

# Nur das Nötigste auf Stall-PC

*Hacker verschlüsselten Daten eines Melkroboters und forderten Lösegeld. Ein Angriff, der bisher noch als Einzelfall gilt.*

**RAPHAEL BÜHLMANN  
ADRIAN HALDIMANN**

Die Vorstellung ist in jedem Fall beängstigend. Das Melksystem, das Herz eines jeden Milchviehbetriebs, funktioniert nicht mehr. Was früher im schlimmsten Fall zu Melkverzögerungen führte, kann heute grösseren Schaden anrichten. Mit dem automatischen Melksystem verknüpft sind meist sämtliche Betriebsdaten. Abkalbungen, Besamungen oder Brunst werden digital erfasst. Sind die Daten weg, bedeutet das für den Betrieb ein ernsthaftes Problem.

So geschehen bei Milchbauer Vital Bircher aus Hagendorn ZG. Im letzten Jahr funktionierte plötzlich die Verbindung zwischen Melkroboter und Computer nicht mehr. Der Grund: Kriminelle hatten sich Zugang zum System verschafft, die Daten verschlüsselt und forderten 10 000 Franken für die Freigabe. «Der Roboter hat zwar noch funktioniert, er hat die Responder der Kühe erkannt, einfach auf sämtliche Daten hatte ich keinen Zugriff mehr», so Bircher.

Bei den grossen Herstellern von Melksystemen spricht man im Fall Bircher von einem Ein-



**Der Huobhof der Familie Bircher aus Hagendorn ZG wurde Opfer eines Cyberangriffs. (Bild: zvg)**

zelfall. Wichtig sei, dass man sich des Problems bewusster werde. Marcel Schwager, Leiter Verkauf bei Lely Schweiz, weist darauf hin, dass grundsätzlich jeder Computer Ziel eines Hackerangriffes werden könne. Unbekannte E-Mails seien schnell geöffnet, und eine schädliche Software könne sich von selbst installieren. «Wir empfehlen, dass auf dem Stallcomputer nur das Nötigste für den Stallalltag erledigt wird.» Und wichtig sei ein tägliches Offline-Back-up. Dafür sollten zwei Sticks verwendet werden. Wenn auf dem einen Stick die Daten von heute gesichert werden, dient

der zweite Stick für die Sicherung der Daten von morgen.

Dieser Fall dürfte viele Landwirte wachrütteln. Wichtig ist, dass Computer sowie Computerprogramme auf einem angemessenen Stand der Technik sind. Man muss sie vor unberechtigtem Eindringen Dritter schützen – etwa mittels Firewall und Antivirusprogramm. Seit zwei Jahren bietet die Emmental Versicherung auch eine Versicherungslösung für Landwirtschaftsbetriebe an. 101 Betriebe haben sich laut Andreas Stucki, Leiter Versicherung von eben dieser Genossenschaft, für diese Versicherung entschieden

– bisher schadenfrei. Die Prämie beträgt 100 Fr./Jahr, und es gilt eine Maximalentschädigung pro Schadenfall von 20 000 Fr. Versichert sind unter anderem Kosten zur Virenbereinigung auch auf betriebseigenen Produktionsanlagen und Maschinensteuerungen wie etwa Melkroboter usw. Stucki rät bei einem Cyberangriff den Support des Unternehmens in Anspruch zu nehmen, das die Anlage auf dem Betrieb installiert hat, und dann den Schaden der Versicherung zu melden. Und: «In jedem Fall bei einem Erpressungsversuch eine Polizeimeldung machen.»



