DLG-Merkblatt 465

Datennetzwerke im landwirtschaftlichen Betrieb

Aufbau, sicherer Betrieb und Nutzung

www.DLG.org

DLG-Merkblatt 465

Datennetzwerke im landwirtschaftlichen Betrieb

Aufbau, sicherer Betrieb und Nutzung

Autoren

– Rolf Feldmann, Landwirtschaftskammer NRW mit der AG Prozessrechner
– Bernhard Feller, Landwirtschaftskammer NRW mit dem Förderkreis Stallklima
– Sven Häuser, DLG e.V., Frankfurt am Main

Co-Autoren:

– C. Hoth, Provinzial Konzern, Münster
– A. Kulke, alcona Automation GmbH, Beckum
– A. Schulz, Big Dutchman International GmbH, Vechta

Unter Mitwirkung der Mitglieder der DLG-Ausschüsse Digitalisierung, Arbeitswirtschaft und Prozesstechnik sowie Technik in der Tierhaltung

Herausgeber:

DLG e. V.
Fachzentrum Landwirtschaft
Eschborner Landstraße 122, 60489 Frankfurt am Main

1. Auflage, Stand: 05/2022

Inhalt

1. Einführung

Für viele ist das „**Netz**“ zum Datentransfer heute eine Selbstverständlichkeit. Wenn ein Datennetzwerk auf dem Betrieb eingerichtet werden soll, wird man teilweise nach Sachverhalten gefragt, die nicht sofort für jeden ganz einfach nachzuvollziehen sind. Zur Orientierung sind in dem vorliegenden Merkblatt ein paar grundlegende Ansprüche, Fragen und Antworten zum Thema nach aktuellem Wissensstand zusammengefasst.

Die erste Frage stellt sich häufig nach Art und Leistung des Netzwerks. Drahtgebundene Netzwerke sind sicher und schnell in der Übertragung, aber häufig ist ein kabelloses Netzwerk, zum Beispiel über WLAN (wireless local area network), die bevorzugte Wahl bei der Vernetzung von Anwendungen und Geräten bzw. Clients, wie sie im Fachjargon heißen. Hierbei handelt es sich oftmals um Verbindungen über ein bestehendes WLAN-Heimnetzwerk zum PC und ins Internet oder aber Verbindungen von Geräten über dieses Netz untereinander. Die begrenzte Reichweite eines solchen Systems ist manchmal der entscheidende Faktor für die Wahl eines verkabelten Netzwerkes, dem LAN (local area network). Außerdem werden oft die Anfälligkeit für Störungen und eine leichtere Angreifbarkeit von WLAN-Systemen als Faktoren bei einer anstehenden Entscheidung genannt. Heute kann durch einige Schutzmaßnahmen vieles sichergestellt werden. Damit eine Systemauswahl leichter fällt und die Betriebssicherheit der Netzwerke erhöht wird, sind im Folgenden die wichtigsten Punkte und Parameter zusammengefasst.

2. Netzwerke auswählen und sicher nutzen

Ein WLAN bietet oft sehr viele Vorteile, wie z. B. eine räumliche Unabhängigkeit, eine größere Flexibilität und geringere Installationskosten durch den Wegfall der Verkabelung. Solange nicht zu viele Daten auf einem kabellosen Betriebsnetz unterwegs sind, wird die Bandbreite (die zur Verfügung stehende Übertragungskapazität) bei den aktuellen und leistungsfähigen Netzwerkkomponenten auch nicht der begrenzende Faktor sein. Wenn aber beispielsweise mit einer großen Anzahl von Kameras/Videodaten gearbeitet wird, sollte man sich beim Fachmann über erforderliche Übertragungskapazitäten informieren.

Auch beim kabelgebundenen Netzwerk (LAN) können sich, insbesondere bei sehr alten Systemen bzw. Komponenten, Einschränkungen z. B. durch niedrige Übertragungsgeschwindigkeiten ergeben. Alte, organisch gewachsene Systeme, für die keine Pläne vorhanden sind, bereiten häufig Probleme bei der Entscheidungsfindung bezüglich Erweiterung oder Erneuerung der Komponenten und der Kapazität des Netzwerks.

Neue Bauteile, besonders Glasfaserkabel, aber auch konventionelle Netzwerkkabel (bis zu einer max. Länge von etwa 100 m) an einem neuen Verteiler (Switch), haben in der Regel mit einer ausreichenden Übertragungskapazität (Durchsatz) kein Problem mehr. Damit in Zukunft alle möglichen Teilnehmer an einem Netz diese Leistung teilen können oder sich Techniker einen Überblick verschaffen können, wo evtl. nachgebessert werden müsste, ist es beim nächsten Netzausbau sinnvoll, sich einen Übersichtsplan bzw. eine Dokumentation der Technik ausfertigen zu lassen. Ein Lastenheft kann einem im Vorfeld dabei helfen, gewünschte Details, die mit der Auftragsvergabe fällig werden, zusammen mit dem Techniker festzulegen. Hinweise auf vorhandene alte oder neu zu erstellende Netzwerkteile können so auch dokumentiert werden.

Tabelle 1: Netzwerktechniken im Vergleich (Quelle: PC Welt)

Technik Mbit/s	Durchsatz$_{max.}$ (theoretisch)	Durchsatz$_{i.d.R.}$ (real*)
Gigabit-Ethernet	1.000	950
Fast Ethernet	100	95
Powerline 1200	1.200	350
Powerline 500	500	120
Powerline 200	200	60
WLAN 802.11ac	1.300	480
WLAN 802.11n	450	120
WLAN 802.11g	54	15

* Bei WLAN und Powerline-Verbindungen hängt die Geschwindigkeit sehr stark von den Entfernungen, baulichen Gegebenheiten und Störquellen ab.

Erklärungen:
Gigabit-Ethernet (neuer) und Fast Ethernet (älter) mit LAN-Kabel.
Powerline ist eine Datenübertragungsmöglichkeit mit Adapter über die Stromversorgungsleitungen.
WLAN mit einer Datenübertragung per Funktechnologie und Reichweiten bis 100 m im Freien.

Auf eine richtige Verdrahtung, über Gebäude und Etagen hinweg, muss immer geachtet werden. Hier entstehen dann oft auch die größeren Kosten, welche jedoch, beispielsweise bei einem gleichzeitigen Anspruch auf ein sicheres Netzwerk, gerechtfertigt sind. Lose Verkabelungen, die an vielen Stellen im Gebäude freiliegen, bilden eine Gefahrenstelle, die z. B. in einem Anschluss-/Patch-Feld in einem Schrank besser geschützt werden können. Neben der baulichen Sicherheit ist der Schutz vor unberechtigtem Zugriff auf das Netz und die Datensicherheit bei Übertragung wesentlich. Moderne Verschlüsselungsalgorithmen ermöglichen im LAN und WLAN, aber auch beim Datentransfer über das WWW (World Wide Web) meistens eine hinreichende Sicherheit. Trotzdem sollten sensible Daten und Informationen so diskret wie möglich behandelt werden.

In der Adresszeile eines Browsers (bspw. Microsoft Edge) steht am Anfang des Eintrags heute anstatt eines „http://...“ in der Regel ein „https://...“, z. B.: „https://www.google.de/…“. Mit diesem Standard wird beim Datentransfer im Internet bereits eine gewisse Grund-Sicherheit gewährleistet. Da diese aber nicht bei jeder Datenverbindung möglich ist bzw. manchmal auch noch zusätzliche Sicherheitsaspekte berücksichtigt werden müssen, sind oft weitere Maßnahmen erforderlich.

