LeeWayne Barrineau

November 15, 2019

Perfect Pizza Database Security

1. User are Employees, Management, Rewards Customer.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Management Permissions | | | | | |
| Table Name | Select | Insert | Update | Delete | Constraints |
| Customer | X | X | X | X |  |
| Customer Order | X | X | X | X |  |
| Employee | X | X | X | X |  |
| Order Detail | X | X | X | X |  |
| Product | X | X | X | X |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Employees Permissions | | | | | |
| Table Name | Select | Insert | Update | Delete | Constraints |
| Customer |  | X\* | Xx | Xx | \* Only when a non-rewards customer wants to become a rewards customer. Even then the employee should just see an empty box.  x Only from a management override |
| Customer Order | X | X | X | Xx | x A total deletion of a customer order should be done with a management override. |
| Employee |  |  |  |  |  |
| Order Detail | X | X | X | X |  |
| Product |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rewards Customer Permissions | | | | | |
| Table Name | Select | Insert | Update | Delete | Constraints |
| Customer | X\* | X | X\* | Xx | \*The Customer should only be able to see their own information and therefore should have the ability to update personal information on their own  x The rewards customer should be able to request the deletion of their rewards account |
| Customer Order |  |  |  |  |  |
| Employee |  |  |  |  |  |
| Order Detail |  |  |  |  |  |
| Product |  |  |  |  |  |

2. Threat analysis of user for the Perfect Pizza database

|  |  |
| --- | --- |
| Role | Management |
| **Threat** | **Description** |
| SELECT | The ability to see personal data of employees and customers |
| INSERT | Data entry or typing mistakes can make the data and reports based on the data unreliable and inaccurate. |
| UPDATE | Updating more records than intended. Changing data malicious. |
| DELETE | Accidental deletion of records |

|  |  |
| --- | --- |
| Role | Employees |
| **Threat** | **Description** |
| SELECT | The ability to see customer phone numbers |
| INSERT | Accidental or malicious customer, order, or order detail entry. Also mistakes during data entry of these tables |
| UPDATE | Accidental or malicious changes to a customer order and order details |
| DELETE | Accidental or malicious deletion of an order’s detail |

|  |  |
| --- | --- |
| Role | Rewards Customer |
| **Threat** | **Description** |
| SELECT | A rewards customer might accidental or malicious obtain access to see confidential information of other rewards customer and other users. |
| INSERT | A possible insert of a new order for another customer |
| UPDATE | False or inaccurate information when update their rewards membership information |
| DELETE | ---------------------------------------- |

3. Roles of the Perfect Pizza database user’s

|  |  |
| --- | --- |
| Role | Description |
| Pp\_management | Grants ownership and full permissions on all database objects. |
| Pp\_employee | Denies access to employee and product tables. Limits access of the customer table to only insert. Grants full permissions to the order details table. |
| Pp\_rewardscustomer | Grants user select and update permissions over select data inside the customer table. Denies insert and delete of customer table. Select, update, insert, delete is also denied on any other table |

4. Creation of user, login and role

Code: Use Master Go

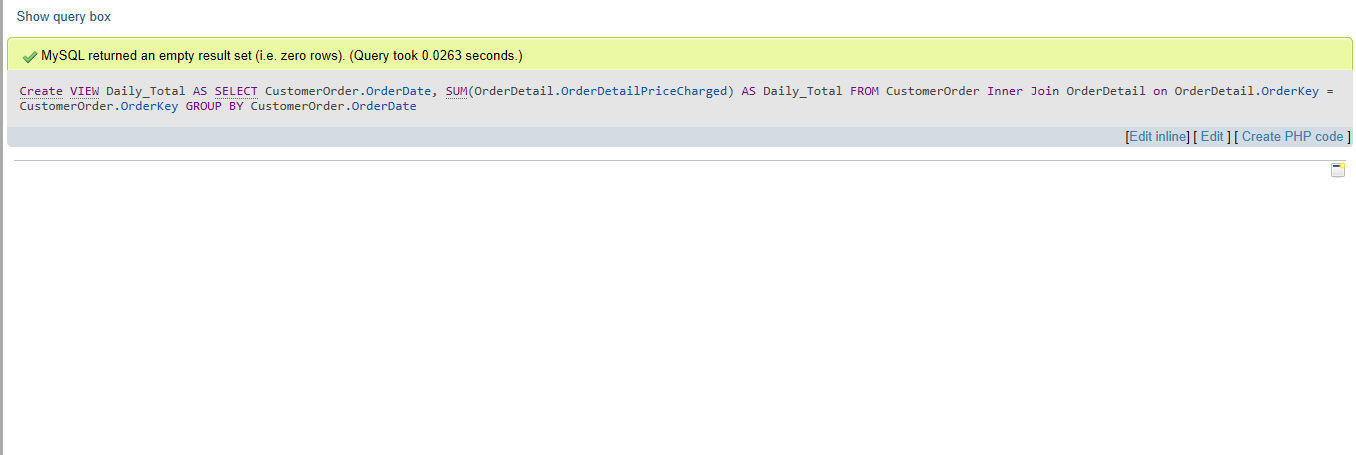
CREATE LOGIN employee WITH PASSWORD=”PizzaIsGr3at” GO;