# Back-up ist entscheidend

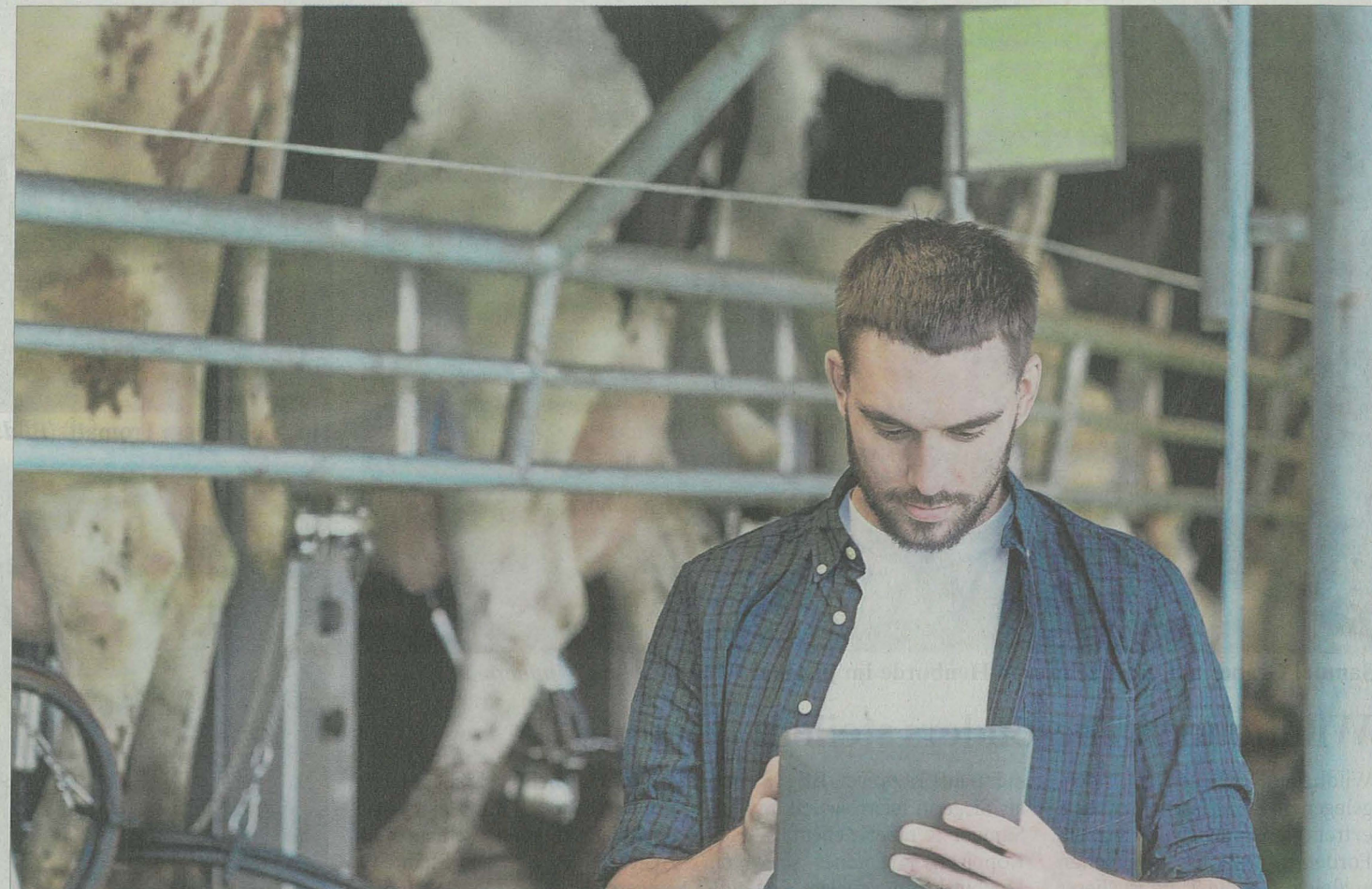
Die Landwirtschaft muss sich vor Hackerangriffen schützen. Im Kanton Zug haben sich Kriminelle Zugang zum Stall-PC mit Verbindung zum Melkroboter verschafft und Daten verschlüsselt, um Geld zu erpressen.

RAPHAEL BÜHLMANN

«Im ersten Moment war ich einfach ratlos und hatte ein mulmiges Gefühl.» Vital Bircher aus dem zugerischen Hagendorn erinnert sich an den Moment im vergangenen Jahr, als er eine SMS auf seinem Handy sieht. «Keine Verbindung zwischen Melkroboter und Computer.» Bircher denkt sich zunächst nicht viel dabei. «Der Roboter hat zwar noch funktioniert, er hat die Responder der Kühe erkannt und konnte weitermelken, einfach auf sämtliche Daten hatte ich keinen Zugriff mehr», so Bircher. Abklärungen beim Hersteller offenbarten dann das Problem. Vital Bircher wurde Opfer eines Hackerangriffes. Kriminelle hatten sich Zugang zum System verschafft, die Daten verschlüsselt und forderten schliesslich 10 000 Franken für die Freigabe der Daten, die Bircher nicht bezahlen wollte. So fehlten ihm aber unter anderem die Besamungsdaten, was am Ende zu 2000 Franken Tierarztkosten und einer toten Kuh führte.

