Unit VII Assignment I: Knowing Your Threats

By Nathan Windisch

MI: Informational Security

Informational Security

Informational Security is highly important as it allows for data owned by both businesses and private individuals to be protected. Keeping an IT system secure is one of the most important system traits as without it then the system can be accessed by outside intruders and your data can be stolen. If informational security is not in place then your personal data is also at risk, possibly resulting in identity theft and fraud caused on your personal or business information.

Threat I: External Malware Attacks

External Malware attacks are very dangerous and can cause lots of damage of let into our system, via FTP, SSH or even email. As we are an Internet Service Provider, or ISP it would be a massive breach of both trust from our users and a catastrophic failure of our previously effective security if malware were to get sent into the system as many people who use our systems could be infected, resulting in mass loss of data and a subsequent loss of profits due to customers cancelling their contracts with us as there has been a data breach, resulting in a loss of trust. A way to keep your systems and data secure would be to prevent access to protcols such as FTP, SSH and email, unless it has been authorised by a senior member of the IT team here at UTCISP.

Threat II: Phishing

Phishing is a major issue to our company as an Internet Service Provider as it can give scammers a way to gain access to data owned by either a business or a private person or people who use our systems. Phishing can be very effective towards individuals who trust official looking documents, even if they are not legitimate. Individuals that are included in this list are old people, who are not computer literate, and people with bad eyesight as they may not notice certain details about an email which may prove it's invalidity. This practice can be detrimental to our industry as if a phishing email is sent from an official email, many customers may be affected by it, leading to a loss in both the amount of trust given to us by our users and the profits that we gain from their subscriptions to our services. A way to keep your systems and data secure would be to send all email traffic that isn't sent by an authorised address to a spam folder for security. A downside to this is that some legitimate emails may be caught in the filter.

Threat III: DoS/DDoS

With a DoS attack, or Denial of Service attack, the resultant attack is hard to block without disabling access to legitimate outside users. DDoS attacks can result in downtime, meaning that our users may stop using our services, resulting in a loss of monitary income. A way to keep your systems and data secure is to have it all backed up onto an external site to prevent the data from being

inaccessible. The data could also be sent to multiple servers to prevent any other DDoS attacks hitting the offsite servers.

Threat IV: BotNets

A BotNet allows hackers to gain access to all computers on our network, meaning that they can use the computer as a ‘slave’, using it to do things using their internet connection to perform things like DDoS attacks, as aforementioned, or using their processing power to perform things such as brute-forcing or bitcoin mining. BotNets will mean that our users lose trust in our services and move over to another ISP, resulting in a mass loss of profits. A way to keep your system and data secure would be to use a similar idea from some of the issues listed previously, such as filtering email sent from unknown sources and storing all your data on an offsite backup facility, such a services including Google Drive, Dropbox and Microsoft OneDrive.