Ist Cyber-Schutz in der Versicherung enthalten?

Kompetente Beratung hilft Unternehmen, Gefährdungen bei der Cloud-Nutzung zu minimieren

Die Nutzung einer Cloud als Speicherort von Unternehmensdaten liegt weiterhin im Trend. Doch wird ein erfolgreicher Hackerangriff auf die Cloud von der Versicherung überhaupt gedeckt? Und in welchen Ländern stehen die Rechenzentren? Fragen, die sich jeder Entscheider stellen sollte, wenn er den Verlust von Unternehmensdaten und einen teuren Betriebsschaden verhindern möchte. Um die Resilienz gegenüber Cyber-Risiken zu erhöhen, können neben den eigenen IT-Verantwortlichen auch externe Berater helfen.

Nigel Todd, FM Global

Made in Germany – weltweit besitzen deutsche Produkte und deutsches Know-how seit Jahrzehnten einen guten Ruf. Im Zeitalter von Digitalisierung und internationaler Vernetzung wird es jedoch immer komplizierter, das eigene Unternehmen vor Sabotage und Spionage durch Hacker zu schützen. Davon betroffen sind ebenfalls die Chemie- und Pharmaindustrie. Mehr als zwei Drittel dieser Branchenunternehmen hatten in den vergangenen Jahren ein Cyber-Security-Problem. Neben dem Bereich Produktion interessierten sich die Kriminellen besonders für die Abteilung Forschung & Entwicklung. Verständlich, denn mit Forschungsdaten lässt sich viel Geld verdienen.

> *Die Nutzung einer Cloud bietet Unternehmen Vorteile, aber auch eine weitere Angriffsfläche.*

Trotz dieser beunruhigenden Angabe scheint es jedoch weiterhin ein fehlendes Verständnis für Cyber-Risiken oder eine zu geringe Beachtung dieser Gefahren innerhalb der Unternehmen zu geben. Denn laut der aktuellen Studie des Ponemon Instituts und Citrix sagen 74 % der deutschen IT-Verantwortlichen, dass ihre Sicherheitsarchitektur dringend erneuert werden muss. 82 % sehen vor allem wertvolle Daten wie geistiges Eigentum in Gefahr.

Externe Sicherheitsrisiken beachten

Hinzu kommt, dass viele Unternehmen trotz bekannter Sicherheitsrisiken nicht auf die Nutzung moderner Tools verzichten möchten und dadurch die Gefahr eines Datendiebstahls unbewusst steigt. Wurden die Daten früher in den eigenen vier Wänden auf isolierten Systemen lokal verwaltet, geht nun der Trend weiterhin zur Cloud: online verfügbare Datenspeicherung, Rechenleistung oder Software, ohne lokale Speicherung. In der aktuellen Studie „Cloud Monitor 2017“ von Bitkom Research und KPMG heißt es, dass bereits zwei von drei Unternehmen in Deutschland (65 %) auf Cloud Computing setzen.

Für Firmen, die für ihre Arbeitsprozesse noch nicht auf Datensicherung in der Cloud setzen, bleiben die Sicherheitsbedenken weiterhin das größte Hemmnis: Rund 60 % befürchten den unberechtigten Zugriff auf sensible Daten. Die Sorge ist verständlich, kann der Verlust von Unternehmenswissen doch den Verlust der Marktposition bedeuten. Auf die Bedenken ihrer Kunden haben die ersten Anbieter reagiert – sie stellen mittlerweile Informationsplattformen bereit, auf denen Anwender sich über den aktuellen Sicherheitsstatus verschiedener Teile der Cloud informieren können.

