**Executive Summary and Plan**

**By**

**Taylor Norman**

On May 25th our team was notified that there had been many complaints from our customers attempting to use our online banking portal, starting around 10 am. Originally it had appeared to be due to the attack of a group of hacktivists, using a skull and crossbone as well as a message claiming they have hacked the network. Unfortunately, this was not the case, and instead after pulling data from logs on the firewall and web server there appeared to be hundreds of pings from a single IP address. This IP address has been known to be a launch point of cyber-attacks and other criminal activity in the past. After recovery of the system from the planted fake hacktivist group, it was found that email messaging servers had connected with the IP address multiple times over the past few days, indicating emails were potentially being send/received. After log reviews it appeared to be a spear phishing attempt on the company employees that sent out over 100 emails containing a malicious link disguised as an email from close relative or friend which many would assume is safe.

Upon investigation and some interviews with staff it was uncovered that the “Super Funny” labeled email had a malicious link which installed a tool to allow a hacker remote access to the targets system. By using this remote access, the attacker was then able to send messages along the chain of command eventually allowing for the release of funds for an urgent matter. Unfortunately, the standard process of signing off a transfer of funds had been skipped due to the CFO being on a vacation and unable to sign off on the money in person.

Due to the ability of the hacker to trick our employees into falling for a phishing attack we have potentially lost a substantial amount of money which may be untraceable. Below in the paper I have identified methods which we can do to improve out network security as well as strengthen our ability to detect intrusions on the network immediately, ultimately reducing the risk of pings to the network, or other network access from going unnoticed. I also recommended the need of future security awareness training to all employees at all levels, this will ensure that all employees will understand the risks associated with using the internet and how to avoid suspicious activities which may cause harm to either themselves of the company.

Among some of the recommendations I have listed are Intrusion Detection software, Custom Firewall rules, recording and analyzing logs of firewalls/web and email servers, virus protection tools, and a complete guide to follow in the event of a breach in the network. By incorporating each of these tools into the network our security team will be able to recognize a threat quickly, allowing for them to ultimately shut it down before any harm come of it, as well as the guide to follow which will allow them to follow standard procedures and best practices to prepare for an incident and how to react when an incident does occur. By being prepared the company will know what information to gather, and how to go about preparing for a potential lawsuit to prosecute the hackers or anyone responsible.

Many laws are in affect that protect user personal private information and health information, including laws like HIPAA. Many of these laws in place require that a company follows best practices in terms of security, as well as reducing information a company can gather about a user. It is the company’s responsibility to protect any data they gather on a person, including names, age, any personal identifiers, and more. Having intrusion detection in place will provide a way to spot any unwanted access into the network potentially before they are able to cause any damage. It is also important that all workers know the dangers of phishing and social engineering because they are the weakest link in a workplace in many situations. This means that all employees should be trained, reducing the risks of falling for phishing attempts and leaking potential private data, or network access. It is important that during the time of an attack we gather as much data as possible, which can later be used to learn from past mistakes as well as report information to the legal team to allow them to handle the case in court if need be.

Because of the sensitive data required for banking operations it is important that all saved data is locked behind a secure storage device/server and is encrypted so that only those who are meant to have access, can access the information. Although in the case of the leak, the remote access was set up on a local employee workstation, which means that if any access to personal files were allowed by that employee then they could have risked losing the information. Because of this it is important to have the intrusion detection and virus scanners to quickly act by suspending a user account thus reducing the amount of damage stolen credentials can do.

