Medizingeräte-Software: Weniger Risiko, mehr Cybersicherheit

Warum an TARA kein Unternehmen vorbei kommt

Die Bedrohungsanalyse und Risikobewertung (Threat Analysis and Risk Assessment / TARA) ist entscheidend für die Entwicklung und Bereitstellung von sicherer Software. TARA identifiziert und schließt kostspielige Lücken in der Cybersicherheit. Daher sollten TARA-Methoden effektiv und in den Software Development Life Cycle (SDLC) und das eigene Entwicklungsökosystem integrierbar sein. Die Auswahl der richtigen Tools zur TARA-Ergänzung ist maßgeblich für die Bereitstellung sicherer Softwaresysteme.

TARA zeigt Schwachstellen auf

Einfach ausgedrückt ist TARA ein Prozess zur Identifizierung potenzieller Risikofaktoren, Schwachstellen und nicht konformer Elemente in Software. Es hilft Entwicklungsteams, unsichere Stellen im Code oder Konformitätsprobleme zu identifizieren. Dadurch können Abhilfemaßnahmen und Sicherheitsimplementierungen früher im SDLC erfolgen. Ein Beispiel ist die Konformität mit ISO 62443, die auch für medizinische Software relevant ist.

TARA zeigt Schwachstellen auf und gibt Hinweise zur Integration von Sicherheitsmaßnahmen in die Entwicklungsarbeit. Im schlimmsten Fall verhindert TARA die Markteinführung eines Produkts oder einer Dienstleistung und spart so Entwicklungszeit und Geld. TARA ist wie ein jährlicher Gesundheitscheck: eine kleine Unannehmlichkeit, die vor echten Problemen schützen kann.

Vier Schritte zu mehr Sicherheit

Bild 1 zeigt den Ablauf bei einer TARA-Methode.

Projektdefinition

Hier wird festgelegt, was aufgebaut werden soll – von grundlegenden Funktionen bis hin zu hochkomplexen Eigenschaften - und sichergestellt, dass alle beteiligten Ressourcen wie u. a. Netzwerkkomponenten, Anwendungen, berücksichtigt werden.

Bedrohungserkennung und Risikobewertung

Es ist nicht zielführend, eine Risikostrategie zu entwickeln, ohne die wichtigsten Bedrohungen zu kennen. Das eigene Projekt muss gründlich auf Problempotenzial untersucht werden. Kenntnis aller potenziellen Bedrohungen ist entscheidend für die Entwicklung einer TARA-Strategie.

Abwehr der Bedrohung

Als nächstes müssen mögliche Bedrohungen und Risikovektoren entschärft werden, z. B. durch die Integration von SEI CERT, einer Sicherheitscode-Analyse, in die CI/CD-Pipeline. Weitere Testmethoden sind API-Sicherheitstests und Tests nach eigenen Sicherheitsanforderungen. Vorteilhaft ist hier der Einsatz einer modernen Lösung automatisiert Unit-Tests, Integrationstests, Systemtests und Code Coverage und gewährleistet so die Vollständigkeit der Tests. Die automatische Generierung von Testfällen reduziert Aufwand und .Kosten und liefert durch automatisierte Reports und Analysen verwertbares Feedback.

Umsetzung und Validierung

In dieser Phase wird sichergestellt, dass die identifizierten Bedrohungen das akzeptable Risikoniveau nicht überschreiten und die verbleibenden Risiken ebenfalls innerhalb akzeptabler Parameter liegen.

Risikomatrizen und andere Messtechniken

Da nicht für jedes Projekt die gleiche Risikobewertung geeignet ist, gibt es verschiedene Methoden, um die Wahrscheinlichkeiten und Auswirkungen von Schwachstellen zu messen. Eine der gebräuchlichsten Optionen ist eine Bedrohungsmatrix (3×3-, 4×4- oder 5×5). Es gibt jedoch auch andere Möglichkeiten:

- **Entscheidungsbaum:** Diese Vorlage kann verwendet werden, um verschiedene Ergebnisse und ihre Wahrscheinlichkeit zu visualisieren und den potenziellen Wert des Projekts, der Dienstleistung oder des Produkts zu berechnen (Bild 2).
- **Bowtie-Modell:** Dieser Ansatz zeigt kausale Zusammenhänge zwischen Bedrohungsquellen und möglichen Folgen auf (Bild 3).

