ENPM 686 – INFORMATION ASSURANCE

FINAL PROJECT

ENHANCING DEATHSTAR'S SECURITY

BY:

PRACHI OZA (118118147)

&

OM VENUGOPAL (118116655)

TABLE OF CONTENTS

SECTION 1: IMPROVING DEATHSTAR'S SECURITY POSTURE

DeathStar, Incorporated is an organization specializing in planetary weaponry under the watchful eye of Emperor Palpatine. Despite the specialization in defense, the company has been under a constant barrage of cyberattacks for over one year. Attacks such as spear phishing, ransomware and DDOS have brought the essential operations of the organization to a halt.

Please note that any assumptions made will be declared in the section where it is being referred as is necessary.

1.1 The Current Network Setup

Now, to further understand the exact issues and consequently provide an appropriate and exact solution for each defined issues, the current setup and assets of the organization must be understood.

As of this moment, we possess an on-premise datacenter with a primary and failover mainframe- both present in the same physical space. The presence of a failover mainframe at the very least helps mitigate the adverse effects of all the attacks the organization has been facing.

We also have a locally hosted web server for the purpose of advertisements and sales as well as a network of Linux and Windows computers. Hosting a server locally within the organization premises would ensure that the administrators would be able to have a more streamlined control over it along with ascertaining more privacy. These might have proved to be some sort of advantages during the security incidents.

Additionally, a Layer 2 firewall has also been installed to add an extra layer for verification. The firewall, although only operating on the 2nd layer of the OSI model, would prove to be some sort of enhanced security to the organization.

Finally, as a new initiative, the emperor had also issued various laptops to many company personnels in order to allow work from starship incentives.

While there are some basic security initiatives taken by the security team, these clearly need to improved upon for stronger security.

1.2 Recent Challenges

Ransomware attacks and DDOS (Distributed Denial of Service) attacks have rendered three out of the five total machines of organization unrecoverable. This poses to be quite a huge a loss to the company as it would reduce productivity, reduce the total number of assets of the company as well as resulting in many projects coming to a total halt- which would have financial repercussions.

Not to mention that since these machines were seized by a ransomware, the sensitive data on these machines would be leaked on the internet by the attackers.

1.3 Defining Goals

To ensure that we are able to present a well-suited security solution for the organization, goals must be defined very clearly- these help us understand the exact requirements for the organization and determine a course of action. We propose a mix of those already mentioned by the Emperor along with ones that we deemed necessary.

Firstly, attacks that cannot be prevented must be detectable. This basically comes under damage control; if an attack has successfully allowed breach of security, then this should be detected as soon as possible so that the security administrators may take quick action to eradicate this threat actor.

Secondly, the company network needs to be made more secure in order to try and prevent attacks in general. This should be a basic feature of the new security structure; the best possible attempts must be made in order to scan and detect attacks.

Thirdly, if an attack remains undetected, then there must be measures set in place to tolerate it. This implies that even if an attacker is able to gain unauthorized access to a system, they should remain unable to take advantage of this situation and steal data or modify any data.

Additionally, a secure communication must be established between all company devices- this helps ensure that it would be very unlikely to compromise multiple machines altogether because of one fault point.

Moreover, regulatory requirements must be met. Compliance is an extremely important part of any secure system; all the security solutions proposed must be in accordance to the appropriate policies.

Finally, the security administrators must set in place a quick response plan in order to fight off any attacks; appropriate personnel must be identified who can be called upon in such an event.

SECTION 2: CURRENT STATE OF DEATHSTAR'S SECURITY POSTURE

To assess the kind of security solutions that need to be in place, it is imperative to also understand what the exact issues are and what malpractices actually let these attacks succeed in the first place. Now, an organization's security posture speaks volumes about the problems that need to be addressed; it collects solutions for data and network security, vulnerability assessments as well as employee training which would eventually help enforce proper security.

As the security posture weakens, the chances for a cybersecurity risk increase. The current security posture of DeathStar, Inc. is very weak. There are constant DDOS attacks on the client login portal and encryption remains disabled due to outdated equipment. As already established, no secure communication has been created, it is very likely that an attacker can easily read all the packets going to and from the company network.

