TRANSACTION SECURITY IN AN ALBANIAN FINANCIAL INSTITUTION HAS BEEN BREACHED – WHAT TO DO NEXT

Enida Puto
Bank of Albania
ALBANIA
enidaputo@yahoo.com

Kozeta Sevrani
Faculty of Economy - UT
ALBANIA
kozeta.sevrani@unitir.edu.al

ABSTRACT

The question for a financial institution is not if they will suffer a cyber-attack, it's when. We focus this study on Albanian financial institutions and potential cyber-incidents that involve fraudulent transactions, as this is the main focus for attackers nowadays. When financial transactions are compromised, a cyber-incident plan helps to minimize the effects of the cyber-attack, the time to bounce back to normal business and also helps minimize financial harm. Although every financial institution should take very strict measures of defense in all the parts of information technology infrastructure, including perimeter, people, policies, procedures, network, PKI, hosts, applications and databases, part of the whole process should also be a plan of what to do in case of a cyber-attack that may or has led to fraudulent transactions. We performed a study in Albania, in order to understand where Albanian financial institutions stand in regard to a cyber-incident plan when financial transactions were compromised. We found out what procedures Albanian financial institutions had in place and what lacked for managing a cyber-incident involving fraudulent transactions. In this paper we analyze the case of a severe cyber-attack, where the institution's data have been breached and possibly stolen, modified or used to impersonate this institution by sending fraudulent transactions. In this perspective, we analyze several Albanian financial institutions on how they deal with it, and what plan do they have in place in case of such a cyber-attack. We suggest a detailed and customized cyber-incident plan according to institution's infrastructure and type of attack and compare this plan against the findings in financial institutions that we examined. Then we come to conclusions of what should be the best way or plan on dealing with these kinds of cyber-attacks.

Keywords: Cyber-attack, defense, data, breach, security, financial.

INTRODUCTION

What is a data breach? A data breach exposes confidential, sensitive, or protected information to an unauthorized person. The files in a data breach are viewed, shared and/or modified without permission. Data breach can cause devastating effects on individuals and business organizations, such as identity theft, which in turn can lead to financial loses and legal issues. For government institutions, the risks can mean exposing confidential information to foreign parties. Military operations, political dealings, and details on essential national infrastructure can pose a major threat to a government and its citizens. [1]

Since money robbing has gone mostly digital, a profiting area for criminals are financial institutions, and criminals' target is to breach the data of financial institutions such as banks and use it to their advantage. With the new working-from-home normal, institutions have seen a growth in cyber-attacks. Let's have a look at some of the biggest data breaches in the financial industry, and what we can learn from them [2]:

Westpac/PayID: third-party account authentication breach. The hackers used an enumeration attack — a brute-force technique to guess or confirm valid users in the bank's system. As a result, hackers exposed the banking details of 98 000 customers, such as phone numbers, names and account information linked to a payment platform (PayID) which allows users to immediately transfer money between banks.
The lesson: Being prepared for a brute-force attack.

Desjardins Group: Canadian credit union breach. It was made possible by an inside job by a malicious IT worker who stole personal information, including social insurance numbers.
The lesson: People should be managed as a security risk in the same way as systems and processes.

Capital One: credit card breach. A tech worker gained access to the company's servers via a misconfigured web application firewall and gained access to social security numbers and 80,000 linked bank accounts.
The lesson: Except for people being the weakest point in security system, basic cyber hygiene can dramatically reduce risk. Employing third-party next-generation firewall services is a practical way to ensure proper maintenance if your internal resources are at capacity.

First American Financial: personal and financial records compromised. The data escaped through what is known as a "business logic flaw". The attacker is enabled to get around the programmed business rules of the application, disguising the hack as a valid web request and exposed approximately 885 million financial and personal records related to real estate transactions.
The lesson: The breach was caused by insufficient process validation. It's critical to make sure that you have the necessary technical resources required to identify and remove these types of vulnerabilities.

Equifax: credit reporting data breach. The hack was via a six-month-old Apache Struts vulnerability which allowed remote coders to hack into Equifax data, exposing the names, social security numbers, birthdates, telephone numbers, and email addresses of 143 million accounts in the United States and 400,000 in the United Kingdom. The hackers also stole credit card numbers of over 209,000 customers.
The lesson: Keep on top of your updates, and regularly review your system vulnerabilities.

