ERP II System Vulnerabilities and Threats: An Exploratory Study

Richard S. Swart, Utah State University, USA; E-mail: richard.swart@business.usu.edu
Bryan A. Marshall, Georgia College and State University, USA; E-mail: bryan.marshall@gcsu.edu
David H. Olsen, Utah State University, USA; E-mail: david.olsen@business.usu.edu
Robert Erbacher, Utah State University, USA

ABSTRACT

Enterprise Resource Planning II (ERP II) systems integrate external entities into an organization's ERP system, primarily through integrating supply chain partners. This integration is facilitated through web services, a loosely coupled, platform independent way of linking applications within different organizations. Though many web services security standards exist, many organizations fail to implement these standards completely, therefore leaving the company vulnerable to security threats. This research study proposes a planning model for ERP II security. Some best practices related to managing and securing an ERP II system are gathered from extensive interviews with industry experts and government officials.

INTRODUCTION

Vendors recognized the significant opportunity for IT integration across departments, and robust ERP systems were developed out of more limited material planning packages for manufacturing. These systems modified the traditional processing paradigm of aligning the IT processes with department functions and instead created systems that tracked the workflow within the organization. This required management to coordinate with IT more closely and align job functions and training to the ERP system requirements. These ERP systems were purchased from major vendors and then customized to fit the particular needs of the organization with extensive help from outside vendors.

ERP systems arguably led to significant cost savings. However, original ERP systems were unable to accommodate the competitive pressures brought on by Just-In-Time (JIT) inventory management, supply chain integration and net-centric business models. These competitive issues led to a transformation of the ERP model into what is now called ERP II systems. These include linkages across the supply chain, and integration of customer relationship management (CRM) and logistics management software. The organizational boundary become diffuse, if not non-existent from the perspective of data flows. Suppliers are able to push transactions through the system with no real-time control by the receiving organization. In fact, network perimeters become obsolete since outside organizations are exchanging data with core business applications inside the organizations' trusted computing zone.

Darwin John, the former CIO of the FBI recently stated that "Security should be number two or three on any CIO's list of priorities" (Darwin John, personal communication, January 2006). While it is true that many vendors sell security solutions by creating a sense of fear, uncertainty and doubt, there is realistic reason to be worried. Carnegie Mellon's CERT Coordination Center's 2004 Annual Report states,

"In every way, the next twenty years will bring more of everything. More threats, more attacks, more resources at risk, more interconnection, more communication, more emergencies."

This highly pessimistic view of security appears to be warranted. The FBI/CSI annual crime report estimates that malicious software cost United States companies at least 170 billion dollars in 2004. This figure does not include loses from insider attacks, theft of intellectual property, or failed IT implementations. Symantec Corporation reports an unprecedented rise in malicious botnets and that malicious software is becoming more sophisticated, stealthy and polymorphic (Rob Clyde, VP of Research for Symantec, personal communication, November 2005).

More troubling than the proliferation of malicious software is the rise of extremely sophisticated and successful attacks on major United States companies, universities and government agencies seeking to steal defense and trade secrets. Though details are closely held by the Federal Bureau of Investigations, it has been widely reported that an active investigation is underway on network intrusion by agents of the Chinese government into highly sensitive United States government agencies under the case name Titan Rain (Espiner, 2005). Individuals associated with the National Security Administration have reported to the researchers that the Chinese government has over 3,000 professional information warfare agents actively attempting to steal United States government secrets, weapons plans and corporate trade secrets.

Many companies engage in routine business practices, which if details about them were discovered, could be used in launching attacks. For example, an attacker would be interested in knowing the shipping schedule of toxic chemicals through populated areas. A foreign agent may attempt to discern the intentions of our military through gaining information about supplies going to certain defense depots or shipping ports. A potential enemy would be very interested in design documentation regarding our weapons systems, and may attempt to counter our force superiority through exploitation of weaknesses in these systems.

