Information Security Updates

Social Engineering

Issue 9

I. Background

Industry Story

Ball State students fooled by phishing attempts

The warnings about password protection from University Computing Services are simple and common sense, but somehow we look past them. 108 students' accounts have been compromised in January 2011, representing a spike on the charts that rivals July's chaotic phishing spree.

Hackers are getting better at fooling us. Loren Malm, assistant vice president for Information Technology, said students need to stay accountable. The most recent attacks are coming from websites in the United Arab Emirates and Indonesia, but the hackers might actually be from anywhere and may have just hacked into these vulnerable websites.

The e-mails warn students their webmail account has expired and urge them to follow a link to update and access their account. At second glance, it's easy to see when an e-mail is being sent from an illegitimate source.

See this article:
http://www.bsudailynews.com/news/ball-state-students-foiled-by-phishing-attempts-1.2435626

What is Social Engineering?

Social Engineering is a technique used to trick an individual into giving up sensitive information that can be used in a malicious activity. The social engineer may use e-mails, voice messages, or even in person visits masquerading as a legitimate or trusted source.

The basic goals of social engineering are the same as hacking in general, which is to gain unauthorised access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network. Typical targets include larger entities such as government agencies, research institutes and hospitals.

Examples of security risks of social engineering include:

- Machines falling into control by Hackers
- Theft of credentials leading to financial loss and reputation damage
- Launch of local attacks to the whole network
- Bandwidth and performance downgrade
- Legal liability arisen from the hacking activities

Reference:
http://www.american.edu/oit/security/Social-Engineering.cfm
http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics
http://technet.microsoft.com/en-us/library/cc875841.aspx

Recent Incident

Facebook bug that allows personal data access, phishing repaired

The vulnerability enabled malicious websites to impersonate legitimate websites, and then obtain the same data access permissions on Facebook that those legitimate websites had received. The bug occurred when a user informed Facebook of his or her willingness to share information with popular websites like ESPN.com or YouTube.
(http://www.sify.com/news/facebook-bug-that-allows-personal-data-access-phishing-repaired-news-international-lcgkOcafaif.html)

Related Article

Social Engineering 101 (Q&A)

One of the more interesting events at 2010 Defcon hacker conference in Las Vegas late last month was a social-engineering contest that targeted big companies like Microsoft, Google, and Apple. Participants pretending to be headhunters and survey takers were able to trick employees at the companies into giving out information over the phone that if it landed in the wrong hands could be used to sneak malware onto machines at the company or otherwise get access to the company's data.

(http://news.cnet.com/8301-27080_3-20013901-245.html)

II. Management

Although advanced technologies have been developed to preserve information security, people are usually the weakest link in the security chain. That is why social engineering is still the most effective method getting around security obstacles.

Since the vulnerability is not only related to technology, social engineering is the hardest form of attack to fight against as it cannot be defended with hardware or software alone.

A successful defence depends on having good policies in place to ensure that all employees follow them.

1. Security Policy addressing Social Engineering

The fundamental level of defence is to set up relevant security policy against social engineering attacks. The security policy can help students or staff to defend against the psychological triggers of authority and diffusion of responsibility or moral duty.

The policy should explicitly set out the responsibilities for students or staff to exercise due care in detecting any potential social engineering activities before giving away sensitive information or privileged access.

2. Security Awareness Training for All Users

Once the foundation of a security policy has been established and approved, all staff or students should be trained in security awareness. Security trainings can make a difference in how staff or students apply the security policy in their real life.

The following areas should also be covered in the security awareness training:

- Identification of valuable data or sensitive information related to the universities and their members in accordance with the information classification standard
- Protection of valuable data or sensitive information based on the information handling standard
- Necessary procedures required for detecting suspicious social engineering events
- Escalation procedures of possible social engineering incidents and preservation of relevant evidence

3. Resistance Training for Key Personnel

Apart from the security awareness training delivered to all students and staff, more advanced resistance trainings should be offered to key personnel within the universities. Key personnel are usually responsible for provision of support to others especially the general public and possess most privileged access to universities' information systems.

Related Article

Beware the Spear-Phishers Online

All universities are seeing "Spear Phishing," a term used to designate a fake e-mail which is designed to look like it comes from a trusted authority, models the employee's everyday language and may ask you for your password or other personal information. Once Spear Phishers have a hold on your password, they will usually try to use it on credit card accounts or other financially-related accounts in the hopes that you use one password for multiple purposes.

(http://media.www.ngcsuthesaint.com/media/storage/paper1392/news/2011/01/21/News/Beware.The.SpearPhishers.Online-3969681.shtml)

Related Article

University of Hull – How to avoid being a victim of Social Engineering

Be careful who you release information to. Do not respond to telephone surveys. Verify the identity of callers asking for personal or unusual information. Do not leave your passwords lying around in your office. Do not reveal your userid and password to anyone and do not let anyone use your PC without you being present. If you see someone who is in an area where you would not expect them to be, challenge them and ask to see some ID. If they are unable to show any ID or if you still have concerns ring the University Report Centre.

(http://www2.hull.ac.uk/acs/ict/anti-virus-and-security/social-engineering.aspx)

Reference:
http://www.iwar.org.uk/comsec/resources/security-awareness/social-engineering-generic.pdf
http://www.sans.org/reading_room/whitepapers/engineering/multi-level-defense-social-engineering_920

II. Management (cont'd)

Good resistance training should include the techniques such as Forewarning and Reality check

4. Regular Reminders

After a series of trainings, staff or students should have a basic concept of information security and the risks of social engineering. However, the resistance to social engineering may only be effective for a short period of time.

