INTERVIEW

Neues Risiko: Die Sicherheit im Netz

Versicherungen kosten je nach Deckungsumfang zwischen 2.500 und 7.500 Euro im Jahr. Von Fachredakteurin **Katrin Klawitter**

Michael Dutz, Versicherungsmakler Dr. Hörtkorn München GmbH (Gräfelfing). Foto: privat

Mit der provokanten Frage „Ist der Gartenbau mittlerweile zu risikoreich?“ beschäftigt sich unser brandaktuelles, dieser TASPO-Ausgabe beiliegendes TASPO dossier. Ein Thema, das die Branche in Zukunft immer mehr beschäftigen wird – und für viele Betriebe (noch) ein Buch mit sieben Siegeln ist, ist die „Cybersicherheit im Gartenbau“.

„Cyberkriminalität ist eine wachsende Bedrohung mit oft existenzbedrohenden Folgen“, betonte Experte Michael Dutz von der Dr. Hörtkorn München GmbH (Gräfelfing) schon im Rahmen der diesjährigen öffentlichen Mitgliederversammlung des Zentralverbandes Gartenbau (ZVG) Ende September in Berlin. Und ZVG-Präsident Jürgen Mertz unterstrich dazu, wie erschreckend schnell ein komplettes Unternehmen im Falle eines Hackerangriffs geschäftsunfähig sei. „Umso wichtiger ist es aus Unternehmersicht, für den Ernstfall vorgesorgt und ein gut geschultes Team zu haben“, so Mertz.

Wie groß aber ist denn die Gefahr für den Gartenbau wirklich – und was kann jeder einzelne dagegen tun? Die TASPO sprach dazu mit Michael Dutz. Der sagt: „In wenigen Jahren wird der Risikotransfer in Form einer Versicherungslösung ähnlich selbstverständlich sein, wie beispielsweise eine Betriebs- oder Feuerversicherung“.

TASPO: Wo liegen die besonderen Gefahren speziell in gartenbaulichen Betrieben?
Michael Dutz: Gartenbauliche Betriebe sind nicht mehr oder weniger gefährdet wie andere Unternehmen. Neben personenbezogenen Daten können Angriffe „Produktionsprozesse“ – Bewässerung, Klimatisierung und anderes – negativ beeinflussen und so Ausfälle bis hin zu Betriebsstillständen verursachen.

TASPO: In Ihrem Vortrag hieß es, Cyberkriminalität sei die Bedrohung der Zukunft mit oft existenzbedrohenden Folgen. Könnten Sie einmal an ein oder zwei Beispielen darlegen, in wie weit speziell ein Gartenbaubetrieb hier in seiner Existenz bedroht sein kann? Wo liegen hier typische Lücken, und was sind die Ursachen dafür?
Michael Dutz: Auch ein Gartenbaubetrieb dürfte heutzutage ohne IT kaum noch handlungsfähig sein. Wie bereits erwähnt, sind Betriebsunterbrechungen vermutlich eine der essenziellen Bedrohungen. Hinzu kommen nicht zu unterschätzende reputationsbedingte Folgen sowie enorme Kosten unter anderem für IT-Forensik sowie die Benachrichtigung aller Kunden und Partner des Unternehmens. Alleine dieser Kostenblock erreicht ohne Weiteres schnell einen sechsstelligen Betrag.

TASPO: Was bedeutet in diesem Zusammenhang ein gutes Risikomanagement? Wie und was kann ein „normales“ mittelständisches Unternehmen hier leisten und dadurch absichern?
Michael Dutz: Vom Grunde her ist entscheidend, dass sich das jeweilige Unternehmen dem Risiko bewusst ist und sich diesem stellt. Die technischen Voraussetzungen für einen angemessenen Schutzgrad müssen vorhanden sein, heißt, am IT-Budget sollte zukünftig nicht gespart werden.

