CAPSTONE

THISISAFAKECOMPANY

Abstract

THISISAFAKECOMPANY email system compromise analysis.

Victor Obiora

Name: Victor Obiora

Contents

1 Executive summary

THISISAFAKECOMPANY is a leader in corporate environmental consultations, providing solutions to help clients reduce their environmental impact and achieve sustainability goals. The company has a team of experienced and qualified professionals, led by Grace Caldwell, the Chief Executive Officer, who has over 20 years of industry experience and holds an MBA from Harvard Business School and a Bachelor's degree in Mechanical Engineering from MIT. The company's other key executives are Marion Rice, the Director of Marketing, who has over 10 years of experience in marketing and communications and holds a Bachelor's degree in Communications from the University of California, Los Angeles, and Tyrone Ramos, the Chief Information Officer, who holds a PhD in Computer Science from Stanford University and a Bachelor's degree in Electrical Engineering from the California Institute of Technology. The company's mission is to help clients achieve environmental excellence and create positive social and economic impacts.

2 Purpose

The purpose of this document is to alert independent contractors of THISISAFAKECOMPANY about a detected security breach. The IT team has identified malicious traffic on the system, indicating an unauthorized attempt to access the company's network. The document aims to provide information about the nature of the breach, the steps taken by the IT team to address it, and the recommended actions for contractors to help secure the network.

2.1 Scope

The scope of this document includes:

- **Incident Description**: Detailing the nature of the security breach, which was initiated through a deceptive email sent on December 4, 2023.
- **Response Measures**: Outlining the actions taken by the IT team to mitigate the breach and prevent further attempts, including notifying the cybersecurity provider.
- **Preventive Actions**: Providing recommendations for contractors to help secure the network, such as avoiding suspicious emails or websites, reporting any unusual activity to IT, and reviewing password strength.
- **Ongoing Monitoring**: Assuring contractors that the IT team understands the importance of network security and will continue to monitor the situation closely, providing updates as necessary.

2.1 Introduction

The purpose of this report is to provide an overview of THISISAFAKECOMPANY, its services, its team, and its achievements. THISISAFAKECOMPANY is a leading provider of corporate environmental consultations, offering a range of services such as environmental audits, carbon footprint assessments, waste management plans, renewable energy solutions, and green certifications. The company was founded in 2015 and has since grown to serve clients across various industries, such as manufacturing, hospitality, retail, and healthcare. The company has offices in Toronto, New York, London, and Sydney, and employs over 100 staff members. The company's vision is to be the global leader in corporate environmental consultations, delivering innovative and effective solutions that meet the needs and expectations of its clients and stakeholders. The company's values are integrity, excellence, innovation, and customer satisfaction.

3 Opensource Investigation

This OSINT report gives and in-depth analysis on THISISAFAKECOMPANY's public information from there webpage. The goal is to use this information to find any leads that can be connected to the compromise of the organization's email system on December 5th 2023.

Findings:

The organization's mission statement

THISISAFAKECOMPANY's mission statement

We are an environmental based company trying to reduce carbon emissions.

The organization's leadership team, including their names, job titles, and biographical information.

The leadership team of THISISAFAKECOMPANY includes:

- **The Chief Executive Officer:** Grace Caldwell runs a company called THISISAFAKECOMPANY, where they help businesses with environmental advice. When she's not working, Grace likes to play golf and loves trying out new recipes in the kitchen. She's been in the industry for more than 20 years and is known for being a great leader who can make smart decisions to help the company grow. Grace studied at Harvard Business School for her MBA and got her Bachelor's degree in Mechanical Engineering from MIT.

Email: grace.caldwell@thisisafakecompany.com

- **Director of Marketing:** Marion Rice is in charge of marketing at THISISAFAKECOMPANY. Outside of work, she likes hiking with her dog and going to live music concerts. Marion has been working in marketing and communication for more than 10 years and is good at creating and running successful marketing plans that bring in money and connect with customers. She got her Bachelor's degree in Communications from the University of California, Los Angeles.

Email: marion.rice@thisisafakecompany.com

- **chief Information Officer:** Tyrone Ramos is the person in charge of information at THISISAFAKECOMPANY. When he's not working on keeping the company's information safe, Tyrone likes playing basketball with his two sons and coaching the local youth team. He also loves traveling and trying out different cultures and foods. Tyrone earned a PhD in Computer Science from Stanford University and got his Bachelor's degree in Electrical Engineering from the California Institute of Technology**.**

Email: tyrone.ramos@thisisafakecompany.com

In today's interconnected world, information about corporate leadership has become more accessible due to the internet and the digitization of records. As a result, threat actors have more opportunities to exploit this information for various malicious purposes through corporate espionage, social engineer and phishing campaigns.

The organization's physical locations, including headquarters, offices, and retail stores.