2.1 Vulnerabilities Likely Exploited

Based on the data provided within the scenario document, we can deduce that the following weaknesses would have been exploited by the attackers in order to perform successful ransomware and DDOS attacks on the network:

- Outdated equipment. Essential equipment such as the primary and failover mainframes are not up to date or up to regulation standards. These can lack the latest security features and software patches, thus leaving open-ended and unresolved exploits still active which could eventually be exploited by the attackers in order to gain unauthorized access to sensitive data and such.

- Unpatched software. As highlighted in the point above, unpatched software within mainframes and servers can lead to exploitable weaknesses still remaining in the system.

- Storage of sensitive data unencrypted. As a firm geared towards defense and planetary weaponry, it would not be a hidden fact that they would store and transit very important data- these could range from high-end clientele's data to schematics of dangerous weapons. All of this data is stored within the firm unencrypted, implying that any ransomware gang would not even need to put in efforts to decrypt the data- they would easily obtain it in plaintext. Not to mention that the absence of secure communication between devices can allow attackers to gather all transmitted packets and read them in plaintext.

- Weak network perimeter security. The firewall that has been installed is only applicable to Layer 2 of the OSI model (i.e., the data link layer)- this would not extend security toward the network and application layers of the model wherein most attacks are targeted vis-a-vis the malware/ransomware attacks and DDOS attacks. A firewall of such a type would allow attackers to bypass the external security safeguarding the network and let them gain unauthorized access to the systems within the network.

- Lack of logging. As the equipment used in the firm is outdated, it can be safe to assume that logging is not done properly. A lack of logging system indicates that the security personnel cannot quickly detect the series of actions that actually led to the attacks. This way, they would not even be able to monitor what steps were taken that led to unauthorized access. Additionally, it would also be difficult to detect this attack beforehand as constant monitoring of system and network logs would not be occurring.

- Improper network segmentation. Given the lack of strong perimeter security, it would not be unlikely that the network has not been segmented appropriately. Network segmentation includes isolation of the network into smaller ones- this allows for fault isolation. If one of the segments is compromised, then it would likely take a large amount of time to affect other network segments, given that secure communications have been established first.

- Lack of employee training and awareness. Employee training is one of the most important lines of defense in cybersecurity. Successful spear phishing campaigns indicate that DeathStar's staff has not been trained in possible attacks and methods to avoid and report these to the correct department.

It is safe to say that many more issues would be present- as a direct consequence of the above highlighted issues or a completely different one.

2.2 Consequences

Every action has a consequence- inaction also has its consequences. Due to the weaknesses present in the overall security structure, there have been a lot of challenges that the organization has to face.

Of the five machines infected by ransomware, three were left unrecoverable. This caused a massive dent in the assets owned by the company, subsequently leading to a steep decline in productivity and meeting of project deadlines.

When attacks such as these occur, the company would have to disclose the details to the affected customers and users at some point- this would cause a loss of trust in the organization by current as well as potential users. If the company's total number of clients decrease, there would be a surplus of unsold products leading to monetary issues. Not to mention that the time and effort invested by the engineers of the company would also be wasted.

Finally, many clients may choose to sue the company over the damages they had to incur which would cause legal issues.

SECTION 3: RECOMMENDED SOLUTIONS

The subsequent subsections will explain each solution we have proposed in detail along with example products provided for each.

3.1 Upgradation of Network Security

It has already been established that the network infrastructure of the organization is fairly weak and unable to deter any incoming attacks. Upgrading the network security by ensuring that the below points have been enforced will greatly improve the overall security of all systems.

3.1.1 Implementing a Layer 7 Firewall

Now, layer 2 firewalls have very limited capabilities when considering higher-level protocol awareness and packet inspection. These only perform packet filtering based on MAC addresses.

We recommend implementing a layer 7 firewall in place of the layer 2 firewall. These operate at the application layer of the OSI model and inspect incoming traffic at the application level; they provide far more security and can even detect as well as prevent application later attacks such as DDoS attacks, SQL injection attacks, etc. Despite them being termed as application-level firewall, they actually secure not only at the application level but also the network and transport layers.

