E-GOVERNMENT: BENEFITS, RISKS AND A PROPOSAL TO ASSESSMENT INCLUDING CLOUD COMPUTING AND CRITICAL INFRASTRUCTURE

Mónica Marlene Baquerizo Anastacio[1], José Antonio Rubio Blanco[1], Luis Javier García Villalba[1], Ali Al-Dahoud[2]

Group of Analysis, Security and Systems (GASS)
Department of Software Engineering and Artificial Intelligence (DISIA)
School of Computer Science, Office 431, Universidad Complutense de Madrid (UCM)
Calle Profesor José García Santesmases s/n, Ciudad Universitaria, 28040 Madrid, Spain
Email: mbaqueri @estumail.ucm.es, {joseantonio.rubio, javiergv}@fdi.ucm.es

[2] Al-Zaytoonah University of Jordan, Amman, Jordan
E-mail: aldahoud@zuj.edu.jo

Abstract

The new information technologies facilitate the transformation of traditional administrative processes to services that can be performed online. The government as part of its technological innovation has also joined the network of Internet services, resulting in what is now known as e-government. Due to the type of information that is managed, computer security is a crucial aspect in these systems. This paper indicates the current status of e-government systems, the internet security vulnerabilities, the benefits and risks to which it is exposed and the identification of the bases to have an e-government security management. For this we propose an assessment model to identify security vulnerabilities in a system.

Keywords - Cloud Computing, Critical Infrastructure, e-Government, e-Government Security Management, Framework Security, Risk Assessment, Vulnerability.

1 INTRODUCTION

Currently, governments have changed the process to provide a service to the citizens that required a government service, by evolving attention from person-to-person to on-line services nowadays [1]. This technological progress involves benefits for both the user and the Government. On the one hand, the user is benefited by saving time and money, and the Government by giving an efficient service demonstrates competence, transparency and technological innovation.

It is remarkable the fact that If a user has a good experience using an e-government, he will probably have a predisposition to use a system of electronic democracy. Electronic democracy is the use of the TIC in order to improve policy and citizen participation in public decision making.

The introduction of new government applications will have to be implemented gradually to get the user to trust them. However, how safe could the system be where the user interacts? Which kind of guarantees for private/classified data are there in order to not expose it to others and ensure its confidentiality? Undoubtedly, security is a crucial factor when it has an online e-government system, and the government has to ensure data security that is exposed on the web because of the sensitivity of these.

In previous studies, it has been possible to identify four direct actors with e-government systems [2]:

- Government agencies to government agencies.
- Government agencies to and from citizens.
- Government agencies to and business organizations.
- Government agencies to and from international organizations and other countries.

As can be seen, government interacts with all entities of society, regardless of race, education, social status, abilities, gender, etc., and it has public, private and classified information of each one of them. Due to e-government system handles data that are essential to society; this can be considered a critical infrastructure, currently an area of special interest and great activity to achieve meet very demanding stringent security measures.

Another current issue is the use of cloud computing. Cloud computing could be defined as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [3].

The use of the cloud has some benefits such as reduced costs in infrastructure and personnel, saving time in configurations, installations; different types of services ready to be hired, among others. Running applications into third party infrastructure, security is a factor to be implemented by the cloud provider. When the provider handles sensitive data, it must to analyze the risks of provider manages private or classified information of an entire country. This topic will be covered in the e-government risk section.

This paper exposed why an e-government is a critical infrastructure and the Internet Security Vulnerabilities to systems that are currently exposed. Besides, it exposes the benefits and risks of e-government including risk analysis to be incorporated in a cloud computing. Finally, it is proposed a framework security and Risk Analysis Methodology.

2 CRITICAL INFRASTRUCTURES

Critical infrastructures have always existed, but over time the ways of attack have evolved in line with existing resources. Two thousand years ago, the way to attack a critical infrastructure was using armies on foot or horseback. Fifty years ago, attackers used armies, tanks, ships, aircraft, or with the resources they had at that time [4]. Currently, the attacks have changed to more sophisticated ways, using technology for these purposes. Just as we can have all the benefits that TICs brings, we must consider that it can also be used for malicious purposes by terrorists. The use of information technology, communications, telecommunications or related to create panic among the people called cyber terrorism or cyber-attack. These could be personal, economic, religious, as well as others.

With regard to cyber terrorism, in 2000 a former employee of an Australian sewage plant was attacked wirelessly. Three years later, the Slammer worm causes shutdown of the nuclear Davis-Besse. In January 2008, the CIA reported that a cyber-attack that caused the loss of electricity in several cities in an unknown location outside the USA. Because cyber-attacks were conducted with more frequency, countries begin with the identification, prioritization and protection of critical infrastructure [4].