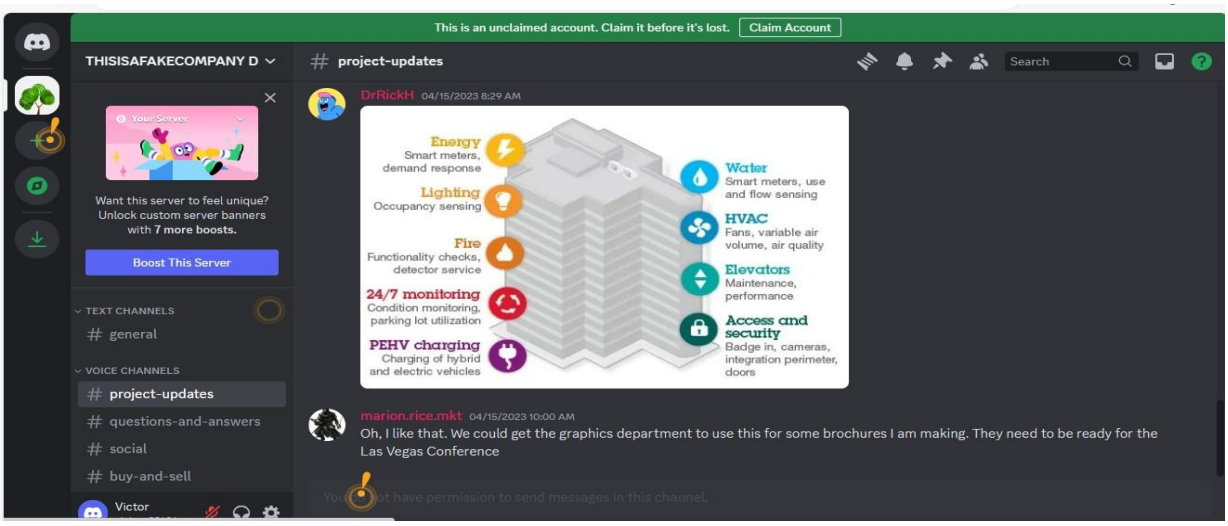
THISISAFAKECOMPANY’s headquarters is located in 438 Richmond St W, Toronto, ON M5V 3S6, Canada.

Threat actors may want this information to disrupt operations and services, and to extort money from the organization by demanding ransom or threatening to expose sensitive data.

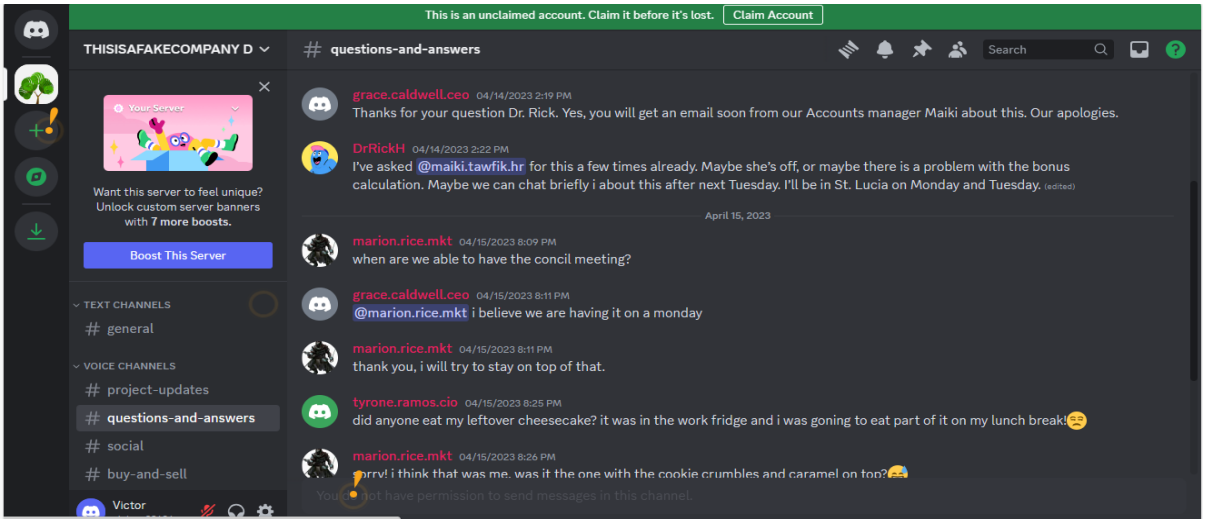
Name: Victor Obiora

Discord server activities:

