PROZESSBESCHREIBUNG

Durchführung eines IT-Grundschutzchecks

Stand: NOVEMBER 2024

Unsere Kernkompetenz – Das Auditieren von IT-Grundschutzbausteinen und Mindeststandards des BSI

Unsere Ausführungsstrategie im Detail

Um unserem eigenen Qualitätsanspruch gerecht werden zu können, haben wir uns bei der Durchführung von IT-Sicherheitsdienstleistungen in der DIGITAL SEC einen standardisierten Prozess auferlegt, den wir Ihnen im Folgenden aufzeigen möchten.

Unser Anspruch:

„Alle unsere Ergebnisse müssen praxistauglich und umsetzbar sein!"

Dabei gilt es die umsetzende Fachseite mit „ins Boot zu nehmen" und gemeinsam realistische Lösungswege zu finden, um eine entdeckte Schwachstelle zeitnah zu schließen. An Ende unserer Dienstleistung erhält der Auftraggeber unsere Ergebnisse, zusammen mit der schriftlichen Abnahme durch die Interviewpartner.

Schritt 1 - Terminabsprache und Vorbereitung

Mit den von Ihnen benannten Interviewpartner nehmen wir Kontakt auf und bieten wahlweise mehrere Audittermine an. Bei diesem ersten Kontakt erläutern wir den Inhalt und den Umfang des Audits und klären zweifelsfrei ab, ob unser/e Gesprächspartner/-in sich für diesen IT-Grundschutzcheck zuständig fühlt und auskunftsfähig ist. Ansonsten werden von uns alternative Ansprechpartner erfrag. Die so ermittelten Interviewpartner erhalten von uns eine spezielle Ausfertigung des zu besprechen Grundschutzschecks, mit der Bitte, sich einzulesen.

Schritt 2 - Durchführung des GSCs (Istzustand aufnehmen)

Unmittelbar vor dem Interview wird der Auftraggeber von uns gebeten in seinem WEAKLESS (sofern vorhanden) den entsprechenden Baustein zu sperren (siehe Menüpunkt „CHECK-OUT"), um spätere Datenkollisionen und Eingabeverluste zu vermeiden. WEAKLESS ist ein von uns entwickeltes IT-Grundschutzverwaltungs-Tool mit einem automatisierten ToDo-Tracking (Nachverfolgung - siehe www.WEAKLESS.de). Das Tool kann von uns auf Anfrage erworben werden. Neukunden ab einem Auftrag von 20 Grundschutzchecks stellen wir WEAKLESS kostenfrei zur Verfügung.

Die IT-Grundschutzchecks werden von uns in Interviewform durchgeführt und grundsätzlich online, bei Bedarf auch vor Ort stattfinden. Unsere IT-Grundschutzchecks werden von uns als Video-Konferenzen über unser Kollaboration-Tool „STACKFIELD" durchgeführt. Dabei erfolgt die Daten- und Videoübertragung Ende-zu-Ende-verschlüsselt und mit einer 2-Faktor-Authentisierung. Stackfield schützt die Daten unserer Kunden DSGVO-konform mit dem Serverstandort Deutschland, in ISO-27001 zertifizierten Rechenzentren (https://www.stackfield.com/de/security).[1]

Dabei wird der Bildschirm geteilt, so dass alle Teilnehmer der Online-Dokumentation des gemeinsam besprochenen Istzustandes folgen können. Somit können Missverständnisse bereits in der Entstehung vermieden werden. Ist ein IT-Grundschutzcheck sehr umfangreich und überschreitet die Dauer von 2 Stunden, so wird aufgrund der sinkenden Konzentrationsfähigkeit der Beteiligten ein Fortsetzungstermin vereinbart.

Fühlt sich der Interviewpartner nicht in der Lage eine konkrete Anforderung zu beantworten, wird wie folgend verfahren:

Option A:
Der Interviewpartner ist zuständig, muss aber zuerst Hintergrundinformationen einholen, um seine Antworten geben zu können.

Unsere Vorgehensweise
Der Sachverhalt wird als Istzustand notiert. Durch unsere Qualitätssicherung (siehe Schritt 5) wird der Interviewpartner schriftlich im Nachgang gebeten, seine Antwort nachzureichen.

