The Weakest Link in Your Network
Randall Miller
Abstract

In this paper I will show how users are the weakest link in the security of company networks. I will examine some of the poor practices that are employed by users and how they make the network vulnerable to attacks. Some of these practices will include password management, Bring Your Own Device (BYOD), authorized access, social engineering vulnerabilities, etc. This paper will also provide some details on the specific attacks and methods used by hackers to gain access. Real world examples and case studies will be presented in order to demonstrate the seriousness of this issue. I will also include some suggestions and recommendations as to what companies can do to mitigate these attacks. Since the weakest link is indeed the human aspect, most of the mitigation will involve what can be done to improve user behavior such as user awareness training and the implementation of policies and procedures.
The Weakest Link in Your Network

There are a tremendous amount of online accounts that users access on a daily basis. Some of these accounts include social sites such as Facebook, Twitter, Google+, Pinterest, etc. There are literally hundreds of social networking sites and the majority of people are members of multiple sites. There are also other online accounts that are more sensitive in nature such as online banking, credit cards, online retail stores, and email. Finally, there are accounts that are provided to users in order for them to access the network at their place of employment. The majority of these work-related accounts typically just require a small string of text and numbers to be entered in order to grant access to the network. In essence, all that stands between a hacker and the sensitive, confidential information on your network are these few little characters we call a password. Most users do not realize the seriousness of protecting their online account information until it becomes compromised. This also applies to the workplace where users continually demonstrate poor practices in regards to information security. But in this case, a compromise affects a lot more than them personally. In the following paragraphs I will discuss the many different ways in which users are the weakest link in the security of your network. I will also offer some recommendations on preventive actions that can be taken to minimize the risks that these threats pose.

One of the biggest issues faced by users is managing all of the passwords used by all of these accounts. One technique users typically employ is to utilize the same password for multiple accounts. A study was completed by Experian, the credit-checking firm, and they found that the average user has 26 online accounts for which they only had five unique passwords. This same study also found that 25-34 year-olds have no fewer than 40 online accounts. (Tagat 2012). The management technique of using the same password for multiple accounts poses a serious security
risk to them and their corporate network. It is highly probably that users do not view the corporate network credentials any differently than the rest of their online accounts and will use the same password for network access that they have used on one of their less secure personal sites. If a single one of these sites become compromised then every other account that uses that password is at risk. Recently, Adobe accounts were hacked, and as of this writing, 150 million accounts and passwords were stolen. Hackers are very familiar with the poor practices of users and will likely try accessing banking sites, online retail stores, and corporate networks with the credentials that were stolen. It is inevitable that they will garner some success by using this tactic. If they are able to access a corporate account with these credentials and the account belongs to an employee with administrative privileges, serious damage could be inflicted upon the company.

Mat Honan (2012) is a senior writer for Wired and fell victim to an attack that destroyed his “entire digital life in the span of an hour.” His Apple, Twitter, and Gmail accounts were all linked together and once hackers gained access to one, they had them all. They were only interested in his gaining access to his three letter Twitter handle, but used his Apple account to remotely wipe his iPhone, iPad, and MacBook in order to delay him getting it back. Mat ended up losing a tremendous amount of data in addition to the time that was lost in the recovery process. This attack was a little more targeted than the average user will face, but it shows how daisy-chaining accounts can exacerbate the damage of a breach. It is easy to say that the solution is to use a unique password for every account, but this is more difficult in practice. An alternative solution would be to use password management software such as LastPass, Password Genie, Roboform, and KeePass. These management solutions only require users to remember one complex password while they maintain the credentials for all their accounts. Some may have
concerns about placing all of their “eggs in one basket” but these companies are the most reputable and seem to utilize good encryption. Either way, users are would be safer than continuing their existing password management.

Rather than relying on users to practice good password management, corporations also have the option of implementing an alternative method of authentication to the network. One of the more popular options available is biometrics. Biometric authentication is accomplished by identifying a unique, physical characteristic of the user, such as a fingerprint or scan of their retina. Fingerprint scanners are becoming more readily available and are now even appearing as a security feature in Apple’s latest update to their iOS 7 platform for their iPhone line. Other devices are likely to soon follow suit. Biometric authentication is most often accompanied by a smart card, PIN, or password. Using multiple methods in tandem is referred to as multi-factor authentication. Implementing multi-factor authentication adds an additional layer of security to the network. These additional layers can add quite a bit of expense if they are implemented at each workstation on the network. Biometric authentication is not without its faults and time must be taken to develop an acceptable level of threshold – the amount of variation between a scan taken during enrollment into the system and later successive scans. If the threshold is set too small, there is a risk of a false negative – a legitimate user is denied access. If the threshold is set too large, there is a risk of a false positive – an unauthorized user is allowed access due to the level of similarity between their scan and an authorized user. Biddle, Chiasson, & Oorschot (2012) state: “Biometric recognition provides more reliable authentication than passwords and identity documents, and is the only way to detect duplicate identities.” They go on to say that even though biometric systems are not foolproof, those in the research community have
continued to make strides to identify vulnerabilities as well as develop the relevant countermeasures.

