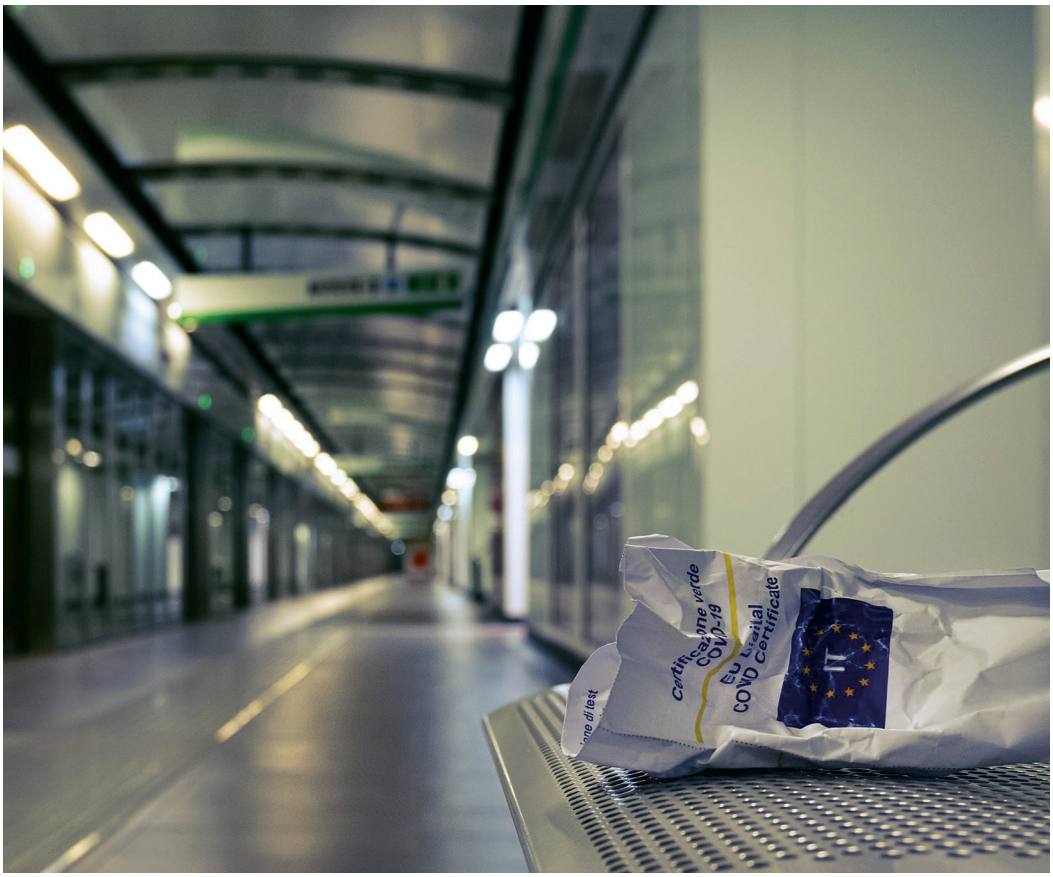

Bild: Pixabay

Wie vermeintliche Zertifikate Unternehmen in die Irre führen können.

Zertifikat ist nicht gleich Zertifikat

In unserer digitalisierten Welt wird Informationssicherheit zu einem entscheidenden Wettbewerbsfaktor. Unternehmen sehen sich vermehrt mit Anforderungen konfrontiert, ihre Prozesse und Systeme nach anerkannten Normen zertifizieren zu lassen.

Eine der prominentesten Normen im Bereich der Informationssicherheit ist die ISO 27001, die die Implementierung eines Informationssicherheits-Managementsystems (ISMS) verlangt. Ein Zertifikat ist der erfolgreiche Nachweis, alles optimal umgesetzt zu haben.

Doch nicht jedes ISO-Zertifikat ist das, was es zu sein scheint. Bei unserem eigenen Zertifizierungs-Audit 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 entsprach. Warum ist also ein Zertifikat nicht gleich ein Zertifikat? Und welche Risiken bergen diese vermeintlich günstigen Angebote?

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

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

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. Diese Angebote folgen oft einem Muster:

- 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 zertifizierenden Stelle selbst durchgeführt – was an sich schon problematisch ist, da hier keine Unabhängigkeit gewährleistet ist.
- 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. Doch kann eine echte, unabhängige Zertifizierung wirklich garantiert werden?