Option B:
Der Interviewpartner fühlt sich für die Darstellung des IST-Zustandes dieser Anforderung nicht zuständig.

Unsere Vorgehensweise
Der Sachverhalt wird als Istzustand notiert. Wir nehmen im Nachgang zum Audit mit den vom Interviewpartner alternativ genannten Ansprechpartnern Kontakt auf, um den fehlenden IST-Zustand zu ermitteln.

[1] ISO-27001-Zertizierung der Stackfield GmbH: https://www.stackfield.com/2t3xygw-3oj115-e1b029d3522d4eb
Whitepaper zur Ende-zu-Ende-Verschlüsselung: https://www.stackfield.com/2t3xygw-nsogh1-aac1398d1dc745c
Vertrag zur Auftragsverarbeitung: https://www.stackfield.com/de/help/vertrag-zur-auftragsverarbeitung-2012
TOMs: https://www.stackfield.com/de/av-tom

Option C:
Der Interviewpartner versteht die Anforderung nicht.

Unsere Vorgehensweise
Der Sachverhalt wird als Istzustand notiert. Durch unsere Qualitätssicherung (siehe Schritt 6) wird der Interviewpartner schriftlich im Nachgang erläuternde Informationen nachgereicht.

Schritt 3 - Umsetzungsbewertung des SOLL-IST-Vergleiches

Erläuterung zum Verständnis:

In Anlehnung an das „alte" IT-Grundschutztool des BSI bedeutet im Auditbogen

- die Farbe Grün: „Diese Anforderung ist umgesetzt",
- die Farbe Gelb: „Diese Anforderung ist nur teilweise umgesetzt",
- die Farbe Rot: „Diese Anforderung ist nicht umgesetzt"
- die Farbe Blau: „Diese Anforderung ist in unserem Hause nicht von Relevanz und daher entbehrlich".

Nach der Dokumentation des IST-Zustandes wird der Umsetzungsgrad dieses Zustandes gemeinsam diskutiert und eine vorläufige Bewertung festgelegt.

Schritt 4 - ToDos erzeugen

Kann der Befragte den IST-Zustand einer Anforderung zweifelsfrei beschreiben und ist die SOLL-Anforderung des IT-Grundschutzes, gemessen an diesem IST-Zustand, nicht oder nur teilweise umgesetzt, so wird zum festgestellten Delta ein oder mehrere ToDos erstellt, die geeignet sind, dieses Delta zu beseitigen. Zur Verdeutlichung: Jedes Delta ist eine potenzielle Schwachstelle!

Alle während der IT-Grundschutzchecks entstehenden ToDos werden in einer zentralen Liste in WEAKLESS gesammelt und bei einer zeitlichen Überschreitung des Wiedervorlagetermins farbig gekennzeichnet. Besitzt der Kunde keine WEAKLESS-Lizenz, findet er seine ToDos in den finalen Auditbögen seiner Grundschutzchecks. Zusätzlich erhält er von uns eine Zusammenstellung seiner ToDos aus allen Audits seines Gesamtauftrages.

Schritt 5 - 1. QS-Stufe durch den Auditor nach dem Interview

In Abstimmung mit einem 2. Auditor werden die dokumentierten Ergebnisse diskutiert und sowohl inhaltlich als auch formal geschärft.

Schritt 6 - 2. QS durch einen unbeteiligten sachkundigen Dritten

Die Dokumentation des IT-Grundschutzchecks wird von einem fachkundigen Dritten, der beim Interview bewusst nicht anwesend war, gegengelesen und bewertet. Dabei arbeitet dieser eine von der DIGITAL SEC erstellte QS-Prüfliste ab und kommentiert Stellen, an denen er als außenstehender Leser Verständnisprobleme mit dem dokumentierten IST-Zustand hat. Beispielhaft sei hier eine unzureichend umfängliche Beantwortung der Anforderung genannt, Abkürzungen, die nicht zuvor erklärt wurden oder offengebliebene weitere Fragen.

Hat der QS-Prüfer Beanstandungen, so notiert er seine konkreten Anmerkungen im Auditbogen und bittet die entsprechenden Ansprechpartner schriftlich um Beantwortung. Dieser Prozess wird solange wiederholt, bis für den QS-Prüfer keine Unklarheiten mehr bestehen.