The upgraded firewalls will also be able to perform in-depth analysis of incoming packets and enforce security policies as defined by the administrators. Additionally, it also ensures that any anomalies in the network are detected and enforces compliance.

The layer 7 firewall can be deployed along the network perimeter to enforce packet inspection on packets coming and going out of the network. It can also be deployed between internet-facing components and internal servers/mainframes- this will help ensure that backups or customer data would not be compromised.

Alternatively, the company may also choose a Next Generation Firewall over a Layer 7 as they also provide anti malware, intrusion prevention and Virtual Private Network (VPN) capabilities. Although, we believe that a Layer 7 firewall would be much more fitting for the company's current requirements.

3.1.2 Implementing Intrusion Detection & Prevention Systems

One of our goals was that unpreventable attacks should at least be detected- now, this has two parts to it. An intrusion detection system (IDS) would help try detect any attacks that could not be prevented and an intrusion prevention system (IPS) would help prevent any attacks.

The IDS is a key element in monitoring network traffic- it raises and sends alerts to the staff that is responsible for managing it. They will be able to deal with the anomaly as quickly as possible which will definitely safeguard the system against the type of attacks that the organization has been suffering from.

The IPS will ensure that attacks are prevented. While the IDS helps detect attacks *after* they have entered the network, the IPS will prevent attacks *before* they infect the organization's systems. Moreover, these systems will also aid auditing processes in the event of a successful breach or a failed attack attempt.

3.1.3 Enforcing Access Control

Access control is extremely important- spear phishing campaigns target employees, so by having access control we can ensure that even if one employee's credentials or machine is infected, the entire organization's security would not be jeopardized.

Additionally, we also believe that access control would be extremely useful when trying to tolerate undetected attacks.

Access control can be implemented in many ways, such as:

- Implementing multi-factor authentication. Making use of employees' distinct features such as their fingerprints, or particularly generated access codes, in addition to their own created passwords would greatly strengthen security. This is to ensure that no threat actor can pretend to be a legitimate employee to gain access to the system.
- Enforcing role-based access control. In our opinion, this method should strictly be enforced- resources should only be available to employees based on their job responsibilities. This can be deployed via specific operating system functionalities.
- Implementing network access control. NAC helps ensure that access to the network is limited and based on a user's profile, identity and device type. This performs device profiling along with isolation capabilities which could prove to be extremely useful in the event of a malware or ransomware attack.
- Compliance with various access control policies. Enforcing compliance makes sure that the mechanisms put in place for access control are all up to standard. NIST's Cybersecurity Framework Policy Template Guide can be referred to; the PR.AC-1 subject defines some access control policy techniques that can be used.
  Moreover, policies such as 'Principle of Least Privilege', 'Zero Trust Approach' and 'Just-in-Time Access' will only further strengthen the access control implemented within DeathStar, Inc.

3.1.4 Establishing Secure Communication

It is known that the company has a network of Linux and Windows devices for research and administrative purposes respectively. A proper and secure communication needs to established between each device within a network as well as inter-network.

To achieve this, we suggest making use of protocols such Secure Copy (SCP), Secure Shell (SSH) and Secure File Transfer Protocol (SFTP/FTPS). SCP will make sure that files are copied securely between each device while making use of SSH to enforce encryption on the files. The SFTP protocol, on the other hand, will ensure secure file transfer between all devices using SSH; FTPS will perform the same task but over the TLS/SSL protocol.

Also, implementing a Virtual Private Network (VPN) that supports all operating systems will prove to be very beneficial in creating a secure communication as it can be used for creating tunnels that can establish encrypted communication when interacting with the Internet.

