Cyberrisiken in Zeiten von Industrie 4.0 – Neue Herausforderungen für Unternehmen und deren Versicherungsschutz

Die Digitalisierung und die dynamischen Entwicklungen rund um die „Industrie 4.0" verändern zahlreiche Wirtschaftszweige nachhaltig. Für viele Unternehmen – gerade aus dem Mittelstand – bringt dies große Chancen mit sich. Doch neben den Potenzialen gibt es auch zahlreiche Risiken, die nicht außer Acht gelassen werden dürfen. Zu ihnen zählt insbesondere die Cyberkriminalität. Sie nimmt rasant zu und stellt Unternehmen aller Branchen vor ganz neue Herausforderungen.

Bild: www.shutterstock.com, Sven Hoppe

AUTOR

Dennis Gottschalk

ist Firmenkundenbetreuer bei der VSM Versicherungsstelle Stahl- und Metallverarbeitung GmbH in Dortmund

Das IT-Netz des Bundestags musste mehrere Tage abgeschaltet werden, und bei zahlreichen Krankenhäusern im ganzen Land fielen EDV-gestützte Systeme längere Zeit aus. Dies sind nur zwei der in letzter Zeit der breiten Öffentlichkeit bekannt gewordenen Beispiele für die Gefahren, die von Hackern und Schadsoftware ausgehen. Auch der Mittelstand gerät zunehmend in das Fadenkreuz von Cyberkriminellen. Das Erschreckende: Buchstäblich jeder kann von einem solchen Angriff betroffen sein. Das geht unter anderem aus einer Studie der Unternehmensberatung Corporate Trust hervor. Danach ist schon fast jedes zweite deutsche Unternehmen einmal Ziel eines Cyberangriffs geworden. Die Frage, die sich Unternehmen stellen müssen, ist daher nicht ob, sondern wann sie Opfer einer solchen Attacke werden.

STEIGENDE FALLZAHLEN

Die polizeiliche Kriminalstatistik spricht ebenfalls eine deutliche Sprache. So listet sie für das Jahr 2014 knapp 247.000 Straftaten im Bereich Internet und etwa 74.000 Fälle im Bereich Computerkriminalität auf. Prominentes Ziel eines Datenangriffs im Jahr 2013 war beispielsweise ein großer Mobilfunkanbieter. Die Täter erlangten Zugang zu Stammdaten von zwei Millionen Kunden. Darin enthalten waren unter anderem Namen, Adressen und Bankdaten. Nur einer von vielen Datendiebstählen im großen Stil. Ebenfalls im Jahr 2013 traf es einen weltweit agierenden Softwareanbieter. Hacker kopierten Adressen, Kreditkartendaten und Passwörter von 2,9 Millionen Kunden sowie die geheimen Quellcodes mehrerer Programme.

Wenn „unsichtbare" Täter beispielsweise Viren und Trojaner in Computersysteme einschleusen oder EDV-Systeme und Produktionssteuerungsanlagen ausfallen, entstehen nicht nur bei

großen Konzernen schnell immense Schäden. Auch für kleine und mittelständische Unternehmen drohen dann existenzgefährdende Folgen. Diese betreffen zum einen die attackierten Unternehmen selbst. Auf sie kommen unter anderem Kosten für kriminaltechnische Untersuchungen, Betriebsunterbrechungen und nicht zuletzt für einen möglichen Reputationsverlust zu. Zum anderen kommen Schadenersatzansprüche Dritter, die Firmen und Institutionen beispielsweise aufgrund einer Datenschutzrechtsverletzung befriedigen müssen, hinzu.

Ein weiteres großes Problem in diesem Zusammenhang: Viele Unternehmensverantwortliche ignorieren die Gefahren noch immer oder unterschätzen die möglichen Folgen. Sie gehen insbesondere beim Versicherungsschutz von falschen Voraussetzungen aus. Denn mitunter herrscht die Meinung vor, dass das eigene Unternehmen bereits ausreichend gegen mögliche Schadenfälle aus dem Cyberbereich abgesichert ist. Dies ist allerdings regelmäßig nicht der Fall. So fehlt für den Eintritt einer Sachversicherung in der Regel ein konkreter Sachschaden und Haftpflichtpolicen greifen nur dann, wenn den Versicherungsnehmer auch ein Verschulden trifft – was meistens nicht der Fall ist.