Implementing new ideas can always help with network security, but a company must have clear change guide policies in place to ensure that all steps are followed when adding or subtracting any applications, tools, firewalls. This will help with tracking what steps have been taken and ensure no new vulnerabilities arise during major network or security changes. This is key in best practices to ensure that by removing one vulnerability you are not adding more in its place.

|  |  |  |
| --- | --- | --- |
| Identify individual steps and list them in logical sequence below: | Identify the role and who performs it below, ensuring it corresponds to the step in the first column in the table: | Identify your rationale behind the assignment, ensuring you address implementation concerns related to the step and the role/responsibility in the first two columns in the table: |
| Detection | | |
| Step: | Role/Responsibility | Rationale Behind Assignment |
| Incident classification | Information Security | Once an incident is detected the IS team should quickly identify what is happening or has happened to allow them to understand the level of severity. |
| Assign Severity | Information Security | Assigning a level of severity is important to ensure the correct response is taken to resolve the incident. The severity can be categorized into 5 levels from Extreme to insignificant. As well as knowing which business processes, and assets were affected. |
| Assess the Situation | IT Auditor, HR | The IT Auditor can help to understand the cause of the incident, comply with procedures, and work with other team members to plan the appropriate response to the situation. |
| Establish Course of Action | Senior Management | The CIO and other Senior management should have already planned for an Incident and created a policy and documentation to follow in the situation of a breach. In this case there was no Security plan so they Senior Management must be quick to act and set a course of action that includes steps towards Isolating, containing, eradicating and recovering a system as well as steps to take to report the incident and learn from the mistakes in the future. |
| Response | | |
| Step: | Role/Responsibility | Rationale Behind Assignment |
| Isolate/Contain | IS, IT/MIS, IT Auditor | It is important that these teams work together to isolate/contain the incident. Using shared expertise and information they can work more effectively to stop the spread of the incident. You do not want the incident to continue spreading through the server or network causing more damage and causing more loss. During isolation you want to ensure that the impact of business operations is accounted for and by containing the incident there may be more disruption. |
| Gather Information | IS, IT/MIS, IT Auditor | It is important for the teams to gather information about the incident which can be used in the future towards building a prosecution case if needed. Also, it is important to gather information that can be used to inform those affected including stockholders in future debriefs. |
| Eradicate | IS, IT/MIS, IT Auditor | The Information Security, IT/MIS, and IT Auditors can work together to eradicate the incident. This can include applying patches, disabling services on the network that aren’t necessary, adding access controls, installing anti-virus software, updating the company security policy and delete any added files that may have been added such as ransomware or trojanware. |
| Recovery | IS, IT/MIS | These teams should check that all steps done during the eradicate phase were properly implemented then restore the system to a working/clean backup that should be monitored before becoming operational again. New tools should be added to help with network surveillance to help with future detection of unauthorized access attempts. |
| Communication and Reporting | | |
| Step: | Role/Responsibility | Rationale Behind Assignment |
| Post Mortem | IS, IT Auditor | This step is important to prepare for future attacks, as well as understand the level of damage that had been done on the company. Using the attack information gathered it is important to decide which type of investigation should be done, each with different levels of cost and time. |
| Documentation | Senior Management, Legal, IS, Public Relations, IT Auditor | Everyone should work together to document all information about the incident in an easy to reference document. This should include audit records, actions performed, persons assigned to which tasks, descriptions of events, full list of details including cost, attack type, time of incident, how long it lasted, and all information gathered to use in reporting to the media in a incident that requires it. |
| Public Media Handling | Public Relations, Legal | This step is important because after a high or extreme level incident it is important to release information to the public and media about the incident. It is important these teams work together to not jeopardize any investigation or legal proceedings. Since this is most likely being told to untrained professionals of IT, the information must be given to public and media in an easy to understand and concise way. |
