NESEC

Gesellschaft für angewandte Netzwerksicherheit mbH

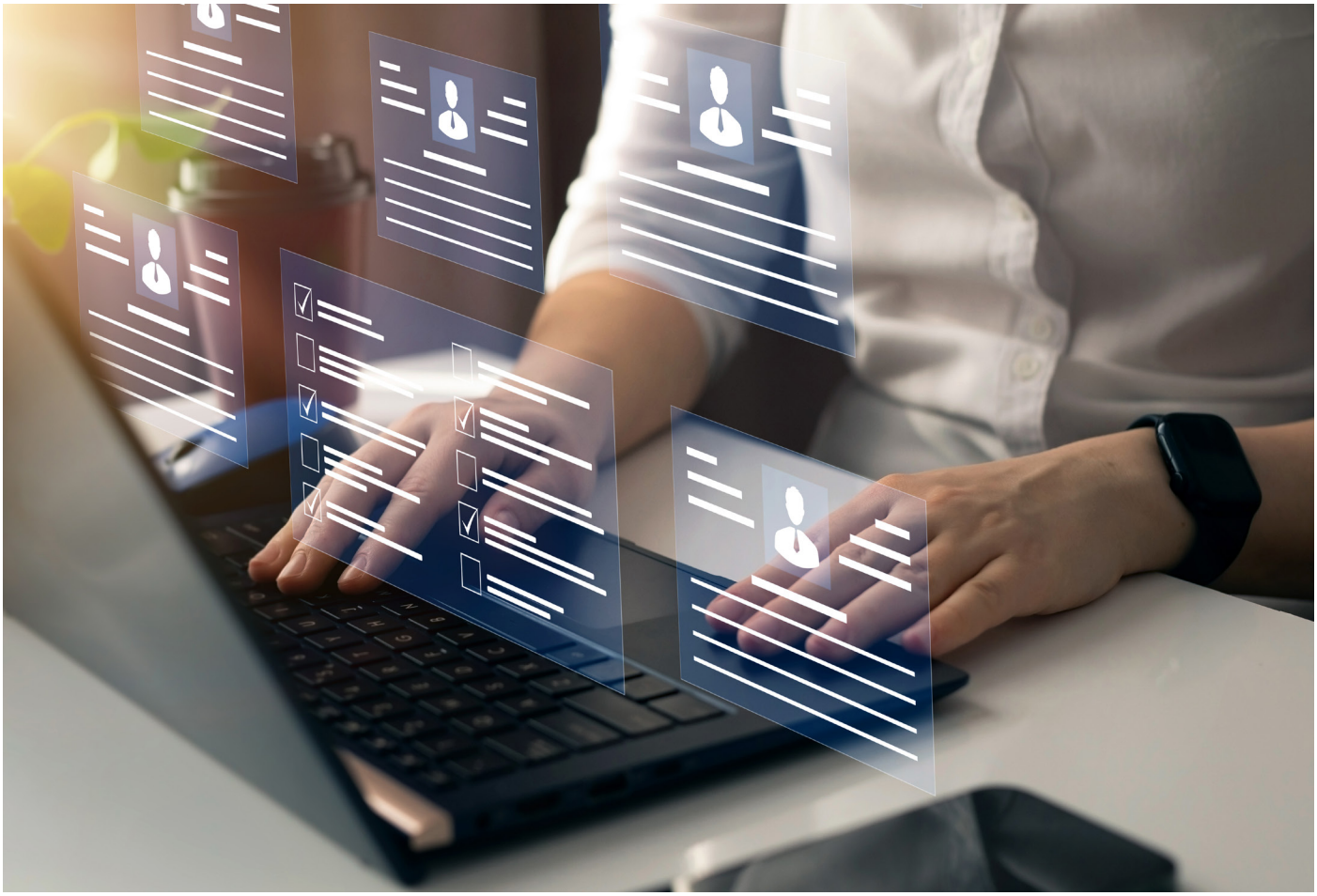
NESEC LEISTUNGEN

Cyber-Sicherheits-Check CyberRisikoCheck nach DIN SPEC 27076

Cyber-Sicherheits-Check

Jedes Unternehmen hängt heute wesentlich von einer verlässlichen und funktionierenden Informationstechnik ab. Angriffe mit Schadsoftware, Denial-of-Service Angriffe aber auch der Diebstahl von Daten und Know-how führen daher schnell zu existenzbedrohenden Schäden. Mittelfristig nehmen die Angriffe sogar noch zu. Das Bundesamt für Sicherheit in der Informationstechnik bewertet die Bedrohungslage weiterhin als hoch.

Mit Hilfe eines Cyber-Sicherheits-Checks können Organisationen das aktuell erreichte Niveau der Cybersicherheit bestimmen und mögliche Defizite identifizieren. Ein Cyber-Sicherheits-Check kann deshalb zu jedem Zeitpunkt erfolgen und ist, anders als ein Audit, nicht an die vorherige Einführung eines ISMS oder an die Umsetzung konkreter Maßnahmen gebunden. Weder müssen bestimmte Dokumente oder Prozesse bereits vorhanden sein, noch wird ein Reifegrad der Umsetzung gefordert. Ein Cyber-Sicherheits-Check kann deshalb auch ideal als Gap-Analyse genutzt werden.

