Chapter X

E-Commerce Security Planning

Daniel L. Ruggles
Vice President, Technology Consulting Associates, LLC
USA

Biography

Daniel L. Ruggles is Vice President, Technology Consulting Associates, LLC. He is a Certified Information Systems Security Professional (CISSP). TCA, headquartered in Atlanta, Georgia, provides expert technology and business consulting services in a wide range of industries. For further information, call 404-303-1795 or visit the company's Web site at http://www.tca-llc.com.

Executive Summary

Multiple levels of potential security risk affect all the elements of an e-commerce site. Truly complete security protects three areas: (1) internal network and application services, (2) perimeter network access and application services, and (3) external network and services. To minimize security risks in these areas as well as to raise overall confidence in the e-
commerce service, businesses must address problems with practical solutions involving privacy and security. Establishing an *e-commerce trust infrastructure* encompasses confidentiality, data integrity, non-repudiation and authentication. Striking the right balance between functionality and accessibility in e-commerce demands technical security measures. It also requires management vigilance with non-technical measures such as routine assessments of vulnerabilities, policies, education and a focus on making processes and policies easy to understand and simple to implement and monitor compliance.

**Introduction**

The design and architecture of an e-commerce site can take on many different appearances, depending on the company’s objective and the type of commerce being conducted at the site. Unfortunately, many architectural decisions are not necessarily based on security considerations, causing potential holes in the overall network environment. E-commerce sites contain multiple levels of potential security risk affecting all their common building blocks: Web servers, commerce servers, database servers, routers, firewalls, network connectivity and the use of DMZs (demilitarized zones). Identifying and protecting sensitive data at all these levels can be accomplished by using various security features and building layers of complexity, commensurate with the value of the commerce being conducted.

**Prevent the Past from Becoming the Future**

**Discussion of Issues**

Based on responses from 503 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institu-
Related Content

E-Mexico: Collaborative Structures in Mexican Public Administration
www.irma-international.org/article/mexico-collaborative-structures-mexican-public/1514/

Impact of E-Learning During SARS Outbreak in Hong Kong
www.irma-international.org/chapter/impact-learning-during-sars-outbreak/30403/

Service-Oriented Architectures and Virtual Enterprises
www.irma-international.org/chapter/service-oriented-architectures-virtual-enterprises/12665/

An Update on Mobile Broadband Availability in the United States
Thomas V. Church and James E. Prieger (2016). Encyclopedia of E-Commerce Development, Implementation, and Management (pp. 1518 -1531).
www.irma-international.org/chapter/an-update-on-mobile-broadband-availability-in-the-united-states/149058/
Temporal Pattern of Communication: Messaging Within a Mobile Social Networking App
[www.irma-international.org/article/temporal-pattern-of-communication/124077/]