By using e-mails, newsletters or memorandums, universities need to regularly reminder their staff and students of the possibility of a hacker attempting to steal information from them and specifically informed of any recent attempts.

5. Centralised Security Log

Having a centralised log of security events that is being monitored by information security personnel can help prevent an effective attack. Any time a staff or student is asked to give out information or reset a password or even has a suspicious call, it should be logged in this central log file.

If a hacker is getting information from one staff or student and using it to talk to another staff or student, the patterns could be noticed in the log. As soon as the pattern is noticed, security personnel can take action to stop the attack by warning all staff or students about the attacker.

Staff or students who are trained and know that they must report all security related requests will be less likely to give out confidential information without taking time to think it through first.

6. Incident Response

There should be a well defined incident response process that a staff or student can begin as soon as he or she suspects something is wrong. This process should aggressively go after the hacker and proactively inform other potential victims.

As soon as a social engineering attempt or incident is discovered in any part of a university, the attack should characterised by the incident response procedure. Meanwhile, any relevant staff or students should be alerted so that immediate counter actions can be taken.

It is important to have one person or a department working very closely tracking these incidents so that the attack can be detected quickly and effectively. This should be the same person that is watching the centralised security logs, independent from anyone who is likely to attract suspicious social engineering attempts.

Reference:
http://www.iwar.org.uk/comsec/resources/security-awareness/social-engineering-generic.pdf
http://www.sans.org/reading_room/whitepapers/engineering/multi-level-defense-social-engineering_920

Statistical Report

Indian colleges respond poorly to police's cyber group initiative

Cyber crime has grown at an annual rate of 80 to 90 per cent in recent years as against the 10 to 12 per cent growth of other crimes like murder, dacoity and body offences. The trend can be established from the number of crimes that get reported to the police's cyber cell. Only five cyber crime cases were reported in year 2003 and the number grew steadily to 79 complaints in 2006; 271 cases in 2009 and 390 cases by end of September 2010.
Almost 30 per cent of the 390 cases were related to Nigerian frauds, 25 per cent were credit card frauds, 20 per cent pertained to phishing attacks, 15 per cent related to crimes on social networking sites and 10 per cent were data thefts.

(http://timesofindia.indiatimes.com/city/pune/Colleges-respond-poorly-to-polices-cyber-group-initiative/articleshow/7407617.cms)

Recent Incident

Climate scientists targeted for fraud

Scientists are sent e-mails directing them to fake conference websites - often imitating the style of real ones. Typically they are told their travel costs will be refunded - but they have to pay first "to reserve a hotel room".

The "phishing" scammers appear to be after information such as e-mail addresses, as well as money.

(http://www.bbc.co.uk/news/science-environment-12219472)

III. General Users

Identify Suspicious Conversations

Staff or students must know the general types of information a social engineer can use and what kinds of conversations are suspicious. They should be sceptical of unsolicited phone calls, visits, or e-mail messages from individuals asking about internal information. If an unknown individual claims to be from a legitimate organisation, try to verify his or her identity directly with that organisation.

Protect Confidential Information

Staff or students should know how to identify confidential information and should understand their responsibility to protect it. They need to know how to say “no” when it is necessary and have the backing of their management on the occasion where it might offend.

Use the Internet Safely

Staff or students should not send sensitive information over the Internet before checking a website's security. They should pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g. “.com” vs. “.net”).

Verify legitimate Requests

If any staff or student is unsure whether an e-mail request is legitimate, he or she should try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request. Instead, check previous statements for contact information.

Make Use of Relevant Software or Features

Staff or students should install and maintain anti-virus software, firewalls, and e-mail filters to reduce some of social engineering attempts according to the guidelines in the universities’ security policies. They should also take advantage of any anti-phishing features offered by the e-mail clients and web browsers provided by the universities.

Conclusion

Social engineering is easy to accomplish but difficult to detect. Because it relies on fooling end users into revealing information, the users or the organisation are often reluctant to admit that they have been deceived.

To protect the sensitive or confidential information in the universities, students, staff and the management should not ignore or underestimate the growing security threats arising from social engineering.

Reference:
http://www.sans.org/reading_room/whitepapers/engineering/multi-level-defense-social-engineering_920
http://www.antiphishing.org
http://www.us-cert.gov/cas/tips/ST04-014.html

Related Article

Fake Lottery

Lottery scam is accomplished by sending e-mails or letters notifying potential victims that they have won the lottery in a foreign country. All that is required is a processing fee in order to obtain the huge sum of money that they have won. Victims will often send money to cover the processing fee even though they had never even heard of the lottery before the letter.
One victim of this type of scam was from Mexico, spoke very little English, and fell headfirst into a “Canadian Lottery” scam.

(http://www.social-engineer.org/framework/Real_World_Social_Engineering_Examples:_Crime_Victims#Check_Scams)

Related Article

Social Engineering Using a USB Drive

Hackers can use USB drives to gain access to sensitive information kept on a computer or network. Hackers may infect one or more USB drives with a virus or Trojan, that when run, will provide hackers with access to logins, passwords, and information on the users’ computer or the network the computer is connected to. The hacker may then leave the infected USB unattended on the floor, in or next to a cluster machine, in hallways, restrooms or any areas with a relatively high volume of traffic. A user who finds a USB drive will often install the device on their computer or on a cluster machine to search for identifiable information that can be used to locate the owner of the USB device.

(http://www.cmu.edu/iso/aware/be-aware/usb.html)