PROXIOS

When the Target of the Attack is You, Not Your Network

A Look at the Dangers of Social Engineering

Overview

Computer networks have been at risk from hackers and other criminals almost as long as they have been in existence. Media reports of cyber-attacks, identity theft and data breaches have become commonplace. To combat these dangers, organizations are constantly implementing new, stronger methods of threat detection and prevention.

As companies get better at protecting themselves against these attacks, the criminals behind them have had to find new ways to infiltrate networks. Where they once used to exploit weaknesses in servers or firewalls, they now have a new target – you.

What is Social Engineering?

The threat of hackers has long been a problem for companies and there are a number of protections that can be put in place to protect networks from their insidious attacks. But what happens when the attack is directed at the individual user, and not the network? That is the danger of social engineering. Social engineering can be defined as a method that criminals use to gain access to a computer through the user. This is generally done by either installing spyware or other malicious software or by convincing the user to divulge confidential information such as passwords, financial data or other personal data.

The main type of social engineering that hackers use to gain user information is commonly known as phishing. Phishing is the act of obtaining and using an individual's confidential information by fraudulently posing as a trusted source. This can be done through several methods, including emails that are disguised as being from a trusted source. The message asks users to open an attachment that contains malware. When they click on the link software is installed, often without their knowledge, which then collects personal information. Another growing method is targeting mobile devices with SMS text messages. In September 2014 an estimated 46% of all bad text messages were phishing scams, an increase of 15% over the previous month. This surpassed both spam and other types of fraud. Phishing can also be done by offline methods such as a phone call where criminals try to get people to divulge confidential information by posing as someone else, such as a representative of their credit card company. This information is then used to get into otherwise secure systems.

Many times, email phishing is used to deliver ransomware, also known as data kidnapping. This is a specific type of malicious software, with perhaps the most famous one known as CryptoLocker. With ransomware, users will receive an email that appears to be safe. The email prompts them to click on a link which then installs software on their computer that encrypts the local drive, rendering it unusable. Users then have to pay a ransom, usually through either a prepaid voucher or BitCoins, to get their files unlocked. This method is growing in use with recorded instances more than doubling from 2012 to 2013. When CryptoLocker was first identified in September 2013, it was estimated to have infected over 500,000 victims. While the perpetrators of CryptoLocker have been stopped through the efforts of law enforcement and IT security companies, it was quickly replaced by CryptoWall, which infected over 625,000 systems and 5 billion files between March and August 2014. These included mapped network shares such as those hosted by cloud providers Dropbox and Google Drive. Even more troubling for companies, in 2014 a new version of this software appeared that specifically targeted network attached storage.

Proxios

Proxios, a pioneer in cloud computing technology since 1999, offers businesses a full range of IT services on a subscription basis including application hosting and VOIP phone systems. Proxios hosts proprietary and third party software, delivering your desktop to your office, home or mobile device. Proxios is headquartered in Richmond, Virginia serving customers across the United States and Canada.

Why has Social Engineering Become a Problem?

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are an integral part of network security solutions and they are very effective at protecting systems. Combined with effective end point protection solutions, it is becoming more difficult for criminals to penetrate systems. This is why they have turned to social engineering. Enterprise security systems have become so secure that it is simply easier to target the human users than it is the network.

Large scale attacks, such as mass emails with fraudulent links that install spyware, have historically been the most common type of threats. However, between the popularity of social and professional media sites and the increase in companies posting employee information online, it has become relatively simple for criminals to obtain at least contact information on most individuals. Once they have that information, it is simple to send out targeted attacks by posing as a trusted source. It is imperative that both companies and individuals take steps to protect themselves from this growing danger.

Protecting Yourself

Proxios has a number of methods to protect companies and individuals from the growing danger of social engineering. Its advanced firewalls and IDS/IPS systems prevent millions of attacks every year, many of them social engineering threats. Users that do receive suspicious emails can immediately contact Proxios, who will help them determine if an email is safe or not.

Direct calls from criminals masquerading as a colleague are harder to protect against. A common impersonation is for the hacker to pretend to be from the corporate IT department and then get people to install software or even hand over control of their system. To combat this type of attack Proxios has put a call back system in place. With this system, anyone who is contacted by a questionable person is free to end that call. They can then directly contact that person using a known good number to verify that the call was legitimate.

Social engineering is growing in use because it has become easier and more effective to attack individuals than highly secure corporate networks. Against this type of threat, a combination of advanced security solutions, such as that provided by Proxios, and a comprehensive educational program to inform individuals of the threat is the best defense.