

30 Minute Release 11*i* Security... *Keeping the Bad Guys Away*

Session Leader

Randy Giefer, Solution Beacon

NCOAUG 2006

Harper College, IL

August 11, 2006

www.solutionbeacon.com

Welcome

- Today's Agenda:
 - ◆ OAUG Membership Benefits
 - ◆ Presenter Introductions
 - ◆ Presentation Overview
 - ◆ 30 Minute Release 11*i* Security
 - ◆ Minute 31 – Your Next Steps
 - ◆ Questions and Answers

OAUG Membership

Member Benefits include:

- **Advocacy** opportunities to influence Oracle on product enhancements, usability, new features, Oracle support, pricing and quality.
- **Knowledge** that showcases the latest trends and techniques used by industry leaders through our national and regional events and our publications, such as OAUG Insight magazine.
- **Communication** with other OAUG members worldwide through participation in OAUG committees, leadership positions, interaction with Oracle Corporation's user initiatives, frequent member surveys, and Oracle management briefings.
- **Education** through the hundreds of career-enhancing presentations in our conference paper database archive, as well as discounts to conferences and Oracle education.
- **Networking** with Oracle customers, industry experts, third-party software firms, and other Oracle Applications specialists through our Member Database and Online Vendor Directory.

Presenter – Randy Giefer

- 20+ years of IT experience
 - ◆ Databases and Applications
 - ◆ 10 years Oracle Apps DBA
 - ◆ Fortune 1-1000
 - ◆ Government
- Founder of Solution Beacon, LLC
- Security Practice
- Email: rgiefer@solutionbeacon.com

Presentation Overview

- 1/2 Awareness
- 1/2 Real World Best Practices

30 Minute Release 11i Security

"Keeping The Bad People Away"

■ Case Studies

- ◆ Disgruntled Worldcom employee posts stolen names, SSN, birth dates of company executives on public website
- ◆ Ex-Employee Steals CRM and Financials Data and Provides to Competitor

30 Minute Release 11/ Security

"Keeping The Bad People Away"

■ Case Studies

- ◆ Employee Sells Credit History Database
- ◆ Employee Manipulates Payroll Data
- ◆ AOL Employee Sells Email Addresses to Spammer
- ◆ Laptops With Sensitive VA Data Stolen

30 Minute Release 11i Security

"Keeping The Bad People Away"

- Q. What do all of these Case Studies have in common?
 - ◆ Disgruntled Employee
 - ◆ Ex-Employee Steals CRM and Financials Data
 - ◆ Employee Sells Credit History Database
 - ◆ Employee Manipulates Payroll Data
 - ◆ Employee Sells Email Addresses to Spammer
 - ◆ Laptop With Sensitive VA Data Stolen
- A. A firewall didn't help!!!

What Is Security?

- What do you think of when someone mentions "security"?
 - ◆ Physical Security
 - ◆ Three Gs (Guards, Gates, Gizmos)
 - ◆ Technology Stack Security
 - ◆ Network (e.g. Firewalls, Proxy Servers)
 - ◆ Server (e.g. Antivirus)
 - ◆ Database (Auditing?)
 - ◆ Application (Access Lists?)

What Is Security?

- Most often, Security is focused on trying to keep the *external* bad people out ...
- But who is keeping out the *internal* bad people?

Today's Message

- The Internal Threats Are Real!

Fact: Internal Threats Are Real

Despite most people's fears that hackers will break into the company and destroy data or steal critical information, *more often than not, security breaches come from the inside.*

Fact: Internal Threats Are Real

- Gartner estimates that more than 70% of unauthorized access to information systems is committed by employees, as are more than 95% of intrusions that result in significant financial losses ...
- The FBI is also seeing rampant insider hacking, which accounts for 60% to 80% of corporate computer crimes

Fact: It may Happen To You

- In 2005, 20 Percent of Enterprises Will Experience a Serious Internet Security Incident – Gartner
- In 2005, 60 percent of security breach incident costs incurred by businesses will be financially or politically motivated – Gartner

Quotes From Industry Experts

- "Insider attacks are where most of the money's lost, where most of the vulnerabilities are."

Frank Huerta, Vice President Intrusion-Detection Product Delivery, Symantec

- "Technological protection from external threats is indeed important, but human problems cannot be solved with [only] technological solutions."

Eric D. Shaw, Keven G. Ruby, & Jerrold M. Post, Security Awareness Bulletin / RAND

Quotes From Industry Experts

- "In the Banking and Finance sector, fraud is typically perpetrated by a non-technical current or former employee. Sabotage, on the other hand, is typically led by a technical disgruntled employee, usually a former employee."

Dawn Cappelli, Carnegie Mellon University
/ CERT / Software Engineering Institute

Fact: It may Happen To You

- Are you prepared?
- Can you prevent becoming a statistic?

What Is Security?

