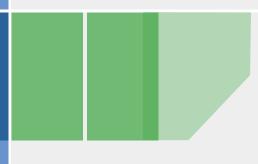


OWASP Germany Applikationen als neuer Security Perimeter



OWASP 20.10.2010

Alexander Meisel art of defence GmbH

alexander.meisel@artofdefence.com

Copyright © The OWASP Foundation Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

The OWASP Foundation http://www.owasp.org

Ich?

- CTO: art of defence GmbH
 - WAF Vendor
- OWASP:
 - ▶ Regelmäßiger Sprecher Chapter Meetings / Congress
 - Mit-Author: Best Practices WAF
- CSA (Cloud Security Alliance):
 - ▶ Mit-Author: CSA Guide 2.0
 - ▶ Mit-Author: Paper Domain 10 (Application Security)



Um was gehts?

- **■** dWAF
 - distributed Web Application Firewall
- Cloud Computing
 - ▶ IaaS
 - Virtuelle WAF
 - Verteilte WAF
 - PaaS
 - Embedded WAF
 - SaaS
 - "Dienstbasierte" WAF
 - Embedded WAF
- Application Architecture NG



dWAF - Teile und Herrsche

- ▶ Enabler Plug-In
 - Web / App Server
 - Applikation selbst!!
 - Load Balancer
 - NW Firewall, IDS/IPS???, ...
- Policy Engine
 - Security Checks
 - Traffic Inspection
 - Traffic "anpassen"
- ▶ Admin
 - Clusterverwaltung
 - Mandantenfähig
 - Multiuser/-admin



Cloud - IaaS

- Infrastructure as a Service
 - virtuelle Images
 - ▶ einfache Welt?
 - ▶ Ziehen wir einfach mal unsere virtuellen Maschinen um, und alles ist gut?
 - Private / Public / Hybrid Cloud
 - ▶ Wo liegen die Daten?
 - Wie bewegen sich die Daten?
 - ▶ Rechtlich alles Sicher!!!
 - Oder doch nicht?
 - Auf den Vertrag kommt es an!



Cloud - PaaS

- Platform as a Service
 - Wir entwickeln die Applikation neu
 - Wir benutzen neue Technologie
 - Google AppEngine, Force.com, MS Azure,
 - Wir vertrauen der Platform!
 - Alle Anbieter sind von Stunde 0 an 100 % sicher!
 - Eher nicht
 - Alle Anbieter bieten granulare Sicherheitsmechanismen?
 - Nein auch nicht
 - ▶ Fazit: DIY Security
 - Geht das gut?
 - Die Erfahrung zeigt: NEIN!!!



Cloud - SaaS

- Software as a Service
 - Wir passen existierende Software an
 - Uns "gehören" nur die Daten aber nicht Software
 - heisst das, dass Application Security uns (dem Kunden) nichts angeht?
 - Der Anbieter verspricht Security
 - Ist diese jedoch transparent?
 - Habe ich Einfluss auf die Security Policy?
 - Rights Management: JA
 - Application Security: NEIN



Application Architecture

- Applikation heute
 - Monolithisch
 - Distributed
 - Event-Driven Architecture
 - MVC (Model View Controller)
 - Client / Server
 - Peer to Peer
 - Filesharing
 - ansonsten BOT-Netzwerke
 - **)**
- Unsere einzige Hoffnung im Moment
 - ▶ SOA (Service Oriented Architecture)



Application Architecture NG

■ Der spannende Teil!

■ siehe Flip Chart ... SORRY :-/

OK ... das war's jetzt endlich!

Antworten zu Fragen stehen zur Diskussion!

- Kontakt:
 - Alexander Meisel
 - ▶ Email: alexander.meisel@artofdefence.com

