Term paper on cyber security and communications

Law, Security

Introduction

The Internet has greatly transformed our everyday lives and is an integral part of our national security. Nowadays communications systems are the mainstay for much of the national infrastructure. The communications sector creates the foundation for vital informational exchange, including audio, video and data connectivity, but with greater openness, interconnection and dependency comes greater vulnerability. The United States of America, just like any other modern and developed country, is very dependent on information infrastructure. Moreover this relation is constantly strengthening. Computer-based systems frequently face cyber attacks, which vary from pure innocent curiosity to critical intrusions. The consequences of these actions can be disastrous to the overall service of control and communications systems. It is clear that it now represents one of the most serious economic and national security challenges we face as a nation. So with the growing volume and sophistication of cyber attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security.

The Beginning

The Communications Act of 1934 was the initial governmental document that generated interest in cyber security. It stated the need of a national system for the defense and promotion of the communications sector security. Along with the development of electronic data processing machine and realizing the critical vulnerability of the latter, the National Bureau of Standards set the initial foundations for cyber security. They were declared

in the Brooks Act of 1965. The National Bureau of Standards started the development of automatic data processing standards and guidelines for Federal computer systems and what is much more important - for computer security.

The First Decision

President Bill Clinton realized that communications sector was under serious risk, so in 1998 he signed Presidential Decision Directive 63, which stated that in order to « to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services», USA set two-stage national goal — achieve an initial operating capability no later than 2000 and « achieve and maintain the ability to protect the nation's critical infrastructures from intentional acts» no later than 2003. The year of 2001 was a significant year in USA history: the country declared 2 « wars» against traditional terrorism and cyber-terrorism. The latter was represented by the President's Critical Infrastructure Protection Board, chaired by the Special Advisor to the President for Cyberspace Security within the National Security Council. Electronic Government Act followed this effort by the following requirement: every Federal agency was to report the progress in fulfillment of the Federal Information Security Management Act.

National Strategy

President Bush succeeded Clinton’s course, stated in PDD-63. Despite of objectives not been achieved, the interest and focus on cyber issues didn’t wane. The situation happened to be absolutely opposite: cyber security

raised its popularity. In February 2003 George Bush released a National Strategy to Secure Cyberspace, which established three major objectives:

- Prevent cyber assaults;
- Reduce national vulnerability;
- Decrease potential damage and recovery time from cyber attacks, if they do happen,

and in cooperation with private industry set 5 national priorities:

- A National Cyberspace Security Response System;
- A National Cyberspace Security Threat and Vulnerability Reduction Program;
- A National Cyberspace Security Awareness and Training Program;
- Securing Governments' Cyberspace;
- National Security and International Cyberspace Security Cooperation.

Homeland Security Presidential Directive 7 (HSPD-7) set certain responsibilities on the Department of Homeland Security. Now it became in charge of analyzing, warning, vulnerability reduction and aiding national information systems. Also Federal agencies had to " develop plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate». As a result of HSPD-7, the National Cybersecurity Division was founded, which was « to build and maintain an effective national cyberspace response system». The Division fulfills the responsibilities with the help of the the US Computer Emergency Response Team (US-CERT) and Cybersecurity Preparedness and National Cyber Alert System. Nowadays the US-CERT is the war front against the cyber terrorism. In 2008 President Bush continued his course against cyber attacks by signing

HSPD-23, which established a new initiative - Comprehensive National Cybersecurity Initiative. It set new objectives to develop and manage single operation center, which would create a government-wide cyber intelligence plan.

New Leader

The United States of America met a new president in 2009 - Barack Obama. The 44th President made cyber security one of his top priorities. President Obama declared that the “ cyber threat is one of the most serious economic and national security challenges we face as a nation” and that “ America's economic prosperity in the 21st century will depend on cybersecurity.” To implement the results of this review, the President has appointed Howard Schmidt to serve at the U. S. Cyber security Coordinator and created the Cybersecurity Office within the National Security Staff, which works closely with the Federal Chief Information Officer Steven VanRoekel, the Federal Chief Technology Officer Todd Park, and the National Economic Council. Also the President supervised a 60-day comprehensive study and adopted a new definition of cyberspace, set in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), as:
The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

The President’s study features a number of major recommendations for critical actions:

- Appoint an official responsible for coordinating the Nation's cyber security policies and activities.

- Develop a system of national education campaign to promote cyber security.

- Create Government positions for international partnerships in the sphere of cyber security.

