

## **Aufklärung und Abwehr von elektronischer Spionage**

### **Fallstudie Januar 1998,**

Das Management der deutschen Anlagenbauer X aus NRW beruft eine Krisensitzung ein. Hintergrund ist die negative Geschäftsentwicklung im asiatischen Wirtschaftsraum. Anfänglichen Zuwachsraten bei Geschäftsabschlüssen folgten immer häufiger fehlgeschlagene Vertriebsaktivitäten und der Verlust einiger bisher stabiler Kundenbeziehungen.

Anfänglich wurden als Hintergrund für die negative Bilanz der Auslandsaktivitäten ein Missmanagement im Vertriebsbereich und ineffiziente Marketingmaßnahmen verifiziert.

Erst durch eine Mitteilung eines Vertriebsmitarbeiters, der berichtete, dass er im Mitte 1998 auf einer Messe von einem Unternehmensberater einer bislang unbekanntem Beratungsfirma kontaktiert wurde, wurde das Management aufmerksam.

In dem unverfänglichen Gespräch wurde M. durch den Unternehmensberater zu fachlichen Aspekten konsultiert. Im Verlauf des Kontaktes, der sich mittlerweile über drei Monate erstreckte, offerierte der "Consultants" ein Jobangebot bei einem Mitbewerber. Aus subjektiven Gründen (Familie, Bindung an die Region (AG)) lehnte M. diese Offerte ab. Nach dem direkten Angebot war der M. verunsichert, da ihm bewusst wurde, dass er im Vorfeld des unverfänglichen Kontaktes, zum Teil unbewusst über firmeninterne Details berichtet hatte. Erst mit dem Bewusstsein, dass der Berater zu einem am Markt bekannten Konkurrenten im engen Kontakt steht, war ihm klar, dass er mit der Preisgabe von Informationen aus seinem persönlichen Umfeld dem Mitbewerber einen Vorteil verschafft hat.

Eine Überprüfung der Geschäftsvorfälle und ein nachhaltiges Recherchieren zu den fehlgeschlagenen Vertriebsaktivitäten ergab, dass in mindestens vier der erfolglosen Akquisen indirekt der Mitbewerber den Zuschlag bekam. In drei Fällen wurden die Anlagen und Wirtschaftsgüter durch eine Unternehmen geliefert und errichtet, welches wirtschaftlich mit dem Konkurrenten verbunden ist. Im vierten Fall war der Mitbewerber direkt aktiv und erfolgreich platziert.

Durch die eingesetzte Task Force, bestehend aus einem Team von Sicherheitsberatern und Ermittlungsspezialisten, wurden nachhaltig Vorkommnisse der vergangenen 24 Monate systematisch analysiert und Handlungsversionen erarbeitet, die möglicherweise mit dem festgestellten Handlungskomplex (Verlust der Trade Securitys) in Verbindung stehen oder zugeordnet werden können.

Unter anderen wurde im Mai 1997 der Verlust eines Notebook des Technischen Direktors während eines Hotel-Aufenthaltes in Berlin registriert.

Das zweite auffällige Ereignis war im Dezember 1997 die Feststellung von Verschmutzungen (Abrieb von Deckenplatten) im Besprechungszimmer der Marketingabteilung. Diesem Umstand wurde damals keine Bedeutung beigemessen.

Diese Ereignisse und Feststellungen in Verbindung mit dem inzwischen bekannt gewordenen Abwerbeversuch ließen den Verdacht aufkommen, dass der Mitbewerber weiterhin mit illegalen Handlungen seinen Konkurrenten "ausspäht", um sich mit den internen Informationen einen Marktvorteil zu verschaffen. Durch das Berater-Team wurde ein Maßnahmenplan, der darauf ausgerichtet war, bereits erfolgte Angriffe des Mitbewerbers zu identifizieren und parallel eine präventive Gefahrenabwehr zu organisieren, erstellt. Die Durchführung einer **komplexen operativ-technischen Überprüfung (Sweep / ECM)** war Bestandteil der Primärmaßnahmen im Objekt des Klienten.