- Security is a PROCESS that occurs (or doesn't occur) at multiple levels
- Security awareness at organizations varies due to:
 - ◆ Business Core Function
 - ◆ Organizational Tolerance (e.g. SOX)
 - ◆ Prior Incidents

Security Is A Process

- “Process” means it occurs more than once!
 - ◆ Policies, Processes and Procedures
 - ◆ Internal and External Checks and Balances
 - ◆ Regular Assessments (Focus = Improve)
 - ◆ Internal
 - ◆ Third Party

Security Is A Process

- “Process” means it occurs more than once!
 - ◆ Audits (Focus = \$ for Auditors)
 - ◆ Necessary Evil
 - ◆ Many Don’t Understand the Apps

What Is Applications Security?

In an Oracle Applications environment,
it's protection of information from:

- Accidental Data Loss
- Employees
- Ex-Employees
- Hackers
- Competition

Application Security

- Part Technology, Mostly User Access
- User Security
 - ◆ Authentication
 - ◆ Authorization
 - ◆ Audit Trail

Application Security

- Authentication – Who are you?
- Authorization – What privileges do you have?
- Audit Trail – Effectiveness is almost useless if you can't ensure:
 - ◆ Individual accounts are used
 - ◆ Individuals are who they say they are

What is "30 Minute Release 11i Applications Security"?

- Guide to Easily Implement Select Security Controls Consisting Of:
 - ◆ User Account Policies
 - ◆ Profile Options
- Quick and Easy to Implement
- Low Investment / High Return Value
- "Big Bang for the Buck"

Best Practice: No Shared Accounts

- Difficult or Impossible to Properly Audit
- How Hard Is It To Guess A Username?
- Release 11i Feature to Disallow Multiple Logins Under Same Username
- Uses WF Event/Subscription to Update ICX_SESSIONS Table
- 11.5.8 MP
- Patches 2319967, 2128669, WF 2.6

Best Practice: No Generic Passwords

- Stay Away From 'welcome'!!!
- 11.5.10 Oracle User Management (UMX)
- UMX – User Registration Flow
 - ◆ Select Random Password
 - ◆ Random Password Generator

11.5.10 Oracle User Management (UMX)

- UMX leverages workflow to implement business logic around the registration process
- Raising business events
- Provide temporary storage of registration data
- Identity verification
- Username policies
- Include the integration point with Oracle Approval Management
- Create user accounts
- Release usernames
- Assign Access Roles
- Maintain registration status in the UMX schema
- Launch notification workflows

Profile: Signon Password Length

- Signon Password Length sets the minimum length of an Oracle Applications password value
- Default Value = 5 characters
- Recommendation: At least 7 characters

Profile: Signon Password Hard to Guess

- The Signon Password Hard to Guess profile option sets internal rules for verifying passwords to ensure that they will be "hard to guess"

Profile: Signon Password Hard to Guess

- Oracle defines a password as hard-to-guess if it follows these rules:
 - ◆ The password contains at least one letter and at least one number
 - ◆ The password does not contain repeating characters
 - ◆ The password does not contain the username
- Default Value = No
- Recommendation = Yes

Profile: Signon Password No Reuse

- This profile option is set to the number of days that must pass before a user is allowed to reuse a password
- Default Value = 0 days
- Recommendation = 180 days or greater

Profile: Signon Password Failure Limit

- Default Value = 0 attempts
- Recommendation = 3
- By default, there is no lockout after failed login attempts: This is just asking to be hacked!

Profile: Signon Password Failure Limit

- Additional Notes:
 - ◆ Implement an alert (periodic), custom workflow or report to notify security administrators of a lockout
 - ◆ FND_UNSUCCESSFUL_LOGINS
 - ◆ 11.5.10 raises a security exception workflow

Profile: ICX:Session Timeout

- The length of time (in minutes) of inactivity in a user's form session before the session is *disabled*.
- Default value = none
- Recommendation = 30 (minutes)
- Also set *session.timeout* in *zone.properties*
- Available via Patch 2012308
(Included in 11.5.7, FND.E)

Minute 31 – Your Next Steps

- Be Paranoid!
- Review/Update/Create Security Processes, Procedures and Policies
- Be Proactive – Monitor Security Sources
- Oracle Critical Patch Update
 - ◆ CPU FAQ: 237007.1
 - ◆ Quarterly Releases

Minute 31 – Your Next Steps (continued)

- Protect Your Data
- No Direct Access
 - ◆ Only Allowed Via An Application
 - ◆ `tcp.invited_nodes` in `sqlnet.ora`
 - ◆ Oracle's Recommendation
 - ◆ MetaLink Note: 277535.1

Minute 31 – Your Next Steps (continued)

- Harden Operating System
- Harden Database
- Harden E-Business Suite Tech Stack
- Internal Assessment
- Third Party Assessment
- Continuous Process Improvement

Questions & Answers

For free Release 11i Tools and helpful information,
please visit our website at:

www.solutionbeacon.com

Real Solutions for the Real World[®]

Thank You!

Randy Giefer
rgiefer@solutionbeacon.com