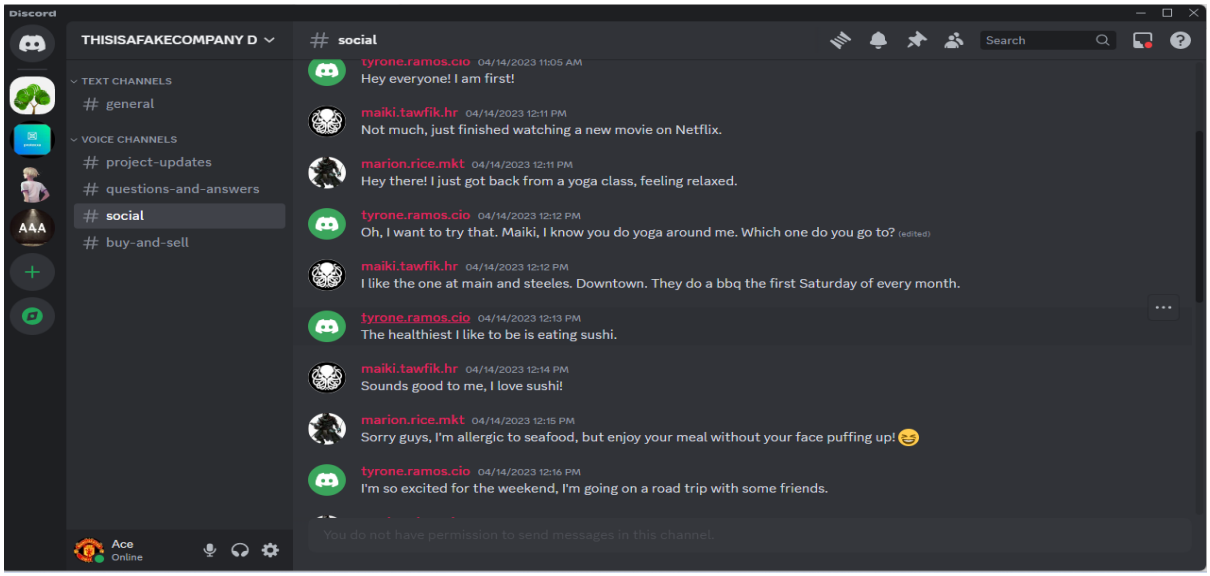
Any information about future projects of the company are easily obtainable by persons outside of the company which give threat actors insight on the company's inner operations.



Important conversations among members are open for everyone to see. Threat actor can gain valuable information from the conversations between these team members.



Threat actor can decide their target by understanding them through their casual conversations.



Conclusion:

According to the information gathered, THISISAFAKECOMPANY displays a lack of cyber intelligence based on the fact that their entire discord discussions are open for all to see. This allows those with malicious intend to observe the company's plans and future projects as well as the company's operations with little effort.

4 Appendix A- Vulnerability report

This section summarizes the threat level based on the vulnerability of the plugins that the threat actors may have used to compromise the company's email system.

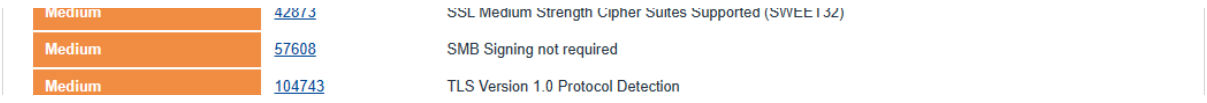
SMB Signing not required plugin

Severity – Medium

Vulnerability Description – It does not require signing in on the remote SMB server. If SMB signing is not required, it means that data being transmitted can be intercepted, read, and modified without detection.

Possible link to incident - The incident details mentioned that the threat actors exploited a vulnerability in the web service plugin to achieve this. The vulnerability specifically involved a remote code execution vulnerability in the web service plugin. While the provided incident details do not explicitly mention the SMB signing vulnerability, it is possible that the attackers exploited multiple vulnerabilities to achieve their objectives. The SMB signing vulnerability mentioned (Nessus Plugin ID 57608) could be one of the potential weaknesses in the organization's network that the attackers exploited as part of their overall strategy.
Risk score: 5

Solution - The solution to this vulnerability involves enforcing message signing on the remote SMB server. Message signing is a security feature that helps ensure the integrity and authenticity of data exchanged between SMB clients and servers. When SMB signing is enforced, it adds a digital signature to the SMB packets, preventing attackers from tampering with or intercepting the communication.



PHP Unsupported Version Detection

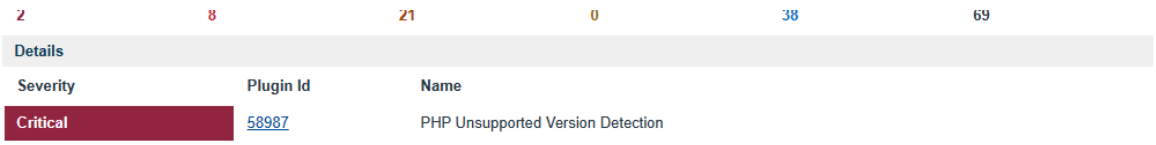
Severity – Critical

Vulnerability description - This indicates that the PHP version installed on the server is no longer supported. The lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Possible link to incident – The incident described by THISISAFAKECOMPANY is related to the unsupported version of PHP on the remote host. The Nessus Plugin ID 58987 specifically identifies an unsupported version of a web application scripting language, in this case, PHP. The description indicates that the installation of PHP on the remote host is no longer supported. This lack of support implies that no new security patches for the PHP version will be released by the vendor, making it likely to contain security vulnerabilities.