Eine Nachfrage nach den Standorten der Rechenzentren ist ebenfalls ratsam. Denn nicht nur Datenschutzgesetze variieren von Land zu Land, sondern auch die Stärke der Bedrohung durch Naturkatastrophen. Immer öfter werden neue Rechenzentren in Asien errichtet, wie zum Beispiel in Japan. Hier werden pro Monat durchschnittlich 73 Beben gemessen, die einen Wert von 4 oder höher auf der Magnituden-Skala erreichen. Neben Japan sind auch Taiwan und Hongkong sehr beliebt – zwei Regionen, die regelmäßig von Taifunen, Überschwemmungen und Erdrutschen heimgesucht werden.

© FM Global/Shutterstock/fotogestoeber

Cyber-Risiken: Resilienz aufbauen

Bevor die Cloud-Nutzung jedoch in Erwägung gezogen wird, ist zu empfehlen, einen Blick in die eigene Versicherung zu werfen. Trotz der zunehmenden Bedrohung durch Cyber-Gefahren verfügen viele Unternehmen über keinen oder keinen ausreichenden Cyber-Schutz bezüglich der Sicherung ausgelagerter Daten. Eine Vorreiterrolle nimmt hierbei der Industriesachversicherer FM Global ein, der Daten klar als versicherte Sachen ansieht. Bei einem Cyber-Angriff auf die Cloud sind im Ernstfall Sach- und Ertragsausfallschäden gedeckt.

Ferner ist es ratsam, dass im Unternehmen ein Business-Continuity-Plan aufgestellt wird, um trotz des eingetroffenen Schadens die Sicherstellung des Fortbestands des Unternehmens zu gewährleisten. Bei der Prüfung von Cyber-Risiken sollten nicht nur die IT-Spezialisten des Unternehmens, sondern auch externe Fachexperten zu Rate gezogen werden. FM Global unterstützt seine Kunden seit über 15 Jahren beim Umgang mit möglichen Cyber-Bedrohungen und hat kürzlich zwei Engineering- und Underwriting-Einheiten gegründet, die das Ziel verfolgen, standort- und kundenspezifische Bewertungsstandards, Instrumente und Methodologien zur weiteren Risikominimierung im Bereich Cyber zu entwickeln.

Die Nutzung einer Cloud bietet Unternehmen Vorteile, aber auch eine weitere Angriffsfläche. Diese kann jedoch durch ein effizientes Risikomanagement minimiert werden. Um Sicherheitslücken zu identifizieren und maßgeschneiderte Lösungen zu finden, sollten Entscheider das kombinierte Fachwissen ihrer IT-Spezialisten und externer Berater nutzen. Denn eine lückenlose Prävention ist stets günstiger als ein Schaden. (mr)

Nigel Todd, Vice President, Client Service Manager, FM Global Deutschland, Frankfurt am Main

- nigel.todd@fmglobal.com
- www.fmglobal.de

Deutsche Cyber-Sicherheitsorganisation

Im August 2016 haben sechzehn deutsche Unternehmen den wachsenden Bedrohungen für die Cybersicherheit der Wirtschaft den Kampf angesagt. Anlässlich der konstituierenden Fachbeiratssitzung der Deutschen Cyber-Sicherheitsorganisation (DCSO) kamen CIOs führender deutscher Unternehmen sowie Vertreter von Bundesbehörden und Forschungsinstituten in Berlin zusammen. Ziel der Zusammenarbeit: Ein intensiver und vertrauensvoller Austausch zu allen Herausforderungen der Cyber-Sicherheit und mehr Schlagkraft in der Abwehr von Bedrohungen aus dem Netz.

Dem Fachbeirat der DCSO gehören u.a. Bayer, BASF, BMW, Daimler, E.ON, Kuka, Siemens, Thyssenkrupp und Volkswagen an. Außerdem sind das Bundesministerium des Innern, der Bundesverband der Deutschen Industrie, das Digital Society Institute der ESMT Berlin sowie das Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC) Mitglieder im Fachbeirat. Zum Vorsitzenden des Fachbeirats wurde Daniel Hartert von Bayer gewählt.

