Mehr Cybersicherheit und weniger Risiko für die Software

Warum TARA eine Notwendigkeit ist

TARA spielt in der Software-Entwicklung und -bereitstellung eine entscheidende Rolle. TARA-Methoden sollten effektiv und in den Software Development Life Cycle und das eigene Entwicklungs-Ökosystem integrierbar sein. Die richtigen Tools zur Ergänzung der TARA machen dabei den entscheidenden Unterschied.

Ricardo Camacho

Einfach ausgedrückt ist die Threat Analysis and Risk Assesment, kurz TARA, ein Prozess zur Ermittlung möglicher Risikofaktoren, Schwachstellen und nichtkonformer Elementen in der Software. TARA unterstützt Entwicklungsteams dabei, unsichere Stellen oder Konformitätsprobleme so aufzuklären, dass Abhilfemaßnahmen und Sicherheits-Implementierungen früher im Software Development Life Cycle (SDLC) erfolgen können.

Die Software-Sicherheit hängt von der Common Weakness Enumeration (CWE) ab, weil sie die Verwaltung von Schwachstellen zugänglicher und leichter verständlich macht. Obwohl MITRE Eigentümer und Verwalter der CWE ist, handelt es sich dabei um einen von der Community betriebenen Katalog verschiedener Risiken in unterschiedlichen Branchen, einschließlich der Automobilindustrie.

Die Konformität mit ISO 21434 ist eines der besten Beispiele dafür, wann eine TARA von entscheidender Bedeu-