Risk score: 10

Solutions – Upgrade to a version of PHP that is currently supported



Apache 2.4.x

Severity - Critical

Vulnerability description - Indicates that the Apache HTTP server installed on the remote host is affected my multiple vulnerabilities because it is running an older version.

Possible link to incident - This plugin identifies multiple vulnerabilities in the Apache HTTP Server version installed on the remote host. The vulnerabilities mentioned in the plugin description include HTTP request splitting with mod_rewrite and mod_proxy, potentially leading to HTTP Request Smuggling attacks. Additionally, there is a vulnerability related to HTTP Response Smuggling via mod_proxy_uwsgi.

Risk score: 10

Solution – Multiple vulnerability issues that involves upgrading the Apache HTTP server to version 2.4.x <, for security patches to protect the server from further potential threats.

Severity	Plugin Id	Name
Critical	58987	PHP Unsupported Version Detection
Critical	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
High	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
High	161454	Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow
High	153584	Apache < 2.4.49 Multiple Vulnerabilities
High	170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
High	150280	Apache 2.4.x < 2.4.47 Multiple Vulnerabilities
High	156255	Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF
High	183391	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
High	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities

Unencrypted Telnet Server

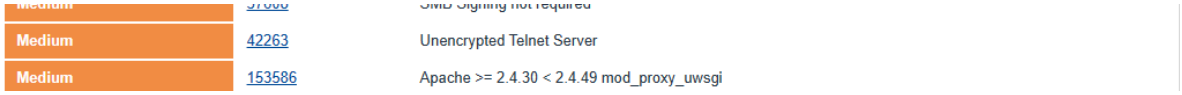
Severity – Medium

Vulnerability description – The lack of encryption leaves sensitive information, including usernames, passwords, and other credentials, exposed during communication sessions.

Possible link to incident - The information provided in the incident details of THISISAFAKECOMPANY suggests that the threat actors exploited a vulnerability in the web service plugin to compromise the organization's email system. However, based on the information you provided, there is no explicit mention of a Telnet server vulnerability in the incident details.

Risk score: 5.8

Solution: Disable the Telnet service and using SSH(Secure Shell) instead.



SMTP Service Cleartext Login Permitted

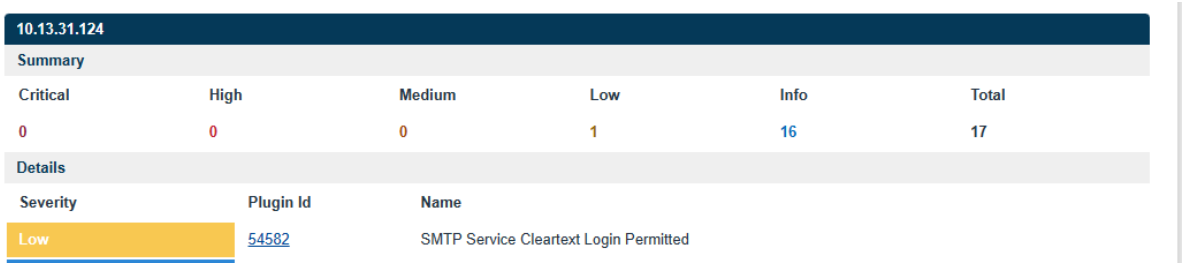
Severity - Low

Vulnerability description – The warning “SMTP Service Cleartext Login Permitted” is raised when the Simple Mail Transfer Protocol (SMTP) server allows cleartext logins over unencrypted connections. This could potentially expose user names and passwords to attackers who are able to sniff the network traffic.

Possible link to incident - The SMTP (Simple Mail Transfer Protocol) service on the remote host is configured to permit cleartext logins over unencrypted connections. Cleartext logins make it possible for an attacker to intercept and view sensitive information such as usernames and passwords by sniffing network traffic, especially if less secure authentication mechanisms like LOGIN or PLAIN are used.

Risk score: 2.6

Solution – Configuring the SMTP service to only support less secure authentication mechanisms over an encrypted channel.



10.13.31.124

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Details

Severity	Plugin Id	Name
Low	54582	SMTP Service Cleartext Login Permitted

5 Appendix B – Risk Assessment

5.1 Introduction

The purpose of this report is to assess the risks to THISISAFAKECOMPANY and to identify which of these could be accepted and which may need some action to be taken to address them after THISISAFAKECOMPANY's email system was compromised on December 5th 2023.

Once this risk assessment report has been approved, specific actions will be identified, discussed, agreed and then documented in a risk treatment plan to be managed as part of the Information Security Management System (ISMS).

This risk assessment report describes:

- The context and scope of the risk assessment
- The assets within scope
- Threats to, and vulnerabilities of, those assets

This report is input to the risk treatment stage of the process and must be signed off by top management before continuing further.