3.2 Upgradation of Endpoint Security

It is imperative to ensure the security of each individual device that is the property of DeathStar, Inc. Endpoint security helps achieve this; the following methods can be put in place:

- Installing a renowned and licensed anti-malware or antivirus software on all devices. These can help detect attacks on individual devices as well as raise alerts if needed.
- Establishing a proper patching and backup strategy. As is known, the equipment used in DeathStar, Inc. is outdated. By employing a patching strategy, security updates would regularly be applied on each machine and software.
  Also, backup procedures should be done regularly- especially for critical and highly sensitive data. Testing and verification of each backup must be done so that that data can be restored to resume operations in the event of an attack that leaves machines unrecoverable.
- Implementing encryption technologies. As data related to defense and weaponry is considered to be highly sensitive, proper encryption techniques must be enforced in the appropriate sections. Each endpoint should have full-disk or at the very least, file-level encryption enforced.

3.3 Hire Additional Staff

The newly hired security administrators can help provide a fresh perspective on the events that have been occurring and suggest implementations of various techniques and tools that can help safeguard the DeathStar, Inc.’s system.

Additionally, increasing the security team’s staff would help ensure that any potential incident is dealt with as quickly and properly as possible.

3.4 Employee Security Training

All employees should be regularly trained on recent security events and techniques. These sessions can help educate them on common threats, best practices as well as methods to safeguard themselves against social engineering attacks. Employees will understand how to report and identify any suspicious links or emails or files that they receive.

3.5 Security Assessments and Penetration Testing

As security is an ever-evolving field, regular vulnerability assessments must be performed to ensure that all systems are appropriately safeguarded against any new attack methodologies. We recommend doing this on a yearly basis, as a start.

Penetration tests on all devices and machinery that makes use of software can identify all possible weaknesses and entry points for attackers; the found vulnerabilities can then be addressed quickly and required product changes can be made as necessary.

3.6 Securing the Web Server

It has also been mentioned that DeathStar, Inc. makes use of a locally hosted web server to sell products; while no risks have been reported concerning this, we have still provided some fixes that can be incorporated to make it more secure.

- Proper coding practices. Developers must ensure that proper coding practices have been undertaken while creating web applications that are hosted on the server. We recommend regular code reviews and tests must be undergone in order to ensure that the web server remains vulnerability-free.
- Secure server configurations. While configuring servers, only the best possible settings must be considered that secures the servers according to the best industry standards and practices. Security updates must be downloaded and installed as they are released.
- Enforcing SSL/TLS. As the web server would be in communication with numerous clients around the Internet, SSL/TLS must be enforced upon the same. A valid SSL/TLS certificate

should be obtained and installed from a trusted certification authority. Additionally, also ensure that HTTPS is enabled.

- Access control and password practices. The administrative interface of the web servers must be strongly secured using proper access control and password practices. RBAC can be used here to ensure that only certain personnel can access these interfaces.
- Log monitoring. As with any equipment in an organization that is Internet facing, logs should constantly be monitored for any anomalies. There can be trusted third-party tools or software that can be used to browse through such large data but we recommend that the employees do so manually and focus on only the alerts and warnings generated.

Additionally, we must also mention that the organization must be PCI-DSS compliant at all times when conducting business that requires any type of online payment to be done by their clients. The 'Payment Card Industry Data Security Standard' is required and endorsed by all credit card companies as well as payment processing banks and companies. This standard ensures that any credit/debit card details entered by the customer remains safe and secure.

This compliance must be verified on a regular basis; failure to have a valid PCI-DSS compliance may lead to a huge fine that the company has to pay.

3.7 Other Comments

Our assumption is that the organization comprises of 150 employees- more or less. In our opinion, we do not believe it is necessary to migrate to the cloud as of yet- this should be a very gradual process as it can lead to a complete overhaul and confusion within employees if not done in a stepwise manner.

In the near future, as the organization's size and operations increase, we recommend migrating to the AWS cloud- they provide a multitude of features along with an extensive list of thoroughly explained manuals for each service. Separate planning and analysis will need to be done to determine how this can be achieved.

Besides that, we also recommend that the failover mainframe be shifted to another physical location altogether with its separate network. Doing this will ensure that any attacks on the

primary mainframe or the main network will not corrupt the backups or data stored on the other mainframe.

Finally, we have also considered risks associated with insider attacks. To eradicate these, extensive background checks must be performed on all employees before they are fully hired. Access control will also greatly decrease risks associated with this.

