Matthias Müller / Sebastian Scholz

Automatisierte Risikoanalyse – Katalysator für das Cyber-Geschäft

Trotz real steigender Bedrohung durch Internetkriminalität kommt das Geschäft mit Cyber-Versicherungen in Deutschland nur zögernd in Gang. Mit ein Grund dafür ist die für Versicherungen aufwändige und für Kunden oft als intransparent empfundene Risikoeinschätzung. Automatisierte Rating-Tools können nun Bewegung in den Markt bringen. Erste Assekuranzen nutzen die neue Technologie bereits.

Die Fakten sprechen für sich: Die Zahl der registrierten Softwarelücken ist 2017 weltweit um 37,5% von rund 8.000 auf 11.003 angestiegen. Die zunehmende Digitalisierung von Wirtschaft und Privatleben schafft eine ständig wachsende Angriffsfläche für Cyber-Attacken. Weltweit summieren sich die jährlichen Schäden durch Cyber-Kriminalität auf rund 490 Mrd. Euro, allein 55 Mrd. Euro hiervon entfallen auf Deutschland, das entspricht 1,6% des Bruttoinlandsproduktes. Jedes zweite Unternehmen hierzulande war zwischen 2015 und 2017 schon einmal Opfer einer Cyber-Attacke in Form von Datendiebstahl, Industriespionage oder Sabotage. Das hat eine gemeinsame Studie des Branchenverbands Bitkom und des Bundesamts für Verfassungsschutz ermittelt.

Die Risiken sind real und vielschichtig: Neben direkten Schäden wie Betriebsunterbrechungen durch Systemausfälle und Wiederherstellungs- und Rekonstruktionskosten können auch Kosten für IT-Forensik, PR-Krisenmanagement oder Spezialanwälte entstehen. Zudem drohen Schadensersatzansprüche Dritter, etwa, wenn vertrauliche Kundendaten an die Öffentlichkeit gelangen.

Schutz gegen Cyber-Attacken bei KMU oft nur mangelhaft

Mit der ständig wachsenden Cyber-Bedrohung steigen die Anforderungen an das IT-Sicherheitsmanagement. Während sich große Unternehmen in der Regel adäquat ausgestattete IT-Abteilungen mit Expertenteams leisten können, reduziert sich der IT-Schutz bei kleinen und mittleren Unternehmen (KMU) meist auf technischen Basisschutz wie Firewalls, Virenscanner und Back-ups. Laut Bitkom verfügen lediglich 20% über Angriffserkennungssysteme, nur 17% führen regelmäßig Penetrationstests durch, bei denen Cyber-Angriffe simuliert werden.

> „Für Versicherer ist es bislang schwierig, eine objektive Beurteilung des Schadenrisikos unter vertretbarem Aufwand durchzuführen“

Entsprechend groß ist das Potenzial für Cyber-Versicherungen im gewerblichen Bereich. Allein im KMU-Sektor gibt es in der Bundesrepublik mehr als 200.000 Betriebe mit einem Jahresumsatz zwischen zwei und 50 Mio. Euro – die mehrheitlich noch keine Policen gegen Cyber-Risiken besitzen. Für die Gesamtwirtschaft prognostiziert die Münchner Rück bis 2020 ein jährliches Prämienvolumen von 8,5 bis 10 Mrd. Euro.

