Securing ERP Applications

Professional Strategies – S21

MODERATOR / PANELIST:

Steve Shofner
GRC Senior Manager
Armanino$^{\text{LLP}}$

ARMANINO PANELISTS:

Junior DeAlba
Senior Consultant - GRC

Eric Greathouse
Senior Manager Consulting – AX

Greg Horner
Manager Consulting – GP

2014 Fall Conference - "Think Big"

Learning Objectives

- Overview of high-level ERP Security *themes*
- Q&A with the Panel

High-Level ERP Security Themes

ERP Complexity

- ERPs are designed to work for companies of all sizes, industries
- Trying to be 'all things to all people'
- Therefore, they are very configurable
- For example: Oracle Financials (circa 2001 ish) reportedly had:
  - ~46,500 Configurable Options
  - ~4,600 had audit implications

One Example of ERP Security Challenges

Can be accomplished in many ways:

Scenario 1:

- Permissions maintain the 'least access principle,' granting access for each user to complete their current job responsibility *only.*

Scenario 2:

- Permissions allow full, unrestricted, administrator access to all users
- While users may have full access via *permissions*, they cannot access all *functions*, restricting their ability to use the system via the *views* or *menus* available within the application, effectively restricting access for each user to complete their current job responsibility *only.*

ERP Implementation Challenges

ERP Implementations & Security

ERP	Cost
Full implementation	$1,750,000
Without "Bells & Whistles"	$750,000

Typically overlooked 'bells & whistles'

Security: Granting everyone administrator access solves a lot of implementation challenges…and brings a lot of risk.

Legal: Implement the owning business unit's needed functionality. However, without Legal's input, the result may create legal, regulatory, or contractual issues.

Audit: Audit is the often-overlooked *system user*. Without their input, systems may not provide audit evidence and/or the evidence process could be significantly more efficient if input was collected at the design phase of the project.

ERP Security

Two Main Areas of Focus

1. Securing the Application

- System "Hardening." Some examples:
  - Restricting network access to critical services with the use of firewalls, for both the application and database servers
  - Require strong passwords with regular changes
  - Remove or disable default user accounts. Change passwords on remaining accounts.
  - Disable all unneeded services on server
  - Strike Passwords From Adpatch Logs
  - Set workflow notification Mailer Send Access_Key To *N*
  - Set Tools Environment Variables
  - Use SSL (HTTPS) Between Browser And Web Server
  - Use Terminal Services For Client-Server Programs
  - Etc.

2. Managing the Users

- Assigning, Managing, Revoking Access
  - Establishing Workflow
  - Enforcing and Monitoring Segregation of Duties

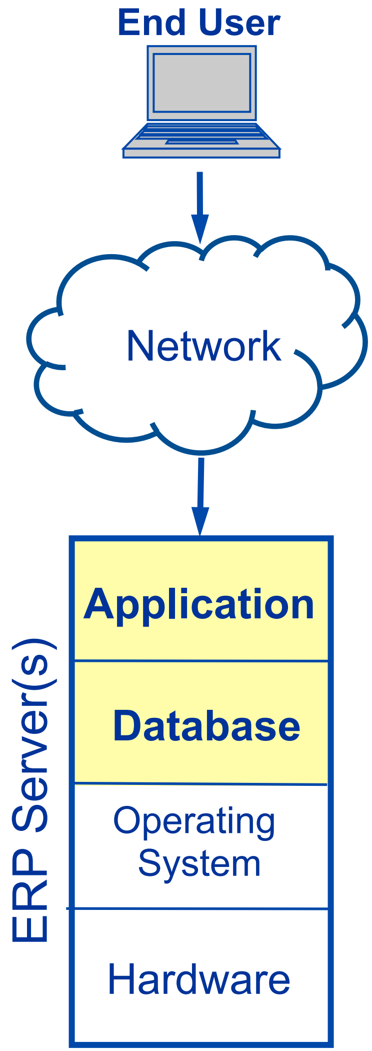
ERP Technology Layers

Security needs to focus on multiple layers of the 'Technology Stack,' primarily:

- Application
- Database

Also consider 'thick' vs. 'thin' client applications

- How secure do workstation need to be?
- Ensure end users can't change security on workstations.



Panel Discussion

CONTACT INFORMATION

Steve Shofner

office:	925.790.2879
mobile:	510.681.6638
email:	steve.shofner@amllp.com

Greg Horner

office:	925.790.2858
mobile:	202.253.9046
email:	greg.horner@amllpl.com

Eric Greathouse

office:	925.790.2839
mobile:	925.549.0358
email:	ericg@amllp.com

Junior DeAlba

office:	925.790.2719
mobile:	510.314.9306
email:	junior.dealba@amllp.com