How phishing attacks have compromised major systems? essay sample

Literature, Russian Literature

Major corporations, governments, and other organizations are hacked each week, mostly by means of phishing attacks. Describe how users and IT organizations should arm themselves against these attacks. In a typical phishing attack, the attacker puts up a Web site that looks nearly identical to the victim’s Web site. Technology changes fast, our genetic code and learned behaviors not so. As security professionals, we must concentrate not on technical measures, but on education, education, education. Phishers often set up the fake sites several days before sending out phishing e-mails. One way to stop them from swindling customers is to find and shut down these phishing sites before phishers launch their e-mail campaigns.

Companies can outsource the search to a fraud alert service. These services use technologies that scour the Web looking for unauthorized uses of your logo or newly registered domains that contain your company’s name, either of which might be an indication of an impending phishing attack. This will give your company time to counteract the strike Phishing attacks bring with them other risks and costs as well; including the direct IT costs to locate the source of data loss. Organizations should establish a cross-functional anti-phishing team and develop a response plan so that they’re ready to deal with any attack. Ideally, the team should include representatives from IT, internal audit, communications, PR, marketing, the Web group, customer service and legal services. Baker, Emiley; Wade Baker, John Tedesco (2007). “ Organizations Respond to Phishing: Exploring the Public Relations Tackle Box”. Communication Research Reports

Although paypal says that it is safe. But people has started to do phishing attack. Once I was selling off my laptop on Ebay. I started to receive emails from paypal. Even From paypal email address that money has been transferred to my account. But when I checked nothing was there. I called paypal and inquired so they told me there is no communication from our side. And to inform those emails looked genuine. “ You may receive a fake email that claims to be from PayPal. Sending fake emails is called “ phishing” because the sender is “ fishing” for your personal information. The email may ask you to:

Employee training is the most vital tool for guard against phishing. This is why in a company or government sector and especially in a financial organization IT’s have many site blocked. If a user clicks on the wrong web page or ente their personal info in a masked or fraudulent web page they are letting hackers into breaching their system and allowing hackers to also getting access to their credit cards etc...

Another way is that encryption method are there for such purpose where the end user need keys to access a system or see a system.

Organizations and the government can establish security firewalls and also have administrators monitor their network 24/7 for phishing attacks. Now with the newer technology routers and firewalls can be programmed for intruder aler alerts and prevent hackers from breaching security. Normally stacked firewalls are in place for a better security if one firewall does not catch the hacker since the data traffic speed is so fast the other fire wall will

catch the hacker from intruding in the system. I would like to add, companies must enforce Ethical Usage of Technology in the workplace, such as but not limited to:

1.) Screen email software for staff employees, or totally do not grant the staff employee to use email outbound. The reason behind this is, some employees are not mature enough to practice caution, more so email etiquettes, when communicating with outsiders. The email of the company, represents the company itself, and might jeopardize the company's image if inappropriate information are communicated outside.

2.) Do not allow access of personal emails in the office.

3.) Identify websites Black List. We did this in my previous company. I had a Product Manager, who I was told was watching online movies during lunch break, so I asked the IT department to track his online behavior and block the websites, because my staff was able to alter the firewall. We all know that online access of movies might potentially carry a virus, and it clogs the system such that other employees who need to use the internet for business purposes might be hindered from doing so. One increasingly popular tactic is a form of spoofing called phishing. Phishing involves setting up fake Web sites or sending e-mail or text messages that look like those of legitimate businesses to ask users for confidential personal data.

The message instructs recipients to update or confirm records by providing social security numbers, bank and credit card information, and other confidential data either by responding to the e-mail message, by entering

the information at a bogus Web site, or by calling a telephone number. EBay, PayPal, Amazon. com, Walmart, and a variety of banks, are among the top spoofed companies. New phishing techniques called evil twins and pharming are harder to detect. Evil twins are wireless networks that pretend to offer trustworthy Wi-Fi connections to the Internet, such as those in airport lounges, hotels, or coffee shops.

The bogus network looks identical to a legitimate public network. Fraudsters try to capture passwords or credit card numbers of unwitting users who log on to the network. Users and IT organizations should arm themselves against these attacks by being mindful that confidential information such as SSN are normally not asked. Look at the URL if the page leads you to a page that is not of a company you transact with. Most financial institutions, i. e. Chase detects the computer you access online banking and if the cookies are not embedded, Chase will prompt you with an option to send you a code via text, call in a phone registered with Chase or via email registered with Chase. And if you are successful in entering the right code, you will be able to access your account in online banking.

(Management Information Systems, 12/e for DeVry University, 12th Edition. Pearson Learning Solutions p. 301). This is a caution to individuals and companies, more importantly to individuals. Here are some steps to avoid phising attacks:

1. Keep anti virus up to date – if you get a MAC, you don’t need an anti virus

2. Don’t click on hyperlinks on emails – this is very tricky especially if we don’t know the sender, or if we know the sender, but his/her email is compromised sending email links which your friend did not even create.

