Elevation of Privilege Anleitung

Artikulieren Sie Bedrohungen klar und nachvollziehbar. Bedrohungen müssen testfähig/überprüfbar sein. Überlegen Sie, wie. Bedrohungen sollen innerhalb des Systems adressierbar sein. Streit um die Gültigkeit einer Bedrohung können Sie mit der Frage auflösen: "Würden wir einen Bugreport, ein Feature-Request oder eine Design-Änderung hierfür akzeptieren?". Ist die Antwort "ja", handelt es sich um eine relevante Bedrohung. Dies bedeutet nicht, dass Bedrohungen außerhalb dieser Betrachtung nicht real sind. Es hilft lediglich, sich auf adressierbare Bedrohungen zu konzentrieren. Bedrohungen die einleiten mit "Ein Angreifer könnte..." werden erläutert im Stile "..und zwar wie folgt". Karten mit "Ihr Code..." werden wie folgt vorgetragen: "Unser Code... und zwar wie folgt". Das Kartendeck enthält einige Spezialkarten: Trümpfe und offene Bedrohungen. EoP Karten sind Trümpfe. Sie gewinnen die Runde, auch wenn sie einen niedrigeren Wert haben, als die Suite/Farbe, mit der die Runde begonnen wurde. Asse sind offene Bedrohungen. Wer ein Ass spielt, muss eine Bedrohung finden, die auf keiner anderen Karte steht und versuchen, sie auf das System anzuwenden. Wenn alle Karten gespielt sind, gewinnt der Spieler mit der höchsten Punktezahl.

Viel Spaß beim Spielen!

Anleitung

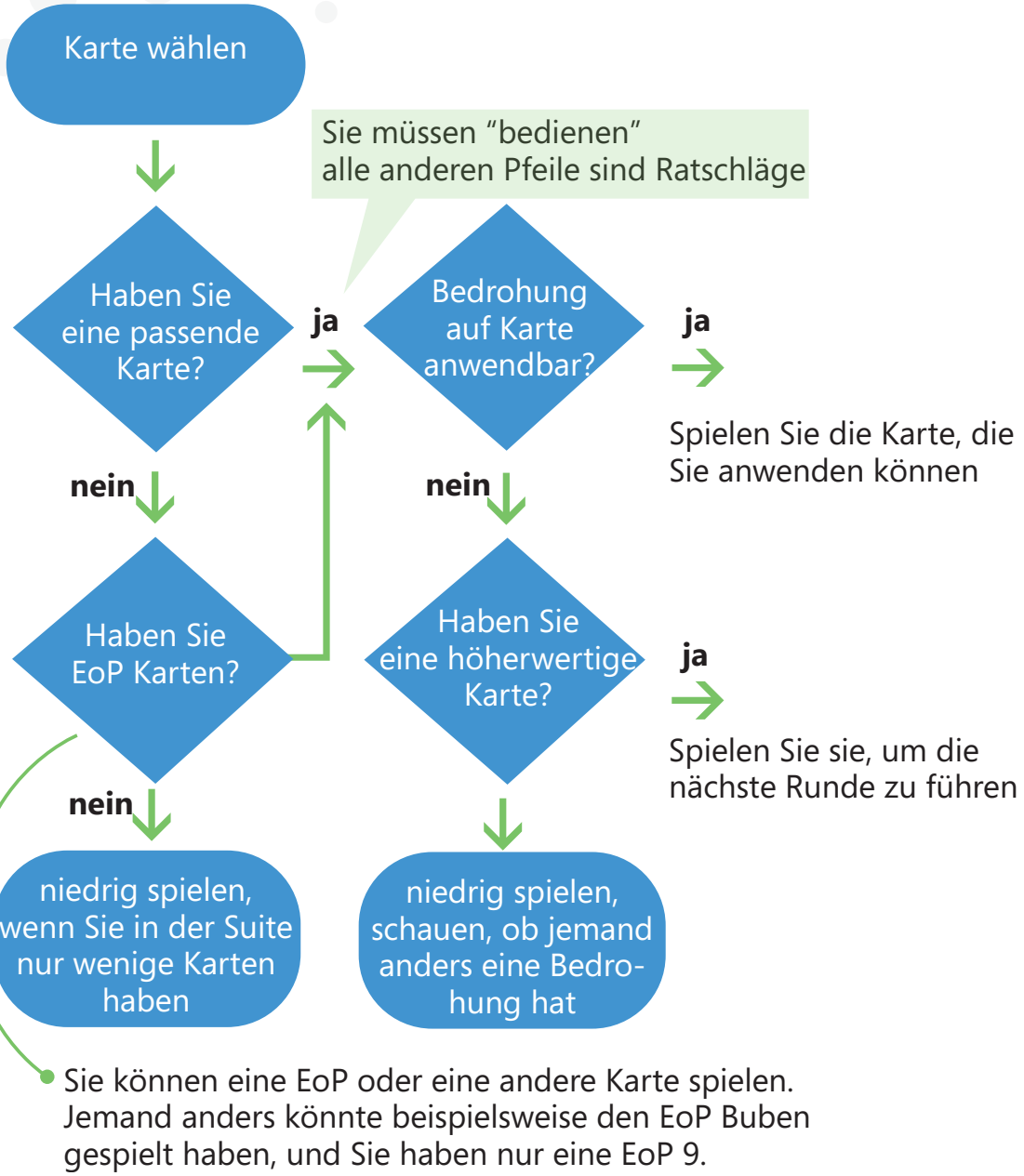
Inhalt:

- **2** Karten mit der Spielanleitung
- **1** Karte mit einem Strategie-Diagramm
- **6** STRIDE “Suites” von Spielkarten:
    1. Spoofing: 2-K, Ace
    2. Tampering: 3-K, Ace
    3. Repudiation: 2-K, Ace
    4. Information Disclosure: 2-K, Ace
    5. Denial of Service: 2-K, Ace
    6. Elevation of Privilege: 5-K, Ace (Trumpf Karten)
- **6** STRIDE Bedrohungs Referenz Karten
- **1** About Threat Modeling und SDL card

Deutsche Übersetzung: Detmar Liesen, test4bounty@gmail.com

Anleitung

Strategie


Karte wählen
Sie müssen “bedienen”
alle anderen Pfeile sind Ratschläge
Haben Sie eine passende Karte?
ja
Bedrohung auf Karte anwendbar?
ja
Spielen Sie die Karte, die Sie anwenden können
nein
nein
Haben Sie EoP Karten?
Haben Sie eine höherwertige Karte?
ja
Spielen Sie sie, um die nächste Runde zu führen
nein
niedrig spielen, wenn Sie in der Suite nur wenige Karten haben
niedrig spielen, schauen, ob jemand anders eine Bedro-hung hat
Sie können eine EoP oder eine andere Karte spielen. Jemand anders könnte beispielsweise den EoP Buben gespielt haben, und Sie haben nur eine EoP 9.

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Microsoft

elevation of privilege

Spoofing cont.

8. Ein Angreifer kann auf einem Server gespeicherte Credentials stehlen und wieder verwenden (z.B. Schlüssel in einer für andere lesbaren Datei).

9. Ein Angreifer, der Zugang zu einem Passwort bekommt, kann es wieder verwenden (nutzen Sie stärkere Authenti- sierungsmethoden).

10. Ein Angreifer kann wählen, dass eine schwächere oder gar keine Authentisierung genutzt wird.

J. Ein Angreifer kann die auf einem Client gespeicherten Credentials stehlen und wieder verwenden.

Q. Ein Angreifer kann den Mechanismus angreifen, mit dem Passwörter zurückge- setzt oder aktualisiert werden (Account Recovery erfordert nicht die Eingabe des alten Passworts).

K. Ihr System wird mit einem Default Adminpasswort ausgeliefert und erzwingt nicht die Änderung dieses Passworts.doesn’t force a change.

A. Sie haben einen neuen Spoofing Angriff erfunden.

Tampering cont.

9. Ein Angreifer kann Statusinformationen beeinflussen.

10. Ein Angreifer kann gespeicherte Daten verändern, weil die Berechtigungen (ACLs) zu wenig restriktiv sind oder eine Gruppe verwendet wird, die letztlich jedem Nutzer Zugriff gewährt.

J. Ein Angreifer kann auf eine Ressource schreiben, weil es keine ACLs gibt, oder weil jeder berechtigt ist (world writable).

Q. Ein Angreifer kann Parameter über eine Trust Boundary hinweg ändern, nachdem sie validiert wurden (z.B. in einem HTML hidden field, oder einem Pointer an eine kritische Speicherstelle im RAM übergeben).

K. Ein Angreifer kann Code mithilfe eines Extension Points einbinden.

A. Sie haben einen neuen Tampering Angriff erfunden.

R

Repudiation cont.

8. Ein Angreifer kann das Logging so austricksen, dass sicherheitsrelevante Logdaten nicht geschrieben werden oder durcheinander geraten.

9. Ein Angreifer kann einen Shared Key nutzen, um sich als jemand anders auszugeben, so dass seine Aktionen ebenfalls unter dieser Identität mitgeloggt werden.

10. Ein Angreifer kann beliebige Logdaten in ein Logsystem einschleusen, weil die Logquellen nicht oder nur schwach authentisiert werden.

J. Ein Angreifer kann unbemerkt Logs editieren, löschen oder deren Übermittlung unterbinden.

Q. Ein Angreifer kann abstreiten, etwas getan zu haben und es gibt keine brauchbaren Daten, um das Gegenteil zu beweisen.

K. Das System hat keine Logs.

A. Sie haben einen neuen Repudiation Angrif erfunden.

Information Disclosure cont.

8. Ein Angreifer kann (sensible) Informationen mithilfe eines Such-Indexers, Loggers oder eines anderen Mechanismus zugreifen.

9. Ein Angreifer kann sensible Informationen in einer Datei lesen, weil deren Zugriffsrechte falsch gesetzt sind (schwache ACL).

10. Ein Angreifer kann mangels Zugriffsbeschränkung eine sensible Datei lesen.

J. Ein Angreifer kann den statischen Schlüssel finden, der zur Verschlüsselung genutzt wird.

Q. Ein Angreifer kann einen Kommunikatioinskanal vollständig mitlesen, weil dieser unverschlüsselt ist.

K. Ein Angreifer kann Netzwerkinformationen lesen, weil keine Kryptografie genutzt wird.

A. Sie haben einen neuen Information Disclosure Angriff erfunden.

Denial of Service cont.

8. Ein Angreifer kann einen Server unverfügbar machen und das Problem besteht fort, nachdem der Angriff aufgehört hat (**Server, authentisiert, persistent**).

9. Ein Angreifer kann einen Client unverfügbar machen, ohne dass je eine Authentisierung stattgefunden hat, und das Problem besteht fort, nachdem der Angriff aufgehört hat (**Client, anonym, persistent**).

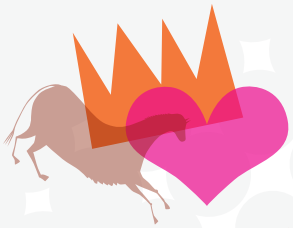
10. Ein Angreifer kann, ohne zu authentisieren, einen Server unverfügbar machen. Das Problem besteht fort, nachdem der Angriff aufgehört hat (**Server, anonym, persistent**).

J. Ein Angreifer kann das Logging-Subsystem außer Betrieb setzen.

Q. Ein Angreifer kann eine verwundbare Systemkomponente dazu missbrauchen, eine (volumenbasierte) DoS Attacke um den Faktor 10 zu verstärken.

K. Ein Angreifer kann eine verwundbare Systemkomponente dazu missbrauchen, eine DoS Attacke mehr als 100fach zu verstärken.

A. Sie haben eine neue DoS Attacke erfunden.

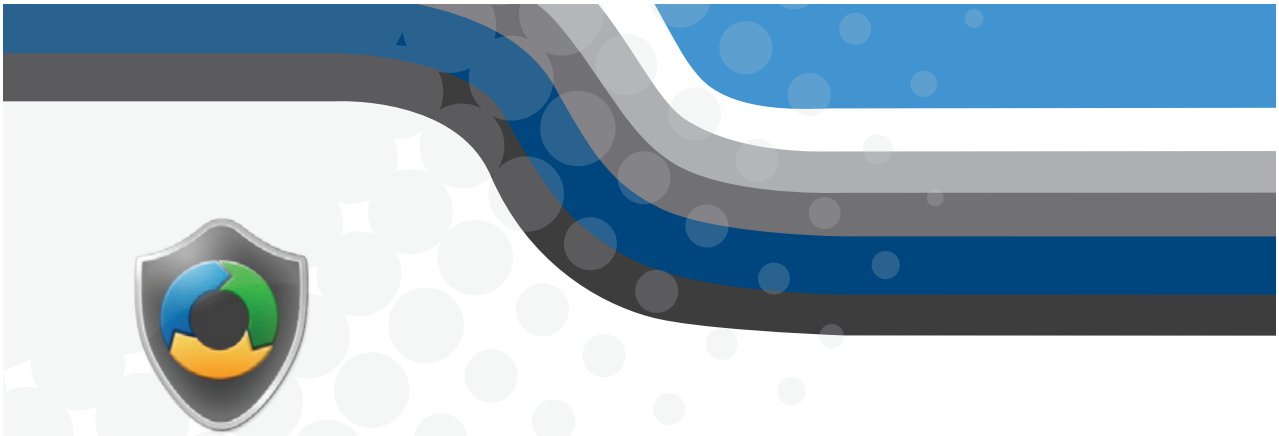


Elevation of Privilege cont.

Q. Sie inkludieren User Generated Content (UGC) in Ihrer Webseite, der auch Inhalte beliebiger URLs etc. enthalten kann.

K. Ein Angreifer kann ein Kommando einschleusen, welches vom System mit einer höheren Berechtigung ausgeführt wird.

A. Sie haben einen neuen Elevation of Privilege Angriff erfunden.



SDL

The Elevation of Privilege game is a fun and easy way to get started understanding the security of your systems by threat modeling. As you discover and correct design-level security problems, it's worth thinking about the other ways security issues can creep into your code. Microsoft has a large collection of free resources available to help you get started with the Security Development Lifecycle (SDL).

To learn more about threat modeling and the Microsoft Security Development Lifecycle, visit our website at **microsoft.com/sdl/**

Microsoft

Security Development Lifecycle