Garantiert sicher: Cybersecurity-Zertifizierungen für Unternehmen

ESET 100% Made in EU IT-Security

Digital Security
Progress. Protected.

ESET.DE | ESET.AT | ESET.CH

Sicherheitslücken und Hacker-Angriffe sind ein hohes Risiko für den Geschäftsbetrieb von Unternehmen. Sie führen zu erheblichen finanziellen Schäden und einem Vertrauensverlust bei Kunden und Geschäftspartnern. Eine wichtige Gegenmaßnahme sind Cybersecurity-Zertifizierungen. Sie beweisen allen Stakeholdern das Engagement für Informationssicherheit und optimieren zugleich die internen Maßnahmen für IT-Security.

Was ist eine Cybersecurity-Zertifizierung?

Eine Cybersecurity-Zertifizierung ist ein Verfahren, mit dem Unternehmen die Einhaltung bestimmter Anforderungen an IT-Sicherheit nachweisen können. Grundlage der meisten Zertifizierungen für Unternehmen sind Managementsysteme wie beispielsweise für Risikomanagement oder Informationssicherheitsmanagement. Solche Systeme normieren Tätigkeiten, Instrumente und Methoden der Unternehmensführung (Governance).

Ein Unternehmen muss dieses Managementsystem zunächst in seine Prozesse integrieren. Dafür gibt es eine Reihe von nationalen und internationalen Standards und Normen, die das Managementsystem genau beschreiben. Anschließend meldet sich das Unternehmen bei einer Zertifizierungsstelle an, die das Erfüllen der Standards und Normen in einem Audit überprüft. Bei einem erfolgreichen Audit erhält das Unternehmen ein gebührenpflichtiges Zertifikat, das in festgelegten Abständen erneuert werden muss.

Welche Cybersecurity-Zertifizierungen sind wichtig für Unternehmen?

Es gibt eine Reihe von Cybersecurity-Zertifizierungen, die sich an Unternehmen richten. Entscheidend sind hier vor allem vor allem die ISO 27001 und der damit kompatible IT-Grundschutz sowie einige branchenspezifische Normen. Darüber hinaus gibt es weitere, nur in einzelnen Ländern genutzte Security-Standards und-Zertifizierungen. Sie sind vor allem interessant für Unternehmen, die in den jeweiligen Ländermärkten Niederlassungen haben und werden hier nicht weiter erwähnt.

Die Basis: ISO 27001

Eine grundlegende und international anerkannte Zertifizierung für Cybersecurity ist die nach dem Standard ISO 27001. In dieser Norm geht es um den Aufbau und die fortlaufende Verbesserung eines Informationssicherheit-Managementsystems (ISMS). Es dokumentiert alle Verfahren und Regeln, mit denen die Informationssicherheit gesteuert wird.

Organisationen erhalten damit klare Leitlinien, die sie allerdings an ihre spezifischen Anforderungen anpassen müssen. Die Norm selbst ist sehr allgemein gehalten und richtet sich an jede Art von Organisation. Sie kann damit ihre Cybersecurity systematisch und strukturiert optimieren. Dabei läuft sie nicht Gefahr, wichtige Aspekte zu vernachlässigen.

Die ISO-Zertifizierung vertritt deshalb einen generischen und prozessorientierten Ansatz. Für die erfolgreiche Zertifizierung des Unternehmens ist deshalb zuerst eine vollständige Risikoanalyse nötig, die letztlich alle einzuführenden Maßnahmen ergibt.

Eine weitere Eigenheit der ISO Norm: Sie macht keine Vorgaben für angemessene Cybersecurity-Maßnahmen. Die Unternehmen müssen sie selbst entwickeln und dabei den Stand der Technik berücksichtigen – ein hoher Aufwand. Eine Hilfe dabei sind die weiteren Normen der ISO-27000-Reihe, vor allem die branchenspezifischen Substandards und die Standards für bestimmte technische Gebiete der Informationssicherheit.

Die Zertifizierung gilt für maximal drei Jahre, danach müssen Sie Unternehmen mit einem erneuten Audit verlängern. Häufig sind dabei auch Anpassungen des Managementsystems sowie der daraus abgeleiteten

Cybersecurity-Maßnahmen notwendig – leider sind Cyberkriminelle sehr kreativ und finden neue Angriffswege.

