



SECURITY *insight*

Fachzeitschrift für Sicherheits-Entscheider

Aus dem Inhalt

Schwerpunkt:
Ausweismanagement

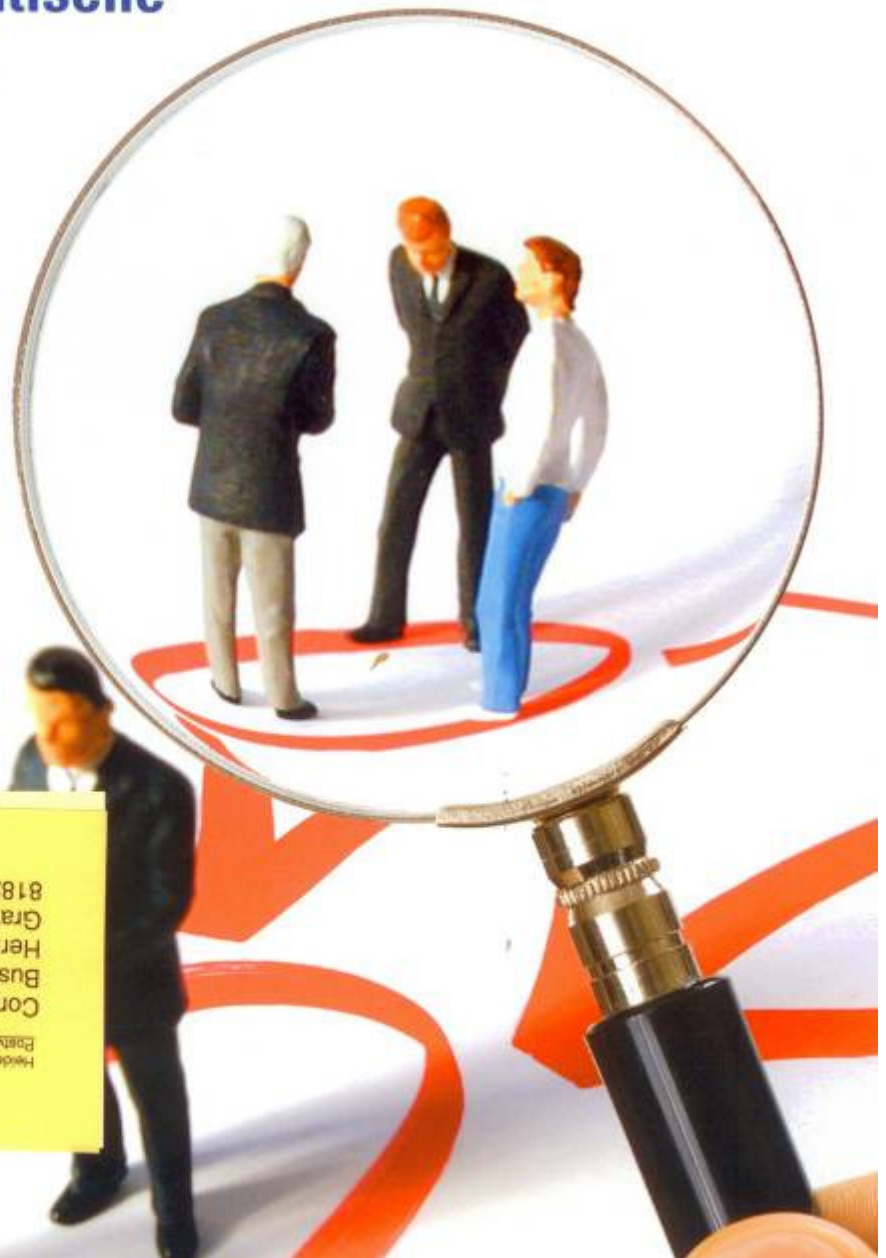
Im Fokus:
Industrie
und Wirtschaft

Serie: Krahecks
Sicherheitsprojekt

Hintergrund:
Informationsschutz

Messe:
„CeBIT“ mit
Sicherheitshalle

Titelthema: Semantische Netze



Heide & Klaus GbR Salaweg 30073454 Hameln
Postfach 2600, Deutsche Post AG, Fernpost bezahlte, 77500
Corporate Trust
Business Risk & Crisis Management GmbH
Herrn Christian Schaat
Graf-zu-Castell-Strabe 1
81829 München



Es muss nicht immer eine eigene Abteilung sein

Wie sich mit einer Outsourcing-Lösung das Sicherheitsniveau eines Konzerns mit dem Budget eines Mittelständlers erreichen lässt

Von Christian Schaaf



Papierdokumente gehören zu zersichert ins Altpapier.

