CISIS12

CISIS12 IN KÜRZE - FÜR ENTSCHEIDER UND ENTSCHEIDERINNEN

In der heutigen digital vernetzten Welt ist Informationssicherheit ein zentraler Erfolgsfaktor für Unternehmen jeder Größe und Branche. Die Herausforderungen, die mit der Sicherung von Unternehmensdaten verbunden sind, werden zunehmend komplexer und vielschichtiger. Dabei sind es insbesondere die Entscheider in Unternehmen, die die Verantwortung tragen geeignete Maßnahmen zur Informationssicherheit zu initiieren und zu überwachen. CISIS12, das „Compliance Information Security Management System in 12 Schritten“, bietet eine praxisorientierte und kosteneffiziente Lösung für die Implementierung eines Informationssicherheitsmanagementsystems (ISMS). Speziell entwickelt für kleine und mittelständische Unternehmen, zielt CISIS12 darauf ab, den Schutz sensibler Daten und die Einhaltung gesetzlicher Anforderungen sicherzustellen.

	DIE 12 SCHRITTE VON CISIS12	WELCHE FRAGEN SOLLTE ICH MIR HIER STELLEN?	WAS IST ZU TUN?
GEMEINSAMES VERSTÄNDNIS-MINDSET	01 Leitlinie erstellen	Welchen Stellenwert messe ich der Informationssicherheit in meiner Organisation zu? Wie erreiche ich Informationssicherheit? Was ist meine Strategie? Welche Ziele setze ich mir, um Informationssicherheit dauerhaft zu gewährleisten und kontinuierlich zu verbessern?	Verpflichtung der Organisationsleitung zur Informationssicherheit und Beschreibung ihrer strategischen Bedeutung. Bereitstellung von Ressourcen und Organisationseinheiten sowie die Definition von messbaren Zielen.
	02 Beschäftigte sensibilisieren	Welche Maßnahmen ergreife ich, um die Beschäftigten für Risiken und Chancen zu sensibilisieren und ihre Akzeptanz für Sicherheitsmaßnahmen zu gewinnen?	Schulungen, Awareness-Maßnahmen, Notfallübungen, Erläuterungen der Richtlinien und Prozesse usw.
AUFBAU DER IT-SICHER-HEITS RAHMENBE-DINGUNGEN	03 Informationssicherheits-team aufbauen	Welche Mitarbeiter und Mitarbeiterinnen sind maßgeblich mit der Einführung und Aufrechterhaltung eines ISMS beauftragt. Wer unterstützt sie dabei und wer setzt die erforderlichen Maßnahmen um?	Benennung des ISB und DSB. IT-Leitung, Organisationsleitung, Betriebsrat, ggf. Berater und IT-Dienstleister werden eingebunden. Regelmäßige Treffen, Verantwortlichkeiten und Rollen werden festgelegt.
	04 IT-Doku-Struktur festlegen	Habe ich alle Dokumente in aktueller Fassung, die für den Betrieb meiner Organisation, für den Notfall und der Wiederherstellung nach einem Notfall notwendig sind? Habe ich eine aktuelle und detaillierte Beschreibung meiner IT-Infrastruktur? Kenne ich die Kontaktdaten aller internen und externen Ansprechpartner? Weiß ich, was zu tun ist, wenn Systeme oder Verantwortliche ausfallen?	Erstellung und Überarbeitung notwendiger IT-Dokumente, wie Betriebshandbuch, Notfallhandbuch, Netzplan usw.), Risikobehandlungsplan usw. Die Dokumentation ist meist erst am Ende der 12 Schritte komplett vorhanden, da wichtige Informationen erst in späteren Schritten erfasst werden.
	05 IT-Servicemanagement Prozesse	Ist in meiner Organisation klar geregelt und dokumentiert, wie Änderungen und Störungen abgewickelt werden? Wer sind die Ansprechpartner? Wie sind die Verantwortlichkeiten geregelt? Gibt es einen Wartungsplan? Sind die Prozesse bei Einstellungen und Ausscheiden von Mitarbeitern klar geregelt?	Hier werden die IT-Servicemanagement-Prozesse Wartung, Störung und Änderungen definiert, Verantwortlichkeiten festgelegt und der On- und Offboarding-Prozess beschrieben.
ERFASSUNG & ANALYSE KRITISCHER UNTERNEHMENS PROZESSE	06 Compliance, Prozesse und Anwendungen	Wo würde im Ernstfall der größte Schaden entstehen? Was sind meine wichtigsten Prozesse? Was sind meine Kronjuwelen, die es besonders zu schützen gilt? Welche Anwendungen brauche ich für diese Prozesse und Kronjuwelen? Wie lange kann ich auf diese Prozesse maximal verzichten und welchen Datenverlust kann ich maximal verkraften. Gibt es gesetzliche Anforderungen an meine Organisation (z.B. DSGVO, NIS2 usw.)? Erfüllen auch meine Lieferanten die Anforderungen an Informationssicherheit (Nachweis nach Sicherheit der Lieferketten)?	Hier werden die wichtigsten Prozesse in der Organisation identifiziert und der Schutzbedarf auf Grundlage des maximalen Schadens festgelegt. Der Schutzbedarf wird auf die dafür notwendigen Anwendungen vererbt. Weiterhin werden in diesem Schritt die gesetzlichen Anforderungen an die Organisation identifiziert und ermittelt, welche Daten und Anwendungen davon betroffen und entsprechend geschützt werden müssen.

