Faktor Mensch

Vorausschauende Unternehmensführung bekämpft Compliance-Verstöße, Cybercrime und Wirtschaftskriminalität frühzeitig. Dabei behält sie besser alle relevanten Akteure im Blick.

Die Taktzahl hat sich erhöht, mit der die Medien mittlerweile spektakuläre Fälle von Cybercrime und Wirtschaftskriminalität aufgreifen. Zuletzt fielen prominente Namen wie Wirecard und Greensill, das Ponzi-Schema von Felix Vossen und Bernie Madoff sowie Attacken auf Daten von Outsourcing-Dienstleistern. Die Täterschaft besteht nicht selten aus überzeugenden und charismatischen Persönlichkeiten, die das Vertrauen ihrer Anleger, Aktionäre und Stakeholder aufs Gröbste missbrauchen.

Ereignisse wie diese lassen bei Betroffenen das beklemmende Gefühl zurück, niemandem vertrauen zu können. Die Handlungsfähigkeit der Verantwortlichen ist in Gefahr. Rationale Entscheidungen sind oft nicht mehr möglich. Zu viele Faktoren beeinflussen das Verhalten und lenken somit ab vom effektiven Krisen-Management, das nun unabdingbar ist. Die Folgen sind verheerend.

> „Verletzlichkeit ist bei einem Ereignis rund um Wirtschaftskriminalität und Cybercrime nach wie vor ein Tabu."

Integrität ist ein strategisch wichtiger Wettbewerbsvorteil

Die Agenden dieser Verantwortlichen sind voll von Themen, die neben dem Tagesgeschäft und Ausnahmesituationen höchste Aufmerksamkeit fordern, um wettbewerbsfähig zu bleiben. Für eine verantwortungsvolle Unternehmensführung im Sinne einer nachhaltigen Ausrichtung langfristig erfolgreichen Unternehmertums und somit deren Fortführung ist eine Auseinandersetzung mit der Thematik auf oberster Stufe der Verantwortungsträger zwingend notwendig. Erfolgreiche Unternehmen erkennen, dass die Unternehmensintegrität als strategischer Wettbewerbsvorteil Nr. 1 in Zeiten von Unsicherheiten und Transformation gehandelt wird. Die anderen sind überzeugt oder hoffen zumindest darauf, dass es „nur die anderen" trifft.

Das Thema der Verletzlichkeit bei einem Ereignis aus den Bereichen der Wirtschafts- und Cyber-Kriminalität ist nach wie vor ein Tabu. Wir sehen bei Interaktionen mit unseren Kunden, wie unterstützend es für sämtliche Verantwortungsträger ist, wenn die Thematik offen angesprochen und Maßnahmen implementiert werden. Die Frage ist nicht, *ob* man Opfer eines Angriffs wird, sondern *wann*. Das schwächste Glied in der Kette: der Mensch.

Wie angesprochen, handelt es sich um ein Tabu. Niemand will sich outen, sich im Geschäftspartner, Mitarbeitenden oder Outsourcing Provider geirrt zu haben. Geirrt in einem anderen Menschen. Der Mensch will grundsätzlich vertrauen können. Selbstverständlich gibt es auch hier Unterschiede je nach Kulturkreis. In der DACH-Region ist dieses Verhalten sehr ausgeprägt. Wenn dieses Vertrauen missbraucht wird – unabhängig davon, in welchem Kontext –, geht ein Teil des Urvertrauens verloren. Gestandene CEOs von global tätigen Unternehmen sind davor nicht gefeit, genauso wenig wie der Patron des Familienunternehmens in der dritten Generation.

Je weiter weg ein Thema ist – so auch bei Wirtschafts- und Cyber-Kriminalität – desto höher die Schwelle der Vorstellungskraft, dass so ein gravierendes Ereignis einen selbst treffen könnte. Der Risikohorizont ist in diesem Bereich noch eher wenig ausgereift auf Stufe Verantwortungsträger, und es wird noch einiges an – leider negativen – Erfahrungen notwendig sein, um ein angemessenes Maturitäts-Level zu erlangen, wie dies in anderen Bereichen des Risiko-Managements bereits vorhanden ist und dem Unternehmen einen Mehrwert generiert.

