Sicherheit und kontrollierter Informationsabfluss

Eine wenig beachtete Symbiose

Gebäudeschutz, Reisesicherheit, Perimeterschutz sind alles Stichworte, die sofort mit Security oder Corporate Security in Verbindung gebracht werden. Kontrollierter Informationsabfluss jedoch nicht – hört sich auch erstmal nicht sexy an. Was ist kontrollierter Informationsabfluss und was er mit Unternehmenssicherheit zu tun.

In den frühen 90er Jahren plante Johnson Controls die Einführung einer neuen Generation von Gebäudemanagementsystemen, computergestützte Systeme zur Steuerung von Heizung, Sicherheit und anderen Funktionen in Gebäuden. Der Entwicklungsprozess war unter großer Geheimhaltung durchgeführt worden, aber die Produkte mussten schließlich mit potenziellen Kunden getestet werden. Genau hier war die Gefahr groß, dass vertrauliche Produktdetails den Weg zur Konkurrenz finden.

Die Entwicklung von Johnson trug den Codenamen „Loba", nach dem russischen Mathematiker Nikolai Lobachevski aus dem 19. Jahrhundert. Johnson hielt im Markt Augen und Ohren offen, ob ihre Neuentwicklung eventuell durchgesickert war. Und in der Tat, einer der Hauptkonkurrenten, hatte ein Gerücht über Johnsons Neuentwicklung eines revolutionären Gebäudemanagementsystems gehört. Klar, der Wettbewerber hielt die eigenen Verkaufsmitarbeiter dazu an, möglichst viele, nützliche Informationen darüber im Markt einzuholen. Typische Quellen dafür: Kunden, Interessenten, Lieferanten, Analys-

ten. Für Johnson lag die Gefahr auf der Hand, würde der Wettbewerb frühzeitig genug über das Produkt erfahren, könnte die Markteinführung torpediert werden. Anstatt nun hektisch den Starttermin vorzuziehen, beschloss Johnson, sich Zeit zu erkaufen, indem es den neugierigen Konkurrenten von der Spur abbrachte. Hilfreich war dabei, dass Johnson wusste, dass dieser einen falschen Projetcodenamen erfahren hatte, nämlich „Lobo". Also beschloss man, die bereits geplante Einführung einer kleinen Aktualisierung eines anderen Produktes „Projekt Lobo" zu taufen.

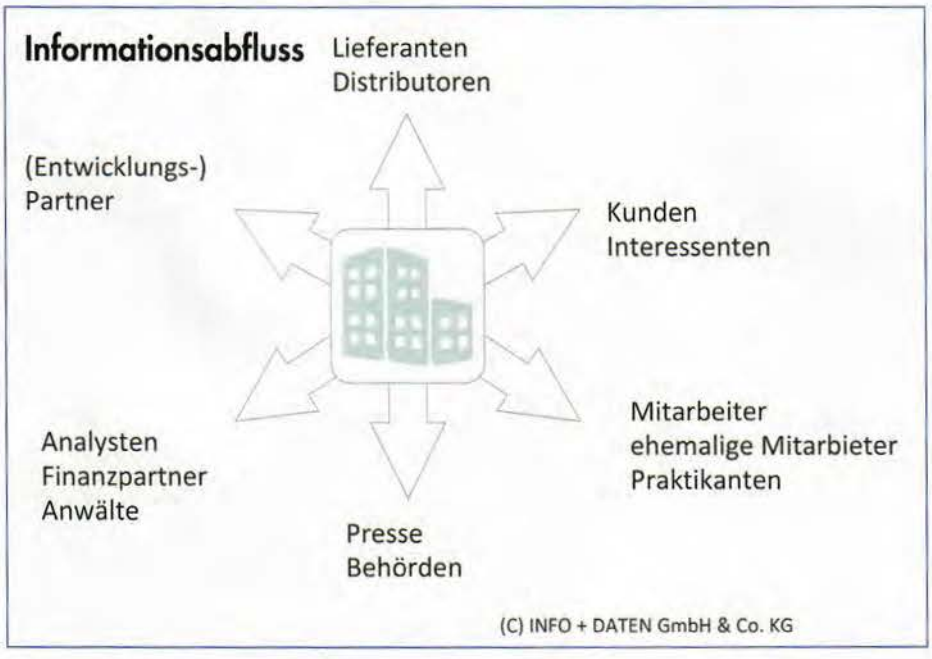
Kontrollierter Informationsabfluss ist sexy

