ISMN5740-TMX bank case

Bojun zhang

11/25/2021

1 Executive Summary

In about business company information technology, a disaster is considered a sudden, unplanned event that results in damage or loss of data value. These threats are often classified as natural and man-made, with data theft or cyber-attacks occurring almost every day, especially against information technology companies. So, identify the company's key assets and prioritize them to keep the company running. As well as identifying vulnerabilities and threats, finding out which assets they affect, and making appropriate controls to reduce their probability and harm. All of these can effectively help the company to understand how to deal with and reduce the loss when the harm happens. And keep the company running as smoothly as possible.

As TMX Bank is a customer-oriented company that relies on the Internet and information technology, it is very important to ensure the normal operation of the company at the technical level. Below is a list of the company's important assets and the main functions of these assets. Then, it will list the vulnerabilities and threats corresponding to the assets, and the occurrence mode and corresponding control of these threats, to help the company's leadership and technical personnel make decisions in the fastest and most effective way when risks occur.

1.1 critical assets of the bank

- **Official website:** which is not only the most expensive asset in the information given by the bank but also the official website is the core to ensure the normal operation of the bank. The app connects to the company's database, the back end of the network, and a large number of customers make transactions on the app every day.

- **Various servers: Web Server, File Server and Mail Server**: These servers support the company's most basic activities. As TMX is a bank, it needs to deal with a large number of clients and deal with a large number of documents, emails and documents every day, so it is very important to ensure the normal operation of these servers.
  Database server: The database is the most central of TMX Bank's key assets. First of all, it has the function of preserving the company's customer data, transaction data, personnel and various data. Secondly, the database and software, as well as the back end of the web page, play a role of connection. For example, people need to add, delete, change and check the database for transactions on the web page or mobile app. TMXbank has a responsibility to protect the confidentiality of the data, and the value of the data is a significant part of the company's property.

- **Firewall:** firewall is the basic to ensure the technical operation of the company's network.

Ensure the security of the company's internal network, prevent unauthorized access, and ensure the confidentiality, integrity, and availability of the company's internal data. In addition, it can isolate the connection between the risky area (Internet or risky network) and the secure area (LAN) without blocking people's access to the risky area.

1.2 vulnerability exist

- **Vulnerability of official website**: In direct customer contact, the most likely vulnerability is the URL redirect vulnerability. URL hopping is a normal service function, and most websites need URL hopping. However, the URL to be jumped to is controllable, so URL jump vulnerability may occur. And the attacker is to use this vulnerability, some normal links to the fraud site. The second one is non https connection, HTTP is transmitted in clear text over the Internet, so the contents of submitted forms, such as passwords, are also transmitted in clear text over the Internet, so there is a risk of eavesdropping. HTTPS is an HTTP channel that aims at security and encrypts transmitted data. A third party cannot intercept, monitor, or tamper with transmitted data, protecting the login page.

- **Vulnerability of Database server:** Servers have many common vulnerabilities, and I will focus on database server vulnerabilities here. First of all, the common vulnerability of various servers is that the default setting is not secure, generally is the permission setting is not rigorous, some FTP passwords are recorded on the server, and some root passwords are directly in the connection file, no security awareness is easy to lead to successful hacker attacks. As for database vulnerabilities, the first is weak password, which is too simple to set the account password, so that hackers can easily crack it, so as to modify the database or steal data. The second is the authority problem, involving access authority, database is facing two major problems: employees are given too much authority than the work needs; Unauthorized or malicious use of valid permissions. Misconfigured databases may be caused by too much work on the part of the administrator, or because business-critical systems simply cannot afford downtime to check the database.

- **Vulnerability of Firewall:** IDS and IPS are not installed. IDS stands for "Intrusion Detection Systems". Professionally speaking is according to a certain security strategy, through the network, system running status monitoring, as far as possible to find all kinds of attack attempts, attack behavior or attack results, to ensure the confidentiality of network system resources, integrity and availability. The second problem is patch management. Patches are not updated in time to achieve the best protection effect. If the firewall is incorrectly configured, or the monitoring area is incorrectly configured, the internal area to be protected cannot be fully protected.

1.3 Threats may exploit the vulnerabilities

- **Threat of official website:** Distributed denial of Service (DDoS) attacks are malicious acts that overwhelm a target server or its surrounding infrastructure with massive Internet traffic to damage the target server, service, or network traffic. A web crawler is a program or script

that can automatically access the Internet and download the content of a web site. It can transfer information from other people's web sites to its own computer. Captured web pages will be stored by the system, certain analysis, filtering, and index.

- **Threat of Database server:** The first is permissions. There are two types of threats to databases -- one external and one internal. It is not uncommon for employees to steal database backups to obtain large amounts of personal information, whether out of revenge or profit. SQL injection: SQL injection is not only the most common database vulnerability, but also the number one threat on the Open Web Application Security Initiative (OWASP) application security threat list. Attackers inject SQL queries into the database to read data, modify data, perform management operations, and even issue instructions to the operating system.

