T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting 2014
Berlin, 03. - 04.11.2014

Bedrohungsanalyse für ein komplettes System

Dr. Yun Ding
Secorvo Security Consulting

Warum Bedrohungsanalyse?

- … all die verschiedenen Möglichkeiten kennen, mit denen ein System angegriffen werden kann
- … verstehen, wer die Angreifer sind, welche Fähigkeiten, Motivation und Ziele sie haben
- …stärkt das Kundenvertrauen in das Produkt

⇨ Gegenmaßnahmen entwickeln, die Angriffe vereiteln

Varianten des Threat Modelings

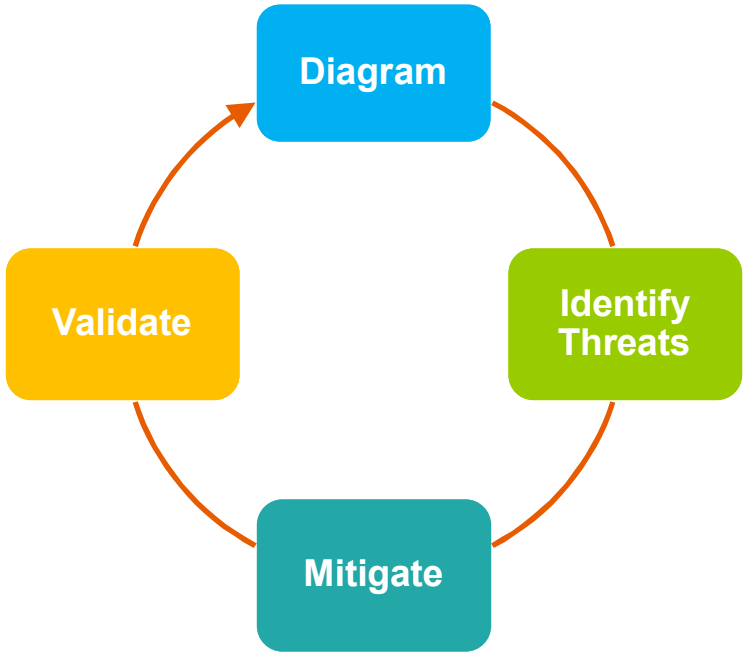
Angreifer

Asset

System

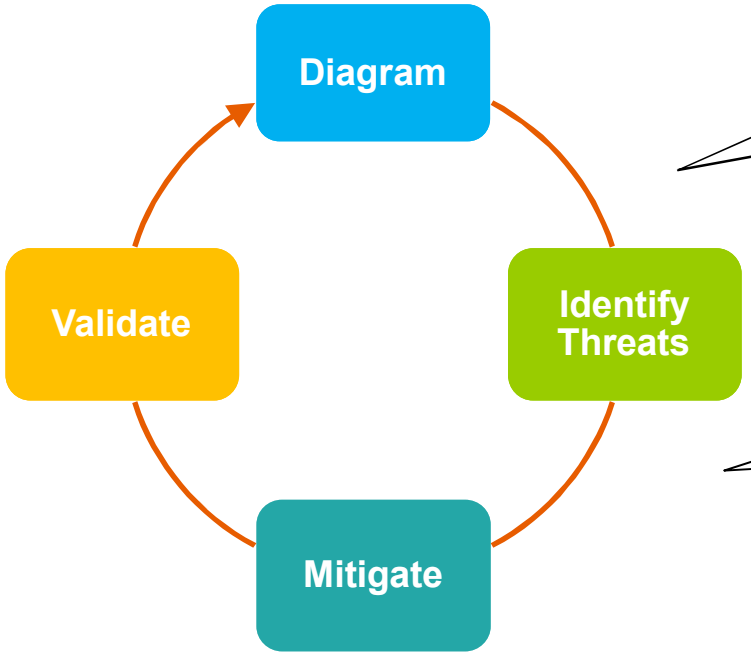
System-zentriert

- Generiere Datenflussdiagramme (DFD) für das System
- Generiere Threats für Elemente und Datenflüsse
- Mitigiere Threats mit Sicherheitsmaßnahmen
- Validierung



Fragestellungen: Bedrohungsanalyse für iPAY

Die mobile Banking App von der iBank



Threats nachvollziehbar dokumentieren

Microsoft STRIDE

Integration mit Entwicklungs-prozeß

Threat-Status verwalten

Zielsetzungen

- Was sind die Best Practices (Tips & Tricks) bei einer Bedrohungsanalyse?

- Welche Wünsche haben wir an ein Tool für Threat Modeling?

Wissenschaft oder Kunst?

Was ist wichtig bei Threat Modeling?

- Erfahrungen: wissen, wonach man sucht
  - *Man findet oft nur die Probleme, nach denen man auch genau sucht.*
- Kreativität: Angreifer sind kreativ!
  - *Ein Angreifer muss eine Schwachstelle finden – ein Verteidiger muss auf alle Bedrohungen vorbereitet sein.*
- Ausdauer
  - *Komplexe Systeme haben große Angriffsfläche.*
  - *Bei sich wiederholenden Aufgaben sucht man nach Prozess-Abkürzungen und lässt (unbewusst, intuitiv) Schritte aus.*

Bildquelle: © Flynt, bigstock.com

Dr. Yun Ding
yun.ding@secorvo.de