Was als kleine Produktveröffentlichung gedacht war, wurde nun mit einer umfassenden PR-Kampagne in der Fachpresse auf eine große neue Produkteinführung aufgerüstet. Das Produkt wurde „Logical Option for Building Operation" System oder kurz „Lobo" genannt. Die veröffentlichten Informationen waren korrekt und haben weder Kunden, Partner noch Marktexperten verwirrt und reichten auch aus, den alarmierten Konkurrenten davon zu überzeugen, dass es sich um das Projekt handelte, von dem er als Gerücht erfahren hatte. In der Folge stoppte dieser die Bemühungen, mehr Informationen und Details zu diesem Gerücht zu sammeln. Johnson hatte sich Zeit gekauft. Die Markteinführung des echten Loba-Produkts wurde zu einem späteren Zeitpunkt erfolgreich durchgeführt und mit dem geplanten Überraschungseffekt auf den Markt gebracht – ganz so, wie es Johnson sich erhofft hatte.

Dieser Fall ist eines der seltenen veröffentlichten Beispiele, das sehr gut illustriert, wie sexy kontrollierter Informationsabfluss ist, weil es wirkungsvoll die Zielerreichung eines Unternehmens unterstützt. Es wird dem informierten Leser aber auch klar, dass die Linie zwischen Verteidigung und Täuschung sehr dünn ist. Aus diesem Grund ist die kompromisslose Abwägung zu Gunsten des Reputationsschutzes unabdingbar. Wer möchte schon als „Betrüger" wahrgenommen werden.
Nichtsdestotrotz gehören defensive Maßnahmen für umfassenden Schutz in das Tool-Kit eines jeden Unternehmens und nicht nur als opportunistisches Werkzeug, sondern als strategisches. Damit sind nicht nur herkömmliche Schutzmaßnahmen gemeint, sondern vor allem die Maßnahmen, die den Schutz von proprietärem Know-How sicherstellen. Diese sollten in jeder Situation genutzt werden, in der es entweder wesentlich oder sogar nur nützlich ist, Wettbewerber und andere Opponenten unwissend darüber zu halten, was wirklich geplant wird und deren Aktivitäten zur Informationsgewinnung fehlzuleiten und nutzlos zu machen. Und es gibt viele feindliche Akteure.

Gefahren kommen aus vielen Richtungen

Ein Unternehmen verliert auf vielfältige Weise kontinuierlich Informationen wie das Schaubild „Informationsabfluss" verdeutlicht. Es lässt sich nicht vermeiden. Die Kommunikation mit der unternehmensnahen Umwelt bedarf auch dieses Informationsflusses, der allerdings kontrolliert sein sollte.