Another area in which users are the weakest link in the corporate network is in their vulnerability to social engineering. Social engineering can be defined as “the art of gaining access to buildings, systems or data by exploiting human psychology, rather than by breaking in or using technical hacking techniques” (Goodchild 2012). An article in the Information Resources Management Journal states that “there are various technical and non-technical means that SE attackers can employ, such as pretexting, phishing, online social engineering, shoulder surfing, and dumpster diving, in order to collect data which can be processed for the attackers to access privileged information” (Luo, Brody, Seazzu, Burd, 2011). All of these tactics can be very effective against the untrained and unprepared user. If the one performing the social engineering is skilled enough, they can even fool the most vigilant user. Chris Hadnagy (2011) is the cofounder of social-engineering.org and in his book, Social Engineering: The Art of Human Hacking, he provides an account of his experience in social engineering a CEO who had informed Hadnagy that “hacking him would be next to impossible” because he “guarded his secrets with his life.” Hadnagy gathered information about the CEO from various sources with most of the details obtained from Facebook. He then calls the CEO posing as a fundraiser from a charity that is dear to the CEO and asks if he can send him a PDF with more information. After enthusiastically agreeing, the CEO received the PDF and upon opening it, he was infected by a script that executed and gave Hadnagy the ability to access the machine remotely. The CEO felt that the attack was unfair, but malicious hackers will mercilessly use any bit of information they can gather to take advantage of users and further their agenda.
Phishing has become one of the more prevalent social-engineering tools employed by hackers. Phishing is primarily conducted via email in which an attacker sends an email message to someone so that it appears to be from a legitimate person or organization. The message will typically encourage the user to either open an attachment or follow a hyperlink that is embedded into the email. The previous story of the CEO and the PDF attachment is a perfect example of phishing. This is a tremendous security concern in the workplace. Many times backdoors and key loggers can be installed once the attachment is opened giving the attacker full access to the network. Muniandy & Muniandy (2013) state that “there are three primary techniques of phishing: URL manipulation. Web site forgery, and phone phishing.” URL manipulation refers to an attacker sending an email message with HTML code that proceeds to open a forged Web site. Attackers spend a lot of time crafting their Web site to look exactly like the legitimate site they are imitating. Many of these phishing emails are made to appear as if they are from banking institutions. The intent is that the user will click on one of the links in the message which takes them to the forged banking site. The attacker hopes that the user will input the credentials for their online banking account. Once this takes place, the attacker has captured these credentials so they can either log in and steal the user’s money or they will sell the credentials to some other entity who has malicious intent.

The best defense against phishing is user education. Though phishing emails have become more convincing, there are always some telltale signs that show that the email is not legitimate. Many of these phishing emails originate from a foreign country. As a result, sometimes there will be noticeable grammar and spelling errors. It is not likely that any reputable organization would send a legitimate email with these types of errors. Secondly, phishing emails are rarely personalized to the recipient. One should be weary when the email begins with “Dear
User” or “Dear Customer.” This is typically a sign that the email was sent out in bulk. A legitimate email would likely address the recipient personally. Finally, users should be aware that if they are on a site that requires the entry of sensitive information, they should ensure that the Web site address begins with https rather than http. Following these tips will protect the user’s data as well as the corporate network.

Social engineering is successful mainly due to the fact that attackers manipulate and prey upon the feelings of their victims. The typical employee tends to respond to an attacker due to sympathy, guilt, fear, indifference, or just because they want to be courteous and helpful. All of these reasons are also why social engineering is so difficult to defend against. Tandage (2005) describes Kevin Mitnick as “perhaps the most notorious hacker of recent years [and he] relied heavily on human vulnerabilities to get into the computer systems of American government agencies and technology companies.” Mitnick was eventually incarcerated for his actions and after spending five years in jail, he became an author and security consultant. After his release he testified in front of a Senate panel on government computer security. During this testimony, Mitnick explained that: “When I would try to get into these systems, the first line of attack would be what I call a social engineering attack, which really means trying to manipulate somebody over the phone through deception. I was so successful in that line of attack that I rarely had to go towards a technical attack. The human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure access devices, and it is money wasted, because none of these measures address the weakest link in the security chain.”