3. Take advantage of anti-spam software – companies usually purchase this but for personal emails like for yahoo, hotmail, gmail, it is common that they are targets of spam attacks

4. Verify https (SSL) – or Secure Socket Layer ensures encrypted transactions between the web servers and browsers. Companies engaged in ecommerce have this. They have the Verisign seal

5. Use anti-spyware software

6. Get educated – the internet has a lot of information on how to detect phising attacks, so it pays to know and remember those. For instance, when you are using a oublic computer or public wifi, do not perform any banking transaction or purchase anything.

7. Firewall

8. Don’t enter sensitive financial information such as your credit card numbers, birthday, full name, mother’s maiden name, and the 3 digit security code at the back of the card.

9. Protect against DNS pharming attacks – this directs your DNS server to a website like ebay or paypal and you think this is legit, but it is not.

10. Finally, get a MAC, an apple macbook pro is not infiltrated with virus, it does not open a website if it is compromised, or does not open an attachment, it just goes blank which means it is compromised.

Reference:

Retrieved on April 17, 2013 from http://www. techrepublic. com/article/12-steps-to-avoid-phishing-scams/5818568

Facebook, linkedin, twitter and other social media

What are the social and security issues for individuals and organizations relative to personal and business use of social media? The lack of physical contact makes it easier to build false profiles too, for example you think you are chatting with a handsome young man from somewhere while you're actually chatting with a completely different kind of person from a completely different place. This made a issue and recently a girl did suicide when she discovered that the person she is chatting with is not a young person, but a old women from her neighborhood. Some of the dangers of Social Networking in Business & Education Includes: Time wasting, Irrelevance, Cheating, Age/ appropriate content, Scams/ Phishing/ Security issues (viruses etc) – much easier than you think on Facebook & Twitter links! Privacy, Negative comments/ Reputation tarnished/ Rumors, Identity theft/ Burglary, and Lost Job/ Opportunity.

LinkedIn's problem isn't as much technology as the common practice of sharing of names, titles, and organizations. It can be very easy to get an organizational chart to be used for an attack. Ranging from information

harvesting to sophisticated things, social networks pose a real yet elusive security threat. There is a vast amount of sensitive personal information available on social networks, and the lack of proper security levels at the user level make these sprawling applications an ideal sandbox for attackers. As shown by the Facebook account hijacking incident, attack can bring real financial damages. Other damages are also possible, only to go up in severity.

Arrington, M. (2008). Phishing For Facebook. Retrieved from http://www. techcrunch. com/2008/01/02/phishing-for-facebook/

Stutzman, F. (2006). An Evaulation of Identity-Sharing Behavior in Social Network Communities. Cave drawings were likely the earliest form of social networking. Today people tweet their thoughts for the world to see. In between we’ ve had instant messaging, MySpace, Facebook, and blogs. Thenext several big things are already being hatched by some students at Stanford or MIT. Online social networking is here to stay – the only change will be in what form it takes. According to a recent survey conducted by Deloitte, 22% of employees say that they use some form of social networking five or more times per week, and 15% of employees admit they access social networking while at work for personal reasons.

Yet, only 22% of companies have a formal policy that guides employees in how they can use social networking at work. Before we can figure out what to do about these exploding media at work, we first need to know exactly what we are dealing with. So, for the uninitiated, the following is a short

lesson on the various types of social networking that are likely being accessed from your workplace right now.

http://www. nyiia. org/events/Social_Media_Whitepaper_(K0272931). PDF Social engineering attacks are personal. Hackers understand that employees are often the weakest link in a security system—they are susceptible to trickery, and their varied responses can give attackers many opportunities for success. “ LinkedIn’s problem isn’t as much technology as the common practice of sharing of names, titles, and organizations. It can be very easy to get an organizational chart to be used for an attack.

Once an attacker finds out the names of who works with whom, for instance, she/he could send a carefully crafted email via LinkedIn to the victim’s human resources department head, posing as a headhunter recommending a candidate for an open position. But his email could carry a malicious Word file, rather than a resume. When opened, the file could gain ownership of the victim PC and steal other company information. Basically, information about how people are connected, the work they do and their positions are all precious information for a potential attacker. “

Reference:

http://www. informit. com/blogs/blog. aspx? uk= Security-Issues-of-Social-Network-

Sites what are some of the security threats in social media outlets? “ Lack of a business policy or lack of enforcement of the policy. As always, the first

line of security should ensure that employees have limits on what can be accessed on company networks and that action is taken when the rules are broken. Friending someone you don’t know. A few weeks ago, I received a request from a stranger who wrote that, because we had a similar interest, we should be friends. I hit the ignore button, which was a good thing. It was part of a phishing scheme. Others did hit the friend button and have had computer issues as a result.

Not thinking twice about clicking on links. One of the great things about a site like Twitter is the sharing of information you might not see elsewhere. The downside is the tiny URLs that hide the true link to Web sites. If you aren’t sure, ask. Letting hijackers into accounts. hackers are finding holesin the software and are taking over individual accounts to spread malware from “ trusted” sources and scam consumers into sending personal information. Third-party application dangers. Hackers are able to retrieve passwords and other personal information through Facebook games. Fake facebook toolbars are taking users to a spoofed site that steals passwords.” http://www. enterprisenetworkingplanet. com/netsecur/five-social-media-security-issues