ein funktionsfähiges Rechtemanagement ohne kontinuierliche Kommunikationsverbindung. Zu diesem Zweck ist ein zeitlich beschränkter *Offline-Modus* in der Software / der RM-Box vorgesehen. Die **Datensicherheit auf dem Übertragungsweg** wird zunächst durch die Verschlüsselung des Kommunikationspfades gewährleistet. Bekannte Mechanismen wie *HTTPS, WPA oder virtuelle Tunnel* bieten effektiven Schutz gegen das Abhören von Kommunikationsverbindungen. Zusätzlich integriert das Konzept Methoden zur *asymmetrischen Verschlüsselung mittels RSA*. Mithilfe von öffentlichen und privaten Schlüsseln kann ein Datensatz nur vom vorgesehen Empfänger (z.B. eine Person, eine Maschine, eine RM-Box) entschlüsselt werden. Möglichen Zwischenstationen auf dem Übertra-

gungsweg (Personen, Maschinen, Datendrehscheiben, etc.) bleibt die Entschlüsselung verwehrt. In einigen Fällen ist ein **uneingeschränkter Datenzugriff** erforderlich, durch den die Datenhoheit des Eigentümers nicht mehr zu gewährleisten ist. Ein Precision-Farming-Anbieter benötigt meist unbeschränkten Zugriff auf Boden- und Ertragskarten, um Applikationskarten zu berechnen. In derartigen Szenarien dienen *digitale Wasserzeichen (Watermarking)* als Hilfsmittel, um Missbrauchsstellen eindeutig zu identifizieren. Zur **manipulationssicheren Dokumentation von Prozessdaten** wird eine gesicherte Hardwareumgebung verwendet. Eine von einer vertrauenswürdigen Stelle geprüfte *Signier-Box* versieht Prozessdaten mit einer *digitalen Signatur*. Im Anwendungsfall Flüssigmistausbringung können Ausbringmengen von einer Behörde zweifelsfrei geprüft werden, da die Signatur eine spätere Datenmanipulation ausschließt. Reine Software-Lösungen sollten aufgrund größerer Angriffsmöglichkeiten vermieden werden.

4 Zusammenfassung

In Zukunft werden die von verschiedenen Akteuren erfassten und verarbeiten Datenmengen in der Landtechnik weiter steigen. Die Datensicherheit wird zum entscheidenden Erfolgsfaktor bei der kooperativen Bearbeitung von Agrarprozessen. Eine einfache Übertragung von Sicherheitskonzepten aus anderen Wirtschaftsbereichen ist aufgrund der spezifischen Charakteristika der Landtechnik ausgeschlossen.

Das Basiskonzept für eine akteurübergreifende Datensicherheit in der Landtechnik setzt auf eine effektive Adaption und Kombination bewährter Sicherheitsmechanismen aus der Informations- und Kommunikationstechnik. Im Fokus der Konzeption steht die Wahrung der Datenhoheit des Eigentümers, der prozessbezogene Datenzugriff in einem verteilten Umfeld mit heterogenen Akteuren und die manipulationssichere Datendokumentation. Das Basiskonzept soll das Problembewusstsein in der Landtechnik schärfen und als Grundlage einer gemeinschaftlichen Diskussion zur Problemlösung dienen.

Literaturverzeichnis

[BSI14] BSI: ICS-Security-Kompendium. 11/2014, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.pdf (19.11.2015).

[Eck06] Eckert, C.: IT-Sicherheit - Konzepte, Verfahren, Protokolle. Oldenbourg, 2006.

[LW11] Lewko, A.; Waters, B.: Decentralizing Attribute-Based Encryption. Proc. of 11th Int. EUROCRYPT Conf., Springer-Verlag, Heidelberg, S. 568-588, 2011.

[Sch15] Schneider, D.: Jeep Hacking 101. IEEE Spectrum, 08/2015, http://spectrum.ieee.org/cars-that-think/transportation/systems/jeep-hacking-101 (19.11.2015).

[Sta03] Stamp, M.: Digital Rights Management - The Technology Behind the Hype. J. Electron Commerce Res., 4. Jg., Nr. 3, S. 102-112, 2003.