Zeitschrift: Schweizer Soldat : die führende Militärzeitschrift der Schweiz
Herausgeber: Verlagsgenossenschaft Schweizer Soldat
Band: 84 (2009)
Heft: 7-8

Artikel: Nachrichten in Unternehmen
Autor: Stoll, Bernhard / Schuppisser, Stefan
DOI: https://doi.org/10.5169/seals-717265

Nachrichten in Unternehmen

«Keine Überraschungen!»: Wie Sie mit Competitive Intelligence und Abwehr Ihr Management dabei unterstützen.

OBERST I GST BERNHARD STOLL UND MAJOR STEFAN SCHUPPISSER

Kein militärischer Kommandant kann bei der Planung und Durchführung seiner Auftragserfüllung auf den Nachrichtendienst und dessen «Intelligence» verzichten. Dies trifft im übertragenen Sinn auch auf jeden Firmenchef zu.

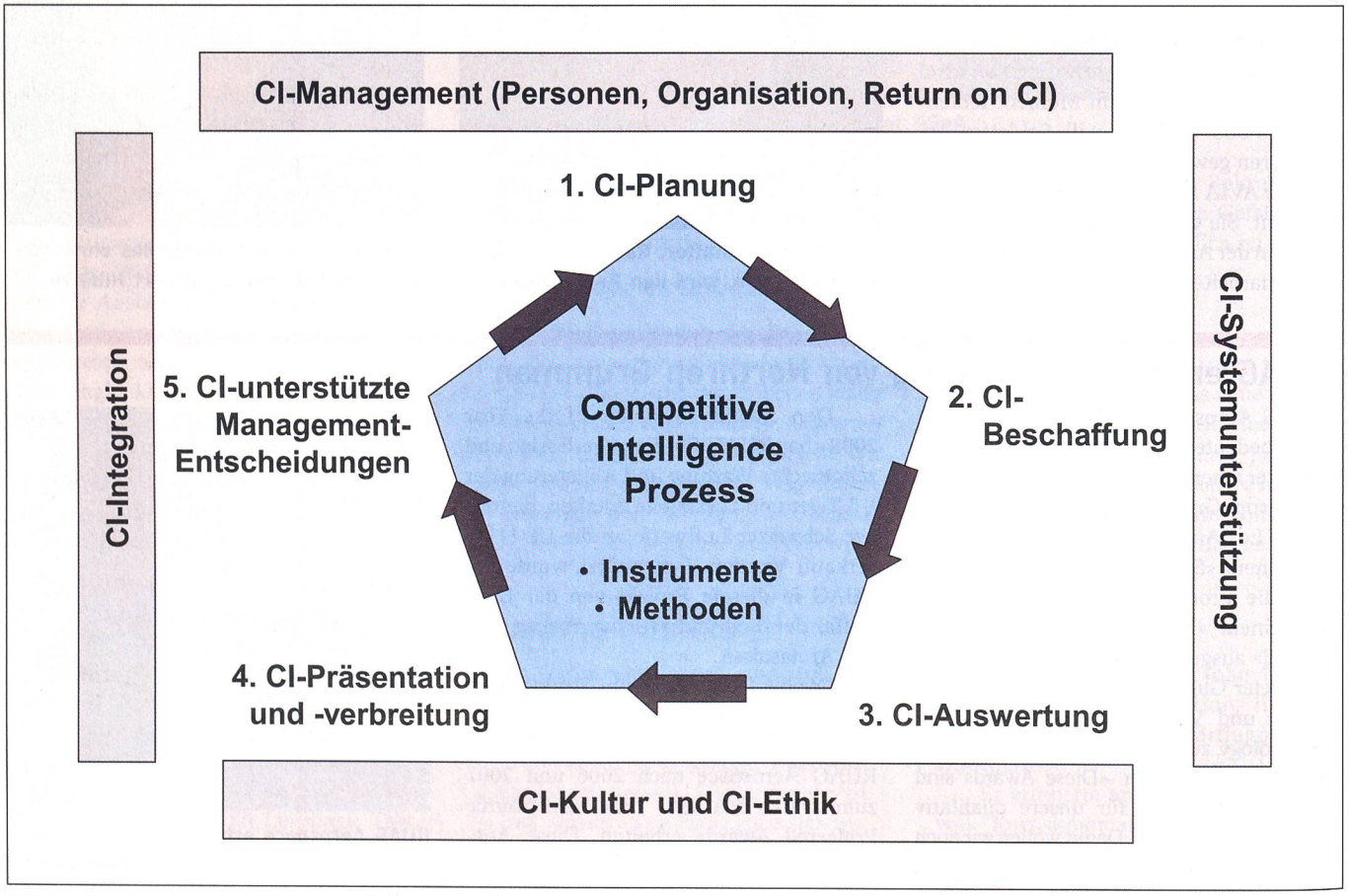
Competitive Intelligence

Nicht nur im militärischen, sondern auch im unternehmerischen Umfeld will man Überraschungen vermeiden. Die plötzliche Senkung von Preisen, die unerwartete Einführung einer neuen Technologie durch einen engen Konkurrenten oder der überraschende Markteintritt eines neuen Wettbewerbers können zur Folge haben, dass Umsätze kurz- und mittelfristig verloren gehen, die eigene Reputation im Markt und bei den Kunden leidet und letztlich die Wettbewerbsfähigkeit beeinträchtigt wird oder gar verloren geht.

Um sich gegen solche Überraschungen zu wappnen, haben Unternehmen seit einigen Jahren begonnen, sogenannte Competitive Intelligence-Fähigkeiten aufzubauen und zu professionalisieren. Als unternehmerische Aktivität umfasst der Begriff Competitive Intelligence (CI) den Betrieb eines umfassenden Programms zur kontinuierlichen Beobachtung und Beurteilung von Verhaltensweisen von Konkurrenten sowie von Umwelt-, Branchen- und Marktentwicklungen. Ziel dabei ist, Verantwortungträgern in Organisationen fundiertere und rechtzeitige Entscheidungen und Handlungen zu ermöglichen. Mit dem Begriff Competitive Intelligence wird zugleich auch das Ergebnis bezeichnet, nämlich das im Zuge der CI-Aktivität aus fragmentierten Einzelinformationen erarbeitete Wissen über Umweltentwicklungen und Konkurrenten.

