IDEA GROUP PUBLISHING ITB12228

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This paper appears in the publication, Enterprise Information Systems Assurance and Systems Security
edited by Merril Warkentin © 2006, Idea Group Inc.

Chapter VI

A Security Blueprint for E-Business Applications

Jun Du, Tianjin University, China

Yuan-Yuan Jiao, Nankai University, China

Jianxin (Roger) Jiao, Nanyang Technological University, Singapore

Abstract

This chapter develops a security blueprint for an e-business environment taking advantage of the three-tiered e-business architecture. This security blueprint suggests best practices in general. It involves (1) security control by layers — from physical access, to network communication, to operating systems, to applications, and (2) different stages of the management process, including planning, deployment, administration, and auditing. Also reported is a case study of the implementation of the proposed security blueprint in a Singapore multinational corporation. Such issues as security control analysis, management process analysis, and cost-benefits analysis are discussed in detail.

Introduction

The Internet has created huge opportunities for new companies and new business for those established organizations formerly bound by a saturated market. E-business is defined as the conduction of business with the assistance of telecommunications and telecommunication-based tools, mainly over the Internet (Clarke 1999), including *busi-*

ness-to-business (B2B), *business-to-customer* (B2C), and intra-organizational commerce (Siau & Davis, 2000). Security is essential and very critical to e-business applications. The importance of information privacy to e-business has been recognized for some time (Agre & Rotenberg, 1997; Bingi, Mir, & Khamalah, 2000; Lichtenstein & Swatman, 2001), with the Gartner Group (2002) nominating information privacy as the greatest impediment to consumer-based e-business through 2006.

However, when building up a secure environment for e-business applications, there are no industry standards for people to follow on their design or implementation jobs. All that can be referred is from the security product manufacturers and system integrators. The truth is that security systems can only provide a certain level of protection to an e-business environment. Therefore, security protection must be in place at different layers, and the management process must be carried out at different stages. From the authors' viewpoint, security is not a by-product; it is a combination of managing technologies and security processes, rather than "put the firewall here, put the intrusion detection system there."

This chapter develops a security blueprint for a typical e-business environment based on the discussion of the major components in three-tiered e-business architecture. This security blueprint includes general security control layered from physical access, network communication, operating system, to application; and security management processes staged from planning, deployment, administration, to auditing.

Typical E-Business Environment

Originally, business computing was carried out as a point task, without any real concept of a networked operation. All the business processes are run on a single platform or single tier. Later, many systems evolved to a two-tiered approach, also known as client/server architecture, where most of the business process runs on the server and the client is mainly concerned with presentation and only holds a limited amount of user-specific data. Today, more and more e-business applications are deployed as a three-tiered architecture owing to its increased performance, flexibility, maintainability, reusability, and scalability, while hiding the complexity of distributed processing from the user. After this, things get more complicated, with additional applications running in different tiers, which is so-called multi-tiered architecture. However, multi-tiered architectures have arisen not necessarily because great thought was given to this choice of architecture; in truth, they are more the result of trying to make the best of what was there.

This section will describe a typical three-tier e-business environment and identify the major components from system architecture perspectives.

Three-Tier E-Business Architecture

When it comes to an e-business environment, usually, these three tiers (layers) can be described as the *presentation* layer, *business* logic layer, and *data* layer. These tiers are