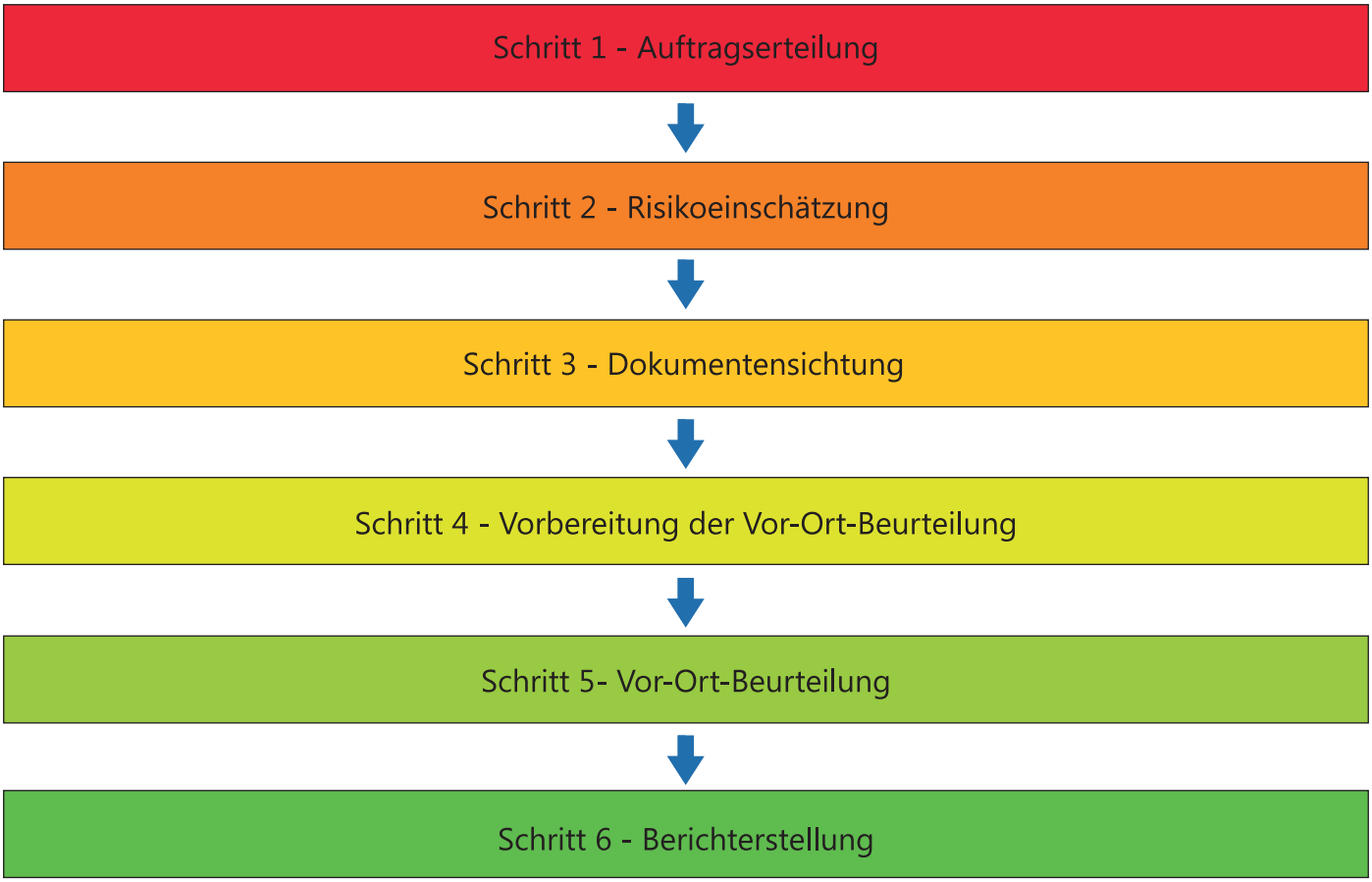


Der Cyber-Sicherheits-Check ist als risikoorientierte Prüfung gedacht. Zur Bestimmung des Risikos für die zu prüfende Organisation muss deshalb eine Risikoeinschätzung durchgeführt werden. Anhand der Risikoeinschätzung wird der zu erwartende Zeitaufwand, die Prüftiefe sowie die Wahl der Stichproben bestimmt.

Die Beurteilung durch den Cyber-Sicherheits-Check erfolgt auf der Basis eines sorgfältig durch die ISACA erstellten Rahmenwerks. In 14 Kategorien werden 55 Maßnahmenziele beurteilt. Zu jedem Maßnahmenziel gibt es Basismaßnahmen, die mindestens geprüft werden müssen. Zusätzlich verwenden wir weitere, von uns ergänzend identifizierte Maßnahmen, die abhängig von der angewandten Referenznorm, z.B. ISO 27001 oder VdS 10000 untersucht werden.

Ablauf des Cyber-Sicherheits-Checks

Der Ablauf des Cyber-Sicherheits-Checks ist in sechs Teilschritte standardisiert.



Schritt 1: Auftragserteilung

Für die vollständige und umfassende Beurteilung der gegebenen Infrastruktur benötigen wir Einblicke in die verschiedenen Bereiche Ihres Unternehmens. Bewertet werden deshalb nicht nur IT-Systeme, sondern auch die Beschaffung, das Lieferantenmanagement sowie das Personalwesen und die physische Sicherheit. Ein Cyber-Sicherheits-Check sollte von der Geschäftsleitung initiiert werden, um die Unterstützung aller beteiligten Geschäftsbereiche zu erhalten.
Unsere Prüfer benötigen außerdem Zugriff auf viele interne, möglicherweise vertraulich eingestufte Dokumente. Der komplette Cyber-Sicherheits-Check sollte daher zusätzlich mit einer geeigneten Vertraulichkeitsvereinbarung abgesichert werden.