Some other cases of data breach include the hacking of local infrastructure of the financial institutions. The consequences from data security breach can be financial loss, operational disruptions, reputational damage, other hidden costs, loss of intellectual propriety etc.
In terms of a financial institution, an attacker might do something as simple as lower the interest rate on their own loan, or manipulate the amount of deposits so there's more money in an account. In other cases, they might raise the limits on a credit card or delete transactions to lower the balance. The effects can be wide-ranging and hard to find. [3]
In more flagrant cases, attackers can send financial transaction to other institutions, with considerable amounts of money.
Below are two examples:
Punjab National Bank, India, in 2018, $1.8 billion. The hack was carried by two junior employees, sending SWIFT messages without recording them on the internal system [4].
Central Bank of Bangladesh's Federal Reserve / Tien Phong Bank, Vietnam / Banco del Austro, Ecuador, in 2015-2016, $ 100 million. The hackers were using a software exploit and

a malware that had been specifically designed to change code in SWIFT's Access Alliance software. That allowed them to tamper with a database recording the bank's activity over the network, allowing attackers to delete outgoing transfer requests and intercept incoming requests, as well as change recorded account balances — effectively hiding the heist from officials [5].

An interesting and helpful guidance is created by The MITRE Att&ck Framework [6], which outlines each phase of a cyberattack. The framework identifies eleven different techniques employed during an attack: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Exfiltration and Command and Control. Each technique has several sub-techniques. It also provides a mitigations list for each technique and sub-technique, and how to detect each of them, but still there is limited information on how to manage the situation in case that the cyber-incident has happened.

In this paper we have taken several Albanian financial institutions as samples and through questionnaires and on-site review, have gathered information on how these institutions do manage a scenario in which the security has been breached. We will not mention these institutions for security reasons. We analyze their strong and week points and suggest our best version scenario for handling the situation of a data breach. Then we compare their handling of the cyber-attack against our methodology explained below.

The findings and conclusions of this paper can be applied in every other institution which has a focus on security. Since Albanian Banks and some other financial institutions communicate electronically with each-other and the Central Bank, and also use other financial systems for processing payments and transactions, it is important that every one of them, maintains a secure local infrastructure, since a data breach in one institution can lead to a chain of events that include other institutions as well.

METHODOLOGY

The reason that we choose this topic, it is because there is a lot of information everywhere on how to prevent a cyber-attack, but practically no information on how to manage the situation when a financial institution's security has been breached.

In order to manage the situation in the best possible way and to minimize the impact, we came up with the following methodology – a plan which includes the following steps:

Detection of compromised components

We will not discuss on this paper the means of detection that a financial institution should have for detecting cyber-attacks, but will assume that the detection already happened and the responsible security team is aware of the hack. After the first awareness, a detailed identification of all compromised systems shall be performed.

Isolation

The compromised systems shall be isolated. This includes applications, machines and network components. The actions can vary depending on the infrastructure, like unplugging the network cable from the compromised systems, suspend virtual machines, isolate the compromised systems in a VLAN etc.

Determining the level of compromise (in terms of infrastructure and data)
After isolation, it is to be considered the level of compromise from the cyber-incident.
After the hackers are in the institution's local infrastructure, the institution should assess the level of compromise in terms of damage in infrastructure and data, which could be corrupted, stolen or modified:

Nothing: the intrusion was detected before hackers could access any valuable information or perform any harm on the system. The system is still considered compromised, as long as attackers accessed it in a way, even if they did not manage to do anything else.
Only infrastructure was damaged, but no valuable information was accessed.
Valuable information was stolen.
Valuable information was corrupted, but no fraudulent transactions were sent.
Valuable information was modified and fraudulent *transactions were sent.*
A combination of the above.

Identification and cancellation of fraudulent transactions (if there are any)
From the determination of the level of compromise, this step is performed if valuable information was modified and fraudulent transactions were sent. If not, then we should continue with the next step.

The business reconciliation process has to be started. If it is possible, sent messages should be retrieved from a clean backup system. Messages might be retrieved from the service provider or counterparties and each message should be verified and compared to the messages in interfaced applications. All fraudulent or suspicious transactions should be canceled as soon as possible. If identification and/or cancellation of fraudulent transactions cannot be done technically or there is no clean environment from where to do it, then correspondents can be contacted over phone or e-mail, and they can be requested to cancel the transactions or stop their further processing.

Evidence collection and analysis
In order to reveal the methods used by the attackers, for better understanding what and how the attack happened and help in the official investigation, evidence collection and forensic analysis shall be performed. The forensic analysis is recommended to be performed by an outside team, because the attacker may be an insider and can destroy the evidence. Also, a chain of controls shall be put in place when collecting evidence, so that it doesn't get lost or destroyed during collection, with or without purpose.