Schlüsselelemente

Es gibt kaum ein Unternehmen, das nicht in der einen oder anderen Form CI betreibt. Umfragen beweisen, dass noch relativ wenige Unternehmen CI systematisch eingeführt haben. Im Zentrum eines CI-Programms steht der aus fünf Schritten bestehende CI-Prozess (siehe Abbildung).



Die Grafik gibt einen umfassenden Überblick über das Nachrichten-Management.

– *CI-Planung:* Für den zielgerichteten Ressourceneinsatz muss in Schritt 1 mit dem Management herausgearbeitet werden, mit welchem Ziel der CI-Prozess in Gang gesetzt werden soll. Im Fokus steht zu definieren, welche wettbewerbsrelevanten Entscheidungen mit CI unterstützt werden sollen. Geht es im Sinne einer Frühwarnung um das frühzeitige Erkennen sich abzeichnender Chancen, Gefahren und Trends im Unternehmensumfeld? Liegt der Hauptfokus auf der Beobachtung/Überwachung von Konkurrenten? Will das Management die Robustheit eigener Strategien einem «Realitätscheck» unterziehen und mögliche Reaktionen von Konkurrenz und Umfeld simulieren? Resultat der Phase der CI-Planung sind die sogenannten Key Intelligence Topics (KIT).

– *CI-Beschaffung:* Liegen die KIT vor, muss in Schritt 2 die CI-Beschaffung definiert werden. Über welche Quellen und Sensoren können zu welchen KIT relevante Einzelinformationen gewonnen werden? Die Beschaffung basiert idealerweise auf einem losen aber zielgerichteten CI-Netzwerk von internen und externen Personen, die aufgrund ihrer primären Aufgaben, z.B. im Vertrieb, relevante Informationen in den CI-Prozess einspeisen können. Informationsspezialisten oder Datenbanken ergänzen die CI-Beschaffung. Neben dem zeit- und kostenmässigen Beschaffungsaufwand ist unter Risiko-Aspekten auch die Einhaltung rechtlicher und auch ethischer Grundsätze zu berücksichtigen.

