THE PAYPAL DATA BREACH

Organization Details

PayPal's Mission: PayPal's mission is to "democratize financial services and enable economic opportunity for everyone." A well-known financial technology (FinTech) business with its headquarters in San Jose, California, is PayPal, Inc.Particularly on platforms like eBay, which was its first major market, PayPal has played a crucial role in revolutionizing digital payments and e-commerce.

PayPal is an operator in the online financial services and digital payments industries. Its main services are as follows:

- Online payments
- Peer-to-Peer Transfers
- E-commerce Integration
- Merchant Services
- Financial Products

What happened ?

On **December 6, 2022**, PayPal had a data breach, which wasn't discovered until December 8, 2022. When Paypal observed unauthorized activities during the period, They eliminated the access for the third parties. During that time the third parties were able to view and acquire personal data of the users.

Order of Events:

The Breach Started With Attackers Getting a List of Leaked Credentials: The breach started with attackers getting a list of usernames and passwords from a prior data breach.

Login Attempts Using obtained Credentials: The attackers made an attempt to log into PayPal accounts using the credentials they had obtained.the attacker used automated scripts to login against paypal's system

Lack of Multi-Factor Authentication (MFA): PayPal did not have multi-factor authentication (MFA) activated for all users at the time of the hack.

Access to Personal Data: A few hackers were successful in getting into a few PayPal accounts. As a result, they could be able to see and get users of PayPal's **personal data, Names, addresses, Social Security numbers,date of births and individual tax identification numbers** were among the data.

Detection and Mitigation: On December 8, 2022, PayPal discovered the issue and took immediate action to halt any further unauthorised access.

User Notification: On January 18, 2023, PayPal contacted impacted users to let them know of the breach and any potential effects it may have had on their personal data.

Exploited vulnerabilities and Background Info:

The Exploited vulnerabilities were Lack of MFA and Failure to Fix Known Vulnerabilities.Paypal was aware of known vulnerabilities that might be exploited by the attacker. However, they had not fixed all of these flaws before the hack, leaving their systems open to attack. Attackers exploit stolen usernames and passwords from earlier breaches to obtain unauthorized access to additional online accounts where users have reused the same credentials, a technique known as **"Credential Stuffing"**.This Attacks include testing different username and password combinations obtained from data dumps on numerous websites in an effort to get access to an account.Using bots that run lists of credentials to "stuff" into login sites for numerous services, this form of attack uses an automated strategy.Credential stuffing targets people who use the same password for several different internet accounts, a practise known as "password recycling."

According to reports, PayPal had 435 million active users in 2022, including those who had completed at least one transaction.With millions of active accounts in more than 200 countries and territories, PayPal is a widely used digital wallet and payment network. Both businesses and people frequently utilise it for different types of financial transactions.

Aftermath:

Over the course of two days, hackers had access to account holders' complete names, dates of birth, postal addresses, social security numbers, and tax identification numbers as well as transaction histories, associated credit or debit card information, and PayPal invoice data all turning into immediate impacts. **34,942** of PayPal's users have been impacted by the incident, according to the company's data breach reports.

In order to lessen the impact of the attack, PayPal quickly blocked the hackers' access to the system and changed the passwords for the compromised accounts. Notably, the warning gave consumers the assurance that the attackers either failed to attempt any transactions from the compromised accounts or did not even try.For the long term impact, paypal lost their reputation and trust with their customers.This data breach aslo puts the affected users at future risk of Identity theft. To stop such breaches, more money has to be put into cybersecurity as a result of the occurrence.

What were the technical and management failures that enabled the incident?

- Multi-factor authentication (MFA) not being used
- Failing to fix identified security Patches
- Network segmentation mistakes
- Inadequate tracking and monitoring techniques
- Unable to have dedicated cybersecurity team in place

How did the organization respond to the incident? In what ways was this response ineffective?

According to PayPal, it acted swiftly to restrict the hackers' access to the system and reset the passwords of the accounts that were proven to have been compromised.After that they notified the affected users.Then implemented MFA for all the users and they also offered 2 years of membership of equifax for the affected members

.

Why was the organization unable to respond more effectively and aid those affected?

Lack of incidence response plan : Paypal did not had well incidence response plan which made it difficult to respond quicky and effectively to breach.

Lack of communication: They were unable to communicate with affected users during the breach and this led to confusion and frustration among the user. Also they were month delayed notifying the issue.

Lack of cybersecurity resources: No proper cybersecurity resources were available and This made it challenging for the business to rapidly identify and address the breach.

Global reach of paypal: As paypal has over 435 millions user across the world and it made difficult for them to communicate.

PART 1

INTRODUCTION AND GENERAL POLICY DEVELOPMENT DISCUSSION

1. Importance of Information Security Policies

Information security policies form the foundation of an organization's cybersecurity posture, preventing and mitigating cybersecurity incidents. They establish a clear framework for protecting information assets, aligning with standards, guidelines, and procedures for effective implementation.

2. Policy Development Process

A systematic policy development process ensures comprehensive and effective information security policies. Key steps include:

Identify Stakeholders: Engage all relevant parties to address their needs and concerns.

Conduct Risk Assessment: Prioritize information security risks to develop targeted policies.

Draft Clear and Concise Policies: Translate risk assessment findings into actionable guidelines.

Rigorous Review: Refine policies through stakeholder feedback before finalization.

Obtain Formal Approval: Secure management support for policy implementation.

Implement and Train: Deploy technical controls and train employees on new guidelines.

Regular Review and Update: Adapt policies to evolving risks and requirements.

PART 2

ADDRESSING VULNERABILITIES IN POLICIES

1. Background

On December 6, 2022, a combination of technological flaws and governmental regulations led to the PayPal data leak. The incident's top three vulnerabilities were found to be:

Weak Authentication Mechanisms: Not asking users to give additional verification beyond a username and password when using multi-factor authentication (MFA). MFA offers an extra layer of protection.

Failing to patch systems for known vulnerabilities: It's critical to patch known vulnerabilities as soon as possible to reduce the amount of time attackers have to take advantage of them.

Inadequate logging and monitoring: Suspicious activity or possible breaches may be quickly discovered with the use of adequate logging and monitoring, which offer insightful information about system activity.

2. Policy Elements and Style:

General Purpose: Clearly state the policy's overarching objective while highlighting the significance of addressing particular flaws that were found in the event, such as shoddy access restrictions, insufficient patch management, and weak authentication. For instance, a policy addressing MFA implementation should clearly state that its purpose is to enhance authentication security by mandating the use of MFA for all users.

Scope: The scope explicitly specify the systems, data, and individuals that are covered by the policy's requirements for addressing vulnerabilities. For instance, a vulnerability management strategy should make it obvious whose data and systems are covered by it as well as who is in charge of finding, addressing, and fixing vulnerabilities.

Responsibility: Policies have to specify precisely who is in charge of carrying them out, keeping an eye on compliance, and taking appropriate action when there are infractions. A data protection strategy, for example, should specify exactly who is in charge of categorizing data, putting access restrictions in place, and routinely reviewing rights for data access.

Standards: Standards set forth particular technical requirements that must be fulfilled in order to abide by the policy. To guarantee that passwords are strong enough to thwart unauthorised access, a policy addressing password management, for instance, could set standards for password complexity, length, and usage limits.

Protocols: Procedures can guarantee that vital activities, like incident response or vulnerability remediation, are carried out reliably and efficiently while addressing vulnerabilities. An incident response strategy, for example, need to include specific steps for locating, looking into, containing, and recovering from security events.

3. Information Security Framework:

For strong and efficient security measures, policy development must be in line with existing information security standards in the wake of the December 2022 PayPal data breach. Frameworks for information security offer an organized method for handling and safeguarding sensitive data. These frameworks provide a uniform set of guidelines, norms, and processes that organizations may utilize to create efficient rules and guidelines.

The vulnerabilities could have been mitigated by aligning policy development with established information security frameworks. Frameworks, such as the NIST Cybersecurity Framework or the ISO 27001 standard, provide guidance on implementing controls that address these specific weaknesses.

For the purpose of developing comprehensive and effective policies that meet the always changing cyber threat landscape, policy creation must be in line with recognised information security frameworks. Strong standards and processes must be put in place to secure sensitive data, as the PayPal data leak provides as a reminder.

4. Governance and Risk Management:

The Information security rules must be implemented and enforced effectively, and governance structures are essential to this process.To Establishing transparent governance frameworks is essential for accountability, supervision, and communication in light of PayPal's data leak.

The strength of the governance institutions that support policy enforcement determines its efficacy. For this reason, in order to support their information security policy framework, organizations should invest in developing robust governance structures.

Developing effective information security rules requires risk management. Policy formulation in the light of PayPal's data breach necessitates a knowledge of and mitigation of risks associated with vulnerabilities. Developing policies requires careful consideration of risk, especially when it comes to cybersecurity. Businesses may greatly lower their chance of experiencing data breaches and other security events by recognizing, evaluating, and mitigating possible risks and vulnerabilities. In order to keep ahead of changing risks, organizations should have a continuous risk management strategy, making necessary adjustments to their policies and processes.

5. Asset Management Policies:

Policy 1: Identification of Assets

Every IT asset in the company has to be recognised and included in the asset inventory.

Information like the asset type, location, serial number, purchase date, and custodian should all be included in the asset inventory.

Policy 2: Classification of Assets

Assets ought to be categorized according to how important they are to the running of the company and how sensitive the data they hold is.It is necessary to create a categorization scheme to specify various criticality and sensitivity levels.

Policy 3: Protection of Assets

It is necessary to safeguard vital resources from unwanted usage, access, disclosure, interruption, alteration, or destruction.Depending on the classification level of the assets, both logical and physical security measures should be put in place to safeguard them.

6. Physical and Environmental Security Policies:

Policy 1: Physical Access Control

Policy 2: Physical Security Monitoring

Policy 3: Environmental Controls

These policies help address the vulnerabilities discovered in the incident analysis by:

Limiting Physical entry to Critical places: Policy 1 reduces the danger of insider threats and unauthorized entry by restricting access to sensitive places.

Monitoring Critical Areas for Security Vulnerabilities: In order to detect and react quickly to attempts at unauthorized entry, Policy 2 encourages monitoring and intrusion detection.

Preventing Data Loss and Downtime by Providing Protection against Fire, Water Damage, and Power.

Protecting IT Infrastructure from Environmental Hazards: Policy 3 safeguards critical IT equipment from fire, water damage, and power outages, preventing data loss and downtime.

7. Access Control Management Policies:

The creation of thorough Access Control Management Policies is essential in reaction to the vulnerabilities found in the December 2022 PayPal data breach. These regulations, which limit access to facilities, data, and systems, should tackle the vulnerabilities brought about by insufficient access controls and unauthorized access.

Policy 1: Access Control Policy

Policy 2: Access Control for Facilities

Policy 3: Access Control Incident Response

The vulnerabilities found in the PayPal data breach are immediately addressed by these rules by:

Putting MFA into Practise for High-danger Accounts: Policy 1 requires MFA for accounts that pose a danger to sensitive data by providing an additional layer of protection.

Limiting Physical Access to Facilities: In order to avoid unwanted entrance and possible data breaches, Policy 2 restricts physical access to sensitive places.

Creating an Access Control Incident Response Plan: Policy 3 offers a structure for handling access control breaches in a way that minimizes harm and exposes as little data as possible.

References

PayPal Hacked: The Aftermath of the 2022 PayPal Breach. (2023, June 15). phoenixNAP. Retrieved October 13, 2023, from https://phoenixnap.com/blog/paypal-hacked

PayPal Hit With Class Action Over Data Breach Affecting 35,000. (2023, March 3). Bloomberg Law News. Retrieved October 13, 2023, from https://news.bloomberglaw.com/litigation/paypal-hit-with-class-action-over-data-breach-affecting-35-000

Sultan, O. (2023, March 4). *PayPal Sued Over Data Breach that Impacted 35,000 users*. Hackread. Retrieved October 13, 2023, from https://www.hackread.com/paypal-sued-over-data-breach/

Toulas, B. (2023, January 19). *PayPal accounts breached in large-scale credential stuffing attack*. Bleeping Computer. Retrieved October 13, 2023, from https://www.bleepingcomputer.com/news/security/paypal-accounts-breached-in-large-scale-credential-stuffing-attack/

Untitled. (2023, January 17). NH Department of Justice. Retrieved October 13, 2023, from https://www.doj.nh.gov/consumer/security-breaches/documents/paypal-20230117.pdf