Business Continuity and Restoration
Business Continuity and/or Fallback/Disaster Recovery procedures are executed and the institution bounces back to normal business. Meanwhile, after the evidence is collected, the compromised systems are restored. This could be done by doing a complete reinstallation. The institution shall be careful when restoring backups, in order not do restore a compromised one.

Access Controls Credentials Change
In all the systems (Primary, Backup, Disaster) all credentials of all users (machine users, application users, non-human users etc.) should be changed in order to be different from the hacked system, so that the attackers cannot re-access them.

Contact with the service providers, central institution and/or counterparties

Service providers may be contacted in order to help in the normalization of the situation at a sooner time, as well as counterparties. Central institution may also take several measures to protect the other institutions that communicate with the affected one via central systems. If counterparties have been informed to cancel transactions, they have to be informed again when it is ok to accept further transactions from the hacked institution.

Corrective actions

As part of Incident and Problem Management procedures, institutions should do a follow-up of the situation and take corrective measures. This includes the correction of the weak points from where the attack was made possible and also a total assessment in terms of its local security infrastructure, implementing all the latest recommendations from its service providers and best practice security recommendations overall. It is suggested to include a security awareness training for the employees, as part of corrective actions.

Our methodology, consists on comparison of the steps of our suggested response plan in case of a cyber-incident that involves fraudulent transactions, against each Albanian financial institution, as represented in Figure 1.

