

Implementation of System and Network Security for an Enterprise

Dr. Sandeep Kumar*

MCA from Kurukshetra University Kurukshetra, PhD from Singhania University

Abstract – Networks today run mission-critical business services that need protection from both external and internal threats. In this paper we proposed a secure design and implementation of a network and system using Windows environment. The basic reasons we care about information systems security are that some of our information needs to be protected against unauthorized disclosure for legal and competitive reasons; all of the information we store and refer to must be protected against accidental or deliberate modification and must be available in a timely fashion. We must also establish and maintain the authenticity (correct attribution) of documents we create, send and receive. Finally, the if poor security practices allow damage to our systems, we may be subject to criminal or civil legal proceedings; if our negligence allows third parties to be harmed via our compromised systems, there may be even more severe legal problems. Another issue that is emerging in e-commerce is that good security can finally be seen as part of the market development strategy. Consumers have expressed widespread concerns over privacy and the safety of their data; companies with strong security can leverage their investment to increase the pool of willing buyers and to increase their market share. We no longer have to look at security purely as loss avoidance: in today's marketplace good security becomes a competitive advantage that can contribute directly to revenue figures and the bottom line. Reviews of latest product with an application to an enterprise with worldwide branches are given.

Keywords: Network Design, LAN, WAN, Security, Encryption, VPN, IPSec, Active Directory.

-----X-----

1. INTRODUCTION

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms [8]. Governments, military, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers. Should confidential information about businesses customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to

lost business, law suits or even bankruptcy of the business. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement. For the individual, information security has a significant effect on Privacy, which is viewed very differently in different cultures.

The field of information security has grown and evolved significantly in recent years. As a career choice there are many ways of entering the field. It offers many areas for specialization including Information Systems Auditing, Business Continuity Planning and Digital Forensics Science, to name a few.

2. SECURITY SERVICES AND PROCESSES

Security is fundamentally about protecting assets. Assets may be tangible items, such as a Web page or our customer database — or they may be less tangible, such as our company's reputation. Security is a path, not a destination. As we analyse our infrastructure and applications, we identify potential threats and understand that each threat presents a degree of risk. Security is about