2.1 Grundsätzliche Hinweise zu elektrotechnischen Anlagen

In Gebäuden oder über mehrere Gebäude hinweg gelten in der Regel die Vorgaben der Elektroinstallation. Da spielen Potentialunterschiede eine große Rolle, welche z. B. beim Gewitter auch die Leistung von einem Datennetzwerk beeinträchtigen können. Ein Potentialausgleich ist bei einer normgerecht ausgeführten Elektroinstallation zwar gegeben, eine richtige Netzwerkinstallation ist aber zusätzlich nötig. Regelkonform werden mehrere getrennte Gebäude am besten in Abschnitte aufgeteilt,

die innerhalb eines Gebäudes oder auf einer Etage zwar mit Netzwerkkabel aus Kupfer verbunden werden können, dann aber gebäudeübergreifend mit Glasfaser- bzw. Lichtwellen-Leiter (LWL) zusammengeführt werden. So werden Anlagenteile bei auftretenden Potentialunterschieden geschützt. Potentialunterschiede können nicht nur bei Gewittern vorkommen, sondern es kann auch zu einem ungewollten Spannungsausgleich über die Netzwerkleitungen kommen. Insbesondere elektronische Bauteile, z. B. in Reglern, Steuerungen und PCs, sind extrem empfindlich gegen Überspannungen und werden ohne entsprechende Schutzmaßnahmen (Einbau von Überspannungsschutzgeräten an relevanten Schnittstellen) zerstört.

WLAN-Systeme haben normalerweise damit kein Problem, hängen in der Regel aber auch an der allgemeinen Spannungsversorgung und an einer weiteren Netzwerkkomponente. Hierfür und für alle anderen elektronischen Komponenten im Netz gibt es (Überspannungs-)Ableiter, die Geräte vor schädlichen Überspannungen schützen.

Sie sollten aber Teil eines kompletten Absicherungskonzepts mit Grob-, Mittel- und Feinschutz sein, um so effektiv die meisten Überspannungen ableiten zu können. Für sicherheitsrelevante Verbindungen, wie Alarmmeldungen, sollten verdrahtete Verbindungen bevorzugt werden **oder** die Kommunikation im Netzwerk durch ein Programm überwacht werden, um Ausfälle zu erkennen. Es gibt auch Geräte, die bei Bedarf eine zweite Alarmweiterleitung (z. B. per GSM) nutzen können (siehe auch Hinweise zur Alarmweiterleitung im DLG-Merkblatt 422).

Zudem sind in größeren Gebäuden auch die Vorschriften zum Brandschutz zu berücksichtigen und alle verlegten Kabel bzw. Durchbrüche auch wieder zu verschließen. Bei unsachgemäßer Ausführung, zusammen mit schlecht verdrahteten Anschlussdosen kann dies zu einem großen Performance-Verlust und größeren Störungen führen. Fehler, die hier gemacht wurden, verursachen oft viel Arbeit und Zeit bei ihrer Beseitigung und haben fast immer einen längeren Ausfall der Netzverbindungen zur Folge.

Überlegungen zur elektrischen Betriebssicherheit sind bei der Planung in das Netzwerkkonzept einzubeziehen und verlangen i. d. R. nach fachlichem Beistand. Gerade der Überspannungsschutz sollte mit einem Profi besprochen werden. Auf landwirtschaftlichen Betrieben sind oftmals spezielle Schutzarten zu berücksichtigen.

3. Allgemeine Kommunikationsfragen

3.1 Grundsätzliche Ansprüche

Die Anzahl, die Art und der Ort der Komponenten (Geräte im Netzwerk), die einen Anschlussstecker haben oder eine (W)LAN-Verbindung benötigen, ergeben in der Regel die Größe und Ausführungsart des Netzwerks.

Um das Netzwerk ausbaufähig zu halten, sollte für jeden fest verdrahteten Teilnehmer ein zweiter oder dritter Anschluss in Reserve gehalten werden. In der Regel werden dafür in Schaltschränken Patch-Felder (vorbereitete Anschlussmöglichkeiten) in einer ausreichenden Anzahl vorgesehen und zu den Endpunkten noch eine Dopplung der dort installierten Netzwerkdosen eingerichtet, bevor dort über

Switche eine weitere Splittung der Anschlüsse vorgenommen wird. Im entfernt liegenden Stallbüro wird man häufig diese Variante nutzen müssen. Für alle Teilnehmer, die hier in Zukunft noch an ein Netzwerk anzuschließen sind, kann nachträglich noch eine „Vor-Ort-Aufteilung“ erfolgen.

Der Anschluss für eine Steuerung (der Fütterung, einer Lüftung etc.) zum Stall-PC wird über eine „fliegende“ Verdrahtung in der Regel nur über ein paar Meter ausgeführt. Es muss entschieden werden, ob es mit einem Netzwerkkabel gebündelt als LAN weitergeht oder jeder Teilnehmer sein eigenes Anschlusskabel z. B. zum Büro-PC oder zu einem Router, mit dem Anschlusspunkt zum Internet, bekommt. Sicherheitsrelevante Aggregate (z. B. Not-Lüftung oder Stromversorgung) sollten, genauso wie Alarme, nur über ein überwachtes Datennetzwerk angesteuert werden, ansonsten sollte die konventionelle Verdrahtung gewählt werden.

Viele der heute angebotenen und am öffentlichen Netz-Anschlusspunkt eingesetzten Router können ein WLAN zur Verfügung stellen. In kleineren Netzen kommen häufig noch zusätzliche (WLAN-) Router mit einer Verteilfunktion in Frage. Die Anzahl der Geräte, die hier geleast, gekauft, eingestellt, gewartet, bei einer Störung kontrolliert und später vielleicht ersetzt werden müssen, sind zu berücksichtigen.

Darüber hinaus führen oft die eingeschränkten Übertragungsreichweiten eines WLAN, durch Abschirmungen oder große Entfernungen, zu weiteren Investitionen. Es ist so auch immer wieder nötig, die Übertragung vor Ort auf dem Betrieb zu testen. Eine genaue Festlegung der Reichweite von jedem WLAN-Gerät, bei unterschiedlichsten Bedingungen, ist schwierig und führt oft zu späteren Nach- oder Umrüstungen.

Sollte bei der Planung im Voraus schon zu erkennen sein, dass aus Sicherheitsgründen bestimmte Segmente des Netzwerks später einmal zu trennen sind, bedarf es in der Regel weiterer Überlegungen. Gibt es beispielsweise Netzwerkteilnehmer, die auf keinen Fall sehen dürfen, was ein anderer im gleichen Netz-Segment macht oder sendet, dann sollte schon an eine Möglichkeit der (virtuellen) Trennung vom Netz nachgedacht werden. Switche oder Router an den Anschluss- und Trennpunkten, die programmierbar sind, könnten dafür vorgesehen werden. Mit der entsprechenden Konfiguration (Einstellung) kann eine Netzwerkverbindung über eine entsprechende Adressierung für Teilnehmer, die nicht miteinander kommunizieren sollen, aufgeteilt werden. Allerdings sind Computer, Router und Switche, die ein VLAN (virtual LAN/voneinander getrennte LAN-Segmente) verwalten und beherrschen, oft teurer. Man benötigt auf jeden Fall Fachkenntnisse, die mittels entsprechender Schulung erworben werden müssen.

