Marshall Eddy

CS331-001

Vincent Skimmer

8 August 2016

Current Technologies and Processes

There are always new processes and technologies coming out to try and better secure the infrastructure of different companies, such as anti-virus software, firewalls, and web filters. There are many different ways to secure information within in a company, but here we will discuss the ways a company can secure information without training their employees to know what not to do since that could potentially a long and expensive process.

One technology that has recently come out is multi-step account verification, such as Google Authenticator. What this application does is is will allow users to essentially have a second password that they do not even know. Using a third party, one can setup their account to require a username, password, and code randomly generated from that user’s device every time they need to login. This just further secures each user’s account, making it more difficult for hackers to infiltrate a company’s infrastructure. Thus making the only way for someone to login to your account would be if they new your username and password, as well as had access to whichever device you may use to receive a code for your account, which is extremely unlikely since you would not even know what that code will be until you get it and it will never be the same making any sort of keystroke RAT useless.

In addition to making accounts more secure with multi-step authentication, companies generally have rules on passwords. These are to help prevent accounts being hacked. Currently, the standard for companies is to make all passwords at least 8 characters and have lowercase, uppercase, numbers and potentially a special character. From a recent security report from USESI, the way their passwords are setup is different for each level of authentication of the account. For User-Level Passwords, they do the standard 8 characters and 3 out of 4 of the following: uppercase, lowercase, numbers, and special character. In addition to this, the password is not allowed to be any of the 5 previous passwords, must be changed every 90 days, and cannot be changed within 2 days of being set. Then the rules get a little stricter for System-Level Passwords: increasing the password length to 10 character, and contains all four of the different types of characters, and the password should be changed every 60 days. The last increase in password construction security is for Domain Administrator Passwords. The length increases to 15 characters.

They also have failed password attempt lockout policies, which range from 5, 4, and 3 failed attempts within 30 minutes, resulting in the account being locked for 60 minutes. If this occurs for a Domain Administrator Account, then they account is locked until another domain administrator resets the account.

Some other processes USESI uses to help keep their information secure is by enforcing these guidelines: Password-protected screensavers or lock screens must automatically activate at 15 minutes or less of inactivity on all devices, Portable devices that have access to the company’s information must have a PIN or other security features, and they encourage users to log off if they plan on being away from the computer for an extended period of time. They also have e-mail guidelines and rules. All incoming and outgoing e-mails are to be monitored for confidential information and malicious e-mails by first traversing through messaging gateways to ensure security of the company’s information being sent, and to prevent hackers from accessing information via malicious e-mails.

A great way for a company to prevent a lot of data leaks is through a firewall with a web filter, which will not allow users to access websites that are known for having malicious links and pop-ups on the website. This can be easily accomplished through use of white-lists and black-lists. Most companies are using black-lists, but recently companies are realized that it is much easier to use a white-list and only unblock certain websites, and if one is blocked, then the user can request a website to be unblocked. White-lists make it easier for IT departments to manage which websites can be accessed on the server as well as better coverage from malicious software from all other websites, since only a few websites can even be accessed in the first place.

A Simple way for a company to help prevent and monitor viruses, as well as clean them up, is through a virus protection software like McAffe. These anti-virus applications, “capture and monitor events, files, host flows, process objects, context, and system state changes that may be indicators of attack (IoAs) or attack components lying dormant, and send intelligence to analytics, operations, and forensic teams” (McAffe).

All in all, these are just a few ways companies use different processes and technology to help prevent any sort of data leak and to protect their overall infrastructure. There are so many different ways to prevent data leaks and they can be extremely simple and easy to implement, yet effective, or extremely complicated and difficult to implement, yet not very effective, or visa versa. These are just a few of the more common ways companies use technology to help with their information security.