Users need to be aware of the various techniques employed by hackers so they can more easily recognize when they or their workplace is being targeted. Luo et al. (2012) maintains that
“a multi-dimensional approach including technology, policies, procedures, standards, employee training and awareness programs, and incident response should be employed to more effectively and efficiently cope with the ever-present threat to the IS security management.” Though all of the defense tactics mentioned are important, incident response is one of the most important. Being a victim of a social engineering attack is not a matter of “if” it will happen, but “when.” Many users will likely know when they have been compromised shortly after it happens. A lot of them will not disclose this fact due to fear, embarrassment, or ignorance. The moments following an attack are the most critical and a fast response can limit the scale and severity of a breach. If an incident response plan is in place, the user will know exactly what to do and who to contact so the incident can be addressed in a timely manner.

If there is an area that could be more dangerous than attacks coming directly from the Internet or email, it would likely be from a phenomenon known as BYOD (Bring Your Own Device). Smaller, portable electronics are taking the world by storm. Foster (2013) states that “for the fourth consecutive year in 2012, consumers purchased fewer PCs than the year before, yet they own more computing devices than ever before.” Users are bringing their personal laptops, tablets, and smartphones into the office. The same USA Today article states that BYOD has become BYOI – Bring Your Own Infection” (Foster 2013). Organizations have no control over what employees do with their personal devices. This becomes a potential problem when the employee connects their personal device to the corporate network. The device could be infected with some type of virus that could potentially spread across the network with devastating effects. Data security also becomes an issue with BYOD. The majority of corporate-owned devices require some type of authentication measures in order to gain access to the locally stored data. If an employee moves data onto their device, the corporation is not able to verify that the employee
protects the data through a PIN or other type of credentials. Foster (2013) spoke with a bank who estimated that 10% of their malware infections came in the front door on personal devices.

One of the largest incidents involving BYOD occurred in 2009 through what is known as the Stuxnet worm. Stuxnet was a specially designed worm virus that sought out particular programmable logic controllers (PLCs) on a computer that was vulnerable. Once its source was located, the virus would establish control over the equipment. It is believed that equipment at an Iranian nuclear plant was the official destination sought by the worm. Farwell & Rohozinski (2011) state: “Those that Stuxnet targeted were ‘airgapped’; in other words, they were not connected to the public Internet and penetration required the use of intermediary devices such as USB sticks to gain access and establish control.” They go on to mention that over 60,000 computers were infected by this worm with more than half occurring in Iran. Stuxnet eventually connected with its target and caused significant damage to Iran’s nuclear plant. It appears that an employee had been bringing their work home and transporting the data on a USB drive. The employee’s home computer eventually became infected and jumped to the USB drive. Once the drive was connected back to their work computer, the virus propagated through the local network until it found its intended destination and as a result set back Iran’s nuclear program by at least two years. This demonstrates how BYOD can be devastating in the corporate environment even when they think they are safe from attacks originating from the Internet.

Preventing threats from BYOD can be very difficult to implement. It is not feasible to develop policies based upon the platform of the device. There are so many different platforms and versions currently out there and the list continues to grow every day. IT staff would not be able to keep up with the influx. Another option is to prohibit employees from connecting their personal devices to the network. However, this would not be good for morale and could also end
up being counterproductive. Foster (2013) describes how traffic patterns generated by malware differ from those that are generated by humans on the network. He states that “we can use what we know about the network and behaviors in the network to identify malware, regardless of the device it was brought in on.” This can be accomplished by implementing a firewall. An article on Cisco’s Web site defines a firewall as “a security appliance that attaches to your network and acts as the protective shield between the outside world and your wired and/or wireless network” (“As Strong as the Weakest Link”). The firewall monitors all traffic coming into the network and if any appears to be questionable, it will be blocked. Workers are then free to use whatever device they are the most comfortable with, improving morale and productivity.

In conclusion, it is quite easy to see how users have become the weakest link in your network. Users continue to employ bad habits in regards to their password management and many are unaware of the numerous threats to the security of the network. There are many other threats that businesses face on a daily basis as a result of poor practices by users and only a few were presented here. This does not mean that nothing can be done to mitigate the risk. I have presented some suggestions and recommendations on how to prevent and manage each of these risks. Most of the mitigation involves additional efforts from the corporation as it is ultimately their responsibility to protect their network. It was mentioned earlier how companies could spend millions of dollars on network security but they would still be vulnerable if they do not address the behavior and threat knowledge of their employees. Though not a guarantee, user awareness training is a necessity if you ever hope for your network to be secure. At the very best, users will always be the weakest link in your network regardless of what measures are implemented. The aspiration of all companies should be to focus on making that link a little stronger.
References


Muniandy, L., & Muniandy, B. (2013). Phishing: Educating the Internet users - a practical