Following the attacks of 11M in 2004, in Spain, which was a series of terrorist attacks on four trains in Madrid commuter rail network, which killed 191 people and wounded 1858, the European Commission (EC) wanted to improve safety different types of EU infrastructure as it was considered "critical." The European Council of June 2004 asked the Commission to prepare an overall strategy to protect critical infrastructure against terrorist attacks because they were on the rise [5].

The European Commission defines a ‘Critical Infrastructure’ as —an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of a failure to maintain those functions. In addition —‘European Critical Infrastructure‘, or ECI‘ means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States [6].

The latest cyber-attack to government institutions, published by the National Institute of Communication Technologies of Spain (INTECO) is Virus Rocra. It is a targeted attack campaign that has been going on for at least five years. It has infected hundreds of victims around the world in eight main categories: Government, Diplomatic / embassies, Research institutions, Trade and commerce, Nuclear / energy research, Oil and gas companies, Aerospace, Military. Currently, Kaspersky Lab in collaboration with international organizations, Law Enforcement, Computer Emergency Response Teams (CERTs) and other IT security companies is continuing its investigation of Operation Rocra by providing technical expertise and resources for remediation and mitigation procedures [7] [8].

As seen in these examples, since e-government handles highly sensitive data, of all entities with which it is related, and the violation of their security could generate panic, this is considered a critical infrastructure. A cyber-attack to this infrastructure would have a social, economic and political impact.

3 INTERNET SECURITY VULNERABILITIES

The rapid growth in the volume of information stored electronically and the uptake of e-commerce within government has heightened the need for increased security to protect the privacy of this information and prevent fraudulent activities [2]. A 2005 e-government security study [9] reported that 82% of the e-government sites around the world were vulnerable to common web application attacks such as/cross site scripting and structured query language (SQL injection). In the first half of 2007 The United Stated was the country targeted by most denial of service (Dos) attacks, accounting for 61% of the worldwide total [10] [11].

According to the annual research reports by SANS Institute (2007), the kinds of vulnerabilities being exploited in 2007 were different from the ones being exploited in 2006 [11]. Because the threats change, security must also be renewed, developing and adapting new security measures [11]. According to the website of SNAS, in January 2013, , these twenty Critical Security Controls have already begun to transform security in government agencies and other large enterprises by focusing their spending on the key controls that block known attacks and find the ones that get through [12]:

- Inventory of Authorized and Unauthorized Devices.
- Inventory of Authorized and Unauthorized Software.
- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers.
- Continuous Vulnerability Assessment and Remediation.
- Malware Defenses.
- Application Software Security.
- Wireless Device Control.
- Data Recovery Capability.
- Security Skills Assessment and Appropriate Training to Fill Gaps.
- Secure Configurations for Network Devices such as Firewalls, Routers, and Switches.
- Limitation and Control of Network Ports, Protocols, and Services.
- Controlled Use of Administrative Privileges.
- Boundary Defense.
- Maintenance, Monitoring, and Analysis of Audit Logs.
- Controlled Access Based on the Need to Know.
- Account Monitoring and Control.
- Data Loss Prevention.
- Incident Response and Management.
- Secure Network Engineering.
- Penetration Tests and Red Team Exercises.

These 20 vulnerabilities were agreed by NSA, Cert of USA. JTFGNO, the Department of Energy Nuclear Laboratories, Department of State, DoD Cyber Crime Center plus the top commercial forensics experts and pen testers that serve the banking and critical infrastructure communities [12]. Having identified the internet security vulnerabilities, organizations know where to focus and to take action and prevent attacks.

Management of this data over the Internet, creates a high risk that they can be modified, obtained, or deleted, creating the possibility of a cyber-attack. An example was presented by National Computer Network Emergency Response Technical Team/Coordination Center of China (CERT) in 2007; they had received 26476 network security incident reports. This is three times more than 2005 incidents [2]. A successful cyber-attack to an e-government system could potentially have catastrophic consequences Therefore, e-government should have strong security measures and have been evaluated according to standards of excellence and safety has been shown through assessment.

