Plötzlich geht nichts mehr

Cyber-Angriff in der Landwirtschaft

»Es gibt zwei Arten von Unternehmen: solche, die schon gehackt wurden, und solche, die es noch werden.«

[Robert Müller, Direktor des FBI a. D.]

Der Vizepräsident des Bundesamts für Sicherheit in der Informationstechnik schrieb im Februar 2023 in seinem Vorwort zur Cyber-Sicherheit für KMU (kleine und mittlere Unternehmen) *„Sagen wir es ganz offen: Die Situation in Bezug auf Cyber-Sicherheit ist in der überwiegenden Zahl der KMU besorgniserregend."*

Schon acht von zehn Landwirten setzen bereits heute auf digitale Technologien. Weitere 10 % planen und diskutieren das. Die Zukunft der Landwirtschaft ist digital: Roboter melken Kühe, Drohnen erkennen Pflanzenkrankheiten und kartieren Ackerschläge und Sensoren erfassen Vitaldaten von Tieren *(Quelle: Deutscher Bauernverband)*. Diese Liste lässt sich noch beliebig erweitern. Motivation für die Landwirte, in diesem Bereich stark zu investieren, sind häufig die Effizienz sowie Themen wie Nachhaltigkeit und ressourcenschonendes Wirtschaften. Dies birgt jedoch ein nicht zu unterschätzendes Risiko für die Landwirtschaft und jeden einzelnen landwirtschaftlichen Unternehmer.

Beispiel **01**

Bild 1 / Precision Farming auf dem Schlepper

Ein Landwirt hat eine Mail mit einem Schadanhang geöffnet **(Bild 1)**. Durch das Öffnen des Anhangs wurde der Trojaner aktiviert und hat sich im System „versteckt". Nach zwei Wochen wurden die vorhandenen Daten verschlüsselt, sämtliche Programme konnten nicht mehr ausgeführt werden. Es wurde ein Lösegeld in Höhe von 25.000 Euro gefordert, das der Landwirt nicht gezahlt hat. Durch das Hinzuziehen von Cyber-Experten konnten die Daten wiederhergestellt werden. Für die Wiederherstellung der Daten sowie die forensischen Untersuchungen sind Kosten in Höhe von **12.000 Euro** entstanden.

Beispiel **02**

Bild 2 / Fütterungssystem

Ein Landwirt, der auch als Lohnunternehmer tätig ist, wurde gehackt **(Bild 2)**. Durch eine Sicherheitslücke bei der eingesetzten Software konnten die Hacker in das System vordringen. Dort wurden dann unter anderem die Kalender verschlüsselt, sodass der Maschineneinsatz nicht mehr koordiniert werden konnte. Dadurch konnten nicht alle Aufträge erfüllt werden und Ansprüche Dritter wurden geltend gemacht, weil Aufzeichnungen (Pflanzenschutzmitteleinsatz, Gülleausbringung oder Ähnliches) und Dokumentierungen nicht möglich waren. Schaden: **128.000 Euro.**

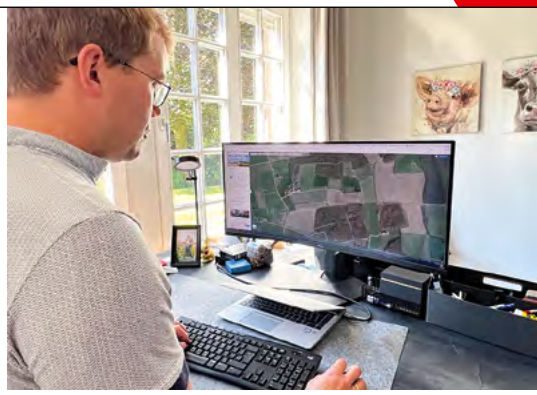

Bild 3 / Pflege der Ackerschlagdatei

Dies sind nur zwei Beispiele, die die Sensibilität dieser Technik aufzeigen. Mit zunehmender Digitalisierung der landwirtschaftlichen Betriebe wächst das Risiko für folgenschwere Cyber-Angriffe.