Prämienvolumen noch gering

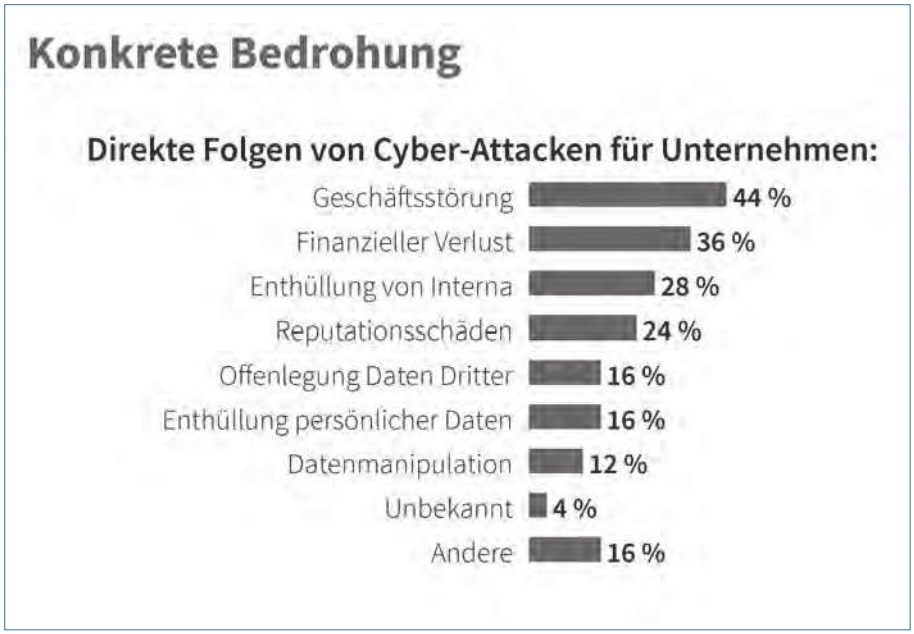
Noch ist der Markt für Cyber-Policen in Deutschland allerdings überschaubar. Der Spezialversicherer Hiscox schätzt, dass erst ein Drittel der Unternehmen überhaupt eine Versicherung abgeschlossen hat. Und das Gesamtprämienvolumen liegt laut KPMG erst bei rund 90 Mio. Euro. Zum Vergleich: In den USA investieren Unternehmen pro Jahr bereits knapp drei Mrd. Dollar in Versicherungen gegen Internetkriminalität.

Abbildung 1: Die Risikolage

Quellen: Bitcom, Centre for Strategic and International Studies

Matthias Müller
Mitglied der Geschäftsleitung der PPI AG und für den Bereich Versicherungen verantwortlich. matthias.mueller@ppi.de
Sebastian Scholz
Senior Manager im Bereich Consulting Versicherung u. a. für das Geschäftsfeld Cyber bei der PPI AG.verantwortlich. sebastian.scholz@ppi.de

Abbildung 2: Welche Gefahren drohen



Quelle: KPMG

Um das Potential zu heben, das im Cyber-Segment schlummert, müssen die Versicherungen zunächst eine Reihe von Hürden überwinden. Das Umfeld ist ausgesprochen komplex und hochdynamisch. Es fehlt an kritischer Masse bestehender Verträge – in der Folge liegen kaum verlässliche Schadendaten als Kalkulationsgrundlage für Aktuare vor. Eine zentrale Herausforderung ist dabei die Risikobewertung im Vorfeld der Policen-Kalkulation.

Für Versicherer ist es bislang schwierig, eine objektive Beurteilung des Schadenrisikos unter vertretbarem Aufwand durchzuführen. Insbesondere in der Prämien- und Policen-Ausgestaltung bestehen nicht zuletzt aufgrund der unterschiedlichen Deckungsbausteine für jeden Versicherer große Herausforderungen. Zur Beurteilung der IT-Sicherheitsausstattung von Unternehmen und den damit verbundenen Risiken ist intern ein hohes Maß an IT-Security-Expertise notwendig.

Abbildung 3: Wachstumsperspektiven in Deutschland

Quelle: Hiscox

Risikoeinschätzung oft noch zu aufwändig

Die einzelnen Deckungsbausteine müssen zudem auf die individuelle Situation des zu versichernden Unternehmens zugeschnitten sein. So unterschiedlich sich die Risiken darstellen, so individuell muss gegebenenfalls auch der Versicherungsschutz maßgeschneidert werden. Unternehmen müssen melden, wenn sie beispielswiese bestimmte Geschäftsprozesse wie das Belegwesen digitalisieren. Der Versicherer muss dann wiederum die Police anpassen. All diese Faktoren treiben die Kosten für die Risikoeinschätzung massiv nach oben.