Also, corporate espionage is a serious threat to large corporations, and these agents often seek similar information as intelligence agents: intellectual property, trade secrets, marketing plans, R & D proposals, merger and acquisition plans, etc. (Crane, 2005). Many foreign corporations actively seek to steal United States companies' trade secrets through placement of agents inside of their IT shops who can install malicious code to circumvent security restrictions, or to allow the agent to directly access the data from the servers.

RESEARCH METHODS

The researchers conducted a literature review regarding ERP II system vulnerabilities; though there is surprisingly little in the academic literature about these issues; after the initial review the researchers reviewed hacker websites and postings regarding these vulnerabilities. These initial reviews revealed that very little information is available on the net about ERP vulnerabilities.

The researchers also conducted a series of interviews with senior executives, IT security professionals, government officials, Big-4 IT security specialists, and other experts to using s a grounded theory approach to qualitative research (Strauss, 1990) to develop an initial model of planning ERP II security based on senior IT executives understanding of IT security in ERP II systems. These interviews were also undertaken to determine what the vulnerabilities are in these systems and to investigate the process of securing organizations in ERP II linkages.

The researchers then reviewed the XML/web services security literature to document security challenges that need to be addressed in ERP II projects (Anzbock, Dustdar, & Gall, 2002; Cremonini, De Capitani di Vimercati, Damiani, & Samarati, 2003; Damiani, De Capitani di Vimercati, & Samarati, 2002; Nadele, 2003). In order to

Copyright © 2007, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

better understand the issues facing IT staff during ERP deployments, a series of interviews with IT professionals in the process of an ERP implementation were conducted. Based on these investigations, the researchers developed an initial best practices guide and a planning model for ERP II Security.

Subjects in the Study

Given the qualitative and exploratory nature of this research, it is important to describe the subjects in some detail. Over a process of several months, telephone and face-to-face interviews were conducted with:

- The former CIO of the Federal Bureau of Investigations
- The current CIO of the Bureau of Alcohol, Tobacco and Firearms
- The Senior Security Consultant to the United States State Department and author of many NIST standards
- A State Chief Information Security Officer
- The CIO of a large multinational corporation
- Current and former federal agents/information security professionals who were/are employed by the FBI, NSA, and DIA
- Hackers
- One of the authors of original Rainbow series who was also one of the authors of the HIPAA legislation
- Two ERP vendors
- Three Big-4 accounting firm information security specialists
- Several faculty members from two of the three universities with the best reputation for IT security training
- ERP managers for two very large organizations
- Project managers for two ERP implementations

Limitations of Methods Used

A number of limitations on the methods used must be acknowledged. First, the sample of subjects was an extended convenience sample with snowballing. The researchers then approached individuals with whom they had contacts, and followed the chain of referrals for subsequent interview subjects. Second, the researchers attempted to contact a number of ERP vendors, IT consulting companies, Big-4 consultants, and companies known to the researchers to be involved with an ERP deployment. Unfortunately, corporations refused to grant access to their systems or discuss specifics about security implementation of their systems. It became apparent that vendors control dissemination of information about system vulnerabilities through Non-Disclosure Agreements and most corporations would not cooperate with this research.

Furthermore, discussions about ERP systems with hackers were not fruitful. Gaining entrance to the hacker community is essentially a "community of practice" process, where one is slowly invited to the community as one develops relationships and demonstrates competency (Wenger, 2002). Given that the subject of discussion is a felony under several provisions of the United States Code, it is understandable that the hackers approached by the researchers were less than forthcoming.

The initial model for ERP II security planning should not be considered a valid model, as it has not been empirically validated. Future work needs to be done to establish the accuracy of this model by testing its usefulness in an actual ERP II implementation.

FINDINGS

In the following section a brief overview of several ERP II security vulnerabilities is reviewed. Then a model is introduced which shows a matrix of polices and best practices which should be implemented to secure ERP II systems.