Noch gibt es keine eigenen Statistiken zu Cyber-Angriffen in der Landwirtschaft, diese werden aber deutlich steigen, denn viele Landwirte sind breitgefächert aufgestellt (GPS-Geräte auf den Schleppern, GPS-gesteuerte Landmaschinen, Steuerung von Biogasanlagen via Handy, Windkraft, Lüftungs- und Melkanlage, Ferien auf dem Bauernhof, Hofladen). Und wenn dann noch sensible Daten (wie z. B. Kontoverbindungen) von Kunden des Landwirtes in die Hand der Hacker geraten, kann es besonders teuer werden. **(Bild 3)**

Laut Bundesamt für Sicherheit und Informationstechnik (BSI) waren im Jahre 2022 69 % aller Spam-Mails Cyber-Angriffe wie Phishing-Mails und Mail-Erpressung. 90 % des Mail-Betrugs war Finance Phishing, d. h., die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein. Im Jahr 2021 wurden 146.000 Cyber-Straftaten gemeldet. Dies entspricht einem Zuwachs von 12 % im Vergleich zu 2020. Die tatsächliche Anzahl liegt vermutlich noch deutlich höher.

Technische und organisatorische Maßnahmen können helfen, den landwirtschaftlichen Betrieb zu schützen, zumindest aber auf einen Angriff vorzubereiten. Mangelhaft abgesicherte E-Mail-Konten, Fernzugriffsrechte, veraltete Rechner und Server stellen eine häufige Schwachstelle dar. ▶

WAS BIETEN HEUTIGE CYBER-VERSICHERUNGEN?

Nach einem Cyber-Angriff drohen hohe wirtschaftliche Schäden, gegen die sich der Landwirt und die landwirtschaftliche Unternehmung versichern können.


© Adobe Stock/Budimir Jevtic

Was die Cyber-Police bieten sollte

Die Cyber-Versicherung bietet im Rahmen von modular wählbaren Bausteinen Versicherungsschutz bei Schäden, die durch eine Verletzung der Informationssicherheit auftreten. Der Versicherungsschutz wird nach den Bedürfnissen der Unternehmung zusammengestellt. Der Versicherer agiert gemeinsam mit dem Landwirt als Krisenmanager, wehrt unberechtigte Ansprüche ab und unterstützt, sollte es zu einem Prozess kommen.

Diese Bausteine können versichert werden:

1 Haftpflichtschäden

- wegen eines Verstoßes gegen Datenschutzbestimmungen
- fahrlässige Bekanntgabe von fremden Betriebs- und Geschäftsgeheimnissen auf dem digitalen Weg
- wegen Weiterverbreitung von Computerviren an Dritte
- wegen einer Verletzung von Persönlichkeitsrechten nach einem Hacker-Angriff
- wegen Verstößen gegen E-Payment-Vereinbarungen

2 Eigenschäden

- Kosten für die Wiederherstellung der Daten, der Systeme und des Netzwerks nach einem Hackerangriff
- Übernahme von Vertragsstrafen wegen Nichterfüllung von vertraglichen Liefer- und Abnahmeverpflichtungen
- Kosten für IT-Forensiker, die den Sachverhalt schnell aufklären, sofortige technische Hilfe garantieren und gerichtsverwertbar dokumentieren
- Kosten für Krisenmanagement und PR-Maßnahmen nach einem Hackerangriff

3 Vertrauensschäden

- Ersatz von Schäden für von Hackern durchgeführte Überweisungen
- Ersatz von eigenen Überweisungen nach Täuschungen über den eigenen gehackten E-Mail-Server
- Schäden infolge von unberechtigter Nutzung der IT-Systeme (Krypto-Mining)

