**COURSEWORK SUBMISSION FORM**

|  |  |  |  |
| --- | --- | --- | --- |
| **STUDENT USE** | | **STAFF USE** | |
| Module Name | Information Security | First Marker’s  (acts as signature) |  |
| Module Code | 6COSCO16C | Second Marker’s  (acts as signature) |  |
| Lecturer Name | Nargiza Akramova | Agreed Mark |  |
| UoW Student IDs |  | **For Registrar’s office use only (hard copy submission)** | |
| WIUT Student IDs | 00010443 |
| Deadline Date | 06.06.2023 |
| Assignment Type | ☑ Individual |
| Word Count | 3048 |

**SUBMISSION INSTRUCTIONS**

**COURSEWORKS *must* be submitted in *both* HARD COPY (to the Registrar’s Office) *and* ELECTRONIC unless instructed otherwise.**

For hardcopy submission instructions refer to: <http://intranet.wiut.uz/Shared%20Documents/Forms/AllItems.aspx> - Coursework hard copy submission instructions.doc

For online submission instructions refer to: <http://intranet.wiut.uz/Shared%20Documents/Forms/AllItems.aspx> - Coursework online submission instructions.doc

|  |
| --- |
| **MARKERS FEEDBACK (Continued on the next page)** |
|  |

**Table of Contents**

**Executive Summary**  2

Pakistan Embassy 2

Organization’s objectives 2

**Analysis of the cyber-attack on Pakistan Embassy** 3

What was the occasion? 3

What factors contributed to the successful attack attempt? 3

Who were malicious actors and what was their incentive? 3

What type the attack can be classified as? 4

What were the attack vectors? 4

What was the financial/operational loss caused to the Pakistan Embassies? 4

Countermeasures 5

**Security Risk Management for the Pakistan Embassy** 5

Determining assets and corresponding threats 5

Risk Assessment 6

Risk Management Framework 6

**Adoption of Information Security Framework for Pakistan Embassy** 8

Critical Analysis of various Security Risk Management Frameworks 8

Challenges of NIST Adoption that Pakistan embassy may experience 10

**Conclusion**  10

**References** 12

**Executive Summary**

Pakistan Embassy

This work is conducted around DDoS attack on Pakistan Embassy websites conducted in April 2023. For the better understanding of the work carried out in this report background on Pakistan and its embassies’ activities and objectives is given down below.

Pakistan is the world's fifth-most populated nation and second-largest Muslim country by population; as such, it has a wide-ranging diplomatic network (Wikipedia, 2023).

Pakistan's diplomatic representation in the capitals of other Commonwealth nations is known as a High Commission. Pakistan is a member of the Commonwealth of Nations (Wikipedia, 2023).

Pakistan has established 137 embassies around the globe each of them serve crucial diplomatic mission to foster mutually beneficial relations with other nations and contribute to the reinforcement of the country (Pakistan Portal, 2023).

Organization’s objectives

The goals of foreign policy can be summed up as follows in light of the ideals established by the founding fathers and the constitution as well as the aspirations of the people of Pakistan:

- Presenting Pakistan as a vibrant, forward-thinking, moderate, and democratic Islamic nation.

- Establishing cordial ties with every nation, especially the world's superpowers and immediate neighbors.

- Protecting geostrategic interests, in particular Kashmir, and national security.

- Reinforcing Pakistan’s economic and commercial ties with the global community.

- Protecting the international interests of the Pakistani diaspora.

- Ensuring that national resources are utilized as efficiently as possible for regional and international collaboration (Ministry of Foreign Affairs, Government of Pakistan, 2018).

**Analysis of the cyber-attack on Pakistan Embassy**

What was the incident?

In April 2023, 10 Pakistan Embassy websites were paralyzed and stopped functioning due to wide-scale Distributed Denial of Service attack. The attack involved Pakistan Embassies in Germany, France, China, Algeria and others. Throughout all these websites the script “Feel the power of Indian hackers” was placed. Several well-known Pakistani Embassy websites, including pakmissionfrankfurt.de, pakconsulatela.org, and pakconsulateist.com, are on the list of domains that the Indian hackers have hacked.

What factors contributed to the successful attack attempt?

First and foremost reason for the attack success is advanced skillset and experience of Indian hacktivist group involved into the incident. Vulnerabilities of Information Security of the Pakistan Embassy websites is also to be assessed later in the report, but expertise of the malicious agents in this case cannot be neglected. From the online sources I made a conclusion that they received support from other hacker groups of India and operated not without assistance of the hacker network.

The following reason stems from proneness of digital infrastructure of Pakistan Embassy websites. The design of the web application did not envision this volume of requests and consequently did not have any protective mechanisms at the time of attack. I consider that request processing speed and capacity failed during the attack and no effective filtering through firewall was performed.

Affected websites were open to the enormous stream of unauthorized requests and their designed did not possess the capacity to deal with this stream, leaving them out of order.

Who were malicious actors and what was their incentive?

Malicious agents that acknowledged responsibility for the incident were Kerala Cyber Xtractors group that is notoriously famous hacktivist group of Indian origin (The Cyber Express, 2023). This group has also been previously recorded to conduct numerous large-scale cyber-attacks on various organizations. However, Pakistan embassy websites attack of April 2023 was one of their serious and prominent crimes. Kerala Cyber Xtractors remain anonymous till present days and are known to possess advanced skillset and remarkable speed of operating. From the posts made by this group it becomes obvious that they have established network and support with many other Indian hacker groups such as Unknown Cyber Cult, Indian Cyber Mafia, Black Dragon Security, United Indian Hackers and etc. (The Cyber Express, 2023).

Overall, motive for the attack is tense relations and ongoing political and religious conflicts and disagreements between India and Pakistan (Indian Defense Research Wing, 2023). In fact, there are series of cyber-attacks performed by hackers from both countries towards various state and private organizations and businesses of each other (The Cyber Express, 2023).

Indian hackers crippled 10 Pakistan Embassy websites worldwide in less than 24 hours after the Pakistani hacker group Team Insane PK claimed to have attacked 23 Indian government and commercial organization websites (Indian Defense Research Wing, 2023). In a statement posted online, they used the purported mistreatment of Muslims in Kashmir and India as justification for their actions. Targeted websites included the Ministry of Defense and high-profile institutions like the Indian Army, Navy, and Air Force (Indian Defense Research Wing, 2023).

Although the majority of Indian websites seem to be functioning normally, a deeper look reveals the attacks' long-lasting effects. DNS records and hosting statuses continue to show symptoms of infiltration, while error codes like "500" serve as a sign of the DDoS fought against them. Hence, the motive for this particular attack was a payback for the large-scale cyber-attack performed by Pakistani hackers earlier. However, I inferred that this attack was inevitable as cyber security turned into another battle field between two countries.

What type the attack can be classified as?

The attack was distributed temperature failure attack, according to reports by numerous sources (Indian Defense Research Wing, 2023). A distributed denial-of-service attack is a subclass of the more common denial-of-service (DoS) assault (Fortiguard Labs, 2021). An intentional attempt to disrupt a server, service, or network's normal traffic by flooding the target or its surrounding infrastructure with an excessive volume of Internet traffic is known as a distributed denial-of-service (DDoS) assault (Cloudflare, 2022). DDoS attacks are so effective and risky for the organizations because they use several compromised computer systems as sources of attack traffic. Machines can be used to exploit computers and other networked resources, such as Internet of Things devices (Cloudflare, 2022).

What were the attack vectors?

Taking into account that Pakistani hackers have often performed heavy DDoS attacks on Indian organizations before leaving noticeable signs on the web even after mitigation and resolving procedures, Pakistan Embassy websites had certain protection against DDoS attacks. Unfortunately, not much data is available regarding attack vectors of this particular attack due to its recent occurrence and political concerns.

From the factors listed above I concluded that attack vectors were of a sophisticated nature and strong affect such as Volumetric attack vector.

1. A huge volume of malicious traffic, including centralized DDoS mitigation scrubbing capabilities, was pumped into internal networks by malicious actors.

2. This application layer assault and volumetric DDoS attack involved sending fraudulent requests that caused a deluge of large reply packets to choke links and, in many cases, disable the target.

3. Weak services including SSDP, Memcached, NTP, and DNS were exploited.

4. The websites of the Pakistani embassy's network infrastructure were taken down.

5. The target network or service was attempted to consume up all available bandwidth, either within it or between it and the rest of the Internet.

What was the financial/operational loss caused to the Pakistan Embassies?

In this particular case there were many other losses apart from financial and operational ones, such as reputation and political status sabotaging.

As embassy is a governmental institution so the losses were born by Pakistan state. Following estimates were made by means of research, comparison and approximate assessment of the situation as information is extremely limited in this regard. Each firm will have a different downtime cost due to a DDoS attack. However, the majority of published estimates from industry surveys place the hourly losses incurred by a small- to medium-sized organization due to downtime in the range of $20,000 to 40,000 (Barney, 2022).

As for operational loss, this breach paralyzed 10 Pakistan Embassy websites in key partner countries that is a severe level of loss for the organization. Running Embassy websites and the institutions themselves include list of payments such as foreign taxes, employing IT staff, web page running services and many similar expenditures. The scope of the operational losses is presumably significant for the Pakistan state as they were experienced throughout 10 headquarters around the globe.

Countermeasures

It is known that institution made intense work right after the breach happened to restore the work of websites. However, following is the list of countermeasures that are applicable in the given situation:

* Detection

To stop a scattered attack, a website must be able to discern between an attack and a large volume of regular traffic. Historical data, typical attack tactics, and IP reputation can all help identify real attacks.

* Response

During the response phase, the DDoS prevention network should be able to accept the remaining traffic while simultaneously intelligently excluding known harmful bot traffic. The network can block the interruption by using WAF page rules for application layer or L7 attacks or another filtration technique for lower-level or L3 and L4 assaults.

* Routing

The remaining traffic should then be properly divided into manageable chunks using an effective DDoS mitigation technology before being intelligently routed.

* Adaptation

A good network should monitor patterns in the traffic, such as attacks from particular nations, offensive IP blocks that repeatedly appear, or wrongly used protocols. Security can be improved to thwart potential future assaults by being aware of attack trends and adapting accordingly.

This particular attack has a very unusual nature compared to a plethora of breaches happening every day in other organizations and businesses as it has political and religious background. Consequently, apart from technical countermeasures, regulating disagreements with opponents and refraining from further cyber wars should be considered.

**Security Risk Management for the Pakistan Embassy**

Determining assets and corresponding threats

Table (1)

|  |  |  |
| --- | --- | --- |
| № | Name of the asset | Name of the threat |
| 1. | Website | Distortion of webpage content, design and components, stopping it from functioning |
| 2. | Database | Database injection, breach |
| 3. | Search Engine Optimization | Unauthorized alterations |
| 4. | Paper and online documentation | Unauthorized access and distortion |
| 5. | Office equipment | Malware , hoax, theft, human error |
| 6. | Server | DDoS, DoS attacks |

**Risk Assessment**

Risk assessment metrics used in this work are depicted in the following tables:

Table (2)

|  |  |  |
| --- | --- | --- |
| Scale | Impact | Likelihood |
| 5 | Catastrophic | Almost certain |
| 4 | Huge | Likely |
| 3 | Moderate | Possible |
| 2 | Minor | Unlikely |
| 1 | Inessential | Rare |

Table (3)

|  |  |  |
| --- | --- | --- |
| Impact | Financial | Operational |
| Catastrophic (5) | >500k | Cancellation |
| Huge (4) | 100-500k pounds | Severe disruption |
| Moderate(3) | 50-100k pounds | Significant disruption |
| Minor (2) | 25-50k pounds | Requires correlative action |
| Inessential (1) | 25k pounds | Requires noting |

Table (4)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Asset | Website | Database | Search Engine Optimization | Paper and online documentation | Office Equipment | Server |
| Mode | Electronic | Electronic | Electronic | Physical and Electronic | Physical | Electronic |
| Value & Impact | 5 | 4 | 1 | 3 | 3 | 5 |
| Likelihood of the threats  Listed in the table(1) | 5 | 5 | 1 | 2 | 1 | 5 |
| Risk Exposure | 25 | 20 | 1 | 6 | 3 | 25 |
| Responsible Party | IT Team | IT Team | IT and Marketing Teams | Staff | Staff and Security Team | IT Team |
|  |  |  |  |  |  |  |

Overall, it is apparent from the risk evaluation and calculating that assets under the highest risk are web application, server and database. Risk exposure was derived by multiplying Value &Impact to Likelihood. Due to political disagreements and ongoing cyber war between India and Pakistan (it is worth not to forget about other potential malicious agents) likelihood of those risks is certain and impact is catastrophic. I recommend Pakistan to expand investment and concern with information security of its embassies around the world. Further sections of the report contain more detailed and precise recommendations.

**Risk Management Framework**

I propose a seven-step NIST RMF framework for risk management for the offices of all Pakistani embassies: prepare, categorize, select, implement, assess, authorize, and monitor. Below is a more thorough explanation of the NIST 7-Step RMF:

- Significant steps to address threats to privacy and security within the company

- Classify the system and the data that is processed, stored, and delivered based on an impact analysis.

- Put the controls in place and document how they were used.

- Verify that the controls are implemented, operating as intended, and producing the required results.

- To secure the system, select a set of NIST SP 800-53 controls based on risk analysis.

- Based on risk, a top authority determines whether to approve the system's (operational) functioning.

- Keeping track of ongoing system risks and controlling the implementation.

Reasoning behind selecting exactly RMF by NIST is derived from comparison of various information security frameworks that is conducted in the next section – adoption of information security framework. Please view that section for more justification on RMF choice.

**Adoption of Information Security Framework for Pakistan Embassy**

Critical Analysis of various Security Risk Management Frameworks

Table (5)

|  |  |  |  |
| --- | --- | --- | --- |
| Framework | Overview | Benefits | Drawbacks |
| NIST | Focuses heavily on evaluating control maturity and integrating corporate goals with cyber security defenses. NIST's domains include identification, protection, detection, reaction, and recovery. (ORNA, 2022). | NIST was founded on older frameworks, is free, and supports numerous compliance requirements. (ORNA, 2022). | May depict results that are already known, and deciding what to do next is difficult. (ORNA, 2022). |
| ISO 27001 family | Initiatives for managing building security are the main topic of ISO 27001 standards. The domains are asset management, asset control, security policy, and human resources for information security organizations. (Khelifi, 2012) | The most well-known international IT security framework and the basis for the majority of compliance requirements are two benefits of ISO 27001 certification (Khelifi, 2012). | The certification is expensive, there is no implementation guide, and it hasn't been updated since 2013 (E-SPIN, 2021). |
| CIS | Uses automated controls to safeguard and keep an eye on high-risk areas (E-SPIN, 2021). The three CIS areas are organizational, basic, and fundamental.  (ORNA, 2022). | actionable items, constant updating, and ease of use (ORNA, 2022). | not exhaustive (ORNA, 2022). |
| CMMI | The capabilities of software engineering processes are the main emphasis of CMMI. Development of products and services, Service establishment and management, and Purchase of products and services are its domains (E-SPIN, 2021). | continual improvement and suitability for large software development businesses (ORNA, 2022). | mere concentration on software development and a requirement for a clearly defined function (ORNA, 2022). |
| COBIT 5 | concentrate on establishing roles, defining responsibilities, and assessing control maturity. Control objectives, maturity models, process descriptions, and management principles are its fields. (ORNA, 2022). | working with many compliance requirements and focusing on IT governance (ORNA, 2022). | lacking in cyber security components (ORNA, 2022). |

Based on the comparison conducted above I recommend Pakistan Embassy network to opt for NIST Framework as this organization needs comprehensive solution for long period of time due to ongoing intensive cyber wars with Indian hackers. NIST provides comprehensiveness and long-term solutions to institution’s needs. In particular, key points of NIST that make it stand out from other frameworks are:

* It creates a long-term, iterative strategy for the cyber security of business

If one utilizes the generally acknowledged framework, the way a company treats cyber security is altered into a state of continuous compliance, which results in a stronger approach to securing the information and assets of the firm (Krishnan, 2021).

