INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Verbesserung in die Unternehmenskultur integrieren

ConSecur

[security and consulting]

Verbesserung in die Unternehmenskultur integrieren. ISMS erfolgreich umsetzen.

ISMS mit ConSecur – das Essentielle vom weniger Wichtigen unterscheiden

Wenn wir über ein Informationssicherheits-Managementsystem (ISMS) reden, sprechen wir über Entscheidungen.

WAS IST WICHTIGER FÜR EINE ORGANISATION?

- Der Server, auf dem Kundendaten liegen, oder die automatische Regelung der Büroklimatisierung?
- Ist es die Steuerung der Produktion oder der Test-Server für die Azubis?
- Sind es die Systeme zur Veröffentlichung der Essenspläne der Unternehmens-KiTa oder ist es die Zutrittskontrolle zum Labor?

Wenn wir zusammen ein ISMS für Ihre Organisation aufbauen wollen, werden wir im ersten Schritt das Essentielle vom weniger Wichtigen unterscheiden.

Das Gesamtbild, das wir im Anschluss an die Betrachtung dieser Informationswerte (Assets) gewonnen haben, gibt uns den Weg zum Informationssicherheits-Managementsystem für Ihre Organisation vor.

Was ist ein Informationssicherheits-Managementsystem (ISMS)?

Ein ISMS stellt Regeln und Verfahren zur Verfügung, um innerhalb eines Anwendungsbereichs (Scope) identifizierte Informationswerte (Assets) auf Basis einer Risikobetrachtung angemessen und koordiniert zu schützen.

Mit einem implementierten ISMS integrieren Organisationen die Verbesserung in die Unternehmenskultur.

GAP-Analyse – Soll-Ist-Abgleich für die Gesamtübersicht

Die GAP-Analyse ist der erste Schritt, mit dem wir in den Aufbau eines jeden Informationssicherheits-Managementsystems einsteigen.

In dieser frühen Phase liefert der Soll-Ist-Abgleich eine Übersicht, um mit dem Blick auf das Gesamte Defizite zu erkennen und sichtbarzumachen.

Dieser Überblick ist eine Orientierung, die wir als Einordnung benutzen und auf die wir im weiteren Verlauf für die detaillierte Betrachtung einzelner Assets zurückkommen werden.

AN WELCHER STELLE STIMMEN SOLL- UND IST-ZUSTAND ÜBEREIN?

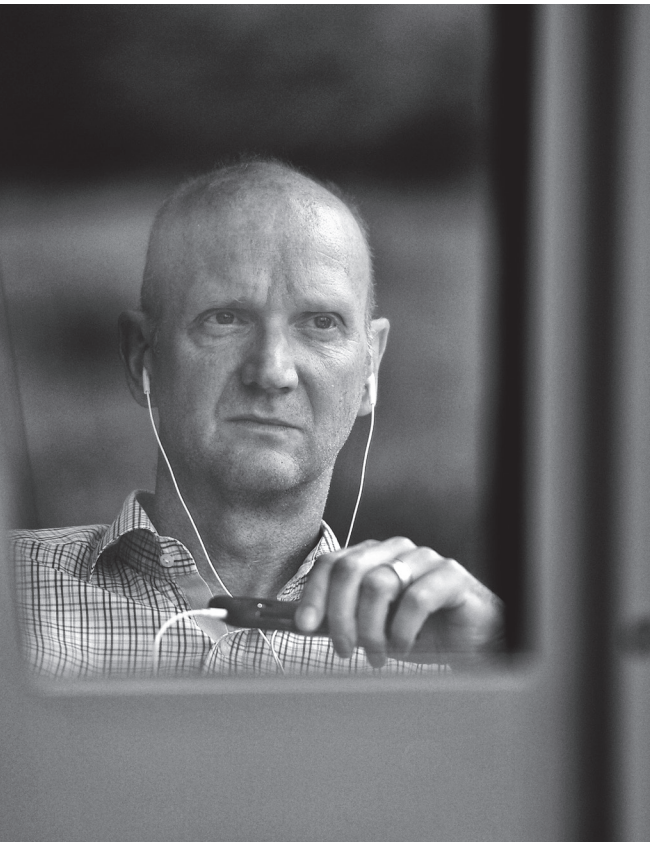
WO WEICHEN SOLL- UND IST-ZUSTAND IN WELCHER AUSPRÄGUNG VONEINANDER AB?

Das Ergebnis ist der Ausgangspunkt auf dem Weg zu einem ISMS.

„Organisationen sind mit einem ISMS dann erfolgreich, wenn sie das Prinzip der Verbesserung in ihre Unternehmenskultur integriert haben.“

JÖRG ECKARDT
ISMS-CONSULTANT CONSECUR GMBH

Quick wins – identifizierte Ziele schnell erreichen



„Quick wins“ nennen wir die infolge der GAP-Analyse identifizierten Maßnahmen, mit deren Umsetzung wir in kürzester Zeit Verbesserungen erzielen können.