|  |  |  |
| Prevention | | |
| Step: | Role/Responsibility | Rationale Behind Assignment |
| Prepare Security Policy | Information Security, Senior Management | Combining knowledge of IT and Senior management there should be new policies created and documented, including punishment for breaking company policies. This is important to ensure that employees understand rules in place while at work. There should be no unrelated site surfing, opening links from outside sources, bringing in untrusted devices to connect to the server, and many more policies in place to help protect the company from Incidents both internal and external. |
| Assign Access Controls | IS, IT, Senior Management | Employee roles should be well defined including giving restrictions to systems, servers, applications, files and other work-related tasks based on roles. This ensures that employees are unable to access files or systems that they are not authorized to access, which creates a safer network and helps ensure confidentiality. |
| Learn from past incidents | All Staff | It is important that all incidents are used as a learning tool towards preventing future attacks, or incidents against the network. By learning about phishing, spam, and following policies you can protect from stolen credentials or theft by an attacker acting like an employee. It is also important for ensuring that the team keeps up with current updates on software and tools. |
| Implement System change policy’s | IT, IS, Senior Management | To ensure that changes on a network do not cause vulnerabilities or unknown outcomes it is important that there is a policy and guideline to follow before implementing any changes. This can include steps to follow when updating software, changing access controls, adding applications, and many more things. This will protect the network from unknown consequences such as downtime, security gaps, or unknown risks which may occur if there were no steps to follow. |
|  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Step 1: Objective: Decide who, what, where and how to conduct the cyberattack. Prior to completing your table, read the scenario. Summarize the attack objective you see in that scenario here to situate yourself prior to completing the table. This requires that you read and fully synthesize the scenario, as the attack objective is not explicitly listed.  A small bank located in upstate New York is likely to be the perfect target for an attack due to the lack of fear of getting attacked. The plan will be to test the bank’s local firewall by sending pings to the public IP address and email messaging server using a the XYZ free Hosting Corporation IP address over a few days in order to avoid detection. Once a vulnerability has been found a spear phishing attempt will be launched which includes personalized subject lines in order to gain trust with an unknowing employee. This message will then trick an employee to click on a link which contains a trojan allowing access to the system remotely. Once access to the system has been made a money request from high ranking employees will be sent out leading to a release of funds that are untraceable back to the attacker. The end goal is to make the bank think a hackativist group is attacking their network for recognition while we are taking money from them during their time of confusion. | | | | | | | | | | |
| Step 2: Attack Methods and Features: To succeed, an attacker must complete all the identified attack steps in the proper sequence before the defender applies countermeasures or some unknown variable changes the operating environment under attack. For this step, you will complete the Attack Phase and Attack Action columns below. Ensure your phase and actions are organized according to their order of execution | | | | Step 3: Detection Location and Methods After completing Step 2, you will fill in the two columns below as indicated. | | | Step 4: Response Method After completing Step 3, fill in the column below by identifying and describing the intent of the countermeasure (i.e. to identify, detect, disrupt, deny, etc.) for the corresponding attack action. Also identify important procedural steps necessary to implement the countermeasure. | | Step 5: Response Objective: After completing Step 4, identify the phase of the IR process in which this countermeasure is most likely to be implemented, choosing from the provided list | |
