  920 Fourth Avenue, Suite 2900, Seattle, Washington 95104

The Case Study of Microsoft Breach Incident

The Case Study of Microsoft Breach Incident

# Introduction

The acknowledgement by Microsoft Corporation regarding an access misconfiguration that led to the exposure of more than 250 million customer records on a public access database that had not password protection caused a global out roar. However, the case prevented an opportunity to analysts and cyber security experts to access the vulnerability of their institutions regardless of size and technical resources. Microsoft is such a big organization, and its market is considered the topmost in the world. In this case study, I want to discuss all my take on security-related practices that should be put into practicality for better and secure networks and will discuss their counterparts. In short, I will add all the details of the case study.

# Potential Consequences

With Microsoft's recent data breach, many were wondering how the company would deal with this situation and what are the potential consequences for all those who used its service. The data breach involved more than 250 000 individuals' information (Novet, 2021). The lost data include names, email addresses, passwords, telephone numbers, and financial details such as bank account numbers and credit card details.

There are four potential consequences of the data breach for Microsoft customers.

*Outage of company services and passwords*

Microsoft revealed that the data breach could result in the suspension or disorientation of service for the users, and their passwords will automatically be reset. The company is currently working to mitigate the situation. It is unclear how long the users will have to wait before resetting passwords. Some users report that they have already experienced the consequences of the data breach (GAO, 202). Some of them have been unable to access their email or have had their passwords automatically reset. However, those who want to regain access to their account must generate a new password, ideally containing a combination of letters, numbers, and special characters.

*Affected services will be restarted*

As mentioned in the previous point, affected services such as Outlook, Hotmail, and Live Mail will have to be restaffed again as they cannot cope with the number of users due to the data breach (GAO, 202). It will result in the accounts being suspended once again.

*Increase in the number of spam messages*

As a direct consequence of the previous two points, Microsoft users could receive up to 30% more spam messages in their mailbox after their accounts are reinstated (Chance, 2021). It is because spammers can access the users' previous email addresses. The users will have to spam their mailbox to prevent this from happening. It is recommended that the users keep their spam filter enabled to decrease the chances of getting emails from spammers. Most spam filters can detect emails sent from known senders and can be set up to not allow emails from these senders to be classified as spam (GAO, 202). It is because some third parties will have access to their online address and email passwords.

*Possible identity theft*

Some hackers will likely be able to access Microsoft users' information after the data breach. Once they have access to their details, they can use them to create fake accounts and steal money from these users (Chance, 2021). To avoid being a victim of identity theft, Microsoft customers should be extra careful with their accounts and ensure strong password combinations and 2-step verification protects them, preventing hackers from accessing their accounts. After the data breach, users also had to deal with the possibility of phishing emails. Since their accounts were suspended, they received messages from other third-party services, and all those who clicked on them had a big chance of suffering from severe identity theft.

# Action Plan

The data breach will cause some losses to the company. The number of users that will stop using Microsoft services is still unknown, but it is certain that the firm will have to deal with a lot of criticism from consumers and must pay fines for failing to protect their accounts and data. Microsoft services must bear the cost of account suspensions and anticipate growth in spam emails. However, to ensure that the company could deal with these losses, Microsoft decided to acknowledge this incident and acted by informing all those who were affected (Chance, 2021). It has helped them gain some trust from their customers and made them able to handle this situation better than it could have been if we had not admitted the data breach.

Four action plans may handle the security breach for the affected enterprises and Exchange Server users

*Consumer Notification*

After the data breach was announced, Microsoft started to send emails to those who had been affected. For those who do not use Microsoft services, their service providers will also send them emails with information about the breach and how they should check if they have been affected. As per the GDPR guidelines, all affected users must be notified of the security breach within 72 hours of the data breach. Notifying both the affected users and unaffected consumers can help both parties prepare. The notifications can be done via email, SMS, or phone. Per the GDPR guidelines, anyone receiving this notification can choose to keep it private.

