Chapter

Paper Präsentation:

“Best Practises: Einsatz von Web Application Firewalls”

Autoren: Maximilian Derman, Mirko Dziadzka, Boris Hemkemeier, Achim Hoffmann, Alexander Meisel, Matthias Rohr, Thomas Schreiber

Aufbau

- Einführung und Zielsetzung
- Charakteristika von Web-Applikationen hinsichtlich Web App Security
- Fähigkeiten von WAFs im Überblick
- Nutzen und Risiken beim Einsatz von WAFs
- Beispiel: Schutz gegen OSWASP-TOP 10 (App vs. WAF vs. Policy)
- Kriterien zur Einsatzentscheidung von WAFs

Einführung und Zielsetzung

- Einführung - Wer ist eigentlich betroffen
  - Online Business, Schwachstelle HTTP, Hinweis auf PCI DSS v1.1
- Begriffsdefinition “Web Application Firewall”
  - Abgrenzung Netwerk Security, Nicht nur Hardware, kein XML/SOAP Gateway
- Zielgruppen und Zielsetzung
  - Tech. Entscheider, Betriebsverantwortliche, Sicherheitsverantwortliche, Applikationseigner

Charakteristika von Web Applicationen hinsichtlich Web App Security

- Übergeordnete Aspekte im Unternehmen
  - Imageverlust, Schadenersatz
  - Genehmigungen
- Technische Aspekte
  - Test- und Quality-Assurance
  - Dokumentation
  - Wartungsverträge

Fähigkeiten von WAFs im Überblick

- Einordnung von WAFs im Gesamtbereich Web App Sec
  - Hauptziele einer WAF
  - Darüberhinausgehende Funktionalitäten
  - Synergieeffekte mit anderen Security Maßnahmen
- Typische Mechanismen von WAFs am Beispiel
  - Tabelle: Wo gut, schlecht, abhängig oder nur teilweise

Nutzen und Risiken von WAFs im Überblick (I)

- Hauptnutzen von WAFs
  - "Grundschutz", Application Lock-Down
  - Compliance
  - Patch-Dilema Lösung
- Zusatznutzen von WAFs (abhängig von Funktionlität)
  - Proatikive Schutzmechanismen
  - Erhöhte Stabilität

Nutzen und Risiken von WAFs im Überblick (II)

- Risiken
  - False positives
  - Erhöhte Komplexität
  - Fehlende Prozesse für:
    - Fehlersuche
    - Administration
  - Kosten (?)

Beispiel: Schutz OWASP TOP 10 (WAF vs. World)

- Drei Ausgangsszenarien für eine Anwendung:
  - Design-Phase
  - Produktiv und einfach anpassbar
  - Produktiv, nicht oder schwer anpassbar
- Tabelle mit Möglichkeiten: App ändern, WAF oder Policy

Kriterien bzgl. Einsatz-Entscheidung von WAFs (I)

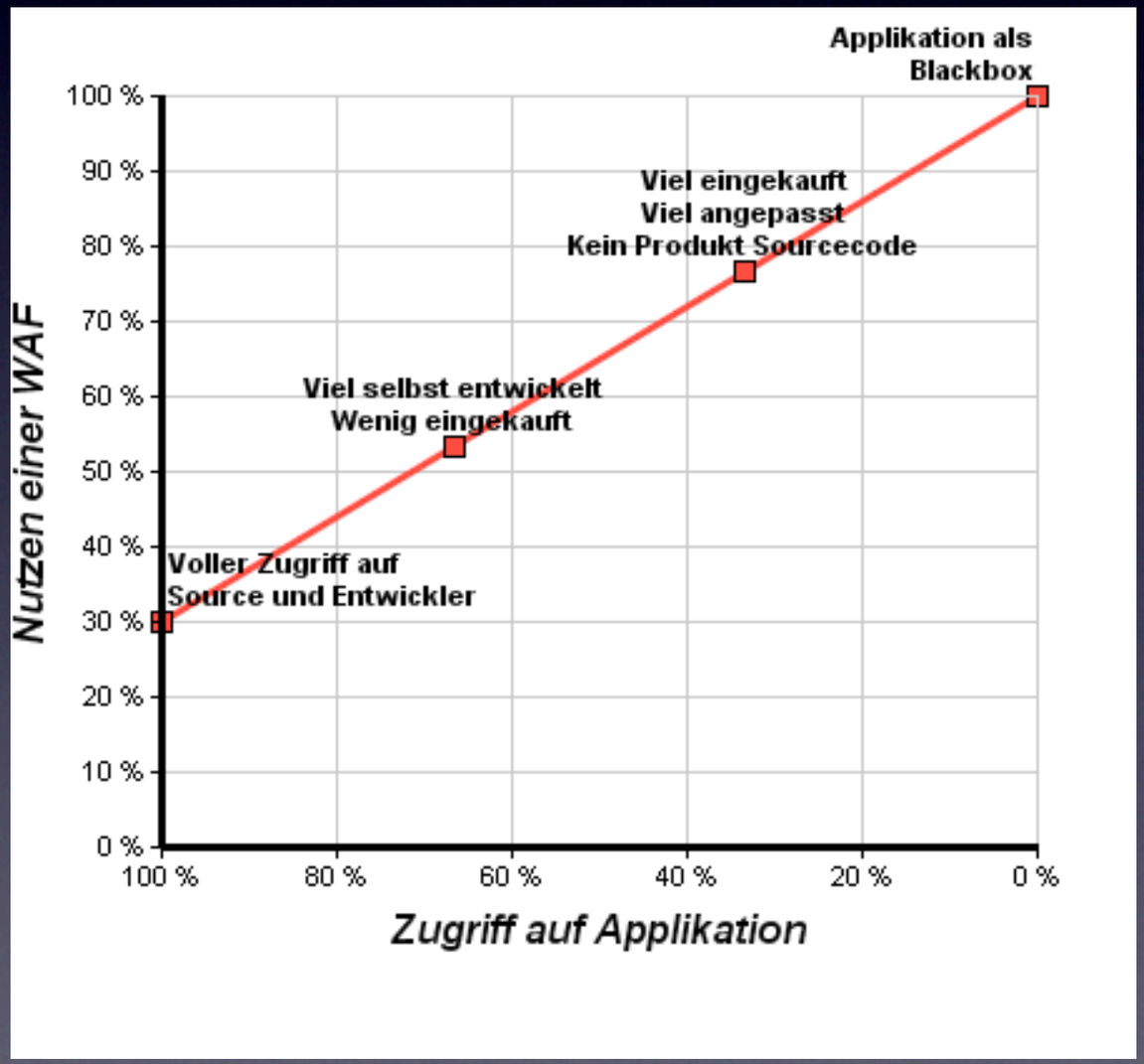
- Unternehmensweite Kriterien
  - Bedeutung (Umsatz, Erfolg, Datenverlust, Kundendaten, Unternehmensgeheimnisse, Image, etc.)
  - Anzahl Applikationen
  - rechtliche Rahmenbedingungen
  - Kosten, Komplexität, Performance, Betriebssicherheit

Kriterien bzgl. Einsatz-Entscheidung von WAFs (II)

- Kriterien hinsichtlich einer Web Applikation
  - Änderungsfähigkeit der Applikation
  - Dokumentation
  - Wartungsverträge
  - Fehlerbebungszeiten für Dritt-Produkte (z. B. CMS, DMS, ...)

Kriterien bzgl. Einsatz-Entscheidung von WAFs (III)

- Bewertung und Zusammenfassung



Best Practices bei Einführung und Betrieb (I)

- Web-Infrastruktur Aspekte
  - Zentral oder Dezentral - absehbare Veränderungen
  - Performance Kriterien
- Organisatorische Aspekte
  - Einhaltung bestehender Policies soweit möglich
  - Neue Rolle: Anwendungsverantwortlicher WAF

Best Practices bei Einführung und Betrieb (II)

- Iteratives Vorgehen bei Implementierung von "Grundschutz" bis zur "Vollversiegelung"
  - 3 Grundschritte + Abarbeitung von Prioritätenliste
- Checkliste: Zugriff auf Web App unter Security-Gesichtspunkten
- Rollemodell beim Betrieb von WAFs

Das wars auch schon!

- Fragen?
- Wünsche?
- Diskussion!