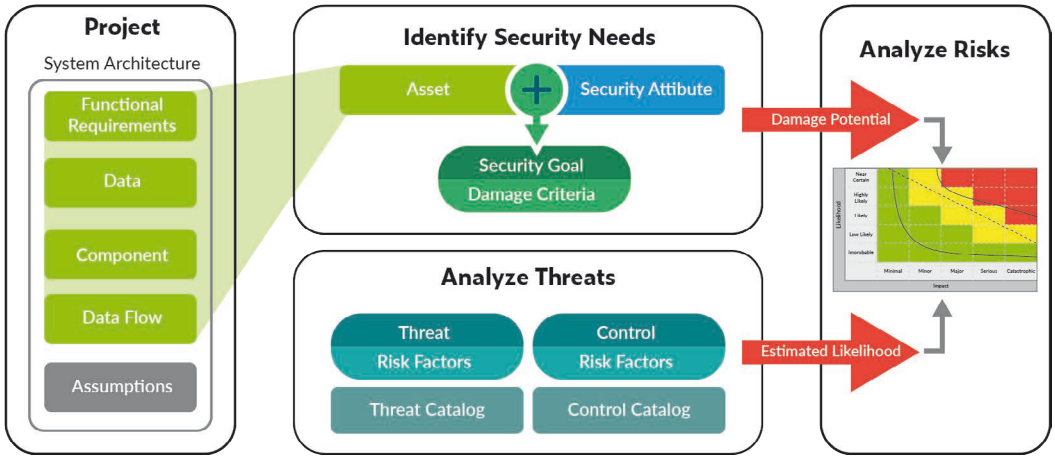

Bild 1: Der Ablauf einer TARA-Methode besteht aus mehreren Schritten. Alle Bilder © Parasoft

Autor:
Ricardo Camacho
Director of
Safety & Security Compliance
Parasoft
https://de.parasoft.com/

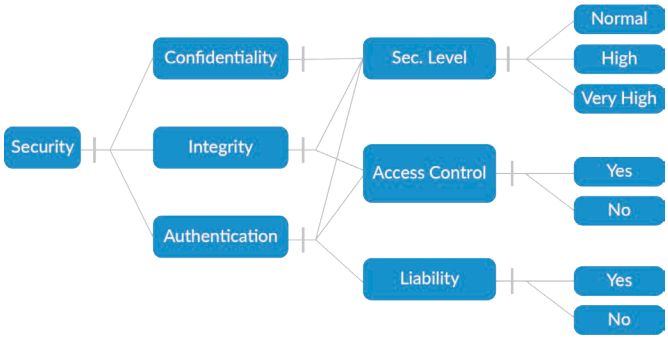

Bild 2: Innerhalb einer TARA ist ein Entscheidungsbaum eine Option zur Risikobewertung für ein Softwareprojekt.

Bild 4: Viele Unternehmen setzen heute die CI/CD-Pipeline zur Rationalisierung ihrer Softwareentwicklung ein.

- **Failure Mode an Effects Analysis (FMEA):** Diese Analyse wurde erstmals in den 1940er Jahren beim US-Militär eingesetzt. Sie eignet sich am besten für die Angebots- oder Entwurfsphase eines Projekts.

Herausforderungen für TARA

Die Vielzahl an Ansätzen und Rahmenwerken zur Bewertung von Cybersicherheitsrisiken, erschwert die Durchführung von Bedrohungsanalysen und Risikobewertungen. Eine große Herausforderung ist die Identifizierung aller potenziellen Bedrohungen und Risikovektoren. Die Integration von Sicherheitsprozessen in die Entwicklung kann für manche Teams eine große Hürde darstellen, wenn sie den darin liegenden Wert oder die Vorteile oder den Aufwand nicht erkennen.

Vernetzte Technologien haben längst Einzug in die Medizintechnik gehalten. Dies erhöht die Wichtigkeit der Implementierung und Verfeinerung von Sicherheitsstrategien. Die TARA-Methoden und -Tools unterscheiden sich in ihren Ansätzen und Vorteilen, um die verschiedenen Branchen und Arbeitsabläufe zu unterstützen.

Viele Bedrohungsmatrizen erfassen potenzielle Bedrohungen und die zu implementierenden Funktionen oder Schutzmaßnahmen. Dies entspricht anerkannten Sicherheitsanforderungen und den anzuwendenden Verifikations- und Validierungsmethoden (V&V). Voraussetzung dafür ist ein solides Anforderungsmanagement-Tool wie Polarion, Jama oder Codebeamer. Umfangreiche automatisierte SAST- und DAST-Lösungen verifizieren und validieren diese Anforderungen. Unternehmen wie itemis bieten auch Tools für das Management von Sicherheitsbedrohungen und -risiken an.