*Checking for Compromise Indicators*

After such a data breach is detected, the affected users need to check for any indicators that suspicious emails could have been sent from their accounts. These indicators are usually called compromise indicators and include a sudden increase in the number of messages from the same sender, more than one email account created with their account, unusual behavior of accounts, and some other measures that may cause alarm in an incident like this. The users should be on the lookout for any suspicious activity resulting from the data breach. For example, they should notice odd behavior in their accounts, such as sending unusual amounts of money to other users or receiving strange emails from third parties. Their service providers should also be able to detect any unusual activity in their accounts and notify them. Compromise indicators include the presence of unknown incoming mails, unusual login activity, the presence of unusual files in their account, etc.

*Creating a Forensic Image*

To create a forensic image of an affected user's mailbox is just like comparing it with a "snapshot" or a "digital footprint." It can help in solving the problem and recovering data from the compromised account safely and quickly. The system would take a snapshot of all data stored in the operating system and compare it with what is stored on the server to ensure all data has not been lost (Chance, 2021). The company should create a forensic image of all the data stored on their servers and ensure that they can provide this image to all users affected by the data breach. The user should not delete any information stored on their account but can use this image to check if all their account data has been compromised. The user will also have information about how much is being stolen and how many users are affected by the security breach. It will help them decide what action to take and prevent identity theft. A forensic image can also ensure business continuity and act against the person or group responsible for the data breach.

*Security Patches*

Microsoft has regularly released patches throughout the security breach to improve its security measures. These patches should be applied to all systems connected to Microsoft networks and protect them from data breaches (Chance, 2021). However, users must ensure that they apply all the necessary patches on their computers and do not install any applications or updates from third parties. The security patches the company implemented should be checked regularly to ensure they can protect the data stored on their servers. All users and their providers should regularly check if they can receive emails from third parties. If suspicious activity is detected, they must report this to their providers, who will then report it to Microsoft.

The security patches that have been released will only work if installed. To ensure they are, the user can check immediately after their account has been suspended if the latest security patches have already been installed on the device they use. Then, they can reinstall the patches to ensure all their data is safe. Patches that safeguard vulnerabilities should be available worldwide against zero-day exploits. Some of the patches are applying to all Exchange servers. It may include Microsoft's best practices, such as transit encryption or proper authentication steps.

Despite the disastrous impact of this data breach, Microsoft has been praised for acting against it and has tried to resolve this incident as quickly as possible by informing those affected about the security breach immediately after it was discovered (Chance, 2021).

# Preferred Course of Action

Companies need to take measures when dealing with a data breach as otherwise, users will lose trust in them and may even stop using their services. Advanced Detection and Response Cloud software is an Artificial intelligence approach to improve the response to cyber-attacks. This new solution provides organizations with improved protection against unauthorized access and use of their cloud infrastructure. It also extends its protection against remote and on-premises devices.

As organizations move their operations and applications into the cloud, they face increasing complexity in monitoring and securing their infrastructures. Existing solutions are not designed to address these challenges effectively and are not easy to deploy and manage. The Cloud Advanced Detection and Response solution provides a comprehensive view of all threat surfaces, allowing organizations to manage their cloud operations confidently (ARIA Cybersecurity Solutions, 2021). The Cloud ADR solution uses a threat modeling approach to analyze and detect threats by their behaviors. It then uses machine learning to find these behaviors in the network data and threat analytics. Its AI-driven approach eliminates human intervention and allows IT staff to deploy and operate the solution quickly.

Cloud ADR is a software-defined approach that combines the capabilities of the application-based solution with the latest threat detection and response capabilities. It enables organizations to improve their protection against unauthorized access and use of their cloud infrastructure. It also extends its protection against remote and on-premises devices. The seven security tools included in the product are designed to provide a comprehensive view of their environment. The Advanced Detection and Response (ADR) solution would provide a virtual AI-SOC that automatically detects and stop cyberattacks without requiring highly trained security personnel (ARIA Cybersecurity Solutions, 2021). It works around the clock and is powered by a big data approach that combines machine learning and advanced analytics. The solution takes advantage of the data collected from various security devices and applications, such as firewalls, operating systems, and cloud services.

