VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

DISASTER RECOVERY AND BUSINESS CONTINUITY MANAGEMENT
BCI-3002

PROJECT TITLE - PREVENTION OF ATTACKS USING ONE CLASS CLASSIFICATION AND AUTO ENCODERS

Team members:
Harshita Pundir 18BCI0192
Rohan Allen 18BCI0247
Rakshith Sachdev 18BCI0109

Metrics of DR and BC:

1. **MTD (maximum tolerable downtime)**

   For each business process, MTD is the maximum time that each business process can be inoperative before significant damage or long-term viability is threatened. Different business functions will have different MTDs. If a business function is categorized as mission-critical, it will likely have the shortest MTD. There is a correlation between the criticality of a business function and its maximum downtime. The higher the criticality, the shorter the maximum tolerable downtime is likely to be.

   Downtime consists of two elements, the systems recovery time and the work recovery time. Therefore,

   MTD = RTO + WRT.

   This project can be divided into functionalities like malware profiling, feature generation, feature database, machine learning classifier, and finally malware detection which separates into malware traffic and clean traffic. Each functionality will have their own MTD based on their criticality. In this the machine learning classifier and malware detection are mission critical, and feature generation and feature database falls into business critical functionalities.

2. **RTO (recovery time objective)**
   Recovery time objective (RTO) is a key metric that helps calculate how quickly a system or application needs to be recovered after downtime so there is no significant impact on the business operations. In short, RTO is the measure of how much downtime can be tolerated.
   If any disaster occurs on this system, the response team begins the recovery process, which starts through the RTO process. This includes restoring backups of feature databases,and machine learning classifiers.

3. **Work Recovery Time (WRT)**
   It is the time critical business functions take to get back up and running once the systems (hardware, software, and configuration) are restored. If the systems are back up and running, they're all set from an IT perspective. From a business function perspective, there are additional steps that must be undertaken before it's back to business. These are critical steps and that time must be built into the MTD. Otherwise, MTD requirements will get overlooked and potentially put the entire business at risk.
   If any disaster occurs on this system, transactions since the last backup might be missing. If so, they are recovered during the Work Recovery Time. Once the WRT is completed, the critical business functions including the feature database and machine learning classifier are fully recovered.

4. **RPO (recovery point objective)**
   Recovery point objective (RPO) is a metric set for the amount of data loss the business can endure and continue to function without any effect on the business operations.
   To calculate the recovery objective values, you need to prepare a list of the workloads and divide them based on their criticality levels. Depending on the priority of applications, individual RPOs and RTOs typically range from 24 hours down to four, down to near-zero measured in minutes.

Criticality level of workload	RTO & RPO values
Mission-critical Workloads	Less than 15 minutes
Business-critical Workloads	2 to 4 hours
Non-critical Workloads	12 - 24 hours

If any disaster occurs on this system, in the RPO phase, critical business functionality of the malware detection and traffic separation function are restored.

5. **Cost of downtime**

   In case of any disaster on this system, the cost of downtime is a combination of lost revenue, business disruption— which includes reputational damage and customer churn, end-user productivity, lost internal productivity, contractor costs, equipment replacement, and employee retention problems.

   To get a quick estimate of a company's probable downtime costs, use the following formula, based on the size of the business and the number of minutes the most recent incident lasted:

   Downtime cost = minutes of downtime x cost-per-minute.

6. **Confidentiality**

   Confidentiality in BCP could for example be the transfer of personal data during a disaster recovery. An objective of disaster recovery is to minimize risk to the organization during recovery. There should be a baseline set of documented access controls to use during recovery activities. They are necessary to prevent intrusions and data breaches during the recovery. The impact here can be one of reputation but also of financial nature. If a competing company can for example obtain a set of investment strategies, it could assist the competing company to invest against them, resulting in significant financial losses and even bankruptcy.

   In this project confidentiality is maintained for the separation system of clean and malware traffic. This protects the private data of the end users from broadly categorized attacks like DoS attack, Probe attack, User to Root attack, and Remote to Local attack.

