DATA SECURITY OVER THE INTERNET

Archana Jayakumar[1], Arul prakash P[2]
[1]Infosys Technologies Limited, Chennai, INDIA
[2]VS & B Containers Private Limited, Chennai, INDIA
Email : [1]archana.jayakumar@yahoo.co.in

Abstract

The computer industry has thrived on technological advancement since its birth. The rising abuses of computers and increasing threat to personal privacy through Internet technologies have stimulated much interest in the technical safeguards for data. Scalable and elastic IT-enabled capabilities are provided as a service to external customers using Internet technologies is cloud computing. Security is becoming more and more important in all business processes and IT application areas. The rising need for secure business critical computing results from a number of economical, social and political trends: The increasing integration of applications and business processes horizontally and vertically in all business services, the ever growing number and variety of clients and mobile always-on network connections and applications to the Internet

Keywords: Security, Data Security, Protection, Access Controls, Cloud Computing, Firewall, Internet

I. INTRODUCION

Today, nearly every single aspect of business and standard of living depends on secure and reliable IT – the supply chain for the local supermarket as well as a telecom network. In order to leverage the competitive advantages of information technology, global handling of finance and goods needs a continuously available IT infrastructure, just like the government and small and medium-sized companies. But the tremendous benefits offered by the IT are more and more threatened by viruses, hackers and terrorists and industrial espionage. This results in a growing need for security throughout the entire IT applications including INTERNET.

- Client with the web browser renders the content to the user
- Network transports the data between the client and the server
- Server with the web application performs the required action.
- Database stores the result

II. CHALLENGE

- Maintain a secure environment
- Life cycle management of vulnerabilities and incidents
- Protect your business from Internet threats without jeopardizing bandwidth or availability
- Protect your end-user from spasm and other productivity drainers
- Conserve resources by eliminating the need for specialized security expertise.
- Ensuring data and intellectual property is not stolen while crossing the internet
- Ensuring that data is not tampered with or altered between the server and the client
- Minimizing cost over the security

III. SECURITY ATTACKS ON INTERNET

Security id now defined through the risk management and compliance disciplines instead of threat and technology disciplines. Secure information technology has assumed a new significance in the third millennium. High-performance data centers and broadband global networking have transformed the computer from a helpful tool into an indispensable engine of progress. Business processes, communication channels, knowledge management, m-business and countless services are based on a secure, functioning IT infrastructure. For a growing number of companies, their entire business consists of functioning IT, such as Telco or outsourcing services. The security of Business Critical Computing (BCC) and Mobility thus represents a core component of business success.

The number of active automated attacks on the web servers was unprecedented. Browsers and web applications are still largely ignored or prioritized below other infrastructure from a security perspective. The number of web crime is rising and the need for security is growing shwon in figure 1.

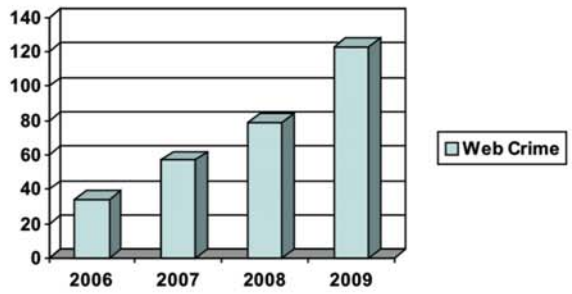

Fig. 1. The number of web crime is rising and the need for security is growing

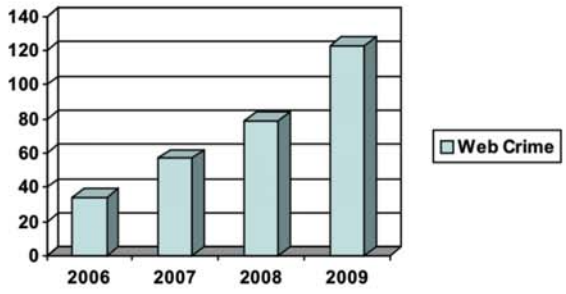

Fig. 2. The amount spend for the data security is high and the need for security is growing

The trend to mobile IT magnifies the request for security. According to Meta Group, more than 70 per cent of all corporate users are expected to have mobile access to their data until 2005. On one hand, this extends the reach of business processes, but on the other hand it means that more and more confidential enterprise data are in use outside the corporate campus(figure 3.)