4 Ertragsausfallschäden

- kommt es zum Beispiel aufgrund eines Virenangriffs zu einem Stillstand eines Biogas-BHKW, übernimmt der Versicherer die durch den Produktionsausfall entstehenden Kosten wie z. B. Gewinnausfall, fortlaufende Kosten
- die Haftzeit beträgt sechs Monate
- nur acht Stunden zeitlicher Selbstbehalt

Was kann der geschädigte Landwirt vom Cyber-Versicherer erwarten:

- sofortige technische Hilfe im Schadenfall (Forensik / Wiederherstellung der Daten), und zwar 24/7/365
- sofortige rechtliche Beratung
- Abwehrkosten bei behördlichen Verfahren
- Abdeckung der Kosten und Aufwendungen

Der Versicherungsfall für alle Bausteine ist die erstmalige Entdeckung der Informationssicherheitsverletzung durch den Versicherungsnehmer. Es gilt eine unbegrenzte Rückwärtsversicherung für bei Vertragsschluss schon vorhandene, aber nicht erkannte Cyber-Schäden. Die Nachmeldefrist (nach Vertragsende) beträgt drei Jahre.

Wie berechnet sich der Beitrag für eine Cyber-Versicherung?

Der Beitrag richtet sich i.d.R. nach dem durchschnittlichen Umsatz der landwirtschaftlichen Unternehmung und der Versicherungssumme. Die Versicherungssumme kann der Landwirt aufgrund seiner eigenen Bewertungen, bezogen auf eine mögliche Schadenhöhe, individuell abhängig von seinen spezifischen Betriebsrisiken selbst festlegen.

WIE KANN DER LANDWIRT SEIN CYBER-SICHERHEITSNIVEAU ERHÖHEN?

Diesen Fragen müssen sich die Unternehmer stellen und sind beim BSI abrufbar und werden dort intensiv beantwortet. *(Quelle: BSI-BroKMU22/001)*

FRAGEBOGEN

1 *Wer ist verantwortlich?*

- Immer der Unternehmer; er kann natürlich delegieren, aber verantwortlich bleibt er!

2 *Wie gut kennen Sie Ihre IT-Systeme?*

- Um die entsprechenden Schutzmaßnahmen abzuleiten, ist eine Bestandsaufnahme notwendig.
- Empfohlen wird die Auflistung:
  - aller Komponenten (Computer, Smartphones, Tablets, lokale Server usw.), dazu gehören auch die Peripheriegeräte (Drucker, Scanner, Router, Stallcomputer usw.),
  - der eingesetzten Software,
  - der Daten und der Datenverarbeitung,
  - der Zugriffsrechte,
  - der IT-Verbindungen mit der Außenwelt.

3 *Führen Sie regelmäßig eine Datensicherung durch?*

- Identifizieren Sie die Daten, die gesichert werden müssen.
- Legen Sie fest, wie häufig Datensicherungen durchgeführt werden sollen.
- Wählen Sie ein geeignetes Speichermedium, mit dem die Daten gesichert werden sollen.
- Prüfen Sie, welche Daten verschlüsselt werden sollen.

4 *Spielen Sie regelmäßig Updates ein?*

- Verwenden Sie aktuelle Hard- und Softwarelösungen.
- Sicherheitsupdates kosten kein Geld! Die Aktualisierung zu unterlassen, reicht häufig schon, weil zu spät oder nicht installierte Updates einer der häufigsten Gründe für erfolgreiche Cyber-Angriffe sind.
- Aktivieren Sie daher automatische Updates.
- Legen Sie fest, wer für den Update-Prozess zuständig ist.

5 *Haben Sie Makros deaktiviert?*

- Eines der Haupteinfalltore für Ransomware sind Makros, die sich in mit E-Mails verschickten Dateianhängen verbergen.
- Wenn man eine Datei öffnet, die einen Makro enthält, fragt das öffnende Programm den Nutzer dafür in der Regel um Erlaubnis.
- Das Problem ist, dass die meisten Nutzer nicht beurteilen können, ob die Datei, die sie da gerade öffnen, legitim ist oder nicht. Cyber-Kriminelle versenden ihre Schadsoftware oftmals über die E-Mail-Adressen von Absendern, die die Empfänger kennen und denen sie vertrauen. Oftmals bezieht sich der Betreff einer Schadcode-E-Mail sogar auf eine bereits bestehende Mailkonversation (was in der Regel heißt, dass der vermeintliche Absender bereits selbst Opfer der Schadsoftware geworden ist).

