Bundesamt
für Sicherheit in der
Informationstechnik

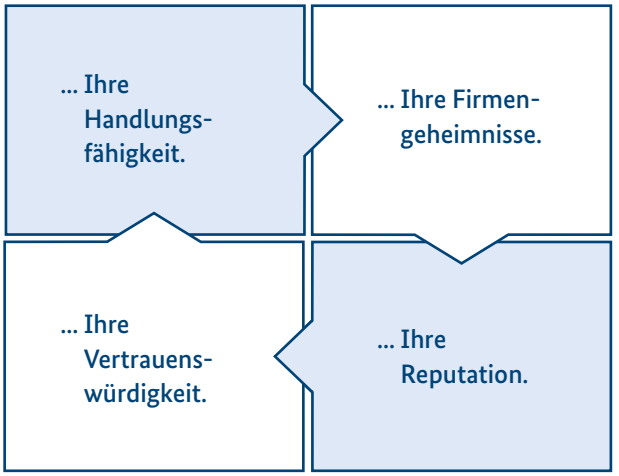
Deutschland
Digital•Sicher•BSI•

Grundlagen des Cyber-Supply Chain Risk Management (C-SCRM)

Effektives Cyber-Supply Chain Risk Management in 5 Schritten

Der Schutz Ihres Unternehmens vor Cyberrisiken in einer digital vernetzten Welt erfordert ein Verständnis für die (Cyber-)Sicherheitsrisiken, die in Verbindung mit der Lieferkette stehen. Um diese Risiken bewältigen zu können und die Resilienz Ihres Unternehmens zu stärken, bedarf es eines ganzheitlichen Cyber-Supply Chain Risk Management, kurz C-SCRM.

Lieferketten Risiken bedrohen...



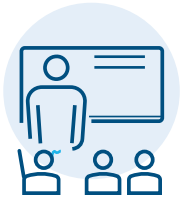
Effektives Cyber-Supply Chain Risk Management in 5 Schritten

Folgende 5 Schritte helfen Ihnen, ein effektives Cyber-Supply Chain Risk Management zu etablieren, um angemessen auf Gefahren in der Lieferkette reagieren zu können:

1. **Identifizieren** Sie alle Mitarbeitenden, die in Verbindung mit der Lieferkette stehen.
2. **Entwickeln** Sie die Richtlinien, Strategien und Prozesse zum Schutz Ihrer Lieferkette.
3. **Wissen** Sie, welche Hardware, Software und Dienstleistungen Sie beziehen und woher.
4. **Erlangen** Sie ein tieferes Verständnis Ihrer Lieferkette und Ihrer Zulieferer.
5. **Evaluieren** Sie die Effektivität Ihrer Lieferkettenpraktiken.

Expertise bündeln

Identifizieren Sie alle Mitarbeitenden, die in Verbindung mit der Lieferkette stehen. Lieferkettensicherheit ist ein vielschichtiges und abteilungsübergreifendes Thema. Bilden Sie ein Team mit Vertreterinnen und Vertretern aller relevanten Abteilungen, wie etwa IT-Sicherheit, Produktentwicklung, Recht, Logistik, Beschaffung oder Marketing, um die verschiedenen Perspektiven und Expertisen zusammenzubringen. Nur durch enge Zusammenarbeit der verschiedenen Abteilungen kann ein ganzheitliches Verständnis gewonnen und die richtige strategische Entscheidung getroffen werden.



Standards schaffen

Entwickeln Sie Richtlinien, Strategien und Prozesse, um Risiken in der Lieferkette begegnen zu können. Stellen Sie standardisierte Prozesse für das Supply Chain Risk Management her und stellen Sie sicher, dass Best Practices, Industriestandards und insbesondere rechtliche Vorgaben berücksichtigt werden. Legen Sie ebenfalls Vorgaben für Ihre Lieferanten fest. Achten Sie stets auf die Angemessenheit Ihrer Maßnahmen.

Assets überwachen und dokumentieren

Sorgen Sie dafür, dass Sie wissen, welche Hardware, Software und Dienstleistungen Ihre Firma von wem bezieht und nutzt. Listen Sie alle Assets auf, die Sie für den Geschäftsbetrieb benötigen oder die in Zusammenhang mit kritischen Vermögenswerten stehen und kennen Sie ihre jeweiligen Zulieferer. Priorisieren Sie ihre Assets entsprechend ihrer Kritikalität für den Geschäftsbetrieb bzw. ihrer möglichen negativen Auswirkungen auf Ihr Unternehmen oder Ihre Kunden. Tragen Sie weiterhin Sorge dafür, dass der gesamte Lebenszyklus Ihrer Assets überwacht und dokumentiert wird.

Kontakte zu Lieferanten und Dienstleistern pflegen

Erlangen Sie ein tieferes Verständnis für Ihre Lieferkette und Ihre Zulieferer. Lieferketten erstrecken sich oftmals über viele Unternehmen weltweit. Um Risiken managen zu können, welche sich aus der Beziehung Ihrer Zulieferer zu deren Zulieferern oder aus anderen technischen und nicht-technischen Einflüssen ergeben, sollten Sie die bestmögliche Transparenz schaffen. Stellen Sie sicher, dass Sie einen engen Kontakt zu Ihren Lieferanten pflegen. Führen Sie entsprechende Kontrollstrukturen und Kommunikationspläne ein, um festzustellen, ob Ihre Zulieferer über eine angemessene Sicherheitskultur verfügen.

Maßnahmen überprüfen

Evaluieren Sie regelmäßig die Effektivität Ihres C-SCRM. Entwickeln Sie die benötigten Metriken, mit denen Sie die Effektivität Ihrer Maßnahmen überprüfen können. Bestimmen Sie, in welcher Frequenz eine Überprüfung stattfinden soll und ggf. Änderungen vorgenommen werden sollen. Nur so können Sie dauerhaft sicherstellen, dass Sie angemessen auf (Cyber-)Sicherheitsrisiken und Disruptionen in Ihrer Lieferkette reagieren können.

Weitere Informationen auf der BSI-Webseite

Impressum

Bundesamt für Sicherheit
in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: 0800 274 1000
E-Mail: bsi@bsi.bund.de
www.bsi.bund.de

Bildnachweis
Adobe Stock / KanawatTH

Stand
Oktober 2023