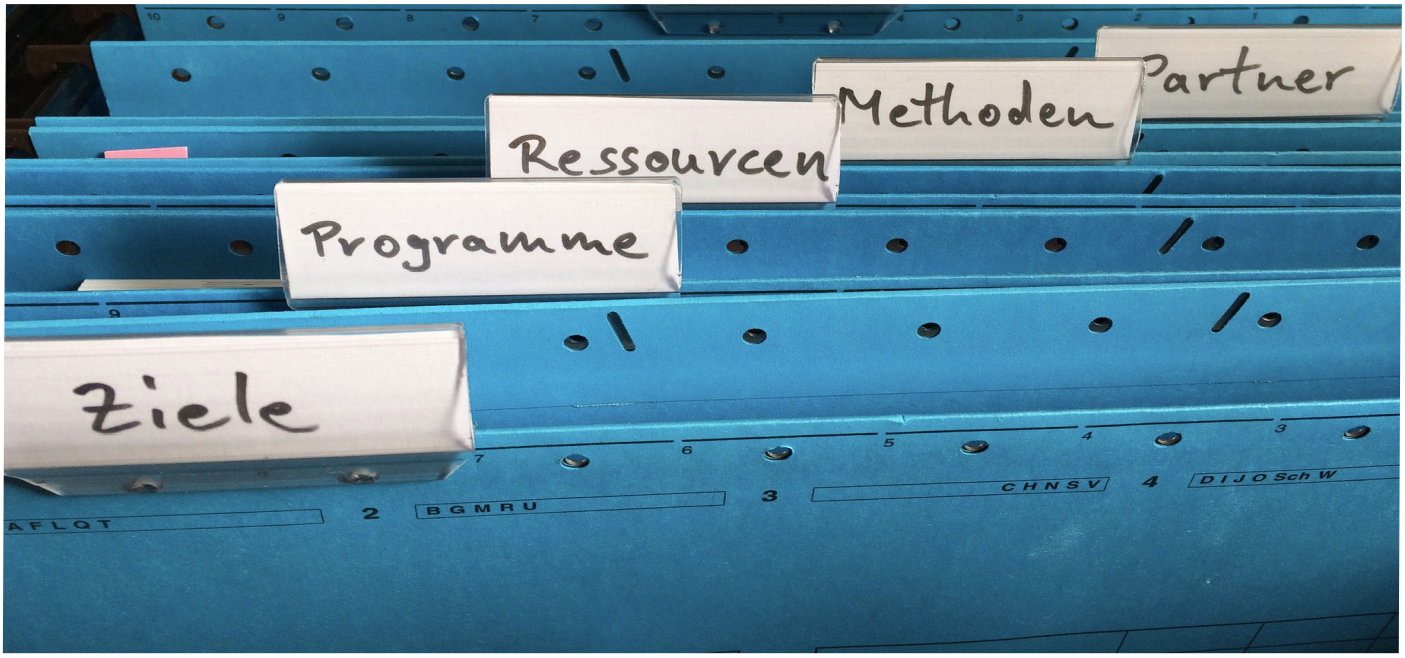
Schritt 2: Bestimmung der Cyber-Sicherheits-Exposition

Der Cyber-Sicherheits-Check verlangt eine Risikoeinschätzung zur Bewertung des benötigten Zeitaufwands sowie einer risikoorientierten Prüftiefe.
Die Risikoeinschätzung basiert auf dem Wert der Daten sowie der Abhängigkeit von der IT bezüglich der Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit der Organisation. Außerdem fließt eventuell vorhandenes Wissen über Angreifer und Angriffe aus der Vergangenheit in die Risikobewertung ein.
In der Regel kann die Risikoeinschätzung direkt von Ihnen durchgeführt werden. Wir haben dafür einen geeigneten Fragebogen entwickelt, den wir Ihnen gerne zusenden.

Schritt 3: Dokumentensichtung

Die Dokumentensichtung hat den Zweck, einen Überblick über die Organisation, die IT-Infrastruktur sowie vorhandene Richtlinien und Konzepte zu gewinnen. Hierbei werden insbesondere, sofern vorhanden, das Organigramm, Netzwerkpläne aber auch die Sicherheitsleitlinie und das Informationssicherheitskonzept geprüft.