Diese „Quick wins“ können wir oft ohne hohen organisatorischen Aufwand direkt aus der GAP-Analyse heraus umsetzen und damit Lücken schließen bzw. Risiken schnell und wirksam minimieren.

Der Scope – Assets im Anwendungsbereich

Im Anwendungsbereich (Scope) sind die Assets angesiedelt, auf denen unser Fokus für die Umsetzung liegt bzw. liegen wird.

Häufig beginnen wir mit den identifizierten Assets, die einen besonderen Schutzbedarf besitzen. Wir sagen gerne „Kronjuwelen“ zu diesen Assets, die entscheidend sind für den Betrieb, für den Erfolg, für die Existenz und für den Fortbestand einer Organisation.

Risikoanalyse – wie ausgeprägt ist der Risikoappetit?

Im Soll-Ist-Abgleich haben wir in einer groben Übersicht Defizite sichtbar gemacht, aus denen unbeachtet eine Bedrohung für eine Organisation erwachsen kann.

Gehen wir ins Detail:

In der Risikoanalyse beschäftigen wir uns mit Eintrittswahrscheinlichkeiten von Bedrohungen oder Schäden sowie mit Schutzmaßnahmen, um für diese Szenarien gewappnet zu sein.

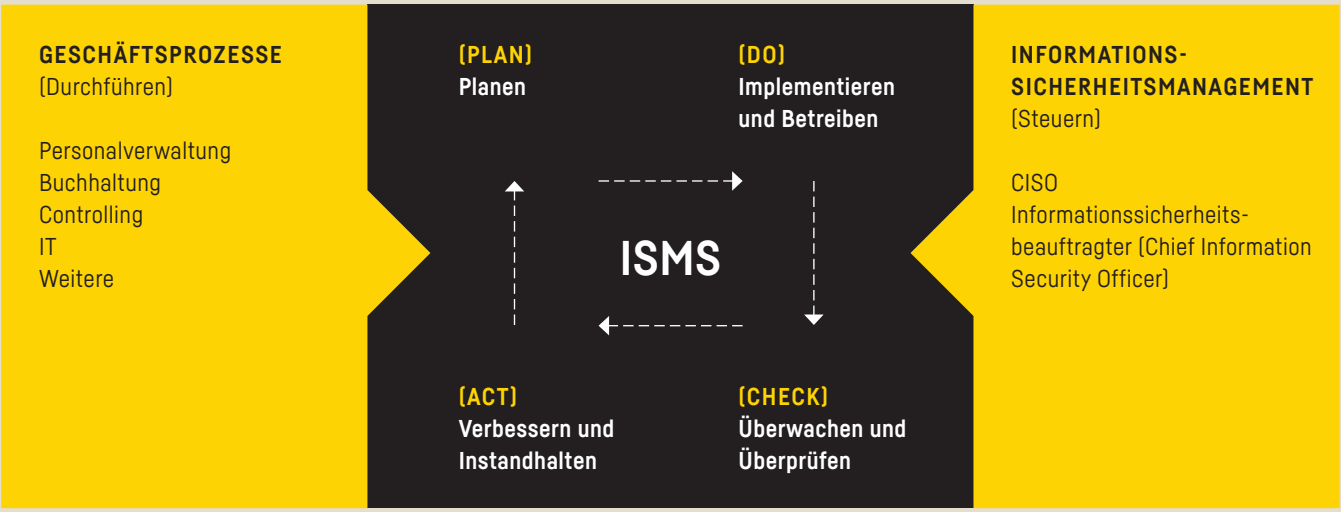
Die Frage, auf die wir an dieser Stelle eine Antwort finden werden, ist, mit welchem Aufwand der Schutz Ihrer „Kronjuwelen“ angemessen und vertretbar ist?

Anders gefragt: Welche Risiken sind Sie bereit einzugehen?

- Was könnte schlimmstenfalls passieren, wenn ein Schadensfall eintritt?
- Was würden Schutzmaßnahmen kosten, um Assets vollständig abzusichern und allen denkbaren Risikoszenarien vorzubeugen?
- Stehen diese Schutzmaßnahmen im Verhältnis zum schlimmstenfalls eintretenden Schadensfall oder übersteigt der Aufwand den möglichen Schaden?
- Was ist, nach Abwägung von möglichem Schadensfall und Aufwand, ein dem Asset angemessener Schutz?

Mit diesem risikobasierten Ansatz erkennen wir, bei welchem Asset welcher Handlungsbedarf in welchem Umfang besteht. Mit dieser Risikobehandlung erzielen wir den nach Risikoabwägung angemessenen Schutz.

ISMS – Die Unternehmenskultur der Verbesserung



Mit welchen Assets beginnen wir? Das ISMS in Betrieb nehmen

Nach Auswertung von GAP- und Risikoanalyse haben wir einen Überblick über den Ist-Zustand der Informationssicherheit innerhalb der Organisation gewonnen.

