KEYSTONE

Massgeschneiderte Informationssicherheit für KMU:

wissen.org Consulting GmbH hilft Ihnen, ein pragmatisches ISMS (Informationssicherheits-Managementsystem) nach ISO 27001 aufzubauen.

In kürzester Zeit und zu geringen Kosten.

Haftung ohne Grenzen

Cyber-Kriminalität Grossunternehmen zwingen KMU und Lieferanten immer mehr dazu, ihre IT aufzurüsten. Weigern sie sich, in die Sicherheit zu investieren, verlieren sie die Aufträge.

Ein nach ISO27001 zertifiziertes Unternehmen erfüllt genau diese Anforderungen.

JORGOS BROUZOS

Die Kleinbetriebe hatten keine Wahl. Um weiterhin zu den Lieferanten eines Schweizer Industriebetriebs zu gehören, mussten sie sich einer elektronischen Plattform anschliessen. Über sie laufen nun alle Bestellungen, die Rechnungen und der Datenaustausch. Hätten sie nicht mitgemacht, wären sie alle lukrativen Aufträge los.

Dieses Vorgehen ist kein Einzelfall. Grosskonzerne geben viel Geld für ihre Informatiksicherheit aus, doch viele kleinere Unternehmen und Zulieferer unterschätzen die virtuelle Bedrohung aus dem Netz. Das rächt sich. Gemäss einer Erhebung der IT-Sicherheitsfirma Symantec gilt rund die Hälfte der weltweiten Cyber-Angriffe Firmen mit weniger als 2500 Mitarbeitern. In der Schweiz liegt die Quote höher. Die Melde- und Analysestelle Informationssicherung des Bundes (Melani) gab kürzlich bekannt, dass 75 Prozent der 885 im letzten Jahr gemeldeten Vorfälle Unternehmen mit weniger als 1000 Mitarbeitenden betrafen. Diese Zahlen lösen bei Schweizer Grossunternehmen Alarm aus. Denn ihre Lieferanten und Partner können über ihre ungenügend geschützten IT-Systeme die Firmengeheimnisse in Gefahr bringen. Offen über dieses heikle Thema will niemand sprechen. Doch mit der Materie Vertraute bestätigen, dass seit einigen Monaten der Druck auf Kleinbetriebe steigt, ihre IT aufzurüsten. Das sei mit grossen Anstrengungen und kostspieligen Investitionen verbunden. Daran führe jedoch kein Weg vorbei, sonst drohe den Zulieferern der Wegfall wichtiger Auftraggeber.

Sicherheit wichtiger als Preis

Schweizer Unternehmen wie Swisscom, Rolex und Novartis tauschen sich im Information Security Forum (ISF) mit internationalen Grosskonzernen über das Problem der IT-Sicherheit aus. Sie sehen sich mit einem neuen Phänomen konfrontiert. «Aus der Unsicherheit bei Kleinbetrieben entsteht ein bedeutendes Risiko für Grossunternehmen», sagt Steve Durbin vom ISF.

Viele kleinere Firmen sind nicht nur Zulieferer, sondern kooperieren auch bei der Forschung mit Grossunternehmen. «Grosskonzerne haben ein Interesse, ihre Zulieferer entsprechend auszubilden und dafür zu sorgen, dass diese möglichst sicher sind», so Durbin. Die Grossen würden nun damit beginnen, ihre Lieferanten zu überprüfen und abzuklären, wo die grössten Risiken zu finden sind.

In der Finanzbranche ist das bereits üblich. Wenn ein Zulieferer die Sicherheitsstandards gemäss den Vorgaben der Bank nicht erfüllt, kommt keine Geschäftsbeziehung zustande. Andere Branchen nehmen sich daran ein Beispiel. Gerade in der Pharmazeutik, Technologie, Rüstungsindustrie, also überall dort, wo Patente wichtig sind, sei dies bereits schon umgesetzt oder verstärkt zu erwarten, bestätigt Thomas Koch, Sicherheitsexperte beim Beratungsunternehmen PwC.