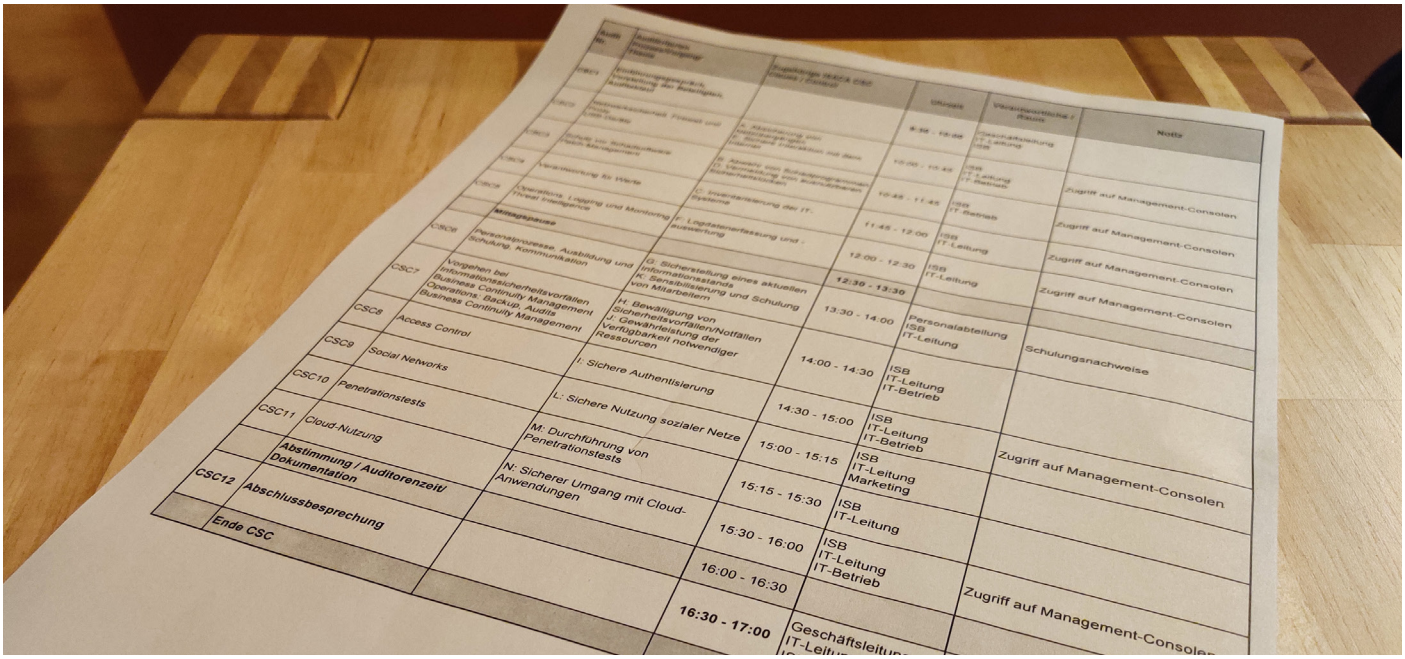
Fehlen Dokumente, wird die Dokumentensichtung durch Gespräche in der Vor-Ort-Beurteilung ergänzt.



Schritt 4: Vorbereitung der Vor-Ort-Beurteilung

Zur Vorbereitung der Vor-Ort-Beurteilung wird vom Prüfer ein Ablaufplan unter Berücksichtigung der Risikoeinschätzung erstellt. Aus dem Ablaufplan ergibt sich der zeitliche Ablauf. Außerdem wird ersichtlich, welche Inhalte geprüft werden und welche Ansprechpartner benötigt werden.

Selbstverständlich kann der Ablaufplan abhängig von der Verfügbarkeit wichtiger Personen angepasst werden.



Schritt 5: Vor-Ort-Beurteilung

Wir beginnen die Vor-Ort-Beurteilung grundsätzlich mit einem Eröffnungsgespräch und der finalen Abstimmung des Ablaufs. Außerdem werden organisatorische Punkte geklärt. Während der Vor-Ort-Beurteilung werden von uns Interviews geführt, weitere Dokumente eingesehen, Räume besichtigt und IT-Systeme sowie Konfigurationen geprüft. Die Bedienung der IT-Systeme bleibt vollständig bei der geprüften Organisation. Insbesondere ist keine aktive Prüfung, z.B. Portscanning oder Vulnerability Scanning durch die Prüfer vorgesehen.

