Samuel Oates

Information Assurance Final Project

CS-465

4/22/2020

Investigation into the Breach of the Democratic National Convention: CIAO Report

Approximately in March 2016, Cyber units of the Russians federations main intelligence directorates of the general staff (GRU) hacked into the Democratic National Committee (DNC) and gained sensitive intellectual property that was then sold and released. As Chief Information Assurance Officer (CIAO) of the DNC, me and my team will be investigating the event and issuing a report to senior leadership on the implications of this cyber event.

This report specifically, will address a background on the DNC's mission, including types of organizational intellectual properties and any strategic alliances, a summary of the 2016 cyber breach, apparent consequences of that breach, and proposed policies and procedures that will reduce the likelihood of it happening again. Central to this investigation will be the Report on the Investigation into Russian Interference in the 2016 Presidential Election, herein referenced as "The Mueller Report" (Mueller, 2019), which details the hack by GRU and gives specific details on their actions. This will serve as a starting point for our team and will direct us on what are the appropriate risk management techniques we should include going forward.

1. **Background on the DNC**

The main goal of the DNC is to elect leaders who fight for equality, justice, and opportunity for all. Our overall agenda is placing our candidates in the best position for success in all races, including the state house and senate, the US House and Senate, and especially the White House (What We Do, 2020). The DNC is a presidential committee and as such, focuses

primarily on the race for president. Part of that focus includes raising money for the presidential race every four years, overseeing the primary/caucus process (including setting rules and debates), as well as organizing and paying for the Democratic National Convention. The DNC also pays for advertisements and on-the-ground organization for the Democratic presidential nominee after the convention ends (Jarman). We are keenly focused and more committed than ever to ensuring a fair and inclusive primary and election, as evidenced by our voter protection and civic engagement activities (What We Do, 2020).

With the DNC's focus centered in one massive endeavor, electing a Democratic president, we maintain a number of strategic alliances in order to further our mission of electing democratic leaders everywhere. In addition to each state Democratic Party and the College Democrats of America, the DNC maintains strategic partnerships with several national organizations including the Democratic Congressional Campaign Committee (DCCC), the Democratic Senatorial Campaign Committee (DSCC), the Democratic Governors Association (DGA), and the Democratic Legislative Campaign Committee (DLCC) (Jarmon).

The DCCC has jurisdiction over House races. It is not controlled by the DNC, but works in close conjunction. The DCCC raises its own funds and spends it only on House races. It is funded by outside donors and its' own Democratic House members. The DSCC is controlled by Democratic leadership in the Senate and is the Senate counterpart to the DCCC. It is also funded by the senators themselves and outside donors, with a goal of winning as much senate races for democrats as possible. The DGA is an organization concerned with electing Democratic governors and allocates electoral resources toward gubernatorial races that are very competitive. The DLCC funds and organizes around the thousands of legislative races around the country yearly (Jarmon).

Each of these organization share the DNC's mission to elect leaders who fight for equality, justice and opportunity for all. As you will see in the next section, the strategic alliance with the DCCC is what contributed to and exaggerated the 2016 breach in to the DNC.

With the DNC's mission as described above comes the generation and protection of sensitive intellectual property. Intellectual property is defined as … The DNC contains intellectual property that comes in the form of internal strategy documents, fund raising data, opposition research and voter data, among others. This is information that is central to our operation and the assurance of this information the main focus of the Chief Information Assurance Officer (CIAO) department. All of the sensitive data was put in jeopardy during the 2016 data breach by the GRU. A summary of the event is detailed in the next section.

2. Summary of Events

The Mueller report is one of many details which pieces together how the Russians hacked the DNC. It is mapped out in details how the Russians planned on meddling in the 2016 election by a social media campaign and hacking and releasing private information. As a cybersecurity professional, it is overwhelming just how much access they gain into our infrastructure.

When we look at the social media method the Russians were able to gain access to various entities within the DNC such as IRA which was a perfect platform to create propaganda and stir up trouble in the political realm and increase social discord in the United States. In February 2016, documents had already shown an order to support Donald Trump and Bernie Sanders while creating an opportunity to attack Hillary and the rest of the candidates.

The IRA posed as Americans purposely hiding their true identify in the shadows. While in the shadows the Russians would ask the Trump campaign for buttons, flyer, and poster for their rallies. Mueller included in his report that the IRA spent over $100,000 for over 3,500 Facebook

advertisements which included anti-Clinton and pro-Trump ads. Mueller was also aware that the Russian military intelligence agency (GRU) had access to into email accounts owned by volunteers and employees of the Clinton campaign.

The report goes into some much depth that they even identify the type of malware that was used to infiltrate into the DNC networks. The GRU would lease off site servers and executed malware called X-Tunnel to send large scales of data to the servers. Keylogger transactions amongst DNC staff was collected and stored among the data was passwords, internal communications between employees, banking information, and sensitive personal information.