SECTION 4: BUDGET CONSTRAINT

We have mentioned many security solutions that should be enforced to ensure the security of the company. A budget constraint of $700,000 was established by Emperor Palpatine which has influenced our list of recommended products to select from.

Assuming the company has 150 employees, each with a company issued laptop we make two suggestions based on the budget that was provided. But first, we establish some common costs associated with each option.

- Salary for 2 additional security staff: $125,000 per person.
  Hiring two additional security staff members ensures dedicated resources to manage and monitor the organization's security infrastructure. These professionals will be responsible for implementing and maintaining security measures, responding to incidents, and proactively identifying vulnerabilities.

- Conduct regular security assessments and penetration testing: $10,000 - $50,000 per assessment. Specific pricing details are provided within each option.

4.1 Option 1

- **Firewall**: Palo Alto Networks - $30,000 - $50,000.
  Palo Alto Networks is a reputable and robust firewall solution known for its advanced features and effective threat prevention capabilities. It provides granular control over network traffic, allowing the organization to define and enforce security policies.

- **IDS**: Snort Intrusion Detection System - Open source.
  Snort offers real-time traffic analysis and detection of malicious activities. It helps in identifying and responding to potential threats promptly.

- **Access Control**: Duo Security - $3 - $5 per user per month: $9,000 per year.
  Duo Security offers multifactor authentication (MFA) solutions, which add an extra layer of security to verify user identities. This helps the organization significantly reduce the risk of unauthorized access and protect sensitive data.

- **Endpoint security**: McAfee Endpoint Security - starts at $35 per device per year.
  McAfee Endpoint Security provides comprehensive protection for endpoints, including antivirus, anti-malware, and advanced threat detection. It helps prevent and detect potential threats on individual devices, safeguarding them from malware attacks.

- **Provide employee security training**: SANS Security Awareness Training - estimated cost: $25 per employee per year, totaling $3,750 per year.
  Employee security training is critical for instilling a security-conscious culture throughout the organization. It may dramatically reduce the risk of human error and insider threats by training staff on cybersecurity best practices, common risks, and how to respond to them.

- **Conduct regular security assessments:** Hire a third-party security consulting firm - estimated cost: $20,000 per assessment (annual assessment recommended).
  Regular security audits and penetration testing are essential for identifying vulnerabilities and flaws in an organization's systems. The organization can correct security gaps and prevent potential breaches by undertaking these evaluations.

So, the total budget for our first option comes out to be: -

Firewall ($50,000) + IDS (no additional cost) + Access Control ($9,000) + Endpoint security ($7,875) + Employee training ($3,750) + Security assessment ($20,000) + Salary for 2 additional security staff ($125,000 x 2) = $90,625 + $250,000 = **$340,625.**

4.2 Option 2

- **Firewall**: Fortinet FortiGate Next-Generation Firewall - $40,000 depending on the model and subscription.
  Fortinet FortiGate is a highly regarded next-generation firewall solution that offers advanced security features, including threat detection and prevention, application control, and VPN capabilities.

- **IDS**: Suricata - Open source.
  It is an open-source IDS that provides real-time network traffic monitoring and intrusion detection capabilities.

- **Access Control** - Okta Identity Management - Estimated cost: $5 per user per month. Total cost: $9,000 per year.
  Okta Identity Management offers comprehensive access control solutions such as single sign-on (SSO), multi-factor authentication (MFA), and user lifecycle management. It can improve access security and streamline user management operations by deploying Okta.

- **Endpoint security** - Symantec Endpoint Protection - starts at $30 per device per year, estimated total cost for 150 devices $6750.
- **Provide employee security training**: Infosec IQ - estimated cost: $20 per employee per year, totaling $3,000 per year.
  Employee security training is critical for instilling a security-conscious culture throughout the organization. It may dramatically reduce the risk of human error and insider threats by training staff on cybersecurity best practices, common risks, and how to respond to them.

- **Conduct regular security assessments**: Hire a third-party security consulting firm - estimated cost: $20,000 per assessment (annual assessment recommended).
  Regular security audits and penetration testing are essential for identifying vulnerabilities and flaws in an organization's systems. The organization can correct security gaps and prevent potential breaches by undertaking these evaluations.