Eine regelmäßig erneuerte ISO-27001-Zertifizierung bietet den Unternehmen erhebliche Vorteile: Sie signalisiert der Öffentlichkeit und damit dem eigenen Kundenstamm die hohe Bedeutung von Informationssicherheit für das Unternehmen und schafft damit Vertrauen. Das gilt nicht nur für das zertifizierte Unternehmen, sondern auch für Geschäftspartner. Sie erkennen die hohe Bedeutung von Cybersecurity zum Beispiel durch den Einsatz von ISO-zertifizierten Zulieferern oder Dienstleistern.

In der Praxis ist die ISO 27001 zu einer Art Pflicht geworden, vor allem für B2B-Unternehmen. Wenn sie nicht zertifiziert sind, erhalten sie oft keine Aufträge. Dies gilt besonders in kritischen Branchen wie der Finanz- und Versicherungswirtschaft, dem Gesundheitswesen oder der Energieversorgung. Kurz: Eine Zertifizierung nach ISO 27001 ist häufig Voraussetzung für den wirtschaftlichen Erfolg.

Die Zertifizierung durch das BSI

Durch den hohen Aufwand für die ISMS-Einführung ist eine ISO-27001-Zertifizierung für kleine und viele mittelgroße Unternehmen oft nur schwer umzusetzen. Es gibt allerdings eine Alternative: Die mittelstandskompatiblen Angebote des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bestehen aus dem IT-Grundschutz und eine daran angepasste ISO-Zertifizierung.

Der IT-Grundschutz ist eine vom BSI entwickelte Vorgehensweise bei der Umsetzung von Cybersecurity. Das sehr umfangreiche und detailgenaue IT-Grundschutz-Kompendium gilt für sämtliche Branchen und wird regelmäßig an neue Technologien und Methoden angepasst. Es ist im Kern eine Sammlung aus Best-Practices. Sie zielt auf Unternehmen mit begrenzten IT-Budgets, die Security möglichst effizient verwirklichen möchten.

Auf Basis des IT-Grundschutzes bietet das BSI eine Zertifizierung nach ISO 27001 an. Der Vorteil gegenüber einer reinen ISO-Zertifizierung: Der IT-Grundschutz ist maßnahmenorientiert. Durch den Detailgrad des Grundschutzkompendiums sind Fehler bei der Umsetzung praktisch ausgeschlossen. Die Unternehmen können also bewährte Maßnahmen für ihre Branche und ihren Geschäftsbetrieb einfach übernehmen. Dadurch entfällt auch die Pflicht zu einer vollständigen Risikoanalyse. Sie ist lediglich in Unternehmen notwendig, die einen erhöhten Schutzbedarf haben.

Trotz aller Vereinfachungen gegenüber dem ISO-Standard ist der IT-Grundschutz für viele kleinere Betriebe zu aufwendig und komplex. Eine Alternative ist der Standard VDS 10000 vom Verband der deutschen Versicherungswirtschaft (VDS). Er zielt auf ein angemessenes Schutzniveau für KMU, ohne das Unternehmen organisatorisch oder finanziell zu überfordern. Die Norm ist aufwärtskompatibel zu ISO 27001 und IT-Grundschutz; bei Bedarf ist sie also die Basis für deren Umsetzung. Zudem ist die Zertifizierung ist einfacher: Auf eine Online-Selbstauskunft folgt ein eintägiges Audit durch Spezialisten das VDS.

Risikomanagement nach ISO 31000

Unternehmen aus kritischen Branchen und mit erhöhtem Schutzbedarf benötigen in aller Regel auch ein Risikomanagement. Die dafür geltende Norm ISO 31000 macht Vorgaben für Risikoanalysen und ein Risikomanagementsystem. Ähnlich wie ISO 27001 ist der Ansatz dieser Normen nicht branchen- oder sektorspezifisch. Ein Unternehmen muss die Vorgaben an ihre eigenen Anforderungen anpassen.

Business Continuity Management nach ISO 22301

Großflächige Stromausfälle, Naturkatastrophen, Kriege und Cyberattacken – viele Notsituationen können den Geschäftsbetrieb vollständig lahmlegen. Unternehmen sollten darauf vorbereitet sein und Business Continuity Management (BCM) nutzen. Es erweitert das Risikomanagement um Maßnahmen für die Fortführung des Geschäftsbetriebs unter Krisenbedingungen.

Diesem Thema widmet sich die ISO 22301. Sie ist ein Leitfaden für Business-Continuity-Managementsysteme für Krisen- und Notfallsituationen. Sie sorgen dafür, dass wichtige Geschäftsfunktionen geschützt werden und die Auswirkungen möglichst gering sind. Grundsätzlich gilt: Jedes Unternehmen sollte sich auf extreme Notfälle vorbereiten, eine Zertifizierung nach ISO 22301 ist überlegenswert – auch hier gibt es viele

Best-Practices, deren Bescheinigung das Vertrauen in ein Unternehmen erhöht.

