Cyber-Sicherheit für kleine und mittlere Unternehmen: Notlösung oder nutzloser Luxus?

ASSCOMPACT VERTRIEBSLEITER ERNST VALLANT INTERVIEWT MAG. CHRISTIANA BRUCKNER UND MICHAEL GANZWOHL, GESCHÄFTSLEITER DER CYRISO CYBER RISK SOLUTIONS GMBH

Cyber-Sicherheit ist eine unabdingbare Notwendigkeit, kein Luxus. Studien von Organisationen wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und verschiedenen Versicherungen zeigen einen stetig wachsenden Trend von Cyberattacken auf kleine und mittlere Unternehmen. Diese Attacken führen nicht nur zu direkten finanziellen Verlusten durch Datendiebstahl oder Lösegelderforderungen (Ransomware), sondern auch zu indirekten Schäden durch Reputationsverlust, Produktionsausfälle und den Aufwand für die Schadensbegrenzung. Eine robuste Cyber-Sicherheitsstrategie ist daher kein Luxus, sondern eine strategische Investition in den langfristigen Erfolg und die Existenzsicherung des Unternehmens.

CyRiSo bietet maßgeschneiderte Lösungen im Bereich der Cybersicherheit an. Was zeichnet Ihre Dienstleistungen besonders aus? Gibt es Mitbewerber?

CHRISTIANA BRUCKNER: Im Themenbereich Cybersicherheit gibt es viele Anbieter, deren Leistungen und Produkte sich oft ähneln oder sogar überlappen. Für den Kunden ist es daher schwierig, das passende Angebot zu finden, das seinen tatsächlichen Bedarf deckt und einen echten Nutzen bringt.

Wir verstehen die Herausforderungen und unterstützen unserer Kunden bei der Bewältigung. Wir helfen kleinen und mittelständischen Unternehmen dabei sicher zu werden.. Wir konzentrieren uns auf langfristige Serviceverträge „As-A-Service“ , die genau auf die Bedürfnisse unserer Kunden zugeschnitten sind. Unsere Unterstützung in den Bereichen technische Sicherheitsüberprüfungen, Hilfe bei Cybervorfällen technische und organisatorische Abdeckung von Standards, Normen und Gesetzen wie z.B. ISO27001, NIS2 oder DSGVO helfen auch dabei, die verfügbaren Mittel sinnvoll einzusetzen und die richtigen Maßnahmen durchzuführen.

Sonst droht ein Wildwuchs and Dienstleistungen und unabgestimmten Produkten, die im Ernstfall nicht den gewünschten Schutz oder Nutzen bringen

Welche spezifischen Sicherheitsbedrohungen sehen Sie derzeit als die größten Herausforderungen für Unternehmen?

MICHAEL GANZWOHL: In letzter Zeit sind Hacker und Cyberkriminelle laut BSI und unseren Erfahrungen deutlich professioneller geworden, und nehmen zunehmen auch kleinere Unternehmen ins Visier. Sie treffen dabei auf Unternehmen, die leider teilweise noch zu unvorbereitet sind und daher einfachere Ziele darstellen. Werden diese Firmen Opfer z.B. eines zielgerichteten Angriffs, dann steigen auch die Kosten für die Vorfallsbeseitigung. Manche Unternehmen überleben das nicht, z.b. wenn durch eine Betriebsunterbrechung Produktionen lahmgelegt werden und Zahlungen der Kunden ausbleiben. Viele Arten von Angriffen können verheerende Folgen haben.

Jüngst ist die bekannte Vodka Marke Stolichnaye Opfer eines Ransomware Angriffs geworden – und ging bankrott.

Was sind aus Ihrer Sicht die größten Herausforderungen, mit denen Unternehmen bei der Umsetzung von Cyberresilienz und Datenschutz konfrontiert sind, und wie unterstützt CyRiSo dabei, diese Herausforderungen zu meistern?