Und all das zu einem unschlagbar günstigen Pauschalpreis. Ein derartiges Lockvogel-Angebot erscheint auf den ersten Blick verführerisch, insbesondere für Unternehmen, die unter starkem Zeit- und Kostendruck stehen. Doch was auf den ersten Blick wie ein attraktives Angebot aussieht, birgt erhebliche Risiken.

Unsere Erfahrungen – Lieferanten-Audits und deren Risiken

Im Rahmen unserer eigenen Audits, besonders bei Lieferantenaudits im Auftrag unserer Kunden, stossen wir immer wieder auf derartige vermeintliche Zertifikate. Diese sind zwar auf den ersten Blick formal korrekt, entpuppen sich jedoch bei genauerer Betrachtung als unzureichend oder gar wirkungslos.

Die Risiken sind dabei vielfältig:

- Keine externe Stelle prüft es: Oft wird das Zertifikat von der eigenen Organisation oder einer nicht akkreditierten Stelle ausgestellt. Es gibt keine unabhängige Überprüfung der Normkonformität.
- Vermutlich nicht alles nach Norm umgesetzt: Es wird vermutet, dass die Anforderungen der ISO 27001 nicht vollständig erfüllt werden, was schwerwiegende Sicherheitslücken zur Folge haben kann.
- Nicht-Konformitäten werden nicht geschlossen: Fehler und Abweichungen, die bei einem echten Audit aufgedeckt würden, bleiben unbeachtet, da kein Mechanismus zur Schliessung dieser Nicht-Konformitäten besteht.

– Wird von Kunden und Lieferanten nicht akzeptiert: Da solche Zertifikate meist nicht von akkreditierten Stellen ausgestellt werden, sind sie auch im geschäftlichen Umfeld nicht anerkannt und führen zu Vertrauensverlust bei Kunden und Lieferanten.

Ein vermeintliches Zertifikat mag kurzfristig als Lösung erscheinen, doch langfristig entstehen erhebliche Risiken – sowohl für die Sicherheit des Unternehmens als auch für dessen Reputation.

Unsere Erfahrungen – Scheinbare Erfüllung der Normanforderungen

In der Praxis zeigt sich zudem, dass bei solchen vermeintlichen Zertifizierungen oft nur das implementiert wird, was ohnehin schon gut funktioniert.

Die weniger gut organisierten Bereiche oder Prozesse bleiben unangetastet. Dies führt zu erheblichen Problemen:

– Es wird nur das gemacht, was man schon gut macht: Es erfolgt keine ganzheitliche Analyse und Verbesserung des gesamten Managementsystems.
– Management-System auf einem schlechten Stand: Das ISMS ist in einem mangelhaften Zustand und wird nicht weiterentwickelt, da keine echten Audits stattfinden, die Verbesserungsbedarf aufzeigen.
– Nicht alle Norm-Anforderungen umgesetzt: Wesentliche Anforderungen der Norm bleiben unerfüllt, welche gegen aussen aber nicht sichtbar sind.
– Kein Druck durch externe Kontrolle: Da keine unabhängige, externe Kontrolle erfolgt, gibt es keinen Druck, das ISMS kontinuierlich zu verbessern oder auf einem hohen Niveau zu halten.

Die fehlende externe Kontrolle und der mangelnde Druck führen dazu, dass das ISMS nicht den gewünschten Nutzen bringt und das Unternehmen anfällig für Sicherheitsrisiken machen kann.

Warum ein (teures) Zertifizierungs-Audit?

Viele Unternehmen fragen sich, warum sie ein teures Zertifizierungs-Audit 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.

Ein akkreditiertes Zertifizierungsverfahren folgt einer strengen, transparenten Struktur:

– Zertifizierungskette: Die Akkreditierung läuft über eine international anerkannte Zertifizierungskette, die bis zur internationalen Akkreditierungsorganisation (IAF) zurückverfolgt werden kann (beispielsweise International Accreditiation Forum, https://iaf.nu → Schweizerische Akkreditierungsstelle, https://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 das Vertrauen von Kunden, Lieferanten und Partnern.
– 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.

Fazit: Vorsicht bei günstigen Pauschal-Angeboten

Am Ende des Tages gilt: Sei vorsichtig bei günstigen Pauschal-Angeboten, 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 von Normen, sondern auch ein Leistungsnachweis für das gesamte Unternehmen.

Für Unternehmen ist es entscheidend, ihre Lieferanten sorgfältig zu prüfen und nur offizielle Zertifikate zu akzeptieren, die von akkreditierten Stellen ausgestellt wurden. Denn letztlich ist ein Zertifikat nicht gleich ein Zertifikat – es ist die Qualität und Glaubwürdigkeit, die den Unterschied macht.