So, the total budget for our second option comes out to be: -

Firewall ($40,000) + IDS (no additional cost) + Access Control ($5,400) + Endpoint security ($6,750) + Employee training ($3,000) + Security assessment ($20,000) + Salary for 2 additional security staff ($125,000 x 2) = $75,150 + $250,000 = **$325,150.**

Both our proposed options are well under budget; we have recommended the best and most economical products the company can use to regain its security stature. We believe that the extra funds may be used for further upgrades, additional equipment purchasing or for any unforeseen circumstances.

SECTION 5: BENEFITS OF RECOMMENDED SOLUTIONS

Highlighting the benefits of enforcing the recommended solutions will help make an informed decision. To begin with, the organization will have their operations, equipment and processes running according to the latest industry standards, which will greatly reduce risks of legal issues and regulatory issues.

The network security infrastructure would be strengthened with endpoint security enforced to keep all company devices safe. Moreover, our recommended solutions also comprise of detection and prevention systems which are crucial in order to deter ransomware and DDoS attacks.

Of course, network disruptions that can result from an ongoing attack would greatly be reduced thus improving business continuity as well as reducing downtime- which can affect the reputation of the company.

As our endpoint security solution mentions implementing backup and patching strategy, there would be very few services and operations interruptions thereby regaining customers' trust in the company. This will also ensure that all IT operations will be much more efficient and streamlined.

Secure communications between devices will increase collaboration and communication between separate teams, devices, and departments within the organization.

Finally, as attacks will mostly be prevented or detected and dealt with, the costs associated with recovering from them will also be reduced as the proposed solutions would take care of most of the issues.

SECTION 6: IMPLEMENTATION PLAN

In this section, we propose an implementation plan for the security solutions we have proposed- it can be considered as a 'timetable' of sorts that can be used by the security team to efficiently complete all the tasks required to get on par with an up-to-date security infrastructure.

6.1 The Plan

Firstly, a quick security roadmap should be created that would help all personnel within the security team understand what is to be completed and by whom. Additional security staff can be hired next so that the following process goes by much quicker and smoothly.

The main issue with DeathStar, Inc.'s security stature is that its existing network infrastructure is weak; the security solutions we proposed to strengthen the network should be implemented before any other fixes are performed. This will ensure that the company will be safe from outside attacks while other technologies such as the intrusion detection system and access control are being implemented.

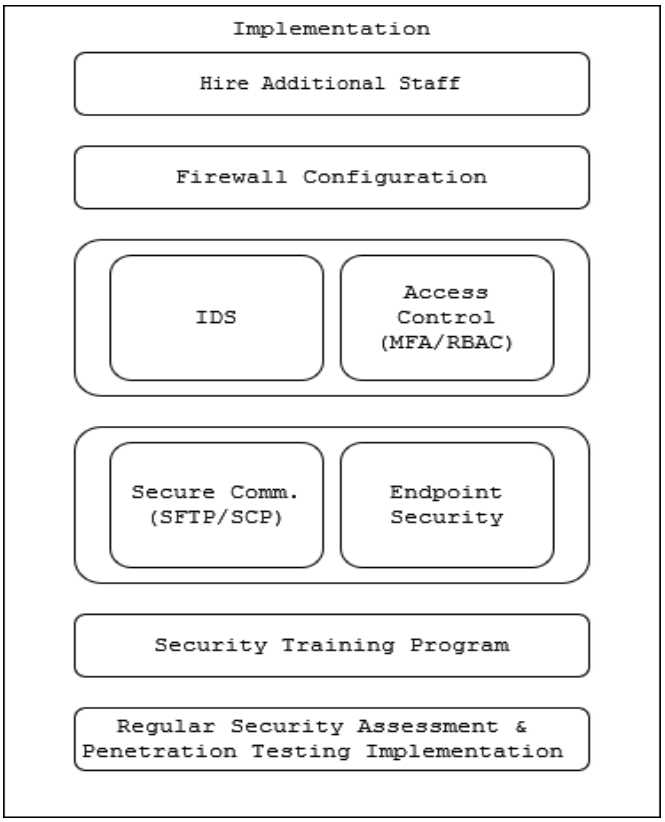
Once the network infrastructure has been recovered, we can then proceed onwards to implement access control and the intrusion detection (& prevention) system as these are imperative when considering avoidance, prevention and detection of attacks.