MICHAEL GANZWOHL: Ich beziehe mich wieder auf unsere Zielgruppe kleinerer und mittlerer Unternehmen. Hier sehen wir nicht nur die klassischen Herausforderungen wie z.B. limitierte Sicherheitsbudgets, Mangel an qualifizierten IT-Fachkräften und daraus resultierend falsche oder wirkunslose Maßnahmen. Jetzt verlangen Kunden, Lieferanten, Partner plötzlich Compliance zu Standards (ISO27001, TISAX,…) und die Behörden erlassen Gesetze zur Erhöhung der Cybersicherheit (z.B. NIS2, DORA). Wir sehen nicht nur kleine Unternehmen die damit kämpfen herauszufinden, was eigentlich gefordert wird und wie Anforderungen adäquat und leistbar umgesetzt werden können. Wir sehen unsere Aufgabe darin, den Dschungel an Anforderungen zu durchforsten und gemeinsam mit dem Kunden die richtigen Pfade zu finden. Das können technische oder organisatorische Maßnahmen sein, oder auch Zertifizierungen. Das Problem ist, dass in Zukunft mangelnde Cyberresilienz und schwacher Schutz von Daten ein deutlicherer Wettbewerbsnachteil für Unternehmen darstellen wird. Dies kann sich unterschiedlich auswirken. Zum Beispiel könnte eine Firma als Lieferant nicht berücksichtigt zu werden oder gar existierende Kunden verlieren, da diese neuen Richtlinien folgen müssen. Diese Entwicklung wird viel deutlichere als noch vor wenigen Jahren, als der Sicherheitsstatus eines Unternehmens intransparenter war. Darüber hinaus können Lücken in der Gesetzeskonformität in ein Haftungsrisiko münden.

Inwieweit berücksichtigen Sie bei Ihren Sicherheitslösungen die speziellen Bedürfnisse von kleinen und mittelständischen Unternehmen, die möglicherweise nicht über die gleichen Ressourcen wie große Unternehmen verfügen?

CHRISTIANA BRUCKNER: Wenn wir für ein Unternehmen tätig werden, stehen immer zwei Themen im Vordergrund – Erstens wie kann mit den verfügbaren Budgets

Mag. Christiana Bruckner und Michael Ganzwohl im Gespräch mit Ernst Vallant

die maximale Wirkung erreicht werden und zweitens welche Risiken können durch die richtigen Maßnahmen eliminiert bzw. minimiert werden. Je kleiner die Budgets und je knapper die Ressourcen sind, desto wichtiger ist die Zielgenauigkeit der Aktivitäten. Wichtig für kleine und mittelständische Unternehmen ist es Mittel möglichst wirksam und effizient einzusetzen. Steigt die Resilienz, so reduzieren sich finanzielle Auswirkungen von Cyberangriffen und die Wettbewerbsfähigkeit der Unternehmen steigt. Unser Fokus liegt darauf, mit den vorhandenen Ressourcen die größte Hebelwirkung zu erzielen und eine optimale Kosten-Nutzen-Relation zu erreichen.

Auch setzen wir eine eigene Plattform ein – das CyRiSo Cyber Cockpit – in dem Kunden ihre Cybercompliance und Cybersecurity zentral und benutzerfreundlich überblicken und managen können.

CyRiSo plant, Vermittlern und Maklern Angebote zur Verfügung zu stellen, um deren Kunden zu unterstützen. Welche konkreten Angebote können Vermittler von CyRiSo erwarten, und wie profitieren sie von einer Zusammenarbeit mit Ihnen?

CHRISTIANA BRUCKNER: Genauso wie Vermittler und Makler im Bereich der Versicherungen, sieht CyRiSo sich als ganzheitlicher Berater im Bereich der Risiken aus Cybersecurity. Somit decken sich die Interessen die Risiken des Kunden zu minimieren. Wir würden gerne im ersten Schritt herausfinden, inwieweit Kunden der Vermittler und Makler von Cyber Risiken betroffen sind, z.B. durch unsere Initiative „Fit for Cyber". „Fit for Cyber" ist eine Übersicht über technische Risiken sowie Abdeckung von Industriestandards und gibt dem Unternehmen einen schnellen Überblick über den eigenen Reifegrad. Dieser Überblick kann auch Aufschlüsse geben, inwieweit eine Cyber Versicherung in Frage kommen kann bzw. in welchen Handlungsfelder gearbeitet werden muss, um den Reifegrad zu erhöhen. Im Rahmen von weiterführenden Projekten werden dann mit dem Unternehmen die notwendigen Maßnahmen umgesetzt. An einem bestimmten Punkt, wird der Kunde einen angestrebten Reifegrad erreicht haben. Dann sind entweder Auflagen aus einer bestehenden Versicherung erfüllt, Basisanforderungen vor dem Überlegen einer Cyber Versicherung abgedeckt, oder es ist sichergestellt, dass der Kund in der Lage ist, einen adäquaten Reifegrad langfristig hoch zu halten oder sogar weiter zu erhöhen.