The Government of the United States of America completely realizes the importance of cybersecurity programs as all levels of the community. In 2011 the House Speaker John Boehner expressed his deep concerns about cyber attacks on national infrastructure. John Boehner and Majority Leader Eric Cantor formally founded the Cybersecurity Task Force. Republican Mac Thornberry became the chairman of this crucial project, which united members from nine committees with profound awareness on the topic, as well as three at-large members. In autumn of the same 2011 the House Cybersecurity Task Force issued a help guide with an analysis of the country's cybercondition and a set of recommendations on the issue. " These recommendations provide sound, concrete steps to help strengthen our cybersecurity now, while also highlighting issues that need more work," - said Mac Thornberry. This set of recommendations included ideas about encouraging the development of cybersecurity standards, tax credits, insurance and grant funding. The help guide emphasizes that the government should inspire and assist private sector corporations to increase their investments in network safety by the means of expanding tax credits (such as R&D tax credit) and government funds. It also states that 85% of the cyberthreat can be eradicated by a so-called « cybersecurity hygiene». This electronic « hygiene» implies awareness of common users in the questions of self-defense. This massive step is said to be able to significantly

decrease the national cybervulnerability. Additionally the Cybersecurity Task Force published a list of laws that in need of amendments in order to reflect progress in technology sphere. The following list presents just a fraction of the whole program:

- Federal Information System Management Act (FISMA) of 2002;
- Computer Fraud and Abuse Act (CFAA) of 1986;
- Cyber Security Research and Development Act of 2002;
- High Performance Computing Act of 1991;

Recommendations from IBM

In 2012 world-famous IBM released an informational booklet « Best practices for cyber security in the electric power sector». IBM engaged its wide experience with clients and technologies and published a set of practical ways to significantly increase corporate-wide cybersecurity. The booklet includes information about a correct management plan, which helps to set a solid foundation for cybersafety program. IBM suggests creating a fully integrated security system, as well as emphasizes on the fact that the only sensible solution is to build a system on the basis of security, but not vice versa. The security component should be one of the most essential in the process of system creation, right from the very beginning – from the first stages of planning. This method has not only the functional benefits, but financial as well. IBM states « If it costs an extra $60 to build a security feature into an application, it may cost up to 100 times as much— $6, 000— to add it later». This principle represents an extremely useful and significant way of thinking – pragmatism – the one, that get the most of the least.

Additionally IBM gives several practical recommendations:

- Protect your networks: « The more you monitor your networks and the more you know about what has previously occurred to them, the better prepared you are for breaches»;

- Train end-users about phishing: « If your organization knows that it could potentially be targeted, employees are more likely to report something suspicious instead of ignoring it»;

- Search for bad passwords: constantly make efforts « to find and fix bad employee passwords»;

- Integrate security into every project plan: « Security must be applied to new projects from the beginning»;

- Have a solid incident response plan: « managing sophisticated, targeted attacks is an ongoing process that involvesbeing able to respond and investigate, learn and adapt».

Conclusion

In conclusion, through out the whole history of electronic communications and computerized processing, the United States of America made considerable efforts to prevent and minimize the cyber attacks on national infrastructure. When it comes to cyber security, government recognizes that everyone – governments, manufacturers, owners and operators – are in this fight together, with common interests to solve a problem that concerns all. The U. S. Government and Presidents of the United States have always been deeply concerned about the security of the national infrastructure and have been making innovative steps towards the safe cyberspace.

References

Lane, Bill. Tech Topic 20: Cyber Security And Communications. Retrieved February 18, 2014, from http://transition. fcc. gov/pshs/techtopics/techtopics20. html

E-Government Act of 2002. Retrieved February 18, 2014, from http://www. archives. gov/about/laws/egov-act-section-207. html

National Cyber Space. Retrieved February 17, 2014, from http://www. dhs. gov/xlibrary/assets/National_Cyberspace_Strategy. pdf

Rollins, J., Henning A. C.. (2009, March 10). Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations. Retrieved February 19, 2014, from http://www. fas. org/sgp/crs/natsec/R40427. pdf

The White House. (1998). Presidential Decision Directive/NSC-63. Retrieved February 17, 2014, from https://www. fas. org/irp/offdocs/pdd/pdd-63. htm

The White House. Cyber Security. Retrieved from http://www. whitehouse. gov/issues/foreign-policy/cybersecurity

IBM. (2010, August). Best Practices for Cyber Security in the Electric Power Sector. Retrieved February 19, 2014, from http://public. dhe. ibm. com/common/ssi/ecm/en/euw03064usen/EUW03064USEN. PDF

Thornberry, M.. (2011, October 5). Cybersecurity Task Force Releases Recommendations. Retrieved March 28, 2014, from http://thornberry. house. gov/news/documentsingle. aspx? DocumentID= 263044

House Republican Cybersecurity Task Force. (2011, October 5). Recommendations of the House Republican Cybersecurity Task Force.

Retrieved March 28, 2014, from http://thornberry. house.

gov/uploadedfiles/cstf_final_recommendations. pdf