Irmina Chmielowska

Kamil Kwiatkowski

Krzysztof Pochrebiennik

Jakub Wrzodek

Przemysław Gradziński

Christian Emmanuel Nteranya

**Internet Shop Contingency Plan**

**1. Introduction**

* 1. Background
  2. Scope

**2. Concept of operations**

**2.1. System description**

**2.1.1. Information system name**

Empiks\_system

**2.1.2. Information system Owner**

Name: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Title: Director of Operations

Agency: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Address: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Email address: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Phone number: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**2.1.3. Authorizing official**

Name: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Title: Manager of Operations

Agency: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Address: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Email address: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Phone number: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**2.1.4. Assignment of security Responsibility**

Name: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Title: Information security officer

Address: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Email address: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Phone number: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**2.1.5. Information System Operational status**

The system is operational and checked regularly, and updated when needed according to the users’ feedback and new efficient technology on the market.

**2.1.6. General system description**

**a. System environment**

The system has realized the function of “an internet shop” and the condition of shopping online will not be restricted by time but will be only accessible to some regions.

**b. Related technologies**

**- Java and JSP:** Java is used in this system as programming language, the reason to choose it is determined by its powerful characteristics. And the technology of the system is JSP (Java Server Page), a mainstream development techniques based on Java Servlets. Therefore, JSP can be cross-platform operation of web development, and makes the web application simpler and faster.

**- Spring architecture:** The Spring framework provides a full-featured MVC module for building Web applications with spring’s pluggable MVC architecture. It is configurable with multiple voew technologies e.g. JSP, Velocity, Tiles, … Spring MVC separates the roles of the controller, model object, dispatcher Servlet and the handler object.

**c. System requirements**

In term of operations, the system runs in Windows, using MySQL database, which has good performance in operation and management.

The system has the following functions:

A personalized user interface and straightforward to use, the systematic proscenium is equipped with display function of commodity information, so that customers can browse and compare commodity.

Classification of goods is followed by, which plays an important role in the convenience of choosing items. The next section is the design of shopping cart, users can add items to it, and change the quantity at pleasure. It is necessary to implement the function of setting up the bulletin board of the commodity and sales ranking of goods, so that customers can get the latest information on shelves and some special offers.

There are two modules included, demonstrating the website module, and background management module. Functions are supposed to be realized by foreground of system. Module of Commodity is consisted of three parts: the part of New Products shows the latest fad products, which is visually appealing and stood out. And products in Special Offers always are more affordable and durable. The sales ranking shows all commodities, which is convenient for users to choose items they prefer. Two main aspects are included in Users Module, they are Users Registration and Users Login. Shopping Cart, as the name implies, the function of it is that adding items to it and Manage items which users choose. And users have permission to modify the number of items and empty the cart. Comments are good for customer communication and it promotes designers to improve the system. Meanwhile, the modules of Adding Comments are convenient for users to communicate

System

Foreground

Function

Graph

Commodity

Users

Message

Board

Shopping

Cart

New Products

Special offers

Sales Ranking

Users Registration

Users Login

Adding Items

The Management of

Shopping Cart

Adding Comments

Checking Reviews

In our system, the first step is users’ operation on client side. For example, users submit forms in client side, and send requests to server and wait server’s response. The next step is operation on server side, the server accept and process request, such as process the data requested by shopping cart, calculate the data. The last step is sending information according to the feedback and display results to users.

Browser

Finish

Server

Request server

(Get / Post)

Receive and

response HTML file

Organize related

resource files

Display pages

Http Request

URL Path

Http Response

Accept Request

Generate HTML files

based on URL parameters

Send HTML files to

browser

User

inAt present, current, mainstream databases include Oracle, MySQL, … The reason to choose MySQL due to comparison with other databases, which is more lightweight than Oracle, and more advanced in performance of query speed and support schema than SQL SERVER. With rapid increase of data, users and number of visitor, the system is confronting higher demand in technology and platform. In order to have better management of data, the system uses MySQL database system, which is mainly used for storing all kind of related information of the commodities, the system mainly establishes the table of commodities, orders, users and messages.

**2.2. Overview of Three phases**

This Information system Contingency plan has been developed to recover and reconstitute the Empiks\_system using a three-phased approach. This approach ensures that system recovery and reconstitution efforts are performed in a methodical sequence to maximize the effectiveness of the recovery and reconstitution efforts and minimize system outage time due to errors and omissions.

