sure[secure]

INFORMATIONSSICHERHEITS MANAGEMENTSYSTEM

UNSER SERVICE IM BEREICH SECURE AWARENESS UND IR-PRÄVENTION

UNSERE SERVICES IM BEREICH „ISMS“

Informationssicherheit ist umfangreich! Durch die jeweiligen internen und externen Anforderungen beeinflusst, sehen sich die Beteiligten des Informationssicherheitsprozesses mitunter einer hohen Komplexität im Umgang mit Informationssicherheit konfrontiert. Wäre es nicht vorteilhaft, wenn all diese komplexen Anforderungen an die IT, beziehungsweise die gesamte Organisation ***irgendwie*** überblickt, die Umsetzung gesteuert und bereits Umgesetztes verbessert werden könnte?

Genau dieses ***irgendwie*** ist das ISMS, also das **I**nformations**S**icherheits**M**anagement**S**ystem.

Um dieses umzusetzen, gibt es diverse Standards. Der gewählte Standard ist mitunter dafür ausschlaggebend, wie viele Anforderungen in welcher Güte erfüllt werden müssen. Die suresecure fokussiert sich auf die beiden gängigsten im deutschsprachigen Raum: ISO 27001 und BSI IT-Grundschutz.

IHR VORTEIL BEI UNS: MEHR ALS NUR BERATUNG

Eines ist uns besonders wichtig: Die vollumfängliche, ehrliche und transparente Beratung. Sie schenken uns Ihr Vertrauen, wir bedanken uns mit einer besonderen Partnerschaft. Unsere Security-Expert:innen haben langjährige Erfahrung im Bereich IT- und Informationssicherheit und arbeiten eng mit unseren Partnern zusammen. Wir entwerfen individuelle, auf Sie und Ihr Unternehmen zugeschnittene Cybersecurity-Lösungen und begleiten Ihr Unternehmen vom Kickoff bis zur Umsetzung. For a safe digital world.

Unser Informationssicherheitsmanagementsystem (ISMS)

Die Einführung eines ISMS ist ein sehr umfangreiches Projekt. Hier bietet es sich an, die Aufgabe in verschiedene Teilschritte zu zerlegen. Daraus ergibt sich die Möglichkeit, die für Sie und Ihr Unternehmen relevanten Aspekte zu identifizieren und einen echten Mehrwert zu generieren.

Sofern Ihr Unternehmen per Gesetz nicht gezwungen ist, das ISMS nach einem bestimmten Standard zu betrieben, ist es möglich, sich aus beiden Standards zu bedienen und jeweils die für das Unternehmen besten Ansätze aus beiden Welten nutzen.

Ihr Vorteil:

- [Optional] ISMS Readiness-Check gegen den gewählten Standard
- [Optional] ISMS-Tool Identifikation und Einführungsbegleitung
- Geltungsbereich (SoA[1]) und Informationsverbund definieren
  - **BSI:** Geltungsbereich, Strukturanalyse und Modellierung
- ISMS-Dokumentation (IS-Leitlinie, ISMS-Richtlinie, Lenkung von Dokumenten, Auditierung, weitere Dokumente aus den Anhängen/BSI Bausteinen abgeleitet)
- **BSI:** Schutzbedarfsanalyse
- **BSI:** IT-Grundschutzcheck
- Risikomanagement-Konzept entwickeln
- **Unterstützende Maßnahmenplanung und Umsetzung:**
  Aus diversen Quellen eines ISMS resultieren Maßnahmen, die es zu steuern und umzusetzen gilt. Wir geben Ihnen die nötigen Werkzeuge an die Hand, um Ihre Maßnahmen zu steuern und identifizieren mögliche Maßnahmenumsetzungen, die wir mit Ihnen gemeinsam durchführen können.
- Security Awareness einführen

Wir empfehlen folgende Services passend zum ISMS:

[Alle Services lassen sich auch unabhängig voneinander buchen! Eine detaillierte Beschreibung in Form einer Leistungsbeschreibung lassen wir Ihnen gerne auf Wunsch zukommen!]

Administrationskonzept

- In jeder IT-Umgebung gibt es Nutzer:innen, die über besondere Zugangsdaten verfügen. So genannte Super-User und Domänen-Administratoren haben umfangreiche Rechte und Möglichkeiten, weitreichende Änderungen an Ihrer IT-Umgebung vorzunehmen. Das ist auch exakt der Sinn dieser Rollen. In den falschen Händen können diese Berechtigungen jedoch sehr großen Schaden anrichten. Daher sind Rollen mit diesen weitreichenden Berechtigungen ebenfalls einzuschränken.

- Um dieses Problem anzugehen, entwickeln wir für Sie eine individuelle Konzept-Grundlage und einen Maßnahmenkatalog, um Ihre IT-Domänenstruktur mit einem Administrationskonzept besser abzusichern.

