

GOWER COLLEGE SWANSEA

M5X01130

Database Management Systems

WIL13807181

1/02/2019

Table of Contents

Introduction	2
Security threats and countermeasures	2
Intrusion	2
Corruption	2
Destruction	3
Integrity Controls	3
Use of views	3
Authorisation/Authentication issues	3
Access control	3
Backup and recovery of the database	4
Roles of users	4
Constraints i.e. use of triggers	4
Audit	4
Encryption	4
Conclusion	5
Referencing	6
Appendix	10

Introduction

The database provided is known as Smart IT Equipment Rentals, the purpose of the company is to rent IT hardware to a number of local schools, and it documents their activity on the equipment that is rented out over a number of years. now the bespoke system needs a redevelopment by editing the database without disturbing the data, once the is secured I am then free to pass the updated database onto the developers, whilst during this I will research into many different databases security threats. And help protect the database.

Security threats and countermeasures

unfortunately, database management system is not safe from threats like intrusion, corruption, or destruction by people (mainly employees), who have a physical access to the network, once the security has been established, from that point the database needs to be protected from unauthorized access by authorized users and unauthorized people.

Intrusion

This security threat has a specific five stages that it will go through [1], the first stage being recon where the threat will study the target before making the attack, it will study the network and its systems. The second stage being intrusion, at this point the threat has gained access to the network and will disguise itself with the networks traffic and try and detect certain information to then exploit or release tools that will inflict damage. the stage three is where the threat will then open additional channels and begin launching its Trojans or RATs [2] (backdoors), to then help gain access to the system, stage four is then where the threat will begin to remove the data decrypting the majority of the data. and finally stage five where the clean-up begins and the threat will then clean up its work, if there is no concern for the threat being detected where if the hacker who implemented the threat is up to the task, they may then begin to clean up their presence from the network leaving no trace of them being there to begin with.

Corruption

Data corruption is actually a very common system error or bug that occurs on the system and the error appears due to the loss of data or invalid or ill written code [3], in other terms data corruption is due to the human error being the most likely term and then hardware and software also being alternative sources of the corruption. sometimes corruption due to a bad program is a common issue that normally occurs due to a computer fault such as not turning the computer off properly or due to not shutting the system down correctly which can cause loss of data or damage to system, sometime data corruption can occur due to damage or incomplete spruce code of a file [3]. Data corruption may also occur due to hard drive failures or bad RAM.

A good idea for the system would to be keep regular backups of an up to date system so that you can revert back to if needed or compare to your current system to determine where the fault had occurred. Using anti-virus software is a good idea also but certain antivirus may mistake source files for viruses and erase them because failure to the system which is why it's a good idea for the backup to always be handy on an external device was said by tutorialspoint "prevention is better than corruption" [3].

Destruction

Destruction of data is done by destroying the hard disks of external devices so that they are left in readable and cannot be accessed by anyone, some companies may even do this intentionally to stop other companies gaining access to their data for unauthorised purposes [4]. Destruction means that the data will no longer be accessible by the operating system or application that the author had used to create it but that won't be enough to completely wipe it a dear destruction software will be used in order to completely destroy the data it will continuously overwrite the available space until it has left the data irretrievable [4].

Integrity Controls

Integrity Controls are used to measure the integrity of data, which is a required component of information security, it helps refer to the accuracy and consistency of data that is stored in the database. integrity controls apply rules that verify database and its operations making sure that the database has no corruptions [17]. (see appendix E for screenshot to show permissions granted).

Use of views

Views are used for security purposes because they are able to provide an encapsulation of the name of the table, a view can be used to show specific data, this could be used to demonstrate simple reports of data about the clients in the system [5].

although views are treated as nothing but logical tables which are used to gather data records from a multiple number of tables, it is a simple reporting tool which is used in Sql. but the difference between a view and a table is that the definitions of the views are built on top of tables and do not hold the data themselves, and if the data is changing in the underlying table, the same changes is reflected in the view. [6]

Authorisation/Authentication issues

Authentication is the process of verifying who you are before you log on to a computer or into a system, When you log into a work or personal computer or system you are required to use a username and password[7], usually the username will be given to you and the password would be personal and will follow constraint of a certain syntax such as (Ex4Mpl3) by doing this you are authenticating whereas authorisation which is the process of verifying that you have access to a resource such as the directory or the hard disk[7].