This risk assessment was carried out by the following people:

NAME	ROLE IN ASSESSMENT
Victor Obiora	Lead risk assessor

Table 1: Risk assessment team

As part of the assessment, the following additional people were consulted:

NAME	TITLE	LOCATION
Tyrone Ramos	Chief Information Officer	Toronto, Canada
Maiki Tawfik	HR Manager	Toronto, Canada

Table 2: People consulted

Internal And External Context

The reason why the assessment was carried out was to identify the vulnerabilities within the organization's email systems and processes. From there they would assess the impact to understand the severity of the incident by knowing what data was compromised and the number of users that were affected, to reinforce compliance with the standards and regulations, prevent future incidents, and to protect the organization's reputation.

The potential benefits for carrying out risk assessment include:

- Risk Mitigation
- Data Protection
- Regulatory Compliance
- Reputation Management

Scope

This assessment addresses the risks by identifying the specific vulnerability in the Twitter API that was exploited, gauging the impact of the breach, the detailed time-line of the events, the security measures that were put in place before the breach, and how effective it was in preventing the breach, and finally, the evaluation of Twitter's compliance with data protection and privacy regulations, as well as any potential legal implications and consequences.

6 Risk Assessment Summary

The recent cybersecurity incident at THISISAFAKECOMPANY has exposed several critical assets to significant threats. The compromise of the cloud server poses a risk of unauthorized access and potential data breaches, leading to the loss of sensitive information. The staff is vulnerable to social engineering and insider threats, which could result in compromised accounts and data leaks. The IT infrastructure is at risk of cyber attacks and system compromise, potentially leading to disruptions in services and data loss. Data security measures, if compromised, may result in policy violations and the loss of data protection. Finally, the breach has the potential to damage user trust, impacting the company's reputation and credibility, with potential consequences for customer confidence and overall business operations. It is crucial for the organization to address these risks through comprehensive security measures and training programs to prevent similar incidents in the future.

7 Asset-Based Assessment

REF	ASSET	TYPE (P/D/I)	THREAT	ADDITIONAL COMMENTS
1	Cloud Server	Digital	Unauthorized access, data breach.	Loss of sensitive data, compromised integrity and confidentiality of information stored on the server. Could lead to reputational damage.
2	Staff	Physical/Informational	Phishing attacks, social engineering.	Compromised user accounts, unauthorized access, potential data breaches, and reputational damage.
3	IT infrastructure	Physical/Digital	Malware, physical damage.	Disruption of services, loss of data, potential financial loss, and compromised network integrity.
4	Data security measures	Digital	Cyber-attacks, hacking.	Compromised data security measures could lead to unauthorized access, data breaches, and potential legal consequences.
5	User trust	Informational	Social engineering, reputation damage.	Loss of customer trust, damage to brand reputation, and potential loss of business.

Table 3: Risk assessment results summary (asset-based)

Figure 1: Asset-based risk assessment

8 Response plan

In response to the recent cybersecurity incident, THISISAFAKECOMPANY acknowledges the critical need for an effective and robust security strategy. This response plan outlines a comprehensive approach to mitigate current risks and prevent future incidents. The plan focuses on key areas, including risk assessment, network hardening, employee training, and incident response.

Risk Assessment and Mitigation:

- Conduct an Opensource Intelligence Assessment of the webpage and a Vulnerability Scan on public IP.

- Compile findings into a risk assessment report, considering Physical (P), Digital (D), and Informational (I) assets.

- Develop a remediation plan based on risk assessment, including revised network architecture and firewall rules.

Network Architecture and Firewall Rules:

- Design a revised network architecture diagram with supporting rationale, incorporating at least one edge device with a firewall.

- Recommend firewall rules to balance security and operational needs. Provide evidence of testing in packet tracer.

Employee Training:

- Develop a comprehensive training plan addressing various topics, with a focus on phishing.

- Define training frequency, target audience, and KPIs to measure compliance.

Phishing Simulation:

- Provide a phishing simulation plan for the first year, including an example simulation.
- Explain the rationale behind the simulation, its target, type, outcomes, and key elaboration points.

Asset-Specific Threat Response:

- Select one asset (e.g., Cloud Server) and identify a credible threat.
- Develop a response plan detailing actions to mitigate the threat and safeguard the asset.

By implementing these measures, THISISAFAKECOMPANY aims to strengthen its security posture, ensuring the protection of physical, digital, and informational assets against potential threats. Regular assessments, training, and simulations will contribute to a proactive and resilient cybersecurity environment.