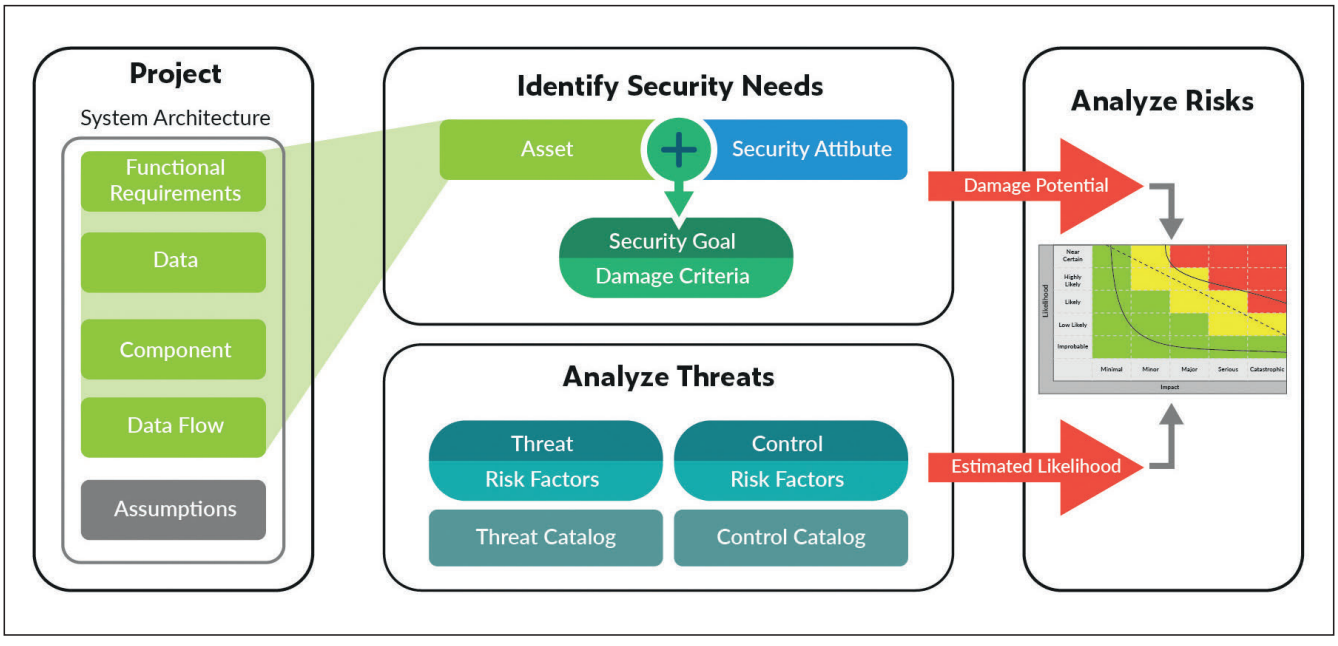


Bild 1: Der Ablauf einer TARA-Methode besteht aus mehreren Schritten. © Parasoft

tung ist. TARA kann Schwachstellen aufzeigen und Hinweise liefern, wie sie Sicherheitsmaßnahmen in ihre Entwicklungsarbeit einbauen können. Eine gut durchgeführte TARA (**Bild 1**) kann vor vermeidbaren Schwachstellen bewahren oder den Unterschied zwischen Erfüllen und Nichterfüllen von Sicherheitsanforderungen machen. Im schlimmsten Fall kann sie darüber entscheiden, ob ein Produkt oder ein Service auf dem Markt lanciert wird, oder ein Rückruf erforderlich ist – wodurch Entwicklungszeit und Geld verloren gehen. Am besten sieht man TARA wie einen jährlichen Gesundheitscheck: Eine kleine Unannehmlichkeit, die allerdings vor echten Problemen bewahren kann.

Vier Schlüsselschritte zum Schutz

Um Cybersecurity zu erhöhen und sich somit besser vor Angriffen von außen zu schützen, sollten folgende Schritte umgesetzt werden:

- Definieren des Projekts
- Identifizieren der Bedrohung und Risikobewertung
- Bedrohungsabwehr
- Umsetzen und Validieren

Definieren des Projekts

Hier wird festgelegt, was aufzubauen ist – von Grundfunktionen bis zu hochkomplexen Eigenschaften – , und sichergestellt, dass alle beteiligten Ressourcen wie u. a. Netzwerkkomponenten und Apps berücksichtigt wurden.

Identifizieren der Bedrohung und Risikobewertung

Eine Risikostrategie zu entwickeln ohne die größten Bedrohungen zu kennen, fruchtet nicht. Stattdessen sollte man gründlich das Problempotenzial des eigenen Projekts ermitteln. Sind die Daten geschützt? Ist man über Bibliotheken oder APIs von Drittanbietern anfällig? Ist es notwendig, mit proprietärer Technologie zu arbeiten, die spezifi-

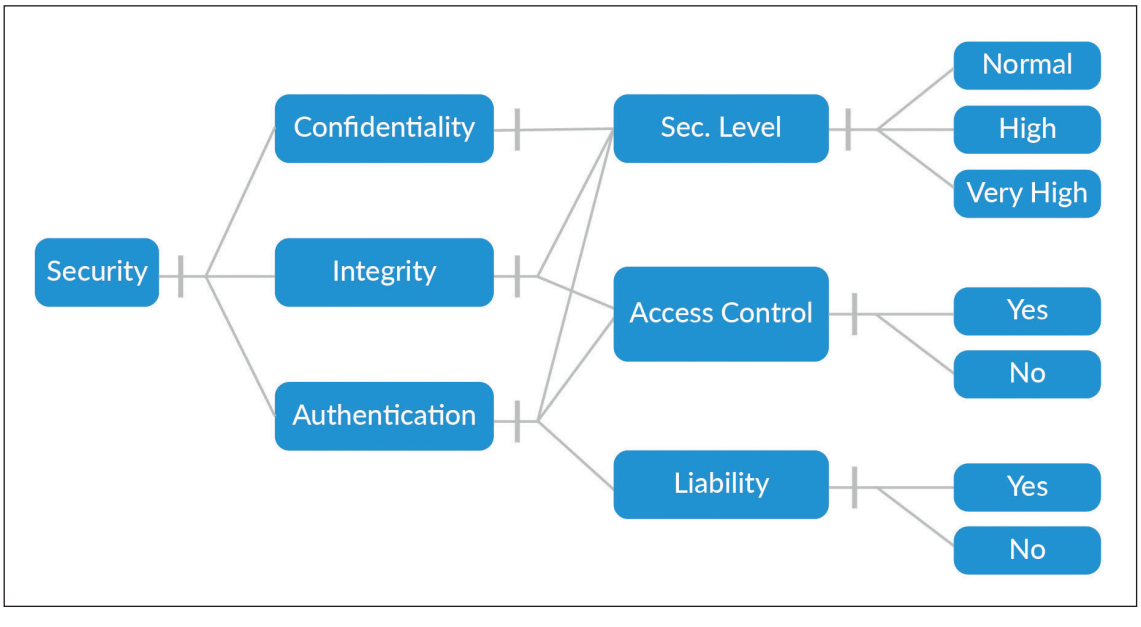


Bild 2: Innerhalb einer TARA ist ein Entscheidungsbaum eine Option zur Risikobewertung für ein Software-Projekt. © Parasoft

sche Anforderungen stellt? Unabhängig von der Situation ist die Kenntnis aller potenziellen Bedrohungsarten und -vektoren ein entscheidender Schritt bei der Entwicklung und Umsetzung einer TARA-Strategie.