6 *Verwenden Sie Virenschutzprogramme?*

- Ein Virenschutzprogramm muss auf allen Systemen installiert werden, vorrangig auf denen, die mit dem Internet verbunden sind (Arbeitsplatzrechner, Dateiserver usw.). Ein Virenschutzprogramm schützt vor bekannten Bedrohungen, die sich sehr schnell weiterentwickeln: Jeden Tag erscheinen Hunderttausende neue Schadcodevarianten (116.6 Millionen Schadprogramm-Varianten in 2022!).

7 *Verwenden Sie sichere Passwörter?*

- Grundsätzlich gilt: Je länger, desto besser. Ein gutes Passwort sollte **mindestens** acht Zeichen lang sein. Idealerweise enthält es auch Sonderzeichen und Ziffern.

8 *Haben Sie eine Firewall eingerichtet?*

- Schützt hauptsächlich vor Angriffen aus dem Internet; eine lokale Firewall ist eine Funktion, die auf den meisten Betriebssystemen verfügbar ist.
- Firewalls werden auch in Kombination mit Antivirus-Software-Pakten vertrieben.

9 *Wie sichern Sie Ihre Mailaccounts ab?*

- E-Mails sind der häufigste Infektionsvektor am Arbeitsplatzrechner (durch das Öffnen von Anhängen, die schädliche Codes enthalten, oder durch das Klicken auf einen Link, der auf eine schädliche Website umleitet [Phishing]).

10 *Wie trennen Sie unterschiedliche IT-Bereiche?*

- Verwenden Sie für jeden Mitarbeiter ein eigenes Nutzerkonto und beschränken Sie die Administratorenrechte auch nur auf die Administratoren (dadurch Einschränkung der Einschleusung von Schadcodes). ▶

- Wenn Beschäftigte das Unternehmen verlassen, müssen ihre Zugriffsrechte widerrufen werden, sodass weder sie selbst noch Dritte diese Zugriffsrechte erneut nutzen können.
- Gleiches gilt für mobile Endgeräte (Apps dürfen nur ausschließlich von offiziellen Plattformen oder von der Website der tatsächlichen Hersteller heruntergeladen werden).

11 *Haben Sie IT-Risiken im Homeoffice oder wenn Sie unterwegs sind im Griff?*

- Statten Sie Ihre Geräte mit Blickschutzfiltern aus.
- Sichern Sie Ihre Daten, damit Sie diese im Fall von Verlust oder Diebstahl der Geräte wiederherstellen können.
- Sorgen Sie dafür, dass Ihre Passwörter nicht gespeichert und automatisch angeboten werden.
- Nutzen Sie Multi-Faktor-Authentisierung.
- Verschlüsseln Sie nach Möglichkeit Ihre sensiblen Daten oder die gesamte Festplatte.
- Verwenden Sie niemals USB-Sticks, die Ihnen auf Messen, Meetings usw. geschenkt werden (oder die Sie gefunden haben).
- Verweigern Sie den Anschluss von Geräten Dritter an Ihre eigenen Geräte (Laptop, USB-Stick, USB-Ladekabel usw.).

12 *Wie informieren Sie sich und Ihre Beschäftigten?*

- Informieren Sie sich beim BSI über präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen.
- Das BSI z. B. hat vor einiger Zeit die „Allianz für Cyber-Sicherheit (ACS)“ initiiert, der Unternehmen kostenfrei beitreten können. Zusammen mit vielen Institutionen verfolgen sie gemeinsam das Ziel, die Cyber-Sicherheit in Deutschland zu gestalten und zu stärken (7.041 Teilnehmer, Stand 15.06.2023).