– *CI-Auswertung:* Die zahlreichen und z.T. widersprüchlichen Einzelinformationen sind dann in Schritt 3 auszuwerten, indem sie nach einer Bewertung bezüglich Aussagekraft und Zuverlässigkeit zueinander in Beziehung gesetzt werden und wie Mosaiksteinchen zu einem Gesamtbild zusammengesetzt werden. Wichtig ist dabei, dass die Auswertung erst als abgeschlossen betrachtet werden kann, wenn neben den beobachteten Entwicklungen auch fundierte Handlungsempfehlungen und mögliche Konsequenzen zu Handen der Entscheidungsträger formuliert worden sind.

– *CI-Präsentation und -verbreitung:* In Schritt 4 ist die Herausforderung, die CI-Ergebnisse den Entscheidungsträgern auf verschiedenen Stufen in einer adressatengerechten Form zur Kenntnis zu bringen. Persönliche Briefings, E-Mail-Alerts, Newsletters oder CI-Reports sind dafür mögliche Formen.

– *CI-unterstützte Management-Entscheidungen:* Die Aktivitäten in den Schritten 1 bis 4 erfolgen vergeblich, wenn die CI-Ergebnisse bei den getroffenen Management-Entscheidungen nicht auch wirklich berücksichtigt werden. Um dies zu begünstigen, muss als Spielregel im CI-Prozess eingeführt werden, dass zu jeder aus dem CI-Prozess resultierenden Empfehlung jeweils festgehalten wird, was die Entscheidungsträger damit anfangen.

Zielgerichtet arbeiten

Hier sind Antworten möglich von «Gesehen, aber keine unmittelbare Bedeutung» über «Muss im Rahmen des CI-Prozesses weiter beobachtet werden» bis hin zu «Löst unmittelbare Änderungen im Bereich ... aus». Aus diesen Stellungnahmen resultieren mit grosser Wahrscheinlichkeit neue Fragestellungen, die zu neuen Key Intelligence Topics führen. Der CI-Prozess schliesst sich und beginnt erneut zu laufen.

Der Einsatz verschiedener CI-Instrumente und -Methoden hilft in den einzelnen Schritten zielgerichtet zu arbeiten. Es gilt aus einer grossen Vielfalt jene auszuwählen und bedarfsgerecht anzupassen, die am besten zur Zielsetzung passen. Die Instrumente und Methoden können dabei von einfachen Kreuztabellen zur Darstellung von KIT und Quellen-Informationen über quantitative Finanzanalysen bis hin zu aufwendigen Simulationen (Business War Gaming) reichen.

Alles integrieren

Je professioneller ein Unternehmen CI betreibt, desto mehr macht es sich auch Gedanken darüber, wie der CI-Prozess unterstützt und in das gesamte Unternehmensgeschehen integriert werden kann:

– *CI-Management:* Ein CI-Prozess kann nur zum Laufen kommen, wenn geregelt ist, wer darin genau welche Aufgaben, Verantwortlichkeiten und Kompetenzen hat. Dies ist vor allem wichtig, wenn es – wie gerade in kleineren Unternehmen häufig der Fall ist – keine eigentliche CI-Stelle gibt. Minimal sollte jemand als CI-Manager bezeichnet sein und die Koordination in einem Teilpensum übernehmen. Der CI-Manager ist Dreh- und Angelpunkt des CI-Programms und für die Gestaltung und Steuerung des CI-Prozesses, die Pflege der KIT, den Aufbau und die Betreuung des CI-Netzwerks, die Ausbildung usw. verantwortlich. Zu seinem Aufgabenbereich gehört auch die Kosten- und die Nutzenseite des CI-Programms zu überblicken und für einen optimalen «Return on Competitive Intelligence» zu sorgen.

– *CI-Systemunterstützung:* Je mehr interne Auftraggeber und Nutzer der CI-Prozess im Unternehmen hat und je umfassender das CI-Netzwerk ist, desto sinnvoller ist es, sich über eine IT-Unterstützung des CI-Prozesses Gedanken zu machen. Sie kann z.B. die dezentrale Datenerfassung durch Personen im CI-Netzwerk erleichtern, die Verarbeitung quantitativer Informationen automatisieren oder die Verbreitung von CI-Ergebnissen beschleunigen und adressatengerechter machen. Web-2.0-Anwendungen werden hier zur Zeit intensiv diskutiert. Die Herausforderung ist aus einer bereits beträchtlichen Zahl von CI-Software-Angeboten, das richtige auszuwählen.

