Datenschutz und Datensicherheit in Betrieben der Milcherzeugung

Ralf Köstler [1], Joachim Spilke[2]

[1]Landeskontrollverband für Leistungs- und Qualitätsprüfung Sachsen-Anhalt e.V
Angerstrasse 6
D-06118 Halle/Saale
[2]Arbeitsgruppe Biometrie und Agrarinformatik
Martin-Luther Universität Halle
Ludwig-Wucherer-Str.82-85
D-06108 Halle/Saale
koestler@lkv-st.de
spilke@landw.uni-halle.de

Abstract: IT security increases in importance. That applies to the milk production in particular. The contribution describes possible sources of danger at two case examples and suggests organizational solutions.

1 Problemstellung

Die technischen und organisatorischen Entwicklungen insbesondere in den letzten 10 Jahren haben zu einer starken Verbreitung von Personalcomputern und Nutzung von Weitverkehrsnetzen in landwirtschaftlichen Unternehmen geführt. Das hat für Milch erzeugende Betriebe eine besondere Bedeutung, da hier die Managementunterstützung und der dafür nötige überbetriebliche Datenaustausch bei Nutzung von Informationstechnik unverzichtbar sind. Mit dieser Entwicklung ist eine enorme Zunahme der Rolle von Datenschutz und Datensicherheit verbunden. Nachfolgend wird unter Datenschutz die Vermeidung der Verletzung von Vertraulichkeit und Sicherheit von Daten natürlicher oder juristischer Personen, unter Datensicherheit die Verhinderung von Verlust oder Verfälschung verstanden [SH02].

Im Beitrag werden mögliche Risikofaktoren für die Milcherzeuger systematisiert und bei Nutzung von zwei Fallbeispielen exemplarisch dargestellt. Basierend auf einer repräsentativen Befragung von Milch erzeugenden Betrieben in Sachsen-Anhalt wird die aktuelle Situation in der landwirtschaftlichen Praxis beschrieben. Darauf aufbauend werden Lösungsansätze zur Hebung des Sicherheitsniveaus aufgezeigt.

2 Bedeutung für Milch erzeugende Betriebe

Die Bedeutung von Datenschutz und Datensicherheit für die Milch erzeugenden Betriebe ergibt sich vor allem aus einem intensiven Datenaustausch, der aus der Unterstützung von Managemententscheidungen, zunehmend aber auch aus einem Einsatz in Qualitätssicherungssystemen resultiert. Speziell die Daten der Milchleistungsprüfung haben als Basis für die Zuchtwertschätzung, Fütterung und Qualitätssicherung einen hohen Schutzbedarf. Im Zuge der Herkunfts- und Identitätssicherung im Landwirtschaftsbetrieb erhobene Daten bilden ebenfalls eine wichtige Säulen innerhalb der Qualitätssicherung der landwirtschaftlichen Produkte und stellen die Grundlage für die Tierseuchenbekämpfung und Prämienberechnung von EU-Mitteln im Rahmen des „Integrierten Verwaltungs- und Kontrollsystem" (InVeKoS) dar. Für die daraus resultierende enge informationsseitige Vernetzung zwischen Landwirtschaftsbetrieb und Dienstleistern sowie Behörden [DS02] sind Weitverkehrsnetze unverzichtbar. Entsprechend steigt aber auch die Bedeutung von Datensicherheit und Datenschutz [Ga04].

3 Fallbeispiele und Gefahrenbewertung

Datensicherheit und Datenschutz erfordern die Bewertung des Gefahrenpotenzials und die Ableitung der durchzuführenden Maßnahmen. Hierbei ist zu differenzieren, ob die Gefahren aus dem eigenen Unternehmen (u.a. Mitarbeiter) oder von außen (Viren, Hacker usw.) wirken. Interessanterweise wird dem Bedrohungspotenzial für Datenschutz und Datensicherheit, das aus dem eigenen Unternehmen stammt weniger Beachtung geschenkt. Die Mehrheit der Sicherheitsprobleme gehen aber auf Fehler in der Anwendung, Organisation und die Unwissenheit der Mitarbeiter zurück [Ar04].
In der Bewertung des Gefahrenpotenzials von außen tragen die Bedrohungen durch Computerviren den Hauptteil [Ha02].