4 E-GOVERNMENT BENEFITS

If a government has implemented an e-government, the user and the government save time and money, as well as strengthening the degree of reliability of the citizen in government systems. Reports of expanding e-government indicated that US. E-government helped save more than U.S $133 million in software costs in 2007 [13]. European Union (EU) citizens saved seven million hours a year on the time they spent for filing their income taxes, and EU firms saved about €10 per transaction with e-government when doing it online [14]. A study of the e-government impact on competitiveness, growth, and jobs, identified that e-government provided users and government agencies with seven tangible benefits [11] [15]:

- Improved quality of information supply
- Reduced work-process time
- Fewer administrative burdens
- Reduced operational cost
- Improved service level
- Increased work efficiency
- Increased customer satisfaction

The resulting benefits can be less corrupt, increased transparency, greater convenience, revenue growth and/or cost reduction [16] [17]. Because an e-government system works online, it can provide their services in different locations, without the need to move to government offices. This is favorable to the government, giving rise to a "virtual office" to everyone, available 24 hours / 7 days a week. This type of interaction reinforces the public sector and creates a close link between citizens and government.

Providing online services benefits the government and entities with whom it interacts, both saving operational and administrative cost. An e-government has the potential to integrate into a system to citizens, public and private institutions, ONGs, international organizations. This model of interrelationship could interact with other public or private organizations, in order to automate processes, establishing an effective communication and mutual collaboration.

Some of the noteworthy benefits include:

- Transparency in public procurement systems, demonstrating fairness and competitiveness in the process.
- Ease and comfort by to collect taxes.
- Agility and ability to execute transactions, linking information between two or more institutions.
- Coordination of related institutions such as police, hospitals, Red Cross, traffic; legal like justice system, courts, prisons, etc.
- Consolidates governance, strengthens participatory and representative democracy.
- Contributes to facilitate and improve the quality of life of citizens.

As can be seen, an e-government system improves efficiency and service quality; it has a closer communication between citizens and government, transparency and citizen participation [18]. By consolidating governance and strengthening public participation, also benefits systems like e-democracy and e-voting, its main feature is the participation of citizens in government decisions and issues. With advancement of technology, you could also access e-government systems from a mobile environment.

If the government has its systems in a cloud environment, depending on the service contracted, it has a significant cost savings, as the provider offers infrastructure, applications and services which are economical. The government saves on staff and time, as the cloud provider has the settings adjusted according to the government's needs.

Cloud computing has an incredible level of information and processing capacity level of data available -the petabyte scale- allow for entirely new approaches to data analysis [18]. The speed at which cloud computing has permeated Internet activities is increasing exponentially. And all these benefits might enjoy e-government if the system would be in the cloud.

However, these benefits must be taken in consideration for security factors because of these sites could become potential targets for attracting hackers and terrorists, so the government should take safety measures and be alert to a threat.

5 E-GOVERNMENT RISKS

E-government systems could bring benefits to the government, as well it can suffer losses which are not only economic, but of even greater impact. Because this is a system that handles highly sensitive confidential data, national interests could be seriously affected if the system suffers some illegitimate modification or an availability failure. This, at government could bring difficulties such as:

- System penetration.
- Government's reputations.
- Insecurity in government.
- Economic loss.
- Social Panic.
- Fraud, scams citizens.
- Alteration of personal data and confidential.
- Public entities out of service, etc.

As can be seen, the damage is the greatest impact. There are different types of threats that e-government systems are exposed. A research indicated, most cyber intrusions and attacks were [9] [10] [11] [19]:

- Dos attacks.
- Unauthorized Access to network.
- Theft of employee or costumer information.
- Online financial fraud.
- Website defacement.
- Web application attacks.
- System penetration.

These attacks mainly targeted networks TCP/IP (Layer 4), SSl (Layer 5), HTTP and FTP (Layer 7), according tro the Open Systems Interconnection Reference Model [11] [20].

The risk is the possible impact or the result of an event in the assets of an organization, including its consequences [21]. Generally, it is measured in money terms, but in this case, “modification, destruction, theft, or lack of availability of computer assets such as hardware, software, data and services”, would have a significant value. It is for this reason that we must have a managing risk that organizations develop risk management programs in order to identify, mitigate and manage risk to achieve acceptable rewards [21].

Risk management is “the process of understanding, costing, and efficiently managing unexpected levels of variability in the financial outcomes for business”. Risk management is not a defensive activity, but the process of developing a risk-adjusted strategy that balances opportunity with consequences of actions [21] [22].

Risks that may have these systems can be of different nature. If e-government has applications in the cloud, it must have a detailed knowledge of the risks to which it is exposed, according to the service has been contracted: IaaS, PaaS or SaaS. For each case, we should have a response strategy to mitigate the risk.