Bedrohungsabwehr

Im nächsten Schritt sind Maßnahmen zum Entschärfen von möglichen Bedrohungen und Risikovektoren zu ergreifen. Das kann die Integration von SEI CERT, einer Sicherheitscodeanalyse, in die CI/CD-Pipeline bedeuten. Andere Testmethoden zur Minderung möglicher Bedrohungen umfassen API-Sicherheitstests und funktionale Tests oder Tests gemäß eigener Sicherheitsanforderungen.

Der Test der Sicherheitsanforderungen kann in der Phase der Software-Einheitsprüfung beginnen. Danach folgt die Integrationsprüfungsphase, gefolgt von der Systemprüfungsphase. Ein einfacher Ansatz ist die Nutzung einer Lösung wie Parasoft sie anbietet, um Einheitstests, Integrationstests, Systemtests und Codeabdeckung zu automatisieren, um die Vollständigkeit der Tests zu gewährleisten. Das automatische Erstellen von Testfällen ist eine weitere Funktion, die Aufwand und Kosten reduziert. Automatisierte Berichte und Analysen liefern umsetzbares Feedback, das auf Schwachstellen hinweist und dazu beiträgt, das Projekt auf dem richtigen Weg und in gutem Zustand zu halten.

Umsetzen und Validieren

In dieser Phase wird sichergestellt, dass von den erkannten Bedrohungen keine über einem akzeptierbaren Risikoniveau bleibt, und dass die verbleibenden Risiken ebenfalls innerhalb akzeptierter Parameter liegen.

Bedrohungsmatrizen und andere Messtechniken

Nicht für jedes Projekt ist dieselbe Risikobewertung passend, darum gibt es verschiedene Methoden zum Messen von Wahrscheinlichkeiten und Auswirkungen von Schwachstellen. Eine der beliebtesten Optionen ist eine Bedrohungsmatrix – üblicherweise in Form von 3×3-, 4×4– oder 5×5-Matrizen. Weitere Möglichkeiten sind die folgenden:

- Entscheidungsbaum: Diese Vorlage kann ein Team dabei unterstützen, verschiedene Ergebnisse sowie die Wahrscheinlichkeit des Auftretens zu visualisieren und den potenziellen Wert des Projekts, der Dienstleistung oder des Produkts zu berechnen (**Bild 2**).

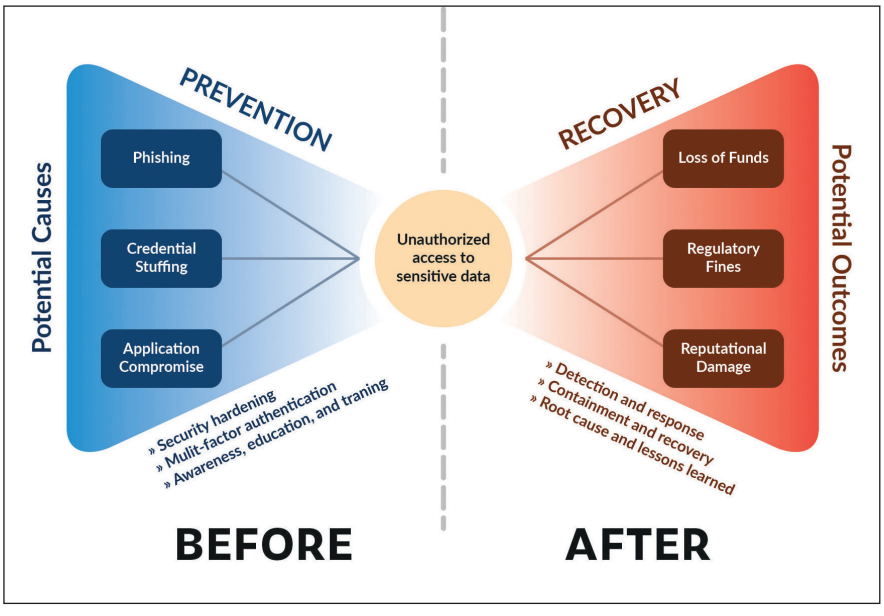


Bild 3: Das Bowtie-Modell ist eine beliebte Variante zum Einschätzen von Risiken bei der Software-Entwicklung. © Parasoft