The three system recovery phases are:

**2.2.1. Activation and Notification Phase**

The activation of the ISCP will occur in the following cases:

- Unavailability of the system

- Servers are down

- Data corruption

- Unavailability of data

- Hacking attempts of the system

Once the ISCP is activated, system owners and users are notified of a possible long-term outage, and a thorough outage assessment is performed for the system. Information from the outage assessment is presented to system owners and may be used to modify recovery procedures specific to the cause of the outage.

**2.2.2. Recovery Phase**

The process of recovery will be determined according to the event occurred.

The activities and procedures for recovery will depend on the event described in order to recover full access and control of the assets.

**2.2.3. Reconstitution**

The Reconstitution phase defines the actions taken to test and validate system capability and functionality at the original or new permanent location. This phase consists of two major activities: validating successful reconstitution and deactivation of the plan. During validation, the system is tested and validated as operational prior to returning operation to its normal state. Validation procedures may include functionality or regression testing, concurrent processing, and/or data validation. The system is declared recovered and operational by system owners upon successful completion of validation testing. Deactivation includes activities to notify users of system operational status. This phase also addresses recovery effort documentation, activity log finalization, incorporation of lessons learned into plan updates, and readying resources for any future events.

**2.3. Roles and Responsibilities**

- Crisis Manager: responsible for directing the recovery of business operations and has full authority to make decisions related to recovery efforts. The Crisis Manager will be responsible for communications with the insurance provider.

- Recovery Management Team : are responsible for implementing the portions of the Recovery Plan for their functional areas and are given authority to do so by the Crisis Manager.

- IT Manager: will implement the IT Systems Recovery program and maintain all IT operations.

- Security Manager

- Engineer

- admins

- monitoring and administer group

-devops team – ICE reestablish the service, block the threat

- Media Relations Manager: will establish and maintain contact with the news media and other organizations concerning disaster recovery operations.

- Vendor/Contractor Manager: will reestablish and maintain contact with vendors and contractors to provide supplies and services during recovery from a disaster.

- Human Resources Manager: will implement any changes or amendments to personnel policies during disaster recovery, and administer personnel relocation or layoff programs.

- Customer Service Manager: will reestablish and sustain communications with customers, and resume other customer services as soon as feasible.

- Recovery Command Center Supplies Manager: will provide basic supplies and services for Command Center operations.

- Suppliers and contractors: suppliers and contractors who have agreed to provide supplies and services following a disaster or any major business disruption will perform work and provide materials and equipment necessary to return to normal operations.

- Critical operations support staff: which consists of key employees that are considered critical for the continuation of business operations after a disaster, will work together as a team to keep the business going during the recovery.

**3. Identify and prioritize resources**

**4. Identify the key risks**

**5. Prioritize risks based on their impact and probability**

**6. Contingency plans**

**6.1 Hacking attempts**

**3. Risk prioritizing criteria**

Following risk prioritizing rules have been chosen:

* Prioritizing by probability of occurrence
* Prioritizing by criteria of impact, as percentage of annual income

Which has been gathered in following tables:

|  |  |  |
| --- | --- | --- |
| Probability of occurence criteria | Point value | Case |
| Rare | 1 | An event can occur only in exceptional circumstances (event that occurs once in 5 years), it concerns individual cases. |
| Unlikely | 2 | It is unlikely that this event will occur (event that occurs once per 2 years), it applies to a few cases. |
| Moderate | 3 | The event is likely to occur in the near future (event that occurs once per year), it applies to some matters |
| High | 4 | The occurrence of the event is very likely (event that occurs at least once per year). It is expected that such an event may occur several times a year. |

Table 1. Probability of occurrence criteria.

|  |  |  |
| --- | --- | --- |
| Level of impact | Point value | Case |
| Trivial | 1 | Negligible effect on the objectives and tasks of the organization, no legal effect; slight financial effect, no impact on employee safety, no impact on the image of the organization.  Less than 0,1% of annual income |
| Minor | 2 | Little impact on the achievement of goals and tasks, without legal effects, little financial effect; no impact on employee safety, little impact on the image of the organization.  0,1 – 1% of annual income |
| Moderate | 3 | The average impact on the implementation of objectives and tasks, potential threats may lead to the failure to perform basic tasks within a specified scope, moderate legal consequences, average financial effect, no impact on employee safety, medium risk of losing good image.  1 – 5% of annual income |
| Major | 4 | Serious impact on the implementation of the task, including a serious threat to the date of its implementation and achievement of the goal; extensive legal consequences; threat to employee safety; high financial losses; loss of a good image of the organization in the environment and in public opinion.  More than 5% of annual income |

Table 2. Level of impact criteria.