Sicherheitslücke schließen

Die Implementierung von QA (Quality Assurance) in die eigene CI/CD-Pipeline (Bild 4) ist eine Sache – die Gewährleistung von Sicherheit in jedem Schritt der Automatisierung kann jedoch noch entscheidender sein. Wenn es etwa um die Konformität mit ISO 61508 geht, berücksichtigen statische Sicherheitstests (SAST) Standards wie CERT, CWE, OWASP und auch andere wie MISRA [1] und ISO 62443, die Sicherheitsrichtlinien enthalten. Die statische Analyse mit hochentwickelten Tools zusammen mit Unit-Tests, Compliance Reporting, Datenflussanalyse und anderen Funktionen ermöglicht es der CI/CD-Pipeline, auch Tests zu automatisieren. Damit kann das Entwicklungsteam seinen Softwareentwicklungszyklus erweitern.

Eigener TARA-Bedarf

Auch in der Medizintechnik ist die Sicherstellung der Konformität und Funktionalität sicherheitskritischer Elemente ein zentraler Aspekt der Entwicklung. So wie eine CI/CD-Pipeline Prozesse automatisiert, die Markteinführung verkürzt, genauere Testergebnisse liefert und Budgets effizienter nutzt, kann TARA Sicherheitsfehler und -bedrohungen reduzieren, Probleme entschärfen und nicht konforme Assets identifizieren.

Während Tests wie die statische Analyse die Einhaltung von Sicherheitsstandards unterstützen, bieten moderne Tools eine einheitliche Lösung für die Automatisierung von Softwaretests und die Erreichung von FuSa (Functional Safety)-Industriestandards umfasst. Sie sollten in keiner TARA fehlen.

Referenz

[1] “MISRA”, “MISRA C” und das triangle Logo sind eingetragene Marken von The MISRA Consortium Limited. ©The MISRA Consortium Limited, 2021. Alle Rechte vorbehalten. ◄

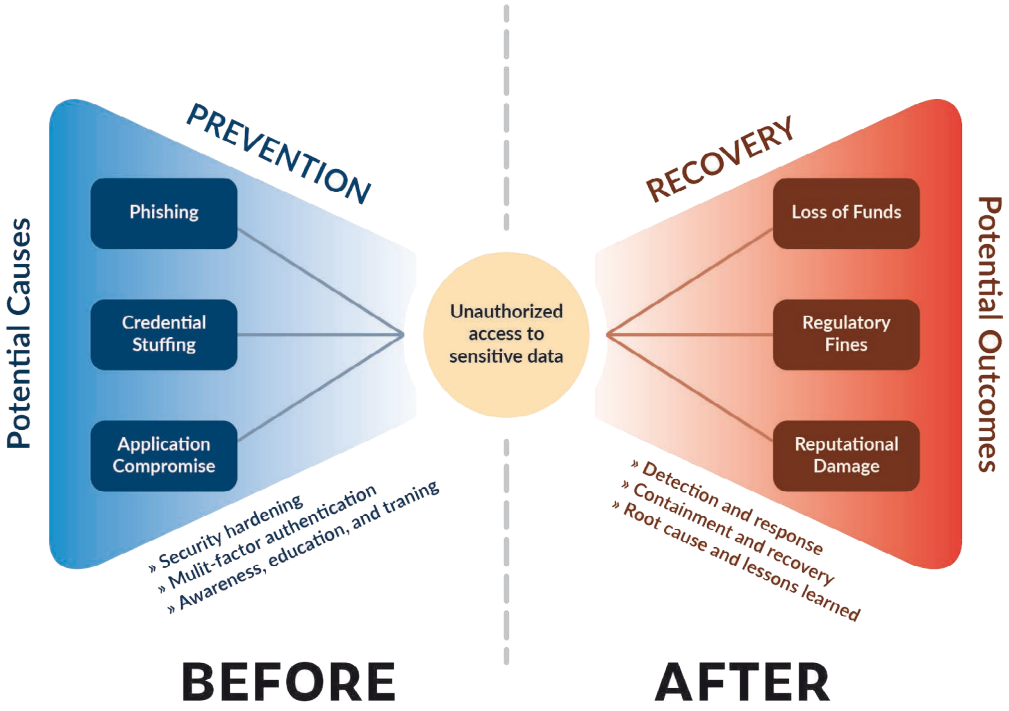

Bild 3: Das Bowtie-Modell ist eine beliebte Variante zum Einschätzen von Risiken bei der Software-Entwicklung.