ALTERSOLUTIONS DEUTSCHLAND

Cyber Security

Sicherheitsanalysen

Security Threat Modeling

Bedrohungsanalysen für Ihre Software, IT-Applikationen und Dienste

Cyber-Angriffe und Datendiebstahl aufgrund von unsicheren IT-Systemen – für viele Unternehmen stellt das in Zeiten der zunehmenden Digitalisierung eine große Herausforderung dar. Externe Angreifer finden zielsicher Sicherheitslücken und Schwachstellen in Systemen und nutzen diese konsequent aus. So sind schnell Daten verschwunden, verschlüsselt, gelöscht oder werden für kriminelle Zwecke genutzt. Doch warum wird es externen Angreifer häufig sehr einfach gemacht, in die IT von Unternehmen einzudringen?Aus diversen Gründen werden Anforderungen an IT-Sicherheit nur widerwillig im Softwareentwicklungsprozess umgesetzt. Von wenig konkreten Anforderungen zur IT-Sicherheit über ausufernde Komplexität bei Applikationen und Systemen bis hin zu immer kürzer werdenden Lieferzyklen sind die Gründe vielfältig.Security Threat Modeling von Alter Solutions Deutschland ist eine bewerte und strukturierte Analyse zur Identifikation von potentiellen Schwachstellen bzw. Risiken bei der Entwicklung und Weiterentwicklung von Software, IT-Applikationen und Diensten sowie beim Einsatz von Fremdsoftware. Unsere Experten arbeiten dabei nach etablierten Industriestandards wie der STRIDE-Methode von Microsoft.

Wir unterstützen

Unsere Leistungen und unsere Vorgehensweise im Bereich des Security Threat Modeling

- Im Rahmen der gemeinsamen Vorbereitung definieren wir den Scope, werten über einen standardisierten Fragebogen relevante Informationen zu dem zu analysierenden System aus und sichten Unterlagen wie Architekturpläne, Datenfluss-Diagramme, etc.Durchführung von IT-Sicherheitsaudits zur Bestandsaufnahme der IT-Prozesse und dazugehöriger technischer Infrastruktur.
- Im Rahmen eines Workshops wird dann mit den relevanten Stakeholdern das System technisch diskutiert und Datenflüsse, Trust Boundaries und vorhandene Security Controls identifiziert.Durchführung von Gesprächen mit den verschiedenen Prozessbeauftragten und Applikation Owner.
- Im nächsten Schritt analysieren unsere Experten die sicherheitsrelevanten Prozesse und Datenflüsse auf mögliche Bedrohungen. Hierzu setzen wir u.a. auf die STRIDE-Methodik.
- Nach der Identifikation von Bedrohungen bewerten und Priorisieren wir diese. Hierzu kommt u.a. das DREAD-Modell zum Einsatz.
- Schließlich definieren wir für relevante Bedrohungen Sicherheitsmaßnahmen und erstellen ein Bedrohungsmodell, das sogenannte Security Profile.

Ihr Mehrwert

Mit Security Threat Modeling auf der sicheren Seite sein

- Threat Modeling eignet sich ideal für den Einsatz in der agilen Softwareentwicklung. Mit Hilfe von Threat Modeling werden konkrete und testbare Anforderungen für die IT-Sicherheit definiert, die analog zu Business User Stories umzusetzen sind.
- Threat Modeling bietet Sicherheit von Anfang an. IT-Sicherheit wird von Beginn an in den Softwareentwicklungsprozess integriert. Bedrohungen werden frühzeitig identifiziert und können mit entsprechenden Gegenmaßnahmen mitigiert werden.
- Threat Modeling reduziert Fehlerbehebungskosten für die IT-Sicherheit. Bei einem frühzeitigen Einsatz von Threat Modeling werden die Aufwände für Penetration Tests sowie nachträgliche Änderung in dem System deutlich reduziert.
- Threat Modeling schafft Akzeptanz. Im Rahmen des Threat Modelings werden die relevanten Stakeholder und insbesondere das Entwicklungsteam aktiv eingebunden.
- Threat Modeling ist flexibel einsetzbar: Jede Art von Software, IT-Applikation und Dienst kann mittels Threat Modeling zu jedem Zeitpunkt des Lifecycles analysiert werden. Dabei ist es nicht relevant, ob es sich um eine Neuentwicklung, Weiterentwicklung oder den geplanten Einsatz von Fremdsoftware handelt. Auch kann Threat Modeling für jedes Betriebsmodell (OnPrem / Cloud) genutzt werden.
- Threat Modeling passt sich Ihren Prozessen an. Threat Modeling ist auf der einen Seite geprägt von einem strukturierten Vorgehen. Auf der anderen Seite bietet es Raum für individuelle Anpassungen. So kann sich bspw. die Bewertung des Bedrohungsrisikos an vorhanden IT-Sicherheitsrichtlinien und -standards orientieren.