The GRU stole information from the DNC network immediately after gaining access. On April 22, 2016 GRU officers downloaded rar.exe on the DCCC's document server. The next day the GRU searched one compromised computer for files containing that of Hillary, DNC, Cruz, and Trump. On April 25, 2016, the FRU collected and compressed PDF and Microsoft documents from folders on the DCCC's shared file server that pertained to the 2016 election. Overall, the GRU exfiltrated over 70 gigabytes of data from this file server. (Mueller, 2019)

The GRU had plans to release all the information stole by April 19, 2016, when Unit 26165 registered the domain dcleaks.com through a service that anonymized the registrant. All these transactions were paid by a pool of bitcoin which was mined by them. GRU posted stolen documents onto the website dcleaks.com on June 2016, including documents stolen from associates of the Clinton campaign. No person in Hillary's campaign was spared from the reckless activities of the Russians. (Mueller, 2019)

Furthermore, the documents and emails who communicated with the Russians was connected to the Republican party. The United States Republican Parties portfolio contained roughly 300

emails from a variety of GOP members shared the same GRU officers who operated a Facebook page under DCLeaks moniker, which was the most used to promote materials.

3. Consequence

Even though a lot of damage impacted the DNC, the event has opened up an opportunity to innovate and create better policies to further our mission. As we approach another election the DNC is taking necessary steps to dramatically reduce the risk of hackers breaching candidates' devices.

A lot of victims to this hack of the election were greatly affected and we only know minimal about what happened to the staff of Hillary Clinton. We are aware that a lot transpired throughout the entire process to acquire information. It is hard to fathom the amount of privacy that has been violated all because of politics and the opposition willing to go to the depth of hell to have an advantage.

The compromise has sent waves throughout our organizations informing us on exactly how vulnerable are system actually was so it will be a tough pill to swallow but this is the time to act now and create an environment where we hold everyone accountable for our data and create a new norm starting with this organization.

4. Prevention

The DNC is known world-wide as a party that elects leaders who fight for equality, justice and opportunity for everyone. When we look at how our government is run, we see two parties who represent people's values. As we look at the approach of each party, we see war within our government to strategically attempt to have major rule of the House of Representatives and the Senate. Prior to the 2016 election, the republicans had been contentiously dealing with the

democratic president Barrack Obama for the past eight years. The potential runner up for the seat, Hillary Clinton, was the favorite to take over the reigns after Obama. Since the republicans were in an uphill battle against Hillary, it would appear they had to pull all the stops. Never would anyone ever believe it would come to potentially coordinating with the Russians to hack into the opposition's infrastructure and attempt, successfully, to steal the election.

The DNC throughout this ordeal still continues to be positive, even with the ever-growing evidence of a stolen election, and remains optimistic about their goals to help the people. Our organization is a resilient bunch that will never give up the cause. Prior to the hack, the DNC worked endlessly to fix any issue that may have arose from this inconvenient ordeal. The entire situation was traumatic but has improved our organizations infrastructure. As early as 2017, our organization has been working diligently to bring in top tech talent to secure our data. The rebuilding of our brand is imperative moving forward into the future. Because of these actions, we are rapidly improving our data warehouses so that not only is our organization and staff protected but our voter data as well.

When policies are defined we look at them as a high-level statement portraying a common goal amongst the organization. The creation of information assurance policies may be driven by the need to comply with laws and regulations or simply reflect executive management's analysis of the organization's information assurance requirements. There can actually be a level of policies with each lower layer providing increasing degrees of details, but still recognizable as policies by their focus on "know what" content rather than "know how." Our organization will plan on developing procedures and standards that elaborate exactly what needs to be done. As we look at policies we have to view them as information assets that safeguard information showing roles and responsibilities specifying the establishment and performance of

information assurance related task or processes. These policies must dictate the establishments ability to conduct risk assessments and be able to change management processes.

As we create policies, we must create a framework to based our information on so we would implement a Risk management framework (RMF) most commonly associated with NIST SP 800-37 guide for “Applying the Risk Management Framework to Federal Information Systems. Its required that all federal agencies must follow this process to secure, authorize, and manage IT systems. We can briefly define the process cycle that is used initially for securing and protecting systems through Authorization to Operate (ATO) all integrating ongoing risk management.