The solution takes advantage of the built-in models in SIEM to analyze and visualize every known threat. Its AI capabilities can identify and prevent attacks by analyzing their behavior patterns. It eliminates the need for daily alerts and significantly reduces attack risk. It is a type of security that can help organizations protect themselves from various attacks, such as ransomware, malware, and DDoS attacks. It can also help prevent data loss, policy violations, and other hidden threats. The Cloud ADR solution is a variant of an application-based ADR that can be deployed within a VM infrastructure (ARIA Cybersecurity Solutions, 2021). The threat surface covers the full spectrum of threats, including the cloud, remote devices, and on-premises infrastructure. With machine learning, you can find and analyze threats through their tell-tale behaviors. Automatic stopping of attacks is also built into the platform, which can be used to prevent attacks from happening immediately.

# Steps to integrating an ADR into a server

The Advanced Detection and Response (ADR) system should be fully implemented with all the resources needed to ensure it functions correctly. It will include deciding who will be part of the response team and hiring outside contractors to get expertise in the area. The system should also address security concerns of confidentiality, integrity, and availability to ensure that the system addresses these concerns. The technical staff should be involved in training the incident response team and informing them of what resources they will need to operate the system. It can be done by integrating security controls into the system so that there are some built-in checks and balances when performing the detection process. Reporting security incidents and carrying out investigations is important for any organization; it is always better to report a breach of confidentiality or integrity immediately so that immediate action can be taken to stop further damage from being caused before it spreads further.

***Create an Incident Response Team*:** When developing an Advanced Detection and Response (ADR), it is important to have a team of people who can respond to a breach. This team should contain Incident Response personnel, Person Responsible, Legal Department, and technical experts organized under the Incident Response Team. This team is responsible for keeping security controls in place and ensuring that they continue working properly; they should be responsible for evaluating the effectiveness of security controls and creating an incident response plan in the case of a security incident.

The Incident Response Team should work with security engineers to create a detection plan for their Advanced Detection and Response (ADR) system. They should be able to detect and respond to security incidents as soon as possible to mitigate the damage before it spreads further. The incident response team will also have to help develop a plan for legal issues arising from the breach of personally identifiable information, trade secrets, or intellectual property; this could include informing customers of the breach, monetary compensation, and consultation from legal experts.

***Automate the Incident Response Process*:** By automating this process, you can improve your response time and reduce the human error aspect that may occur by having humans carrying out manual procedures. When the Advanced Detection and Response (ADR) system is being developed, it is important that it can be easily configured and adapted; this can be done using an API to integrate security controls into the incident response process. The incident response process should be automated to continue working properly in the case of a breakdown; this allows for an Advanced Detection and Response (ADR) to function in an environment that may have damaged or compromised hardware and software. All security controls should have a set time frame to work when installed. It can be achieved by using clear instructions to ensure the system is set up correctly.

***Integrate Security Controls into the Incident Response Process***: All security controls should be integrated into the Advanced Detection and Response (ADR) process to ensure that they work together; this can be done by developing a well-structured API to integrate security controls into the incident response system.

***Make sure that the incident response process is communicated to staff members:***

All staff members should be informed and trained on what to do in the case of a security incident; this can be done using written procedures and training sessions that staff members conduct.

***Establishing partnerships with other organizations and agencies to share information, expertise, and experience:*** The response team will need communication channels open with other organizations to share information, expertise, and experience in handling security incidents that could occur within their organizations. They should be able to share information on breach incidents, new security controls, training, and development. New security controls should be brought forward so the team can evaluate them before implementation. They should also be able to recommend any new security controls that may affect the incident response process.

***Developing a plan for handling breaches of personally identifiable information, trade secrets, or intellectual property with an Advanced Detection and Response (ADR):***

The Advanced Detection and Response (ADR) system should be able to notify the incident response team as soon as possible so that they can begin working on the problem and implement their plan. This plan should also include contacting outside parties to ensure that incidents are handled properly. This process can be further improved by integrating an Incident Handling System into the Advanced Detection and Response (ADR) system, whereby all information is logged and can easily be acted upon by the response team.

***Establishing a service level agreement with the information technology staff:***

All staff members should be informed and trained on what to do in the case of a security incident; this could include informing customers of the breach, monetary compensation, and consulting with legal experts. This process can be further improved by integrating an Incident Handling System into the Advanced Detection and Response (ADR) system, whereby all information is logged and can easily be acted upon by the response team.