– *CI-Kultur und CI-Ethik:* Im Idealfall ist jeder Mitarbeitende des eigenen Unternehmens ein Sensor, der Informationen beschafft und in das Unternehmen hineinträgt. Konkurrenz- und Zukunftsorientierung als in der Unternehmenskultur verankerte Einstellungen begünstigen die CI-Aktivitäten. Gleichzeitig sollte aber auch daraufhin gearbeitet werden, dass allen klar ist, wo die rechtlichen und ethi-

Was heisst ASIS?

Die American Society for Industrial Security ASIS ist mit ihren 36 000 Mitgliedern der weltweit grösste Zusammenschluss von Sicherheitsexperten.

Er dient dem Erfahrungsaustausch, der Fortbildung, den Qualifikationen und der Wahrnehmung der Verantwortung im Umfeld der Sicherheitsfragen. Wissenstransfer, Kontakte, Gedankenaustausch und Networking vor Ort, prägen auch die Arbeit des seit 25 Jahren bestehenden Schweizer Chapters. Im Internet:
www.asisonline.org (international)
www.asisonline.ch (Chapter 160 Schweiz)

Was ist SCIA/SCIP?

Die Swiss Competitive Intelligence Association (SCIA) ist eine schweizerische Vereinigung. Sie hat zum Ziel, die Ausbildung und Problemlösung in der strategischen Wettbewerbsanalyse zu fördern. Sie engagiert sich für einen hohen Qualitätsstandard und die Effizienz von Competitive Intelligence. Im Internet: *www.swisscia.org.*

Die Society of Competitive Intelligence Professionals (SCIP) ist als globale Berufsorganisation bestrebt, höchsten Ansprüchen gerecht zu werden. Im Internet: *www.scip.org*

schen Grenzen z.B. bei der Beschaffung von Konkurrenz-Informationen (z.B. bezüglich Geschäftsgeheimnissen) liegen. Die Berufsorganisation «Society of Competitive Intelligence Professionals (SCIP)» (vgl. Kasten) hat dazu einen Berufskodex erlassen, der die ethisch nicht vertretbaren Praktiken aufzählt. Im Sinne eines Risikomanagements tut jedes Unternehmen gut daran, die eigene Reputation zu schützen und für die Einhaltung dieses Kodex zu sorgen.

– *CI-Integration:* Erfolgreiche Betreiber von CI sorgen nicht nur dafür, dass der CI-Prozess für sich in Schwung kommt und bleibt, sondern beginnen den CI-Prozess auch gezielt mit den anderen Prozessen zu integrieren. Sie überlassen es z.B. nicht dem Zufall, ob die Verantwortlichen des Produktentwicklungsprozesses ihre Arbeit unter Berücksichtigung von CI-Ergebnissen aufnehmen, sondern zeigen konkret auf in welcher Phase CI-Informationen einfliessen müssen. Solche inhaltlichen und zeitlichen Verzahnungen sind auch bezüglich anderer Prozesse nötig, wie z.B. Strategieüberprüfung und –entwicklung, Forschung und Entwicklung, Marketing und Vertrieb, Produktion, Personalgewinnung usw.

Wer beginnt sich mit der Einführung eines CI-Programms zu beschäftigen, wird bald merken, dass CI ja nicht nur eine Einbahnstrasse ist – auch die Konkurrenten betreiben allenfalls CI und versuchen das eigene Unternehmen und seine Strategien aufzuklären! Dabei kann nicht immer davon ausgegangen werden, dass nur rechtlich und ethisch vertretbare Praktiken zum Einsatz kommen.

Im Gegensatz zu Competitive Intelligence beinhaltet der Begriff Spionage illegale Tätigkeiten zur Erlangung von Informationen wie z.B. Nötigung, Erpressung, Diebstahl, Einbruch, Verstösse gegen das Fernmeldegesetz, das Gesetz gegen den unlauteren Wettbewerb oder Persönlichkeitsverletzungen. Konkurrenzspionage geht von privaten Unternehmen aus und befasst sich mit den jeweiligen Konkurrenten. In der Wirtschaftsspionage lenken oder unterstützen staatliche Stellen die Ausforschungstätigkeit von Konkurrenten, um einheimischen Unternehmen Wettbewerbsvorteile zu verschaffen. Die Methoden der Spionage sind im Laufe der Jahre im Zusammenhang mit den rasanten technologischen Entwicklungen raffinierter und effektiver geworden.

