Cybersecurity Current Events Assignment:

2016 Election

In the 2016 Presidential Campaign momentous event that occurred several incidents targeting political organization and particular people in the United States. One of the main targets were hacking (DNC) Democratic National Committee and Hilary Clinton presidential Campaign. The Hackers pursued multiple tactics such as email phishing, malware infections and network intrusions. They used phishing techniques to acquire personal login information to gain access into the government system. A lot of scandals was known because of the information that pulled from Government official’s personal emails. The emails were generated into media and the public gained knowledge of this and this impacted the 2016 election dramatically with pertaining to Hilary Clinton’s scandal. To get a handle the U.S intelligence agency stepped in and started investigating in the attacks as well as looking into the congressional committee to see if this was an inside job. After thoroughly investigating the U.S Intelligence Agency in 2018, the U.S. Department of Justice indicted 12 Russian military intelligence officers for their involvement in the hacking. The U.S. intelligence agency resulted the incident as the Russian military intelligence agency known as GRU, conducted the series of cyberattacks on the USA. With the attacks happening was defiantly a rude awakening the world on how it is important to secure your information. In 2019 the Senate Intelligence they deepened the investigation and found out that there were do a deal with Trump to help him with winning the election 2016. The Senate also felt the need to keep an eye on Russia to see if they would try to the same tactics for the 2020 election that was about to occur. Officials are more than aware and conducting action to further this from happening in the future. They have started training and showing different ways of how they can be caught back into to hacking situation.

Ukraine Ransomware

In 2017 Ukraine developed a software for tax filing MEDoc as the source of infections on companies in 64 countries including banks in Ukraine, Russian oil giant Rosneft, British advertising company WPP and US law firm DLA Piper. As Jane Wakefield has stated in her report. The global cyber-attack has sent shock through all company’s worldwide and everything start pointing towards the MEDoc software. The developer denied all claims and accusations of the corruption the numbers are increasing including malware expert, Marcus Hutchins gave evidence that the software was infecting people still. They called it the Ransomware attack. Ransomware attack exposed the vulnerable angles where the software update showed that the pre consequential motivated the attacks. The attack’s method of spreading the decryption stemmed from the email attachment being able to get into the networks and connect to their servers. It was known widely when there was an attack on NSA (National Security Agency) the decryption leaked information online. With NSA trying to hide this information that they have been attacked they kept it away from Microsoft and others leaving them open to be exposed to the hackers. They demanded a ransom payment for the information that they were blackmailing NSA with. On Wired.com they have found ways to recover from a Ransomware attack and it hasn’t been fully resolved. They are still conducting research and they have stopped the use of MeDoc servers to be discontinued with. They have yet to stop them from coming through different sources with the same decryption and ransom. No one can pinpoint where the source came from in Forbes article called “Is this Ukrainian Company the Source of the ‘NotPetya’ Ransomware Explosion?”; Thomas Brewster states that it believed the Ukrainian Company was just a vessel/pawn to be used such as. In this case the evidence points to the Ukrainian company they attacked themselves to seem like a victim. Government Officials did arrest a Ukrainian national name Yaroslav Vasinskyi with being involved in the cyber-attacks.