Case Study

techem - softwaregestütztes Sicherheitsmanagement mit QSEC

Informationssicherheits- und Risikomanagement als Managementaufgabe

Sebastian Fingerloos, IT Security Manager bei Techem, berichtet über Herausforderungen und Erfahrungen im Informationssicherheits- und Risikomanagement mit QSEC

Techem ist ein international agierender führender Anbieter für Energieabrechnungen und Energiemanagement. In Deutschland ist das Unternehmen Marktführer im Bereich der verbrauchsgerechten Erfassung und Abrechnung von Wärme und Wasser in Immobilien. Die Dienstleistungen von Techem umfassen den Energiebezug über die Erfassung und Abrechnung des Wärme- und Wasserverbrauchs bis hin zu detaillierten Analysen. Techem ist einer der führenden Servicepartner für grüne und smarte Gebäude. Der Fokus liegt auf Energieeffizienz entlang der gesamten Wertschöpfungskette in Immobilien. Das Unternehmen fördert Wohngesundheit, Prozesseffizienz und Klimaschutz. Der Hauptsitz des Unternehmens ist in Eschborn. Von hier aus steuert Techem mit ca. 3750 Mitarbeitern die weltweiten Aktivitäten. Dazu gehören ca. 60 Standorte in Deutschland und viele weitere Standorte in 20 weiteren europäischen Ländern. Ebenso betreibt Techem Niederlassungen in Brasilien und den Vereinigten Arabischen Emiraten.

Weltweit ist das Unternehmen in rund 150 Niederlassungen vertreten und führt die Erfassung und Abrechnung in 11 Millionen Haushalten durch.

Die Ausgangssituation

Ziel von Techem war es, ein performantes Informationssicherheitsmanagementsystem zu etablieren, um Risiken zukünftig nachhaltig und effizient bewerten zu können. Maßnahmen zur Risikobegegnung sollten daraus abgeleitet werden können und über den Reifegrad sollten Aktivitäten gemessen und weiterentwickelt werden. Eine grundsätzlich wichtige Anforderung dabei war, ein unternehmensweit einheitliches Vorgehen zu etablieren um vergleichbare, valide Daten als Grundlage für Entscheidungen zu generieren. In Bezug auf die Umsetzung dieser Ziele wurde schnell deutlich, dass bei der Komplexität der Aufgabenstellung und dem Umfang der Anforderungen die Umsetzung mit professioneller Softwareunterstützung im Vergleich zum Betrieb eines ISMS mit Bordmitteln oder einer Eigenentwicklung der wirtschaftlichste und effizienteste Ansatz sein würde.

Als Eckdaten für eine Softwareevaluierung wurden im ersten Schritt die Anforderungen an eine Softwarelösung definiert. Zusammengefasst sollte eine moderne datenbankbasierte Softwareunterstützung gefunden werden, die flexibel anpassbar alle Managementanforderungen inkl. des Risikomanagements vollumfänglich abdecken und sukzessive in die gesamte Organisation ausgerollt und implementiert werden kann.

Der Entscheidungsprozess - Warum QSEC?

Die wesentlichen Kriterien für eine Entscheidung seitens Techem in Richtung QSEC waren,

- die datenbankbasierte Webapplikation, die bereits im Standard umfangreichen Content offeriert und dennoch über Customizing flexibel an die individuellen Anforderungen von Techem anpassbar ist
- dass in QSEC alle Anforderungen aus dem Informationssicherheits- und Risikomanagement detailliert innerhalb der Lösung abgebildet und umgesetzt werden können
- die leicht verständliche, schulungsarme Usability mit umfassender Workflow-Unterstützung, durch die auch in den Fachabteilungen hohe Nutzerakzeptanz erzielt wird
- die unternehmensweite Etablierung der gleichen QSEC Methodik mit vergleichbaren Arbeitsergebnissen und aussagekräftigen Reports

QSEC konnte in den obengenannten Punkten den Anforderungen im Vergleich zu den anderen evaluierten Systemen am besten überzeugen.

Des Weiteren überzeugte der umfassende fachliche Content von QSEC mit unterschiedlichen Anwendermodi für Experten und Anwender aus den Fachabteilungen und die hohe Integration aller QSEC Module die Entscheider.

Case Study

Nexis GRC ist ein erfahrener ISMS Hersteller mit langjähriger Umsetzungserfahrung von ISMS und Risikomanagement-Projekten. Einerseits überzeugte die Kompetenz der Mitarbeiter von Nexis GRC und andererseits die flexible Handlungsweise eines Mittelstandsunternehmens.

Das Vorgehen zum Informationssicherheitsmanagement (ISMS) bei Techem

Für die Einführungs-, Einrichtungs- und Umsetzungsphase sowie den Betrieb des Techem-ISMS wurde nach den 4 Phasen (Plan-Do-Check-Act) des ISMS vorgegangen:

Plan **Einführungsphase**
Wissen über die Organisation (wer sind wir)?
Wissen über die Abläufe (was tun wir)?
Wissen über die Unternehmenswerte (was haben wir)?