Zu Beginn der Untersuchungsmaßnahmen wurde eine Schwachstellenanalyse zu den betroffenen Unternehmensbereichen realisiert. Angriffsmöglichkeiten und realistische Handlungsszenarien wurden als Version erarbeitet und gemeinsam mit dem Klienten auf den realistischen Hintergrund geprüft. Infolge der für den Klienten transparenten Vorgehensweise, stellte die Unternehmensleitung die notwendigen Informationen für die Sicherheitsanalyse und die Erarbeitung einer realen Bedrohungslage, schnell und umfassend zur Verfügung.

Als Sofortmaßnahme brachte man das **Sweep-Team (ECM)** in der Marketingabteilung, der Verwaltung und dem Managementbereich zum Einsatz.



In Rahmen der funktechnischen Untersuchungen wurde im Besprechungsraum der Marketingabteilung, dort wo man den Abrieb festgestellt hatte, ein Mikrofon entdeckt, welches im Deckenbereich eingebracht wurde. Vom Mikrofon aus führte ein ca. 40 Meter langes Kabel über die Zwischendecke, oberhalb des Hauptflures zum Treppenaufgang (Notausgang). Dort befand sich ein Netzsender (137,5 Mhz) der von einem 230-V-Lichtanlagen-Element mit der notwendigen Netzspannung versorgt wurde.

Die ursprünglich auf ca. 20 cm-Länge vorbereitete Antenne (Kupferkabel) war zur Verminderung der Sendeleistung zusammengewickelt worden.

Die noch intakte Sendeanlage wurde sofort auf ihre Reichweite getestet. Dabei wurde festgestellt, dass der Transmitter eine Sendeleistung von ca. 50-85 Meter, abhängig vom Standort des Empfängers hatte. Dieser Senderadius lag im unmittelbaren Bereich eines öffentlichen Parkplatzes, der an Objektperipherie lag und auch von firmenfremden Personen genutzt wurde (Anlieger).

Die dort in der Nacht der Untersuchung abgestellten Kraftfahrzeuge wurden für weitere Untersuchungen dokumentiert. Im Interesse der Unternehmensreputation konnte eine Offizialisierung der Ergebnisse gegenüber den Strafverfolgungsbehörden nicht erfolgen. Die Offenlegung der Tatangriffe hätten mit Sicherheit zu einer Verunsicherung strategischer Partner und Kunden geführt.



Nach Ausmessen der entsprechenden Sendeleistung, wurde entschieden, den Sendebetrieb zu unterbrechen und die Sendeanlage sicherzustellen. Eine Folgeuntersuchung ergab, dass Teile der Sendetechnik mit hoher Wahrscheinlichkeit innerhalb der Bundesrepublik gekauft wurden. Dafür sprach das Spezialmikrofon und das Systemkabel der Firma S. und der bequarzte Minisender.

Parallel zu den Untersuchungsmaßnahmen wurde durch die Spezialisten für Kommunikationstechnik die gesamte Telefonanlage auf Manipulationen überprüft.

Im vorliegenden Fall handelte es sich um eine ISDN-Telefonanlage, die von Seiten der Telekom von einem Primärmultiplexer (S 2 M-Schnittstelle mit 30 Kanälen).

An den für Außentäter nutzbaren Schnittstellen und auch an den zugänglichen Leitungsbereichen wurden keine Hinweise oder konkret eingesetzte Sprachdokumentationssysteme festgestellt.



Präventiv wurde entschieden, den sogenannten D-Kanal zu überwachen, um mögliche Manipulationen, die von außen realisierbar sind, zu registrieren. Die Sondertechnik wurde innerhalb von sieben Tagen zum Einsatz gebracht.

Zeitgleich mit der operativ-technischen Untersuchung wurde der bisher relativ ungesicherte Zugang zum Managementbereich mit verdeckter Videotechnik für eine operative Zugangskontrolle gesichert.

In den betroffenen Bereichen wurde gleichzeitig die zwischenzeitlich veraltete und nicht mehr überschaubare Schließanlage durch eine Werksanlage der Firma KESO ersetzt. Für die gefährdeten Bereiche wurden gleichzeitig Neuerungen in der Logistik (Zugangskontrolle, Schlüsselregime, Besucherabfertigung, Vernichtung von Arbeitsunterlagen) vorbereitet und umgesetzt.