If the government decides to use the cloud, it has to consider the risk that a third party (supplier) has governmental applications and confidential citizens's data. Due to excess in the international standards for cloud, the European Union is making new guidelines to assure that personal information kept in remote locations is protected [23]. Because the information is handled, the government should check and evaluate the security mechanisms used and the supplier should undergo external audits to ensure full security of the whole system.

6 PROPOSAL

Studies show that a good technology platform and network infrastructure is not guaranteed to have a secure system. It is necessary to have an administrative management to identify, analyze and propose measures to mitigate vulnerabilities. For this, we need to audit the entire system, analyzed from macro issues to the micro.

Studies have shown that there is a link between security issues, e-government and management [24], and technical infrastructure is as important as non-technical when it tries to save an organization's information [25] [26]. The non-technical part is related to security management [24] [27] and should be considered when implementing an e-government system [2].

The system should be evaluated in all its aspects, from its architecture, web application, cloud (if using this type of technology) to know if they meet quality standards, they have defined procedures for any type of event or routine, among others. Assess and know what are the most vulnerable of the system to carry out control, take action and implement. Thus, it will increase the capacity to respond to a cyber-attack that could have the system. This assessment has to be constant, in order to have an overview over the evolution in time of security that the system has had.

At present, some authors have developed frameworks to assess security in e-government systems, under the pillars of integrity, availability, and confidentiality. Within this context, the aim of our research currently under development is to update and improve the existing assessment models up to now, with the following deliverables:

Firstly, a security model assessment for e-government systems based on the existing frameworks. The purpose of the framework is to assess the system safety requirements, which should be implemented. To make the framework, it is necessary to consider the current vulnerabilities, risks and the tools used for security. This assessment model has the following considerations:

- The analysis of an E-government based on cloud computing environment. Cloud computing is a new model for providing services model Internet technologies, either software, hardware or network. This analysis is now considered important and interesting because information technologies are converging to this new business model. Due to the fact that E-government manages high sensitivity data, It must be taken into account the use of the cloud without risking the security of the data or applications that are providing services to the society.
- Identifying technological details regarding to critical infrastructure field. Breaching of these systems could generate panic in the affected sectors, as well as having an economic, political and social impact.

Secondly, a Risk Analysis Methodology for e-government systems, within which are considered own casuistry of these systems. A way to do this, is through analyzing the phrases for the identification and valuation of assets and threats, as well as establishing safeguards and setting priorities on them in order to reduce risks. Additionally, our methodology considers the challenges posed by cloud computing and critical infrastructure, these are very important factors in the future development of e-government infrastructure.

The proposed framework is to identify security mechanisms to strengthen the foundation for security management and reduce those vulnerabilities in e-government. Recall also ISO standards exist, that are intended to provide a methodology for implementing the security of information in an organization [28]. This will also be another area to evaluate by the framework. Also, other authors have identified essential issues that should have e-government systems, which will be added to throughout this study. In the end, it will capture everything that should have an e-government system considered like critical infrastructure, in order to have better security.

Also, it assesses strict standards in place if the institution has a management framework that employees could apply protocols defined in case of system failure, learning from them, etc. As a result of the evaluation, we will know system vulnerabilities, to what extent and areas, allowing making corrections and improving the system. Currently, the first part of the proposal is in development.

7 CONCLUSIONS

Value represents the worth, utility, or importance of an entity. An entity can create value if the difference from others and Government can create value by reducing cost [1]. In fact, e-government is a system that creates value because it innovate ways to interact between different actors.

Nowadays there are ways to encrypt data, ISO standards for improving the quality of systems, networks that prevent the attack or intrusion filtering, but e-government systems should be evaluated. The purpose of this evaluation system is to know how much the system is serving the community and how reliable it is. Also, it respects the privacy protection, if they have multiple authentication methods, if tolerable to cyber-attacks, and if the system could re-connect or recover the service in a short time, etc. The result will be to find out how safe the e-government system is. This way we would know how robust the system is and what aspects strengthen and improve.

At the end of the research, the evaluator framework will consider aspects like critical infrastructure and cloud computing, so trends technology converges to this new business model.

ACKNOWLEDGMENTS

This work was supported by the Agencia Española de Cooperación Internacional para el Desarrollo (AECID, Spain) through Acción Integrada MAEC-AECID MEDITERRÁNEO A1/037528/11 entitled Implementation of a Secure and Accessible E-Government Platform for Rural Areas in Jordan. This work was also supported by the Ecuadorian Government through Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT, http://www.educacionsuperior.gob.ec/).