13 *Deckt Ihre Versicherungspolice auch Cyber-Risiken ab?*

- Sicherstellung der Abdeckung der für den Fortbestand des Unternehmens bedeutendsten Risiken

14 *Wissen Sie, wie Sie bei einem Cyber-Angriff reagieren müssen?*

- Bei einem Vorfall in einem Informationssystem sollten Sie als Erstes Ihre Geräte oder das Informationssystem Ihres Unternehmens vom Internet trennen (Netzwerkstecker vom Router ziehen oder WLAN-Dienste deaktivieren).
- Schalten Sie die vom Angriff betroffenen Computer und Geräte nicht aus und verändern Sie sie nicht, um die Arbeit der IT-Forensiker/Ermittler nicht zu behindern.
- Rechtliche Aspekte: Unternehmen, die personenbezogene Daten verarbeiten und der Datenschutz-Grundverordnung unterliegen, müssen die Anforderungen dieser Verordnung einhalten und bei einem Vorfall zudem die zuständigen Datenschutzbeauftragten und ihre Kunden informieren.

Zusammenfassend lässt sich festhalten:

Cyber-Attacken auf Unternehmen (auch und zukünftig sicherlich verstärkter in landwirtschaftlichen Unternehmungen) sind längst eine tägliche Bedrohung und können zu schweren Produktionsausfällen und Renommee- bzw. Reputationsschäden führen.

Cyber-Versicherungen können die finanziellen Risiken abdecken. Sie decken Schäden ab durch Internet-Kriminalität, übernehmen die Kosten für die Wiederherstellung der Systeme und gleichen Verluste nach Betriebsstillstand aus.


©Adobe Stock/Serhii

Technische Begriffe, die Sie im Zusammenhang mit Cyber kennen sollten:

©Adobe Stock/sodafish visuals

* AUTHENTIZITÄT

In der Informationssicherheit bezeichnet Authentizität die Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit. Die Überprüfung einer behaupteten Eigenschaft wird als Authentifikation bezeichnet. Durch Authentifikation des Datenursprungs wird nachgewiesen, dass Daten einem angegebenen Sender zugeordnet werden können, was durch digitale Signaturen ermöglicht werden kann.

* BACKDOOR / HINTERTÜR

Hintertüren sind Schadprogramme, die dazu dienen, einen unbefugten Zugang zu einem IT-System offen zu halten, der einen unbemerkten Einbruch in das System ermöglicht und dabei möglichst weitgehende Zugriffsrechte besitzt, beispielsweise um Angriffsspuren zu verstecken.

* BOT-NET / BOT-NETZ

Bei einem Bot handelt es sich um ein Programm, das von einem Angreifer auf dem Rechner eines Anwenders ohne dessen Wissen installiert wird, z. B. über entsprechende Schadsoftware, und das aus der Ferne Anweisungen des Angreifers ausführen kann.

Werden viele Bots zusammengeschlossen, entsteht ein Bot-Netz. Bot-Netze werden für viele illegale Aktivitäten eingesetzt. Der massenhafte Versand von Spam-Mails oder E-Mails mit bösartigen Anhängen und Links (z. B. für Phishing), aber auch die Aufzeichnung von Tastaturanschlägen (Keylogging) und damit einhergehend die Entwendung bzw. der Diebstahl persönlicher Informationen (Passwörter, PIN etc.) oder vertraulicher Geschäftsinformationen (Wirtschaftsspionage) sind Einsatzgebiete von Bot-Netzen.

Darüber hinaus können mit Bots infizierte Rechner missbraucht werden, ▶

FORTSETZUNG **CYBER-LEXIKON**

um dort illegale Software abzulegen oder diese sogar über die infizierten Rechner anzubieten, z. B. per File-Sharing. Eine besonders für Netze und Dienste sehr ernst zu nehmende Angriffsform sind sogenannte DDoS-Angriffe (Distributed Denial of Service). DDoS-Angriffe werden aus politischen, ideologischen, vorwiegend aber aus finanziellen Gründen heraus unternommen.

