Prompt 1: 2016 Election

Let’s begin with the unlikely “coincidences” that people from different departments failed to stop or warn about the attack. One being the FBI communication to the IT department, you’re telling me the FBI can tell that one of the computers was vulnerable but couldn’t located that exact computer for the IT department? Two, the IT department not shutting down their hardware to try and solve that issue or even properly communicate about the issue to the DNC. Three, the technician who conveniently made a typo to the politician about the email being tampered/illegitimate. Having a breach in government systems and leaving it alone from September 2015 all the way until March 2016 seems a bit odd to me, one would think it was a setup or ploy. I digress. The type of cybersecurity attack was a phishing attack. This is when someone sets up an email that copies the look of a legitimate email and baits the victim into clicking a link in order to then retrieve personal data. The vulnerability was discovered when the FBI knew one of the computers were compromised. When John Podesta fell for the hacker’s bait that is when the hackers were able to really take over. They then created more bait that would give them access to at least 30 DNC computers/emails. The security measures that could have been taken would have been to shut down the computers until the IT department found out what compromised the original computer. The lack of communication and action from the FBI and the IT department is appalling. It could have been avoided if the three “coincidences” above did not happen at all or there was different action taken. Bottom line is, the measures that should have been taken were not, the people in the DNC were too gullible and should’ve had better communication with each other, and the timing on how fast actions were taken were too slow.

Prompt 2: Ukraine Ransomware

Well, here we go again with another hack that may possibly revolve around politics. This time we have a malware attack that may have started from a company called MEDoc. It is believed that the cyberattack mostly wanted to infiltrate Ukraine’s systems. That is what one is to assume when the cyberattack targeted Ukraine 80% and the second most targeted country was Germany at 9%. The vulnerability was that the systems were set up to automatically download updates. However, the hackers made it so that the updates were not actually updates but rather malware and viruses that would install on the system. This type of virus or hacker attack made it possible to infect a large amount of computers. The hackers took that vulnerability and delayed work for many companies, forcing them to stop daily business. The hackers also held the data hostage so to speak. Something similar happened at my job, a hacker got into the system and locked out the company then demanded some sort of payment for the access back in. The hackers saw that vulnerability as a way to make money and maybe hurt Ukraine’s intel.The security measures that should have been in place would be to not have the updates update automatically. As well as that I would also say that there should have been more obstacles in the way protecting the updates if they wanted to run it automatically. It is a bit hard to give more measures due to the fact that updates being automatic doesn’t give the people affected much time if any to realize they are being hacked. Most of the time they may not even notice and update on their computer especially if it updates in the background. Maybe they could have had a system in place where one computer will get an update and if it runs smoothly after the update is installed then it could pass a command onto the rest of the computers to download that update.