References

[1] J. Esteves, R. C. Joseph, A Comprehensive Framework for the Assessment of e-Government Projects. *Government Information Quarterly*, Vol. 25, No. 1, pp. 118-132, January 2008.

[2] J.-F. Wang, e-Government Security Management: Key Factors and Countermeasure. *Proceedings of the Fifth International Conference on Information Assurance and Security*, Vol. 2, pp. 483-486, August 2009.

[3] P. Wilson, Positive Perspectives on Cloud Security. *Information Security Technical Report*, Vol. 16, No. 3-4, pp. 97-101, August-November 2011.

[4] A. Villalón, J. M. Holguín, N. Belda, J. Vila, S2 Grupo: Protección de Infraestructuras Críticas, 2011 (in Spanish).

[5] M. Sánchez Gómez-Merelo, Protección de Infraestructuras Críticas: Un Nuevo Reto para la Convergencia de las Seguridades, May 2012 (in Spanish).

[6] COUNCIL DIRECTIVE 2008/114/EC on the Identification and Designation of European Critical Infrastructure and the assessment of the need to improve their protection, Brussels, December 2008.

[7] INTECO: http://www.inteco.es/home/national_communications_technology_institute/INTECO (in Spanish).

[8] Secure List, January 2013: www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies.

[9] V. Moen, A. N. Klingsheim, K. I. Fagerland Simonsen, K. Jorgen Hole, Vulnerabilities in e-Governments. *International Journal of Electronic Security and Digital Forensics*, Vol. 1, No.1, pp. 89-100, 2007.

[10] Symantec, Symantec Internet Security Threat Report. Symantec Enterprise Security, Vol. 12, pp. 01-30, January 2008.

[11] J. J. Zhao, S. Y. Zhao, Opportunities and threats: A security Assessment of State e-Government Websites. *Government Information Quarterly*, Vol. 27, No. 1, pp. 49-56, January 2010.

[12] SANS Institute, Critical-Security-Controls, January 2012.

[13] K. S. Evans, Expanding e-Government: Achieving Results for the American people, July 2008.

[14] European Commission, E-Government Services Yield Real Benefits for EU Citizens and Businesses, October 2005.

[15] F. Chevallerau, The Impact of e-Government on Competitiveness, Growth, and Jobs. The IDABC eGovernment Observatory of European Communities, January 2007.

[16] World Bank. Retrieved March 27 2009, from http://go.worldbank.org/M1JHE0Z280.

[17] S. E. Colesca, Understanding Trust in e-Government. *Inzinerine Ekonomika-Engineering Economics*, Vol. 3, pp. 7-15, 2009.

[18] E. Rodal, Programa para el Establecimiento del Gobierno Electrónico en América Latina y el Caribe, April 2004 (in Spanish).

[19] L. E. Halcnin, Electronic Government: Government Capability and Terrorist Resources. *Government Information Quarterly*, Vol. 21, No. 4, pp. 406-419, 2004.

[20] B. C. McNurlin, R. H. Sprague, Information Systems Management in Practice, 7th ed. Upper N. J. Saddle River, Pearson Prentice Hall, 2006.

[21] S. Pquette, P. T. Jaeger, S. C. Wilson, Identifying the Security Risk Associated with Governmental Use of Cloud Computing, 2010.

[22] M. Crouhy, D. Galai, R. Mark, The essentials of risk management, McGraw-Hill, 2006.

[23] The New York Times, New European Guidelines to Address Cloud Computing, 2007.

[24] M. T. Siponen, H. A Oinas-kukkonen, Review of Information Security Issues and Respective Research Contribution. *SIGMIS Database*, Vol. 38, No. 1, pp. 60-80, February 2007.

[25] G. Dhillon, G. Torkzadeh. Value-Focused Assessment of Information System Security in Organizations. *Information System Journal*, Vol. 16, pp. 293-314, 2006.

[26] S. Alfawaz, L. J. May, K. Mohanak, e-Government Security in Developing Countries: A Managerial Conceptual Framework. *Proceedings of the International Research Society for Public Management Conference*, Queensland University of Technology, Brisbane, March 2008.

[27] F. Hadi, FahadT. Bin Muhaya: Essentials for the e-Government Security. *Proceedings of the International Conference on Information,* pp. 237-240, June 2011.

[28] Information Security & Business Continuity Academy (IS&BCA), March 2013: http://www.iso27001standard.com/es/que-es-la-norma-iso-27001 (in Spanish).