3.2 Internet und (VoIP) Telefonie

Auf einem großen Teil der landwirtschaftlichen Betriebe wurden in den letzten Jahren unterschiedliche Kommunikationsverbindungen oder -möglichkeiten eingerichtet. Angefangen vom Telefonanschluss über ein Modem, bzw. später einem Router, zum PC oder Stallrechner. Die elektronischen Stall-Komponenten, welche in der Regel nach Firmenvorgaben angeschlossen wurden, führten zu unterschiedlichen Schnittstellen. Auch heutzutage muss man diese Endgeräte und andere bereits vorhandene Systeme, mit ihren gegebenen Kommunikationsmöglichkeiten bei einer betrieblichen Netzwerkplanung berücksichtigen. Es müssen nicht sofort alle älteren Schnittstellen beim Aufbau eines neuen Netzwerks getauscht werden. Oft kann man sie auf aktuelle Schnittstellen umrüsten, was gelegentlich aber sehr aufwändig und teuer werden kann.

Das Internet mit seinen Datenübertragungsmöglichkeiten, einschließlich der Sprach- und Videodienste, wird mittelfristig das Medium der Wahl sein. Alle Geräte die Daten liefern, empfangen und dann vielleicht auch auswerten sollen, müssen mit ihren Schnittstellen daran zu koppeln sein. Ein Beispiel hierfür ist die Umrüstung der Telefonendgeräte auf IP-fähige Varianten. Damit werden in Zukunft alle Daten, Sprach-(**V**oice) und Videodateien über **I**nternet-**P**rotokoll/**o**ver **IP** (VoIP) gesendet. Nach Umstellung auf VoIP dürfen auch analoge Telefonwählgeräte für Alarmierungsfunktionen nicht mehr genutzt werden. Zwar stellen einige Router noch Analoganschlüsse bereit – doch stellt dies keine sichere Verbindung dar. In diesem Fall werden die analogen Signale digitalisiert. Es kann zu gestörten, verzögerten bzw. unterbrochenen Übertragungen aufgrund von Kompatibilitätsproblemen und fehlerhaften Datenkompressionen kommen. Bei der Umstellung auf neue Standards müssen alle bisher eingerichteten Verbindungen, z. B. für Alarmanlagen überprüft werden.

Neue IP-fähige Telefonverbindungen, die über einen Internetanschluss umgesetzt werden, können ohne Spannungsversorgung nicht mehr betrieben werden. Sie müssen dann bei angeschlossenen Alarmanlagen mit einer Notstromversorgung ausgestattet werden. Das können z. B. Akkus, Batterien oder unterbrechungsfreie Spannungsversorgungen (USV) sein.

Es gibt aber leider immer noch Regionen, in denen Teilnehmern keine ausreichende Datentransferrate zur Verfügung steht, z. B. weil die bauliche Anbindung an das öffentliche Netzwerk durch den Provider in ländlichen Regionen veraltet oder nicht vorhanden ist. Sie können teilweise zwar telefonieren, aber für das Internet reicht die zur Verfügung stehende Bandbreite nicht aus. Hier kommen die bisher angebotenen Dienste oder Einrichtungen, oftmals mit stark eingeschränkten Leistungen, u. a. beim Datentransfer, an ihre Grenzen. Auch die Anbieter dieser Dienste zeigen sich, gerade in ländlichen Gebieten mit ihren Angeboten für ein schnelles Netz, nicht von ihrer besten Seite. Wenn man aber über eine ausreichende, zukunftsweisende Infrastruktur auf dem Betrieb, bzw. ins öffentliche Netz nachdenkt, ist immer auch eine ausreichende Datentransferrate relevant.

Neue (Festnetz-/IP-)Telefonanschlüsse werden wohl kaum noch große Schwierigkeiten bereiten, ausreichende Übertragungsgeschwindigkeiten bei Daten zu erzielen. VDSL, eine Zwittertechnik aus Glasfaser und Kupferleitung, erreicht in der Regel auch schon die Geschwindigkeiten, welche für eine gute Bildübertragung geeignet sind. Hausanschlüsse mit Glasfaserkabel (Lichtwellenleiter) bieten für aktuelle und zukünftige Ansprüche eine ausreichende Sicherheit.

Tabelle 2: Aktuell verfügbare Varianten der Mobilfunktechnik

Technik	Durchsatz (theoretisch) bis
GSM (Mobilfunk)	10 kbit/s
GPRS (Mobilfunk 2G)	171 kbit/s
UMTS (Mobilfunk 3G)	384 kbit/s
LTE (Mobilfunk 4G)	1.000 Mbit/s
In Vorbereitung: 5G	10.000 Mbit/s

Ein entscheidender (Auswahl-)Punkt bei der Nutzung eines Mobilfunk-Standards ist die angebotene Datentransferrate. Hier sollte man mindestens eine LTE- oder 4G- (bald 5G-)Verbindung haben, um komplexere Internetdienste nutzen zu können und somit auch die dabei anfallenden Datenraten zu bewältigen.

3.3 Netzwerk und BUS-Systeme

Unterschieden werden auf betrieblicher Ebene auch Netzwerke und BUS-Systeme. Typischerweise sind mehrere Computer an einem Verteiler (Hub, Switch, Router) Teilnehmer eines Netzwerks. Hier können in der Regel weitere Teilnehmer relativ leicht angeschlossen werden. Standards, wie z. B. RJ45-Stecker, die an einem Netzwerkkabel verwendet und mit dem Endgeräte angeschlossen werden, sollen möglichst die gleichen Übertragungsprotokolle nutzen, wie sie auch andere Teilnehmer im Netz verwenden. Dann wird eine Verbindung schnell möglich.

Bei BUS-Systemen gibt es ebenfalls standardisierte Verbindungen zwischen den einzelnen Teilnehmern, sie besitzen in der Regel aber nicht sofort eine Plug-&-Play-Fähigkeit. Das heißt, es können nur Geräte angeschlossen werden, die angepasste bzw. eingestellte Schnittstellen haben und von den Firmen, die das individuelle System aufgebaut haben, dafür zuglassen wurden. Als Beispiele seien hier das BUS-System auf Landmaschinen oder die internen Verbindungen zwischen Lüftungsreglern auf dem Stallgang genannt. Diese sind bei den Herstellern der Geräte, auch wegen ihrer Robustheit, recht beliebt. Ein BUS-System ist somit kein adäquater Ersatz für ein Ethernet-Netzwerk.

Spezielle Anwendungen sollten aber mit Vorsicht genutzt werden. Haben wir mit jedem Computer die Möglichkeit, über ein Netzwerk auf andere Teilnehmer im Netz zuzugreifen, so gelten auch für diese die gleichen Sicherheitsmaßnahmen, wie sie beim Computer angewandt werden müssen. Mit der Struktur eines BUS-Systems lässt sich dieser Aufwand vermeiden. Bei nötigen Veränderungen muss zwar der Installateur des Systems vorbeikommen, in der Regel ist der Kommunikationspfad aber vor Angriffen geschützt.

Vor- und Nachteile: Offene Netzwerkstrukturen können weitgehend eigenständig konfiguriert werden, allerdings ist gegenüber geschlossenen BUS-Systemen ein höherer Sicherheitsaufwand erforderlich.