Name: Victor Obiora

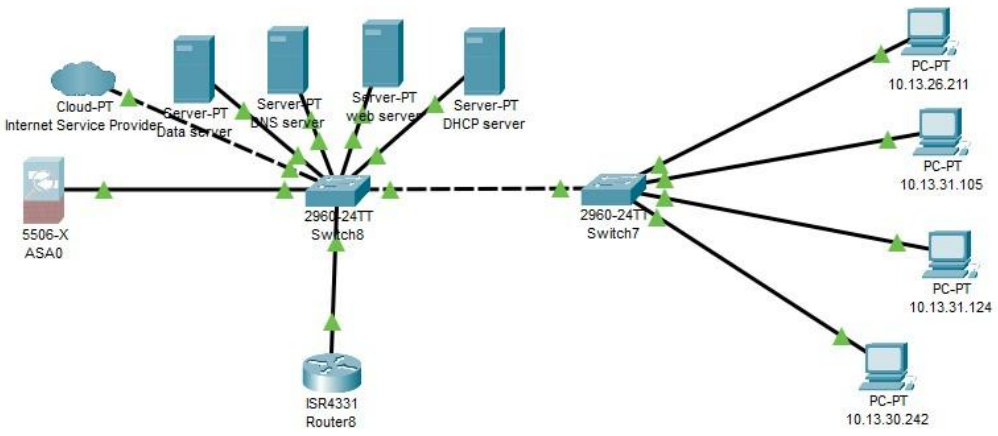
In response to the incident on December 5, 2023, THISISAFAKECOMPANY is committed to enhancing its cybersecurity measures and ensuring the protection of its assets. The following response plan outlines hypothetical scenarios, potential impacts, and recovery methods for identified assets, along with assigned responsibilities.

ASSET	HPOTHETICAL SCENARIO	POSSIBLE IMPACT	METHODS OF RECOVERY	RESPONSIBILITY
Cloud Server	Malware compromise leading to data exfiltration.	Data loss, reputational damage, legal consequences.	Isolate affected server, conduct forensics, restore from backup.	IT Security Team
Staff	Phishing attack leading to credential theft.	Unauthorized access, data manipulation.	Educate staff on phishing, enforce strong password policies.	HR and IT Security Team
IT infrastructure	Malicious code execution on servers.	Disruption of services, data integrity compromise.	Implement firewall rules, conduct vulnerability scans, patch vulnerabilities.	IT Operations Team
Data security measures	Compromise of encryption keys.	Unauthorized access to sensitive data.	Update encryption protocols, monitor key usage, implement multi-factor authentication.	IT Security and Data Governance Team
User trust	Loss of trust due to phishing emails.	Reduce employee confidence, and reputational damage.	Conduct cybersecurity awareness training, implement email filtering.	Marketing and IT Security Team

Table 4: Response plan outline including possible scenarios and methods of remediation for major

9 Network Architecture Diagram

Below is a revised network architecture diagram which shows the visual representation of THISISAFAKECOMPANY's physical and logical network structure and how the data flows throughout the system



The network diagram showcases four hosts, labeled as PC-PT, each with a unique IP address. These hosts, which are the company's computers, are used by employees or end users to access network services.

The network also includes six servers, namely Data Storage, DNS, Web, and DHCP servers. These servers provide essential services like file sharing, email, web hosting, and database management.

Two routers, labeled ISR4331 and 2960-24TT, are present in the network. They route traffic between different networks or subnets, ensuring connectivity among hosts, servers, and other network devices, as well as between the internal network and the Internet or other external networks.

Lastly, a firewall, labeled 5506-X ASA, is strategically positioned to filter traffic from an external cloud service provider. This security device restricts network access and protects against unauthorized access or attacks. It can be configured to restrict or allow specific types of traffic based on the network administrator-defined rules and policies.

10 Firewall Rules

In response to the recent cybersecurity incident, THISISAFAKECOMPANY is implementing stringent firewall rules to safeguard its network infrastructure. The firewall rules outlined below aim to establish a robust defence mechanism against potential threats while ensuring seamless business operations. The rules are designed to regulate incoming and outgoing traffic, prevent unauthorized access, and protect sensitive data from compromise.

Rule 1: Restrict Incoming Traffic
- Allow only essential incoming traffic on designated ports.
- Deny all incoming traffic from unknown or suspicious IP addresses.

Rule 2: Outbound Traffic Monitoring
- Regularly monitor and log outbound traffic to detect unusual patterns.
- Block outgoing connections to known malicious IP addresses.

Rule 3: Application Layer Filtering
- Implement deep packet inspection to scrutinize the content of incoming and outgoing traffic.
- Block specific applications and protocols that pose a potential security risk.

Rule 4: VPN Access Control
- Allow VPN connections only from authorized devices and users.
- Block unauthorized VPN access attempts.

Rule 5: Intrusion Prevention
- Enable intrusion prevention mechanisms to detect and block suspicious activities.
- Regularly update intrusion detection signatures to stay ahead of emerging threats.

Rule 6: Deny by Default
- Adopt a default-deny stance for incoming and outgoing traffic.
- Allow only explicitly permitted traffic based on organizational needs.

By implementing these firewall rules, THISISAFAKECOMPANY aims to strengthen its network security, safeguard critical assets, and prevent future cybersecurity incidents. Regular testing and updates will be conducted to ensure the effectiveness of these rules in maintaining a secure and resilient network environment.