ERP II SECURITY VULNERABILITIES

Inherent Security Vulnerabilities in ERP II Systems

Vendors have done a good job creating secure ERP systems. Most have robust access control, auditing, and user authentication features. Their security architecture in general is sound. While early systems had significant weaknesses, no well-known ERP system on the market has a reputation for inherent weaknesses.

However, ERP systems are extremely complex pieces of software, and as with all code, there are going to be vulnerabilities. These systems are also vulnerable to weaknesses in the underlying databases. SAP R/3 had a known vulnerability that allowed users to gain super-user access to the ERP (Net-Security.org, 2001). With this privilege, an attacker could access or corrupt any data. In one sense, the incredible complexity of these systems facilitates security since their users will only have knowledge about a limited set of the system's functions. Their opportunities to launch attacks will necessarily be limited by their incomplete knowledge of the system architecture. This complexity also exposes the essential design flaw in these systems, and the need for custom configuration of thousands of options to ensure security. While auditing standards exist for ERP II systems, no known methodology allows enterprises to ensure that their customization conforms to the security policies of the organization (Magklaras & Furnell, 2005).

From a usability perspective one concern is that some ERP II systems still have a look and feel reminiscent of the old main-frame environment. Systems may require users to remember the names of screens for input and provide no contextual cues to guide the user. Usability research shows that users will circumvent security that they believe to be onerous or to interfere with their ability to accomplish work (Cranor, 2005). Thus, if users are not able to remember screen names or navigation sequences, they will augment their memory with reminders. These reminders become vulnerabilities themselves, as they often contain detailed guidance on accessing the systems and can include user IDs and passwords for screen access.

Vectors of Attack

Experts agree that the most likely vector of attack on ERP system will be through privilege escalation by an insider. Given that the data contained in the ERP II relates to customers, suppliers, vendors and employees, there is little data in the system of interest to a casual hacker seeking systems that can be compromised. Most professional hacking today is done for monetary gain. Much of it is related to identity theft and online fraud. Again, these forms of computer crime do not lend themselves to attacks on ERP II systems. However, an insider may attack the ERP II system through sabotage of key files, modifying passwords on accounts to halt the work flow, or by modifying DTDs or XML schemas to block the exchange of data (Polivy & Roberto, 2002).

A professional attacker will study the system for vulnerabilities and attack the system at the point where his skill, training and experience tells him that he is most likely to gain access without detection. This is one of the reasons why focusing on the security of the ERP II system alone cannot provide for effective security. For example, an attacker could access the network through a compromised web server and then install sniffing software on that machine to monitor the network for passwords. With a username and password combination, the attacker could then log directly into the ERP II system. This highlights the key roles that continual auditing and patch management play in maintaining the security of these systems.

Competitive Intelligence Threats

Inference is a well-known problem in access control (Morgenstern, 1987). Essentially, a user can submit a series of queries to a database with his access permissions. Using logic, the attacker is then able to identify specific attributes about one subject in violation of the access control policies. This issue is of paramount importance in the planning of an ERP II deployment. Most security features within ERPs are created in reference to specific screen views. An employee is granted access to particular screen, usually based on their role. While many ERP IIs use a form of RBAC, the need to customize thousands of screens leads to many unintended consequences that violate the organization's security policies.

Aggregation is the threat of unintended disclosure that arises from the combination of many items of data that allow deductions about some process or event about which the attacker has no other information (Jaeger, 2001). For example, if an attacker knew that the US Military had requisitioned air transport to Central Africa, had ordered lightweight summer clothing for 5,000 troops, and that vaccinations for malaria had been ordered for the third week of July, he could surmise that approximately 5,000 troops are being sent to Central Africa. If the attacker also had knowledge of the cargo being shipped ahead of time, one could make conclusions about the nature of the mission. This same form of intelligence gathering occurs in attacks on large corporations. In an insider is able to access many parts of the ERP II system, she may be able to determine true costs of products, discounts offered to particular vendors, marketing plans, R&D budgets, or financial issues that have not been released to the public. Many of the security experts interviewed stated that most ERP II systems have significant vulnerabilities related to unintended access control combinations, and that insider will exploit these vulnerabilities to gather specific confidential information.

