Governmental Institutions Security

Introduction

In our modern fast paced society, technology is the best tool that helps us respond to our duties as fast as possible. However, the fact that technology is used everywhere to such a great extent very often attracts people who want to take advantage of security gaps in our technology. Usually their targets include countries and their governments as well as their institutions. But in what way do these people or organisations or governments take advantage of technological insecurity?

Useful words

Hacker: In the computer security context, a hacker is someone who seeks and exploits weaknesses in a computer system or computer network.
Phishing: is the attempt to acquire sensitive information by masquerading as a trustworthy entity in an electronic communication.
Malware: Short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

Intranet: An intranet is a computer network that is used to share information, operational systems, or computing services within an organization.

Problems

There are many problems regarding security gaps of governmental institutions. For example there have been many cases regarding employees or people involved in a governmental project which has been leaking material. An example of this is WikiLeaks. In addition to that, a major issue as far as governmental security is concerned is of course hacker* attacks. There are many kinds of such attacks such as phishing, web based attacks and also viruses and malware in general

Security suggestions
To prevent hacker attacks governmental institutions are advised spend more money for digital safety. Some examples would include antivirus software, web filters, better encryption of folders, and of course the use of safer passwords. Also it is important that new patches for fixing security gaps are downloaded immediately after the software companies launch them.

As mentioned above a major threat to governmental institutions can be an employee from inside the governmental institution. In this case, a useful suggestion would be to forbid all kinds of removable disks such as usb, sd cards etc, inside the institutions facilities and offices. This is because these kind of disks are ideal for saving information temporarily without anyone knowing and also can contain malicious software and infect computers. In addition to that installing an intranet* inside the institution would be ideal so that leaking information would be eliminated from the inside of the institution.

However the most important thing as far as security is concerned is user awareness. All users must have the appropriate education and critical abilities to recognize all possible -known and unknown- threats they might encounter. This is crucial for the institutions because otherwise the whole security system will collapse. Thats exactly the reason why attacks such as phishing, web based attacks, malicious removable disks and many others are so successful

Useful Links and Sources

http://www.threatmetrix.com/hackers-stealing-u-s-university-education-millions-of-hack-attacks-weekly-against-school-research-programs-threaten-ip-and-free-flow-of-information/

http://www.diariolibre.com/noticias_print.php?id=329879&s=

http://www.newsmax.com/Finance/Kleinfeld/IRS-computer-GAO-information/2014/04/14/id/565382/

http://en.wikipedia.org/wiki/Intranet

Real cases
June 2011: Hackers spied the g-mail-accounts of US-governmental workers to search for some governmental secrets. There were also workers from the white house affected. The same thing was done to chinese people, which are against the regime, journalists, and also governmental workers from South Korea. Google could trace back the attacks to China. They dispute, that the attacks were done by them.

Real cases
April 2015: Hackers from the terror organization IS hacked the French TV-Sender TV 5 Monde, which is owned by the state. With this attack they paralyzed the programs on TV5 and they hacked the social-network-accounts. Experts said tis is a new escalation at the propaganda war of the Jihadists. IS interrupted the tv-shows first, after it they wrote on the homepage ”I am the IS”. They traced back the attack to Algeria and Iraq.

January 2013:
The Hacker Aaron Swartz took his life in New York. He deploys for free information exchange in the internet. He stole millions of scientific articles and published it in the internet. Aaron was arrested a he was supposed to get an imprisonment for a lot of years and a fine up to one million dollars. The punishment was very hard to deter other hackers It was a thing Aaron can’t stand and he wasn’t able to stand this onus. After that Anonymous hacked some governmental pages. They also published some secret information of The US-government.

Summary

As a conclusion, technology is a part of our society and we must secure our institutions from threats that take advantage of it. To do that we must ensure that all vital software for safety is installed and that it is constantly updated. Also denying access of removable disks and installing an intranet inside the facilities are useful advices. But to do all these, first we must secure ourselves and we must receive education and awareness of all the dangers that exist. Of course, we can't have enough knowledge for all the possible dangers out there as there are being created new every day. So that’s why we must be adaptable and have enhanced critical thinking so as to process twice everything we see and read on a computer. The only way to be secure is to be critical about what we see.

Group members

Adam
Anita
Karolina
Odysseas
Simon