11 12 Month Security Plan

In response to the recent cybersecurity incident, a comprehensive 12-month training plan has been developed to empower employees with the knowledge and skills necessary to enhance the company's security posture. The plan focuses on various topics, including phishing awareness, and is tailored to specific roles within the organization.

Training Topic	Goal/Description	Frequency	Key Performance Indicator	Target Audience
Phishing Awareness	Recognize and avoid phishing attempts	1st Quarter	Phishing Simulation Results, Completion Rates	All Employees
Password Security	Strengthen password practices	2nd Quarter	Password Policy adherence	All Employees
Malware Defense	Identify and mitigate malware threats	3rd Quarter	Incident Response Time	IT Operations Teams
Social Engineering	Improve awareness of social engineering tactics	1st Quarter	Employee Reporting Rates	HR & Management
Data Protection	Ensure proper data handling and protection.	1st & 4th Quarter	Compliance with Data policies	Data Handling Team
Network Security Basics	Enhance knowledge of network security	2nd & 3rd Quarter	Successful implementation of Firewall Rules	IT Team

Table 5: Categorization of training plan

This training plan aims to build a security-aware culture within THISISAFAKECOMPANY, reducing the risk of future incidents and fostering a proactive approach to cybersecurity across all levels of the organization.

12 Training Session Outline

Phishing poses a significant threat to THISISAFAKECOMPANY's cybersecurity. The following guideline outlines a 12-month plan to combat phishing, focusing on employee education and continuous improvement.

Month 1: What is Phishing?
- Provide introductory training on recognizing phishing emails.
- Simulate basic phishing attacks to assess employee awareness.

Month 2: Principles of Influence
- Educate employees on recognize and resist phishing tactics.
- Conduct realistic phishing simulations with evolving techniques.

Month 3: Types of Phishing
- Give employees an overview of the various types of phishing.
- Conduct exercises that where they have to identify the right type of phishing tactic used.

Month 4: Social Engineer
- Explaining social engineering
- Conduct realistic phishing simulations with evolving techniques.

Month 5: Speat Phishing
- An in-depth session on spear phishing and how they are conducted.
- How to protect yourself from spear phishing attempts.

Month 6: Whaling
- Under standing and identifying whaling emails
- Identifying the principles of influenced used in the whaling exercises

Month 7: Smishing
- Educate employees on threats posed on SMS messages.
- Conduct realistic smishing simulations to avoid falling for deceptive SMS messages.

Month 8: Vishing

- Explaining vishing attacks.
- Conduct scenarios on vishing.

Month 9: Email spoofing
- Demonstrations of spoofing attacks.
- Conduct activities on spoofing.

Month 10: Incident response
- Educate employees on what to do in a case that you were phished
- Conduct realistic phishing simulations requiring them to identify, analyze, mitigate phishing attacks and the recovery process.

Month 11: Reporting and Incident Response
- Emphasize the importance of reporting suspicious emails promptly.
- Simulate incident response scenarios to test reporting mechanisms.

Month 12: Continuous Improvement & Final Assessment
- Analyze data from previous simulations to identify areas for improvement.
- Provide refresher training and incorporate lessons learned.
- Conducting a simulation assessment that encompasses everything learned in the entire year.

This guideline aims to create a resilient defense against phishing attacks through continuous education, simulation, and improvement, ensuring employees remain vigilant and adaptive to evolving threats.