Da war der Vertriebsleiter des norddeutschen Maschinenbauunternehmens durchaus verwundert. Die Ersatzteile für seine eigens entwickelten Maschinen bekamen seine Kunden zunehmend von anderen Lieferanten angeboten. Dabei war das Ersatzteilgeschäft sehr lukrativ und überstieg den Gewinn aus der eigentlichen Entwicklung und Konstruktion bei Weitem. Bei genauerer Betrachtung stellte man sehr schnell fest, dass die Ersatzteile der Fremdanbieter als Originalersatzteile verkauft wurden und sogar das eigene Firmenlogo verwendet wurde. Das Unternehmen hatte zu diesem Zeitpunkt keinen Sicherheits-Verantwortlichen, und auch die IT-Struktur war nicht gegen internen Informationsabfluss geschützt. Solche Fälle von Wirtschaftsspionage sind keine Seltenheit. Doch in wirtschaftlich schwierigen Zeiten nimmt ihre Zahl nachweislich zu. Gerade mittelständische Firmen sind darauf oft nicht vorbereitet.

Deutschland als Exportweltmeister ist stark international ausgerichtet. Vor allem mittelständische Unternehmen mit ihrer hohen Innovationsfähigkeit sind auf unterschiedlichsten Gebieten Welt-

marktführer. Internationale Ausrichtung bedeutet jedoch auch globale Risiken und damit die Anforderung, sich auf diese Risiken vorzubereiten, gerade auch während einer Wirtschaftskrise. Es geht



dabei nicht nur um die wirtschaftlichen Risiken, sondern in zunehmendem Maße um Fragen der Sicherheit.

Bei Geschäften in Osteuropa werden Schmiergelder gezahlt, um an Aufträge zu kommen. Ein Mitarbeiter wird auf einer Geschäftsreise bei einem Überfall oder Bombenanschlag im Hotel verletzt. Die IT-Abteilung stellt einen Hackerangriff auf die Unternehmensserver fest. All das sind realistische Bedrohungsszenarien. Darüber hinaus steigt in Zeiten kriselnder Wirtschaft häufig die allgemeine Kriminalität, weil mehr Menschen in einen finanziellen Engpass geraten. Die Unternehmenswerte sind bedroht, weil die Zahl von Diebstahl, Einbruch und Überfall ebenso zunimmt wie die Angst vor Arbeitsplatzverlust. Dadurch steigt die Gefahr der Mitarbeiterkriminalität. Wenn vorsorglich Daten kopiert werden, um für einen neuen Arbeitgeber interessanter zu sein, führt das vermehrt zu Schäden. Diese Szenarien können für ein Unternehmen weit reichende Folgen haben, nach innen wie außen; die Reputation ist bedroht.

Der Einkäufer war's

Die meisten Konzerne sind auf diese Szenarien gut vorbereitet. Sie unterhalten in der Regel eine Corporate-Security-



Unser Autor Christian Schaaf ist Geschäftsführer der Corporate Trust Business Risk & Crisis Management GmbH, ein strategischer Partner namhafter Unternehmen im Risiko- und Krisenmanagement. Als Unternehmensberatung unterstützt Corporate Trust Unternehmen, Organisationen und Privatpersonen auf dem Gebiet der High-Level-Security.

Abteilung, in der sich Spezialisten um alle Sicherheitsbelange kümmern. Diese Konzernsicherheit umfasst teilweise mehrere hundert Mitarbeiter. Im Mittelstand sieht das anders aus. Der Aufbau einer eigenen Sicherheitsstruktur ist für mittelständische Unternehmen oft nicht wirtschaftlich, daher fehlen oftmals die nötigen Sicherheitsprozesse. Was aber, wenn ein Mitarbeiter im Ausland verletzt oder ein Bestechungsfall in den Medien bekannt wird? Was passiert, wenn bei einer Kontrolle zufällig auffällt, dass ein Mitarbeiter die gesamte Kundendatenbank oder alle Entwicklungsdaten auf einen USB-Stick kopiert und der Konkurrenz zugespielt hat?

Die Prüfung durch externe Spezialisten ergab bei besagtem norddeutschem Maschinenbauunternehmen, dass sich

ein Mitarbeiter aus dem Einkauf sämtliche Konstruktionszeichnungen und Materialbeschreibungen vom Server gezogen hatte. Er hatte gute Kontakte zu einem Vorlieferanten aus einem osteuropäischen Staat aufgebaut, der für das eigene Unternehmen tätig war. Ihm stellte er die Daten zur Verfügung, sodass dieses Unternehmen in der Lage war, fast alle Ersatzteile originalgetreu herzustellen. Da der kriminelle Mitarbeiter auch bei den Vertriebskontakten „beihilflich“ war, konnten sehr schnell Kunden mit den entsprechenden Maschinen akquiriert werden.