| Attack Phase  Identify the phase of the Kill Chain most closely aligned with the specific attack actions.  (Targeting, Reconnaissance, Weaponization, Exploitation, Installation, Command and Control, Actions on Objective) | Attack Action(s)  Fill in the attack actions (the list of specific malicious tasks performed to complete the attack) and number them in the order in which they would be performed | | | Indicator(s) of Attack  List an anomalous event or effect that can serve as a signal to a defender that the attack is underway. | | Detection Point  Identify a likely target system or asset for the attack action you have identified in Step 2. | Defensive Countermeasure(s) Describe your defensive course of action. (Note: In a professional setting, you may find it valuable to create a library of countermeasures using a standard template, and to simply reference the specific procedure document in the box below. Courses of action tables are intended to be living documents that change as attackers evolve their attacks and incident responders mature their defensive capabilities.) | | Defensive Phase  Identify the phase of the incident response process most closely aligned with each countermeasure. (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned) | |
| Step | | Describe Malicious Task |
| Targeting | | 1 | Identify insecure public-facing target system | | ∙ Spike(s) in network traffic from unusual IP address(es) | ∙ Public-facing web server log(s) ∙ Perimeter firewall log(s) | ∙ Catalog and suspicious IP address(es) for further analysis  ∙ Conduct targeted research into IP Address registration and DNS data | | | Preparation |
| Reconnaissance | | 2 | Develop information about planned targets including organization hierarchy, employee information for social engineering, and hard data information | | ∙Appearance of port scans on network  ∙recent social engineering attempt(s) | ∙Email logs  ∙Firewall logs  ∙Browser logs | ∙Collect website logs  ∙Web administrators review web analytics and build automated detection for typical reconnaissance behavior |  | | |
| Weaponization | | 3 | Find Vulnerability, develop an exploit or find a toolkit to implant into system, followed by testing of exploit | | ∙Recently changed/created files | ∙System files | ∙Keep systems patched  ∙Conduct Malware analysis  ∙Collect files and metadata for future analysis  ∙Build detection for weaponizers |  | | |
| Delivery | | 4 | Send targeted spear phishing attack via email to the bank funds transfer clerk containing Trojan | | ∙Non work-related emails  ∙Strange links  ∙Emails from employees on vacation | ∙Employees with influence  ∙Email logs | ∙Gather, block and review outside sourced emails |  | | |
| Exploitation | | 5 | Target victim triggers the exploit by clicking on the malicious link | | ∙Broken links  ∙Trojan files appear in system files  ∙Suspicious emails from employees asking for money out of protocol | ∙Untrained Employees  ∙Employees with admin privileges | ∙Phishing and internet security awareness training  ∙ find command-and-control traffic from compromised host  ∙Analyze Traffic spikes in email servers  ∙Regular vulnerability scanning and penetration testing to catch attacker | Identification | | |
| Installation | | 6 | Target installs trojan to allow backdoor remote access to system, creates autorun of fake hacktivist attack on server | | ∙Recent system file changes  ∙Remote logins from unknown IP Address(es) | ∙Common Installation paths  ∙Kernal level access/changes | ∙Implement HIPS to prevent known and unknown malware from making changes  ∙Disable remote access  ∙Temporarily block affected system and user account from the network  ∙Gather attack information for later analysis and learning opportunities | Containment | | |
| Command and Control | | 7 | Utilize C2 channels remotely over email to take advantage of confusion exploiting the hierarchy within company, Launch hacktivist front | | ∙Hacktivist image on webserver  ∙High number of complaints about banking portal  ∙High CPU and memory system use  ∙New ping traffic from a unknown IP address | ∙User Banking portal  ∙Banking website  ∙Banking fund hierarchy | ∙Discover C2 Infrastructure by analyzing malware  ∙ Remove malware and recently installed tools  ∙After tools and malware have been removed reset impacted accounts and users.  ∙Force password changes  ∙Add patches to fix vulnerabilities | Eradication | | |
| Actions on Objective | | 8 | Disrupt communication, Email unsuspected targets from internal email. Collect and exfiltrate user credentials, and money from CFO | | ∙ Difficulty using SSH on appliance  ∙XYZ Free Hosting Corporation IP address known for launching of frequent attacks | ∙received and sent email logs  ∙bank transfer funds  ∙out of town employee | ∙Recover network back to working state  ∙Undue any changes made by attacker  ∙Document all attack details for preparation of pending court case  ∙Contact legal team and update policy and new security counter measures | Recovery | | |
|  | |  |  | |  |  | ∙Implement new email and site usage policy  ∙Begin analyzing attack data to use to learn to protect from future attacks  ∙Begin a new Security awareness training program  ∙Add documentation for network and system changes to help track updates and better implement new patches. | Lessons Learned | | |

