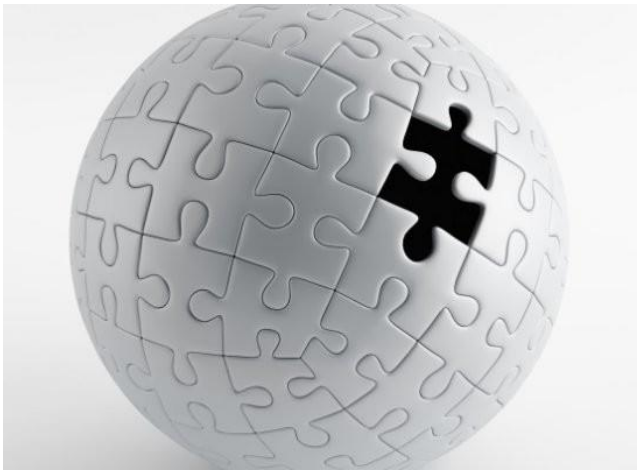
Der „Sicherheitskultur“ deutscher KMUs fehlt es an Awareness, Strategie und Nachhaltigkeit



Kleine und mittelständische Unternehmen (KMUs) sind unverändert ein zentraler Faktor in der deutschen Wirtschaft. Doch ihre „Kronjuwelen“ – ob Produkte oder Dienstleistungen, Daten und Know-how – sind ungenügend geschützt. Das ist das Ergebnis einer **Studie** des **Instituts für Wirtschaftsschutz und Sicherheitsforschung (IWiS)**, Berlin.

Dabei gilt es, das Prädikat „Made in Germany“ nach einem Jahrhundert Erfolgsgeschichte zu verteidigen, denn es ist nach wie vor ein Schlüssel zum Erfolg deutscher Unternehmen im globalen Wettbewerb. Weltweit verbindet man mit „Made in Germany“ technologischen Fortschritt, höchste Qualität und Präzision. Es verwundert daher nicht, dass neue, zukunftsträchtige Technologien, Unternehmens- und Marktstrategien auf so großes Interesse stoßen, dass mancher sich dessen auch auf illegalem Wege zu bemächtigen sucht – seien es staatliche Nachrichtendienste oder ausländische wie inländische Mitbewerber. Die Motive sind vielfältig und reichen vom Wunsch, am Innovationsvorsprung zu partizipieren, bis hin zum Versuch, sich durch Sabotage eines unliebsamen Konkurrenten zu entledigen.

Diesen Gefahren müssen sich nicht nur Konzerne stellen, sondern auch KMUs. Doch wie sieht das in der Praxis aus?

Oft wird dem Mittelstand vorgeworfen, dass es ihm an Strategie fehle – ob für digitale Angelegenheiten, für Kommunikation oder für Einsatzplanung (ERP). Das ist auch für das strategische Thema Unternehmenssicherheit der Fall.

Dabei zeigt sich bei der Gesamtbetrachtung deutlich, dass das Thema Sicherheit bei KMUs nicht unbekannt ist. Dies ist vor allem dem Umstand geschuldet, dass die (gesamtgesellschaftlichen) Gefahren durch Cyberattacken seit drei, vier Jahren einen herausragenden Stellenwert in der medialen Berichterstattung einnehmen. Zugleich verstellt das jedoch den Blick auf andere potenzielle Risiken. Daneben ist das Risikobewusstsein mit Blick auf die unternehmerische Tätigkeit im Mittelstand grundsätzlich vorhanden.

Gleichwohl lässt sich feststellen, dass KMUs der Unternehmenssicherheit nicht oberste Priorität einräumen. Aus der Auswertung wird erkennbar, dass ihr Risikobewusstsein bei Weitem nicht so weit entwickelt ist, wie es bei den meisten Großunternehmen der Fall ist. Viele Probleme werden verharmlost oder gar nicht erkannt und die Risiken daher unterschätzt, auch weil es in den Unternehmen offenbar an der Vorstellungskraft mangelt, sich selbst als potenzielles Opfer für mögliche Angriffe zu sehen.

Eine derart nachlässige Haltung gegenüber den eigenen Produkten und Technologien ist unter rationalen Gesichtspunkten kaum nachvollziehbar. Dass dieses Sich-in-Sicherheit-Wiegen mitunter fatale Folgen hat, belegen die Erkenntnisse staatlicher Sicherheitsbehörden (z. B. Verfassungsschutz der Länder und des Bundes, Bundesamt für Sicherheit in der Informationstechnik), wonach jedes Jahr gerade bei mittelständischen Unternehmen Schäden in Milliardenhöhe entstehen, die durch Wirtschaftsspionage, Sabotage oder Cyberangriffe verursacht werden. Leider wird diese immer wieder genannte Schadenssumme nirgendwo nachvollziehbar belegt.

