ISSN: 2348-0351

E-Governance and Data Security

Mr.Santoshkumar M. Wadkar
Asst.Professor (B.Sc(Cs), MCA)
Vasant Kale College of Computational and Management Sciences, Visnupuri, Nanded-431606.

Abstract
The rise of e-government has been one of the most striking developments of the web world. As the Internet supported digital communities evolve, and assuming that they do indeed grow to incorporate individuals around the country and globe, they present the national governments with a number of challenges and opportunities. In an e-government project, a substantial amount of documentation is done like maintenance of land records, police records and so on. Each department is critical so that only authorized people get into the network and access the information. The effective management of information security is a key factor as willingness, of the different users (citizens and other parties), to use e-Government services will heavily depend on the trust they have on the data security of this service. An understanding of the Data security technology and the need for its implementation is key for safer, secured and smooth functioning of e-governance undertaking.
Keywords: Data Security Technology, E-Governance-Government.

I.INTRODUCTION

Global shifts towards increased deployment of IT by governments emerged in the nineties, with the advent of the World Wide Web. The term e-Government is defined by the Organization for Economic Cooperation and Development (OECD) as the use of new information and communication technologies (ICTs) by governments as applied to the full range of government functions. In particular, the networking potential offered by the Internet and related technologies have the potential to transform the structures and operation of government. The technology as well as e-governance initiatives have come a long way since then. With the increase in Internet and mobile connections, the citizens are learning to exploit their new mode of access in wide ranging ways.

They have started expecting more and more information and services online from governments and corporate organizations to further their civic, professional and personal lives, thus creating abundant evidence that the new "e-citizenship" is taking hold. While the emphasis has been primarily on automation and computerization, state governments have also endeavored to use ICT tools into connectivity, networking, setting up systems for processing information and delivering services. Every state government has taken the initiative to form an IT task force to outline IT policy document for the state and the citizen charters have started appearing on government websites. The generally accepted definition is: E-governance is the application of information & communication technologies to transform the efficiency, effectiveness, transparency and accountability of informational and transactional exchanges with in government, between government and government agencies of National, State, Municipal and Local levels, citizen & businesses and to empower citizens through access and use of information. "e-government" or electronic government refers to the use of Information and Communication Technologies (ICTs) by government agencies for any or all of the following reasons:

- Speedier and more efficient delivery of public services
- Improving internal efficiency
- Exchange of information with citizens, businesses or other government departments
- Reducing costs or increasing revenue

ISSN: 2348-0351

- Re-structuring of administrative processes

There are similarly endless ways to utilize Information and communication technologies to provide efficient and transparent solutions to citizens without security threats.

II. OBJECTIVES OF STUDY

- To Understand E-governance And Data Security
- To Identify Data Security Threats
- To Improve Security in E-Governance

III. DATA SECURITY

Data Security Policies are the cornerstone of information security effectiveness. The Security Policy is intended to define what is expected from an organization with respect to security of Information Systems. A central challenge of e-Government service is how the new technology can be used not only to increase efficiency for public administration, but also to strengthen confidence in privacy measures by creating mutual transparency between public administration and citizens. The overall objective is to control or guide human behavior in an attempt to reduce the risk to Data assets by accidental or deliberate actions. Data security policies underpin the security and well-being of Data resources. They are the foundation, the bottom line, of Data security within an organization. In an organization, having the right Data at the right time can make the difference between success, and failure. Data Security will help the user to control and secure information from, inadvertent or malicious changes and deletions or unauthorized disclosure. There are few aspects of data security:

Authentication: capability to identify who is using the services (person or software program). Processes of verifying that you are who you say you are.

Authorization: capability to give rights access to resources. Process to verify someone has the rights to do what he/she is trying to do.

Confidentiality: refers to protection of information from unauthorized disclosure e.g. to the press or to release through improper disposal techniques, or to those who are not entitled to have the same.

Integrity: is about protecting Data from unauthorized modification, and ensuring that Data, such as a beneficiary list, can be relied upon and is accurate and complete.

Availability: is to ensure that the Data is available when it is required.

Non-repudiation: capability to prevent the intervening person or system in an event or action to denying or challenging their participation on the event.

IV. DATA SECURITY THREATS

Incidents come in all shapes and sizes. They can come from anywhere on the Internet, although some attacks must be launched from specific systems or networks and some require access to special accounts. A cyber-attack may be a comparatively minor event involving a single site or a major event in which tens of thousands of sites are compromised. A typical attack pattern consists of gaining access to a user's account, gaining privileged access, and using the victim's system as a launch platform for attacks on other sites. It is possible to accomplish all these steps manually in as little as 45 seconds; with automation, the time decreases further. Though, it is difficult to characterize the people who cause incidents. Thus, the networks providing data to the end users of the e-Government remain vulnerable to variety of threats such as packet sniffing, probing etc.

A. Packet Sniffer

A packet sniffer, sometimes referred to as a network monitor or network analyzer, can be used legitimately by a network or system administrator to monitor and troubleshoot network traffic.

B. Probe

Probe is a class of attacks where an attacker scans a network to gather Data or find known vulnerabilities.

C. Malware

Malware, short for malicious software, consists of programming (code, scripts, active content,

ISSN: 2348-0351

and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior. Malware includes Trojan horses, viruses, and worms.

D. Denial of Service (DOS) attack

A denial of service attack is a class of attacks where an attacker makes a computing or memory resource too busy or too full to handle legitimate requests, thus denying legitimate user access to a machine e.g. neptune, teardrop, smurf, pod, back, land. Attackers may "flood" a network with large volumes of data or deliberately consume a scarce or limited resource, such as process control blocks or pending network connections.