4. Netzwerke einrichten

4.1 Netzwerkstruktur

Eine wichtige Entscheidung im Computer Netzwerk ist die (Adress-)Struktur. Die meisten privaten Netze werden in der Regel noch mit einer sogenannten IPv4-Adressierung betrieben und man kann sich damit für die meisten Anwendungen erstmal zufriedengeben. Wichtig ist, dass mit Hilfe einer parametrierbaren Netzumgebung spezielle Adress-Bereiche für unterschiedliche Anwendungen reserviert bzw. verwendet werden können. Wie schon in der Einführung bemerkt, können so private und geschäftliche Bereiche, die über ein Kabel laufen, voneinander getrennt werden.

Allerdings muss bekannt sein, welche Bereiche des Betriebs hier voneinander getrennt werden dürfen. Nicht jede betriebliche Anwendung sollte in einem abgeriegelten Netzwerkteil betrieben werden.

Oftmals spielen die Verbindungsmöglichkeiten zu anderen PCs oder nötige Verbindungen in das Internet eine essentielle Rolle. Die meisten Hersteller von Fütterungscomputern, Melkständen oder anderen betrieblichen bzw. landwirtschaftlichen Anwendungen benötigen z. B. für die Fernwartung eine Anschlussmöglichkeit des eigenen Gerätes am öffentlichen Netz. Ohne eine Internetverbindung ist bei einer Störung die schnelle Hilfe über eine Service Hotline in der Regel nicht möglich.

Als erste Sicherheitsmaßnahme wird ein Netzwerk mit seinen Komponenten so aufgebaut, dass ein direkter Anschluss oder Eingriff für Unberechtigte ausgeschlossen werden kann. Dabei wird auf sichere Standorte der Netzwerkkomponenten innerhalb eines Gebäudes genauso geachtet, wie auf die einzurichtenden Passwörter für unterschiedliche Teilnehmer.

Zwei Bereiche sollten in der Regel **immer** getrennt werden

- Anwendungen für die rein private Nutzung, wie z. B.: Mediendienste, Verkaufsportale und Apps zur Unterhaltung.
- Programme zur betrieblichen Nutzung, z. B. Fütterungs- und Lüftungsprogramme, Management- und Melktechnikprogramme sowie die Bereiche mit Programmen für den Austausch von Daten mit dem LKV, die Nutzung der Ackerschlagdateien, die Meldungen zur HI-Tier oder aber für die Schlachtdatenauswertung.

Fragen werden sich auch hier ergeben, z. B. betreibe ich das Portal zum Onlinebanking eher im privaten PC-/Netzwerkbereich oder auf dem betrieblichen Rechner? Wird aber bedacht, dass betriebliche Daten heute relativ sensibel sind und einen hohen Schutz benötigen, beispielsweise über einen aktuell zu haltenden Virenschutz und regelmäßige Datensicherungen, fällt die Entscheidung zum Onlinebanking auf einem Betriebs-PC schon wieder leichter.

Eine professionelle Unterstützung bei strukturellen Netzwerkfragen kann sehr hilfreich und das Honorar dafür eine gute Investition sein. Bei der Firmenauswahl muss bedacht werden, dass Erfahrungen und Referenzen in landwirtschaftlichen Betrieben vorhanden sind. Anders als Großunternehmen in Industrie und Verwaltung haben Landwirte normalerweise keine eigene, unterstützende IT-Abteilung.

Erste Lösungsansätze in einer Netzwerkstruktur konnten so schon aufgezeigt werden. Bereiche, die nicht untereinander kommunizieren müssen, können über ihre IP-Adressen (siehe Kommunikationsstruktur) mit einem eventuell nötigen Deaktivieren der automatischen Adressvergabe (im öffentlichen Bereich sonst der Normalfall), voneinander getrennt werden. Wer aber einen Internetzugang benötigt, bleibt über diese Schnittstelle immer angreifbar.

Darüber hinaus reservieren sich größere Unternehmen oder Organisationen auch gerne weitere Adressbereiche, die es ihnen ermöglichen ein sogenanntes „Subnetting“ zu betreiben. Aber auch das wird alleine keinen ausreichend erhöhten Schutz bieten. Gegen mögliche Angriffe auf den PC und Ausfälle des Systems sollte daher ein spezielles Schutzsystem aufgebaut werden.

Steuerungsrechner sind häufig miteinander verbunden und führen komplexe Steuerungsfunktionen in Echtzeit aus. Diese Produktivsysteme dürfen auf keinen Fall gestört werden, da sonst das Tierwohl gefährdet ist. Werden Farm-PC und Produktivsystem miteinander verbunden um z. B. Management-Programme einzubinden, dann muss gewährleistet sein, dass bei Übernahme des PC durch Hacker

weitere Sicherheitsmechanismen greifen, die eine Manipulation der Steuerungsrechner verhindert. Permanent upgedatete **Virenscanner**, eine Änderung der Standard-Passwörter, sowie **zusätzliche Passwörter** für entsprechende Funktionen sind hier als ein Mittel der Wahl anzuführen. Oftmals machen sich allerdings die Betriebe nicht die Arbeit, die vom Inbetriebnehmer eingerichteten Zugangsrechte mit eigenen Profilen zu ergänzen und diese regelmäßig zu ändern. Hier ist ein neues Bewusstsein notwendig, da der Schaden immens sein kann.

4.2 Nötige Komponenten

Die wichtigsten Netzwerkkomponenten sind die aktiven Teilnehmer. Sie unterliegen zwar immer noch Änderungsansprüchen, aber bei den meisten PCs, Reglern und Steuerungen, die aktiv an einem Datenaustausch teilnehmen, hat sich heute eine einheitliche Schnittstelle durchgesetzt. Dabei wird ein Netzwerk-Standard verwendet, der zusammen mit dem „Ethernet-Protokoll“ und einheitlichen Buchsen und Steckern einen schnellen Verbindungsaufbau ermöglicht. Viele Geräte, und nicht nur solche, die eine Internetverbindung benötigen, verfügen über sogenannte RJ45-Buchsen.

Mit immer größeren Datenübertragungsraten wird es an einigen Stellen nötig sein, beispielsweise Lichtwellenleiter einzusetzen, die über einen Glasfaserkern die Daten per Licht übertragen können. Diese Verbindungen werden, besonders wegen ihrer Sicherheit gegen Überspannungen, gerne in der gebäudeübergreifenden Verkabelung eingesetzt.

Um das Lichtsignal nutzen zu können, sind Medienkonverter nötig, die Stromsignale in Licht und umgekehrt wandeln können. Neue Anschlüsse im Haus werden heute schon vom Netzbetreiber damit ausgestattet.