An diesen abfließenden Informationen und weiteren Interna sind alle Widersacher brennend interessiert. Nicht nur Wettbewerber, sondern auch Staaten, radikale Interessengruppen, Gewerkschaften, oder Head Hunter. Eine weitere Gruppe von Widersachern mit möglicherweise feindseliger Gesinnung sind Banken, Due Diligence Spezialisten, Unternehmensberatungen, Wettbewerbsbehörden, Presse und Journalisten, Investmentfirmen, Behörden, Konsumentenschützer und -verbände. All diese Akteure versuchen, nicht immer mit bösen Absichten, interne Informationen über die Geschäftsaktivitäten eines Unternehmens zu gewinnen.
Fakt ist, dass nicht alle Informationen in einem Unternehmen gleichwertig geschützt sind. Und das führt zu einer Sicherheitslücke (Internal Security Gap), die dringend adressiert werden muss. Der Sicherheitsmarkt wird von einem Fokus auf Cyber-, physische und IT-Sicherheit getrieben, um den Betrieb eines Unternehmens zu sichern. Dies ist jedoch eine sehr eingeschränkte Sicht auf die Sicherheit. Der schwächste Teil der Unternehmensverteidigung ist und bleibt der Arbeitnehmer, der Angestellte, der Mensch. Trotz der viel diskutierten und veröffentlichten Bedrohung durch CEO Fraud funktioniert dieser bösartige Angriff immer noch. Warum? Menschen scheitern. Letztendlich besteht immer noch ein Bewusstseinsdefizit für die Bandbreite an Bedrohungen. Zudem gilt: Informationsbeschaffung erfordert nicht unbedingt den Einsatz von Technologie. Gespräche mit Menschen reichen oft aus, um vertrauliche Informationen über Organisationsstrategien und -pläne wie auch anderes proprietäres Know-How zu erhalten. Gleichzeitig fehlt es vielen Organisationen an einem strukturierten und stringenten Ansatz, um selbst Informationen über den Markt und die wichtigsten Wettbewerber zu sammeln. Einige Unternehmen brillieren, die meisten jedoch nicht. Auch hier fehlt es oft auf der Führungsebene an der Erkenntnis, dass und wie ein strukturierter Ansatz der Informationsgewinnung nicht nur der Strategie eines Unternehmens, sondern auch dessen operativen Tätigkeiten und der Sicherheit zugutekommt.

Nicht nur im Wettbewerb ist die Informationshoheit entscheidend für Erfolg

Wettbewerb wird weithin als ein offensiver Prozess wahrgenommen, bei dem Vorteile gesucht und indem überlegene Ressourcen

Udo Hohlfeld, Geschäftsführer der INFO + DATEN ist spezialisierter Anbieter von offensiven und defensiven Intelligence-Leistungen. 2019 gründete Herr Hohlfeld mit Partnern aus den USA, Russland und GB die Counter Force Group, eine globale Allianz für Corporate Counter-intelligence Services.

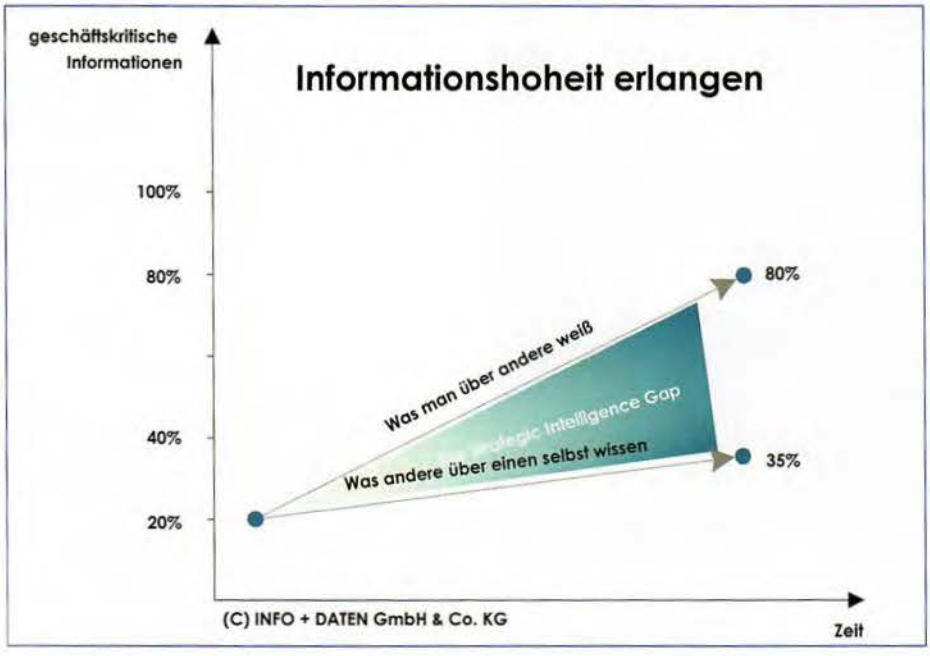
eingesetzt werden. Ein wesentliches Element für Erfolg im Wettbewerb ist der Überraschungseffekt. Für die Unternehmenssicherheit ist es die Voraussicht auf Lageentwicklungen. Für beides benötigt es Informationen, zuverlässig und zur richtigen Zeit. Quintessenz: erreichte Informationshoheit mündet in erhöhte Wettbewerbsfähigkeit und Resilienz gegen Gefahren.