Verdrängen hilft selten

In der Praxis ist die primäre Haltung der Verantwortungsträger oft noch so, dass sie sich nicht als Ziel sehen – weder bei Wirtschaftskriminalität im Sinne von „Fraud" noch bei Cyber-Kriminalität. Man sei zu klein, zu lokal, zu gut geschützt, zu wenig interessant oder zu wenig exponiert. Diese Meinungen zur Thematik – um nicht Ausreden zu sagen – spiegeln wider, was sich die Verantwortlichen einzureden versuchen, um sich dem Risiko nicht stellen zu müssen. Nur: Verdrängen hilft selten.

Und wen soll das Thema nun etwas angehen? Die IT-Verantwortlichen, weil wir vom Territorium Cyber sprechen? Oder

Vertrauensverlust und Verletztlichkeit sind bei Verantwortlichen große Themen nach Compliance-Verstößen oder kriminellen Angriffen.

doch lieber die Compliance-Abteilung? Vielleicht sogar die „Human Resource"-Verantwortlichen oder doch der Einkauf? Der Schutz der Vermögenswerte durch Ereignisse in den Bereichen Wirtschafts- und Cyber-Kriminalität gehört auf höchster Ebene angesiedelt. Es reicht bei Weitem nicht, das Thema ausschließlich in der operativen Verantwortung ansiedeln zu wollen.

Der Aufbau einer resistenten und resilienten Unternehmensintegrität genauso wie deren Verteidigung gehören auf oberster Verantwortungsstufe angesiedelt und sind somit Teile der Unternehmensstrategie. Die strategische Betrachtung ist einer der wichtigsten Erfolgsfaktoren zur Bekämpfung von Wirtschafts- und Cyber-Kriminalität genauso wie die Reaktion darauf im Ereignisfall.

Die Veränderungen in den vergangenen beiden Jahren aufgrund der Corona-Pandemie und der verschärften geopolitischen Lage, welche uns aufzeigt, wie rasch ein Gefüge ins Wanken kommt und wie stark auch Unternehmen abhängig voneinander sind, haben vielen die Augen geöffnet. Studien belegen, wie stark erfolgreiche Cyber-Angriffe zugenommen haben und wohin der Trend geht. Er wird nicht abflachen – im Gegenteil.

Die Unternehmensverantwortlichen tun gut daran, sich diese bereits erhobenen und öffentlich zugänglichen Daten strategisch und operativ zunutze zu machen. Die globale Risikolandschaft hat sich verändert und wird Einfluss auf das individuelle Risikoprofil des jeweiligen Unternehmens haben. Unternehmerische Lösungen sind gefragt.

Sensibilisierung als Initiative zum Start besonders effektiv

Unabhängig von der Größe der Organisation zeigen die Erfahrungswerte aus der Praxis, dass die initiale Maßnahme der Sensibilisierung die effektivste ist. Richtig implementiert kann dadurch der Erfolgsfaktor Mensch in seinem Potenzial genutzt werden, um die Vermögenswerte des Unternehmens zu schützen.

Springer Professional

Risk Management

Timtschenko, F.: Professionelles Sicherheitsmanagement für Unternehmen, Wiesbaden 2021
www.springerprofessional.de/link/19834014

Frahm, G.: Enterprise Risk Management, Wiesbaden 2021
www.springerprofessional.de/link/19538780

Sonja Stirnimann, Expertin im Bereich Governance, Risk und Compliance, unterstützt global Kunden der Structuul AG präventiv und im Ereignisfall. Sie trägt Verantwortung als Verwaltungsrätin börsennotierter und privater Unternehmen. Sie hält einen internationalen Executive MBA in Financial Services & Insurance, ist diplomierte Wirtschaftsprüferin, Certified Fraud Examiner (CFE) und hält das Board of Director Diploma des IMD.