Copyright © 2007, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

Supply Chain Partnership Model Weaknesses

One threat from opening up your system to supply chain partners is that once inside your system, it is possible for partners to "explore" the rest of your corporate data (Domke, 2001). Unisys Vice-President Peter Regent cautions companies that "You'll have to reengineer your processes to align with security. Otherwise, you won't get any return on your investment [in supply chain systems]" (Paul, 2004). Unfortunately, most ERP II systems are not engineering around security. The usual model is for the supply chain partners to agree on data exchange formats and to identify their common business processes. Security features are then added onto whatever existing mechanisms allow for the exchange of data.

Another serious concern that is often ignored in the implementation of ERP II systems relates to planning for the dissolution of the supply chain partnership. Too few organizations plan how to protect their data once they decide to remove an organization from the supply chain. An explicit procedure needs to be implemented to protect the confidentiality of data once the decision is made to remove someone from the chain. This can require extensive modifications to code when using web services.

Many of the consultants interviewed for this research caution that most supply chain linkages allow access to too much data by the parties. Essentially, organization A will be granted permission to access company B's ERP II system, but company B will not invest the resources needed to ensure that the data accessible by agents of organization A is minimally sufficient. Many organizations place the outside organization into an existing role. However, this can lead to the outside partner having access to information about true prices, marketing strategies, etc. that can give them competitive advantage. Research is underway at Purdue University to address how to arrange for encrypted exchanges of pricing and cost data so that both parties can gain maximum advantage through the relationship (Clifton, 2004). Essentially, organizations in an ERP II linkage still do not entirely trust the other participants, so the data on costs, production, shipping, etc., may be altered or otherwise obfuscated to protect the party releasing the data. This leads to an erosion of the potential value for all participants in the supply chain partnership.

Lastly, from a network security perspective, the creation of linkages with supply chain partners has two significant effects. First, the organization loses its network perimeter. In effect, the IT systems are merged into a unified system and each party allows outside organization access to the internals of its IT system. Second, everyone connected in a supply chain is exposed to whatever vulnerabilities exist in every partner's systems (Bragg, Rhodes-Ousley, & Strassberg, 2004). Thus, despite an organization's best efforts at protecting its systems, if one of its partners is compromised by malicious software, that partner's system can infect other organizations' system or introduce significant vulnerabilities into their IT architecture.

A MODEL FOR ERP II SECURITY PLANNING

The researchers developed the following model for ERP II security planning based on the seminal Information Assurance Model and the results of the interviews. See Figure 1.

This model is based on three components:

1. Security Services
2. Management Considerations
3. Targets of Security Planning

Each of these components is represented by an axis in the model. There are forty-five cubes within this model, and the researchers propose that effective ERP II security planning requires organizational effort to address each of these thirty-six cubes. For example, Database Security x Audit Methodology x Integrity would require that the organization define an audit methodology to ensure the integrity of data in the database through an analysis of existing database security measures.