- **Threat of Firewall:** Mainly hacking attacks, some of the technical aspects of the attack are listed below. IP spoofing attacks, which modify the source, destination IP addresses, and ports of packets, imitate legitimate packets to fool the firewall. Trojan horse attacks are the most effective attacks against packet filtering firewalls. Once you install Trojan horses on the internal network, the firewall is basically powerless.

1.4 Top 3 risks

1.4.1 official website blocked

- **Description:** The risk can be divided into two situations. The first is that the server responds slowly due to heavy customer traffic. Another is malicious attacks by hackers, who use DOS or DDOS technology to attack the website of TMXbank, leading to the direct failure of the website.

- **Result:** Official website, from the source the value of the mirror network is 64000, all estimates of the official website value is 150000. According to Gartner, the average cost of network downtime is around $5,600 per minute. That calculates to roughly $300,000 per hour, In addition to the monetary injury, IT downtime wears heavily on your productivity levels and ongoing business operations.

- **Control:** The use of high-performance network equipment, adequate network bandwidth guarantee, network bandwidth directly determines the ability to resist attacks. Secondly, the installation of professional anti-DDOS firewall, the most secure way is to use the third party professional anti-attack firewall for defense, simple match can open protection. Second is to set up a mirror site, when the main site cannot work properly, you can switch to mirror site services.

1.4.2 Database data loss

- **Description:** This refers to malicious theft of data from a database, or data in the background

of a web page. Generally more common have SQL injection, crawler. Some hackers use technology to steal confidential data, which leads to the disclosure of users' and companies' private information. And through the operation of the database, tamper with the database of specific web pages, directly resulting in profit loss.

- **Result:** The value of Customer data and Daily transcation Data from data backup is 64,000$, and the estimated value of company data is about 80,000$. A breach may also include the loss or theft of physical documents that include PII or portable electronic storage media that store PII, the inadvertent disclosure of PII on a public website. A customer-focused company like TMXbank should protect the privacy of its customers.

- **Control:** Rights distribution follows the principle of minimum rights. Only employees are granted the minimum rights required to complete their work. Database access is also carefully monitored to ensure that employee permissions are only used for authorized operations. During development, SQL injection tests are performed on input variables. After the development, use firewall to protect the Web - oriented database. Encrypt archived data and closely monitor archived data access and usage.

1.4.3 Firewall is invalid or damaged

- **Description:** Firewalls are a fundamental part of any company's network security architecture. There are five common risks, such as Insider Attacks, Missed Security Patches, Configuration Mistakes, A Lack of Deep Packet Inspection, DDoS Attacks, which can cause firewalls to fail to secure internal software or servers.

- **Result:** The cost of TMXbank's firewall is $64,000, exposure Factor is 50%, and there are two successful firewall attacks a year. According to quantitative analysis, SLE is $32,000, AND ALE is $64,000. Secondly, after the firewall is destroyed, it may also lead to the theft of internal documents and confidential data, which may bring huge losses.

- **Control:** Update patches in time to ensure that the firewall is in the latest and most appropriate version. The proper location of the firewall can ensure the security of the internal network and confidential network area to the greatest extent. If you need to find a third-party company, looking for professional companies to set up a firewall, can make the firewall higher performance, but also more convenient management, more security.

2 Cost benefit analysis

2.1 Mirror Website Control

The first control concerns network congestion that makes it impossible for the company to operate normally. The method adopted is to set up a mirror network. The server cost in the figure is from TMXbank data, the staff salary is the average salary of IT staff, and the venue cost is the estimated value.

Category	Details	Cost In First Year($)
lease servers	If primary server is unavailable the redundant mirror can replacement for the primary serve	125,000
Hire two more operation staffs	Salary, including benefits Recruitment costs Orientation and training	$120,000 $11,250 $3,000
one additional workstations	Furniture and hardware Software licenses	$3,000 $1,000
total		**263,250**

Benefit	Benefit within one year($)
20 percent revenue increase from website	$1,000,000
Improved customer service and retention	500,000
total	**1,500,000**

2.2 Data breach Control

This control is mainly to find third-party institutions to back up data. Daily transaction data and customer data are uploaded to the third-party platform. If data is lost or damaged, it can be imported from the third-party platform. At the same time, you can also set up a firewall against the database, making security higher. The cost comes from the quotation of the third party platform, the salary comes from the average salary of IT personnel, and the company's policy is the estimated value.

Category	Details	Cost In First Year($)
Cloud Data Backup (Recovery Point Objective)	Get the server's data from the data center and put it back on the new server	36,000
Database Firewall	usually on a proprietary operating system	10,000
Hire one more operation staff	Salary, including benefits Orientation and training	70,000 3,000
Security policy	Company internal database security policy, to ensure that employees operate the database properly	$1,000
total		**120,000**

Benefit	Benefit within one year($)
Reduce losses of breach data	$320,000
Guarantee related company projects(website,transaction software)	$500,000
Customer information security, improve satisfaction	$300,000
total	**1,120,000**

2.3 Firewall Control

Every business organization that's connected to the Internet needs a firewall to protect the internal network from attacks but selecting the right firewall can be an overwhelming task. In the data of TXMbank, it shows that they have purchased a firewall for the front end of the web page, but I noticed that there is no firewall for other areas, so MY control is to add firewalls for loan software, customer processing software and host server. These firewalls are purchased from outside, and the price comes from outside platforms.