DO **Einrichtungsphase**
Wer ist in der Organisation wofür zuständig?
Wie ist der ISMS-Reifegrad?
Was wird in den Abläufen (Prozessen) verarbeitet?
Wie hoch ist der Schutzbedarf?
Welche Risiken müssen bearbeitet werden?

Check **Überprüfungsphase**
Interne Assessments
Zertifizierung nach ISO/IEC 27001

Act **Regelmäßige Anpassungen**
Was hat sich geändert?
Was muss neu geplant werden?

Projektbeschreibung

Die Umsetzung des Projekts „ISMS-Tooleinführung mit QSEC“ startete ca. Mitte 2019.

In der ersten Projektphase (Plan-Phase) wurde QSEC nach den Vorgaben von Techem ausgeprägt, wobei die ISO/IEC 27001 für die ISMS- und die ISO/IEC 27005 für die Risiko- Anforderungen im Mittelpunkt standen. Die Konzepte für Unternehmensstruktur und Untersuchungsbereiche wurden erstellt und in das QSEC-System übernommen.

Dabei wurde bereits mit der Planung festgelegt, dass die gesamte Organisation betrachtet wird, aber in der ersten Phase nur die Unternehmenszentrale in Eschborn auditiert werden soll. Im Zuge dieser Planung wurde die gesamte Legal-Entity-Struktur erfasst und die Berechtigungsanforderungen festgelegt. Alle in der AD für die QSEC-Nutzung festgelegten Mitarbeiter wurden importiert und können sich über Single Sign On (SSO) anmelden. Die erforderlichen Dokumente (Leitlinien, Richtlinien etc.) wurden erstellt, verabschiedet, ins System übernommen und mit den Controls der ISO/IEC 27001 verbunden.

Ebenso wurde in dieser Projektphase die Controls der ISO/IEC 27001 Annex A reifegradbewertet und als SoA (Statement of Applicability) abgeleitet.

Die Ablauforganisation mit allen Prozessen wurde aus bestehenden Excel-Dateien übernommen bzw. manuell ergänzt. Die Unternehmenswerte (Infrastruktur, IT-Systeme etc.) wurden strukturiert und gruppiert in QSEC übernommen bzw. erfasst.

In der Einrichtungsphase (Do-Phase) wurden die Geschäftsprozesse, Schwerpunkt Kernprozesse, mit Informationsobjekten verbunden und die Kritikalität (Vertraulichkeit, Integrität, Verfügbarkeit) bewertet und mit den notwendigen Unternehmenswerten (Assets) verbunden. Für die verbundenen Assets wurden aufgrund der Einstufungen der Prozesse bzw. Informationen der Schutzbedarf bestimmt. Damit konnten die Asset (-Gruppen) im Risikomanagement aufgrund der verbundenen Risikokataloge (individualisierter Bedrohungs- und Schwachstellenkataloge) risikobewertet werden. Die ermittelten Risiken je Asset wurden in einem Risikobehandlungsplan bewertet.

Besonders hervorzuheben ist die erfreulich reibungslose Einbindung der Fachabteilungen in die Prozessbewertung, die u.a. durch die anwenderfreundliche und schulungsarme Integration von Workflows in QSEC erzielt wurde.

In der in Vorbereitung befindlichen Check-Phase ist mit Unterstützung des Vorstandes eine ISO27001-Zertifizierung für Mitte 2022 geplant.

Weiterer Ausblick/Planungen:
Es wird aktuell geprüft, ob bei Techem auch weitere Themen wie z.B. das Qualitätsmanagement mit in QSEC abgebildet werden sollen.

FAZIT

Techem hat mit QSEC ein Informationssicherheits- und Risikomanagementsystem eingeführt, über das alle zugehörigen Aktivitäten nachhaltig umgesetzt, dargestellt und lückenlos belegt werden können. Die Erkenntnisse aus der Umsetzung der Anforderungen ermöglicht alle compliance- und risikorelevanten Entscheidungen auf Basis einer validen Datengrundlage zu treffen. Die Partnerschaft mit Nexis GRC hat sich in jeder Projektphase als vertrauensvoll und kompetent erwiesen.

„Die in QSEC im Standard bereits integrierten Methoden und Prozesse haben uns wesentlich beim professionellen Aufbau und Betrieb unseres Informationssicherheitsmanagementsystems unterstützt. Die Reifegradbetrachtung und -entwicklung ermöglichen es unser Techem-ISMS mit QSEC ressourcensparend kontinuierlich zu betreiben, zu monitoren und weiterzuentwickeln.“
Sebastian Fingerloos: Head of Information Security

Kontakt
Nexis GRC GmbH • Zimmerstraße 1, 22085 Hamburg • +49 40 650336-0 • info@nexis-qsec.com