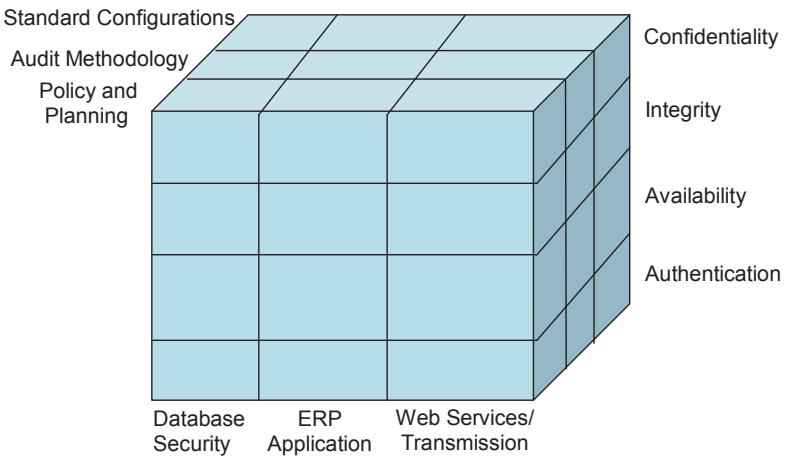
Security Services

The original IAM model proposed the well-known CIA triad for information security: confidentiality, integrity and availability. These are the security services that any system can provide. There is an inherent tension between these services, as ensuring the integrity and confidentiality of data often interferes with the availability of data. This model was later expanded to include authentication of users and non-repudiation of transactions (Schou, 2004). Accordingly, this planning model requires all participants in an ERP II enabled supply chain to address confidentiality, integrity, availability, authentication and non-repudiation of transactions. These services are provided by the ERP II system, but planning needs to ensure that the features of the systems are fully implemented.

Management Considerations

The second axis of the ERP II Security Planning Model discusses the three broad areas for management attention: standard configurations, audit methodologies, and policies and planning. The best practices portion of this paper will address specific issues related to standardized configurations which are suggested in order to reduce the complexity of the security planning process, to enable better patch and configuration management, and to reduce the overall vulnerability of the system through reducing the types of operating systems and applications. Audit methodologies will also be discussed in detail in the best practices guide. Senior executives report that reliance of the existence of third party IT audits does not guarantee the security of a system. Each firm has its own audit methods. This issue becomes even more crucial when considering international partnerships. ITIL, ISO 17799, and Control Objectives for Information and related Technology

Figure 1. The ERP II security planning model



Copyright © 2007, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

(COBIT®) (ITIL, 2006) COBIT are three widely used IT audit frameworks, but they vary greatly in their focus, level of detail, and scope of review. Effective security demands that all partners agree ahead of time on a standardized audit methodology to ensure that vulnerabilities are discovered and addressed in all partner organizations. Lastly, there needs to be a formal process, a well-managed project to plan the policies that will guide users of the ERP II system. This process must be conducted internally, and cannot be wholly delegated to the ERP II implementation consultants.

Targets of Security Planning

Throughout this project, ERP II managers emphasized the critical interdependencies between the underlying databases and the ERP II applications. It was also discovered that all major ERP II vendors are using web services to facilitate inter-company communication. Accordingly, we have defined three areas that require management attention in planning. First, the database must be secured. In most ERP II systems, the ERP II appears to the database as a single user. However, the ability to connect to the database exists outside of the ERP architecture. An attacker may be able to sabotage the ERP II or steal data via unauthorized access to the database. The configuration of the ERP II is also a critical challenge as there are literally thousands of possible configuration options and screens to address. An effective ERP II implementation requires a minimum of 5% of the resources to be dedicated to planning access control models and searching for security policy violations that could occur (West, B., personal communication, March 2006). Lastly, there are significant weaknesses in the implementations of most web services projects. These weaknesses occur through using only a limited set of the web services standards, which results in providing only part of the CIA triad.

FUTURE RESEARCH

The researchers realize that perhaps the most important piece of this research may be missing. Currently we are working on mapping the collected qualitative data, essentially a list of best practices to the model developed in this paper. We hope to demonstrate a systematic approach to securing ERP II implementations.

REFERENCES

Anzbock, R., Dustdar, S., & Gall, H. (2002). Software configuration, distribution, and deployment of web-services. Paper presented at the Twelfth International Software Engineering and Knowledge Engineering, Ischia, Italy.

Bragg, R., Rhodes-Ousley, M., & Strassberg, K. (2004). Network Security: The Complete Reference. New York: McGraw Hill.

Clifton, C. (2004). Privacy-preserving data integration and sharing. Paper presented at the ACM SIGMOD workshop on Research issues in data mining and knowledge discovery, Paris, France.