Im Einzelnen sind diese Beurteilungsmethoden vorgesehen:

- Mündliche Befragung (Interview)
- Inaugenscheinnahme von IT-Systemen, Orten, Räumlichkeiten und Gegenständen
- Beobachtung (Wahrnehmungen im Rahmen der Vor-Ort-Beurteilung)
- Aktenanalyse (hierzu gehören auch elektronische Daten oder statistische Auswertungen)
- Datenanalyse (z.B. Konfigurationsdateien, Logfiles, Auswertung von Datenbanken)
- Schriftliche Befragung (z.B. Fragebogen)

Sofern von uns schwerwiegende Sicherheitsmängel gefunden werden, werden Ihnen diese unmittelbar bekanntgegeben. Andernfalls wird im Abschlussgespräch eine erste Einschätzung zur Cybersicherheit abgegeben.

Schritt 6: Nachbereitung / Berichterstellung

Nach der Vor-Ort-Beurteilung erstellen wir den Abschlussbericht, der neben einer Zusammenfassung auch eine Liste der festgestellten Mängel bezogen auf die Maßnahmenziele enthält. Selbstverständlich ergänzen wir auch jeden Befund mit Empfehlungen zur Verbesserung. Sie können daraus direkt entnehmen, in welchen Bereichen vermehrte Aktivitäten zur Erhöhung des Cyber-Sicherheits-Niveaus notwendig und sinnvoll sind.

Maßnahmenziel	Ergebnis	
A – Absicherung von Netzübergängen	Sicherheitsmangel	
B – Abwehr von Schadprogrammen	Empfehlung	
C – Inventarisierung der IT-Systeme	Sicherheitsmangel	
D – Vermeidung von ausnutzbaren Sicherheitslücken	Schwerer Sicherheitsmangel	
E – Sichere Interaktion mit dem Internet	Sicherheitsmangel	
F – Logdatenerfassung und -auswertung	Sicherheitsmangel	
G – Sicherstellung eines aktuellen Informationsstands	Kein Befund	
H – Bewältigung von Sicherheitsvorfällen/Notfällen	Schwerer Sicherheitsmangel	
I – Sichere Authentisierung	Sicherheitsmangel	
J – Gewährleistung der Verfügbarkeit notwendiger Ressourcen	Empfehlung	
K – Sensibilisierung und Schulung von Mitarbeitern	Kein Befund	
L – Sichere Nutzung sozialer Netze	Sicherheitsmangel	
M – Durchführung von Penetrationstests	Kein Befund	
N – Sicherer Umgang mit Cloud-Anwendungen	Sicherheitsmangel	

Unsere Vorgehensweise ist im Detail im Leitfaden zur Durchführung von Cyber-Sicherheits-Check Version 2 der ISACA beschrieben. Der Leitfaden kann entweder direkt von der Webseite der ISACA heruntergeladen oder von uns bezogen werden.

Darum Cyber-Sicherheits-Check von NESEC

Wir verfügen über jahrelange Erfahrung in der Beurteilung und Prüfung der Informationssicherheit von Infrastrukturen und IT-Systemen.
Selbstverständlich werden von uns im Rahmen des Cyber-Sicherheits-Checks ausschließlich qualifizierte und von der ISACA geprüfte Mitarbeiter eingesetzt.

CyberRisikoCheck nach DIN SPEC 27076

Die Norm DIN SPEC 27076:2023-05 ist ein 2023 veröffentlichter Beratungsstandard zur effizienten Verbesserung der Informationssicherheit in kleinen Unternehmen mit bis zu 50 Beschäftigten. Die Entwicklung wurde vom Bundesministerium für Wirtschaft und Klimaschutz in der Initiative IT-Sicherheit in der Wirtschaft finanziert und vom BVMW e.V. geleitet. Ein CyberRisikoCheck nach DIN SPEC 27076 hat das Ziel, Kleinstunternehmen sowie kleinen Unternehmen eine IT-Sicherheitsberatung mit überschaubar geringem Aufwand zu ermöglichen.