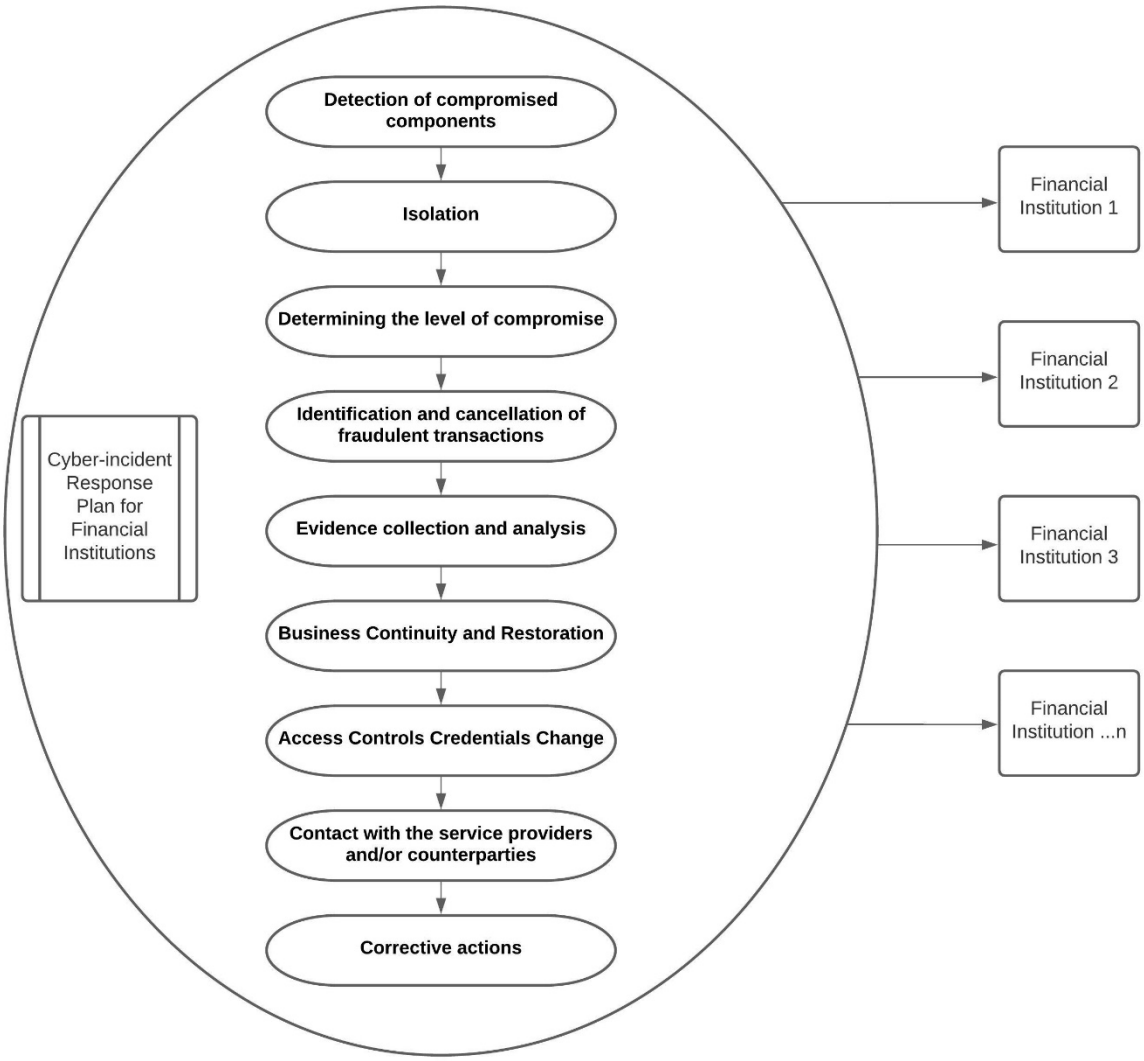

Figure 1 – Comparison of the steps of our suggested response plan in case of a cyber-incident against each financial institution

Our findings and recommendations are discussed next.

RESULTS AND DISCUSSIONS

From our investigation, it resulted that all Albanian financial institutions that we contacted and studied for the purpose of this paper, had an Incident Management procedure in place and a Disaster Recovery procedure, but less then half of them had a defined plan in case of a cyber-incident involving fraudulent transactions, and only one of these institutions had this plan tested as real-life scenario.

Below we have provided our findings, so that the financial institutions shall focus on the areas that need the most improvement in order to better manage a cyber-incident situation.

All institutions should have a response plan with at least the steps that we provided. This plan shall be further detailed according to the institution, in order to be easily executed. Further details include a list of all components of the most important systems that store valuable data and can be used to send transactions. This can come handy in the first steps of the plan – the compromised components are checked in the list and then isolated. Financial institutions should also be able to isolate each of the above components. A list of all correspondents (phone numbers and e-mails) and of service providers of abovementioned systems could be handy. The service providers may be contacted at any level of compromise, while correspondents may be contacted if fraudulent transactions were sent. Also, a list of what kind of evidence should be collected, like Active Directory, operating system, application and network logs, snaps of virtual machines, disk images etc. should be included in this plan. An important element is the timeframe allowed to stay out of business, which can help decide when to perform the business continuity or disaster recovery procedures. A list of internal staff and higher-ups that should be contacted and informed for the situation should be added as well, and also not to forget a list of all human and non-human users, which credentials should be modified after a cyber-attack. An important part of the plan is also a team for analyzing and deciding for corrective actions.

The plan should be updated and tested at least once a year.
Another important consideration is that the hacking methods that the suffered institution discovered, to be shared anonymously or not, so that other institutions can protect itself.
Also, the central institution shall be contacted as soon as possible, in order to isolate the affected participant from important central systems until further notice.

CONCLUSIONS

As the number of cyber-incidents including fraudulent transactions are growing globally, Albanian financial institutions should be prepared for such an event.

Of course, it is very important to take every known preventive measure and update and implement security recommendations frequently, but in case that a cyber-attack happens, a response plan with clear steps on how to deal with the situation will help lessen the impact, both reputational and financial. With well documented and executed steps of the plan, the time that the business needs to bounce back also shortens. The involved parties are informed in time, and each of them provides their help and benefit to solve the situation and prepare better for the future. In this paper, we focused on cyber-incidents involving fraudulent

transactions, as this not only causes harm for the affected institution, but also triggers a chain of events including other parties.

The most important vulnerabilities that we found were the lack of a plan in case of a cyber-incident involving fraudulent transactions, the lack of its testing and not very well-defined actions and actors in the steps of the plan, for the institutions that had such plan.

It is very important to understand that business continuity procedures are not the same as this plan and not a substitute for it.

The findings of this paper, although Albanian Financial institutions were in scope, can be applied in every system that is focused on high information security.

REFERENCES

[1] https://www.kaspersky.com/resource-center/definitions/data-breach
[2] https://www.6dg.co.uk/blog/biggest-data-breaches-financial-services/
[3] https://sqnbankingsystems.com/blog/manipulated-data-new-bank-hack/
[4] https://medium.com/@kvantorcom/top-5-biggest-swift-hacks-52fca78145c
[5] https://www.infosecurity-magazine.com/news/swift-software-exploited/
[6] https://attack.mitre.org/