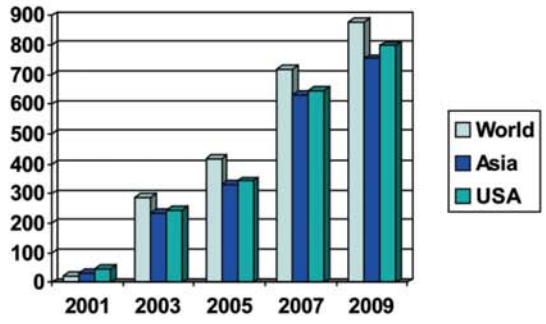

Fig. 3. The number of mobile Internet users is rising and the need for security is growing

IV. THE CORNERSTONES OF DATA SECURITY

In order to protect an organization's IT infrastructure from harmful influences, security measures are needed at any and all potential weak points. Complete integration into the existing applications landscape will be as much a key to the success of any such measures as security-conscious employees. For example, it is not enough to employ an extremely sophisticated encryption technology for network links if the gateway, the applications server or one of the network clients is insufficiently secured. There are numerous programs on the Internet that seize upon passwords, transaction information or network services directly when they are being entered at a monitor before encryption or signature can be carried out. In extreme cases, all it takes is one such security leak to nullify whatever protection any other security measures might provide.

The components are grouped according to their security function into the segments authentication, authorization, access control, audit, administration and awareness.(Table 1.)

Table 1. Security Function and Solution MethodsI

Security Function	Solution Methods
Authentication	passwords, one-time logins, biometrics, Smartcards
Authorization	protecting user rights by roles and privileges, secure application environment
Access Control	Secure database technology (e.g. Virtual Private Database), network encryption (e.g. IPSec), data encryption, domain-based access control, firewall
Audit	manipulation-proof protocols, intrusion detection (capturing and retaining actions), no repudiation
Administration	security management, central security update strategy, single sign-on, directory service
Awareness	training, penetration tests, content security

The Right Choice for Secure File Sharing:

When searching for a network folder encryption solution, several factors should be considered.(Table 2.) The majority of these parameters should fall in line with the overall strategy of the organization, its security goals and its technology environment. While not a complete, comprehensive list, the following provides a baseline framework for beginning a search for a network folder encryption solution

Crime on the Web :

Long-term forensic studies have revealed that up to three percent of the population is susceptible to criminal dealings, even though only a small percentage of these will actually become a threat. There are an estimated one billion potential Internet users, which means that there are potentially 30 million criminals out there. Language barriers and lack of know-how have kept much of this potential at bay up till now but the appearance of largely automated assault and theft tools has greatly magnified the threat. Even the technically uninitiated can find tools easily wielded with the click of a mouse on Web sites or IRC channels. These tools are capable of automatically locating unprotected servers, breaking in and using sophisticated methods to camouflage themselves. For example in 2000, a technically unsophisticated journalist was able to steal thousands of credit card numbers within just a few minutes from an American e-commerce business, without even understanding the system in detail.

Table 2. Network Folder encryption

Factor	Description	Example
Centralized Management	The latest solutions include centralized management that offer easy-to-use options for administrators, and can help eliminate or reduce expensive training.	A new employee is hired and requires access to a group of encrypted folders. In one action, an administrator can modify access for folders the person needs, instead of changing access for each folder separately.
Ease of Use	The solution should be automatic and transparent, and not have an adverse effect on the user's work environment. End-users can easily collaborate and share information within the corporation, or with select third parties.	An end-user creates and manages folder access without the need to contact a network administrator.
Persistent Encryption	The inclusion of persistent encryption is a valuable feature that secures a file or folder no matter where it is stored.	A former employee has sensitive files on a USB drive at home. Encryption of the files remains intact, as his/her access is removed from the centrally controlled server.
Leverage Existing Workgroups	The solution should seamlessly integrate with the existing infrastructure for workgroup information.	Workgroups may already be defined in an Active Directory (e.g., global, sales or marketing).
Flexible Authentication	A sophisticated solution should upport a variety of authentication methods, including Windows and digital certificates.	The solution could be integrated with other third-party hardware products for storage of digital certificates to enable Multifactor authentication.