Dabei stehen folgende Ziele im Vordergrund:

- Die Ermittlung des IST-Zustands der Informationssicherheit mit den wichtigsten Informationssicherheitsrisiken inklusive Risikowert und Visualisierung der Schwachpunkte
- Die Identifizierung und Priorisierung von Handlungsempfehlungen und weiteren Maßnahmen für das Unternehmen
- Die Sensibilisierung der Geschäftsleitung und verantwortlicher Mitarbeiter in Hinblick auf die Informationssicherheit
- Eine Übersicht über relevante Fördermaßnahmen die bei der Umsetzung der IT-Sicherheits-maßnahmen in Frage kommen

Ein CyberRisikoCheck nach DIN SPEC 27076 ist ausschließlich Interview-basiert und dauert in der Regel maximal 2-3 Stunden. Als Ergebnis des CyberRisikoChecks erhalten Sie einen Bericht, der u.a. die erreichte Punktzahl und für jede nicht erfüllte Anforderung eine Handlungsempfehlung enthält.

Nr.	TOP	Themenbereich	Anforderung	Leitfrage
A. Organisation & Sensibilisierung (11 Punkte)				
01	TOP	Organisation & Sensibilisierung	Die Geschäftsführung muss die Gesamt verantwortung für die Informations sicherheit im Unternehmen tragen.	Wer trägt die Gesamtverantwortung für IT- und Informationssicherheit in Ihren Unternehmen?
02-1		Organisation & Sensibilisierung	Die Geschäftsführung muss sofern sie sich nicht alleine um die IT kümmert - eine verantwortliche Person benennen können.	Haben Sie jemanden, der für die IT- und Informations-sicherheit zuständig ist? Wenn ja, wer ist das?

Ablauf des CyberRisikoCheck

Ein CyberRisikoCheck nach DIN SPEC 27076 ist ausschließlich Interview-basiert und dauert in der Regel maximal 2-3 Stunden. Als Ergebnis des CyberRisikoChecks erhalten Sie einen Bericht, der u.a. die erreichte Punktzahl und für jede nicht erfüllte Anforderung eine Handlungsempfehlung enthält.

Der Ablauf eines CyberRisikoChecks besteht deshalb aus den folgenden Schritten:

1. Erstinformation und Beauftragung
2. Durchführung des Interviews
3. Auswertung der vorliegenden Informationen und Erstellung des Berichts
4. Präsentation des Berichts und der abgeleiteten Empfehlungen

Verpflichtend ist die Teilnahme der Geschäftsführung am gesamten Prozess.