Welche Zertifizierungen sind für meine Branche wichtig?

In einigen Branchen sind Zertifizierungen verpflichtend für die Auftragsvergabe oder sogar durch gesetzliche Vorgaben unvermeidlich. Hier gibt es zum Teil besondere Anforderungen und Maßnahmen für die jeweilige Branche. Besonders wichtig in der deutschen Wirtschaft sind drei Zertifizierungen für Unternehmen der kritischen Infrastrukturen, die Autoindustrie und Versorgungsunternehmen.

Kritische Infrastrukturen: KRITIS-Nachweis

Die Betreiber kritischer Infrastrukturen müssen nachweisen, dass ihre IT-Sicherheit dem aktuellen Stand der Technik entspricht. Unternehmen gehören laut Gesetz zu den kritischen Infrastrukturen, wenn sie mehr als 500.000 Personen versorgen und in den folgenden Branchen arbeiten: Strom- und Gasversorger, Wasser, Ernährung, IT und Telekommunikation, Gesundheit, Transport und Verkehr, Finanz- und Sicherungswesen.

Die KRITIS-Verordnung beschreibt, welche Anlagen in den jeweiligen Sektoren als kritisch gelten und fordert von den Betreibern einen Nachweis über den Schutz ihrer Informationstechnik. Hinzu kommt laut IT-Sicherheitsgesetz die Pflicht, ein System zur Angriffserkennung zu etablieren und einen entsprechenden Nachweis vorzulegen.

Autoindustrie: TISAX-Assessment

In der Automobilbranche sind Entwicklungskooperationen weit verbreitet. Die großen Autohersteller (OEMs) beziehen ihre Zulieferer eng ein, wodurch ein intensiver Datenaustausch in beiden Richtungen notwendig wird. Deshalb erwarten sie von Zulieferern ein hohes Niveau der Informationssicherheit, der im Anforderungskatalog das Information Security Assessment (ISA) niedergelegt wurde. Entwickelt haben ihn die ENX Association, ein Zusammenschluss europäischer Unternehmen in der Automobilbranche und der deutsche VDA (Verband der Automobilindustrie). Sie haben den Katalog aus der ISO 27001 abgeleitet und zusätzlich an die Bedürfnisse der Branche angepasst.

Bisher hat jeder Hersteller seine eigenen Lieferanten überprüft. Dies führte jedoch zu Mehrfachprüfungen, da die meisten Zulieferer für mehrere OEMs arbeiten. Deshalb haben die beiden Verbände den Prüf- und Austauschmechanismus TISAX (Trusted Information Security Assessment Exchange) aufgebaut. Dort werden die Ergebnisse eines Assessment allen Interessenten aus der Branche auf einer Online-Plattform angeboten.

IT-Sicherheitskatalog für Versorger

Für Strom- und Gasnetzbetreiber ist seit 2018 eine Zertifizierung nach dem IT-Sicherheitskatalog der Bundesnetzagentur Pflicht. Auch hier geht es um ein ISMS ähnlich ISO 27001, das jedoch mit spezifischen Standards für die Steuerung von Energienetzen erweitert worden ist.

Welche Kosten hat die Zertifizierung?

Die genauen Kosten für eine Zertifizierung sind nur schwer anzugeben, da in jedem Unternehmen der Aufwand für Vorbereitung und Umsetzung unterschiedlich hoch ist. Das eigentliche Audit kostet aller Erfahrung nach ab etwa 6000 Euro für kleine und bis zu 25.000 Euro für größere Unternehmen.

Mit rund 3000 Euro ist die BSI-Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz deutlich kostengünstiger. Außerdem ist hier wegen der detailgenauen Vorgaben der Aufwand für die Implementation geringer. Bei anderen Zertifizierungen sind die Kosten in etwa vergleichbar mit der einer ISO-2701-Zertifizierung.

Ist eine Zertifizierung empfehlenswert?

Grundsätzlich ist eine Zertifizierung der Sicherheitsmaßnahmen empfehlenswert, sie wird jedoch viele Unternehmen überfordern – vor allem kleinere Mittelständler. Sie sollten die weniger komplexen Alternativen zu ISO 27001 wie den IT-Grundschutz für mittelgroße Unternehmen oder VDS 10.000 für kleinere Unternehmen ins Auge fassen. Sie begrenzen damit den Aufwand für die Entwicklung von Maßnahmen und die Kosten für die Zertifizierung selbst. Die wichtigsten Gründe für eine Zertifizierung sind:

Senken von Risiken: Eine strukturierte und an Standards ausgerichtete Vorgehensweise in der Cybersecurity senkt das Risiko von Schäden und Kosten. Das Unternehmen kann sich sicher sein, den aktuellen technischen Stand zu verwirklichen und Best-Practices einzusetzen.