Of course, as the company comprises of various devices that employees can make use of to complete tasks, we recommend creating a secure communication within each of these networks next. This should naturally be followed by the implementation of endpoint security- to assure that the established secure communication lines are not compromised due to individual endpoint devices. Additionally, endpoint security would also extend to company issued laptops that employees can take home- thereby successfully eradicating the risk factor associated with the same.

Once the new security procedures, policies and equipment are put in place, the employees can then be provided with ample training to help educate them on security issues and procedures.

Finally, to ensure that the company remains free of threats and weaknesses, regular security assessments and penetration testing should be performed. Any findings reported must be dealt with as quickly as possible.

The image below provides a diagrammatical insight into our implementation plan that can further be used and elaborated upon by the designated officials as the need arises. The distribution of this can be broken down into a weekly plan as well.



6.2 Concerns and Challenges

It is natural that with such significant changes in the organization, challenges are bound to arise. We have identified some that can be used to effectively eradicate the problems beforehand.

- Resistance to change. Any new change amongst previously used software and procedures can raise concerns within employees. They may be resistant to changes in their routines and the devices they make use of. To address this, a quick training and guidance to those who are unable to understand it can alleviate the issues.
- Compatibility problems. The new security solutions we have provided may clash with any software or device that is already present and essential to the company's operations. To ensure that this does not happen, we recommend that a proper compatibility analysis is performed by security administrators before anything is implemented.
- Issues with data migration. As three out of five machines targeted remain unrecoverable from the ransomware, the company may purchase additional devices to replace these; the migration of data from older devices to newer ones may prove to be time consuming and complex. To eradicate this problem, a migration plan can first be developed, and the necessary resources can then be allocated to ensure a smooth transition.
- Employee training. Training employees on different and complex procedures is never an easy task but this can easily be addressed by making use of online courses that the employees can complete at their time- within a set number of weeks- so that they can quickly get on track with the current situation.

SECTION 7: CONCLUSION

We strongly believe that our proposed security solutions would definitely prove to alleviate most of the concerns the organization has been facing. Due to the constant attacks DeathStar, Inc. has been facing since the past year, it is understandable that morale and operations might have noticeably slowed down. Therefore, implementing our solutions as quickly as possible may address a lot of concerns along the way.

But to ensure that the security infrastructure remains strong over a long period of time, employees must be trained on the basic security practices and the ways an attacker can perform social engineering to gain access to sensitive credentials.

SECTION 8: REFERENCES

- Fortinet. Intrusion Detection Systems. https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system
- Fortinet. (2021). FortiGate Next-Generation Firewall. https://www.fortinet.com/products/next-generation-firewall
- Offensive Security. (2021). Penetration Testing with Kali Linux. https://www.offensive-security.com/documentation/penetration-testing-with-kali.pdf
- Cisco Secure Firewall. https://www.cisco.com/site/us/en/products/security/firewalls/index.html
- Suricata IDS. https://suricata.io/features/
- Okta Identity Management. https://www.okta.com/pricing/
- Duo Security. https://duo.com/
- Symantec Endpoint Security. https://www.broadcom.com/products/cybersecurity/endpoint
- Cisco. Next-Generation Firewalls. https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html
- J. Fruhlinger, "PCI-DSS Compliance Explained". CSO. [Online] https://www.csoonline.com/article/3566072/pci-dss-explained-requirements-fines-and-steps-to-compliance.html
- CIS Security. NIST Cybersecurity Framework Policy Template Guide. https://www.cisecurity.org/-/jssmedia/Project/cisecurity/cisecurity/data/media/files/uploads/2021/11/NIST-Cybersecurity-Framework-Policy-Template-Guide-v2111Online.pdf
- R. Mohanakrishnan, "What is IDPS?". SpiceWorks. [Online] https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-idps/