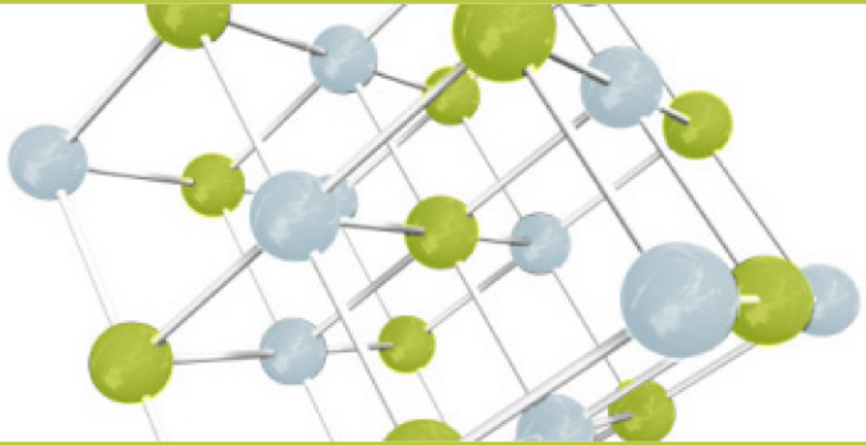
OpSource™
The Business of Web Operations

Securing Web Business Applications: An Overview



Presented by:
Rick Dyer
Director, Product Management
OpSource

July 30, 2008

Security Overview

- Utilize a “defense-in-depth strategy” where a series of security layers are implemented so that a no single solution is relied upon to provide security.

- Six Key Areas to Address
  1. *Physical Security*
  2. *Network Security*
  3. *Host Security*
  4. *Application Security*
  5. *Certification & Compliance*
  6. *Organizational Security & Incident Response*

Physical Security

- **Security starts at the data center with control over the physical environment housing your application**
- **Look to place your application in a facility with appropriate security features and controls:**
  - *Access only for authorized personnel with auditable logs of who & when access occurs*
  - *Secured access to server area with locks and/or biometric verification*
  - *Camera surveillance of server area & facility with archival storage*
  - *System for inventory of physical assets and tracking as assets are added/removed*
- **When outsourcing, a SAS-70 audit can provide insight into how these controls are implemented**

Network Security

- **Firewall Implementation and Maintenance**
  - *Develop a documented firewall configuration that denies all traffic, except for protocols required by your application*
  - *Identify processes and procedures for:*
    - *Ongoing Maintenance - patches and upgrades*
    - *Review and Approval of proposed rule set changes*
    - *Regular analysis of firewall logs to keep abreast of traffic patterns and identify any unusual activity*
- **Network Intrusion Detection**
  - *Consider a solution that analyzes network traffic and reacts by blocking, replacing, or alerting when suspicious activity is detected*
    - *Examines packets at both the IP protocol level and at the application*
    - *Identify and mitigate against "zero day" threats not yet identified*
- **Flow-based Network Traffic Analysis**
  - *Anomaly detection and fingerprinting can detect security hazards such as DoS attacks, worms or botnets as well as traffic and routing instability, equipment failure or other network issues*

Host Security

- **Securing the O/S and Application is an ongoing challenge**
  - *Make sure you have a standard configuration in place for your system components that addresses all known security vulnerabilities*
    - *See standards from SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).*
  - *Develop procedures to review security bulletins for all components, apply patches to affected systems, and update your configurations*
  - *Implement and follow change control procedures for all system and software configuration changes and make sure a security review is part of your signoff procedures*

- **Host-Based Intrusion Detection**
  - *Correlation and analysis engine that integrates log analysis, file integrity checking, Windows registry monitoring, centralized policy enforcement, rootkit detection, real-time alerting and active response*

Application Security

- **Integrate Secure Coding into your development process**
  - *Develop secure coding policies and procedures and processes for the development of your software code*
    - *See Open Web Application Security Project (OWASP)*
  - *Consider having custom code reviewed by an organization that specializes in application security*

- **Analyze and Address your user's security concerns**
  - *Consider a broad risk assessment of the type of data your application holds on behalf of your users*
    - *Identify protected resources, possible attackers, likelihood of attacks, and attack routes*
    - *Add roadmap deliverables to protect most likely attack routes and valuable resources handled by your application*

Certification and Compliance

- **Identify Certification/Compliance Areas that apply to your line of business and/or your user base, such as**
  - *PCI-DSS if you handle credit card data*
  - *HIPAA if you handle health care patient data*
  - *EU Safe Harbor if you handle personal information of EU citizens*
  - *Salesforce AppExchange Certification for Salesforce applications*
  - *BITS for financial industry applications*

- **Consider broader security standards and certifications**
  - *ISO 27002 is a set of information security best practices*
  - *ISO 27001 is an implementation of ISO 27002 that you can be certified against, and is popular in Europe & Asia*

Organizational Security & Incident Response

- **Identify a Security Policy Owner**
  - *Someone who can work across the organization on*
    - *Design of security policies and procedures*
    - *Ensuring successful implementation of those policies*
  - *Effective security requires communication – the best policies of no use if nobody understands them well enough to implement them*

- **Identify 24x7 Monitoring and Incident Response Plans**
  - *Have policies/procedures in place so that personnel can identify problems 24x7 and respond to security threats and intrusions*
  - *Coordinate and communicate with any partners to ensure everyone's on the same page should an event occur*

- **Consider Periodic Third Party Testing**
  - *Regular vulnerability scanning and/or penetration testing can identify weaknesses and ensure compliance to policies*

OpSource™ proudly presents
SaaS Summit 2009
SAVE THE DATE! March 11-13, 2009 | San Francisco, CA | The Westin St. Francis

"The OpSource team continues to run one of the most important industry events year after year. Attendees get a full course of topics that matter most to SaaS ISV's or companies planning to migrate their offering to the SaaS model."

--Rick Nucci, Chief Technology Officer, Boomi

Mark Your Calendars!
SaaS Summit 09, March 11 - 13, 2009

www.saassummit09.net for Sponsorship Opportunities