Schritt 7 - Freigabe des GSC Bogens durch Interviewpartner

Als Nächstes erhält der/die Interviewpartner/-in die Dokumentation des IT-Grundschutz-checks mit der Bitte um Freigabe.

Schritt 8 - Übergabe der Dokumentation des IT-Grundschutzchecks an den Auftraggeber

Nach der Freigabe des Auditbogens durch den Interviewpartner fertigt unser GSC-Disponent zu diesem IT-Grundschutzcheck einen Abschlussbericht. Dieser beinhaltet die Dokumentation des IT-Grundschutzchecks mit einer deutlichen Kennzeichnung der identifizierten Schwach-stellen (nicht umgesetzte Anforderungen), eine Liste der vereinbarten ToDos sowie eine Berechnung des Umsetzungsgrades dieses IT-Grundschutzchecks.

Schritt 9 - Freigabe des GC Bogens durch den Auftraggeber

Nachdem der Auftraggeber die Dokumentation des IT-Grundschutzchecks erhalten und geprüft hat, wird er gebeten, diesen IT-Grundschutzcheck der DIGITAL SEC gegenüber als „erfolgreich durchgeführt" freizugeben.

Projektabwicklung und -lieferungen

Die Lieferung der Dokumentation eines finalisierten IT-Grundschutzchecks erfolgt wahlweise per E-Mail oder Download in einer AES-256 verschlüsselten ZIP-Datei. Zu Beginn des Projektes wird mit dem Auftraggeber ein gemeinsamer Schlüssel hierzu ausgetauscht.

Wir bieten Ihnen zur Besprechung der Abwicklung und zu Details des Projektverlaufs zu Anfang des Projektes ein **kostenfreies** Kick-Off-Meeting.

Anmerkung

Nach jedem Import und im Verlauf des gesamten Auftrages ist der Auftraggeber in der Lage, in seinem WEAKLESS durch den Aufruf des Menüpunktes „Statistik" sich über den Fortschritt der IT-Grundschutzchecks und die Umsetzungsgrade der einzelnen Bausteine einen Gesamtüberblick zu verschaffen.

Erfahrungsgemäß gibt es bei bestimmten Bausteinen mehrere Zielobjekte, deren IST-Zustände sich in Bezug auf die Umsetzung einzelnen Anforderungen stark voneinander unterscheiden und daher nicht in einem einzigen IT-Grundschutzcheck gemeinsam abgebildet werden können. Hier ist es ratsam den Baustein in mehrere IT-Grundschutzchecks aufzuteilen. Beispielhaft sei hier der Baustein „INF.1 Allgemeines Gebäude" oder der Baustein „APP.4.3 Relationale Datenbanksysteme".

Die dadurch eventuell zusätzlich benötigten IT-Grundschutzchecks bieten wir Ihnen zu den gleichen Konditionen an, wie die von Ihnen ursprünglich gewünschten IT-Grundschutzchecks.

Dienstleistungsgeber

Firma DIGITAL SEC - Cyber Security Strategy

Iversheimerstraße 29
53894 Mechernich-Wachendorf

https://digital-sec.de
support@digital-sec.de

Begründer und Inhaber: Dietmar Lorenz-Herweg
Geschäftsführerin: Julia Westermann

Qualifikationen unseres Auditors

- 45 Jahre Berufserfahrung im öffentlichen Dienst, davon
- 25 Jahre als Informationssicherheitsbeauftragter in
- 8 verschiedenen Bundesbehörden darunter
- 3 Jahre in der IT-Sicherheitsberatung des BSI,
- 8 Jahre in der Bundesfinanzaufsicht (BaFin) und
- 4 Jahre im Bundesministerium für Familie (BMFSFJ)
- Zertifizierter IT-Sicherheitsbeauftragter in der öffentlichen Verwaltung (ISBöV)
- BSI-Zertifikatsstufe 3 (EXPERT), Zertifikatsnummer 4 von 4
- sicherheitsüberprüft nach SÜG3
- Bachelor in Wirtschaftsinformatik (B.Sc.)
- Master of Computer Science (M.Comp.Sc.)
- Senior Consultant – Ministerialer Regierungsdirektor a.D.