13 Simulation Email Test Outline

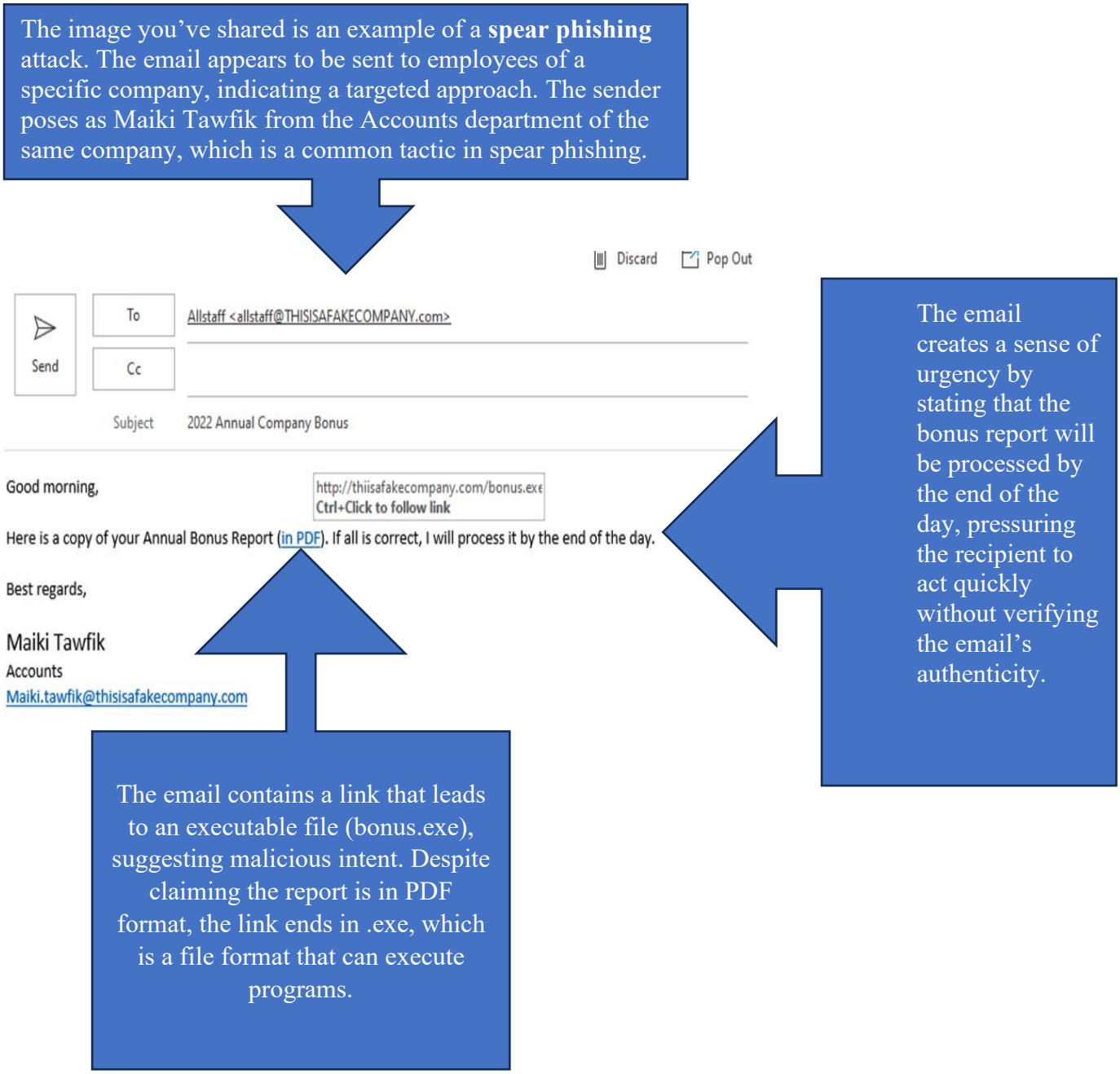
Simulation email tests are essential to assess and improve employees' ability to recognize and respond to phishing threats. The outline below provides a structured approach for conducting realistic phishing simulations.

Simulation Email Test Outline:

1. Develop a realistic phishing email mimicking recent incidents.
2. Tailor scenarios to the training topics covered each month.
3. Include elements of social engineering, spear phishing, and other tactics.
4. Ensure the simulation is non-disruptive to daily operations.
5. Collect data on employee responses for analysis.
6. Provide immediate feedback and guidance for improvement.
7. Incorporate lessons learned into subsequent simulations.
8. Conduct periodic surprise simulations to maintain awareness.

This comprehensive approach aims to create a resilient cybersecurity culture within THISISAFAKECOMPANY, fostering continuous improvement and adaptability to evolving threats.

14 Phishing Simulation example



The simulation above shows an example of a phishing email which was sent by threat actors pretending to be Maiki Tawfik who is the HR Manager after hacking into THISISAFAKECOMPANY's email system. This can serve as a reminder to the employees, to always verify the sender's identity and be cautious of email links, especially those leading to executable files.

15 Summary

THISISAFAKECOMPANY, a leader in corporate environmental consultations, recently experienced a security breach initiated through a deceptive email on December 4, 2023. The incident involved unauthorized attempts to access the company's network. The response plan includes an Opensource Intelligence Assessment, Vulnerability Scan, network architecture redesign, and firewall rule implementation.

The Opensource Investigation revealed vulnerabilities in the leadership team's online presence, particularly on Discord, which could expose the company's plans and operations. The Vulnerability Report identified several weaknesses, including unsupported PHP versions, Apache vulnerabilities, and unencrypted services. The Risk Assessment outlined potential risks and asset-specific threat responses.

A revised Network Architecture Diagram was presented, emphasizing routers, servers, and firewalls to enhance security. Firewall Rules were proposed to regulate incoming and outgoing traffic, emphasizing strict control measures. A 12-Month Security Plan focused on employee training, phishing simulations, and asset-specific threat responses.

The Training Session Outline outlined a year-long plan covering phishing awareness, principles of influence, types of phishing, social engineering, and incident response. A Simulation Email Test Outline provided a structured approach to realistic phishing simulations, aiming to continuously improve employees' ability to recognize and respond to threats.

In response to the incident, THISISAFAKECOMPANY is committed to strengthening its security measures, protecting assets, and fostering a security-aware culture through comprehensive training and proactive cybersecurity strategies.