	07 IT-Struktur analysieren	Welche IT-Systeme und Räume brauche ich für meine Prozesse und Compliance-Anforderungen? Wie kann ich diese schützen und wie hoch muss dieser Schutz sein, um den Schutzbedarf zu erfüllen.	Für die Prozesse und Compliance-Anforderungen aus Schritt 6 werden die dafür notwendigen Anwendungen, IT-Systeme und Gebäude erfasst, detailliert beschrieben und in eine übersichtliche Struktur gebracht (Netzwerkplan, Betriebshandbuch, Systemsteckbriefe). Der Schutzbedarf der Prozesse und Compliance-Anforderungen vererbt sich auf die dafür notwendigen IT-Systeme und Gebäude. Aus dem CISIS12-Katalog werden die jeweiligen Bausteine den IT-Systemen und Gebäuden zugeordnet. Die im CISIS12-Katalog genannten Sicherheitsanforderungen werden auf die bestehenden IT-Systeme und Gebäude übertragen und angepasst (modelliert).
PROBLEM IDENTIFIZIERUNG RISIKOBETRACH-TUNG	08 Risikomanagement	Welche Bedrohungen gibt es für meine relevanten Systeme, wo sind Sicherheitslücken und wie hoch sind die Wahrscheinlichkeiten eines Notfalls? Welches Risiko resultiert aus der Schadenswahrscheinlichkeit und der Schadenshöhe? Haben wir bereits angemessene Maßnahmen ergriffen, um Risiken zu vermeiden oder abzumildern? Welche Maßnahmen sind noch zu ergreifen? Haben wir die Risiken bewertet, d.h. gibt es Risiken, die ich in Kauf nehmen kann oder die unbedingt abgesichert werden müssen?	Der Betrieb von IT-Strukturen, Diensten und Anwendungen beinhaltet Risiken, unabhängig davon, ob man sie selbst betreibt oder im Outsourcing von Partnern betreiben lässt. Die Risikoanalyse ermöglicht eine nachvollziehbare Priorisierung der Maßnahmen und des Ressourceneinsatzes, um systematisch und fokussiert das Sicherheitsniveau zu erhöhen und kontinuierlich zu verbessern. Die erkannten Risiken können verringert, übertragen, vermieden oder akzeptiert werden.
	09 Soll-Ist-Vergleich	Welche Unterschiede gibt es zwischen meinen bestehenden Sicherheitsmaßnahmen und den im CISIS12-Katalog genannten Maßnahmen für die relevanten Bausteine?	Hier werden die in den vorausgehenden Schritten identifizierten Maßnahmen von den jeweiligen Fachexperten in der Organisation(Fachabteilung/ Abteilungsleitung/ Prozess-Verantwortliche, Know-How Träger) nach Umsetzungsgrad bewertet und kommentiert. Ziel im ISMS-Prozess ist es, dass sukzessive sämtliche Maßnahmen dem Soll entsprechen und die Lücke vom IST geschlossen wird.
SYNTHESE, STRATEGIE & UMSETZUNG	10 Umsetzung planen und umsetzen	Welche Maßnahmen müssen umgesetzt werden, damit die Sicherheitsrisiken abgemildert, bzw. verhindert werden? Gibt es eine Priorisierung der Maßnahmen bei der Umsetzung? Wer ist verantwortlich für die Umsetzung? Welche Ressourcen (Mitarbeiter, Budget, Technologie, etc.) werden für die Umsetzung der Maßnahmen benötigt? Habe ich den Umsetzungsplan freigegeben und unterschrieben? Wie erfolgt die Kommunikation und Abstimmung mit den relevanten Stakeholdern, um deren Unterstützung sicherzustellen?	Aus dem vorherigen Schritt sind offene, unvollständige bzw. teilweise umgesetzte, sowie derzeit abgewählte Maßnahmen dokumentiert. Diese müssen nach Kriterien in eine Reihung gebracht werden, die eine effiziente und effektive Umsetzung ermöglichet. Dabei sind Schutzbedarfe, Risiken, Wirtschaftlichkeit, Umsetzungszeit oder auch die Budgetkontrolle wichtige Indikatoren.

KONTINUIERLICHE ÜBERPRÜFUNG BEWERTUNG VERBESSERN

11 Internes Audit	Habe ich mit allen bisher identifizierten und umgesetzten Maßnahmen die wichtigsten Sicherheitsrisiken erfolgreich abgemildert, bzw. verhindert? Gibt es Verbesserungspotential? Haben meine Mitarbeiter das Bewusstsein für Informationssicherheit und Compliance und die Kenntnisse darüber? Reichen meine umgesetzten Maßnahmen aus um CISIS12-konform (ggf. auch noch weitere Anforderungen) zu sein?	Mit der Durchführung eines internen Audits bei der Einführung von CISIS12 können Organisationen sicherstellen, dass ihre Informationssicherheitsmaßnahmen umgesetzt werden, Risiken angemessen behandelt und kontinuierliche Verbesserungen angestrebt werden. Es trägt zur Stärkung der Informationssicherheit und zum Schutz sensibler Informationen bei.
12 Revision	Entsprechen die Dokumente und umgesetzten Maßnahmen noch meinen Zielvorgaben in der Informationssicherheit (gibt es neue Risiken, Prozesse?)? Welche Verbesserungen oder Änderungen wurden seit der letzten Revision im ISMS vorgenommen und wie effektiv waren sie? Wurden die Empfehlungen aus den letzten internen und/oder externen Audits umgesetzt? Haben wir uns als Organisation kontinuierlich verbessert oder gibt es noch Handlungsbedarf?	Durch die regelmäßigen Revisionen des Informationssicherheits-Prozesses können Aussagen über deren wirksame Umsetzung, Aktualität, Vollständigkeit, Angemessenheit und den aktuellen Zustand der Informationssicherheit getroffen werden.