Category	Details	Cost In First Year($)
host-based firewall	simple, low cost programs or devices intended to protect a single computer	30,000
Software Firewall	usually on a proprietary operating system	10,000
Hardware firewall	basically dedicated PCs with hard disks and those that are solid state devices built on ASIC (Application Specific Integrated Circuit)	10,000
other	Software licenses	$1,000
total		**51,000**

Benefit	Benefit within one year($)
Reduce firewall losses	$320,000
Reduce losses when servers are attacked	$13,000
Reduce loan and customer software losses	$200,000
Reduce losses of breach data	320,000
total	**853,000**

3 Business impact analysis

Scope the Business Impact Analysis

As a customer-oriented company, TMXbank deals with a large number of transactions and provides services to a large number of customers every day, so ensuring business continuity is critical. Business Impact Analysis (BIA) is a systematic process used to identify and assess the potential impact of disruptions in critical business operations due to disasters, accidents, or emergencies. The first thing to determine is what needs to be protected, disasters are usually divided into physical and technical, physical including natural disasters, power failure, machine aging, etc., the system has database security, information security, etc. Both are important, but I prefer to focus on system-level disasters here to ensure that problems are identified, impacts determined, and solutions addressed.

Prioritize impact from top to bottom

- **Official website problems**

  Usually, the official website is the most vulnerable to attack, and IT is also the most important component of a company. When the official website fails to work properly (under hacker attack, or the server cannot bear the heavy customer flow), the affected departments include HUMAN resources, communications, and IT. The positions in charge are website operations, IT, and management. The affected business area is almost all online transactions, customers are unable to view, trade and other activities.

  The frequency of the official website not working normally is about 4 times a year, which is very critical, because every hour will bring millions of yuan of losses. RTO should be controlled within 1 hour, and MAO should be controlled within 4 hours to avoid huge losses to the company.

  strategy

  Contact the COMPANY's IT department and network operation and maintenance personnel, enable the mirror website, find the cause of the fault, and rectify the fault as soon as possible.

- **Database and data security issues**

  TMXbank needs the database to connect to various activities, for example, the background of the official website is connected to the database, bank APP, customer and Loan Software are connected to various databases, so it is very important to ensure the security and availability of the database. In addition, attention should also be paid to PII. The company has a large amount of data every time, including valuable transaction data and customer information, so it is also important to ensure the confidentiality of these data.

  When a database is compromised or does not work, it affects almost all the activities associated with that database, so there is a lot of damage. The affected departments are marketing, IT, finance and customer service. Database breaches happen about twice a year, which is critical because it affects most of the company. RTO should be controlled within 1 hour and MAO within 2 hours.

  strategy

  Contact a third party to import prior data (RPO), if there is a problem with the database server, enable the standby server data, and the IT department conducts a full review to discover whether IT is an internal or external factor.

- **Firewall issues**

  All the time, hackers are studying the technology and means of attacking firewalls, and the methods and technologies of attacking are becoming more and more intelligent and diversified. But on the process of hacker attack firewall, it can probably be divided into three types of attacks. The first method of attacking a firewall is to detect what kind of firewall system is installed on the target network and find out what services are allowed by this firewall system. We call it a probing attack on a firewall.

  The second type of attack firewall is to take address spoofing, TCP serial number attacks and other methods to bypass the authentication mechanism of the firewall, so as to destroy the firewall and internal network.

  The third kind of attack firewall is to find and use the firewall system implementation and design of security vulnerabilities, so as to launch targeted attacks. This kind of attack is difficult, but very destructive.

  If the firewall fails, then all confidential documents and data of the company are in danger of being stolen. I cannot find the frequency, I think the design time as soon as possible, control within 30 minutes of redeployment.

  strategy

  If the firewall fails, contact the third-party company for help. At the same time, contact the internal IT department of the company to monitor the network and ensure Intranet security.

Reference

Essential Features of a Loan Management System. NIDHI AGARWAL, OCTOBER 22, 2020, from https://www.leadsquared.com/loan-management-system-features-benefits/

How to protect yourself against hackers. (n.d.). Retrieved April 26, 2021, from https://www.ag.state.mn.us/consumer/publications/HowtoProtectYourselfAgainstHackers.asp

Eric Dosal, 2018/04/12, 5 Firewall Threats and Vulnerabilities to Look Out For, from(www.compuquip.com)

Effective solution to web site network blocked, 2018/01/16, from https://jingyan.baidu.com/article/fec7a1e5c5261d1190b4e7f7.html

ChipsDie, 2020-09-14, HOW to Defend against SQL injection Attacks, from https://www.php.cn/faq/419041.html

How to secure you site with HTTPS, Google search, from https://developers.google.com/search/docs/advanced/security/https

How Much Does Data Backup Cost for Small Business?, March 31, 2015 https://resource.optimalnetworks.com/blog/2015/03/31/cost-data-backup-small-business

Choosing a Firewall, Deb shinder, 2004,02 23, from https://techgenix.com/choosing_a_firewall/