Ihr Unternehmen ist eine Tochtergesellschaft der Vienna Insurance Group (VIG). Wie beeinflusst diese Partnerschaft die strategische Ausrichtung und die angebotenen Dienstleistungen von CyRiSo, insbesondere im Hinblick auf die Bedürfnisse der Versicherungsbranche und deren Kunden?

MICHAEL GANZWOHL: CyRiSo wurde gegründet, um die Cyber Resilienz im KMU-Sektor zu stärken. Das ist unabhängig von den Eigentumsverhältnissen, wir sind da sehr eigenständig. Wir haben unser Serviceangebot aber teilweise in Abstimmung mit der Vienna Insurance Group geformt, um uns noch besser auf die Anforderungen der Kunden aus dem Versicherungssektor vorzubereiten und ein komplementäres Service zu bieten. Setzen sich Unternehmen mit den eigenen Risiken, ▸

den Umgang mit den Restrisiken und Möglichkeiten des Risikotransfer auseinander erhöht sich die Cyber Resilienz und das ist positiv für den gesamten Sektor.

Wie gehen Sie mit der ständigen Weiterentwicklung der Bedrohungslandschaft um, und wie stellen Sie sicher, dass Ihr Unternehmen und Ihre Kunden immer auf dem neuesten Stand der Cybersicherheit bleiben?

MICHAEL GANZWOHL: Man muss die Bedrohungslandschaft ständig im Auge behalten. Es ändert sich schnell. Wir sind durch unseren Fokus auf den Mittelstand auch in der Lage, sektorspezifische Bedrohungen besser abzuschätzen und stellen unseren Kunden gerne dementsprechende Informationen zur Verfügung. Das ist auch der Vorteil unseres as-a-Service Ansatzes. Durch den kontinuierlichen Kontakt mit unseren Kunden – beispielsweise, wenn wir den externen Security Verantwortlichen/CISO können wir zeitnah mit dem Kunden auf neue Bedrohungen reagieren oder rechtzeitig vorsorgen.

Wie sehen Sie die zukünftige Entwicklung des Marktes für Cybersicherheitslösungen? Welche neuen Technologien oder Trends könnten in den kommenden Jahren eine bedeutende Rolle spielen?

MICHAEL GANZWOHL: Am Grundkonzept wird sich eher weniger ändern. Die Neuheiten findet man in den Details und hier sehen wir auch in Zukunft oft wichtige Verschiebungen. Am besten lässt es sich anhand eines Beispiels erklären: Phishing. Wie Phishing verteilt wird, welche Ziele es verfolgt und was man benötigt, um sich zu schützen bleibt auch in Zukunft ungefähr gleich. Jedoch sehen wir gesteigerte Effizienz und Überzeugungskraft aufgrund von der Nutzung von KI. Anfangs nur zum Verfassen der Texte, doch schon seit einiger Zeit auch um Stimmen nahestehender Personen zu nutzen, um diesen per Voice Message noch einmal besser zu überzeugen. Der Markt wird auf solche Themen natürlich reagieren und entsprechend werden Phishing Filter dann auch in ihren Fähigkeiten erweitert. Aktuell sehen wir natürlich viele Trends aus den Bereichen KI-basierte Angriffe und tatsächlicher digitaler Kriegsführung. Gleichzeitig sehen wir immer mehr den Trend zum Home-Office. Oft ein eher schwer zu schützender Bereich.

Was zukünftig daher wichtiger wird ist weniger die einzelne Lösung als der korrekte Mix aus unterschiedlichen Lösungen und Herangehensweisen. Frameworks helfen hier sehr bei der vielschichtigen Betrachtung, aber es ist zu empfehlen einen Berater heranzuziehen, um diese individuell an die Gegebenheiten der Firma anzupassen. Da der Aufbau eigener Kompetenz in einer Firma teuer ist wird ein Trend sicherlich auch zum Outsourcing von solchen Kompetenzen führen. Hier kann kosteneffizienter und auch oft besser geholfen werden, da die Ressourcen einfach zentral bereitstehen und Teil des Kerngeschäfts der Sicherheitsfirma ist und nicht eine teure Stabsstelle in der eigenen Firma.

Zusammenfassend, was spricht für CyRiSo?

CHRISTIANA BRUCKNER: Standardisiert aber mit individuellen Anpassungen der Leistungen. Budgetfreundliche Lösungen und Services die unseren Kunden helfen Cybersecurity und Cybercompliance zu meistern. Wir verstehen deren Cyberrisiken und bekommen sie gemeinsam in den Griff. •