V. IMPROVING SECURITY IN E-GOVERNANCE

To make Data available to those who need it and who can be trusted with it, a robust defense requires a flexible strategy that allows adaptation to the changing environment, well-defined policies and procedures, the use of robust tools, and constant vigilance. It is helpful to begin a security improvement program by determining the current state of security at the site. Methods for making this determination in a reliable way are becoming available. Integral to a security program are documented policies and procedures, and technology that support their implementation.

A. Security policy

All of the security policy is enforced by mechanisms that are strong enough. A policy is a documented high-level plan for organization-wide computer and Data security. It provides a framework for making specific decisions, such as which defense mechanisms to use and how to configure services, and is the basis for developing secure programming guidelines and procedures for users and system administrators to follow. Because a security policy is a long-term document, the contents avoid technology-specific issues.

A. Security Practices

System administration practices play a key role in network security. Checklists and general advice on good security practices are readily available. Below are examples of commonly recommended practices:

- Ensure all accounts have a password and that the passwords are difficult to guess. A one-time password system is preferable.
- Use tools such as MD5 checksums a strong cryptographic technique, to ensure the integrity of system software on a regular basis.
- Use secure programming techniques when writing software. These can be found at security-related sites on the World Wide Web.
- Regularly check with vendors for the latest available fixes and keep systems current with upgrades and patches. Regularly check on-line security archives, such as those maintained by incident response teams, for security alerts and technical advice.
- Audit systems and networks, and regularly check logs. Many sites that suffer computer security incidents report that insufficient audit data is collected, so detecting and tracing a cyber-attacks is difficult.

Best practices are things done - steps taken - actions and plans carried out. For example, encryption is a best practice and not a product or tool. There are many commercially and freely available tools which may prove to be most suited for a best-practice model.

C. Security Procedures

Procedures are specific steps to follow that are based on the computer security policy. Procedures address such topics as retrieving programs from the network, connecting to the site's system from home or while traveling, using encryption, authentication for issuing accounts, configuration, and monitoring.

VI. SECURITY TECHNOLOGY

A variety of technologies have been developed to help organizations secure their systems and information against intruders. These technologies help protect systems and information against attacks, detect unusual or suspicious activities, and respond to events that affect Security.

ISSN: 2348-0351

A. One-Time Passwords

Intruders often install packet sniffers to capture passwords as they traverse networks during remote log in processes. Therefore, all passwords should at least be encrypted as they traverse networks. A better solution is to use one-time passwords because there are times when a password is required to initiate a connection before confidentiality can be protected. There might be initial exchange between the user and server that may be monitored by intruders, it is essential that the passwords arc not reusable.

B. Cryptography

Sometimes it becomes necessary to encrypt the message sent, with the goal of preventing any one who is eavesdropping on the channel from being able to read the contents of the messages. One of the primary reasons that intruders can be successful is that most of the Data they acquire from a system is in a form that they can read and comprehend. One solution to this problem is, through the use of cryptography, to prevent intruders from being able to use the Data that they capture.

Encryption is the process of translating information from its original form (called plain text) into an encoded, incomprehensible form (called cipher text). Decryption refers to the process of taking cipher text and translating it back into plaintext.

C. Firewalls

A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.) Firewalls are typically the first line of defense against intruders; their configuration must be carefully implemented and tested before connections are established between internal networks and the Internet.

D. Analysis tools

There is strong need for analysis tool because of the increasing sophistication of intruder methods and the vulnerabilities present in commonly used applications, it is essential to assess periodically network susceptibility to compromise. Critics argue that such tools, especially those freely available to the Internet community, pose a threat if acquired and misused by intruders.

F. Monitoring tools

Continuous monitoring of network activity is required if a site is to maintain confidence in the security of its network and data resources. Network monitors may be installed at strategic locations to collect and examine Data continuously that may indicate suspicious activity. It is possible to have automatic notifications alert system administrators when the monitor detects anomalous readings, such as a burst of activity that may indicate a denial-of-service attempt.

VII. CONCLUSION

It is evident from above discussion that Data security in an essential part of any e-governance initiative. In Indian e-governance scenario, however, the security aspects are not being taken as seriously. In large number of cases it is not difficult to see that the decision-makers in the government prefer to compromise when it comes to high-end technology adoption, implementation and maintenance. Data security is critical in e-governance initiatives. Confidentiality of any transaction or Data available on the network is crucial. The government document and other important material have to be protected from unauthorized users in case of e-governance projects. Hence security is critical for successful implementation of such projects. E-governance coupled with security systems providing adequate protection is the requirement of any system design effort to beat the inertia.

REFERENCES

[1]E-government in India: Opportunities and challenges, JOAAG, Vol. 3. No. 2, 2008.

[2]Shailendra Singh, Sanjay Silakari. A Survey of Cyber Attack Detection Systems, International Journal of Computer Science and Network Security, ISSN-1738-7906, Vol.9 No.5, pp1-10 May 2009.

ISSN: 2348-0351

[3]International Conference on Computer Science and Information Technology (ICCSIT'2011) Pattaya Dec. 2011
[4]Shailendra, Sing; Singh Karaulia (2011). "E-Governance: Information Security Issues". International Conference on Computer Science and Information Technology (ICCSIT'2011). http://psrcentre.org/images/extraimages/1211468.pdf
[5]ISO/IEC 2700:2009 (2009). Information technology — Security techniques — Information security management systems — Overview and vocabulary.