***Having Response and Notification Procedures from the Advanced Detection and Response (ADR) for Breaches of Personally Identifiable Information, Trade Secrets, or Intellectual Property with an Incident Handling System:***

Formal written procedures should be prepared and distributed to all staff members and kept updated in case of any changes. The Incident Handling System should be able to notify the Advanced Detection and Response (ADR) Service when an incident has occurred. It should also log all security events to allow for analysis. All the Advanced Detection and Response (ADR) team members should evaluate their response plan regularly to prevent human error within the process. Advanced Detection and Response (ADR) can help organizations improve their detection capabilities; by integrating security controls into the system, they can detect attacks more easily before they cause further damage.

***Developing a relationship with outside contractors for an Advanced Detection and Response (ADR)***

The incident response team will need to establish a relationship with outside contractors for the Advanced Detection and Response (ADR) to gain access to their expertise and analyze their findings. It can be done by sharing information and trial runs on the incident response process. These trials could be with other organizations to test it out before it is fully implemented by the Advanced Detection and Response (ADR) team. It can also be done by starting with a trial run in the strategic plans department before adding it to the incident response process.

***Establishing a Service Level Agreement with the information technology staff:***

When developing an Advanced Detection and Response (ADR), an agreement must be established between the team and the Information Technology Department. It will help them determine how they can help each other when different incidents occur. This agreement can be generated during the development of an Advanced Detection and Response (ADR) system so that there is clear communication between both teams. The Incident Response Team should work with security engineers to create a detection plan for their Advanced Detection and Response (ADR) system. They should be able to detect and respond to security incidents as soon as possible to mitigate the damage before it spreads further. The incident response team will also have to help develop a plan for legal issues arising from the breach of personally identifiable information, trade secrets, or intellectual property. It could include informing customers of the breach, monetary compensation, and consultation from legal experts.

***Developing a set of procedures for detecting and responding to security breaches:***

A procedure is needed to ensure consistency between these different detection mechanisms. The procedures will also explain how to follow up on a security incident and what to do in a major incident. The Information Technology Department has to ensure that all security controls are set up correctly for the Advanced Detection and Response (ADR) system to function.

***Gaining approval of this process from the organization's senior management to ensure that it will be implemented correctly:*** The Senior Management has to be involved in developing this plan to clearly understand the Advanced Detection and Response (ADR) system will be doing for them. Developing the plan is also a good time to communicate any concerns they may have with their staff. Senior management must give the go-ahead for this new procedure to ensure there is support from the organization's top. It will help reduce any barriers or opposition when implementing this process.

***Performing testing and training to ensure that the response procedures work correctly:***

The response team should test this process in the strategic plans department before fully implementing it in the Advanced Detection and Response (ADR) system. It can be done by performing a trial run in this department first and then expanding it to other departments as time goes on. Training for the team should include how it will be implemented, what resources they will need, how to use them, and how to develop their skills to deal with any security incidents that may arise within their organization. Performing testing and evaluation is a crucial part of an Advanced Detection and Response (ADR) system; it can be done by performing tests on security breaches within the Strategic plans department before expanding it into other departments.

**References**

ARIA Cybersecurity Solutions. (2021, December 23). *Best of 2021 - what we can learn from the 2021 Microsoft Data breach*. Security Boulevard. Retrieved August 6, 2022, from https://securityboulevard.com/2021/12/what-we-can-learn-from-the-2021-microsoft-data-breach/

Chance, C. (2021, March 17). *Microsoft Data Breach: Risk, regulation and managing a crisis*. Clifford Chance. Retrieved August 6, 2022, from https://www.cliffordchance.com/briefings/2021/03/microsoft-data-breach--risk--regulation-and-managing-a-crisis.html

GAO. (202AD, January 13). *Federal Response to SolarWinds and Microsoft Exchange Incidents*. U.S. Government Accountability Office. Retrieved August 5, 2022, from https://www.gao.gov/assets/gao-22-104746.pdf

Novet, J. (2021, March 10). *Microsoft's big email hack: What happened, who did it, and why it matters*. CNBC. Retrieved August 6, 2022, from https://www.cnbc.com/2021/03/09/microsoft-exchange-hack-explained.html