CYBERVERSICHERUNGEN SCHÜTZEN

Abhilfe bieten zum einen geschützte IT-Systeme, die ein Eindringen sowie das Stehlen und Manipulieren von Daten bestmöglich verhindern. Hinzu kommen sogenannte „Cyberversicherungen", die vor den Folgen einer aus Hackersicht erfolgreichen Attacke schützen und von immer mehr Assekuranzen angeboten werden. Sie werden direkt über die Versicherungen oder über spezialisierte Makler vertrieben und bieten Schutz vor Eigenschäden und Drittschäden.

AUFTRETEN VON EIGENSCHÄDEN

Als Eigenschäden werden Schäden am Vermögen des versicherten Unternehmens selbst bezeichnet. Hierzu zählen zum Beispiel entgangene Gewinne. Dies könnte beispielsweise dann der Fall sein, wenn Entwicklungsdaten der nächsten innovativen Produktgeneration eines Unternehmens von einem Hacker gestohlen und an einen Wettbewerber verkauft werden. Der Eigenschaden tritt dann ein, wenn das bestohlene Unternehmen feststellen muss, dass unmittelbar vor der beabsichtigten Markteinführung dieser Wettbewerber ein gleichartiges Produkt auf den Markt bringt.

Bekommen Hacker Zugriff auf interne Unternehmensdaten, die beispielsweise Geschäftsstrategien betreffen, kommt es vor, dass diese Cyberkriminellen das Unternehmen mit deren Veröffentlichung bedrohen und damit erpressen. Um eine Veröffentlichung der geheimen Daten zu verhindern, zahlen Unternehmen dann häufig eine Art „Lösegeld".

In beiden Fällen springt die entsprechende Police ein und der Versicherer ersetzt die Eigenschäden des Versicherungsnehmers beispielsweise in Form von

- Schadenbeseitigungskosten, Kosten der Wiederherstellung von Daten oder der technischen Verfügbarkeit von IT-Systemen
- Kosten, die durch Betriebsunterbrechungen entstanden sind
- Kosten der Information gegenüber Dateninhabern bei Verlust personenbezogener Daten sowie
- Lösegeldzahlungen an Hacker bei Erpressungen nach Datenverlust.

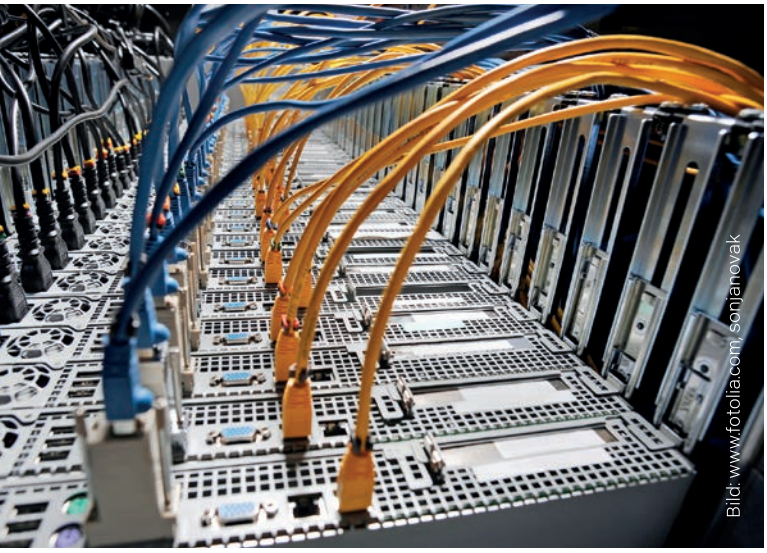
Bild: www.fotolia.com, sonjanovak


Bild: www.fotolia.de, Thomas Pajot

Von erheblicher praktischer Relevanz sind sogenannte Betriebsunterbrechungsschäden. Sie erreichen schnell existenzgefährdende Ausmaße. Von Betriebsunterbrechungen betroffen sind sowohl produzierende Unternehmen als auch Dienstleister und Händler, die beispielsweise ihren Vertrieb infolge von Hackerattacken über längere Zeit nicht betreiben können.