* DENIAL-OF-SERVICE-ATTACKE/DOS-ATTACKE

Denial of Service – oder kurz DoS – bedeutet so viel wie etwas unzugänglich machen oder „außer Betrieb" setzen.

Bei DoS-Attacken wird ein Server gezielt mit so vielen Anfragen bombardiert, dass das System die Aufgaben nicht mehr bewältigen kann und im schlimmsten Fall zusammenbricht.

Auf diese Art wurden schon bekannte Web-Server, wie z. B. Amazon, Yahoo, eBay, mit bis zur vierfachen Menge des normalen Datenverkehrs massiv attackiert und für eine bestimmte Zeit für normale Anfragen außer Gefecht gesetzt.

* KEYLOGGER

Als Keylogger wird Hard- oder Software zum Mitschneiden von Tastatureingaben bezeichnet. Sie zeichnen alle Tastatureingaben auf, um sie möglichst unbemerkt an einen Angreifer zu übermitteln. Dieser kann dann aus diesen Informationen für ihn wichtige Daten, wie z. B. Anmeldeinformationen oder Kreditkartennummern filtern.

* MAN-IN-THE-MIDDLE-ATTACKE

Ziel bei einem Man-in-the-Middle-Angriff ist es, sich unbemerkt in eine Kommunikation zwischen zwei oder mehr Partnern einzuschleichen, beispielsweise um Informationen mitzulesen oder zu manipulieren. Hierbei begibt sich der Angreifer „in die Mitte" der Kommunikation, indem er sich gegenüber dem Sender als Empfänger und dem Empfänger gegenüber als Sender ausgibt. Als Erstes leitet der Angreifer eine Verbindungsanfrage des Senders zu sich um. Im nächsten Schritt baut der Angreifer eine Verbindung zu dem eigentlichen Empfänger der Nachricht auf. Wenn ihm das gelingt, kann der Angreifer unter Umständen alle Informationen, die der Sender an den vermeintlichen Empfänger sendet, einsehen oder manipulieren, bevor er sie an den richtigen Empfänger weiterleitet. Auf die Antworten des Empfängers kann der Angreifer wiederum ebenfalls zugreifen, wenn nicht entsprechende Schutzmechanismen wirksam sind.

* PHARMING

Beim Pharming werden Manipulationen an der Namensauflösung von Internet-Domainnamen vorgenommen, um Client-Zugriffe auf gefälschte Server umzuleiten. Ein Angreifer kann damit beispielsweise erreichen, dass im Browser des Opfers eine gefälschte Webseite statt der eigentlich gewünschten Seite angezeigt wird. Pharming hat sich aus Phishing weiterentwickelt. Der Begriff „Pharming" leitet sich aus „Phishing" und „Farming" ab.

* PHISHING

Phishing ist ein Kunstwort aus „Passwort" und „Fishing" und bezeichnet Angriffe, bei denen Benutzern gezielt Passwörter, Kreditkartendaten oder andere vertrauliche Informationen entlockt werden. Hierzu werden häufig Methoden des Social Engineering, teilweise in Verbindung mit Identitätsdiebstahl, verwendet. Beispielsweise können die Angreifer geschickt formulierte E-Mails an die Benutzer senden. Wenn das Opfer meint, den Absender zu kennen und diesen als vertrauenswürdig einstuft, wird es meist auch die E-Mail als vertrauenswürdig einstufen und darin beschriebene Schritte durchführen, z. B. einen beigefügten Link oder Anhang öffnen. Andere Formen des Phishing verwenden spezialisierte Schadprogramme, die direkt an die Benutzer gesendet werden oder über Umwege auf den Computern der Opfer platziert werden.

* SCHWACHSTELLE

Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.

* SOCIAL ENGINEERING

Social Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch „Aushorchen" zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie