Pressemitteilung
Paris, 17. April 2013

# DenyAll ermöglicht ein schnelles virtuelles Patching von Applikationsschwachstellen

***Eine neue von Deny All in Auftrag gegebene Studie von Forrester Consulting hebt die Vorteile des Applikations-Schwachstellen-Patchings in Bezug auf Skalierbarkeit und zeitnaher Reaktion auf moderne Angriffe hervor. Virtual Patching ist der zentrale Aspekt der DenyAll-Integrationsstrategie zwischen der Web Application Firewall Plattform und den dynamischen Application Security Testing-Tools, die gerade mit neuen Releases der Produktlinien Detect und Protect auf den Markt gekommen sind. Neue Sicherheitsfunktionen in DenyAll rWeb 4.1, Feature Pack 1, liefern neuartige Security-Mechanismen gegen moderne Angriffe.***

## Eine neue Forrester Analyse zeigt wichtige Applikation Security Trends auf

Im ersten Quartal des Jahres 2013 beauftragte DenyAll Forrester Consulting mit der Analyse von 50 europäischen Organisationen (mit Sitz in Deutschland, Großbritannien und Frankreich) in Bezug auf ihren Standpunkt zum Thema « Absicherung von Web-Anwendungen ». Der Report beinhaltet nachfolgende Schwerpunkte:

- Aufgrund des Security-Fachwissens sowie dem Markteinführungsdruck sagen **nur 40% der Unternehmen**, dass sie **ausgereifte und umfangreiche Security Prozesse für Applikationen** haben;
- Entsprechende **Trainings für Entwickler** werden von **60%** als eine langfristige Maßnahme angegeben; es kann keine kurzfristige oder in sich schlüssige Code-Sicherheit gewährleistet werden;
- Web Application Firewalls (WAF) sind der derzeit meist verbreitete Mechanismus zum Schutz von Anwendungen; **75% der Befragten haben bzw. planen den Einsatz von WAFs in naher Zukunft.**

Die Umfrage zeigt, dass Experten für Applikation-Security der WAF folgende Vorteile zuordnen: wirksamer Schutz vor Angriffen auf Applikationsebene und Skalierbarkeit sowie die Fähigkeit, Software-Schwachstellen dank der Integration des „Dynamic Application Security Testing“ (DAST) Tool schneller zu patchen. Der vollständige Bericht wird zeitnah auf der Website von DenyAll (www.denyall.com) verfügbar sein.

## Eine innovative Lösung zum Patchen von Anwendungsschwachstellen

Beim Virtuellen Patching für Applikationen werden WAF-Einstellungen auf Basis der Ergebnisse einer Schwachstellen-Analyse so verändert, dass erkannte Schwachstellen durch die WAF geschlossen werden, bis sie im Ursprung behoben sind (z.B. durch Code-Änderungen oder System-Patches). Virtuelles Patching kann die Zeitspanne, in der die sensiblen Daten möglichen Angriffen ausgesetzt sind, drastisch reduzieren.

Seit der Übernahme von VulnIT im Sommer 2012 hat DenyAll an der Zusammenführung seiner WAF- und DAST-Technologien gearbeitet. Die neu releasten Produkte, **DenyAll rWeb 4,1 Feature Pack 1 (FP1) und DenyAll Detect 5,1** stellen zusammen einen ersten Schritt in Richtung der Verfügbarkeit einer zukunftweisenden integrierten Applikationssicherheitslösung von DenyAll dar.

**Diese Lösung ist die erste, die detaillierte Empfehlungen für Regelanpassungen liefert** und Administratoren hilft, zeiteffiziente Entscheidungen entsprechend den Unternehmensprioritäten zu treffen. Scan-Berichte können leicht von den DenyAll Detect Produkte exportiert und in rWeb importiert werden. Die WAF bietet dem Administrator dann Security Policies als Änderungsvorschläge an. Dies können unterschiedliche Möglichkeiten sein, abhängig von den Schwachstellen und den Unternehmensprioritäten: Minimierung der False Positive, Maximierung der Sicherheit oder Maximierung der Performance.

## Erweiterte Analyse-Tools erhöhen den Schutz von modernen Applikationen

Mit Feature Pack 1 bieten alle DenyAll Protect-Produkte verschiedene Verbesserungen und neue Funktionen, wie z. B. Log-Komprimierung, Syslog-Weiterleitung und eine Steuerung für die Automatisierung von Aufgaben. rWeb 4.1 FP1, die führende Lösung dieser Produktlinie, beinhaltet jetzt die Möglichkeiten des „Virtuellen Patchings“ und eine neue Gruppe von Sicherheits-Mechanismen. Diese erweiterten Analyse-Tools wurden zum Schutz vor WAF-Umgehungstechniken, vor modernen Angriffen und die Erhöhung der Applikationssicherheit mit neuen Sprachen entwickelt. Dazu gehören:

- Ein neuer Ansatz zum Schutz vor SQL-Injection basierend auf grammatikalischer Analyse der gesendeten Daten;
- Ein Skriptsprache Injektion Detection Modul als Schutz vor verschachtelten Blöcken in Java, PHP, SSI (Server Side Include) und JavaScript;
- Schutz gegen HTTP Response Splitting;
- Die Fähigkeit, XSS Angriffe in HTML4/5 Tags und Attributen zu identifizieren und zu blocken;
- Erweiterter Schutz gegen Directory Traversal Confusion Versuche.

## Verbesserte Automatisierung in DenyAll Detect 5,1

DenyAll´s Schwachstellen-Scanner wird basierend auf den Kundenanforderungen ständig weiterentwickelt. In der neuesten Version 5.1 des DenyAll Vulnerability Managers stehen neue Funktionen zur Verbesserung des Asset-Managements, der Team-Delegation sowie der Performance im Vordergrund:

- **Asset Management**:
  - Auto-Grouping klassifiziert Assets basierend auf vordefinierten Kriterien,
  - Einmal-Analysis können direkt aus dem System gestartet werden,
  - Gap Analyse-Berichte zeigen, wie die Organisation sich im Laufe der Zeit verbessert.
- **Team-Delegation** und Aufgabentrennung:
  - Benutzergruppen können bezogen auf ihre Wertigkeit erstellt werden,
  - Eine neues Delegation-Modell ermöglicht die Zuteilung einzelner Wertigkeiten und Aufgaben an bestimmte Personen, was speziell in größeren Organisationen und gehosteten Umgebungen sehr wichtig ist.
- **Performance**:
  - Verbesserung des OpenVAS Startups,
  - Neuer Password Triviality Test für White Box Scans unter Unix und DBMS,
  - Neue Taskleiste-Benachrichtigung für den Benutzer, wenn ein Scan im Hintergrund läuft.

## Webinar-Ankündigungen

Ausführliche Informationen über die Neuheiten von rWeb 4.1 FP1 (erweiterte Analyse-Tools) und die DenyAll Virtuell Patching Lösung erhalten Sie auch in unserem Webinar am 23. April 2013. Weiterhin empfehlen wir unser nächstes 'CTO Talk' Webinar, das sich auf HTML5 Sicherheitsfragen konzentriert. Dies findet am 29. Mai 2013 statt. Registrieren Sie sich einfach unter: http://www.denyall.com/news/events_en.

**About DenyAll**

Deny All ist der innovative Marktführer im Bereich Applikationssicherheit. Das Unternehmen zählt zu den Pionieren auf dem Gebiet der Anwendungssicherheit (Web Application Firewalls – WAF) in Europa. Basierend auf mehr als 10 Jahren Erfahrung auf dem Gebiet der Absicherung und Beschleunigung von webbasierten Applikationen wird Deny All auch weiter an Neuentwicklungen arbeiten, um den Anforderungen von Unternehmen aller Größenordnungen gerecht zu werden. Seine Lösungen decken Schwachstellen auf und schützen Infrastrukturen gegen Angriffe auf der Applikationsebene. Weitere Informationen finden sie unter www.denyall.com.


| Press contacts: | | |
|---|---|---|
| **DenyAll**<br>Stéphane de Saint Albin<br>Tél.: +33 1 46 20 96 21<br>sdesaintalbin@denyall.com<br>www.denyall.com | **Kafka Kommunikation**<br>Ursula Kafka<br>Tel.: +49 89 747470-580<br>info@kafka-kommunikation.de<br>www.kafka-kommunikation.de | **DenyAll**<br>Thomas Kohl<br>Tél.: +49 6233 66 75 39<br>tkohl@denyall.com<br>www.denyall.com |