Auch aus Sicht der gewerblichen Versicherungsnehmer ist der Anbahnungsprozess – konkret also Risikoeinschätzung und Preisfindung – oftmals schwierig und teilweise nicht nachvollziehbar. Welche Voraussetzungen und Obliegenheiten verlangt der Versicherer und wie definiert er diese? Erfüllt das IT-System des eigenen Unternehmens diese? Welche Risiken deckt die Versicherung überhaupt ab?

Für die Risikoanalyse nutzen Versicherer bislang hauptsächlich drei Möglichkeiten: Zum einen die vom GDV entwickelten unverbindlichen Musterbedingungen zur Cyber-Versicherung. Sie sind für die Bewertung von KMU mit einem Umsatz von bis zu 50 Mio. Euro konzipiert. Der durchaus umfangreiche Fragebogen kann jedoch nur eine Basiseinschätzung darstellen, insbesondere weil er die Selbstwahrnehmung der Unternehmen wiedergibt. Rückfragen der Kunden bei Verständnisproblemen sowie unvollständige oder inkonsistente Angaben machen den Fragebogen zudem fehleranfällig. Dauer und Aufwand der Auswertung steigen dadurch.

Dilemma für Anbieter und Nachfrager

Viele Versicherer führen zudem Risikodialoge mit potenziellen Kunden, um so die notwendigen Informationen zur Bedeutung von IT-Anwendungen und über den Status der IT-Sicherheit im Unternehmen zu erhalten.

IT-Audits, die dritte Option der Risikoeinschätzung, bieten den Versicherern ein hohes Maß an Risikotransparenz, weil sie eine äußerst detaillierte Einschätzung liefern. Die Verfahren sind jedoch sehr zeit-, personal- und kostenintensiv. Für Unternehmen mit Jahresumsätzen zwischen

einer und zehn Mio. Euro sind solche Audits in der Regel nicht rentabel. So verfügt laut Bitkom Research lediglich ein Viertel der Unternehmen in Deutschland über Audits durch externe Spezialisten.

Das derzeitige Instrumentarium zur Risikoanalyse offenbart das Dilemma, in der sowohl Anbieter wie Nachfrager stecken: Sehr viele Unternehmen sind zu groß, als dass ein einfacher Fragebogen zur Risikoeinschätzung ausreichen würde, aber nicht groß genug, so dass sich ein Audit rentieren würde. Betroffen sind hier vor allem Mittelständler.

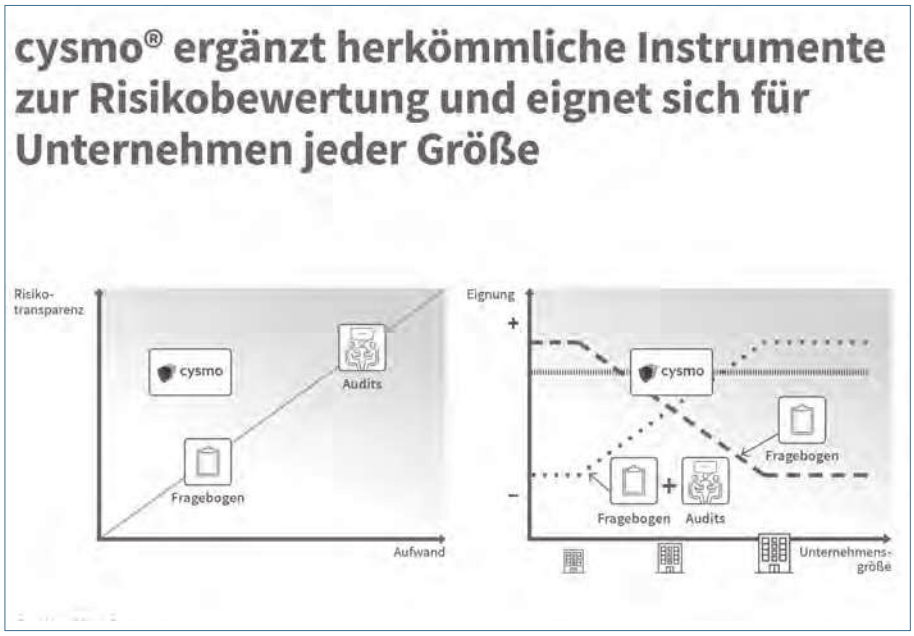
Vollautomatisierte Risikobewertung bringt Bewegung in den Markt