7. **Integrity**

   These measures include file permissions and user access controls. Version control may be used to prevent erroneous changes or accidental deletion by authorized users from becoming a problem. In addition, organizations must put in some means to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash.In terms of availability the risk to business continuity is often explained as a service interruption on a critical system, e.g. a payment gateway of a bank goes down, preventing transactions from occurring. The short- and long-term impact are financial losses due to the bank not being able to process transactions, but also clients becoming more and more dissatisfied.

In case of a disaster, the integrity of the feature database must be maintained for the smooth functioning of protection of the network.

8. **Availability**

   This core security principle is defined as the ability to grant authorized users uninterrupted access to systems and information. In more general terms, if someone is supposed to have access to a system or information, then that system or information should be made available to them at all times.There are many cyberattacks used to violate availability including, computer viruses, malware and denial of service (DoS). There are also circumstantial events that violate availability such as hardware failure and natural disasters.

   This system cleans the traffic of all the dangerous attacks like DoS, Probe, User to Root and Remote to local, hence preserving the availability of the network devices.

9. **Risk Impact assessment**

   Assessing risks is one of the first steps required in finding a way of reducing them and therefore keeping your infrastructure safe. Creating an effective disaster recovery plan starts with searching for potential threats and vulnerabilities of your infrastructure elements, as well as the ways to respond to them. Risk assessment is not a one-time process. You should regularly update your risk assessment policies, especially if you are running a constantly changing infrastructure.

   Disaster recovery risk assessment is a document that contains a description of potential risks to the functioning of an organization. It covers both natural and man-made disasters and estimates the probability of each scenario occurring. The results of the estimation are then multiplied by the consequences of an incident. The value you receive defines your organization’s level of protection against a given threat. Some of the basic topics the document is supposed to highlight are the following:

   - Potential damage the incident may cause;
   - Amount of time and effort required to mitigate the effects of the incident & associated costs;
   - Preventative measures to reduce disaster risks;
   - Instructions to reduce the severity of an incident.

10. **Business Impact analysis**

    A business impact analysis (BIA) is the process of determining the criticality of business activities and associated resource requirements to ensure operational

resilience and continuity of operations during and after a business disruption. The BIA quantifies the impacts of disruptions on service delivery, risks to service delivery, and recovery time objectives (RTOs) and recovery point objectives (RPOs). These recovery requirements are then used to develop strategies, solutions and plans.

It is critically important for the survival of your business to identify processes, systems, and operations that are of eminent priority; that is the central focus of the business impact analysis (BIA). Its purpose is to determine how the interruption of your business operations may affect your organization. Potential effects include the loss of data, equipment, and revenue, loss of staff, reputational damage, and other types of business losses. Business impact analysis is an important stage in developing a disaster recovery (DR) plan, the mission of which is to ensure operation of a company's infrastructure and applications in case of a major outage. A comprehensive disaster recovery BIA report is one the most crucial elements required to devise an emergency response strategy.

In this system, functionality like machine learning classifiers and malware detection are critical to the mission, and feature generation and feature databases are critical to the business. With this the priority of the functions can be set to get the impact analysis.

Problem Statement:

As the modern day and age become digital, the network and end point devices become a target for attacks and exploitation; therefore, many systems have become associated with security-related issues. Therefore, making systems safe and secure is very important. According to the 2020 Unit 42 Threat Report, almost all gadget traffic is decoded, which means that most of the classified and individual user information in the network is highly vulnerable to cyber-attacks. Network security is used to delay unintentional harm which can be done to the network's private information, its users, or its devices. The main purpose of network security is to secure the network running and for every single authentic client.

In this project, we aim to prepare one-class classifiers to utilize generous information to recognize ordinary and dangerous traffic redirected to an end device. The idea is to train the system to differentiate between bad network traffic which might contain some virus, malware to the system, or any other type and normal network using machine learning. The model is to be trained to predict false data and henceforth prevent the installation of any particular software during the risk of an attack, which results in an increased cost. The main key objective is to provide maximum accurate results by using

unsupervised learning/ one class-based modelling with auto encoders approaches and reducing the processing time significantly.