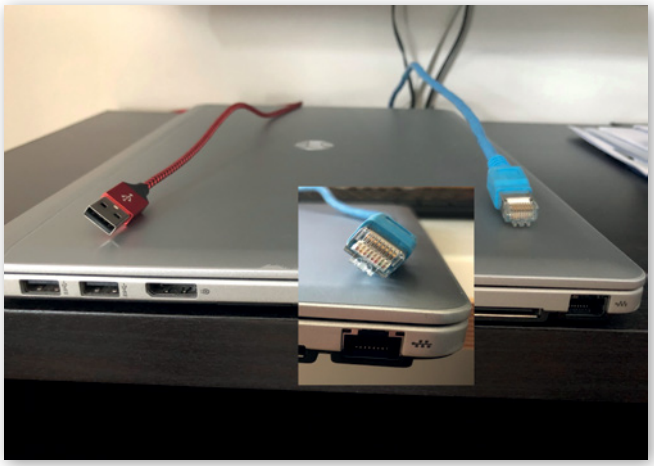


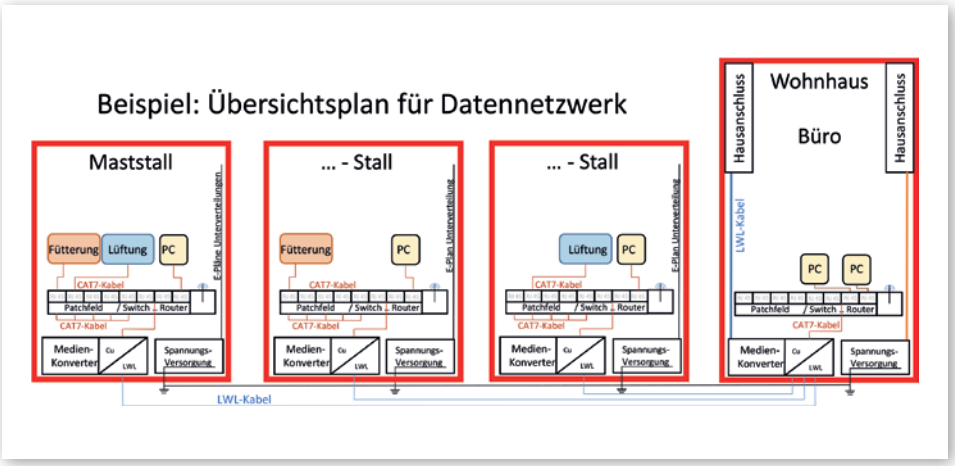
Abbildung 1: PC-Anschlüsse RJ45 und USB (Quelle: Feldmann)

Abbildungen 2 und 3: LWL-Kupplung, links mit Bajonettverschluss, rechts 2x am Medienkonverter (Quelle: Feldmann)

4.3 Router und weitere Geräte

Neben dieser physikalischen Verbindung ist auch noch ein aktives Gerät nötig, über das kommuniziert werden kann. Am Netzanschlusspunkt im Haus wird ein Signal aus einem Kupfer- oder Lichtwellenleiter über eine Anschlussdose zur Verfügung gestellt. In örtlicher Nähe werden meistens die bereits genannten Router verbaut. Die Router verfügen über eine gewisse Intelligenz und speichern z. B. auch die Benutzerdaten vom Kunden oder weitere grundlegende Parameter für den Anschluss. An den entsprechenden Buchsen des Routers können mehrere Geräte angeschlossen werden. So wird eine erste interne Verteilung im lokalen Netzwerk hergestellt.

Dann folgen in einem einfachen Netz auch schon die aktiven Netzwerkteilnehmer wie Computer und Steuerungen. Diese nutzen bei einer Kommunikation untereinander auch die zuvor genannten Kabel und eingesetzten Verteiler. In einigen Fällen ist für diese Geräte aber auch ein anderer Anschluss am PC nötig. Häufig sind das USB-Schnittstellen, die neben den mobilen Teilnehmern auch von bzw. für Daten-Sticks genutzt werden.



Abbildungen 4 und 5: Netzwerkschrank (links) und Netz-Übersichtsplan (rechts)

Eine heute sehr verbreitete Art der Verbindungen über das eigene Netzwerk, welche auch Router am Anschlusspunkt im Haus zur Verfügung stellen können, sind die bereits erwähnten Zugänge über ein WLAN mittels Wireless Access Point. Diese Technik stößt aber an physikalische Grenzen und die dafür notwendigen Sicherheitsaspekte sind umfangreich. Die Nutzung eines WLAN-Netzes hängt von verschiedenen baulichen und technischen Voraussetzungen ab. Bei Nutzung entsprechender Router und Antennen mit Sichtverbindung ist eine Datenübertragung auch über größere Entfernungen möglich.

Eine schlechte Verbindung oder Erreichbarkeit innerhalb eines WLAN kann oft mit einer zusätzlichen Ausstattung verbessert werden. Da, wo ein Netzwerkkabel nicht neu verlegt werden kann oder soll, ist ein Repeater in der Lage, ein schwaches Funk-Signal zu verstärken. Mit entsprechenden Übertragungsgeräten können über Power-Line-Verfahren auch die Leitungen der elektrischen Ge-

Abbildung 6: An Power-Line-Adapter können übliche Netzwerkkomponenten angeschlossen werden (Quelle: AVM)

bäudeinstallation für eine Daten-Übertragung genutzt werden. Wenn die gleiche Phase der Stromleitung an den gewünschten Anschlussstellen vorhanden ist, kann eine Datenübertragung recht einfach stattfinden. Sollten in unterschiedlichen Gebäudeteilen unterschiedliche Phasen liegen, gibt es dafür Phasenkoppler, die in der Strom-Hauptverteilung installiert werden. Allerdings ist die Power-Line-Datenübertragung im landwirtschaftlichen Betrieb durch Schalthandlungen von großen Verbrauchern häufiger störanfällig.

Neuere PCs mit geringer Ausstattung stellen in einem Netz andere grundsätzliche Ansprüche. Viele dieser Geräte haben heute keine physikalischen Anschlussbuchsen für einen Netzwerkanschluss mehr und sind auf Funkverbindungen angewiesen. Dazu müssen aber auch die entsprechenden Teilnehmer/Gegenstellen im Netz über diese (Funk-)Standards erreichbar sein bzw. damit ausgestattet werden.

Bei Sichtkontakt (bis ca. 10 m) können z. B. Tablet-PCs, bei entsprechender Ausstattung, untereinander auch über Bluetooth-Verbindungen relativ leicht Daten austauschen. Diese Verbindungen erfordern keine besonderen Netzwerkkenntnisse, sind in der Regel aber auch in der Anzahl der teilnehmenden Geräte begrenzt und nicht besonders sicher.

Teilnehmer einer Bluetooth-Verbindung sind für andere sichtbar und keine geschlossene Gruppe. Die nötigen Zugangsbedingungen wie auch die Datenverschlüsselung und andere Sicherheitsmaßnahmen werden oft nur minimalistisch ausgeführt.

Gibt es eine größere Anzahl von Netzwerkteilnehmern, eventuell mit gemeinsamem Internetzugang, und stehen sie räumlich weiter auseinander, wird oft ein WLAN-Netzwerk (nach IEEE-Standard WiFi genannt) genutzt, Bluetooth scheidet schon aufgrund der geringen Reichweite aus. Im WiFi-Standard sind bei freier Sicht Entfernungen von rund 100 m möglich. Diese Strecke kann aber durch Gebäude oder andere Dinge, die unterschiedlich stark abschirmen, beeinträchtigt bzw. reduziert werden. Ist das der Fall, müssen wieder zusätzliche Einwahlpunkte (= Access-Points) eingesetzt werden, die untereinander meistens mit einem Kabel verbunden werden. Nur in bestimmten Fällen kann ein empfangenes schwaches Signal über einen Repeater verstärkt und per Funk weitergegeben werden. Die örtlichen Bedingungen (z. B. in Gebäuden mit viel Beton oder Stahl) zwischen Sender und Empfänger entscheiden über die nötigen, sehr individuellen Ausstattungsvarianten.

Abbildung 7: WLAN Access Point (Quelle: Feldmann)

Zusammen mit dem physikalischen Aufbau eines WLAN muss immer eine sicherheitstechnische Konfiguration des Netzes erfolgen. Ganz wichtig ist heute ein guter Verschlüsselungsalgorithmus (z. B. WPA2 im WiFi) mit sicheren Schlüssel- bzw. Passwörtern. Viele WLAN-Router oder Access-Points sind damit standardmäßig ausgestattet. Es ist sinnvoll, die Zugangsdaten individuell anzupassen.