Um diese Informationshoheit zu erlangen, sind zwei Komponenten unerlässlich: die eine ist, bestens über das Unternehmensumfeld wie auch den Markt und alle Marktteilnehmer mit einem Interesse am Unternehmen Bescheid zu wissen (Offensive Intelligence); die zweite ist, seine eigenen Aktivitäten vor anderen bestmöglich zu verbergen (Protective Intelligence). Kann ein Unternehmen beides umsetzen, dann hat es die Informationshoheit und kann den erreichten Wissensvorsprung (The Strategic Intelligence Gap) für seinen strategischen Vorteil nutzen, wie die folgende Grafik „Informationshoheit" veranschaulicht.

Die Informationshoheit wird also erreicht über aktive Informationsgewinnung (Offensive Intelligence) darunter fällt u.a. Market Intelligence, Competitive Intelligence, Patent Intelligence, und über aktiven Informationsschutz (Protective Intelligence) wie Patente, Intellectual Property oder IT-Security aber auch der klassischen Sicherheit. Letzteres schützt allerdings oft nur die offensichtlichen Güter und Werte und es gibt dedizierte Abteilungen und Mitarbeiter für die Umsetzung. Das proprietäre Know-How wird hier nicht mitabgedeckt und eine verantwortliche Stelle gibt es dafür ebenfalls nicht.

Schutz von proprietärem Know-How

Nur wenn ein Unternehmen weiß, wer an seinen geschäftskritischen Informationen interessiert ist, und welche Ressourcen er zur Verfügung hat, diese Informationen zu erlangen, kann sich bzw. sein proprietäres Know-How effektiv schützen.



Wo findet sich proprietäres Know-How in einer Organisation? Die folgende Liste ist nicht komplett, zeigt aber die wichtigsten Kategorien wie

- Neue Produkteinführungen
- Produktmodifikationen
- Neue Preisstrategien
- Neue Servicerichtlinien
- Eintritt in neue georgraphische Märkte
- Personelle und organisatorische Veränderungen

Die Arbeit in all diesen Kategorien, kann sich monate-, wenn nicht jahrelang in der Planungsphase befinden. Während dieses Zeitraums besteht die stete Gefahr, dass Informationen über die Initiativen an Wettbewerber weitergegeben oder von anderen Akteuren abgegriffen werden. In dieser Situation ist es eindeutig von Vorteil, geschützt und vorbereitet zu sein für den Fall der Fälle. Leider haben Organisationen dafür keine geeigneten Prozesse und Kapazitäten definiert. Dabei wäre es sehr einfach und beruhigend, diese zu etablieren. Maßnahmen im Bereich der Protective Intelligence sichern hier Investitionen, Ressourcen und Know-How, welche den zukünftigen Unternehmenserfolg sicherstellen sollen. Es lohnt sich also, darüber nachzudenken, welche Informationen aus dem Unternehmen abfließen und wie dieser Prozess am besten kontrolliert werden kann.