The ease of such actions means that intruders are often content with even minor scams. Moreover, the virtual world allows hackers to avoid having direct contact with their victims. Any eventual scruples are cast aside with the argument, "Well, it's their own fault - they deserve it if they're going to leave data just lying around like that!" The unscrupulous mouse-clickers never get to see the fate of their victims. All that counts is a quick hack. Several attacks that started out "just for fun" rapidly assumed more serious proportions in the face of burgeoning Internet transactions. The result is millions in damage. Parents of "script kids" are often even proud of their purportedly intelligent offspring. Companies can only react by upping security measures. Just like manufacturing facilities and warehouses, virtual buildings need all the protection they can get.

The threat doesn't necessarily always come from the outside, however. Breaches of security can come just as well from workers within the network. Sabotage, vandalism and theft of data are often ways for frustrated employees to get back at the organization or to earn some extra money. Besides log functions and frequent education, specific measures are needed to ensure that each user gets only the access that he or she needs at a particular time and for a particular purpose.

What needs to be secured?

- Integrity: Unauthorized manipulation of documents , Web sites or e-mails, forging of documents, reprogramming of services
- Availability: Interruption of system operations, networks or services, breakdowns due to hackers, service costs due to viruses, spam or break-in attempts
- Confidentiality: Loss of data: temporary or permanent, removal or deletion of business data, unauthorized use of computers, networks or software, industrial espionage
- Accountability: Data abuse: unauthorized use of confidential data such as personnel files, passwords, e-mails, address lists, appropriation of payment information.

V. CONCLUSION

Business is constantly evolving as are its workers, its associates' structures and its customers. Potential threats, be they from new viruses, hacker attacks, new file formats or tools are also constantly evolving. Every security infrastructure therefore requires constant maintenance. Since security solutions often begin at central points in the infrastructure, they must also fulfill the highest standards of operating security and they must be up to date. For example, every anti-virus bulletin should immediately be disseminated throughout all of the organizations' anti-virus programs - and not only months afterward. As the hacker attack on Microsoft headquarters demonstrated, a delay in distributing such information can result in considerable damage.

Security should serve to support growth and the exploitation of new opportunities. It is for this reason that there is no substitute for expert know-how in operating and modifying security solutions. External service providers can augment internal security processes using service packages flexibly, depending on corporate strategy. The offerings range from one-time security checks to the complete operation of security components on behalf of the client.

REFERENCES

[1] http://news.zdnet.com

[2] http://www.interhack.net

[3] www.cs.columbia.edu/~smb/papers/distfw.html.

[4] Kurose and Ross, “Computer Networking a Top Down Approach Featuring the Internet”.

[5] ANDERSON J.P, "Information security in a multuser computer environment in Advances computers”, Vol.12, Morris Rubinoff (Ed.), Academic Press, New York.

[6] BECK L.L, “ A security mechanism for DENN79C stattstical databases”, Dept. Computer Science and Engineering, Southern Methodist Univ., Dallas, Tex.

[7] COHEN E, 1977, "Information transmission in computational systems", Proc. 6th Symp. Operating Systems Principles, (special is- sue) Oper. Syst. ReD. (ACM) 11, 5, pp. 133-139.

[8] DENNING D.E, 1979, “Securing databases under random sample queries”, ComputerScience Dept., Purdue Univ., W. Lafayette, Ind.

[9] "Programming semantics for multiprogrammed computations," Communication. ACM 9, 3 (March 1966), pp.143-155.