Die DCSO wurde bereits im November 2015 als Gemeinschaftsunternehmen von Allianz, BASF, Bayer und Volkswagen gegründet und hat die Aufgabe, die Spitzenunternehmen der deutschen Wirtschaft bei der Cyber-Sicherheit robuster zu machen. Dazu bietet die DCSO eigens entwickelte Dienstleistungen an, die von den IT-Sicherheitsteams der Kundenunternehmen in Anspruch genommen werden können.

Gemeinsam mehr Cyber-Sicherheit erreichen

„Cyber-Sicherheit ist eine Gemeinschaftsaufgabe. Denn die Bedrohungslage wird zunehmend komplexer und anspruchsvoller. Das kann die vernetzte Wirtschaft künftig gemeinsam viel effizienter und effektiver bewältigen“, ist Martin Wülfert überzeugt und erklärt: „Die DCSO bündelt Wissen, technische Analysen sowie Abwehrkompetenzen und stellt sie allen Kunden zur Verfügung.“

© Alex - Fotolia.com

Ein Team von IT-Sicherheitsexperten der DCSO unterstützt die Unternehmen mit eigens entwickelten Lösungen und Beratungsleistungen in den Bereichen Bedrohungserkennung und -abwehr (Threat Intelligence), Erkennung von sicherheitsrelevanten Ereignissen und ihre Behebung (Incident Detection & Response Services) sowie Governance, Risk & Compliance Management (GRC) an. Außerdem evaluiert die DCSO im Auftrag ihrer Kunden als herstellerunabhängiger Dienstleister am Markt verfügbare Sicherheitslösungen und -technologien.

Die DCSO verfolgt das Prinzip „Optimieren durch Teilen“. Das bedeutet, dass operative Erkenntnisse über Cyber-Gefahren und ihre Bekämpfung von den Kunden an die DCSO zurückgespielt und von ihr in anonymisierter Form automatisch an alle Kunden verteilt werden. So entsteht eine selbstverstärkende Rückkopplung, die für alle Unternehmen zu mehr Sicherheit führt.

„Bayer ist Mitinitiator der DCSO, weil eine höhere Cyber-Sicherheit neue Wege erfordert und im Interesse aller Unternehmen ist“, erläutert Daniel Hartert. „Die Mitglieder des Fachbeirats kennen die vielfältigen Herausforderungen der stetig wachsenden Cyber-Bedrohungen aus ihrem eigenen Umfeld. Umso effektiver ist es, offen miteinander zu sprechen und von der Entwicklung gemeinsamer Abwehrstrategien zu profitieren. Da die DCSO unabhängig von Technologieanbietern agiert und Gewinne in Forschung und Entwicklung reinvestiert werden, entsteht ein echter Mehrwert für alle beteiligten Unternehmen.“ (mr)

- www.dcso.de

IT-Sicher in die Zukunft – aber wie?

Trotz der wachsenden Zahl medienwirksamer Cyber-Attacken fehlt es vielen Unternehmen noch immer an Handlungsmotivation. Die vergangenen Wochen haben gezeigt, dass sich Unternehmen zunehmend Gefahren ausgesetzt sehen, die sich von altbekannten Bedrohungslagen deutlich unterscheiden. Unternehmen müssen sich aktiv an diese neue Ausgangssituation anpassen, mit ihr lernen und sich von alten Sicherheitskonzepten verabschieden.

Im Bereich IT-Sicherheit wird es maßgeblich darauf ankommen up-to-date und gut vorbereitet zu sein. Eingefahrene Prozesse, wie etwa sich alle drei bis fünf Jahre mit einer neuen Sicherheitslösung zu befassen, müssen deutlich agileren und variableren Modellen weichen. Das Thema trifft dabei gleichermaßen international agierende Konzerne als auch den kleinen produzierenden Betrieb. Während früher im Bereich Cyber-Kriminalität Themen wie Industriespionage im Vordergrund standen sind die heutigen Angriffsmodelle deutlich banaler. Stefan Hörhammer, COO des IT&C Systemhauses Medialine, erläutert:

Stefan Hörhammer, Medialine

„Hacking ist einfach geworden. Sie können sogar Hacker, Bot-Netze und Cyber-Angriffe im World Wide Web kaufen – ebenso einfach zusammengeklickt wie eine Bestellung bei Zalando oder Amazon.“

Ein Tag ohne eingehende oder ausgehende E-Mails? Keinen Zugriff mehr auf die buchhalterischen Vorgänge? Der Verlust aller Kundendaten? Stillstand in der Produktion? Es geht längst nicht mehr um den Diebstahl von geistigem Eigentum, Konstruktionsplänen oder Rezepturen bzw. darum, wie viel eine einzelne Information für den Angreifer wert sein könnte, sondern wie viel funktionierende Geschäftsprozesse und sichere Daten für das Unternehmen selbst bedeuten. IT wird in vielen Unternehmen noch immer als Nebensache gesehen, obwohl sie längst das Rückenmark des Unternehmens bildet. Zu den wirtschaftlichen Risiken kommt im Ernstfall leicht noch der Reputationsschaden bei Mitarbeitern, Kunden und Lieferanten hinzu. Ein Cyber-Angriff wird so schnell existenzbedrohend. Im Ernstfall zählt nur wie gut ein Unternehmen vorbereitet war. Ohne Prävention kann lediglich Schadensbegrenzung betrieben werden.

Es gibt jedoch Lösungswege, die Unternehmens-IT sicherer zu machen. Zunächst einmal sollten sich Unternehmen mit guten Standards ausstatten: Antivirenschutz, Firewall, Antispam-Lösung, Client-Management, Mobile-Device-Management sind unverzichtbar. Wichtig ist aber vor allem auch, dass diese Lösungen gut konfiguriert sind und keine Sicherheitslücken bieten. Dies gilt ebenso für die Konfiguration der IT-Infrastruktur, welche im Geschäftsalltag häufig vernachlässigt wird. Da Geschäftsmodelle individuell sind, muss es auch das Sicherheitskonzept sein. Mit einer individuellen Analyse der Geschäftsprozesse können Experten ein maßgeschneidertes Sicherheitskonzept für Unternehmen anfertigen. (mr)

- www.medialine.ag

IT- Sicherheitsexperten gefragt

Angesichts weltweiter Cyber-Angriffe wachsen die Anforderungen an die IT-Sicherheit in Unternehmen, Behörden und Organisationen. „Der aktuelle Hacker-Angriff ‚WannaCry‘ in mehr als 100 Ländern hat sehr deutlich gezeigt, wie groß der Bedarf an IT-Sicherheitsexperten ist“, sagt Sonja Pierer, Geschäftsführerin der ManpowerGroup-Tochter Experis. Die aktuellen Entwicklungen bestätigt eine internationale Studie. Demnach gehört Wissen über Netzwerksicherheit zu den wichtigsten Fachkenntnissen, die Unternehmen von IT-Experten erwarten.

Die Studie basiert auf einer aktuellen Online-Umfrage unter mehr als 1.100 IT-Managern, CIOs und Personalverantwortlichen in elf Ländern, die in Einstellungsentscheidungen von IT-Experten involviert sind. Gefragt wurde nach den wichtigsten fachlichen Fähigkeiten, die IT-Experten für unterschiedliche Funktionen wie etwa die Durchführung von BI-, ERP- oder Analytics-Projekten mitbringen müssen.

Die Studie zeigt, dass Unternehmen in Ländern wie den USA, Japan und Indien das Thema IT-Sicherheit noch etwas höher einstufen als in Deutschland. Dagegen sind Führungskräften, Managern und Personalverantwortlichen im Inland Big Data-Kenntnisse deutlich wichtiger als ihren internationalen Kollegen. Drei Viertel aller Befragten aus deutschen Firmen erwarten Fähigkeiten in der Datenanalyse, global sind es dagegen nur gut zwei Drittel. (mr) ■