Gefahren und Akteure

Spionage und Competitive Intelligence bedrohen schutzwürdige Informationen von Unternehmen. Darunter fallen beispielsweise Spitzentechnologien, Unternehmens-, Markt- und Absatzstrategien, Produkte und Produktentwicklungen. Akteure sind – neben den Konkurrenten – staatliche Stellen, Hacker, die Medien und auch eigene Mitarbeiter. Eigene Mitarbeiter können von sich aus aktiv werden, von der Konkurrenz eingeschleust oder angeworben worden sein oder aus Angeberei oder fahrlässig Informationen abfliessen lassen.

Im Bericht 2007 über die Innere Sicherheit der Schweiz findet man interessanterweise kaum Angaben über die Aktivitäten staatlicher Akteure in der Schweiz. Schaut man jedoch in entsprechende ausländische Berichte werden konkret Staaten wie beispielsweise China, Russland, Indien

genannt. Gleichzeitig wird darauf hingewiesen, dass sich auch westliche Industrienationen ihrer Nachrichtendienste bedienen, um ihrer eigenen Wirtschaft Wettbewerbsvorteile zu verschaffen.

Die moderne Informations- und Kommunikationstechnik schafft laufend neue Risiken. Internet, Telekommunikationsanlagen, drahtlose Verbindungen wie WLAN-Technologie, Bluetooth-Schnittstellen und Mobiltelefone sowie mobile Endgeräte wie Laptops, Personal Digital Assistants und USB-Sticks können es Unbefugten erlauben, sich Zugang zu schutzwürdigen Informationen zu verschaffen. Ebenso stellen elektronische Attacken auf Computernetze eine Gefahr dar. Daher sollte sich ein Unternehmen systematisch Gedanken über Counterintelligence machen.

Counterintelligence

Auf der Basis einer seriösen Risikoanalyse sollten Massnahmen mindestens in den folgenden Bereichen geplant und durchgesetzt werden:

– *Personell:* Bei Einstellungsverfahren sind Hintergrundabklärungen über die Bewerber durchzuführen. Je nach Bedeutung der Kundenbeziehung oder des Arbeitsplatzes lohnt es sich, mit Spezialisten persönliche Befragungen durchzuführen.

– *Organisatorisch und technisch:* Die schutzwürdigen Informationen sind zu bezeichnen und zu klassifizieren; für die einzelnen Klassifizierungskategorien sind die angemessenen Behandlungsvorschriften und Informatikmassnahmen zu definieren. Insbesondere zu regeln sind die Massnahmen am Arbeitsplatz (Sichtschutz, Diebstahlschutz, Peripheriegeräte), bei der Übermittlung (Papierversand, Telefon/Fax, Internet/Intranet, mobile Kommunikation, E-Mail) und bei der Informatik (Passwörter, Viren, Laptops, Vernetzung).

Entscheidend ist, dass die Massnahmen intern bekannt gemacht, instruiert und verstanden werden. Geboten sind eine konsequente Umsetzung mit Kontrolle und Ahndung. Man muss aber auch wissen, dass es trotz konsequenter Abwehrmassnahmen keinen absoluten Schutz gegen Spionage und Competitive Intelligence gibt. Die im Kasten erwähnten Organisationen ASIS und SCIA/SCIP unterstützen die Bestrebungen für Counterintelligence und Competitive Intelligence.

Schlussfolgerungen

Competitive Intelligence und Counterintelligence sind Chefsache. Die Ausarbeitung und Einführung eines CI-Programms braucht Zeit. Wer sich einen Wettbewerbsvorsprung sichern, die Rentabilität verbessern und das langfristige Gedeihen des Unternehmens garantieren will, nimmt deshalb diese Arbeiten lieber heute als erst morgen in die Hand.

Bernhard Stoll, Oberst i Gst, lic. iur., bis 2007 Sicherheitsverantwortlicher, Stabschef Untergruppe Nachrichtendienst und Abwehr sowie Verteidigungsattaché im Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS). Inhaber Bernhard Stoll, Consulting (Kontakt: b.stoll@stoll-consulting.ch)

Stefan Schuppisser, Major, Nof Stab Ter Reg 4. Mehrjährige Tätigkeit als Unternehmensberater. Seit 2007 Leiter des Centers for Strategic Management an der School of Management and Law der ZHAW (Zürcher Hochschule für angewandte Wissenschaften). (Kontakt: sste@zhaw.ch)