Um das Potenzial des Marktes zu heben, müssen Versicherer in die Lage versetzt werden, in einem ersten Schritt die IT-Risiken eines Unternehmens individuell, aber effizient einzuschätzen – allerdings ohne dabei den Vertriebs- oder Antragsprozess in die Länge zu ziehen. Eine innovative Lösung ist vollautomatisiertes Echtzeit-Rating, das jetzt in Deutschland erstmals speziell für Versicherungen verfügbar ist. Das Analysetool cysmo der PPI AG erlaubt Versicherern die schnelle und präzise Bewertung von Cyber-Risiken im gewerblichen Bereich.

Underwriter in den Versicherungen können direkt während des Antragsprozesses die IT-Angreifbarkeit des jeweiligen Unternehmens online testen. Basis für das Online-Rating ist der Domainname des zu prüfenden Unternehmens. Weder Versicherer noch antragstellendes Unternehmen müssen hierfür Zeit und personelle Ressourcen aufwenden. Ziel: Das browserbasierte Analyse- und Bewertungstool soll innerhalb weniger Minuten eine transparente, nachvollziehbare und fundierte Risikobewertung erstellen. In das von cysmo erstellte Scoring fließen technischen Empfehlungen und Vorgaben von Branchenstandards wie BSI- oder VDS-Richtlinien mit ein.

cysmo untersucht aus Angriffsperspektive die IT-Umgebung der Firma, checkt beispielsweise Netzwerk-Traffic, Routing Bereiche oder Server-Konfigurationen. Die Prüfung läuft vollautomatisch, ohne Rechenlast auf das jeweilige System zu erzeugen oder gar einzudringen. Das Analyse-Tool dokumentiert Sicherheitslücken in den sicherheitsrelevanten Bereichen: Hierzu zählen unter anderem offene Ports, sichtbare Zugänge, Mailverschlüsselungsverfahren, aber auch die Fähigkeit des Systems, sogenannten Distributed-Denial-of-Service (DDoS) -Angriffen zu widerstehen, die das System durch eine Vielzahl von Anfragen lahmlegen können.

Abbildung 4: Ein Instrument zur Risikobewertung



Quelle: PPI AG

> „Sehr viele Unternehmen sind zu groß, als dass ein einfacher Fragebogen zur Risikoeinschätzung ausreichen würde, aber nicht groß genug, so dass sich ein Audit rentieren würde. Betroffen sind hier vor allem Mittelständler“

Die Online-Analyse erlaubt Underwritern eine schnelle objektive Risikoeinschätzung und somit eine marktgerechte Kalkulation der Versicherungs-Police. Die Einzelergebnisse des Scorings können im Antragsprozess den jeweiligen Deckungsbausteinen einer Police zugeordnet werden.

Software identifiziert IT-Schwachstellen

Anhand der Analyse können Versicherer ihren Kunden nicht nur die Konditionen ihrer Cyber-Police nachvollziehbar erklären. Der Kunde erhält dadurch auch erste Anhaltspunkte zur Verbesserung der IT-Sicherheit in seinem Unternehmen. Davon können letztlich beide – der Versicherer und sein Kunde – profitieren, denn das niedrigere Schadenrisiko schlägt sich auch in der Prämie nieder.

Versicherungen könnten das Tool beispielsweise als zusätzlichen Service oder für die Analyse des Bestands nutzen. Beispielsweise können Assekuranzen ihren Kunden bei Abschluss einer Police regelmäßig Cyber-Reports und damit ein nutzwertiges Monitoring ihrer IT-Angreifbarkeit zur Verfügung stellen. Eine Win-win-Situation: Der Kunde erlebt diesen Service seiner Versicherung als sehr dienlich, da er ihm dabei hilft, sicherer zu werden. Und gleichzeitig wird die Combined Ratio positiv beeinflusst.