KOBAN SÜDVERS

Stark beraten, exzellent versichert

PRESSEINFORMATION

Pulverfass Cyberrisk:
Existentielle Bedrohung für Österreichs Wirtschaft

Alarmierend: Nur rund ein Drittel der heimischen Unternehmen hat eine Cyberversicherung abgeschlossen. Und dass, obwohl die Anzahl der Cyberattacken laufend zunimmt: Allein von 2019 auf 2020 ist sie um 26,3 Prozent gestiegen. Vermehrtes Home-Office und der Technologieschub der letzten Monate spitzen die Lage noch einmal dramatisch zu. Die vielfältigen Gefahren gut abzusichern ist aber mit vielerlei Fallstricken verbunden, manches ist aufgrund von Ausschlusskriterien gar nicht versicherbar. Um die Cyber-Risikosituation von Unternehmen optimal evaluieren zu können, greifen die Experten von KOBAN SÜDVERS auf das innovative Risikoevaluierungs-Tool „cysmo" zurück. Mag. Kerstin Keltner, Expertin für Cyberversicherung bei KOBAN SÜDVERS, berichtet im Zusammenhang damit zudem von einem bemerkenswerten Wandel: „Die Cyberversicherung entwickelt sich immer mehr weg von der reaktiven Risikoabsicherung hin zum proaktiven Risikomanagement durch die Versicherer."

Vielfältige Gefahren
Phishing, Ransomware, Malware, Fraud oder DoS sind nur einige der aktuellen Cyber-Risiken. Neben gezielten oder zufälligen Angriffen von Dritten auf das eigene Unternehmen können auch Eigenverschulden oder Elementargefahren massive Schäden und damit Kosten verursachen. Beispielsweise, wenn ein Brand den Server und sämtliche darauf gespeicherte Daten zerstört und eine entsprechende Sicherung fehlt. Oder wenn große Datenmengen irrtümlich an den falschen Empfänger gesendet werden. Neben den Wiederherstellungskosten gibt es eine Reihe anderer Probleme, die einem Unternehmen im Fall der Fälle teuer zu stehen kommen können, etwa Datenschutzverletzungen oder Betriebsunterbrechung.

Versicherer als Feuerwehr
Schon bei den ersten Ungereimtheiten sollte reagiert werden. „Sofortiges Handeln kann den Schaden eingrenzen", weiß Keltner. „Nur, wenn man weiß, wo der Feuerlöscher steht und wie er funktioniert, kann man auch schnell löschen", so Keltner weiter. Dementsprechend wären neben einer Cyberversicherung auch Notfallpläne und ein gut funktionierendes Krisenmanagement essenziell, inklusive regelmäßiger Schulungen und Trainings. Der erste Weg bei einem bemerkten Cyberangriff sollte jedenfalls zu einem IT-Sicherheitsexperten und dann unverzüglich zur Polizei führen. „Oft wird dann die IT-Abteilung angerufen, die aber – wenn überhaupt gleich erreichbar - meist nur wenig bewirken kann", betont Keltner.

Anbieter von Cyber-Versicherungen bieten im Krisenfall Assistance-Leistungen an: Von einer Rund-um-die-Uhr besetzten Hotline bis hin zur Forensik um den Angreifer, die Art des Angriffs und damit das Schadenausmaß genau feststellen zu können. Dem komme Keltner zufolge insbesondere beim Einsatz von Schadsoftware enorme Bedeutung zu: „Was kann die Software, wurden die Daten kopiert, gesperrt oder gelöscht? Gibt es eine Lösegeldforderung? Oder werden die abgezogenen Daten womöglich am Schwarzmarkt angeboten?". Durchschnittlich dauere es 287 Tage, ehe Datenschutzverletzungen überhaupt entdeckt und eingegrenzt werden können.

Der Teufel steckt im Detail
Wer eine Cyberversicherung abschließen möchte, ist gut beraten, die Versicherungsdetails ganz genau zu lesen und zu vergleichen. „Krisenmanagement, Haftpflicht,

Betriebsunterbrechung, Datenwiederherstellung, Erpressung, Rechtsschutz, vorsätzliche Schädigung und Benachrichtigungskosten sind in so gut wie jedem Versicherungsprodukt enthalten. In den Details gibt es aber große Unterschiede. Insbesondere Sublimits, also die Limitierung von Teilleistungen innerhalb eines Versicherungsvertrages, schränken die Versicherungssumme enorm ein", betont Keltner. Für bestehende Verträge rät die Expertin zu einer jährlichen Kontrolle. Dabei werde anhand einer Checkliste abgearbeitet, ob sich die Risikosituation verändert hat, beispielsweise durch die Zusammenarbeit mit neuen Dienstleistern oder Computersystemen.

Gerade in diesem heiklen Themenfeld sei gute, objektive Beratung durch einen unabhängigen Makler besonders wichtig. „Die erste Frage sollte sein ‚Wovor fürchten Sie sich am meisten?' und danach geht man alles im Detail durch", so Keltner. Um die IT-Sicherheit eines Unternehmens zu überprüfen, setzen die Experten von KOBAN SÜDVERS auf ein innovatives Risikomanagement-Tool namens cysmo. Im Zuge einer passiven Überprüfung wird die IT-Infrastruktur anhand von Schwachstellen, die öffentlich von außen einsehbar sind, innerhalb weniger Minuten bewertet. Dabei wird insbesondere das Darknet nach Daten über das Unternehmen abgefragt und der Mailserver oder andere kritische Dienste auf Fehlkonfigurationen hin untersucht. Aus den Ergebnissen werden Handlungsempfehlungen abgeleitet, die wiederum als Basis für das Riskmanagement und die -absicherung dienen.

KOBAN SÜDVERS
Der inhabergeführte Versicherungsmakler und Berater in Versicherungsangelegenheiten richtet sich mit seinem innovativen Leistungsportfolio an Industrie-, Gewerbe- und Privatkunden. Er agiert national über Niederlassungen in ganz Österreich (Wien, Graz, Klagenfurt, Villach, Salzburg, Sillian und St. Pölten). Aktuell beschäftigt das Unternehmen in Österreich 140 Mitarbeiter und verwaltet ein Prämienvolumen von rund 90 Mio. Euro. Spezialisierungen und Kerngeschäft bilden: Industrie- und Gewerbeversicherungen, Risikoanalysen und -management, Vertrauensschaden-, Garantie- und Kreditversicherungen, betriebliche Alters- und Gesundheitsvorsorge, D&O und Cyberversicherungen sowie Beratungen im Schadenfall. Als Österreich-Repräsentant des vor 30 Jahren gegründeten Worldwide Broker Networks (kurz: WBN) liegt ein besonderes Augenmerk auf der Betreuung international tätiger Unternehmen und Risiken.

Wien, 21. Oktober 2021

Informationen zu KOBAN SÜDVERS unter www.kobangroup.at

Presseanfragen bitte an:
PR-Büro Halik, Sparkassaplatz 5a/2, 2000 Stockerau
Tel.: 02266/674 77, E-Mail: office@halik.at