TITELTHEMA
Cyber-sicherheit

Interview

Gegen Cyberkriminalität absichern

Im Gespräch mit Thomas Brink, geschäftsführender Gesellschafter der Versicherungsagentur Diepenbrock in Lingen (Emsland/Niedersachen), und Tim Zevenhuizen, zertifizierter Fachberater für Cyber-Risiken, über die Möglichkeit, sich gegen Cyber-Angriffe abzusichern.

Interviewer: Dipl.-Ing. agr. (FH) Martin Bensmann

Thomas Brink (links) und Tim Zevenhuizen raten Biogasanlagenbetreibern eine Cyberrisikoversicherung abzuschließen.

BIOGAS Journal: Herr Brink, wie ist Diepenbrock im Bereich Versicherungen aufgestellt?
Thomas Brink: Diepenbrock ist ein freier Versicherungsmakler. Das Unternehmen ist seit 1968 in Lingen ansässig. Wir vertreten keine Versicherung und sind somit nur unseren Kundinnen und Kunden verpflichtet. Wir wählen für unsere Kunden nach deren individuellen Anforderungen und Bedürfnissen unter zahlreichen Versicherern denjenigen aus, der am besten zu dem abzusichernden Risiko des Betriebes passt.
Wir nutzen den Wettbewerb der Versicherer, um für die Kunden die strategisch und preislich jeweils beste Leistung zu erzielen. Wir haben uns spezialisiert auf Gewerbe- und Industriekunden im Bauhaupt und -nebengewerbe sowie im Bereich der produzierenden Betriebe und der Logistik. Mit einer eigenen Sparte bieten wir insbesondere Lösungen für den Agrarsektor. Darüber hinaus haben wir Angebote für Freiberufler oder auch Spezialkonzepte für Autohäuser.

BIOGAS Journal: Sie sagen, dass Diepenbrock eine grüne Seite hat. Was heißt das?
Brink: Das bedeutet, dass wir im Bereich Landwirtschaft Unternehmen im vor- und nachgelagerten Bereich versichern. Wir vermitteln Versicherungskonzepte speziell für landwirtschaftliche Betriebe und Biogasanlagen. Von den insgesamt 62 Beschäftigten in unserem Hause sind in der Agrarsparte allein zehn Personen angestellt. Das sind Spezialberater. Zum Beispiel Agraringenieure mit einer Zusatzausbildung zum Versicherungskaufmann.

BIOGAS Journal: Wie viele Biogasanlagen haben Sie in Ihrem Kundenstamm?
Brink: Rund 150 Biogasanlagenbetreiber haben bei uns eine Feuerversicherung. 110 davon haben eine Maschinenschaden-Versicherung. Bislang haben erst 50 Biogasanlagenbetreiber eine sogenannte Cyberrisikoversicherung abgeschlossen. Die Zahl ist viel zu niedrig. Wir empfehlen jedem Anlagenbetreiber, eine Versicherung abzuschließen, die die Kosten eines Cyberangriffs deckt. Zu einer resilienten Energieerzeugungsstruktur gehört auch der Schutz vor Cyberangriffen.

BIOGAS Journal: Wie oft haben Sie in der Agentur mit einer Cyberattacke bei Ihren Kunden zu tun?
Zevenhuizen: Bezogen auf den gesamten Kundenstamm haben wir pro Woche mindestens einen Verdachtsmoment. Wenn Kunden keine eigene interne IT-Abteilung haben, die mit entsprechenden Erstmaßnahmen im Zuge der Vorfallsanalyse gegen einen Cyberangriff vorgeht, melden sie sich bei uns. Wir beauftragen dann bei Bedarf IT-Spezialisten, die sich des Problems annehmen.
Positiv fällt uns auf, dass Biogasanlagenbetreiber das Thema Cyberkriminalität stärker in den Fokus rücken. Sie informieren und warnen sich untereinander. Dennoch müssen sie sich viel stärker bewusst sein darüber, dass sie sich schützen müssen. Ich möchte an dieser Stelle betonen, dass ein Cybervorfall keinen Fall von Schwäche des Betroffenen darstellt. Dies zu verheimlichen, sollte keine Lösung sein. Bekannte Vorfälle der Vergangenheit zeigen, dass auch namhafte Betriebe trotz vorhandener IT-Sicherheitsvorkehrungen einen Vorfall erleiden mussten.

BIOGAS Journal: Welche Fehler können Anlagenbetreiber vermeiden?
Zevenhuizen: Der größte ist grundsätzlich, sich nicht mit dem Thema Cyber-Sicherheit zu beschäftigen. Die Eintrittswahrscheinlich kann in der täglichen Praxis reduziert werden, wenn man grundsätzlich bei der E-Mailkorrespondenz aufmerksam ist. Auf keinen Fall Anhänge einer E-Mail unbekannter Herkunft öffnen.
Konkret heißt dies, nicht auf eingefügte Links klicken oder Dateien herunterladen, auch wenn man dazu aufgefordert wird. Es könnte sich Schadsoftware dahinter verbergen, die sich beim Klicken unbemerkt ausführt. Passwortlisten sollten nicht in einer Datei auf einer Festplatte oder einem externen Speichermedium, das an den PC dauerhaft angeschlossen ist, abgespeichert sein. Über den ungewollten Zugriff von außen auf Passwörter kann großer Schaden angerichtet werden.
Betriebssysteme und Software sollten regelmäßig mit dem vom Hersteller bereitgestellten Update versorgt werden. Das Gleiche gilt für Firewalls etc. Wer verreist und aus dem Urlaub Bilder postet, der sollte im Vorfeld in seinem Unternehmen

Foto: Martin Bensmann | Illustration: AdobeStock / Visual Generation

oder einer Unternehmensabteilung seine Kolleginnen und Kollegen bezüglich potenzieller Cyberattacken sensibilisieren. Aufgrund täuschend echter E-Mails mit manipulierten Bankverbindungen in Rechnungen, die bezahlt werden, kann sehr großer Schaden entstehen.