Effizienzgewinne: Die Einführung standardisierter und zertifizierbarer Prozesse verbessert generell die internen Abläufe und hilft den Unternehmen dabei, eine bessere Sicherheitsstrategie entwickeln.

Wettbewerbsvorteile: Eine Security-Zertifizierung ist ein gutes Marketingargument gegenüber Kunden sowohl im B2C- als auch im B2B-Sektor. Die Zertifizierung schafft Vertrauen und erleichtert den Kunden die Auswahl der Produkte und Services.

Haftung: Die Zertifizierung eines ISMS vermeidet im Schadenfall unter Umständen ein Organisationsverschulden und senkt somit die persönliche Haftung der Geschäftsführung.

Datenschutz: Die Zertifizierung erleichtert es, europäische Datenschutz Grundverordnung zu erfüllen.

Nachweise: Die Zertifizierung dient als Nachweis für die Befolgung von grundlegenden Cybersecurity-Maßnahmen in Verträgen, rechtlichen Auseinandersetzungen oder bei Nachfragen von Behörden.

Welcher Zertifizierer ist empfehlenswert?

Wenn ein Unternehmen auf der Suche nach einem empfehlenswerten Zertifizierer ist, sollte es sich bei der Deutschen Akkreditierungsstelle informieren. Das ist die nationale Akkreditierungsbehörde für Zertifizierungen in allen Bereichen der Wirtschaft. Unternehmen finden dort in der „Datenbank der akkreditierten Stellen“ einen Überblick über sämtliche Zertifizierungsstellen für Managementsysteme.

Die Auswahl ist groß, allein für die ISO 27001 gibt es im Moment in Deutschland weit über 35 unterschiedliche Zertifizierer. Das sind unter anderem die bekannten Prüforganisationen TÜV und Dekra, Prüfunternehmen wie KPMG und viele weitere Zertifizierer, die sich auf Cybersecurity spezialisiert haben.

FAZIT:

Vertrauen schaffen mit Zertifizierungen

Unabhängig von Branche und Größe ist für jedes Unternehmen eine anerkannte Zertifizierung empfehlenswert. Branchenspezifische Zertifizierungen sind zum Teil unvermeidlich, da die Auftragsvergabe immer stärker davon abhängt. Es ist sinnvoll, sie gleichzeitig mit einer branchenübergreifenden Zertifizierung zu verwirklichen. Unternehmen können mit beiden Arten von Zertifizierungen Risiken senken und das Vertrauen der Kunden in ihrer Geschäftstätigkeit stärken.

ÜBER ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Unternehmensgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihr Netzwerk mithilfe von Cloud Sandboxing frei von Zero Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungsprodukte unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen.

Unsere XDR-Basis mit Endpoint Detection and Response Lösung, Frühwarnsysteme (bspw. Threat Intelligence) und dedizierte Services ergänzen das Angebot im Hinblick auf Forensik sowie den gezielten Schutz vor Cyberkriminalität und APTs. Dabei setzt ESET nicht allein auf modernste Technologien, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

ZUFRIEDENE KUNDEN

BVB 09 Champion Partner

Seit 2019 ein starkes Team
auf dem Feld und digital

Allianz Suisse

Seit 2016 durch ESET geschützt
Mehr als 4.000 Postfächer

ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT

Secur|Ty made in EU
Trust Seal
www.teletrust.de/itsmie

ESET wurde das Vertrauenssiegel
„IT Security made in EU" verliehen

ISO 9001 SGS

ISO/IEC 27001 SGS

Unsere Lösungen sind nach den Qualitäts- und Informationssicherheitsstandards ISO 9001:2015 und ISO/IEC 27001:2013 zertifiziert

ESET IN ZAHLEN

110+ Mio.
Geschützte Nutzer weltweit

400k+
Geschützte Unternehmen

195
Länder & Regionen

13
Forschungs- und Entwicklungszentren weltweit

welivesecurity by ESET

ESET Digital Security Guide

ESET Deutschland GmbH | Spitzweidenweg 32 | 07743 Jena | Tel.:+49 3641 3114 200

ESET.DE | ESET.AT | ESET.CH