Eine weitere und mitunter erhebliche Position der Eigenschadendeckung sind Informationskosten. Unternehmen sind nach § 42a Bundesdatenschutzgesetz verpflichtet, im Fall eines Verlustes von personenbezogenen Daten nicht nur die zuständige Behörde, sondern auch sämtliche Betroffene zu informieren. Betrifft dies – wie bereits beschrieben – Millionen von Datensätzen, fallen mitunter extrem hohe Kosten an. Diese resultieren sowohl aus dem klassischen Anschreiben von Betroffenen, als auch aus dem publik machen eines solchen Diebstahls – zum Beispiel durch das Schalten von Anzeigen in führenden Printmedien. Nach jüngsten Verschärfungen dieser Vorgaben wird es aller Voraussicht nach auch in Zukunft zum weiteren Anstieg derartiger Ausgaben kommen.

ZWEITER LEISTUNGSBESTANDTEIL: SCHÄDEN AM VERMÖGEN DRITTER

Schäden durch Cyberrisiken können nicht nur am eigenen, sondern auch am Vermögen von Kunden oder Geschäftspartnern entstehen. In diesen Fällen handelt es sich um sogenannte Drittschäden. Um diese abzusichern, befasst sich der zweite wesentliche Leistungsbestandteil von Cyberpolicen mit der Haftpflichtdeckung. Diese zielt auf den Fall, dass ein versichertes Unternehmen bei einem Dritten durch einen Cybervorfall einen Vermögensschaden verursacht und der Dritte infolgedessen Schadenersatz verlangt.

Auch hier ein konkretes Beispiel: Hacker bekommen Zugriff auf aktuelle Kreditkartendaten von Kunden eines Online-Händlers, mit denen Zahlungen vorgenommen werden können. Bestand bei dem betroffenen Händler ein Datenleck, welches sich die Hacker zunutze machten, haben geschädigte Kreditkarteninhaber, Kreditkarteninstitute und Geschäftspartner gegebenenfalls das Recht, Schadenersatz gegenüber dem Online-Händler geltend zu machen.

Insbesondere der Verlust von persönlichen Daten von Kunden oder Geschäftspartnern birgt ein weiteres großes Risiko für Unternehmen: das von schwerwiegenden Reputationsschäden. Dabei verlieren sie Vertrauen und büßen an positivem Image ein. Über ein zur Schadenbegrenzung erforderliches Krisenmanagement – wie beispielsweise eine zielgerichtete Pressearbeit im Krisenfall – verfügen betroffene Unternehmen in der Regel nicht. Cyberpolicen können deshalb als zusätzliche Bestandteile sogenannte Unterstützungsleistungen enthalten. Sie greifen, wenn externe Hilfe durch Experten wie PR-Berater, Rechtsanwälte, IT-Forensiker zur Datenwiederherstellung nötig wird oder beispielsweise technischer Support, wie zusätzliche Serverkapazitäten, bereitgestellt werden muss.

ANGEBOTE UNÜBERSICHTLICH – FACHKUNDIGE BERATUNG NOTWENDIG

Selbst wenn der Wille vorhanden ist, sich bestmöglich gegen Hacker und Schadsoftware abzusichern, gibt es Hindernisse, die dem mitunter im Weg stehen. So empfinden viele Sicherheitsbeauftragte in Unternehmen das aktuell am Markt verfügbare Angebot rund um Cyberversicherungen als unübersichtlich und nur schwer vergleichbar. Wesentliche Unterschiede existieren dabei sowohl in den einzelnen Konzeptionen als auch in den Inhalten der Policen.

Hinzu kommt, dass denjenigen, die sich schützen wollen, nicht immer klar ist, welche Risiken bei ihnen konkret vorliegen und wie diese bestmöglich abgesichert werden können. Dies alles macht eine entsprechende Beratung durch einen fachkundigen und erfahrenen Partner dringend notwendig.

Dennis Gottschalk
VSM Versicherungsstelle
Stahl- und Metallverarbeitung GmbH
Hohenzollerstr. 2, 44135 Dortmund
Tel.: +49 231 5404-521
Fax: +49 231 5404-7521
dennis.gottschalk@leue.de