Auch er beobachtet, dass Grossunternehmen zunehmend sensibler mit der IT-Sicherheit bei Lieferanten umgehen. «Nicht mehr nur der Preis entscheidet darüber, ob eine Firma als Zulieferer zum Zug kommt, sondern auch, wie die Firma bezüglich Datensicherheit aufgestellt ist», sagt Koch. Die Grossunternehmen sehen sich die Zulieferer genauer an und führen eine Due-Diligence-Prüfung durch. «Wie es um eine Firma steht, findet man nur heraus, wenn man sie sich ansieht», so Koch.

Markus Martinides, unabhängiger Sicherheitsexperte und Firmenchef von SUA Telenet, fordert gar eine regelmässige Qualitätssicherung der externen Lieferanten durch unabhängige Auditoren. Sonst stellten sich Lieferanten selbst ein Attest aus, das immer gleich ausfallen würde: Alles im grünen Bereich. Diese Sicherheit ist aber trügerisch. «Bei Zulieferern können sehr grosse Risiken entstehen, weil oftmals unklar ist, wer auf die gespeicherten Daten Zugriff hat», erklärt Martinides. Das können sich die Angreifer zunutze machen. Denn laut Max Klaus, dem stellvertretenden Leiter von Melani, ist das Vorgehen der Cyber-Kriminellen immer wieder das gleiche. «Ein Trojaner wird in ein Unternehmen eingeschleust, dann werden Daten abgezogen.» Die Angriffe reichen vom Diebstahl von Kreditkartennummern bis zur Erpressung oder Wirtschaftsspionage.

Die Kosten für die IT-Sicherheit müssen die Zulieferer übernehmen.

Das schreckt Grossunternehmen auf. Bestehende Partnerschaften werden stärker analysiert, und Zulieferer enger miteinbezogen, so PwC-Mann Koch. Wie die Einbindung vor sich geht, kommt auf die Wichtigkeit des Subunternehmens an. Es geht aber so weit, dass Lieferprozesse bei den Zulieferern umgestellt werden und über das Hauptunternehmen laufen. Zudem geben Grossunternehmen zunehmend IT-Know-how an kleinere Firmen weiter: «KMU stören sich nicht daran, dass bei ihnen die Sicherheit auf diese Weise verbessert wird», sagt Koch.

Die hohen Kosten für die Einhaltung der Informationssicherheitsstandards sind aber oftmals ein Problem, denn finanzielle Unterstützung erhalten kleine Firmen für ihre Investitionen nicht. Dabei gehen die notwendigen Massnahmen und Reports ins Geld. «Die Unternehmen müssen diese Kosten schon zu Beginn in ihre Offerte einplanen», sagt Koch. Die Anforderungen zu erfüllen sei aber unausweichlich.

Haftung unbegrenzt

Der auf IT-Recht spezialisierte Anwalt Alexander Schmid stellt fest, dass Kunden ihren Lieferanten sichere IT-Systeme in den Verträgen vorschreiben. «Gerade bei Outsourcing-Transaktionen sehen wir striktere Regelungen.» Vertragliche Pflichten für Lieferanten verlangen sichere Systeme, die vor Viren und Malware geschützt sind. Es wird aber nicht vorgeschrieben, welche Systeme verwendet werden müssen. Bei einigen Verträgen werden ausserdem sogenannte Chinese Walls verlangt – das heisst, dass nur Mitarbeiter, die in ein Projekt involviert sind und Zugang auf sensitive Informationen haben müssen, Zugriff auf die entsprechenden Dokumente, Informationen und Daten haben dürfen. Schmid weist ferner darauf hin, dass zumeist Haftungsbegrenzungen ausgeschlossen werden, wenn es um Geheimhaltungs- und Datenschutzverletzungen geht.

