Zertifikat ist nicht gleich Zertifikat

von Andreas Wisler

Bei unserem eigenen Zertifizierungsaudit stiessen wir auf ein Zertifikat, das auf den ersten Blick überzeugend aussah: «ISO 27001 zertifiziert durch Firma XY». Doch bei genauerer Betrachtung handelte es sich um ein fragwürdiges Angebot, das nicht den strengen Anforderungen einer ISO-Zertifizierung entspricht. Warum ist also ein Zertifikat nicht gleich ein Zertifikat? Und welche Risiken bergen diese vermeintlich günstigen Angebote?

LOCKVOGEL-ANGEBOTE – WENN DER PREIS ZU GUT KLINGT, UM WAHR ZU SEIN

Viele Unternehmen, insbesondere solche mit begrenztem Budget, werden von verlockenden Zertifizierungsangeboten angezogen, die mit schnellen und günstigen Lösungen werben.

- Aufbau: Die Grundstruktur des Managementsystems wird oft pauschal vorgegeben, ohne Rücksicht auf die tatsächlichen Anforderungen des Unternehmens.
- Notwendige Dokumente enthalten: Viele dieser Angebote liefern vorgefertigte Dokumente, die nur oberflächlich an die Unternehmensbedürfnisse angepasst werden.
- Internes Audit als Bestandteil: Ein internes Audit wird in das Angebot eingeschlossen, jedoch häufig von der gleichen Person durchgeführt – eine Unabhängigkeit ist nicht gewährleistet.
- Rasche Umsetzung garantiert: Die Umsetzung des ISMS wird innerhalb kürzester Zeit versprochen, oft innerhalb weniger Wochen.
- Garantierte Zertifizierung: Ein besonders auffälliger Punkt – die Zertifizierung wird garantiert. Und all das zu einem unschlagbar günstigen Pauschalpreis. Doch was auf den ersten Blick wie ein attraktives Angebot aussieht, birgt erhebliche Risiken.

RISIKEN – ES IST NICHT ALLES GOLD, WAS GLÄNZT

- Keine externe Stelle prüft es: Das Zertifikat wird durch den Berater ausgestellt. Es gibt keine unabhängige Überprüfung der umgesetzten Massnahmen.
- Nicht nach Norm umgesetzt: Vermutlich sind nicht alle Anforderungen der ISO 27001 vollständig erfüllt, was schwerwiegende Sicherheitslücken zur Folge haben kann.
- Nichtkonformitäten werden nicht geschlossen: Fehler und Abweichungen, die bei einem echten Audit aufgedeckt würden, bleiben unbeachtet.
- Wird von Kunden und Lieferanten nicht akzeptiert: Da solche Zertifikate nicht von akkreditierten Stellen ausgestellt werden, sind sie auch im geschäftlichen Umfeld nicht anerkannt und führen zum Vertrauensverlust bei Kunden und Lieferanten.

WARUM EIN (TEURES) ZERTIFIZIERUNGSAUDIT?

Viele Unternehmen fragen sich, warum sie ein teures Zertifizierungsaudit bei einer akkreditierten Stelle durchführen sollten, wenn es doch vermeintlich günstigere Alternativen gibt. Die Antwort ist einfach: Nur ein echtes Zertifikat bietet die nötige Sicherheit und Glaubwürdigkeit.

- Zertifizierungskette: Die Akkreditierung läuft über eine international anerkannte Zertifizierungskette, die bis zur übergeordneten IAF zurückverfolgt werden kann (International Accreditation Forum, https://iaf.nu > Schweizerische Akkreditierungsstelle, www.sas.admin.ch > Akkreditierte Organisation). Diese Struktur gewährleistet die Unabhängigkeit und Professionalität der Prüfung.
- Zugewiesener Auditor mit Fachkenntnissen: Der Auditor, der das Audit durchführt, muss über Fachkenntnisse und Erfahrung in dem zu prüfenden Bereich verfügen. Dies stellt sicher, dass das Audit fundiert und praxisnah durchgeführt wird.
- Weltweit anerkanntes Zertifikat: Ein Zertifikat, das von einer akkreditierten Stelle ausgestellt wird, ist weltweit anerkannt und geniesst dementsprechend Vertrauen.
- Leistungsausweis: Ein echtes Zertifikat ist ein Leistungsausweis für das Unternehmen. Es zeigt, dass das Unternehmen in der Lage ist, hohe Standards im Bereich der Informationssicherheit umzusetzen und zu halten.

AM ENDE DES TAGES GILT:

Seien Sie vorsichtig bei günstigen Pauschalangeboten, die eine schnelle und einfache Lösung versprechen. Ein ISMS ist mit Aufwand verbunden und wird nicht «geschenkt». Eine akkreditierte Stelle bringt das notwendige Know-how und die Unabhängigkeit mit, um ein fundiertes, wertvolles Zertifikat auszustellen. Ein offizielles Zertifikat ist nicht nur ein Nachweis für die Erfüllung der Norm-Anforderungen, sondern auch ein Leistungsnachweis für das gesamte Unternehmen. ●

Andreas Wisler ist Inhaber und Senior Security Consultant der goSecurity AG ISO 27001, 27701 und 22301 Lead Auditor

www.goSecurity.ch | www.27001.blog | www.angriffslustig.ch