Das schwache Risikobewusstsein und daher die höhere Risikoakzeptanz führen im Ergebnis dazu, dass das Thema Unternehmenssicherheit nur partiell Niederschlag im betrieblichen Alltag findet. Die Studienergebnisse zeigen, dass die Unternehmen ihre Aufmerksamkeit auf physische/technische (Videoüberwachung, Alarm- und sonstige Notfallanlagen, Zutrittskontrollen etc.) sowie personelle (Wachschutz) Sicherheitsmaßnahmen richten. Zudem wird im IT-Bereich viel Wert auf den Schutz von Netzwerken und der anderweitig elektronischen Kommunikation gelegt. Aber auch hier gibt es teilweise erheblichen Nachholbedarf.

Die von Studienteilnehmern geschilderten Sicherheitsmaßnahmen offenbaren deutliche Schwächen, insbesondere bei der Bewertung und Gewichtung von Gefahrenbereichen, beim Umgang mit Sicherheitsvorfällen und der Kontrolle. Denn es handelt sich nicht um in Prozesse eingebundene und in Konzepten verknüpfte Maßnahmen, sondern um Insellösungen.

In den meisten befragten Unternehmen werden zwar sicherheitsrelevante Informationen verarbeitet und Ziele definiert. Aber in den meisten Fällen gibt es weder Konzepte, Arbeitsgrundlagen, noch Schulungen usw., auf die die jeweils Verantwortlichen als Arbeitsgrundlage zurückgreifen können, um ein Rüstzeug zu haben, wie mit den Ergebnissen zu verfahren ist. Es werden daher intuitiv Einzelfalllösungen gesucht. Zudem werden die Sicherheitsmaßnahmen häufig weder aufeinander noch in Bezug auf andere Unternehmensprozesse abgestimmt. So werden beispielsweise die Gefahren, die im Zusammenhang mit der Nutzung sozialer Netzwerke oder Home-Office-Arbeitsplätzen entstehen, zwar erkannt, aber nicht in vollem Umfang ernst genommen.

Alle Studienteilnehmer halten die vorhandenen Richtlinien hinsichtlich der Nutzung sozialer Netzwerke während der Arbeitszeit für ausreichend, ohne zu kontrollieren, ob diese Richtlinien zur Kenntnis genommen, geschweige denn erfüllt werden. Auffällig ist des Weiteren, dass die Sicherheitsmaßnahmen keine Kontinuität aufweisen und letztlich auch nicht so erklärt werden, dass die Mitarbeiter Notwendigkeit und Funktion verinnerlichen können.

Die Studie zeigt eine häufig fehlende Einbindung des Sicherheits-Managements in die Unternehmensprozesse. Auch was den „Risikofaktor Mitarbeiter“ angeht, besteht in vielen Unternehmen Nachholbedarf. Seitens der befragten Unternehmen besteht eine sehr geringe Risikowahrnehmung gegenüber den eigenen Beschäftigten. Die Studienergebnisse zeigen, dass technische Sicherheitsmaßnahmen eher im Fokus stehen als Maßnahmen gegen Mitarbeiterkriminalität. Das „gute Betriebsklima“ und das Vertrauensverhältnis zwischen Mitarbeiter und Unternehmensführung gelten als Allheilmittel, das weitere Anstrengungen unnötig macht.

Die Notwendigkeit und Effizienz von Schulungen und Trainings für das Personal wurden bei der Befragung zur Studie zwar nicht bestritten und von allen Studienteilnehmern auch für

nützlich gehalten, aber sie führten es nur sehr selten von sich aus an. Nach Aussagen der Studienteilnehmer werden solche Maßnahmen mangels Ressourcen häufig verschoben oder ganz gestrichen.

Das mangelhafte oder inkonsequente Personalmanagement unter Sicherheitsaspekten ist eine gravierende Sicherheitslücke der Unternehmen und deutet darauf hin, dass die damit verbundenen Risiken kaum beherrscht werden. Verkannt und zum Teil auch verdrängt wird, dass Schäden auf Grund technischer Ausfälle oder Defekte seltener sind als die durch menschliches Verhalten verursachten Schäden.

Der Psychologe Jens Hoffmann warnt in einem Interview mit der Wochenschrift *Die Zeit* vor Psychopathen, die es überdurchschnittlich oft schaffen, in Führungspositionen aufzusteigen. Hoffmann konstatiert: „Sie denken nicht an das Unternehmen, sondern handeln nur in ihrem eigenen Interesse. Sie haben Spaß an Dominanz und Kontrolle. Sie demütigen gern andere und mögen es oftmals auch, wenn andere Angst vor ihnen haben. Selbst haben sie keine Angst. Gerade das macht sie in Führungspositionen gefährlich, denn sie treffen oft hochriskante Entscheidungen, die ein Unternehmen in den Ruin treiben können."

Im Ergebnis kann selbst die beste Sicherheitstechnik nicht vor Risiken schützen, wenn die Mitarbeiter sensible Unternehmensdaten anderweitig nutzen, kritische Unternehmensstrukturen angreifen oder Prozesslücken ausnutzen. Wenn die Unternehmen weiterhin auf ihre Fähigkeit vertrauen, im Notfall schnell und situationsabhängig zu reagieren, ist zu befürchten, dass viele kleinere Angriffe und Fehlleistungen gar nicht bemerkt werden. Legt man zudem die Aussagen der befragten Führungskräfte zu Grunde, wonach die – nicht nur durch das Personal verursachten – Reputationsverluste schlimmere Auswirkungen für das Unternehmen haben können als die Produktions- und Lieferausfälle, so muss das Unternehmen gerade an diesem Punkt ansetzen statt ihn zu vernachlässigen. Ein sicherheitsbezogenes Personalmanagement ist somit ein Thema, mit dem sich KMUs unbedingt auseinandersetzen müssen.

Angesichts des festgestellten Missverhältnisses zwischen realer Bedrohung und Risikobewusstsein ist es nicht überraschend, dass eine lediglich geminderte Einsicht in die Notwendigkeit von (präventiven) Sicherheitsmaßnahmen besteht. Nach Aussagen der befragten Sicherheitsexperten wird die Unternehmenssicherheit meistens nicht als Teil der Wertschöpfung betrachtet. Aus Sicht vor allem der Geschäftsführer unter den Befragten besteht kein direkter Zusammenhang zwischen der Sicherheit einerseits und der wirtschaftlichen Leistung des Unternehmens andererseits, sodass die Sicherheitsaspekte im Vergleich zu Organisation und Strategie lediglich eine Nebenrolle spielen.

Sicherheitsmaßnahmen werden als zusätzlicher, aber nicht notwendiger Kostenfaktor angesehen. Es entstehen daher häufig Spannungen bei der Verteilung von personellen und finanziellen Ressourcen, die bei mittelständischen Unternehmen oft ohnehin sehr begrenzt sind. Die meisten Unternehmen zögern daher mit dem Aufbau eines Sicherheitssystems, das alle Unternehmensprozesse umfasst. Dabei wird verkannt, dass die meisten Sicherheitsprozesse in die bereits vorhandenen Unternehmensprozesse integriert werden können und müssen, sodass ein Sicherheitssystem auch für ein mittelständisches Unternehmen nicht zwangsläufig hohe zusätzliche Investitionen nach sich ziehen muss. Um nur ein Beispiel zu geben: Das Ortungssystem GPS kann zur Diebstahlssicherung für den Fuhrpark eingesetzt

werden oder zur Kontrolle, dass die Fahrzeuge auftragsgemäß eingesetzt werden; es kann aber auch einem modernen Flottenmanagement dienen.

Grundsätzlich lässt sich eine gewisse „Hilflosigkeit“ und fatalistische Grundhaltung gegenüber der Unternehmenssicherheit feststellen. Selbst wenn sich die Verantwortlichen Gedanken dazu machen, wissen sie nicht recht, an wen sie sich wenden sollen. Externe Beratung gilt – meist ohne empirische Grundlage – als zu teuer, den Kontakt zur Polizei scheut man, so lange nichts passiert ist, und Sicherheitsverbände sind weitgehend unbekannt. Und die mediale Berichterstattung über Sicherheitsvorfälle steigert meist nicht den Willen zur Abwehr, sondern lässt Fatalismus aufkommen: Wenn es der Weltkonzern nicht schafft, seine Kundendaten zu schützen, was kann der kleine Mittelständler schon ausrichten?

Im Ganzen ist zu konstatieren, dass von einer „Sicherheitskultur“ im Sinne von Belyová und Banse bei den allermeisten befragten KMUs nicht die Rede sein kann. Mag auch die theoretische Ebene in Form von Regeln und Anweisungen ansatzweise vorhanden sein, so sucht man die praktische vielfach vergebens. Der Grund liegt im fehlenden Risikobewusstsein sowohl auf der Führungsebene als auch in der Belegschaft. Damit fehlt die Erfüllung der wichtigsten Anforderung an eine Sicherheitskultur, nämlich, dass deren Notwendigkeit von allen Mitgliedern der Organisation akzeptiert wird, dass an deren Gestaltung alle Mitglieder mitwirken und dass sie permanent aufrechterhalten und verbessert wird. Es ist daher schon als „sicherheitssensibel“ zu betrachten, wer Sicherheitsmaßnahmen zumindest als Insellösung implementiert.

Die KMU-„Sicherheitskultur“ lässt sich am besten mit der Schlussbemerkung im Interview von Trigema-Geschäftsführers Wolfgang Grupp zur Unternehmenssicherheit zusammenfassen: „Wir machen das, was normal ist. Zudem ist es meine tägliche Aufgabe, die kleinen Probleme zu lösen, und nicht, mir große auszudenken, die gar nicht kommen!“

– veröffentlicht von Hans-Günter Laukat –

Bezug der Studie über: www.iwis-institut.de