Cyber-Sicherheits-Checks
auf Basis des
Leitfadens
von
ISACA / BSI / Allianz für Cyber-Sicherheit

Cyber-Sicherheits-Checks

Die Unternehmens-IT ist tagtäglich einer Vielzahl von Bedrohungen ausgesetzt. Dabei kann es sich sowohl um absichtlich herbeigeführte Störungen handeln, wie zielgerichtete Cyber Angriffe durch gut organisierte und professionell ausgestattete Angreifer, aber auch um Störungen, die auf Grund von Fahrlässigkeit oder Unwissenheit herbeigeführt werden.

Abbildung 1

Mittels eines durch die ISACA, in Zusammenarbeit mit dem BSI und der Allianz für Cyber Sicherheit[1] erstellten Leitfadens[2] und dem festgelegten Verfahren bekommen Sie eine Übersicht über den Zustand ihrer IT- und Informationssicherheit.

Um was geht es?

Abbildung 2

Durch das im Leitfaden festgelegte Vorgehen ist es möglich, den aktuellen Status ihrer Informations- und Cyber-Sicherheit zu erfassen und von anerkannten Experten beurteilen und bewerten zu lassen.

Der Leitfaden und die dem Leitfaden zugrunde liegenden Maßnahmenziele für die Beurteilung setzen auf dem bewährten Konzept der drei Verteidigungslinien (Management, Risikomanagement, Audits) auf, fokussieren sich dabei aber ganz auf den Aspekt Cyber-Sicherheit.

Als Ergebnis erhalten Sie mit vergleichsweise geringem Aufwand einen guten Überblick über Ihre Sicherheitsmaßnahmen und den Zustand ihrer Cyber-Sicherheit. Dabei bildet der Cyber-Sicherheits-Check wesentliche Aspekte des BSI-Grundschutzes, der ISO 27001, COBIT und dem PCI DSS ab.

[1] https://www.allianz-fuer-cybersicherheit.de/
[2] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/ACS/leitfaden_CSC_v2.html

Vorgehensweise

Die Vorgehensweise zur Durchführung eines Cyber-Sicherheits-Checks gliedert sich in folgende Schritte:

1. Auftragserteilung
   Die Beauftragung eines Cyber-Sicherheits-Checks sollte durch die Leitung/das Management der betreffenden Institution erfolgen.

2. Risikoeinschätzung
   Zur Bestimmung des Risikos für die zu beurteilende Institution muss von dieser im Vorfeld eine Risikoeinschätzung durchgeführt worden sein. Dabei soll mittels Schadenshöhe und Eintrittswahrscheinlichkeit eine Risikokennzahl ermittelt werden. Ausgehend davon wird der zu erwartende Zeitaufwand, die Beurteilungstiefe sowie die Wahl der Stichproben bei der Durchführung des Cyber-Sicherheits-Checks risikoorientiert durch die prüfende Institution bestimmt.

Abbildung 3

3. Dokumentensichtung
   Mittels der Dokumentensichtung bekommt der Prüfer einen Überblick über die Aufgaben, die Organisation und die IT-Infrastrukturen der Institution und die Dokumente werden grob gesichtet. Im Rahmen dieser Dokumentensichtung werden, soweit vorliegend, das IT-Rahmenkonzept, die Liste der kritischen Geschäftsprozesse, die Sicherheitsleitlinie, das Sicherheitskonzept und der Netzplan beurteilt und bewertet. Für den Fall, dass keine ausreichenden informativen Dokumente vorhanden sind, wird die Dokumentensichtung durch Interviews ergänzt, um den erforderlichen Überblick zu erhalten.

4. Vorbereitung des Vor-Ort Termins
   Ausgehend von der Vorbereitung und der Dokumentensichtung wird für die Vor-Ort-Beurteilung ein Ablaufplan erstellt, der festlegt, welche Themenbereiche wann und mit welchen Ansprechpartnern besprochen werden sollen.

5. Vor-Ort-Beurteilung
   Bei der Vor-Ort-Beurteilung werden Interviews mit relevanten Ansprechpartnern geführt, stichprobenartig Dokumente und Nachweise eingesehen und ggf. auch technische Sachverhalte überprüft. Dabei wird nicht in laufende Systeme oder Anwendungen eingegriffen, sondern die jeweiligen Ansprechpartner demonstrieren bzw. zeigen, wie Sachverhalte umgesetzt sind. Das Ganze endet mit einem Abschlussgespräch und einer ersten Bewertung des Standes der Cyber-Sicherheit in der Institution durch die Prüfer.

6. Berichterstellung
   Im Nachgang an den Vor-Ort-Termin wird ein Bericht erstellt, der einen Überblick über die Cyber-Sicherheit der Institution liefert. Mängel werden entsprechend festgehalten und wo möglich, allgemeine Empfehlungen zur Beseitigung aufgezeigt.

Abbildung 4

Bei der Bewertung des Zustandes der Cyber-Sicherheit einer Institution werden die im Leitfaden für Cyber-Sicherheit festgelegten Maßnahmenziele in Abhängigkeit von der jeweiligen Risikoeinschätzung der Institution abhängig gemacht. Je nach Einstufung werden die einzelnen Maßnahmenziele unterschiedlich tief geprüft.

Unsere Prüfer

Die Qualität, das Ergebnis und mögliche Verbesserungsempfehlungen hängen maßgeblich von der Erfahrung der jeweiligen Prüfer ab.

Bei SECIANUS führen die Cyber-Sicherheits-Checks ausnahmslos langjährig erfahrene ISO 27001 Lead Auditoren, BSI-Grundschutz-Auditoren oder BSI zertifizierte IS-Revisoren durch. Alle unsere Prüfer verfügen über umfangreiches technisches Wissen und sind neben ihrer Tätigkeit als zertifizierte Auditoren auch als Berater für die Einführung und Umsetzung von Informations- und Cyber-Sicherheitssystemen tätig.

Unsere Prüfer halten sich dabei streng an die im Leitfaden der ISACA vorgegebene Herangehensweise.

Über uns

Die SECIANUS GmbH & Co. KG ist vom Bundesamt für Sicherheit in der Informationstechnik zum zertifizierten und lizenzierten IT-Sicherheitsdienstleister des Bundes ernannt. Die letzte erfolgreich bestandene Begutachtung durch das BSI erfolgte im Februar 2020.

Unser Fokus liegt dabei auf Dienstleistungen rund um das Thema Informationssicherheit, Datenschutz, Cyber-Security und IT-Compliance. Dazu zählen auch Informationssicherheitsrevisionen, die Auditierung von Informationssicherheitsszenarien, die Beratung und Unterstützung beim Aufbau von Informationssicherheitsmanagement-Systemen (ISMS), dem Datenschutz, sowie der Cyber-Security. Darüber hinaus bietet die SECIANUS GmbH & Co. KG auch technische Überprüfungen, sog. Penetrationtests an. Diese folgen den Empfehlungen des PTES (www.pentest-standard.org), den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik und dem OWASP (www.owasp.org).

Interesse?

Sie haben Interesse an einem Cyber-Sicherheits-Check auf Basis des Leitfadens der ISACA? Nehmen Sie einfach unverbindlich mit uns Kontakt auf.

Sie erreichen uns:

Postalisch:

SECIANUS GmbH & Co. KG
Further Str. 14
905390 Wendelstein

Mail:

info@secianus.de

Telefonisch:

09129/2929808

Wir freuen uns auf Ihre Anfrage.

Bilder:
www.pixabay.com, freie kommerzielle Nutzung,
Abb.1: Darwin Laganzon, Abb.2: Tumisu, Abb.3/4: Gerd Altmann