Wir kennen die „Kronjuwelen" unter den materiellen und immateriellen Assets, die im Scope sind, denen in dieser Phase die ganze Aufmerksamkeit gehört.

WELCHE SCHUTZMASSNAHMEN BESTEHEN FÜR DIESE ASSETS BEREITS?

WELCHE VERBESSERUNGEN SIND NOTWENDIG, UM EIN FÜR DIESE KRONJUWELEN ANGEMESSENES SICHERHEITSNIVEAU ZU ERREICHEN?

Mit Umsetzung der formulierten Verbesserungsschritte nehmen wir das ISMS in Betrieb.

ISMS – Kreislauf für kontinuierliche Verbesserung

Das etablierte Informationssicherheits-Managementsystems (ISMS) ist ein lebendiger Kreislauf mit der Zielsetzung, alle geplanten und implementierten Prozesse kontinuierlich zu verbessern.

Bei der Umsetzung orientieren wir uns an gängigen Standards wie ISO/IEC 27001, VDS10000 oder BSI-Grundschutz.

Mit der Implementierung des ISMS als Kreislauf haben wir eine Konstante für Verbesserung ins Leben gerufen, die nun zum Tagesgeschäft einer Organisation gehört wie Buchhaltung und Vertrieb, Produktion und Montage, Angebotserstellung und Auslieferung.

- PLAN: planen & einrichten
- DO: implementieren & betreiben
- CHECK: überwachen & überprüfen
- ACT: verbessern & instand halten

Wann ist ein ISMS erfolgreich?

Organisationen sind mit einem ISMS dann erfolgreich, wenn sie das Prinzip der Verbesserung in ihre Unternehmenskultur integriert haben.

Diese Organisationen geben dem ISMS den Raum, die organisatorische Grundlage, die Ressourcen und den Stellenwert, um Informationswerte angemessen zu schützen und damit Unbefugten immer einen Schritt voraus zu sein.

ConSecur begleitet Sie bei diesem Prozess dauerhaft als externer Berater oder in der Rolle eines externen CISO.

Chief Information Security Officer (CISO)

Der CISO trägt innerhalb der Organisation die strategische Verantwortung für Informationssicherheit. Die Rolle des CISO kann von einem Mitarbeiter ausgefüllt werden oder von einem externen Partner wie der ConSecur GmbH.

Aufgaben eines CISO sind unter anderem

- strategische Verantwortung für Informationssicherheit
- Beratung des Managements / der Geschäftsleitung
- Verantwortung für das ISMS
- Führen der Informationssicherheits-Organisation
- Lenken und steuern des Informationssicherheits-Prozesses

Welche Zertifizierung benötigen Sie?

VERPFLICHTENDE ZERTIFIZIERUNG

Besitzt Ihre Organisation eine wichtige Bedeutung für das staatliche Gemeinwesen? In diesem Fall könnte es sein, dass Sie den Sicherheitsvorgaben der KritisV unterliegen und zu einer Zertifizierung Ihres ISMS verpflichtet sind.

ZERTIFIZIERUNG FÜR DEN GESCHÄFTSERFOLG

Es ist sehr gut vorstellbar, dass eine Zertifizierung einen positiven Beitrag für den Geschäftserfolg leistet. Im Einzelfall sind die Vor- und Nachteile mit allen firmeninternen Interessengruppen, unter Umständen auch mit externen Großkunden oder Partnern, abzuwägen.

Standards für Informationssicherheit

ConSecur
[security and consulting]

ConSecur GmbH

Als herstellerunabhängiges Beratungs- und Dienstleistungsunternehmen befasst sich die ConSecur GmbH mit der Planung und Umsetzung von Maßnahmen zur Informationssicherheit. Unsere Leidenschaft ist die Entwicklung, Bewertung und Realisierung von IT-Sicherheitskonzepten für Unternehmen. So beschützen wir die Information, die Sie täglich für Einkauf, Produktion, Dienstleistung, Logistik und Korrespondenz benötigen. ConSecur hat sich darauf spezialisiert Informationssicherheit an die Geschäftsprozesse im organisatorischen und informationstechnischen Umfeld anzubinden. Hierbei setzen wir auf die bestehenden unternehmerischen Prozesse und eingesetzten Technologien unserer Kunden auf. Wir etablieren lösungsorientierte, standardisierte und effiziente Maßnahmen, die unsere Kunden in die Lage versetzen, ihre informationstechnischen Risiken zu beherrschen und bestehenden regulatorischen Vorgaben zu genügen. Ziel unserer Arbeit ist es, nur berechtigten Personen den Zugriff auf Informationen zu gewähren und Informationen vor Übergriffen Unbefugter zu schützen

ConSecur – next level information security

ConSecur
[security and consulting]

ConSecur GmbH
Nödiker Straße 118
49716 Meppen

TEL.: +49 5931 9224-0
info@ConSecur.de
www.ConSecur.de