STUDIE ZUR UMSETZUNG UND ZUM REIFEGRAD DES ISMS

Umfrage unter den 750 itSMF-Mitgliedern

KRZYSZTOF PASCHKE • KPASCHKE@GRC-PARTNER.DE • WWW.GRC-PARTNER.DE

Im November 2016 organisierte das **itSMF**-Fachforum „**Cyber Defense**“ unter der Leitung von Krzysztof Paschke eine Umfrage zur Umsetzung und zum Reifegrad des Managementsystems für Informationssicherheit (ISMS) unter den 750 **itSMF**-Mitgliedern (Wirtschaftsunternehmen und Institutionen der Öffentlichen Verwaltung).

Es ging darum zu erfahren, welche Themen für künftige Veranstaltungen und Projekte des Fachforums für die Teilnehmer von Bedeutung sind. Die Umfrage befasste sich ganzheitlich mit dem ISMS-Prozess: von der Planung und Umsetzung bis hin zur Aufrechterhaltung und Verbesserung. Ziel der Umfrage war die Beantwortung folgender Fragen:

- Wie gut sind die **itSMF**-Mitglieder bereits auf Cyber-Angriffe vorbereitet?
- Welche Standards haben sie für die Umsetzung des ISMS verwendet?
- Mit welchen Problemen wurden bzw. sind sie konfrontiert?
- Welchen Beitrag kann das Fachforum „**Cyber Defense**“ für die **itSMF**-Mitglieder bei der Umsetzung und Verbesserung eines ISMS leisten?

Die Umfrageorganisation übernahm **itSMS** GmbH, die Geschäftsstelle von **itSMF**. Die statistische Auswertung der anonymisierten Umfrageergebnisse erfolgte durch die Leitung des Fachforums.

ZUSAMMENFASSUNG DER ERGEBNISSE

UNTERNEHMENSGRÖSSE – An der Umfrage haben insgesamt 58 Unternehmen und Behörden teilgenommen. Davon sind 46% der Organisationen einer Größe von bis zu 999 Mitarbeitern, 33% bis zu 4.999 Mitarbeitern und 21% Konzernen mit 10.000 Mitarbeitern und mehr zuzuordnen. Etwa 21% der befragten Organisationen gehören zur KRITIS, also zu Organisationen mit besonderer Bedeutung für das staatliche Gemeinwesen.

BRANCHE DER KRITIS – Bei KRITIS Organisationen steht die IT- und Telekommunikationsbranche mit über 46% an erster Stelle, gefolgt von der Energie- und Wasserwirtschaft mit 30%. Die öffentliche Hand und Transport und Verkehr teilen sich den dritten Rang der Befragten mit jeweils 15%, gefolgt von der Gesundheitsbranche mit 8%.

BRANCHE ALLGEMEIN – Bei der Betrachtung der Geschäftstätigkeit der nicht-KRITIS Organisationen steht die IT- und Telekommunikationsbranche mit über 46% an erster Stelle, gefolgt von der Dienstleistungsbranche mit 28%. Die öffentliche Hand belegt den dritten Rang mit jeweils 12% gefolgt von Hochschulen mit 6%.

UMSETZUNGSGRAD DES ISMS – Bei mehr als 30% der Befragten ist ein sehr hoher Reifegrad in der Umsetzung des ISMS erreicht worden, d.h. vollständig umgesetzt und dokumentiert. Genau 30% der Organisationen haben das ISMS partiell (Teilbereiche der Organisation) umgesetzt. Rund 12% der Befragten haben die Einführung des ISMS beschlossen, eine Umsetzung jedoch noch nicht begonnen. Jeweils 6% entfallen auf Organisationen, die zurzeit keine Einführung des ISMS planen oder deren Status unbekannt ist. Eine erfolgreiche Zertifizierung des ISMS haben 29% der Befragten vorzuweisen.

MOTIVATION – Als wesentlichen Grund für die Umsetzung des ISMS sind 63% der Teilnehmer ihren Sorgfaltspflichten gefolgt. Von denen haben 42% interne/externe Audits als Grund angegeben. Eine Erfüllung der geltenden Gesetze und Auflagen der Behörden nannten 45%. Die Anforderung an Geschäftspartner ist für 30% der Motivator für die Umsetzung. Mehrfachnennungen waren möglich.

HINDERNISSE – Die überwiegende Mehrheit der Befragten (76%) nannte fehlende personelle Ressourcen als Haupthindernis. Knapp 69% der Befragten haben als Grund die Überzeugung der Organisationsleitung und der Mitarbeiter genannt, gefolgt

von fehlenden finanziellen Mitteln (36%). Etwa 29% der Befragten gaben nicht ausreichend vorhandene Kenntnisse über die Planung und Umsetzung eines ISMS als Hindernis an. Mehrfachnennungen waren möglich.

STANDARDS – Mehr als 74% der Befragten haben die Norm ISO/IEC 27001 umgesetzt, gefolgt vom IT-Grundschutz (BSI-Standard 100-1, 100-2 und 100-3) mit 33%. Knapp 5% der Befragten haben die im Jahr 2016 veröffentlichte VdS Richtlinie 3473 ausgewählt.

RISIKOANALYSE – Die Mehrheit von 57% der Befragten führte die Risikoanalyse gemäß der ISO/IEC 27005 durch, gefolgt vom BSI-Standard 100-3 (33%). Die Norm ISO 31001 ist genau bei 10% der Befragten verwendet worden.

ISMS-TOOL – Über 87% der Befragten nutzen MS Office für die Dokumentation des ISMS gefolgt von Dokumentmanagementsystemen (DMS) 22%. Eine speziell für die Planung, Umsetzung und Dokumentation eines ISMS konzipierte Software nutzen 12% der Implementierer. Eine Mehrfachnennung war möglich.

Im zweiten Teil der Umfrage wurden gezielt Fragen zu den **zukünftigen Aktivitäten des Fachforums „Cyber Defense“** gestellt. Hier eine Zusammenfassung der Ergebnisse:

AKTIVITÄTEN DES FACHFORUMS

57% der Befragten hat den Wunsch nach Informationsworkshops zu ausgewählten ISMS Themen geäußert, gefolgt von Beiträgen (56%) in der *it*SMF Fachzeitschrift und Projektarbeiten zur Erarbeitung von Positionspapieren etc. zu ausgewählten Themen (47%).

AKTIVITÄTEN BEI VERANSTALTUNGEN

- Regionale Foren: 49%
- L!VE Event: 36%
- Jahreskongress: 33%.

FAZIT

Die Studie basiert auf 58 validen Datensätzen. 30% der Befragten haben einen sehr hohen Reifegrad des ISMS erreicht. Nur 6% der Teilnehmer der Umfrage planen zurzeit keine Einführung. Sehr positiv sind die Sorgfaltspflichten als primäre Motivation für die Umsetzung der betrieblichen Kontinuität zu bewerten. Die nicht verfügbaren Ressourcen (76%) bei der Einführung des ISMS sind ein wichtiger Hinweis für die Verantwortlichen in den Organisationen. Die Befragung zeigt, dass Informationsworkshops zu ausgewählten Themen gefolgt von Beiträgen und Veranstaltungen unterschiedlicher Art die interessantesten Varianten zur Vertiefung der Kenntnisse der *it*SMF-Mitglieder sind.