Counter Measures Analysis

It is important that Defensive countermeasures are planned in advanced using things such as a policy for any network or system changes or updates, as well as having access controls set for employees. Having a standardized method in place for making changes will help to ensure that all updates and changes done to the network or systems are tracked and follow the appropriate steps, allowing the organization to ensure there are no new vulnerabilities which arise before releasing the changes to the live environment. Having access controls in place early will provide a decent start towards countering hacked accounts from being able to access specific sites, applications, links or other potential threats which may cause harm the systems within a network. It is important to prepare for attacks in advanced because this is the most vital time to help with preventing an attack on a network all together. Steps I recommended in the courses of action chart included using an intrusion detection system which can catalog suspicious IP addresses accessing the network which will allow the Information security team to analyze and research the IP address and DNS data to potentially block it before the user can cause harm to the network. This same intrusion detection system can quickly spot port scans attempts or access to blocked files notifying them of attempted malicious activity by a hacker.

Having an intrusion detection system in place is a great advantage towards protecting your system because it can instantly notify you of attempts against your network potentially before the hacker can cause any real damage. A firewall with custom rules which help to block outside traffic as well as emails from outside sources will help to protect from workers unknowingly accessing malicious links spread through web browsers or email. This has been proven to be one of the weakest links in a organizations system and network security. Adding rules to prevent workers from doing tasks that are unrelated while at work will help to reduce risk of them accessing a link or site which may spread a virus, trojan throughout the system, which can implant toolkits causing further harm to the organization. But preparing the network defense is not the only step required to prevent a hack on the network. As seen in this case the attack was initiated through email using a spear phishing technique. Because of this attack working it is important that going forward workers are given proper security awareness training to prepare them for the risk or using a network and the potential threat of things such as phishing and social engineering attempts. Having these steps in place will prevent a hacker from tricking an employee to click a malicious link but will also prevent the link from making it through the email servers in the first place. This will prevent the hacker from effectively gaining remote access of the system and using it to plant malicious code to allow them to shut down the systems while they attempt to steal money through social engineering.

If in the situation a hacker can break through the network through a vulnerability, whether it’s a bug, phishing, or other vulnerability, this can cause a large amount of damage to a company’s organizational operations. In this case a hacker was able to not only cause issues for users trying to access the online portal but completely block access the server by implanting a fake Hacktivist front, all while using phishing and social engineering to gain valuable system access to send emails allowing him to collect money from unknowing workers. By running regular vulnerability scanning and penetration testing a security can reduce a risk of a vulnerability being left around long enough to be used against them. In many cases the length of time a vulnerability is left available will increase the likelihood to be exploited. That is why running these tests weekly at minimum is important, because by doing so you can potentially shut down all the options a hacker has to access a network and cause organizational operation damages. This can be either shutting down systems, networks, stealing money, or even the reputation of the bank from users who may have been affected. The trust of clients can be damaged if their information is stolen which could in turn cause more damages to the operations than the initial attack done in the first place. Therefore, quickly performing containment, eradication, and recovering the operations to a working state is so key. The longer a system is unavailable the more likely there is to be extensive damage and loss of trust. Having a method and guideline to follow will increase the speed to fixing a network and getting it functional as quickly as possible.

iii. Explain how your security countermeasures will reduce the negative impacts from these types of attacks on your personnel (roles and resources).

Personnel within the company who make mistakes such as falling for a social engineering or phishing attempt can feel like they are to blame for an attack on a network. This can cause them to lose morale, or even cause rifts in the workplace between other employees, creating an environment they are no longer happy to work in. By implementing security awareness training, company policies, email filtering, and security controls, there can be a reduced risk of an attack at a personnel level. Having a team who has learned from past mistakes will help them to document and improve on those mistakes in the future. This can prepare them to expect social engineering and phishing attempts while also giving them the tools and resources to spot them and turn them in to the security team before they cause trouble. In order to prepare employees and give them practice, we will send out various fake phishing emails periodically to allow them a chance to learn to identify and report phishing attempts.

A stronger intrusion detection system, firewall, security training, log management, and documented guideline will prepare a company for all situations and prepare for an attack in advance. Although there is never a guarantee that a hack won’t happen it is best to use best practices to prevent them, while also giving guidelines and policies to help with recovery. This will reduce the risk or system failure, stolen credentials, loss of IP, and loss of user information causing loss of trust in the organization. That is why it is important to know how to spot signs or reconnaissance and targeting early to hopefully stop an attack before it ever happens, and this can be done by collecting, analyzing and reviewing logs.

Wayback Machine. (2020). Retrieved from <https://web.archive.org/web/20180712175118/http://www.visa-asia.com/ap/center/merchants/riskmgmt/includes/uploads/AIS_incident_response_procedure.pdf>

Roberts, S., & Brown, R. (2017). *Intelligence-driven incident response* (p. Chapter 3). Sebastopol, CA: O'Reilly Media.

Sood, A., & Enbody, R. (2014). *Targeted cyber attacks*. Waltham, MA: Syngress.