

**BCIS 5740**

**Information Security Management**

**Assignment 2**  
**“The case study of Microsoft Breach Incident”**

**Submitted to: Prof. Obi Ogbanufe**

**Submitted By:**  
Preeti Chaudhry -11559290

This Microsoft breach incident happens in 3 stages in the year 2021. The incident was first reported in the month of January, then March. Here is how it gets noticed -   
  
- On 5 Jan 2021, there’s a security testing company named DEVCORE has made the earliest announcement that there’s some vulnerability for Microsoft data which Microsoft itself confirms on 8 Jan 2021. Later Volexity, a cybersecurity company confirms that hackers are spying on two Microsoft users and alerted Microsoft of the same.   
  
- On 2 March 2021, another cybersecurity company ESET announced that multiple hackers are trying to access the data. The analysts of the security team have made the confirmation that hackers are running the crypto mining software not the servers.   
  
- On 10 March 2021, security researcher Nguyen Jang intentionally posted a code on GitHub regarding how the exploit words comprised of lots of errors, so that the hackers wouldn’t be able to use the code to hack the servers. Later, this code was removed as it requires minimal modification to make the code work.  
   
This attack was planned by the Chinese-based hacking group in which Hafnium is know how to install the web shell on the servers. But the Chinese government is not ready to accept any of these allegations and said that’s it all groundless. This incident impacts 30,000 organizations within the US which include the government sector, IT sector, defense, and all educational institutions also.  
  
This incident was first reported at the beginning of Jan 2022. There were some zero-day exploits discovered on the Microsoft campus. This breach incident leads to the sharing of data, personal information, and passwords of the affected users by the hackers. They also get access to the administrative rights on that system as a result of the breach. Hackers also have access to all the connected devices that are part of the main affected device. Hackers use the backdoor policy for this attack. So, anyhow they’ve full access to the system even if Microsoft updates the version or the previous version features will no longer be available.  
   
Hackers used the four separate zero-day policies to access the systems. This targets Microsoft outlook and from here it’ll get access to all the calendar invites, passwords, emails and the whole work, and ultimately this will allow access to the entire servers which hackers can use to target. Hackers used to do this process in a very strategic way, using the process of mass scanning to find all the nearby vulnerable servers available, and get the address of the server. Once you get the address of the server, then use the two exploits policy which will work out in 2 steps -   
  
- Connect to the server as a false authenticate user  
- exploited standard user access to the admin rights.  
   
Once one gets the admin privileges, a hacker can play in the way he/she wants. Simply copy the code of the server to any of the locations and it runs out perfectly because the hacker has admin rights. Hackers are used to installing the web shell in the system, once the web shell is installed, Backdoor entry is possible. Backdoor entry allows you to access the system all the time from any location if your web shell is active there. Once a web shell is installed, hackers can access anything in the system.  
   
This hacking attack impacts all the data of Microsoft in terms of email communications. Everything communicated over email to an organization or related organization gets exposed.  
   
This incident happened because there were some vulnerabilities in the Microsoft system. Though the organization released patches to resolve these vulnerabilities, customers need to update their system to install these patches. Till the time this practice is not performed by people, we’re still at risk of any future hijack.  
  
The main target of the hacking team is just to get all the email addresses and personal information from all of Microsoft’s allied industries also. Further, hackers used to send unwanted emails with phishing links and content and make people foolish. They want to do this to get money, and all banking data from people to access their credentials for their own sake.  
  
Breaching data leads to the flow of information on a massive scale directly from the people to the hackers. This information leads to the sharing of various personal ids starting from an email address, phone number, organizational data, and internal security things, and consequently, it can affect all the personal security of an individual and hackers have all the data. There’re several other companies that are owned by Microsoft, their data also gets shared. People start getting unwanted calls, fake job offers, and emails with unwanted attachments that are just spam and don’t have any relation to the job. People start getting fake job offers like you’re selected for this company with an average package of this. Come and let’s join——kind of things. Microsoft lost a million dollars because of this crisis.  
   
The company starts falling to loss and starts firing employees. This leads to so many layoffs. Skilled people suddenly search for jobs and can’t find them anymore frequently. A wave of recession starts hitting the market for IT employees.

I still remember one of my cousin's brother got fired from Microsoft at that time. I remember that he got placed in his dream company and how badly this thing hurt him!  
 At that moment, I didn’t have much awareness of this thing, but when I met him personally, he told me the things that happened with him, it was about various other people that also got fired. Firing from such kind of organization soon after you complete your master's is a kind of shock!  
People are dealing with this mental pressure along with the hustle of searching for another job.  
  
