Business Continuity Plan

FONTEYN VAKANTIEPARKEN

Md Farhan Tahmid, Marc Kock, Rowen de Vries, Nikola Hristov, Murthid Al habsi

Table of Contents

Business Impact Analysis

The Fonteyn Vakantieparken has multiple time-sensitive services that has to be functional and secure 24*7. These resources contain sensitive information about the business and its customers. Any disruption to these services will impact the uptime of the total service and also the confidentiality of information. These services and the detailed functionality of these are identified below:

1. **Database**: The on-premises server hosts a database which contains credentials of the customers and the admins. It also has information regarding events, purchased tickets, etc. The database needs to be up 24*7 for access, and it is only accessible through the website. If there is any disruption in the service of the database and it is down, then the website will lose its functionality. Therefore, the business will be un-operational taking both financial and organizational losses. Login, ticket purchase, refund functions will not work if the database is un-accessible. Moreover, any compromise in data of the database will result in security threats. User credentials including email address and hashed password will be compromised. Although the encrypted passwords will most probably be secure and meaningless to the attacker, the email address might be spoofed. Database integration in the website also needs to be secure, any SQL injection will lead to data leak.

2. **Webserver and website**: The website are also hosted in a on-premise webserver. It contains the database as well as the website. If the webserver is down, the website will be inaccessible. Therefore, it will cost the company financially. Any security threat in the webserver will also lead the data to be compromised. The RFID entry validation system will be down as well, therefore, physical access to the events will be hampered. It means any disruption to the webserver will impact the whole business. The website also must be made secure through the HTTPS protocol and made sure that packages are encrypted.

3. **Cloud Components**: The cloud service for this business is Azure Cloud by Microsoft. The azure apps will be the main components in the cloud service. The sandbox and azure cloud admin credentials should be secure with two factor authentication, limiting any third-party access. If the credentials are leaked, anyone with these credentials can login to the cloud, change settings and steal data. The service will also be disrupted.

4. **RFID Entry verification**: The RFID readers are connected to the network directly. It can access the database to verify the identity of the guests accessing park events. The RFID cards/chips contain information about the guests based on their purchase of event tickets. Therefore, if connectivity to the network is hampered, it will not be possible to verify any identity of the guests in events. Therefore, the events will be postponed, impacting the business financially.

5. **Network**: The network connection of the park is split into 4 parts. Admins, IT infrastructure, stuffs, and guests. If the network is compromised, the data and the security

devices such as cameras will not function properly. Device information such as MAC, IP will also be compromised. It will impact the whole service of the business. The domain controller is connected in the IT Infrastructure network, it contains information about the registered users, security groups etc. Any downtime will hamper the identity verification.

6. **Server headroom**: If the on-premises servers run out of resources, the servers might crash, resulting in interruption of service and uptime. If the cloud servers and apps run out of resource, it will need to be scaled up, which will incur additional costs.

Recovery

If for any reason any of these above-mentioned services are down, it needs to be recovered as soon as possible with backup measures in hand. The process to recovery of these items is discussed below:

1. **Database**: Any alteration in the database needs to be handled by the administrators. Due to cost and resource limitations, it is not possible to have a backup database. Therefore, in case of disaster, the user information will need to be verified by comparing it to the users in domain controller. The database admin is responsible to recover the database and to get it up and going in minimal possible time.

2. **Webserver and website**: In case the webserver is down or compromised, the server admin is responsible to recover it. If the resources and cost allow to have enough space for a backup, the website and database can be restored to a previous state using the backup. Currently, a backup is scheduled every week. Therefore, the website and webserver can be made up and going by restoring the backup.

3. **Cloud Components**: By default, azure offers backup for cloud resources. Therefore, if for any reason azure cloud services is down, Microsoft is responsible to fix it and it is out of control of the business park. Anyways, if a certain server in inaccessible, the cloud data are hosted in a backup server in each region, therefore the servers are up for almost 100% of time. Any change in sandbox and azure cloud configuration can be fixed by the cloud admin easily.

4. **RFID entry verification**: If the RFID system is disconnected from the network, the system can be connected directly with the server through USB and can be made functional as a backup measure. Meanwhile, the network connection can be fixed and restored to ensure regular activity again.

5. **Network**: If the network is unreachable or has any malware, all the services are to be disconnected until it is secured, to prevent further spread of the malware. In case the network has any other access problem, the network manager is responsible to fix it. In the meantime, the regular activity of the park can be handled without internet through local network connection.

6. **Server Headroom**: If the on-prem server is out of resources, the current activity of the server will be affected. In that case, some resources needs to be freed up to resume the services. In the worst case, upscale resources might be necessary, which will incur costs.

Organization and Planning

Due to cost and employee limitation, it is not possible to have a continuity team standby all the time. In case of emergency, a temporary continuity team will be created to fix the problem. It will contain the following members:

1. The Problem and Change management team
2. Server Manager
3. Network Manager
4. Scrum Master
5. Cloud Admin
6. Website admin
7. Team lead

This team will then analyze the event/disaster and propose solutions. The most effective and time-saving solution will be followed. Upon the resumption of the services, the problems will be forwarded to the Change and Problem management to fix it. The goal is to fix the problems/ recover on a temporary basis in the shortest possible time. The Change management will be responsible for the proper change to prevent further incidents.

The change and problem management team will continuously be monitoring the service to detect any unusual activity. There are additional services such as IDS/IPS at their disposal to detect unusual behavior. Therefore, any major future incident might be avoided.