BIOGAS Journal: Was kostet eine Cyberrisikoversicherung im Jahr?
Zevenhuizen: Zum Start einer Marktausschreibung fragen wir den Netto-Jahresumsatz einer Biogasanlage ab, anhand dessen die Risikoträger grundsätzlich das potenzielle Schadenrisiko abschätzen können. Dann schauen wir uns den IT-Bereich genau an. Wir prüfen, ob Hard- und Software auf dem aktuellen Stand sind und ob bereits ein gewisser Schutzstatus besteht. Gegebenenfalls muss der Anlagenbetreiber nachbessern.
Die durchschnittliche Deckungssumme beträgt eine Million Euro. Dafür muss der Anlagenbetreiber pro Jahr etwa 1.000 Euro bezahlen. Die Deckungssumme darf aus der Erfahrung ruhig höher sein, da eine Cyber-Versicherung mehrere Leistungsbausteine beinhaltet, die im Schadenfall entstehende Kosten, wie zum Beispiel IT-Forensik, IT-Wiederherstellung oder Schadensersatzansprüche Dritter abdecken.
Brink: Als freies Versicherungsbüro arbeiten wir individuelle Verträge aus, die zu dem Kunden passen. Wir suchen immer Wege, einen Kunden versicherbar zu machen. Nicht nur Betreiber von Einzelanlagen sollten einen Versicherungsschutz haben. Bei der Einspeisung von Biomethan haben wir es immer häufiger mit sogenannten Clusterprojekten zu tun. Hier steigt das Risiko eines Ausfalls aufgrund einer Cyberattacke. Dann hat plötzlich die Gemeinschaft das Problem, wenn eine oder mehrere Anlagen stillstehen.

BIOGAS Journal: Wenn ich als Anlagenbetreiber betroffen bin, was ist dann formalrechtlich zu tun?
Zevenhuizen: Sobald auch nur der Anfangsverdacht besteht, dass Angreifer unerlaubten Zugriff auf gespeicherte Daten und demnach Zugriff auf das IT-Systems einer Biogasanlage hatten, ist innerhalb von 72 Stunden nach dem Erkennen eine DSGVO-konforme Meldung bei der Landesdatenschutzbehörde abzugeben. Die Meldung muss ein Datenschutzbeauftragter machen.
Es empfiehlt sich, das zuständige Landeskriminalamt einzubinden, wenn es zum Beispiel um Lösegeld geht, das für eine Freischaltung vonseiten der Hacker erpresst werden soll. Es muss seine Zustimmung geben, wenn Lösegeld gezahlt wird, wenn nichts anderes mehr möglich ist, um zum Beispiel eine Insolvenz abzuwenden.
Grund dafür ist: Es kann sogar so weit gehen, dass eine Hackergruppe im Ausland Lösegeld bekommt, die als terroristische Vereinigung eingestuft ist. Das wäre dann sozusagen die Finanzierung einer Terrorgruppe. Das kann zu Problemen beim Einreisen in bestimmte Länder (zum Beispiel die USA) führen.
Brink: Wir bieten unseren Kunden aber auch Schulungen an als präventive Schutzmaßnahme. Wir machen sogenannte innere und äußere Scans der Kundensysteme oder sensibilisieren die Mitarbeitenden. Mit entsprechenden präventiven Maßnahmen können Kunden zum Beispiel die Höhe ihrer Selbstbeteiligung um einige Prozentpunkte reduzieren. Mit unseren Versicherungs-Policen kaufen sich unsere Kunden den Krisenstab mit ein. Dazu gehören dann Juristen, die Polizei, IT-Experten, Forensiker, Kommunikationsexperten oder auch Verhandler, wenn es um Lösegeld geht.

BIOGAS Journal: Aktuell gibt es immer mehr sogenannte Smarte Systeme. Das sind zum Beispiel vernetzte Rauchmelder in Räumen oder Kameras außen an Gebäuden. Wie anfällig sind solche System für Hackerangriffe?
Brink: Besonders problematisch sind Kameras außen an Gebäuden. Wenn die zu billig gekauft wurden, dann haben die in der Regel einen schlechten Schutz. Passwörter können dann leicht abgegriffen werden, sofern sie ab den Werkseinstellungen jemals geändert wurden. Über die Plattform Shodan kann jedermann überprüfen, welches Gerät von außen über das Netzwerk zugänglich ist. Über die Kameras lässt sich zum Beispiel von außen feststellen, wann Gebäude und Grundstücke von Personen frequentiert werden und wann nicht. Zudem lassen sich gehackte Kameras abschalten. Der Einbruchschutz ist dann nicht mehr gegeben. In einer Zeit, in der die Digitalisierung in allen Lebensbereichen angekommen ist, heißt es: aufmerksam und skeptisch sein.

BIOGAS Journal: Herr Brink, Herr Zevenhuizen, vielen Dank für das Gespräch! ●

INTERVIEWER
Dipl.-Ing. agr. (FH) Martin Bensmann
Redakteur Biogas Journal
Fachverband Biogas e.V.
0 54 09/90 69 426
martin.bensmann@biogas.org
www.biogas.org