- Bowtie-Modell: Dieser Ansatz zeigt kausale Verbindungen zwischen Bedrohungsquellen und potenziellen Folgen auf. Auf der linken Seite steht die Ursache, in der Mitte das auslösende Ereignis/Risiko und auf der rechten Seite die möglichen Folgen (**Bild 3**).
- Fehlermöglichkeits- und Einfluss-Analyse (FMEA): Erstmals wurde diese Analyse in den 1940er Jahren beim US-Militär eingesetzt. Sie eignet sich am besten für die Angebots- oder Entwurfsphase eines Projekts. Der Teil „Ausfallmodus" definiert Probleme, potenzielle Probleme und Ausfälle. In der „Auswirkungsanalyse" wird untersucht, welche Folgen die Fehler haben können.

Herausforderungen bei TARA

Die vielen Ansätze und Rahmenwerke zur Einschätzung von Cybersicherheitsrisiken, wie NIST, ISO, OCTAVE oder NCSA, können das Durchführen von Bedrohungsanalysen und Risikobewertungen verkomplizieren. Eine der größten Herausforderungen bei der Einschätzung von potenziellen Gefährdungen besteht darin, alle tatsächlichen Bedrohungen und Risikovektoren zu identifizieren. Auch die Einbindung von Sicherheitsprozessen in die Entwicklung kann für manche Teams ein großes Hindernis darstellen, wenn sie nicht den darin liegenden Wert oder die Vorteile erkennen oder den Aufwand scheuen.

Längst haben vernetzte, embedded Geräte, das IoT, die Cloud, Automatisierung und andere Technologien Einzug in Dinge des täglichen Gebrauchs wie Fahrzeuge gehalten. Darum ist es von entscheidender Bedeutung, dass Strategien für Sicherheit und Risikobewertung implementiert und verfeinert werden. Um die verschiedenen Branchen und Arbeitsabläufe zu unterstützen, unterscheiden sich die TARA-Methoden und -Tools in ihren Ansätzen und Vorteilen. Es muss keine unüberwindbare Aufgabe sein, herauszufinden, welche Tools sich am besten für das eigene Projekt eignen. Unter Zuhilfenahme von Bedrohungsmatrizen lassen sich das passende Werkzeug und die TARA-Strategie leichter ermitteln.

Viele Bedrohungsmatrizen erfassen eine Reihe potenzieller Bedrohungen und die Funktionen oder Schutzmaßnahmen, die eingeführt werden sollten. Das entspricht den anerkannten Sicherheitsanforderungen und den Arten von Verifizierungs- und Validierungsmetho-

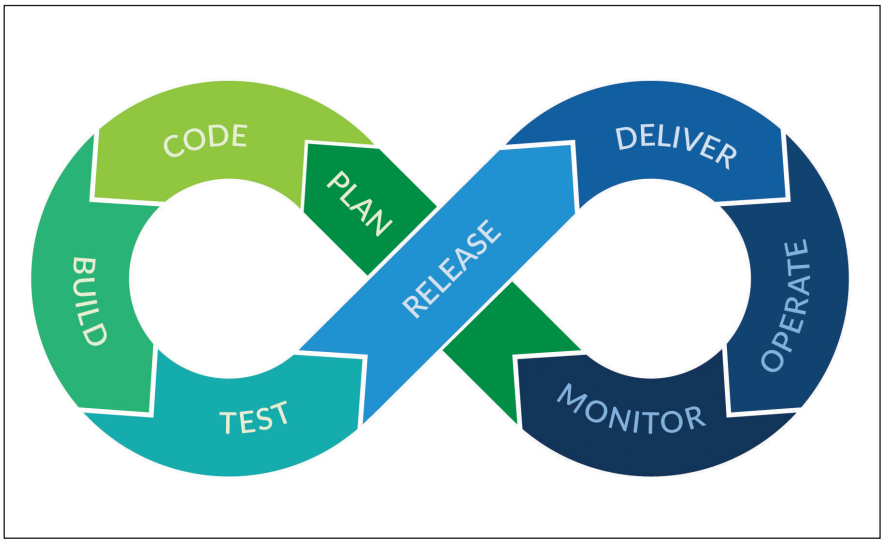


Bild 4: Viele Unternehmen setzen heute die CI/CD-Pipeline zur Rationalisierung ihrer Software-Entwicklung ein. © Parasoft

den (V&V), die angewendet werden müssen. Voraussetzung ist ein solides Anforderungsmanagement-Tool wie Polarion, Jama oder Codebeamer. Man kann diese Anforderungen mit automatisierten SAST- und DAST-Lösungen, wie der von Parasoft, verifizieren und validieren. Auch Unternehmen wie itemis bieten Tools für das Management von Sicherheitsbedrohungen und Risiken an.

Schließen der Sicherheitslücke

Das Implementieren von QA in die eigene CI/CD-Pipeline (**Bild 4**) ist eine Sache, das Gewährleisten der Sicherheit in jedem Abschnitt der Automatisierung kann aber entscheidender sein. Wenn es um Dinge wie die Konformität mit ISO 21434 und ISO 26262 geht, werden bei statischen Sicherheitstests (SAST) Standards wie CERT, CWE oder OWASP berücksichtigt – ebenso wie MISRA und andere Standards, die Sicherheitsrichtlinien in die Norm aufgenommen haben. Die statische Analyse zusammen mit Unit-Tests, Compliance-Reporting, Datenflussanalyse und anderen Funktionen der Parasoft-Tools ermöglicht es der CI/CD-Pipeline, auch Tests zu automatisieren. So kann das Entwickler-Team seinen bereits agilen SDLC um sicherheitsorientierte und automatisierte Prozesse erweitern.

Der eigene TARA-Bedarf

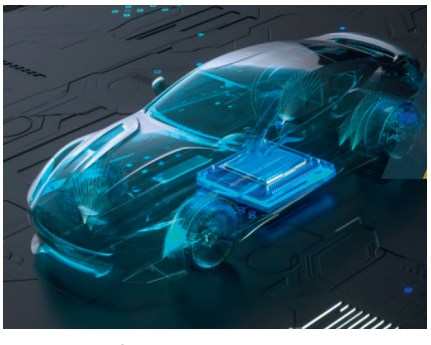
In jeder Branche gehört das Sicherstellen von Konformität und Funktionalität sicherheitskritischer Elemente zum Einmaleins der Entwicklung. So wie eine CI/CD-Pipeline die Automatisierung nutzt, um die Markteinführung zeitlich zu straffen, genauere Testergebnisse zu erzielen und Budgets effizienter zu nutzen, kann TARA den Zeitaufwand beim Beheben von Sicherheitsfehlern und -bedrohungen reduzieren und gleichzeitig zukünftige Probleme entschärfen und nicht konforme Assets identifizieren. Während Tests wie die statische Analyse die MISRA-Konformität unterstützen, bietet beispielsweise Parasoft C/C++test eine einheitliche Lösung zur Automatisierung von Software-Tests, die SAST- und DAST-Testmethoden und Support beim Erzielen der Standards für funktionale Sicherheit umfasst. Sie sollten in keinem TARA fehlen. ■ (eck)

www.parasoft.com

Ricardo Camacho ist Director of Safety & Security Compliance bei Parasoft. © Parasoft

IAR Systems unterstützt MCU-Serie von GigaDevice

Die Version 9.32.1 der IAR Embedded Workbench für Arm von **IAR Systems** unterstützt nun auch die MCU-Serie GD32 von **GigaDevice**. Die GD32A503-MCUs von GigaDevice basieren auf einer Prozessplattform für Automobilelektronik, die dem Designkonzept und den Produktionsstandards von Automobilanwendungen folgt. Die Mikrocontroller können in verschiedenen Automobilanwendungen wie Karosseriesteuerungsmodulen, Fahrzeugbeleuchtungssystemen, intelligenten Cockpitsystemen und vielen anderen Motor- oder Leistungsapplikationen eingesetzt werden. Die Bausteine eignen sich auch für Fahrerassistenzsysteme (ADAS). Die Serie entspricht in Bezug auf Entwicklungstools und unterstützende Software den Industrieprodukten, wodurch ein Maximum an Kompatibilität und Wiederverwendung erreicht wird – das spart effektiv Entwicklungszeit und reduziert Herausforderungen in der Entwicklung.



Unterstützt die MCU-Serie GD32 von GigaDevice: Die neue Version der IAR Embedded Workbench für Arm. © IAR Systems

Die IAR Embedded Workbench für Arm ist eine komplette Entwicklungs-Toolchain für GD32-MCUs und beinhaltet einen hochoptimierenden Compiler sowie erweiterte Debugging-Funktionen. Mit Hilfe der Code-Analyse-Tools C-STAT und C-RUN können Entwickler potenzielle Probleme im Code früher erkennen und die Code-Qualität verbessern. Das Tool ist in einer von TÜV SÜD zertifizierten Functional-Safety-Version erhältlich.

www.iar.com