Die Haftung für Schäden ist dann nicht mehr gegen oben begrenzt. «Das wird in der Regel vom Kunden gewünscht», sagt Schmid. Für die Lieferanten ist das ein Nachteil, denn eine Haftungsbegrenzung macht das Risiko eines Vertrages kontrollierbar. Das Fehlen einer Haftungsbegrenzung kann für die Unternehmen fatale Folgen haben, wenn es zu einem Datenverlust kommt. Dann kann bereits ein illoyaler Angestellter zum Risiko für eine Firma werden und einen enormen Schaden verursachen.

SICHERHEIT

Bund setzt auf freiwillige Meldungen

Schutz vor Cyber-Attacken Die Melde- und Analysestelle Informationssicherung des Bundes (Melani) schützt die kritischen Infrastrukturen der Schweiz. Dazu arbeitet sie mit ausgewählten Betreibern zusammen, etwa in der Telekommunikations- und Energiebranche. Zudem informiert Melani die Bevölkerung über Risiken im Internet. In der Vergangenheit gab es mehrere parlamentarische Vorstösse. Sie zielten auf einen Ausbau der Dienstleistungen von Melani. So forderte die Motion «Melani für alle», dass die Meldestelle auch für Kleinunternehmen und Bürger zuständig sein sollte. Sie wurde vor kurzem im Nationalrat aber deutlich abgelehnt.

Strategie des Bundes Im Sommer verabschiedete der Bundesrat die nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken. Die definierten Massnahmen sollen bis Ende 2017 umgesetzt werden. Unter anderem sollen die zuständigen Stellen beim Bund ausgebaut werden.

Keine Mindeststandards Bei der Ausarbeitung der Strategie wurde auch darüber diskutiert, ob der Bund den Unternehmen Mindeststandards vorschreiben soll, so Max Klaus von Melani. Der Vorstoss fand jedoch nur wenig Unterstützung. Die Privatwirtschaft hätte eine finanzielle Beteiligung des Bundes erwartet. Zudem wäre die Massnahme nur schwer zu kontrollieren und durchzusetzen gewesen.

KEYSTONE/GAETAN BALLY

Sicherheitsleck: Viele Firmen verschweigen Cyberattacken lieber.

Verschwiegenheit «Ich kenne nicht viele Unternehmen, die freiwillig ein Sicherheitsleck bekannt machen», sagt ein Sicherheitsexperte. Er macht daher einen gewissen Bedarf an obligatorischen Publizitätsvorschriften aus. Die Frage sei dann aber, wie und gegenüber wem der Zwischenfall offengelegt werden muss. Denn die Wirkung von Sicherheitslücken auf Unternehmen dürfe nicht unterschätzt werden. Da der Ruf der Firma unter Umständen stark leidet, wollen viele Firmen ihre Informationen in einer geschützten Umgebung austauschen.

Grösseres Vertrauen In einigen Staaten, etwa den USA, wurde bereits eine Meldepflicht für Unternehmen bei kritischen IT-Sicherheits-Problemen eingeführt oder es finden Diskussionen dazu statt. Eine solche Vorschrift steht in der Schweiz derzeit nicht zur Debatte. Es sei oftmals nicht einfach zu definieren, wann ein Sicherheitsproblem für ein Unternehmen kritisch sei, so ISF-Experte Steve Durbin. Bei Melani machte man die Erfahrung, dass betroffene Unternehmen auskunftsfreudiger sind, wenn sie Zwischenfälle freiwillig melden. Das sei sogar von Vorteil, denn im Ausland würden von den Firmen oftmals nur die vorgeschriebenen Vorfälle gemeldet, stellt man fest. Der Rest wird unter den Tisch gekehrt.

ANZEIGE

Mit einem ISMS (Informationssicherheits-Managementsystem) nach ISO 27001 erhalten Sie massgeschneiderte IT-Sicherheit bei einem optimalen Kosten-Nutzen Verhältnis.

Gratis Fibu & Infos: www.buspro.ch

Das Business-Programm

© Alle Rechte vorbehalten - Axel Springer Schweiz AG, - Jede Veröffentlichung und nicht-private Nutzung exklusiv über www.as-infopool.de/lizenzierung HANDELSZEITUNG-2012-11-22-tui- c7eb10a6fa6300004f5dcd8a6510c7d4