Crane, A. (2005). In the company of spies: When competitive intelligence gathering becomes industrial espionage. Business Horizons, 48(3), 233-340.

Cranor, S. G. (2005). Security and Usability : Designing Secure Systems that People Can Use Sebastapol, CA: O'Reilly Media.

Cremonini, M., De Capitani di Vimercati, S., Damiani, E., & Samarati, P. (2003). An XML-based approach to combine firewalls and web services security. Paper presented at the ACM Workshop on XML security 2003, Fairfax, VA.

Damiani, E., De Capitani di Vimercati, S., & Samarati, P. (2002). Towards Securing XML Web Services. Paper presented at the ACM Workshop on XML Security 2002, Fairfax, VA.

Espiner, T. (2005). Security experts lift lid on Chinese hack attacks [Electronic Version]. ZDNet News. Retrieved March 11, 2006 from http://news.zdnet.com/2100-1009_22-5969516.html.

ITIL. (2006). IT Infratstructure Library.

Jaeger, T. T., Jonathon E. . (2001). Practical safety in flexible access control models. ACM Transactions on Information and System Security 4(2), 158-190.

Magklaras, G. B., & Furnell, S. M. (2005). A preliminary model of end user sophistication for insider threat prediction in IT systems. Computers & Security, 24(5), 371-380.

Morgenstern, M. (1987). Security and inference in multilevel database and knowledge-base systems. Paper presented at the ACM SIGMOD international conference on Management of data, Proceedings of the 1987 ACM SIGMOD international conference on Management of data.

Nadele, M. (2003). Standards for XML and Web Services Security. Computer, 36, 96-98.

Net-Security.org. (2001). SAP R/3 Web Application Root Compromise. Retrieved February 5, 2005, from http://www.net-security.org/vuln.php=853

Paul, L. G. (2004). Keep it moving. Retrieved February 5, 2005, from http://www.csoonline.com/read/093004/moving.html

Polivy, D. J., & Roberto, T. (2002). Authenticating Distributed Data Using Web Services and XML Signatures. Paper presented at the ACM Workshop on XML Security, Fairfax, VA.

Schou, C., Frost, J., Maconachy, WM. (2004). Information assurance in biomedical informatics systems Journal of Organizational and End User Computing, 23(1), 110-118.

Strauss, A., & Corbin, J. (1990). Basics of qualitative research: Grounded theory procedures and techniques. Newbury Park, CA: Sage.

Copyright © 2007, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

0 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/proceeding-paper/erp-system-vulnerabilities-threats/33216

Related Content

Design and Implementation of an Intelligent Moving Target Robot System for Shooting Training
Junming Zhaoand Qiang Wang (2023). *International Journal of Information Technologies and Systems Approach (pp. 1-19).*
www.irma-international.org/article/design-and-implementation-of-an-intelligent-moving-target-robot-system-for-shooting-training/320512

Formal Verification Methods
Osman Hasanand Sofiène Tahar (2015). *Encyclopedia of Information Science and Technology, Third Edition (pp. 7162-7170).*
www.irma-international.org/chapter/formal-verification-methods/112414

A Framework for Understanding Information Systems Development
Andrew Basden (2008). *Philosophical Frameworks for Understanding Information Systems (pp. 224-264).*
www.irma-international.org/chapter/framework-understanding-information-systems-development/28084

Big Data Issues and Challenges
Stephen Kaisler, Frank Armour, William Moneyand J. Alberto Espinosa (2015). *Encyclopedia of Information Science and Technology, Third Edition (pp. 363-370).*
www.irma-international.org/chapter/big-data-issues-and-challenges/112346

The Influence of Digital Currency Popularization and Application in Electronic Payment Based on Data Mining Technology
Xiaoyuan Sun (2023). *International Journal of Information Technologies and Systems Approach (pp. 1-12).*
www.irma-international.org/article/the-influence-of-digital-currency-popularization-and-application-in-electronic-payment-based-on-data-mining-technology/323193