Sicherheitskonzept Backup-Management

- Institutionen speichern immer mehr Daten und sind gleichzeitig immer stärker auf sie angewiesen. Gehen Daten verloren, z. B. durch defekte Hardware, Malware oder versehentliches Löschen, können gravierende Schäden entstehen. Dies kann klassische IT-Systeme – wie Server oder Clients – aber auch Firewalls, Router, Switches oder sogar IoT[2]-Geräte betreffen. Alles diese Systeme speichern schützenswerte Informationen. Dazu zählen neben den firmenvertraulichen Daten auch Konfigurationen und technische Logs.

- Durch regelmäßige Datensicherungen lassen sich negative Auswirkungen von Datenverlusten minimieren. Das Datensicherungskonzept, oder Sicherheitskonzept Backup Management, beschreibt, welche Daten wann und wie in Ihrer Organisation gesichert werden. Das Datensicherungskonzept nimmt somit auch eine zentrale Rolle in der Notfallplanung ein.

[1] Statement of Applicapility [2] IoT – Internet of Things

Administrationskonzept

- Im Kontext der IT-Sicherheit geht es beim Risikomanagement darum, Risiken zu erkennen und geeignete präventive Maßnahmen zu entwickeln. Risikomanagement ist dabei die Basis für Maßnahmenentscheidungen in der Informationssicherheit.

Sie erhalten:

- eine individuelle, unternehmensspezifische Richtlinie zum Risikomanagement von Informationssicherheitsrisiken
- Excel-Tool zum Erfassen der Risikoanalysen
- Vollständig durchgeführte Risikoanalysen

Secure Awareness

Grundlegende IT-Security benötigt neben technischen Lösungen auch die Aufmerksamkeit Ihrer Mitarbeiter:innen. Je höher die Awareness für IT-Security ist, desto geringer sind die Erfolgschancen für Angreifende. Gezieltes und auf Ihr Unternehmen angepasstes Training geht auf Ihre Mitarbeiter:innen und Führungskräfte ein und bringt Ihnen das Thema schrittweise näher.

- Ein webbasierter Eingangstest ermöglicht es, den aktuellen Wissenstand Ihrer Mitarbeiter:innen zu erfassen.
- Die definierten Themen und Inhalte werden anschließend bedarfsgerecht als webbasierte Trainings sowie optional in Präsenz- und Onlineveranstaltungen durchgeführt.
- Im Anschluss folgt ein erneuter Test zur Evaluation, um den Erfolg der Schulungsmaßnahmen zu ermitteln.
- Optionale Phishing-Kampagnen: Simulation von E-Mail-Angriffen und weitere automatisierte Trainings.

Incident Response Management Plan (IRMP)

Als präventive Vorbereitung auf einen Sicherheitsvorfall, der Ihre gesamte IT-Umgebung oder Teile davon lahmlegt, empfehlen wir die Erstellung eines Incident Response Management Plans.

Dieser IRMP beschreibt strukturiert den technischen und organisatorischen Umgang mit Cyber-Sicherheitsvorfällen. Der IRMP soll gewährleisten, dass bei einem Sicherheitsvorfall schnell, angemessen und umfassend reagiert werden kann.

Ihr Vorteil bei uns:

- Der IRMP wird auf Basis des Incident-Handling-Frameworks des SANS Institutes erstellt.
- Wir berücksichtigen Ihre organisatorischen und technischen Voraussetzungen und Rahmenbedingungen und passen das Framework geeignet an.
- Erstellung und Lieferung eines individuellen Incident Response Management Plans, sowie ergänzender Dokumente zur strukturierten Behandlung von IT-Sicherheitsvorfällen.
- Die einzelnen Maßnahmen sind einfach, eindeutig und klar formuliert, um eine intuitive Umsetzung im Falle eines Incidents gewährleisten zu können.

HABEN SIE FRAGEN ZU UNSEREN SERVICES?

Alle unsere Services können individuell auf die Bedürfnisse Ihres Unternehmens angepasst werden. Gerne beraten wir Sie umfänglich, welche Security-Services für Ihre Ziele die richtigen sind. Beachten Sie dazu auch gerne unsere weiteren Services, die wir Ihnen in einem persönlichen Gespräch gerne vorstellen oder unter suresecure.de rund um die Uhr für Sie zu finden sind. Sie haben auch Fragen zu Umfängen der Leistungen oder haben weitere Fragen? Zögern Sie nicht uns anzusprechen.

Sie haben Fragen zu unseren Services?
Unsere IT-Security-Expert:innen sind gerne für Sie da!

ANFRAGE SENDEN

KONTAKTIERT UNS

Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60
Telefax: +49 (0) 2156 975 49 78

kontakt@suresecure.de
www.suresecure.de

FOLGT UNS

/suresecure.de

/suresecure.de

/suresecure-gmbh