Cyber Supply Chain Risk Management

Studiengang: MAS Cyber Security

Der „Solarwinds Incident“ Ende 2020 erhielt weltweite Aufmerksamkeit. Viele Organisationen überlegten sich, mit welchen Massnahmen die eigene Sicherheit in der Lieferantenbeziehung besser auf einen ähnlichen Fall vorbereitet werden könnte. So auch das Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements (ISC-EJPD). Die Studie zeichnet den Diskurs nach und gibt eine auf den Software-Entwicklungsprozess beim ISC-EJPD angepasste Empfehlung ab.

Diskurs

Der Solarwinds Incident hat einen Niederschlag in einer Vielzahl von Standards, Frameworks und Best Practices gefunden, welche angepasst und neu erstellt wurden. Die Studie verfolgt diesen Diskurs sowohl in den USA wie auch in der Schweiz, stets in Hinsicht darauf, was sich am besten für die Bedürfnisse des ISC-EJPD eignet. Schlussendlich identifiziert die Studie eine Serie von drei Dokumenten, welche zwischen August und Oktober 2022 von der Arbeitsgruppe Enduring Security Framework (ESF) erstellt wurden. Die Serie „Securing the Software Supply Chain“ richtet sich in Form eines Recommended Practice Guides an die jeweiligen Rollen innerhalb des Software-Lifecycles: Developer, Supplier und Customer. Die Serie selbst stützt sich stark auf das revidierte Secure Software Development Framework (SSDF) NIST SP 800-218 ab.

Definition

In einem zweiten Schritt geht es darum, das Cyber Supply Chain Risk Management (CSCRM) für den weiteren Verlauf der Studie zu definieren. CSCRM ist ein sehr weitgehender Begriff. Zentral ist das Verständnis, dass der Gegenstand des Risk Managements nicht ein Angriff auf eine Supply Chain, sondern ein Angriff über eine Supply Chain ist. Dabei wird zwischen Lieferanten und Kunden unterschieden. Der Angriff erfolgt immer über mindestens einen Lieferanten und zielt auf die Assets des Kunden ab. Die Studie wendet die Taxonomy der EU Agency for Cybersecurity (ENISA) für Supply Chain Attacks an, welche es ermöglicht, bestimmte Muster zu erkennen und basierend darauf Annahmen für die weitere Entwicklung zu treffen. Durch den Diskurs und die Definition wird der Fokus immer wie enger.

Anwendung

Schlussendlich werden die bisherigen Erkenntnisse auf das Umfeld des ISC-EJPDs angewandt, spezifisch auf die Zusammenarbeit mit Lieferanten in der Software-Entwicklung beim ISC-EJPD. Die bis hierher gesammelten Empfehlungen richten sich in der Regel an eine spezifische Rolle im Software-Lifecycle. Das ISC-EJPD ist jedoch in einer Doppelrolle als Developer und Customer. Dadurch ergeben sich für das ISC-EJPD im Kontext des SSDFs Möglichkeiten, die sich einem reinen Customer entziehen. Die Idee ist, dass auf die Lieferanten eine mindestens gleichhohe SSDF-Maturität vertraglich übertragen werden soll. Voraussetzung dafür ist, dass das ISC-EJPD ein SSDF konsequent umsetzt.

Martin Trutmann