Risk values have been calculated as multiplication of impact and probability.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risk | | Impact | | | |
| 1 | 2 | 3 | 4 |
| Probability | 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 6 | 8 |
| 3 | 3 | 6 | 9 | 12 |
| 4 | 4 | 8 | 12 | 16 |

Table 3. Risk values

We consider risk as: Low – [1 to 2], Medium [3 to 7], High [8 to 16]

**4. Risk identification and prioritizing**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Probability | Impact | Risk |
| Technological Issue | | | |
| Infrastructure failure | 2 | 2 | 4 |
| Software virus | 1 | 2 | 2 |
| Interface problems | 2 | 1 | 2 |
| Data corruption | 2 | 2 | 4 |
| Hacking attempts | 3 | 4 | 12 |
| Users data leakage | 3 | 3 | 9 |
| Fraud (e.g. access without authorization) | 3 | 3 | 9 |
| Unavailability of product suppliers | 2 | 2 | 4 |
| Gap in the software used | 2 | 2 | 4 |
| Internal software errors | 3 | 2 | 6 |
| Political Issue | | | |
| Changes of law | 1 | 4 | 4 |
| Competitive Issue | | | |
| Unfair competition | 2 | 2 | 4 |
| Piracy sites | 4 | 3 | 12 |
| Significant decrease in the number of customers | 1 | 3 | 3 |
| Lack of goods providers | 1 | 3 | 3 |
| Resources Issue | | | |
| Physical theft of computer equipment | 1 | 4 | 4 |
| Hardware failure | 2 | 3 | 6 |
| Service delays | 3 | 3 | 9 |
| Loss of power supply | 2 | 3 | 6 |
| Physical damage | | | |
| Flood | 1 | 3 | 3 |
| Fire | 2 | 3 | 6 |
| Cost issue | | | |
| Budget exceeded | 1 | 3 | 3 |

Contingency plan for hacking attempts

1. Introduction

The hacking attempts are divided according to the areas they affect.

First area is applies to attacks directed directly at the system (internet shop).

Second area applies to attacks directed at workers (programmers, testers). Due to epidemiological threat, many of them is forced to work remotely, what   
opens up new opportunities for attacks.

Last, third area applies to attacks directed at user, e.g. stealing their login credentials.

2. Preparation

Security information and event management provides reports for unusual traffic and behaviors detected in network. They are grouped into 3 categories, based on threat level, in order to make them maintainable. Any incident or breach detected, classified at level 2 is saved separately. If incident or breach is well known and described, automated steps can be taken. If so, they are also reported.

Any incident or breach detected, classified at level 3 causes immediate alert to the first contact administrator. In this case, the first contact administrator checks, what resources have been compromised, and then takes further steps.

Other incidents are aggregated into one document, evaluated weekly. They are sorted into categories and increased grow in one of them may be the reason to initiate the investigation.

Any person involved in contingency plan, must be must be trained, in order to determine the method of communication. After serious incident, all people involved in the process are informed via company’s communicator, and text message. After that, an online meeting is taking place at company’s video communication platform, in specially prepared room. In case, when company’s network is unavailable, the meeting takes place directly at company’s building, in specified conference room. When one of people involved is unable to arrive within one hour, he informs about this fact the first contact administrator, and have to be on a standby on phone until the meeting is finished, in order to get information what steps needs to be taken.

3. Detection and analysis

Detection of incident is based log aggregation solution and intrusion prevention system (IPS).

Areas that are monitored are:

1. suspicious, unusual activity on users and employees accounts
2. recognition of brute force attack (e.g. multiple connections from same address)
3. filtering and blocking emails

After detection of incident, the suspected address is added to the watch-list for 24 hours. If new suspicious actions are detected in this period of time, the incident level of risk is increased and the incident is reported.

Any e-mail, that contains links is considered as suspicious, alike e-mails from unknown senders. After confirming an malicious e-mail incident or breach, all messages from sender are blocked.

Login attempts are monitored and logged. If there appears a significant number of login attempts to single account, the owner of the account is informed about it via e-mail.

Also, geolocalization is used, in order to detect anomalous connections.

Any unusual traffic from single user is logged. This includes also monitoring the external/removable data sources (like monitoring usb ports of workers). If many of incidents are detected, then specific user is reported as suspicious of being compromised (e.g. affected with malware).

Unavailability of any of the services offered by the system, when detected, is marked as maximum threat level. The first contact administrators are immediately informed about that fact, and manually take further steps. If it is possible ( implemented procedures includes such event), automated actions are taken ( like disconnecting device from company’s networks) in order to stop the spread of threat.

4.Containment and alarming

Appearance of incident or breath of third level of significance requires immediate action. First contact administrator is informed and starts the investigation. Having access to data connected with incident, he has to evaluate the seriousness and impact of problem.