Zusätzlich sind externe Checks wie Penetrationstests und IT-Sicherheits-Audits in regelmäßigen Abständen sinnvoll. Organisatorische Maßnahmen sind oft ohne großen finanziellen Aufwand zu realisieren. Beispielsweise ein implementiertes Berechtigungsmanagementsystem oder ganz banal eine ordentliche Passwortrichtlinie erhöhen die Sicherheit immens. Einer der wesentlichen „Schwachstellen“ in der IT-Sicherheit ist der Mensch. Hier gilt es, das entsprechende Bewusstsein wie zum Beispiel durch regelmäßige Mitarbeiterschulungen oder Geheimhaltungsvereinbarungen zu schaffen. Ein funktionierendes Risk-Management liegt in der Verantwortung des Managements.

TASPO: Was raten Sie dem normalen Gartenbaubetrieb jetzt, akut als erstes zu tun, um sich abzusichern? Und was sollte er langfristig bedenken und in Angriff nehmen?
Michael Dutz: Wichtig ist für Gartenbaubetriebe, die eigene Sicherheit zu analysieren oder durch professionelle Dienstleister analysieren zu lassen und geeignete Maßnahmen zu treffen. Hierzu zählt selbstverständlich auch die Absicherung des Restrisikos über eine Versicherungslösung.

Die digitale Bedrohung wächst stetig. Wir gehen daher davon aus, dass eine Cyberversicherung ähnlich selbstverständlich zum Versicherungsportfolio zählen wird, wie eine Betriebshaftpflicht- oder Feuerversicherung.

Gegen Cyberangriffe versichern

Stichwort Cyberangriff: Sie sagten in Berlin, eine umfassende Versicherungslösung für Unternehmen jeder Branche werde künftig essenziell. Was ist speziell für den Gartenbau denn bereits versicherbar, wie und zu welchen Kosten? Und was wird sich hier in naher Zukunft tun?
Auch hier unterscheidet sich die Branche Gartenbau nicht wesentlich von anderen Geschäftsmodellen. Eine Cyberversicherung hat neben der Absicherung der wirtschaftlichen Risiken, dem Bilanzschutz, einen nicht zu unterschätzenden Mehrwert für die Kunden. Dieser Mehrwert stellt der Assistance-Baustein. Hier werden unsere Kunden im Schadenfall durch Spezialisten vom ersten Verdachtsfall bis hin zur Wiederherstellung der Systeme begleitet und unterstützt.

Die Kosten einer solchen Versicherungslösung variieren genau wie die Deckungsumfänge noch immer stark am deutschen Versicherungsmarkt, abhängig von der individuellen Risikosituation, der gewünschten Versicherungssumme sowie der Selbstbeteiligung. Die Preisspanne liegt für ein mittelständisches Unternehmen, beispielsweise mit 50 Millionen Euro Jahresumsatz, je nach gewünschtem Deckungsumfang zwischen 2.500 und 7.500 Euro. Die Cyberversicherung ist noch immer ein „junges Produkt“. Die Bedingungen werden sich stetig weiterentwickeln, ebenfalls auch die Preise. Mit zunehmenden Schadenfällen werden risikogerechte Anpassungen der Versicherungsprämien unumgänglich. *(kla)*

TASPO: In Berlin wurde auch die Zentrale Ansprechstelle Cybercrime (ZAC) vom LKA Berlin als kompetenter Ansprechpartner bei IT-Sicherheitsvorfällen genannt. In welchen Fällen kann und sollte sich ein Unternehmen zuerst dahin wenden und wie kann diese Anlaufstelle helfen?
Michael Dutz: Ein Cyberangriff führt schnell zu einer existenzbedrohenden Unternehmenskrise. Meldungen an Behörden wie die ZAC, die „Zentralen Ansprechstellen Cybercrime der Polizei der Länder und des Bundes für die Wirtschaft“, nicht zuletzt hinsichtlich der Strafverfolgung, sollten eine Selbstverständlichkeit sein.

Auch Cyberversicherungen bieten eine Krisenhotline an, hinter dieser Hotline verbergen sich hochprofessionelle IT-Forensiker die 24/7 zur Verfügung stehen. Eine Priorisierung der Meldefolge ergibt sich nicht. Behörden und eventuelle Krisenhotlines sollten umgehend und am besten parallel kontaktiert werden.

Datenverluste können für einen Gartenbaubetrieb immense Folgen bis zur Betriebsunterbrechung haben. Fotos: Fotolia/privat