4.4 Kommunikationsstruktur (zur Sicherheit)

Für die Kommunikation wird in einem Netz erst einmal ein Adressbereich verwendet und es bedarf dann keiner weiteren Struktur. Greifen verschiedene Teilnehmer voneinander getrennt auf den gleichen Adressbereich zu und nutzen damit die gleichen Ressourcen, kann eine Aufteilung sinnvoll sein. Das hängt von den Komponenten ab, die angeschlossen werden. Die notwendige Regelung ist in Absprache mit Sachkundigen der jeweiligen Hersteller von anzuschließenden Komponenten zu treffen. Die einmal getroffene Regelung wird auch zukünftig für neue Netzwerkteilnehmer entscheidend sein und muss deshalb dokumentiert werden.

Beispiel:

Über den Internetanbieter und den am Hausanschluss eingesetzten Router ist die IP-Adresse: 192.168.**2.**1 für die eigene Nutzung vorgesehen. Damit befindet man sich in einem Adressbereich, der auch als Subnetzmaske bezeichnet wird. Diese Subnetzmaske hat z. B. die Bezeichnung: 255.255.255.0 erhalten. Alle Geräte, die mit diesem Anschlusspunkt gekoppelt werden, bekommen dann durch eine automatische Adressvergabe (DHCP-Funktion) eine Geräteadresse zugewiesen. Diese kann am Ende von *.*.*.0 bis *.*.*.254 hochlaufen und alle Geräte, die in diesem Bereich liegen, können miteinander kommunizieren. Ist eine Trennung der Geräte über verschiedene Netzwerkadressen erwünscht, so kann das dadurch ermöglicht werden, dass man für diese Teilnehmer beispielsweise die Adresse 192.168.**3.**1 verwendet. Somit können unter dieser Adresse auch wieder Clients bis *.*.*.254 (automatisch) adressiert werden.

Achtung: Ein Datenaustausch über unterschiedliche Adressbereiche hinweg ist nur möglich, wenn man in einem Router entsprechende Ausnahmen zulässt!

Manchmal ist die Entscheidung wichtig, ob die DHCP-Funktion mit einer automatischen Adressvergabe der richtige Weg ist. Geräte, die sporadisch an ein Netz angeschlossen werden, behalten nicht unbegrenzt die ihnen einmal zugewiesene Adresse. Hier kann es sinnvoll werden, bestimmten Geräten eine feste Adresse zuzuweisen. Das muss dann in der Netzwerkkonfiguration des Gerätes (hier Client) und auch in der Konfiguration des Routers (= Server) berücksichtigt und dokumentiert werden.

Jede Einstellung beim Netzaufbau, die über den PC oder im Router erfolgt, kann auch wieder mit Ausnahmen versehen werden. Wird eine physikalische Netzwerkstruktur für mehrere Adressbereiche benutzt, sind oft auch programmierbare Switche an den Schnitt- oder Übergangsstellen der Netzwerke nötig, um Ausnahmen oder Regeln in der Kommunikationsstruktur zuzulassen. Ein typisches Beispiel ist immer dort gegeben, wo sich z. B. Netzwerkteilnehmer aus unterschiedlichen Bereichen einen Drucker teilen.

Diese speziellen Einstellungen sollten mit Netzwerkprofis besprochen und geplant werden. Für jeden, der einen neuen Client auf dem Betrieb oder im Büro anschließt, muss die Struktur erkenntlich und dokumentiert sein. Nur so können spätere Installationen schnell ausgeführt oder durch Anpassungen integriert werden.

Dabei ist es entscheidend, wie das Netzwerk aufgebaut wurde.

Stern- oder Baum-Topologien sind oft der gewünschten oder nötigen Funktion entsprechend über die Verkabelung vorgegeben. Nicht jeder PC kann sofort mit einem anderen Teilnehmer kommunizieren, ohne dass eine entsprechende physikalische Verbindung eingerichtet worden ist.

Die Netzwerkkabel aus den Geräten werden heute meistens sternförmig zu einem zentralen Verteiler zusammen und von dort aus gemeinsam zu einem nächsten Punkt weitergeführt.

Die Baum- und die Bus-Topologie werden in der PC-Welt nur bei der Verbindung von Sternpunkten eingesetzt. Alles zusammen entscheidet über den Einsatz der nötigen Bauteile sowie der zu verlegenden Kabel und muss für die Fehlersuche und den Anschluss neuer Teilnehmer dokumentiert werden.

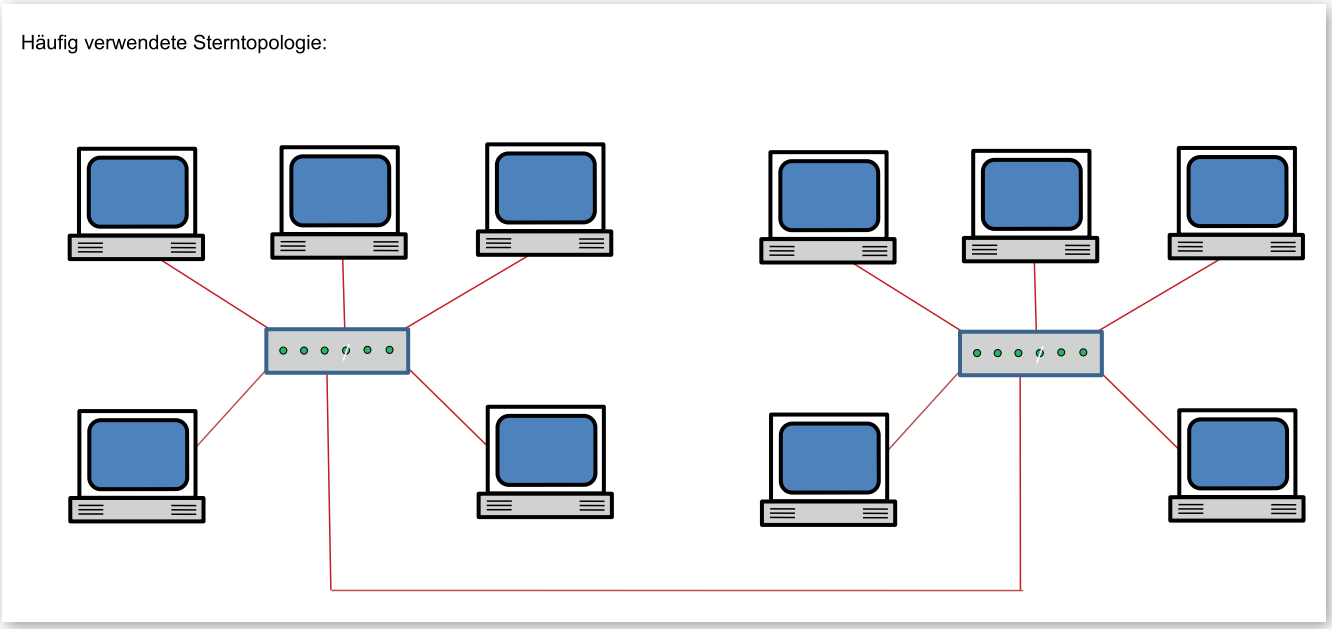


Abbildung 8: Häufige Versionen sind Baum-, Bus- und Stern-Topologien

Um eine spätere Wartung zu ermöglichen und den Überblick im eigenen Netz zu behalten, ist eine möglichst genaue Dokumentation nötig. Diese ist fast so wichtig wie das Netz selbst. Ohne sie kann man bei den kleinsten Problemen vor großen Herausforderungen stehen und wird viel Zeit mit einer unnötigen Störungssuche verbringen.