After determining the sources of danger, and affected parties further actions are taken.

If alert turns out to be false (no action needed), then these information should be included in learning phase. Otherwise, the step against spreading of the issue are taken. Also, depending on initial threat analysis, the right people are put on standby.

1. If problem concerns employees, specific employee is blocked in system until case is resolved. That means, he is unable to access any of company’s data, nor communicate with other devices inside network. The worker gets notification about the issue, and should wait for further information.

2. If problem concerns unavailability of services, the administrator has to check, if are they critical to the correct work of shop. If it is possible, and there is and existing procedure for such case,

admin can restart such service in order to make it work again. If it is not the case, such affected service should be isolated from the rest of the system during the investigation. Also, IT Manager is notified about that fact immediately. The website should be changed to previously prepared one, containing information about technical break and apology.

3. If problem concerns other system related threat, admin has to investigate the seriousness of it and affected assets. If unknown (not noted before) problem occurred, and possible damages are impossible to predict, IT Manager is notified immediately, and the meeting is taking place.

4. If problem concerns users, that means a lot of similar incidents, related to users appeared.

For example, significant number of login attempts may be result of some databases leakage. Someone is trying to use leaked data for other websites (many users use same password).

In this case, first step is to change tuning of monitoring tools, in order to focus on incidents connected with attack vector. Users should be notified on possible threat via email. The email can contain (depending on situation) recommendation to change password. Customer Service Manager should be notified about this fact to prepare eventual statement to users.

Generally, any incident reported, that can not be classified as false positive and cannot be handled automatically, leads to investigation. If basic services or data stored might be in danger, IT Manager is notified immediately. If there is a suspicion, than incident is intentional action of one of the employees, the Human Resources Manager is notified.

If possible sources of problem are found, the monitoring devices are tuned to recognize similar ones and report them for at least 7 days.

Next step is to identify damage caused. If data leakage or loss is confirmed, then Media Relations Manager is notified. If there is an evidence of fake transactions, that might took place due to attack (like shopping without payment), the Vendor/Contraction Manager is notified about that fact.

If a violation of these goods is discovered at a later stage, the same persons should be informed.

5. Eradication and Recovery

In cases, when IT Manager is involved his duty is to establish actions that will allow system recovery. Provided information from first contact administrators, he has to found out the source of problem, identify the consequences and contact the Crisis Manager in order to get authorization for

actions needed. With help of his team, he performs:

1. neutralize the danger: depending on situation in may be blocking specific requests, that led to unauthorized actions
2. in case of service loss: restarts affected services, recovers system back to work

* after data loss: checking backups in order to restore data, estimates the size of data that cannot be restored
* after data leakage: estimates the size and data sensitivity

All estimations are forwarded to the Crisis Manager, who is responsible to take eventual business, legal or other actions, supported by Critical Operations Support Staff.

In case, when the attack cannot be stopped immediately (like in case of well prepared DDoS attack),

the IT Manager is in charge of stopping the system, or it’s affected part and convening a team meeting (the team is predetermined and consists of the most experienced programmers and architects in the company) in order to create fixes that will allow recovery.

After all, IT Manager creates report that will allow to avoid such incidents in the future. This may include changes in procedures, including new ones, that will allow to automate similar incidents in the future, or new security features that should be implemented in the system in order to prevent.

In cases where the IT Manager is not called, the administrator is responsible for fixing the problem.

When one of your employees' computer is at risk, removing the threat involves checking the infected machine in person. If it is not possible to get rid of the problem non-invasively (for example, the disk was encrypted by the attacker) possible data losses are determined. On this basis, a decision is taken on further action. The employee's computer may be restored to factory state, or further attempts are being made to solve the problem non-invasively.

If incident, that is being monitored starts to appear more frequently, First Contact Administration is obliged to inform the IT Manager about this fact.

6. Learning

Learning phase includes usage of information acquired during the alert. In general, nearly half of alerts are so called false positives, that do not require action, but only wastes the time of First Contact Administrators who have to check them.

After alert, that found out false, there should be applied tuning to the detection system. It may include the higher rate of similar incidents needed to trigger the alert – connected for example with growing number of users. Finding correlated assets and binding them together is one of the ways.

If alert seemed to be serious, but not in the specific environment (like SQL Injection attack on part of the system that does not have access to the database), is should be addressed more accurately, including not only the attack itself, but also the context that in which it appears.

The tuning should be done continuously.

The recommendations in reports that are created by IT Manager after recovery should be included in the system as soon as possible. The Recovery Management Team is subject responsible for applying changes, after they are confirmed by Crisis Manager.