* Helps companies get a high degree of cyber security

The NIST Framework has been developed using the expertise of numerous information security professionals from around the world. The most extensive set of controls of any framework, it is widely recognized as industry best practice and enables your company to address any potential cyber security blind spots (SSH Academy, 2020).

- It allows for faster business expansion and gives vendors and suppliers a competitive edge.

Through positive interactions with supply chains, using a standard like NIST enables businesses to advance more quickly (Krishnan, 2021).

- A flexible and adaptive structure is necessary regardless of the organization's size and type (the Pakistan Embassy is a large organization with many branches; SSH Academy, 2020).

Because it is designed to be a risk-based, outcome-driven approach to cyber security, the NIST Framework is quite customizable. The NIST framework is readily accepted by small and medium-sized businesses as well as critical infrastructure companies in the energy and financial sectors due to its optional nature, which makes it simple to customize to businesses' particular needs in terms of cyber security (SSH Academy, 2020).

- A method that makes long-term compliance simple

The NIST Framework has given organizations a strong framework for practicing cyber security (Krishnan, 2021).

Additionally, NIST RMF was chosen because of its extensive acceptance of all quirks and best practices. For managing information security and privacy risk for businesses and systems, the NIST Risk Management Framework (RMF) provides a comprehensive, flexible, repeatable, and quantifiable 7-step procedure (Krishnan, 2021). The Federal Information Security Modernization Act's (FISMA) criteria for risk management program implementation are supported by connections to a number of NIST standards and guides (Computer Security Division, 2016).

Challenges of NIST Adoption that Pakistan embassy may experience

All challenges of NIST adoption stem from no instructions on how to implement it, difficulties associated with this can include wrong, incomplete implementation; extra time, energy and resource consumption, difficulty to find specialists that will take on this task (Strout, 2015).

NIST, similarly to other standards, is descriptive rather than prescriptive, therefore it is up to the organization to determine the specifics of how to adopt it. This was planned because there would have been loud objections if the government had established a set of cyber security practices. In truth, there had been yearly attempts in Congress to establish cyber security legislation regarding data breach notification and sharing, but nothing had been adopted owing to ideological disagreements about the various ways. This changed with the president's directive (Strout, 2015).

Another challenge in adopting the NIST CSF is that it is not a framework that fits all situations. This implies that what might be a successful execution strategy for one organization could not be for another (Belding, 2020).

Automation and workforce issues are among the major implementation obstacles firms face, according to a new survey. Over 50% of firms, according to the poll, have cyber security programs that are less than 25% automated, while less than 10% report having programs that are more than 75% automated. A majority (almost 100%) anticipate their function will expand over time, whereas about 50% report that their cybersecurity program is understaffed (Belding, 2020).

**Summary**

One of the main findings in this work is extremely frequent exposure and certain nature of the cyber-attacks on the Pakistan Embassy that are mainly posed by Indian hackers. However, Pakistani hackers attack Indian institution just with the same frequency and fierceness. In these conditions, state should take considerate and long-term steps to prevent and mitigate breaches as whole population of the country, country’s status and international relationships can be severely damaged.

Attack impact and damage was significant as it involved 10 websites in key partnering countries. DDoS attack was professionally carried out without chance to prevent it.

The selected organization is unique in its nature compared to other entities with its tremendous branches and political significance. I recommend Pakistan embassy to adopt NIST Framework because it is able to embrace full spectrum of peculiarities that the organization has. Furthermore, if Pakistan wishes to prevent upcoming breaches it will have to tackle political disagreements with its neighbor and refrain from taking revenge. This step is inevitable to save valuable resources and time spent on information security of Pakistan Embassy.

Reference list

Barney, D. (2022). What’s At Stake If Your Business Is Hit With a DDoS Attack - Kemp. *kemptechnologies.com*. Available from https://kemptechnologies.com/blog/ddos-attack-how-to-keep-business-safe-from-financial-loss-ransom#:~:text=The%20cost%20of%20downtime%20associated [Accessed 29 May 2023].

Belding, G. (2020). NIST CSF: Implementing NIST CSF. *Infosec Resources*. Available from https://resources.infosecinstitute.com/topic/nist-csf-implementing-nist-csf/ [Accessed 4 June 2023].

Cloudflare. (2022). What is a DDoS attack? *Cloudflare*. Available from https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

Computer Security Division, I.T.L. (2016). NIST Risk Management Framework | CSRC | CSRC. *CSRC | NIST*. Available from https://csrc.nist.gov/Projects/risk-management#:~:text=The%20NIST%20Risk%20Management%20Framework [Accessed 4 June 2023].

E-SPIN. (2021). Comparison Between Cybersecurity Frameworks Types. *E-SPIN Group*. Available from https://www.e-spincorp.com/comparison-between-cybersecurity-frameworks-types/.

Fortiguard Labs. (2021). What is a DDoS Attack? DDoS Meaning, Definition & Types. *Fortinet*. Available from https://www.fortinet.com/resources/cyberglossary/ddos-attack#:~:text=DDoS%20Attack%20Meaning [Accessed 29 May 2023].

Indian Defence Research Wing. (2023). In counter Cyber attacks Indian Hackers Paralyzes Pakistan Embassy Website – Indian Defence Research Wing. *idrw.org*. Available from https://idrw.org/in-counter-cyber-attacks-indian-hackers-paralyzes-pakistan-embassy-website/ [Accessed 29 May 2023].

Khelifi, A. (2012). Table 1 Advantages and Disadvantages of Using IT Standards in the UAE. *ResearchGate*. Available from https://www.researchgate.net/figure/Advantages-and-Disadvantages-of-Using-IT-Standards-in-the-UAE\_tbl1\_320654835 [Accessed 30 May 2023].

Krishnan, M. (2021). 6 NIST Framework Benefits. *www.stickmancyber.com*. Available from https://www.stickmancyber.com/cybersecurity-blog/6-nist-framework-benefits [Accessed 4 June 2023].

Ministry of Foreign Affairs, Government of Pakistan. (2018). Guiding Principles and Objectives – Ministry of Foreign Affairs. *Mofa.gov.pk*. Available from https://mofa.gov.pk/guiding-principles-and-objectives/ [Accessed 28 May 2023].

ORNA. (2022). NIST, ISO, COBIT, ITIL – Which Cyber Framework Rules Them All? *ORNA*, 6 September. Available from https://www.orna.app/post/nist-iso-cobit-itil-which-cyber-framework-rules-them-all [Accessed 30 May 2023].

Pakistan Portal. (2023). List of diplomatic missions of Pakistan. *Wikipedia*. Available from https://en.wikipedia.org/wiki/List\_of\_diplomatic\_missions\_of\_Pakistan [Accessed 28 May 2023].

SSH Academy. (2020). Overview of the NIST Cybersecurity Framework. One critical aspect for compliance proper management of SSH, the ubiquitous security protocol. *www.ssh.com*. Available from https://www.ssh.com/academy/compliance/cybersecurity-framework [Accessed 4 June 2023].

Strout, A. (2015). Improving Cybersecurity and the Challenge of Implementing the NIST Framework. *APQC*. Available from https://www.apqc.org/blog/improving-cybersecurity-and-challenge-implementing-nist-framework [Accessed 4 June 2023].

The Cyber Express. (2023). Indian Hackers Mount ‘Payback’ Attack On Pakistani Embassy. Available from https://thecyberexpress.com/indian-hackers-attack-pakistani-embassy/ [Accessed 29 May 2023].