Die Entscheidung für eine bestimmte Struktur hängt als erstes von den Aufgaben des Netzwerks ab und davon, wie aufwändig das Netz gestaltet wird. Es muss immer daran gedacht werden, dass die eingesetzten Komponenten sehr schnell veralten und keine langen Standzeiten haben. Darüber hinaus sollte berücksichtigt werden, dass die preiswerten Geräte für die Büroumgebung und den Hausgebrauch mit einer Schutzklasse IP21 (tropfwassergeschützt) im Stall keine langen Überlebenschancen haben.

Drei bis fünf Jahre für elektronische Geräte oder zehn Jahre für andere Hardware sind gute, realistische Abschreibungszeiten. Mit zunehmendem Umfang der ausführbaren und nötigen Funktionen wurden die bisher möglichen Einsatzzeiten immer kürzer. Im einfachsten Fall kann ein Gerät mittels Updates weiter betrieben werden. Dafür müssen Schnittstellen vorhanden sein, die die notwendigen Updates ermöglichen. Zu bedenken ist in diesem Zusammenhang, dass diese Updates nicht immer kostenlos sind.

5. Datenübertragung und Datensicherheit

5.1 Sicherheitsaspekte

Ein großer Teil der Clients/der Geräte am Netz kommuniziert bei Bedarf über externe Strukturen wie das Internet mit anderen Geräten. Die Geräte verbinden sich aber auch mit Hard- oder Softwarehäusern. Der Anschluss eines externen Datenträgers oder die Kommunikation mit externen Strukturen macht die Systeme unsicher. Es kann daher vorkommen, dass mit Angriffen von außen gerechnet werden muss. Schadsoftware und Viren übernehmen die Kontrolle der eigenen Geräte und der eigene Zugriff darauf wird beeinträchtigt oder unmöglich. Dies kann dazu führen, dass Datenbanken zerstört oder verschlüsselt werden. Eine Wiederinbetriebnahme ist dann nur nach Zahlung eines Lösegeldes oder überhaupt nicht mehr möglich.

Da, wo es möglich ist, muss eine Firewall zwischen externem Netz und dem eigenen Gerät vor Fremdzugriffen schützen. Da trotzdem Schadsoftware und Viren auf die eignen Geräte gelangen können, sollten (Viren-)Schutzprogramme mit unterschiedlichen Funktionen installiert und immer auf einem aktuellen Stand gehalten werden. Mittlerweile geht es aber nicht nur um Datendiebstahl, auch vor Hackerangriffen gilt es sich und sein System zu schützen. Hier ist definitiv Unterstützung von Experten nötig, um ausreichende Sicherheit zu gewährleisten.

Außerdem sollten Betriebssysteme in leicht zugänglichen Strukturen, z. B. auf PCs, regelmäßig mit aktuellen Updates versorgt werden. Da es dennoch zu einem Ausfall, vielleicht auch wegen Störungen an der Hardware, kommen kann, sollte regelmäßig ein Backup (= aktuelle Datensicherung) der eigenen Daten gemacht werden. Viele dieser Aufgaben, die heute zum großen Teil auch schon automatisch ablaufen, können auch manuell eingerichtet werden.

Über ein Werkzeug in der Firewall des PC-Netzes (Access List) kann außerdem eine erste Auswahl getroffen werden, wem überhaupt welcher Zugang zum eigenen Bereich oder Rechner gewährt wird. Hierbei ist es erforderlich, dass die IP-Bereiche (oder -Adressen) bekannt sind und klar ist, welcher Dienst oder welcher Datenverkehr von den Netzwerkteilnehmern normalerweise ausgeht und somit zugelassen werden muss. Der normale Anwender kommt ab diesem Punkt in Bereiche hinein, die auch bei kleinen Betriebsnetzen von Kennern der Materie aufgestellt werden sollten. Nicht jeder, der eine Anwendung oder ein Betriebsmittel für den landwirtschaftlichen Bedarf auf dem Betrieb installiert, weiß sofort, welcher Bereich im Netz für die eigene und die Steuerungen von nebenan gebraucht und für interdisziplinäre Anwendungen zugelassen werden muss.

Wichtige Sicherheitsaspekte:

Es sollte eine Firewall für die Netzwerkteilnehmer aktiviert sein, ein aktuell gehaltenes Virenschutzprogramm auf den Geräten laufen, beim WLAN eine Verschlüsselung z. B. nach WPA2-Standard genutzt und die Gerätesoftware aktuell gehalten werden.

5.2 Datensicherung

Für den Fall, dass lang erarbeitete Daten zerstört wurden, sollte eine möglichst aktuelle Datensicherung vorhanden sein.

Dazu können unterschiedliche Möglichkeiten genutzt werden. Eine Möglichkeit ist, sich z. B. nur auf das eigene System zu verlassen. Ein automatisches Backup, bei vielen Betriebssystemen oder Anwendungen bereits mitgeliefert, ist ein erster Rettungsschirm. Bei speziellen landwirtschaftlichen Anwendungen wie z. B. Herdenmanagementsystemen oder Finanzprogrammen sollten Hersteller bzw. Lieferanten auf jeden Fall ein firmeneigenes Sicherungssystem oder -konzept anbieten. Datensicherungen für Betriebssysteme stellen bei einem Crash in der Regel nicht die speziellen Dateien einer Anwendung wieder her. IT-Systeme können, wie alle anderen technischen Systeme auch, entweder durch technisches oder menschliches Versagen ausfallen. Auch wenn das Risiko klein erscheint, können auch vergleichsweise kurze Ausfälle erhebliche Folgen haben (z. B. Ausfall der Stalllüftung oder der Abruffütterung mit den Daten für jedes einzelne Tier). Es sollten immer Pläne vorhanden sein, wie bei einem Ausfall vorgegangen wird und entsprechende Einrichtungen wie z. B. Notstromaggregate einsatzbereit vorgehalten werden.

Um für den Extremfall gut gerüstet zu sein, sind auch Datensicherungen immer eine wichtige Maßnahme. Deshalb gehören entsprechende Strategien auch in einem Netzwerk immer dazu. Generell geben viele ihre Daten nicht gerne an Dritte weiter und versuchen, ein Konzept im eigenen Netz aufzubauen. Ein wichtiger Sicherheitsaspekt ist dabei immer, die zu sichernden Daten nicht auf dem gleichen Rechner abzuspeichern, auf dem auch die eigentliche Anwendung läuft. Wird dieses System, z. B. durch ein Überspannungsereignis zerstört, hilft oftmals auch nicht die zweite Festplatte an der gleichen Spannungsversorgung. Ein externer Speicherplatz ist immer die bessere Wahl.

Baut man ein Betriebsnetz auf, können separate Speicherplätze, die nicht an der gleichen Spannungsversorgung im Stall hängen und für mehrere Sicherungsaufgaben gleichzeitig eingesetzt werden, eine Verwendung finden. Dabei werden häufig NAS-Server (Network Attached Storage) eingesetzt, die kleine Rechner sind und oft mehrere Festplatten zur ein- oder mehrfachen Datensicherung haben.