In einem anderen Fall erpressten tschechische Geschäftspartner das tschechische Tochterunternehmen eines Mittelständlers aus Süddeutschland. Bei den Tätern handelte es sich um Mitar-



Menschen und Werte schützen.

Sicherheit geben, Know-how bewahren, Gebäude überwachen – mit der ZEUS® Zutrittskontrolle schützen Sie zuverlässig und diskret Menschen, Daten, Werte und Know-how.



Zeitwirtschaft
WebWorkflow
Personaleinsatz
Betriebsdaten
Zutrittskontrolle

Zutrittskontrolle

ISGUS GmbH
Oberdorfstr. 18-22
D-78054 Villingen-Schwenningen
Tel. +49 7720 393-0
info@isgus.de





beiter eines Lieferanten, zu dem bereits seit Jahren geschäftliche Beziehungen bestanden. Die Erpressung belief sich zuerst auf einen Betrag in einstelliger Millionenhöhe. Der Vorwand: Das vereinbarte Auftragsvolumen sei nicht eingehalten und die Reputation des Unternehmens durch den deutschen Partner geschädigt worden. Dafür stellte man „Schadenersatzforderungen“ und drohte damit, die Produktion einzustellen beziehungsweise die zur Verfügung gestellten Werkzeuge nicht mehr herauszugeben. Der Mittelständler wäre selbst bei seinen Kunden in Lieferschwierigkeiten geraten und scheute die hohen Verzugsstrafen. Daher wurde die Forderung bezahlt.

Da sich das Unternehmen auf diese Weise als leicht erpressbar zu erkennen gab – die Zahlungsabwicklung erfolgte über einen tschechischen Notar –, war es als interessantes Opfer identifiziert. Nur zwei Monate später – das Unternehmen hatte sich entschieden, auf Grund des Vorfalls den Lieferanten zu wechseln – kam die zweite Erpressung. Diesmal belief sich der Betrag bereits auf eine zweistellige Millionensumme. Das deutsche Unternehmen wurde abermals damit erpresst, dass die Werkzeuge, die in Kürze zum neuen Lieferanten verfrach-

tet werden sollten, nicht mehr herausgegeben würden.

Aufbau von Risiko- und Notfallstrukturen

Die Fälle zeigen: Auch mittelständische Unternehmen sollten umfangreiche Sicherheitsvorkehrungen treffen, um sich präventiv zu schützen und im Notfall mit einem funktionierenden Krisenmanagement handlungsfähig zu sein. Dabei ist es nicht erforderlich, die Strukturen eines großen Konzerns vorzuhalten. Mit einem wirtschaftlich vernünftigen Ansatz können diese Risiko- und Notfallstrukturen im Unternehmen aufgebaut und durch eine maßgeschneiderte Outsourcing-Lösung an Sicherheitsspezialisten ausgelagert werden. Externe Spezialisten stehen dann jederzeit, rund um die Uhr, mit den nötigen Strukturen, dem entsprechenden Know-how und einem internationalen Netzwerk zur Verfügung. Voraussetzung ist nur die Etablierung eines Basis-Sicherheitskonzepts. Die Unternehmen binden damit keine eigenen Ressourcen, es entstehen keine unnötigen Kosten und sie können sich weiterhin auf ihre Kernkompetenzen konzentrieren.

Im genannten Fall wandte sich das süddeutsche Unternehmen nach dem ers-

ten Vorfall an einen professionellen Krisenberater, um für ähnliche Fälle besser vorbereitet zu sein. Der Sicherheitsspezialist erstellte einen Basisnotfallplan und etablierte die nötigen Krisenstabsstrukturen im Unternehmen. Deshalb lief die zweite Erpressung ganz anders ab. Der Krisenstab war auf seine Rolle vorbereitet, die nötigen Sicherheitsvorkehrungen vor Ort wurden sofort ergriffen und die Verhandlungen liefen nach einem strukturierten Muster. Die Kriminellen reduzierten die Lösegeldforderung erheblich, übergaben die Werkzeuge unbeschädigt und die Gefahr für die Mitarbeiter konnte auf ein Minimum beschränkt werden.