Fallbeispiel 1 – Virenübetragung über E-Mail

Der Virus W32/Netsky.X (WORM NETSKY.X) trat am 20.04.2004 das erste Mal auf. Die Viruswall des Landeskontrollverbandes prüft stündlich auf aktuelle Updates beim Hersteller. 13:01 Uhr eine E-Mail mit NETSKY.X passiert unerkannt die Viruswall. Der Virus wurde auf dem Clientrechner von der Antivirensoftware eines anderen Herstellers erkannt und eliminiert. 16:00 Uhr Update für Viruswall enthält erstmals Virensignaturen von Netsky.X. In der Zwischenzeit passierten keine weiteren E-Mails mit NETSKY.X das Gateway. Die nächste Mail mit einem NETSKY.X traf um 18:25 Uhr ein. Bis zum nächsten Morgen trafen weitere 7 NETSKY.X verseuchte Mails ein. Alarmierend ist die Geschwindigkeit der Verbreitung von Netsky.X. Legt man das Eintreffen der ersten Mail fiktiv als Erscheinungszeitpunkt zugrunde, verblieben 3 Stunden bis zur Immunisierung des Systems. Interessant sind weiterhin die Wirksamkeit der verschiedenen Scannerengines durch die Nutzung unterschiedlicher Verfahren zur Erkennung auf der Viruswall und dem PC. Auf dem Client wurde der Virus generisch entdeckt, das heißt über Ähnlichkeiten ohne spezielles Muster. Offensichtlich ist das für Netsky.X ein wirksameres Erkennungsverfahren.

Legt man nur ein einschichtiges Sicherungskonzept zugrunde, so hätte für drei Stunden kein Schutz vorgelegen.

Fallbeispiel 2 – Systemzugriffe ohne eigene aktive Dienstnutzung

Noch wesentlich schneller wird die Sicherheit der IT auf die Probe gestellt, wenn die Verbindung mit dem Internet hergestellt wird. Um dies zu veranschaulichen, wurde ein PC wie er üblicherweise in landwirtschaftlichen Betrieben zu finden ist, mit Windows 98 vor die Firewall des Landeskontrollverbandes gestellt. Die Grundeinstellungen entsprachen einer Basisinstallation ohne nachträgliche Herstellerpatches. Für acht Stunden wurden die Zugriffe auf das System registriert, ohne dass das System selbst zum Internet hin aktiv wurde. Das Ergebnis ist alarmierend. Sofort nach der Verbindungsaufnahme waren Zugriffe auf den Port 80 (http) zu verzeichnen. Nur 30 Sekunden später erfolgte der Zugriff auf Port 139 (netbios). Insgesamt wurden 119 Zugriffe verzeichnet. Zwei externe IP-Adressen waren über den gesamten Zeitraum über den Netbios-Port verbunden, ein idealer Einstiegspunkt zur Manipulation des PC und der Daten. Verdeutlichen soll Fallbeispiel 2, dass nicht einmal die eigenen Aktivitäten sondern allein die Präsenz ausreichend ist, um das Interesse ungebetener „Gäste" zu wecken. Des weiteren zeigt es, dass das Problem der IT-Sicherheit weitaus komplexer ist und die Installation eines Virenscanners nicht ausreichend ist. Bezogen auf landwirtschaftliche Betriebe besteht die Aufgabe, die Betriebsfähigkeit der Informations- und Kommunikationstechnik durch geeignete Maßnahmen, wie Antivirussoftware und regelmäßige Betriebssystem-Updates, zum Schließen von systembedingten Sicherheitslücken zu erhalten. Die potenziellen „Infektionsstellen" für eine Virusverseuchung liegen bei den zahlreichen Schnittstellen im Datenverkehr und insbesondere dort, wo Daten über das Internet ausgetauscht werden (vgl. Abschnitt 2). Da die Milcherzeuger durchaus mit mehreren Partnern in Kommunikation stehen, potenziert sich die Gefährdung insbesondere unter Beachtung der oben genannten Verbreitungsgeschwindigkeiten. So sind der Datenschutz und die Datensicherheit durch Virenschutz durchaus kein Einzelinteresse, sondern eine partnerschaftliche Verantwortung. Hierzu gehört natürlich auch die Information der bekannten Kommunikationspartner bei der Feststellung von Virenverseuchungen. Für die konkrete Einordnung des Bedrohungspotenzials und die geeigneten Maßnahmen, speziell für das Einzelunternehmen, gibt das IT-Grundschutzhandbuch konkrete Hinweise [Bu04].