Themen im Interview

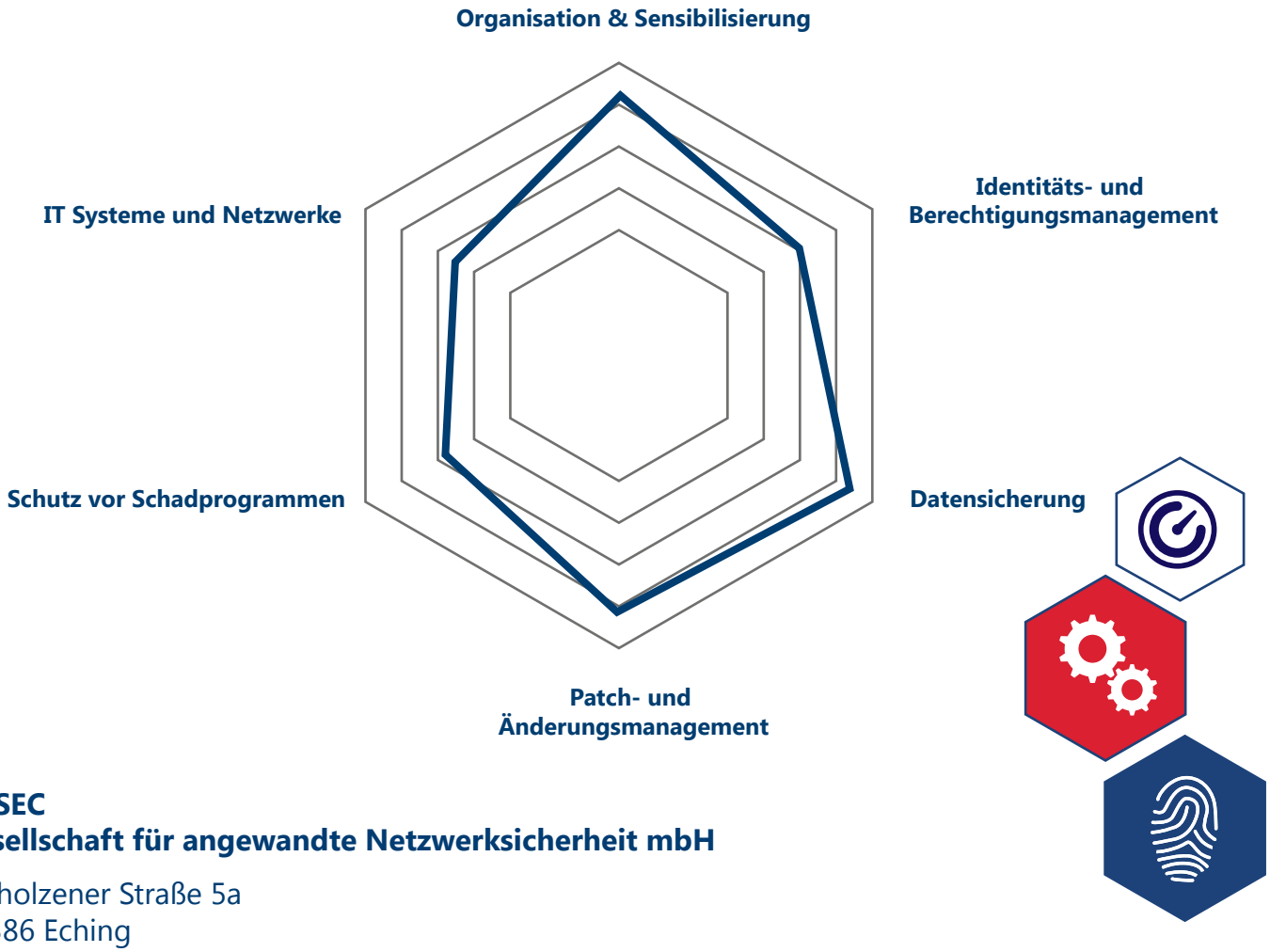
Im eigentlichen Interview werden 27 Anforderungen aus 6 Themenbereichen abgefragt, um zu prüfen, ob und wie weit Ihr Unternehmen diese erfüllt. Für die Antworten werden nach den Vorgaben der DIN SPEC 27076 Punkte vergeben. Das Gespräch zur Erhebung des IST-Zustands kann als Präsenztermin, Videokonferenz oder Hybrid durchgeführt werden. Sofern vorhanden, sollten Konzepte und Sicherheitsrichtlinien, z.B. zum Virenschutz und zur Datensicherung oder ein Notfallkonzept während des Gesprächs vorliegen.

Themenbereiche des CyberRisikoChecks:

1. Organisation & Sensibilisierung
2. Identitäts- und Berechtigungsmanagement
3. Datensicherung
4. Patch- und Änderungsmanagement
5. Schutz vor Schadprogrammen
6. IT-Systeme und Netzwerke

Die Erhebung des IST-Zustands ist ausdrücklich nicht als Beratung konzipert sondern als reine Bestandsaufnahme. Aus den Handlungsempfehlungen des Berichts kann sich für das geprüfte Unternehmen jedoch weiterer Beratungsbedarf ergeben.

Ergebnis



NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH

Fürholzener Straße 5a
85386 Eching

Telefon: 089 - 45217100
E-Mail: welcome@nesec.de
Internet: www.nesec.de

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH