Kai Jendrian

Spielerische Bedrohungsanalyse

.. eine ernste Angelegenheit

Anwendungen oder Systeme werden nicht durch Zufall sicher: Bedrohungsanalysen können müheselig sein und es ist vor allem für Entwickler schwer, einen Zugang zu diesem Thema zu finden. Ein spielerischer Einstieg in das Thema kann hier sehr effizient und effektiv sein.

1 Bedrohungsanalyse: Was, Wer, Wann?

Sicherheit entsteht nicht durch Zufall. Für alle Anwendungen oder Systeme, für die im Rahmen von Risikoanalysen ein hohes Schadenspotenzial festgestellt wird, sind in der Regel angemessene Schutzmaßnahmen festzulegen. Es bietet sich häufig an, diese Maßnahmen mit Hilfe von systematischen Bedrohungsanalysen abzuleiten. Bedrohungsanalysen können sowohl für Anwendungen als auch für komplexere IT-Systeme durchgeführt werden.

Dabei sollten möglichst viele unterschiedliche Personen beteiligt werden, insbesondere aber diejenigen, die das System am besten kennen – zum einen die aus der Geschäftsperspektive Verantwortlichen, zum anderen die Architekten, Entwickler und Betreiber des Systems. Je früher eine Bedrohungsanalyse durchgeführt wird, desto eher lassen sich Sicherheitsprobleme erkennen und beheben. Es ist wichtig, dass man sich mit allen relevanten Bedrohungen im Nachgang auseinandersetzt und definiert, wie mit diesen umgegangen werden soll.

Im Idealfall wird ein Defekt festgestellt und dessen Behebung initiiert (bspw. über ein Ticket). Im Folgenden wird eine mögliche Vorgehensweise für die Bedrohungsanalyse betrachtet, bei der man mit Datenflussdiagrammen [13] arbeitet und Bedrohungen anhand der von Microsoft entwickelten S.T.R.I.D.E.-Methode ermittelt.

2 Vorgehensweise

2.1 Dokumentation der Schutzobjekte

Bei einer Bedrohungsanalyse wird zunächst dokumentiert, welche Werte besonders zu schützen sind. Hierbei handelt es sich oft um greifbare Werte, an denen ein Angreifer ein direktes Interesse haben könnte (bspw. Daten in einer Datenbank, Passwörter, vertrauliche Geschäftsdaten oder Computerressourcen).

Es gibt aber auch nicht-greifbare Werte, die zu schützen sind, auch wenn ein Angreifer unter Umständen kein unmittelbares Interesse an ihnen hat, sie aber als Folge seines Angriffs beeinflusst (bspw. der Ruf einer Firma, die Motivation der Mitarbeiter, das Vertrauen der Kunden). Für diese Werte gilt es, die Objekte zu identifizieren, deren Störung eine Beeinträchtigung der nicht-greifbaren Werte zur Folge hätte. Generell gilt: Alle IT-Systeme, die einem Angreifer den Weg zu seinem Ziel ebnen können, müssen angemessen geschützt werden.

2.2 Dokumentieren der Architektur

Der nächste Schritt ist die Dokumentation der Anwendungs- oder Systemarchitektur. In der Praxis hat es sich bewährt, mit Datenflussdiagrammen zu arbeiten, deren Detaillierungsgrad man passend wählen sollte. Das Hauptaugenmerk sollte darauf liegen, dass alle Beteiligten anhand des Modells ein einheitliches Verständnis gewinnen und alle relevanten Details zu Aktoren, Prozessen, Datenspeichern und Kommunikationsverbindungen sichtbar werden.

2.3 Vertrauensbereiche einteilen

Zur Vereinfachung arbeitet man in der Praxis meistens mit sogenannten Vertrauensbereichen oder -grenzen, um zu verdeutlichen, in welchen Bereichen einer Anwendung keine zusätzlichen Schutzmaßnahmen vorgesehen sind. Ein Beispiel für einen Vertrauensbereich im echten Leben ist die eigene Wohnung. Diese ist durch eine Wohnungs- und ggf. Haustür sowie Fenster gesichert. Jedoch findet jemand, der Zutritt zur Wohnung hat, dort nur noch in Ausnahmen weitere Schutzmaßnahmen (wie einen Tresor) vor. Innerhalb von Vertrauensbereichen wird in der Regel nicht nach Bedrohungen gesucht. Allerdings kann es sinnvoll sein, die Angemessenheit der Festlegung von Vertrauensbereichen zu diskutieren.

2.4 Bedrohungen identifizieren

Ist das System oder die Anwendung zur Zufriedenheit aller Beteiligten dokumentiert – was meistens an sich schon einen großen Gewinn darstellt – gilt es, relevante Bedrohungen zu finden. Ein systematischer Ansatz hierzu ist die Verwendung der sogenann-

Kai Jendrian

Security Consultant bei der Secorvo Security Consulting GmbH, lizenzierter Auditor und OWASP-Mitglied. Beratungsschwerpunkte: Information Security Management und Anwendungssicherheit.
E-Mail: kai.jendrian@secorvo.de

ten S.T.R.I.D.E.-Methode, die von Microsoft populär gemacht wurde. Das Akronym S.T.R.I.D.E. steht für

- Spoofing (Vortäuschen einer falschen Identität)
- Tampering (Verfälschen von Daten)
- Repudiation (Abstreiten von Handlungen)
- Information Disclosure (Unberechtigte Kenntnisnahme von Daten)
- Denial of Service (Verhinderung von Diensten) und
- Elevation of Privilege (Unberechtigte Nutzung erhöhter Systemprivilegien)

S.T.R.I.D.E. beschreibt die jeweilige Klasse von Bedrohungen. Hierdurch kann man systematischer nach Bedrohungen suchen und den gefundenen Bedrohungen passende Schutzmaßnahmen gegenüberstellen. Neben dem traditionellen Ansatz, Bedrohungen gegen jedes Objekt zu suchen, sucht man inzwischen vor allem auch nach Bedrohungen, die sich auf die Datenflüsse (Ursprung, Ziel und Interaktion) beziehen.

2.5 Bedrohungen behandeln

Jede Bedrohung, die im Rahmen der Analyse ermittelt wurde, sollte in angemessener Form behandelt werden. Wird im Rahmen einer Bewertung festgestellt, dass einer Bedrohung eine Schutzmaßnahme entgegengesetzt werden soll, sollte dies gleich festgehalten und kommuniziert werden. Hierzu bietet sich die Nutzung eines etablierten Werkzeuges an – in vielen Umgebungen wird hierfür ein Ticket-System eingesetzt.

3 Spielerische Herangehensweise

In der Praxis sind die meisten an einer Bedrohungsanalyse Beteiligten zu Beginn nicht gut geübt im Finden von passenden Bedrohungen. Im Gegenteil: Gerade Entwickler tun sich oft schwer, nach Schwächen und Fehlern im eigenen Code zu suchen. Die Suche nach Missbrauchspotenzial mit Hilfe von Bedrohungskatalogen ist sehr mühselig und meistens nicht als Einstieg in das Thema geeignet.

Auch wenn es im Geschäftsumfeld vielleicht verpönt ist: Ein spielerischer Einstieg in Bedrohungsanalysen kann Spaß machen. Aber nicht nur das: Er ist vielmehr durchaus dazu geeignet, die genannten Hürden zu überwinden und stellt eine effiziente Methode dar, mit wenig Aufwand sehr greifbare erste Ergebnisse zu erzielen.

Der Autor Adam Shostack hat dieses Potenzial erkannt und das Kartenspiel „Elevation of Privilege" entwickelt. Dieses Spiel kombiniert den beschriebenen systematischen Ansatz für die Bedrohungsanalyse mit Elementen von sogenannten „Serious Games" [10], bei denen das spielerische Element vor allem Mittel zum Zweck ist. Alle Beteiligten einigen sich auf ein Modell des zu betrachtenden Systems oder der Anwendung und zeichnen dies auf. Die Karten des Spiels enthalten mögliche Bedrohungen, die dann die Mitspieler reihum auf das System anzuwenden versuchen.

Jede relevante Bedrohung beschert dem Spieler einen Punkt (und wird durch einen Protokollanten erfasst). Die höchste Karte einer Runde beschert dem jeweiligen Spieler einen Zusatzpunkt. So stehen am Ende des Spiels gleich mehrere Sieger fest: Vordergründig der Spieler mit den meisten Punkten – viel wichtiger aber: Das gesamte Team, das mit wenig Aufwand und viel Spaß einen Einstieg in die Bedrohungsanalysen gefunden und mit hoher Wahrscheinlichkeit Verbesserungspotenzial identifiziert und dokumentiert hat. Gleichzeitig wurde das Thema systematisch bearbeitet.

4 Und danach?

Nach dem spielerischen Einstieg in die Bedrohungsanalysen bietet es sich an, das Thema systematisch weiter zu vertiefen. Hierzu stehen einige Werkzeuge zur Verfügung. Das bekannteste Werkzeug dürfte das „Microsoft Threat Modelling Tool 2016" sein [5]. Mit diesem Threat-Modelling-Werkzeug lassen sich zunächst die Datenflüsse von Anwendungen und Systemen dokumentieren und danach die für jede Interaktion relevanten Bedrohungen erfassen. Das Werkzeug bietet vielfältige Anpassungsmöglichkeiten. Außerdem kann man Bedrohungen exportieren, um sie in ein Ticket-System zu übernehmen. Wichtig ist dabei, dass Bedrohungen systematisch und sorgfältig analysiert und verfolgt werden.

Wer sich vertieft mit dem Thema auseinandersetzen möchte, findet eine sehr detaillierte Übersicht in dem Buch „Threat Modeling: Designing for Security" [2] – das ebenfalls von Adam Shostack verfasst wurde – sowie an vielen anderen Stellen im Netz.

5 Fazit

- Bedrohungsmodellierung ist kein Hexenwerk.
- Bringen Sie alle Beteiligten an einen Tisch und lassen Sie sie die Anwendung attackieren.
- Eliminieren Sie Hürden durch einen spielerischen Einstieg.
- Dokumentieren Sie alle relevanten Bedrohungen und kümmern Sie sich um eine Behandlung.

Literatur

[1] Shostack, Adam: *Drawing Developers into Threat Modelling*. https://www.usenix.org/system/files/conference/3gse14/3gse14-shostack.pdf

[2] Shostack, Adam: *Threat Modeling: Designing for Security*. http://threatmodelingbook.com

[3] *Elevation of Privilege Game*. https://www.microsoft.com/en-us/sdl/adopt/eop.aspx

[4] *EOP Game (deutsch)*: https://github.com/test4bounty/EoPCardGameGerman/tree/master/PDF-all-cards

[5] Microsoft: *Microsoft Threat Modelling Tool 2016*. https://blogs.microsoft.com/microsoftsecure/2015/10/07/whats-new-with-microsoft-threat-modeling-tool-2016/

[6] RFC 3552: *Guidelines for Writing RFC Text on Security Considerations*. https://tools.ietf.org/html/rfc3552

[7] OWASP: *OWASP Threat Risk Modelling*. https://www.owasp.org/index.php/Threat_Risk_Modeling

[8] *CWE – Common Weakness Enumeration*. http://cwe.mitre.org/

[9] *CAPEC – Common Attack Pattern Enumeration and Classification*. https://capec.mitre.org/

[10] Wikipedia: *Serious Games*. https://en.wikipedia.org/wiki/Serious_game

[11] *10 common traps*. http://www.tripwire.com/state-of-security/security-data-protection/threat-modeling-10-common-traps-you-dont-want-to-fall-into/

[12] Bericht über OPM hack: https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf

[13] Wikipedia: *Datenflussdiagramme*. https://de.wikipedia.org/wiki/Datenflussdiagramm