When this kind of incident happens, social Engineering people and teams start taking advantage of the soft crowd emotionally. They kind of start building the feeling of fear, helplessness, urgency, and neediness. All this will ultimately lead to the people falling prey and the loss of money, and credibility for the previous organization.  
  
This incident impacted on an overall 250 million customer records. The target population included people from all the majors like government people, non-government organizations, people from the defense, students, IT people everyone. Though Microsoft is such a big organization, it’s on the verge of rising all the time. It didn’t have much effect on the various factors. I want to list some of them with a comparison from the previous year's data.  
  
- **Revenue**   
In the year 2020 - $143.015 billion

In the year 2021 - $168 billion  
   
Microsoft has noticed an upgrade in terms of revenue, an increment of 18% noticed in comparison to the previous year.   
  
- **Stock Price** Microsoft noticed an Increment in terms of stock price also. There’s a bump in the prices of stock compared to the previous year 2020.   
  
In 2020 - 193.0261  
 In 2021 - 275.9408  
  
- **Reputation** - Any major breaching incident affects the people working there or want to work there in some or other way. This impacted on the current workers in terms of getting fired from the company and other potential employees who want to work there take a step back because they are also under fear of getting fired. Later, Microsoft is such a big name and makes a strong comeback in the market with better stocks and revenues, and from then till now its stocks and revenue value is increasing every year. Again, the big organization gains the unbreakable trust of people, and it continues to persist.  
  
Even before this breaching incident happened, Microsoft used a lot of safety precautions to protect the data from any kind of security means. These are some of the processes that Microsoft used to -  
  
- Awareness among the people who’re working in the organization. Once employees get to be kind that they’ve some data that hackers are always in need of. They will access things more diligently and with knowledge. Microsoft used to have some other kinds of training programs within the organization to train the employees on how to deal with data.  
 - Classification of data based on sensitivity.  
 - Have restrictions of access on the basis and other protected rights should be given based on authority.  
 - Store all the necessary information and sensitive content within the cloud.  
 - All the devices which have some secure and sensitive information stored should have the capabilities enabled.  
 - Access to sensitive information should have individual sensitive credential access.  
 - Always emphasize the strength of passwords. - Multi-factor authentication is installed to access almost every sensitive piece of information which is very important and essential for protecting the security of the data.  
 - Encryption of security data is very important while storing and transferring it.  
 - Back up and production work should be separated.  
 - Always make sure that the system is properly up to date. Updating of the system instills the new updated version with a more secure connection.  
 - Always have the security and networking team members look over the activities that are happening within the organization.  
  
And I would like to write that these kinds of incidents are problematic for everyone. When I’m reading it, sometimes I also feel like that if it’s someone accessing my information from somewhere. I can also be part of this kind of incident. To be on the safer side, I started using 2-factor authentication on almost all the apps where it’s possible. I stopped writing my passwords on the notepad. I started to be more aware of the strength of the password, now I prefer to use passwords that are good in strength, and difficult and try to remember them and learn in my way. And recently, 4 months prior there’s a kind of scam happened with me in which I lost my 3250 USD. Being a student, it’s a very big amount for me. I still remember how I came out of this fear. It’ll take me a month to accept it. it. But this gives me a lifelong lesson on how to be very aware and protective regarding the security of your data.  
  
**Mitigation Strategies**  
  
- On 12 March 2021, the Microsoft security intelligence team deployed a new family of ransomware called DearCry to all the affected servers. This will demand the payment to recover the earlier files. And there is no guarantee that after making the payment, you will have access to the content.   
  
- On 2 March 2021, Microsoft releases a one-click power PowerShell tool, which installs the protection updates against a particular threat, runs out of malware to detect the installed web shells in the system. These are all some temporary mitigation measures.  
  
**References**

Methodology/Impact  
<https://en.wikipedia.org/wiki/2021_Microsoft_Exchange_Server_data_breach>Breaching Initiation  
<https://auth0.com/blog/the-worst-data-breaches-of-2021-q1-and-q2/>**.**  
  
Exposition Of Data  
<https://www.lifelock.com/learn/data-breaches/microsoft-exposed-250-million-customer-records>Wikipedia Source  
<https://en.wikipedia.org/wiki/2021_Microsoft_Exchange_Server_data_breach#Impact>Mitigation Strategies  
<https://en.wikipedia.org/wiki/2021_Microsoft_Exchange_Server_data_breach>Steps Microsoft had taken before security breach  
<https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/avoid-security-breaches-how-to-protect-your-data>