Sicherheit in Liefe-rantenbeziehungen

Für viele Systeme ist es heute unabdingbar, externe Unterstützung beizuziehen. Wenn diese dann auch Zugriff auf Firmenwerte haben, gilt es diese speziell zu schützen. Das Kapitel A.15 definiert daher das Ziel: Für Lieferanten zugängliche Werte des Unternehmens sind geschützt.

Doch was sich so einfach liest, ist gerade in grösseren Firmen eine Herausforderung. Daher gilt es an einer zentralen Stelle eine Liste mit allen involvierten Partnern zu erstellen. Darin enthalten sind neben Namen, Adresse(n) und Kontaktmöglichkeite(n) die Beschreibung der Zusammenarbeit, die Ansprechpersonen, das definierte SLA, allenfalls übergebene Werte (zum Beispiel Laptop, Token usw.), die Zugriffsmöglichkeiten (direkter Zugriff, VPN, TeamViewer, vergebene Rechte auf Systeme und Daten usw.) sowie die Anforderungen an die Informationssicherheit.

Die Dokumentation muss der Firma gehören

Jede Partnerschaft gilt es im Auge zu behalten. Auch wenn diese hervorragend läuft, gilt es einen standardisierten Prozess und Lebenszyklus einzuhalten. Dazu gehören Regeln zur zulässigen Nutzung, Regeln zu Sub-Lieferanten (erlaubt, nicht erlaubt, Informationspflicht, usw.), Handhabung von Vorfällen, Schulung und Sensibilisierung, Verfahren zur Überwachung der definierten Anforderungen (Stichwort SLA), allenfalls auch Überprüfungen durch Dritte, sowie Fehlerbehebungs- und Konfliktlösungsprozesse. Werden Abweichungen festgestellt, müssen diese diskutiert und Lösungen gefunden werden.

Wird die Betreuung der IT an einen externen Spezialisten übergeben, muss im Vorfeld definiert werden, dass die Dokumentation der eigenen Firma gehört. Diese wird aus meiner Erfahrung sträflich vernachlässigt und vor Ort ist entweder keine oder eine stark veraltete vorhanden. Doch diese gehört zwingend dazu und muss immer aktuell sein. Oft erlebe ich in der Praxis, dass Rechte für ein Unternehmen vergeben werden und nicht auf eine Person bezogen. Tritt ein Mitarbeiter beim Partner aus, erfolgt keine Benachrichtigung. Somit wird das Passwort nicht gewechselt und der ausscheidende Mitarbeiter hat auch in Zukunft weiterhin Zugriff auf die Daten. Daher ist es zwingend, dass Rechte immer persönlich sind und das eigene Unternehmen über jede Veränderung informiert werden. Dazu muss eine Namensliste aller involvierten Beschäftigten des Lieferanten erstellt, gepflegt und mindestens halbjährlich mit dem Lieferanten abgeglichen werden.

Bild: Archiv

Informationen dürfen nicht in die falschen Hände gelangen.

Eigenen Überwachungsprozess etablieren

Weiter gehört die Verpflichtung dazu, wenn Störungen oder Ausfälle auftreten, dass umgehende Benachrichtigung erfolgt. Gerade in der DS-GVO (Datenschutz Grundverordnung der EU) ist die 72-Stunden-Regel definiert. Diese ist auch in der Schweiz vorgesehen. Innerhalb von 72 Std. müssen die Kunden und/oder Behörden über den Vorfall informiert werden. Daher muss die Lieferkette durchgängig und schnell sein – auch am Wochenende und an Feiertagen.

Gerade die Lieferkette ist heute eine grosse Herausforderung. Oft ist nicht mehr bekannt, welche weiteren Firmen in ein Projekt involviert sind. Dazu müssen klare Anforderungen an die Informationssicherheit definiert und eingefordert werden. Die erstellten Bedingungen gelten auch für mögliche Unterlieferanten, falls überhaupt erwünscht und erlaubt. Der Lieferant muss seine Sub-Lieferanten im «Griff» haben und einen eigenen Überwachungsprozess etablieren. Veränderungen in dieser Beziehung sind auch dem Auftraggeber innert kürzester Fristz mitzuteilen. Bei besonders schützenswerten Daten ist dabei äusserste Vorsicht geboten. Schnell kann die Übersicht verloren gehen und Informationen in die falschen Hände gelangen. Verschiedene erfolgreiche Angriffe zeigen, dass Hacker Daten über Sub-Lieferanten beschafft haben. Diesen Umstand gilt es in der Risiko-Analyse zu berücksichtigen.

Vertrauen ist gut, Kontrolle ist besser

Der externe Partner muss alles unternehmen, um die übergebenen Daten vor fremden Zugriffen zu schützen. Hier lohnt es sich, auch einmal auf die Finger zu schauen. Dazu sollte im Vorfeld ein Audit-Recht in die Vereinbarung aufgenommen werden. Treu dem Motto: Vertrauen ist gut, Kontrolle ist besser. Fehler oder Missverständnisse können passieren, das ist daher nicht negativ gemeint, sondern soll die Partnerschaft bereichern. Abweichungen oder Fehler können festgestellt und zusammen gelöst werden.

Jede Partnerschaft ist Veränderungen unterworfen. Das Umfeld ändert sich stetig. Verbesserungen, Weiterentwicklungen und Neuerungen gehören zum Lebenszyklus. Gerade in der IT ist heutige Technologie morgen bereits wieder veraltet. Je nach Kritikalität ergeben sich damit Anpassungen an Verträgen. Mit einer aktiven Lieferantenbewirtschaftung kann dies berücksichtigt und schnell reagiert werden.

Ohne Lieferanten kann heute kein Unternehmen mehr existieren. Diese Partnerschaften gilt es zu pflegen. Änderungen gehören zum Lebenszyklus dazu. Werden entsprechende Vereinbarungen definiert, die Partnerschaft regelmässig überwacht und Veränderungen berücksichtigt, kann die Informationssicherheit jederzeit gewährleistet werden und einer erfolgreichen Zusammenarbeit steht nichts im Weg.

INFOS | KONTAKT

goSecurity GmbH
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch