ISSN No:-2456-2165

Online Database Security Threats and Solutions: The NetFlix Incident

*Kalu, Jonah[1], Igbo, Michael Elem[2], Igbo, Nkechinyere Elem[3], Oko, Christian Obinna[4], Njoku, Chiemezuo[5].
[1,2,3,4] Physics Unit, Department of Science Laboratory technology, School of Sciences, Akanu Ibiam Federal Polytechnic Unwana, Afikpo, Ebonyi State, Nigeria.
[5]Department of Electrical Electronics Engineering Technology, School of Engineering, Akanu Ibiam Federal Polytechnic Unwana, Afikpo, Ebonyi State, Nigeria.

Abstract:- In April 2018, millions of subscribers around the globe were greeted with an embarrassing and frightening report from Irdeto that it had discovered for sale, eight hundred and fifty four (854) personal credentials from sixty nine (69) different sellers across more than fifteen (15) dark web marketplaces. Incidentally, these turned out to be personal and very sensitive details of subscribers to forty two (42) streaming services including Netflix, HBO, Direct TV, as well as Hulu. With the report of this security breach made public and the dire consequences it portends, days passed by, weeks passed by, and even after several assurances and reassurances by Netflix, majority of its more than seventy million (70,000,000) estimated subscribers who were hitherto regular users of its streaming services were still very apprehensive of logging into the platform as they felt the integrity of the system has been seriously compromised and that the confidentiality of their personal details can no longer be guaranteed by the service provider. Huge monetary and non- monetary losses were encountered by both Netflix and its customers alike. This paper investigates the damages which the security breach caused both Netflix and its customers, and equally recommends security control measures that can be employed to prevent a repeat of such security breach in the future.

Keywords:- *Control Measures, Database, Netflix, Security, Streaming.*

I. INTRODUCTION

Online streaming has become one of the most popular entertainment activities over the years, generating tons of network traffic from subscribers, who prefer streaming due to its affordability and convenience. Some confidential information of users of these streaming services are usually held in an online database as these users are required to login with such details to gain access each time they need to use the streaming platform.

Statistics show that over the years, online database attacks have been on the increase and there are strong indications that the major reason for this trend is the constant rise in number of persons having access to the databases of these streaming services. Research findings also indicate that the biggest motive behind most of the recent attacks remains data theft for the purpose of making money [1].

The 2018 Netflix security attack has proven to be one of the biggest online database security breaches in recent years as very reliable statistics later revealed that as at the end of 2017 Netflix actually had more than a hundred and seventeen million subscribers on its database, which is actually far above the number of persons (approximately 70,000,000) initially estimated as being the subscriber density as at the time of the security breach in April 2018 [2].

A similar security breach had hit Sony Corporation's PlayStation platform few years ago, where sensitive information like credit card data, date of birth, contact addresses, phone numbers, and other confidential information were compromised as a result of the attack. Though the company restored the network's availability and functions some days after the incident, and allowed users to select certain free games as a form of compensation for the period of downtime, the attack eventually had to devastating impacts on the system as a whole [3].

As shown below in figure 1. One of the reasons why online database systems are easily the target of many hackers is the remote connectivity it offers its multiple users who can connect to the system and access its services from different locations at the same time.

Fig. 1. An Online Database System.

ISSN No:-2456-2165

II. LITERATURE REVIEW

Over the years, researchers have conducted lots of investigation into database security threats and breaches, with a view to uncovering the immediate and remote causes of these incidents, and proffer solutions on how to provide greater database security, especially as it concerns online systems.

Perelman *et al.* [4] analyzed Sony PlayStation 3 game traffic using the wired Ethernet interface of the system and discovered that the desire by users for a more flexible system that gives them more control to personalise their own set up, watch movies, and play Linux games while enjoying the hardware activities of the PlayStation makes the system even more vulnerable to attacks.

Chen *et al.* [5] demonstrated the existence of many susceptible vectors which attackers can possible use due to the increase in the level of player-driven customization by users. It was revealed that the programming interfaces accessible to users and players and the contents generated by these users are mostly responsible for the vulnerabilities in the gaming system. It was also shown that new and increased attacks vectors will emerge as flexibility remains the greatest attraction to users in the gaming community.

Ghorbanzadeh *et al.* [6] stated that one of the factors that make the management of security in online database systems more challenging is that it is a distributed database i.e. a database that is distributed across multiple databases, and managed by the distributed database management system (DDBMS). This system requires multilevel security, which poses major challenges in terms of authentication, data confidentiality, identification, and access control due to the complex nature of the entire system.

Bhagat and Bhagat [7] suggested a layered security network model as the best approach in combating different forms of online security attacks.

Sanchez [8] recommended the result of the SANS institute top 20 critical security controls as effective measures that can be employed by organizations to protect their systems and deal with different forms of security attack by hackers.

III. METHOD

This research will be based on various reports and investigations which have been conducted into the **"Netflix Security Attack of April 2018"** to ascertain the immediate and remote causes that led to a successful breach of the company's database security. Based on existing critical control measures, recommendations will be made concerning the control measures that are most suitable to prevent similar attacks in the future.

IV. RESULTS AND DISCUSSION

Some of SANS Institute's top critical controls as outline by Sanchez [8] would have been very effective to either minimize the impact or completely prevent the occurrence of the Netflix attack. This paper after investigating the NetFlix attack, selected the following critical security controls as a suitable preventive measures that can be adopted to guard against such security attacks in the future:

A. CRITICAL CONTROLS

Control 1. Data Encryption - Perform an assessment to identify sensitive information like emails, usernames, passwords, social security numbers that might be present in the database. Such information should be encrypted to make it extremely difficult for the hackers to decipher their contents and upload such information in clear text to the internet.

Control 2. Periodic Scan - Conduct scans at regular intervals on the network servers to check if there are sensitive information that still left in clear text form and get them encrypted. This would ensure that the confidentiality of such information is maintained at all times.

Control 3. Network Monitoring - Deploy automated monitoring tools along the network borders to detect the exfiltration of these sensitive information across the borders, block such information transfer, and alert the personnel in charge of network security instantly.

Control 4. Data Monitoring - Constantly monitor traffic entering and leaving the network to detect unauthorized use of encryption; as most hackers use channel encryption to bypass installed security guarding the network. This is an effective approach in detecting and terminating rogue connection, and remedying system infection.

Action 5. Anti Malware - Apply network-based malware defenses that will prevent copying of files from the network, and alerts the security personnel immediately something unusual starts happening within the systems.

Control 6. Controlled Network Access - Implementing multi-level authentication, which involves additional authentication for administrative accounts through a One Time Password (OTP), smart card certificates, and biometrics will prevent compromising sensitive information as only a few privileged individuals will have access to such information.

Control 7. Maintenance, Monitoring, and Log Audit Analysis – This involves deploying a security log analytics tool such as the Security Incident and Event Management (SIEM) that can detect activities that do not correlate but deviates from the known pattern. This would have effectively detected malicious activity from the attackers had it been in place in the system.

Control 8. Penetration Testing – Regular external (outside the network perimeter i.e. wireless connections or internet), and internal (i.e. internal network) penetration test should be conducted to detect vulnerabilities and the presence of attack vectors existing within the network. This is to help the organization ascertain its security status at all times, and take appropriate actions.

Control 9. Secure Network Engineering - Network segmentation should be implemented to create separate trust zones with individual boundary defenses for each zone. This will create better control of system access and ensure that individuals operate only within the level where they have been authorized.

B. DAMAGES SUFFERED FROM THE ATTACK

Confidentiality, Integrity, and Availability (CIA) are considered as the major foundations of information security [10]; and protecting an organization against cyber attacks need good understanding of CIA. The Netflix security breach certainly did serious damage to the CIA triad in the following ways:

i. Confidentiality

The goal of Confidentiality is simply to ensure that sensitive information do not get into wrong hands by adhering to the principles set out in the Data Protections Act. This requires that actions be taken by custodians of such information to ensure that unauthorized disclosure of information is prevented and that only individuals that are legitimately authorized have access to the information do so, and on a "need to know" basis.

The Netflix attack proved that the organization failed in its statutory obligation to its subscribers by virtue of its failure to ensure that their personal and sensitive details placed in NetFlix custody is held in strict confidence as stipulated in the Data Protection Act.

ii. Integrity

The principle of Integrity aims to ensure that at all times, information remains valid, accurate, and trustworthy throughout its life cycle. This can only be achieved by taking adequate measures to prevent the alteration of information whether during transmission or during the storage of such information.

Guaranteeing Integrity of an information system also entails putting in place control measures to restore information that may have been altered, implement backups regularly, establish effective access controls, and validate inputs.

The Netflix attack which successfully exposed sensitive details of its subscribers and made such details available in the public domain is a serious compromise on the Integrity of the system. This is so as the hackers apart from stealing sensitive information from the database, may have equally "**altered"** some of the information stored in the database.

iii. Availability

Availability refers to authorized persons being able to have access to information as and when it is required. Ensuring availability involves rigorous maintenance of the hardware, software, communication links, and other equipments used in the storage and processing of information.

The attack on Netflix led to a momentary "**reduction in availability"** as the organisation had to limit the availability of the streaming service to subscribers during the course of its investigation into the security breach.

C. IMPLICATIONS OF THE ATTACK.

The Netflix attack had far-reaching costs impacts on both Netflix and its subscribers. Even though analyst did not attribute some negative trends observed in NetFlix performance index after the April 2018 report concerning the Netflix attack, a careful study of the statistics clearly reveal the following:

Netflix revenue for Q2, 2018 ($3.91 Billion versus $3.94 Billion) as shown in figure 2, was not as strong as predicted when compared to that of Q1, 2018($4 Billion), i.e. before the attacks which surpassed predictions. Q1 was before the attack while Q2 was after the attack as shown in figure 2[9] below.

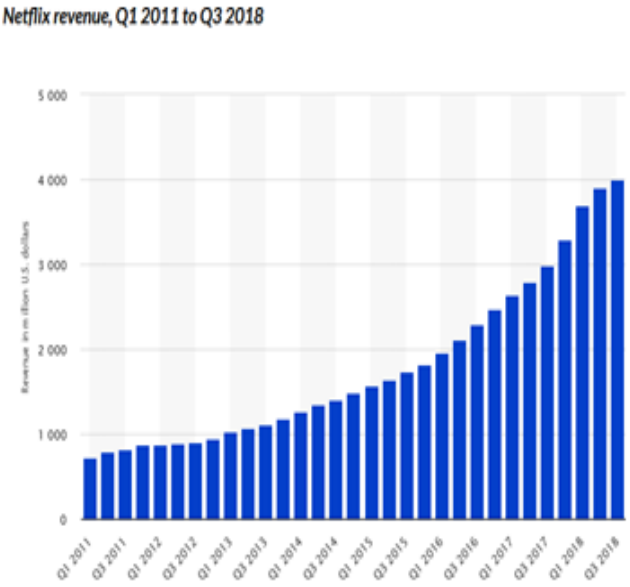

Fig. 2. Netflix revenue from Q1 2011 to Q3 2018.

Netflix's income dropped sharply from $674Million in the second quarter (Q2) 2018 to $403Million in the third quarter (Q3) 2018 as shown in figure 3[9].

ISSN No:-2456-2165

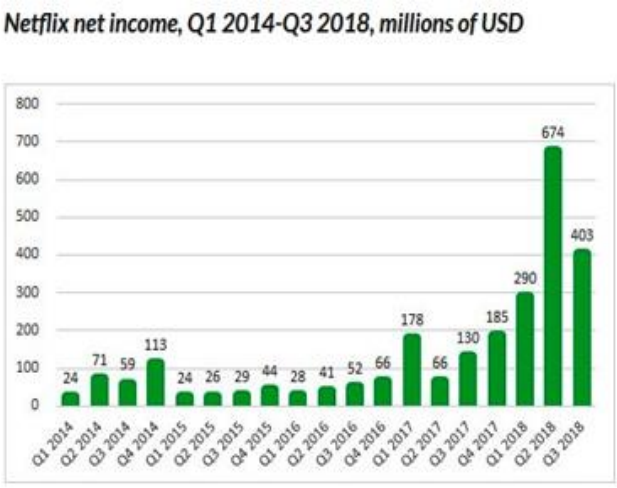

Fig. 3. Netflix net income from 2006 to 2018.

Netflix's share value dropped from about $320 in April to $260 in December, i.e. eight months after the attacks were reported. This represents the lowest value recorded within the last eight months of 2018 as shown in figure 4[9].

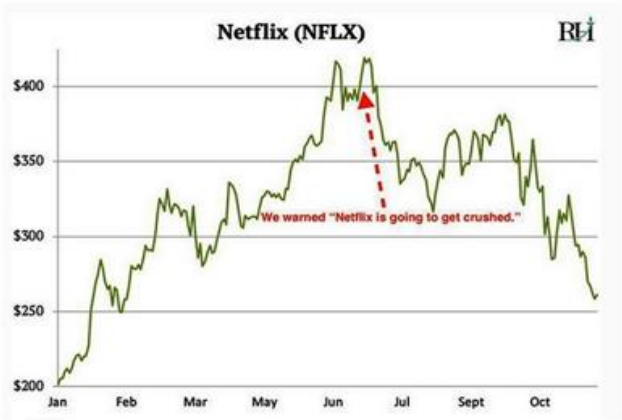

Fig. 4. Netflix's share value from January to October 2018.

Netflix market capitalization dropped from about $148 in April 2018 to about $128 by December 2018 as shown in figure 5[9]. This represents a 13.5% loss in share value, which is unprecedented in the history of the company.

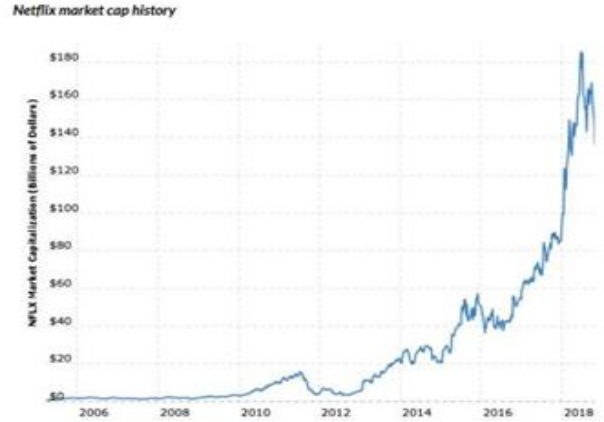

Fig. 5. Netflix market capitalization from 2006 to 2018.

D. SCALE OF THE SECURITY BREACH (THE DATA PROTECTION ACT)

Findings from various investigations into the Netflix attack revealed that the scale of the security breach is high. Netflix fell short of recommended best practice rules as outlined in "The Data Protection Act" which stipulates that organizations should be responsible to put in place the right technology, processes and people in place to handle the quality of the data that are in their custody. Important activities which such organizations should consider include:

1. Regular evaluation of the quality of the data that you hold and are continuing to collect. Contact Data Validation and Data Cleansing are good ways of doing this.
2. Ensuring you have the right roles and responsibilities set out for your data management including the focal point of a Data Protection Officer.
3. Analysis and profiling of your data to identify any potential gaps or issues that could cause problems to arise.

It is evident that Netflix did not adhere to the provisions of The Data Protection Act.

E. COST OF FIXING THE BREACH

The cost of fixing the breach can be divided into financial and social costs as follows:

A. Financial Cost

The financial cost of the fixing the breach can be divided into two broad areas as follows of technical costs and costs of non compliance [12]:

i. Technical Costs.

These include: (a) Cost of investigating the breach. (b) Cost of database repairs. (c) Cost of putting an effective security structure in place

ii. Cost of Non-Compliance

These include: (a) Government mandated fines (b) Legal fees from litigations. (c) Cost of executing breach response.

b. Social Cost

The Netflix attack had very negative impact on the company's reputation, leading to uncertainty in its stocks and a massive loss of the company's market share in the sector. Many of the subscribers lost confidence in the system and migrated to other service providers thereby causing a serious dip in Netflix revenue, market capitalization, and share value as shown in figures 6 [9].

Figure 6 [9] shows that while other competitors in the sector were able to market value of their stock, while that of NetFlix which had attained the value of $423.21 in June, 2018 rapidly crashed to $300 before the end of 2018 fiscal year.

ISSN No:-2456-2165

Fig. 6. Comparison of NetFlix Capitalization and Competitors

In order to restore the confidence of its users, Netflix will need to take the following actions:

a. Put in place effective security control measures to guarantee the confidentiality, Integrity, and Availability of the system at all times.
b. Embark on aggressive campaigns to assure its current and intending users that the system is secure so as to give them the needed confidence to use the service without any fears.
c. Adopt some measures to compensate former users who may have abandoned the service due to fear or suffered some form of loss so as to encourage them to return.

F. IMPLICATIONS OF "NOT DISCOVERING THE BREACH"

Had the Netflix security breach gone undetected it would have reached a point where the organization would have been shut down. As the time taken to discover and respond to such attack increases, the level of damage done by the hackers drastically increases.

If the activities of the hackers do not completely crumble the network and the services rendered by Netflix to its customers, the technical cost of repairing the damages, settlement of litigations from aggrieved customers, payment of fines for non-compliance with regulatory provisions, etc will get so high that the business will be forced to collapse.

V. CONCLUSSION

Every organization is prone to attack by hackers who may attempt or even succeed in compromising the integrity of its system. Netflix is one of the organizations that has fallen victim to attackers recently seen in the 2018 report from Irdeto. The exposure of sensitive personal data of NetFlix subscribers to the public by the cyber pirates created a lot of damage to both the service users and service provider.

The occurrence of such incidence is a great lesson for every organization and a serious call to review the effectiveness of its security structure. On many occasions, a security breach in any organization usually occurs due to a complete breakdown or poor control measures in certain aspects of their operations, hence every serious minded organization need to take adequate steps to ensure the effectiveness of its security structure at all times.

RECOMMENDATIONS

Netflix and every serious minded organization should put in place effective critical control measures like malware defenses, effective monitoring, regular security audits, data encryption, as well as strict database access control techniques as already discussed in this paper. These should be strictly implemented to effectively reduce the risks of experiencing such attacks in the future.

Organizations should equally entrench the culture of conducting regular audits to ascertain how effective their security systems are, so as to identify gaps that may still exits and explore possible actions can be adopted to further strengthen the level of security within the system.

REFERENCES

[1]. N. A. Al-Sayid and D. Aldlaeen, "Database security threats: A survey study," *2013 5th International Conference on Computer Science and Information Technology*, Amman, 2013, pp. 60-64. DOI: 10.1109/CSIT.2013.6588759

[2]. T. Spangler. "Hundreds of stolen passwords for Netflix, HBO, Hulu and more discovered for sale on 'dark web". Retrieved on 10/04/2019 from https://www.aol.com

[3]. J. Schreier. 25/5/11. "Sony Estimates $171 Million Loss from PSN Hack". Retrieved on 13/04/2019 from https://www.wired.com

[4]. M. Perelman, Ping Ji and W. Chen, "Traffic and security analysis on Sony PlayStation 3, "2009 *IEEE International Conference on Intelligence and Security Informatics*," Dallas, TX, 2009, pp. 272-275. DOI: 10.1109/ISI.2009.5137325

[5]. L. Chen, N. Shashidhar, D. Rawat, M. Yang and C. Kadlec, "Investigating the security and digital forensics of video games and gaming systems: A study of PC games and PS4 console," *2016 International Conference on Computing, Networking and Communications (ICNC)*, Kauai, HI, 2016, pp. 1-5. DOI: 10.1109/ICCNC.2016.7440557

[6]. P. Ghorbanzadeh, A. Shaddeli, R. Malekzadeh and Z. Jahanbakhsh, "A survey of mobile database security threats and solutions for it," *The 3rd International Conference on Information Sciences and Interaction Sciences*, Chengdu, 2010, pp. 676-682.

[7]. Bhagat, A.R. Bhagat, V.B. "Mobile Database Review and Security Aspects," *International Journal of Computer Science and Mobile Computing*, Vol.3 Issue.3, 2014, pp. 1174-1182.

[8]. G. Sanchez. Case Study: Critical Controls that Sony Should Have Implemented 2015. *"SANS Institute Information Security Reading Room"*. Retrieved on 14/04/2019 from https://www.sans.org

[9]. M. Iqbal. "Netflix Revenue and Usage Statistics (2018)". Retrieved on 15/04/2019 from http://www.businessofapps.com/data/netflix-statistics/.

[10]. S. McBride. “Netflix's Worst Nightmare Is Coming True”. Retrieved on 15/04/2019 from https://www.forbes.com
[11]. The CIA Triad: The key to Improving Your Information Security, 2018. Retrieved on 15/04/2019 from https://commissum.com
[12]. The Cost of Non-Compliance, 2018. Retrieved on 16/04/19 from https://4iq.com/cost-non-compliance/