## Daten täglich sichern

Nehmen Hackerangriffe in der Landwirtschaft zu? Die «Luzerner Zeitung», die den Zuger Fall publik machte, schreibt von einem Einzelfall. Thomas Haas, Berater am Berufsbildungszentrum Natur und Ernährung des Kantons Luzern, erklärt gegenüber der Zeitung, dass die Digitalisierung und das Risikomanagement in den Beratungen ein Dauerthema seien. «Die Kurse für Digitalisierungsprozesse werden stark nachgefragt. Die Cybersicherheit ist eher neu hinzugekommen. Vielleicht braucht es genau solche Fälle wie jenen im Kanton Zug, um die Leute wachzurütteln», so Haas gegenüber der «Luzerner Zeitung». Er wisse zudem von Hackerattacken auf Betriebscomputer oder Verkaufsplattfor-



Die Datensicherung ist auf dem modernen Milchviehbetrieb unerlässlich. (Bild: fotalia)

men. Marcel Schwager, Leiter Verkauf bei Lely Schweiz, weist darauf hin, dass grundsätzlich jeder Computer Ziel eines Hackerangriffes werden könne. Wichtig sei zu wissen, dass ein Angriff auf den Computer grundsätzlich auf den Astronaut-Melkroboter keinen Einfluss hat. Dieser melke wie gewohnt weiter, auch ohne PC. Unbekannte E-Mails seien schnell geöffnet, und eine schädliche Software könne sich von selbst installieren. Wichtig sei deshalb, dass stets ein gutes Virenschutzprogramm und eine Firewall aktiv seien. «Wir empfehlen, dass auf dem Stallcomputer nur das Nötigste für den Stallalltag erledigt wird», so Schwager. Zudem sei es empfehlenswert, die Daten regelmässig, möglichst täglich, auf einen externen Offline-Speicher (USB-Stick) zu laden und an einem anderen Ort aufzubewahren. So kann bei einem Schaden am Computer in aller Regel mit dem Back-up vom Vortag weitergearbeitet werden. «Denn auch Wasser oder Feuer können Daten vernichten», so Schwager weiter.

Generell sind Cyberattacken im Bereich und im Umfeld der Melktechnik Einzelfälle.

## Updates sind wichtig

Matthias Heyer, Geschäftsführer von De Laval AG in Sursee LU, erklärt: «Wir sind von der Herstellerseite stets bedacht, die höchstmöglichen Sicherheitsstandards einzuhalten und laufend zu optimieren. Unter anderem durch tägliche und doppelte Datensicherung, geschützten Fernzugriff sowie eigenen Stallcomputer mit eigenem Netzwerk, Router und Firewall. Antivirus-Programme werden standardmässig auf dem PC vorinstalliert.» Unbestritten aber sei, dass es wichtig sei, dass jeder Landwirt, der einen Melkroboter im Stall habe, zum Thema Cybersicherheit sensibilisiert sei. De Laval empfiehlt daher regelmässige Updates der Betriebssysteme, regelmässigen Austausch mit Servicetechnikern und Händlern und sofortige Reaktion, falls auf dem PC eine auffällige Veränderung erkannt werde.

## CYBER-ANGRIFF VERSICHERN

Erst seit zwei Jahren hat die Emmental Versicherung auch für Landwirtschaftsbetriebe ein Versicherungsprodukt im Angebot, das Schäden bei einem Cyber-Angriff deckt. «Wir bieten eine kleine, auf Bauernbetriebe zugeschnittene Lösung an, die nicht so umfassend ist wie diejenige anderer Versicherungsgesellschaften», erklärt Andreas Stucki, Leiter Versicherung bei der Emmental Versicherung. Die Prämie für die sogenannte VirusPlus-Versicherung beträgt 100 Franken pro Jahr, und es gilt ein Selbstbehalt von 200 Franken sowie eine Maximalentschädigung pro Schadenfall von 20 000 Franken. Versichert sind Kosten zur Virenbereinigung auch auf betriebseigenen Produktionsanlagen und Maschinensteuerungen wie etwa Melkroboter usw. Weiter werden Kosten für die Wiederherstellung von Daten übernommen. Auch Schäden bei

einer Betriebsunterbrechung können mit der Versicherung abgedeckt werden. Nicht gedeckt sind etwa Erpressungsgeldzahlungen. 101 Betriebe haben sich laut Stucki für diese Versicherung entschieden – bisher schadenfrei. Stucki rät bei einem Cyberangriff zuerst den Support des Unternehmens in Anspruch zu nehmen, das die Anlage auf dem Betrieb installiert hat und dann den Schaden der Versicherung zu melden. Und: «In jedem Fall bei einem Erpressungsversuch eine Polizeimeldung machen.» Stucki weist weiter auf die Sorgfaltspflicht hin: «Der Versicherungsnehmer verpflichtet sich, Computer sowie Computerprogramme auf einem angemessenen Stand der Technik zu halten und vor unberechtigtem Eindringen Dritter zu schützen.» Daten seien regelmässig zu sichern und vom Quellsystem zu trennen. hal