Zu beachten:

- Bei einem einzelnen Gerät kann meistens direkt auf diesem oder auf einem angeschlossenen Datenträger abgespeichert bzw. gesichert werden.
- USB-Sticks oder zusätzliche Festplatten die intern, mobil und auf externen (Netzwerk-)Geräten installiert sind, werden dabei häufig auch genutzt.
- Eine täglich, wöchentlich oder monatlich wechselnde Nutzung von mehreren, mindestens zwei oder drei getrennten Speichermedien, erhöht die Sicherheit.
- Vernetzte Systeme nutzen in der Regel den gleichen Speicherplatz, so braucht man für dort eingerichtete Datensicherungsmöglichkeiten nur einmal Aufwand betreiben.

Wichtig: Daten auf mehreren, physikalisch bzw. elektrisch voneinander getrennten Speichern sichern, damit beim Geräteausfall oder einer Überspannung nicht sofort alles verloren ist!

Außerdem besteht natürlich bei allen einzelnen oder netzwerkbasierten PCs und Geräten, die an das Internet angeschlossen sind, die Möglichkeit, eine Sicherung im Netz vorzunehmen. Cloud-basierte Lösungen ermöglichen es, eine Foto-, Musik- oder Daten-Datei überall dort zur Verfügung zu haben,

wo mit einem Endgerät das öffentliche Netz erreicht wird. Von Buchhaltungsunterlagen bis zum allgemeinen Schriftverkehr kann heute alles online abgespeichert werden.

Auch Firmen, die spezielle landwirtschaftliche Lösungen haben, bieten entsprechende Systeme für ihre Kunden an. Vorteilhaft ist auf jeden Fall ein möglicher Datenzugriff von verschiedenen Standorten, bei gleichzeitiger externer Absicherung der Daten.

Eine Voraussetzung ist dabei wieder ein permanent verfügbarer Internetzugang, der gut abgesichert sein muss und vor allem eine ausreichende Datenübertragungsrate hat. Für die Dienstleister der Datenabsicherung besteht in der Regel eine Sorgfaltspflicht, welche meistens in den AGBs der Firmen aufgeführt ist.

Es gibt sogar Online/Cloud-Lösungen, die interdisziplinär arbeiten, d. h. verschiedene Anwendungen in einem Betrieb stellen ihre abgespeicherten Daten für autorisierte Dritte zur Verfügung. Ein Weg, der in den nächsten Jahren wohl an Bedeutung zunehmen wird und einige Anwendungen auf dem Betriebs-PC überflüssig macht. Dort werden dann nur noch Apps zur Erfassung und Auswertung der Daten installiert sein. Die meisten Daten, die dann noch für spezielle Fragen gebraucht und ausgewertet und im Anschluss wieder abgespeichert werden, befinden sich zukünftig in einer Cloud.

5.3 Besonderheiten

Für Besucher in Wohnhäusern oder Betrieben hat es sich heute schon etabliert, einen Gast-Zugang in das Netz, in der Regel über das WLAN, zur Verfügung zu stellen. Dieser Zugang kann über eine separate Adressierung und ein spezielles Kennwort im abgeschirmten Bereich zur Verfügung gestellt werden und zur weiteren Sicherheit beitragen. WLAN-Systeme gibt es in den Bereichen 2,4 GHz (Standard) und 5 GHz (meist höhere Bandbreite). Bei der Benutzung bestimmter Kanäle, z. B. in der Nähe von Flugplätzen, kann es lokal rechtliche Einschränkungen geben.

Wenn der Netzanschluss im Außenbereich nur unzureichend ist, also kein entsprechender Kabel- oder Glasfaseranschluss oder eine 4 bzw. 5G-Funkverbindung besteht, dann bleibt als Alternative nur noch die Internetanbindung über eine Satellitenanlage. Hier wird per normaler Telefonverbindung eine Datenanforderung an das Netz gestellt und über Satelliten kann diese dann, mit angemessener Übertragungsgeschwindigkeit, empfangen werden. Gerade Betriebe in ländlichen Gebieten können davon betroffen sein. Sie haben damit allerdings nur eine ausreichende Downloadrate, die Uploadrate zum Einstellen von Daten ins Internet ist noch deutlich niedriger.

6. Regelwerke und Richtlinien

Es existieren viele Hinweise und Regularien, die bei der Auswahl und Installation von Netzwerken eine Rolle spielen und immer wieder als Quelle zur Klärung offener Fragen herangezogen werden. Die Forderung an Installateure ist deshalb, relevante Richtlinien einzuhalten und vor allem die immer wieder neuen Vorgaben seitens des BSI (Bundesamt für Sicherheit in der Informationstechnik – https://www.bsi.bund.de/), besonders im Bereich der Empfehlungen zur Einhaltung einer nötigen Datensicherheit, zu berücksichtigen.

6.1 Relevante Organisationen und Verbände

- Die IEC (International Electrotechnical Commission) ist eine internationale Normungsorganisation für Normen im Bereich der Elektrotechnik und Elektronik mit Sitz in Genf (https://www.iec.ch/).
- Einige Normen werden gemeinsam mit der ISO (International Organization for Standardization) entwickelt (https://www.iso.org/).
- Das IEEE (Institute of Electrical and Electronics Engineers) ist ein weltweiter Berufsverband von Ingenieuren aus den Bereichen Elektrotechnik und Informatik. Er bildet unter anderem Gremien für die Standardisierung von Technologien, Hardware und Software (https://www.ieee.org/).

7. Fazit

In landwirtschaftlichen Betrieben steigen mit zunehmender Spezialisierung die komplexen Anforderungen an die Regelung, Steuerung und Überwachung von Produktionsanlagen sowie die Auflagen zur Datenauswertung, Dokumentation und Datenweitergabe an Dritte deutlich an. Voraussetzung für das Gelingen dieser Aufgaben ist die betriebsinterne Vernetzung der vielen elektronischen Geräte und PCs. Dadurch wird der Zugriff auf die an unterschiedlichen Stellen im Betrieb anfallenden Daten erst möglich.

Bei der Einrichtung einer umfänglichen Vernetzung ist die Unterstützung durch Fachfirmen sinnvoll. Es sollten nur Firmen beauftragt werden, die über Erfahrungen und Referenzen in landwirtschaftlichen Betrieben verfügen. Im Gegensatz zu Industrieunternehmen oder Behörden ist der Betriebsleiter oft der einzige „Angestellte“ in der IT-Abteilung. Er muss den Durchblick und die Übersicht behalten. Die Sicherung vor Angriffen und Datendiebstahl von außen muss ebenso bedacht werden wie die Sicherung der Betriebsdaten durch regelmäßige Backups.

DLG-Merkblätter.
Wissen für die Praxis.

- DLG-Merkblatt 447
  Digitalisierung in der Landwirtschaft
- DLG-Merkblatt 446
  Investitionsrechnung in der Landwirtschaft
- DLG-Merkblatt 434
  Mehrgefahrenversicherungen in der Landwirtschaft
- DLG-Merkblatt 428
  Digitalisierung 4.0 für das landwirtschaftliche Büro
- DLG-Merkblatt 422
  Alarmierungs- und Sicherungseinrichtungen in Stallanlagen

Download unter www.DLG.org/Merkblaetter

DLG e.V.
Mitgliederservice
Eschborner Landstraße 122 • 60489 Frankfurt am Main
Deutschland
Tel. +49 69 24788-205 • Fax +49 69 24788-124
Info@DLG.org • www.DLG.org