Use lbarinea\_Perfect\_Pizza GO

CREATE ROLE Pp\_employee GO

Create

5.



Grant Select on Daily\_Total to Pp\_management

6. **Disaster Recovery Plan for Bookstore**

During day to day operation a backup that includes employee information, monthly and annual sales, customer information, web site information (files, and data) and catalog of the books will be done at 7:00 p.m. During the backup a hard drive with the oldest information from the set of 10, 1 terabytes hard drive will be used to hold the information. Once complete that hard drive will be used to upload the data to the cloud from the cloud service provider. When the backup to the cloud is made the hard drive will then be shipped to a secure location.

If a disaster warning is occurring, the reaming hard drive will be grouped up in groups of 2 or 3. A total backup will then be written to each drive apart of the groups. A set of hard drives will then be to the most trusted individuals apart of the company. When the first is done a backup from that hard drive to the cloud provider will also be done to provide ample amounts of recovery locations. If no warning were issued following the day to day normal backup operations.

When recovery occurs the hard drive from the secure location will be retrieve. When that hard drive get to the business, the hard drive that overwritten the earliest will be used to upload the data to the system. IF there are any issues with the system, the issues will be restored to normal operation. If there is any missing data recover that data by reviewing paper receipts, invoices the catalog and other necessary materials.

**Policies**

* Database server machines will have at least 1 physical drive and a cloud.
* Total information will be stored on the drive and a backup from that drive will be sent to the cloud.
* Backups will be done at 7:00 p.m.
* The backup drive will be stored off-site in a secure site.
* The drive will be stored for a 3 day be retrieving.
* The cloud will be updated once a day at 9:00 p.m.
* The hard drive will be labeled with a day and time that the backup occurred before it shipped.

**Backup Procedure**

* The company will maintain 10 hard drives and a cloud.
* A round 7:00 p.m. the drive with the oldest backup data will be retrieve.
* Once the hard drive is retrieved a total backup that includes employee information, monthly and annual sales, customer information, web site information (files, and data) and catalog of the books will be placed on the drive.
* Label the drive with current data and time.
* From that hard drive make a cloud backup based on that drive.
* Once cloud and hard drive backups are completed, mail the drive to the secure location of the business choosing’s.

**Recovery Procedure**

* If there are damages to the server machines or the computer fix the necessary problems.
* Retrieve all hard drive from the secure location.
* Restore the database with the hard that has the most recent backup date.
* Verify that the database has all necessary information to continue business.
* If there is any lost data attempt to recover the lost data by reviewing paper receipts, invoices and any other necessary materials.
* When the database is rebuilt, begin the backup procedures again

7. CourseKey NCHAR (10), StudentKey NCHAR (10), RequestKey NCHAR (10)

8. RequestKey, CourseKey, Date, Status, StudentKey

9. A new request record will be create with the RequestKey, CourseKey, Data, Status and StudentKey as values for the record.

10. The query will roll back the transaction.  
11. A try catch is need for the transaction because if an error occurs this will allow the transaction to recall the transaction. This allow the user to stop the error from causing any other issues.