

Das Sicherheitsmanagement-System für das System Maritime Verkehrstechnik (SiMaS-SMV)

Dipl.-Ing. Jan-Hendrik Oltmann, WSD Nord

Das küstenweite System Maritime Verkehrstechnik (SMV) unterstützt die Prozesse der Maritimen Verkehrs-sicherung u. a. durch Bereitstellung

- navigations-relevanter Daten für die Schifffahrt (z. B. mittels Funknavigationsdiensten oder mittels der visuellen Schifffahrtszeichendienste),
- von Schiffsverkehrsdaten für die Aufgaben der WSV, nämlich insbesondere für die Verkehrszentralen, und
- Schiffsverkehrsdaten für angeschlossene Dritte, also für Behörden und privaten Einrichtungen, im Rahmen geltender gesetzlicher Bestimmungen zu deren jeweiliger Aufgabenerfüllung.

Das SMV wird von den jeweils örtlich zuständigen Behörden der WSV des Bundes an der deutschen Küste gemeinsam und behördenübergreifend geplant, errichtet und betrieben.¹

Die küstenweite Erstreckung und der ganzheitliche Ansatz des SMV bedingen eine ebenso ganzheitliche Betrachtung der Sicherheit des SMV über Zuständigkeitsgrenzen dieser Behörden hinweg.

Die Bundesregierung hat bereits in der letzten Legislaturperiode einen sogenannten „Umsetzungsplan Bund (UP Bund)“ beschlossen. Dieser bezweckt, die Sicherheit der „Informationstechnik“ in der gesamten Bundesverwaltung zu gewährleisten, indem ein flächendeckender Mindeststandard für die Sicherheit der „Informationstechnik“ etabliert wird.

Dabei bilden einschlägige Standards des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) den notwendigen inhaltlichen Rahmen in sinngemäß übertragener Anwendung.

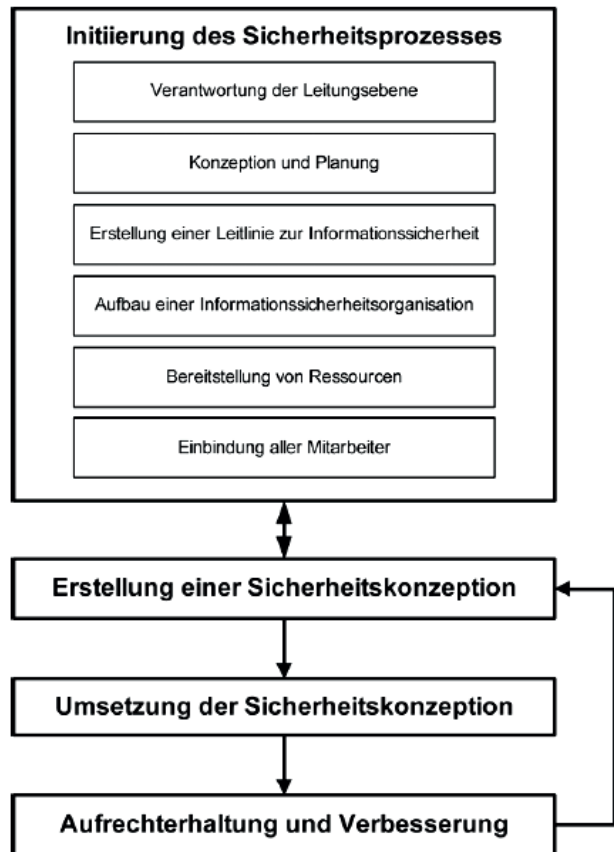


Abb. 1: Phasen des Sicherheitsprozesses

¹ Eine ausführliche Darstellung des SMV ist in dem Jahresbericht der WSD Nord 2008 enthalten.

Seitens des Bundesministeriums für Verkehr, Bau und Stadtentwicklung ist für das SMV ein so genannter „SMV-Sicherheitsprozess“ eingeleitet worden, der die spezifische fachliche Ausprägung des SMV gegenüber der allgemeinen Beschreibung eines Sicherheitsprozesses (vgl. Abb. 1; Quelle: BSI-Standard 100-2²) berücksichtigt. In den kommenden Jahren soll so ein Sicherheits-Management-System für das SMV (SiMaS-SMV) eingerichtet werden, angesiedelt im unmittelbaren Verantwortungsbereich der Leitungen der Küstendirektionen.

Das SiMaS-SMV wird in Analogie zum BSI-Standard nach seiner Einführung u. a. umfassen:

- eine SMV-Sicherheitsleitlinie, die beschreibt, „für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit hergestellt werden soll. Sie beinhaltet die angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Die Sicherheitsleitlinie beschreibt damit auch über die Sicherheitsziele das angestrebte Sicherheitsniveau. Sie ist somit Anspruch und Aussage zugleich, dass dieses Sicherheitsniveau erreicht werden soll.“ (gekürztes Zitat BSI-Standard 100-2, S. 21, § 3.3)
- ein SMV-Sicherheitskonzept, das eine strukturierte und dokumentierte Vorgehensweise zur Abwehr möglicher Angriffs- und Schadensszenarien darstellt.

Es umfasst die Beschreibung des SMV als Informationsverbund unter Sicherheits Gesichtspunkten, die Risikobewertung sowie die daher zu ergreifenden Sicherheitsmaßnahmen. Das SMV-Sicherheitskonzept unterliegt wie die SMV-Sicherheitskonzeption einem Lebenszyklus im Rahmen des SMV-Sicherheitsprozesses.

- eine SMV-Sicherheitskonzeption: Die SMV-Sicherheitskonzeption ist die in Umsetzung des SMV-Sicherheitskonzeptes gelebte und in der Praxis ausgestaltete Gesamtheit aller sicherheitsrelevanter Maßnahmen, Planungen und Dokumentationen zu einem gegebenen Zeitpunkt. Die erfolgreiche Umsetzung kann durch Zertifizierung nach ISO 27001 („BSI-Zertifikat“) nachgewiesen werden. Die SMV-Sicherheitskonzeption wird auch nach erstmaliger Erstellung und Umsetzung laufend aufrecht erhalten und kontinuierlich verbessert.
- eine SMV-Sicherheitsorganisation: Es wird eine gemeinsame Stabstelle beider Küstendirektionen für SMV-Sicherheit eingerichtet.

Nach erfolgreicher Einführung des Sicherheits-Management-Systems für das SMV (SiMaS-SMV) wird das SMV die Maritime Verkehrssicherung also mit dem dann erreichten Sicherheitsniveau unterstützen können.

² Bundesamt für die Sicherheit in der Informationstechnik. 2008. BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise. V2.0