The six-step process step one categorizes information systems which is administrative and involves gaining an understanding of the organization. The system boundaries should be defined based on information types associated with the system that can be identified. Information about an organization and its mission should have its roles and responsibilities as well as the systems operating environment intended use and connections with other systems may affect the final security impact level determined for the information system. (NIST Special Publications 800-30, 800-39, 800-59)

Step 2, selecting the security controls are the management operational and technical safety nets which employ organizations within the information systems that protect confidentiality, integrity and availability of the system and its information. (CIA Triad) Assurance accelerates confidence that the security controls are implemented within the systems are effective in their applications. (NIST Special Publications 800-30, 800-53, 800-53A)

Step 3, when implementing security controls requires an organization to create security controls and figure out how the controls are employed within the information system and its

environment of operation. Policies should be customized to each device and configured with the required instructions. (FIPS Publication 200; NIST Special Publications 800-30, 800-53, 800-53A)

Step 4, assessing the security controls will require using the necessary assessment procedures to figure out the extent which controls are launched correctly making sure they are operating as they were intended to do. (NIST Special Publication 800-53A, 800-30, 800-70)

Step 5, the authorization of information systems operations is created on the idea of risk operations and individuals, assets, other organizations and the nation resulting from the operation of the information system and decide if the risk is acceptable. This will furthermore create a platform that will allow tracking and status of any failed controls. (NIST Special Publications 800-30, 800-39)

Step 6, dealing with monitor security controls entails continuous monitoring programs allow an organization to maintain the security authorization of an information infrastructure. Over time implementing a high dynamic operating environment where systems adapt to changing threats, vulnerabilities, technologies, and business processes. Risk management can become a real-time through the use of automated tools. These tools will help with configuration drift and other potential security incident associated with unexpected change on different core components and their configurations as well as provide ATO standard reporting. (NIST Special Publications 800-30, 800-39, 800-53A, 800-53, 800-137)

Throughout the Mueller report, we were highly alarmed by how many malicious software tools were used to do this job. The credential harvesting tool used with the keylogger was very tricky and sneaky and because we never had any alarms they were freely able to have their way with our network. A harden system would have picked up on traffic going outbound and trigger

an alarm prompting for an investigation alongside the automation tools would provide us with packets showing us how much data is being pulled and where it is being pulled from to the exact location.

Overall, the Risk Management Framework places standards across government by aligning controls and language and improving performance. Using these tools will help create a faster response and allow our infrastructure to adapt to future issues that may arise over time. The federal agency cybersecurity will be more involved in every day actions for better around the clock monitoring and effective reporting.

The roll out of tools to effectively monitor our infrastructure should inform us whenever there is suspicious activity going on by sending alerts to our staff whenever an offense occurs. The tools we use will all be wrapped into one big package in the cloud which will provide tons of functionality. The cloud is the wave of the future allowing us to innovate and give us opportunity to build upon a solid foundation. The cloud functionality will create security incident events which come with LogRhythm's along with packet captures. Furthermore, screen captures will give our teams visuals without visiting any questionable sites. Also tied into the cloud we will have other investigative software giving them investigation more functionality. Included with these tools, we will have access to ESA/WSA's watching the traffic that goes inbound and outbound from our email servers. When something suspicious comes through our email servers will can investigate every single content within the packet.

5. Conclusion

The overall situation of the 2016 election hack is very alarming and disgusting to read. Even though as acting CIAO, I am to help implement various policies to secure our infrastructure. We cannot advance our agenda without further involving congress to pass more

strict laws when dealing with private data. Our infrastructure has proven to be very expansive for the reason that the actors were not only able to access our network but multiple networks in correlations to us. This project is very expansive and will require and bridge program not only to the DNC but to other networks so that we are properly segmented appropriately. There have been other hacks in federal domains where they gain access to the entire network accessing one part of the system. Safe practices will be implemented from the top to the bottom. As stated before, the details so far have been very alarming but it is necessary to create positive change and to make sure this does not happen again on our watch. I believe adopting a cloud-based infrastructure will help us out. Being able to work side by side with complex automated tools will give us the advantage against the opposition.

The vast majority of our issues was that the Russians were not only able to penetrate our network but do it by knocking our door down without being alarmed and taking everything, we had compromising not only the candidate and ruining her campaign but the people working for her. This epic failure is unacceptable and our actions should reflect our mission of greatness and that we care about our people. We must act and recruit talent and have a network so secure that it will rival anybody. If we set the tone for a harden system then other entities will flow us. Which leads to our main mission to lead and promote a culture of success for the future.

Works Cited

Mueller, Robert S. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. Mar. 2019, www.justice.gov/storage/report.pdf.

What We Do. 2020, democrats.org/who-we-are/?utm_source=gs_medium=ads&gclid=EAIaIQobChMIvYWEycP66AIVyuDICh1JYQ2cEAAYASABEgLuwfD_BwE.

Jarman, D. DNC, DCCC, DSCC: *How to Decipher the Alphabet Soup of Democratic Party Organizations. Democratic National Committee*. 21 Apr. 2020, www.dailykos.com/stories/2017/4/17/1653154/-DNC-DCCC-DSCC-How-to-decipher-the-alphabet-soup-of-Democratic-Party-organizations.