Corporate Trust bietet hier das speziell auf den Bedarf von mittelständischen Unternehmen zugeschnittene Sicherheitskonzept „Basic Trust“. Das neu entwickelte Dienstleistungsangebot ist eine maßgeschneiderte Outsourcing-Lösung zur Gefahrenabwehr und Risikominimierung. Mittelständlern erschließt sich damit eine Dimension an Sicherheit, wie sie bisher nur für Großunternehmen zu realisieren war.

Das Basis-Sicherheitskonzept umfasst eine erste Analyse der tatsächlichen Bedrohungssituation. Hier bewerten die Spezialisten unter anderem, wel-



Elektronische Augen sehen mehr als menschliche. Doch solche singulären Schutzmaßnahmen, wie man sie gerade in mittelständischen Betrieben beobachten kann, nutzen wenig. Besser sind individuell erstellte Sicherheitskonzepte.



Passt der mittelständische Maschinenbauer nicht auf, genügt nur ein kleiner Container für die Bestellung seiner Original-Ersatzteile. Die von der Konkurrenz gefälschten Ersatzteile brauchen dann weitaus mehr Lagervolumen.



che Unternehmensprozesse kritisches Potenzial in sich bergen, ob es ein erhöhtes Risiko für Informationsabfluss oder Korruption gibt, wie die Sicherheitsvorkehrungen für Reisen in Risikoländer sind und ob die objektsichernde Maßnahmen den tatsächlichen Anforderungen entsprechen. Auch die Sicherheit der IT-Landschaft, die Vorkehrungen für den medialen Umgang mit einem öffentlich gewordenen Schadensfall und die Strukturen für einen möglichst schnellen Wiederanlauf der Geschäftsprozesse nach einem Schadensereignis können dabei näher betrachtet werden.

Aus den Erkenntnissen wird ein Basisnotfallplan entwickelt, der es im Ernstfall ermöglicht, schnell zu reagieren und gezielt die richtigen Gegenmaßnahmen zu treffen. Dieser Plan definiert die Krisenorganisation des Unternehmens und legt die Verantwortlichkeiten fest. Es gibt Handlungsempfehlungen für die Mitglieder im Krisenstab, die Kommunikation im Krisenfall und das Verhalten bei verdächtigen Wahrnehmungen. Hinzu kommen Checklisten für die Krisenstabssitzungen und eine Gefährdungsanalyse bei einem kriminellen Angriff. Der Basisnotfallplan enthält auch Hinweise zu rechtlichen Belangen. So muss die Stellung jedes



Welches Ungemach bei der Geschäftsreise ins Ausland droht, kann man natürlich nie genau voraussagen. Aber man kann sich darauf vorbereiten.

Mitglieds im Krisenstab klar definiert sein und eine Vollmacht für die Krisenberater vorliegen.

Im Unternehmen sollte ein Sicherheitsverantwortlicher institutionalisiert werden, der als Ansprechpartner für die Geschäftsleitung und alle Mitarbeiter zur Verfügung steht und das Bindeglied zur externen Sicherheitsorganisation darstellt. Ist durch die Erstanalyse und den Basisnotfallplan der grundsätzliche Rahmen gesteckt, hat das Unternehmen eine funktionale Struktur, um auf kriminelle Angriffe oder Sicherheitsrisiken professionell zu reagieren. Der Bedarf im Rahmen von „Basic Trust“ kann vielfältig sein und reicht vom Informationsschutzkonzept bis zur Reisesicherheit.

Reisesicherheit

Gerade die Reisesicherheit spielt für viele Mitarbeiter eine zunehmend wichtigere Rolle. Die Zahl der Länder mit erhöhtem Risiko steigt. Wirtschaftlich interessante Projekte bieten sich häufig auch in diesen Regionen. Das Unternehmen ist gefordert, bereits bei der Reiseplanung und -vorbereitung die Sicherheitsaspekte mit einzubeziehen. Es sollte standardisierte Prozesse für das Reisemanagement geben, in dem es neben einer Risikobewertung für das jeweilige Land auch detaillierte Sicherheitsinformationen zur entsprechenden Region oder der Reisezeit gibt. Auch Schulungen für das sicherheitsgerechte Verhalten und eine Risikominimierung sollten den Mitarbeitern angeboten werden.

Eine professionelle Outsourcing-Lösung ist für mittelständische Unternehmen also die ideale und wirtschaftlichste Lösung zur Gefahrenabwehr und Risikominimierung. Sie bietet nicht nur ein hohes Maß an Sicherheit, sondern auch kalkulierbare Festkosten und die Möglichkeit, nur gezielt die Leistung abzurufen, die gerade benötigt wird.

WWW.CORPORATE-TRUST.DE