4 Ergebnisse einer Betriebsbefragung

Im Rahmen einer Befragung von Milcherzeugern im Bundesland Sachsen-Anhalt zur IT wurde unter anderem auf die Datensicherheit und den Datenschutz eingegangen. An dieser Fragebogenaktion beteiligten sich 300 Betriebe. Von diesen gaben 275 an, mindestens einen PC zu nutzen, 64 verfügen über ein Netzwerk. Diese 275 bilden die Basis für die folgenden Aussagen. Datensicherung führen 87 Prozent der befragten PC Nutzer durch. Die Hälfte von ihnen täglich. Der verbleibende Teil in größeren zeitlichen Abständen, maximal aber monatlich. Das Internet nutzen, zur Informationsbeschaffung und zum –austausch, 87 Prozent. Davon gaben 57 Prozent an, sowohl über einen Virenschutz zu verfügen als auch regelmäßig Datensicherung durchzuführen (täglich bis monatlich). Aber nur etwa die Hälfte der Befragten aktualisieren die vorhandenen Virenscanner.

5 Diskussion und Schlussfolgerungen

Unsere Ergebnisse bestätigen eine aktuelle Analyse des Antivirus-Software Herstellers Sophos. Die Firma befragte im Zeitraum von Januar bis April 2004 fast 4.000 kleine und mittlere Unternehmen (KMU) zu ihrem Einsatz von Antiviren-Software und ihren Erfahrungen im Umgang mit Spam und Viren. Die Umfrage ergab, dass zwar durchaus ein Bewusstsein für die Thematik vorhanden ist, aber die Investitionen oft ins Leere laufen. Danach haben 87 Prozent der Befragten Virenschutz-Maßnahmen ergriffen, aber nur 63 Prozent sichern die notwendigen Aktualisierungen [So04]. Man kann davon ausgehen, dass ein grundlegendes Gefahrenbewusstsein in den KMU, zu denen auch landwirtschaftliche Betriebe zählen, vorhanden ist. Auf Grund der kurzen Innovationszyklen der IT ist es jedoch für die Betriebe schwierig, den Überblick über neu entstehende und sich schnell verändernde Gefahrenpotenziale zu sichern. Hinzu kommt, das es in den Betrieben kaum Mitarbeiter gibt, die ausschließlich für IT-Probleme zuständig sind. Die steigende Funktionalität und Vernetzung der Systeme erhöht die Abhängigkeit der Betriebe, und bietet eine größere Angriffsfläche. Fallbeispiel 1 zeigt, dass erst mehrschichtige Sicherheitskonzepte einen ausreichenden Schutz bieten. Fallbeispiel 2 zeigt, dass Systeme auch gegen offene Ports geschützt werden müssen, um Anschlägen von Viren wie W32.BLASTER.WORM und WORM_SASSER zu verhindern. Der Schutz der Daten vor physischem Verlust erlangt besonderes Gewicht, wenn man sich vor Augen hält, dass Einzeltierdaten nach Verlust kaum widerbeschaffbar sind. Ohne diese Daten sind aber künftige sinnvolle Managemententscheidungen kaum denkbar. Dazu sind vielfältige Aufgaben (Betriebssystem-Updates, gestaffelte Sicherheitslösungen, Backup) erforderlich. Um den Landwirtschaftsbetrieben Unterstützung zu bieten, sind Information und Aufklärung zu den Risiken und entsprechende Maßnahmen sowie die Bereitstellung von Outsourcing-Lösungen zwingend. Hierbei geht es um die Erarbeitung von Sicherheitskonzeptionen, der Einbindung in regionale Sicherheitslösungen und in der verstärkten Nutzung von IT-Services zur Systempflege. Entscheidend für eine Akzeptanz bei den Landwirten sind neben der Entwicklung von Gefahrenbewusstsein die Praktikabilität und die Finanzierbarkeit solcher Lösungen.

Literaturverzeichnis

[Ar04] Armstrong, A.: IT-Mittelstand. 3/2004; S. 58. Medienhaus Verlag, Bergisch Gladbach.

[Bu04] Bundesamt für Sicherheit in der Informationstechnik – BSI, http://www.bsi.de, 05.05.2004.

[DS02] Doluschitz, R.; Spilke, J. (Hrsg): Agrarinformatik. 2002, S. 16; 324. UTB, Ulmer-Verlag, Stuttgart.

[Ga04] Gambichler, Th.: IT-Mittelstand. 3/2004; S. 66. Medienhaus Verlag, Bergisch Gladbach.

[Ha02] Hammerschmidt, C.: IT-Sicherheit2002.pdf. http://www.silicon.de, 14.07.2003.

[SH02] Stahlknecht, P.; Hasenkamp, U.: Einführung in die Wirtschaftsinformatik. 2002; S.481. Springer-Verlag, Berlin, Heidelberg, New York.

[So04] Sophos, http://www.sophos.de/20040503kmu.html, 03.05.2004.