Access control

The authorisation and authentication issues i have decided to implement access control where I am able to grant permissions to people allowing them to select edit or insert into the database [14], by allowing users to use the function is risky but can be taken away from users if the tool permissions are used inappropriately. (see appendix A for screenshot to show permissions granted).

But upon looking into the database I discovered that the customer being able to select insert and update tables was a bit too much power for them so I revoked their permission to do so. (see appendix A for screenshot to show permissions revoked).

Backup and recovery of the database

A backup of a database is a copy of data from your database that can be used to reconstruct that data or actually as the same state's backup as in a replacement is the original is damaged and cannot be saved, ideally a backup should also be kept up to date as well as the original so that not a huge amount of data will be lost[8], a physical backup would be kept on the person as the original may be damaged by a system error so the backup will not be damaged as it's kept away from the system and then a logical backup can be an exported version of the database where the file will be stored in binary form for later re-importing into a database[9]. I have created an of network backup for the database.(see appendix F for screenshot to show audit).

Roles of users

Roles will act sort of as a template for the user in a way to help assign permissions to a database user. the roles that could be assigned follow as "read and write" or "read only" and lastly "write only" [10] and depending on the role that is granted to the user will then determine the permissions that the user is granted.

Constraints i.e. use of triggers

Constraints are rules that must be obeyed on the data columns of a table, these are used to limit types of data that can go into certain tables, this will then help to ensure the reliability of the data entered into the database, constraints are kept on either a column level or also on a table level [11]. A trigger is an automatic response that is used in a database that takes effect when an event happens in the database server. DML triggers will take effect when a user tries to manipulate using DML events such as "insert", "delete" and "update", which are the statements that are used on the table or the view [12].

Audit

Using a trigger, I was able to create a manual audit for the customer so it would be able to show, who modified a certain record and when it was done [15], which will later allow the user to query and report on. (see appendix c for screenshot to show audit).

Encryption

Database encryption is split into three different types, there's column level which is voted the best as it is the most used in people's databases, and it works by encrypting the columns that are in the database [13]. then there's tablespace encryption which is generally used as safeguarding data, tablespace allows the user to encrypt all data that the tables are referring. allowing the user to choose specific data they want to protect [13], and lastly their file-level which as the name indicated protects the whole file rather than row by row or column by column, and when read it will decrypt data into the database cache allowing the database to work as id no encryption has taken place [13]. I have now encrypted the database to help make it more secure and to protect the customer details [16], (see appendix D for screenshot to show Encryption).

Conclusion

In conclusion I feel like I have reached database protection, by following certain procedures I was able to then encrypt the database to help protect it against certain aspects and threats, a point I would like to make is that due to the protection techniques I have taken I find that I have been able to protect the database from when users were able to gain access to data they were not allowed to. I can now say I feel as though I helped develop the bespoke system by modifying the structure of the database to help it to be more secure.

Referencing

Article title: The five stages of a cyber intrusion -- Defense Systems

Website title: Defense Systems

URL: <https://defensesystems.com/articles/2015/10/21/navy-the-five-stages-of-a-cyber-intrusion.aspx> [1]

Article title: Backdoor, Remote Access Tool/Remote Access Trojan (RAT) | ESET Virusradar

Website title: Virusradar.com

URL: <https://www.virusradar.com/en/glossary/backdoor> [2]

Article title: How to Prevent Data Corruption

Website title: www.tutorialspoint.com

URL: <http://www.tutorialspoint.com/articles/how-to-prevent-data-corruption> [3]

Article title: What is data destruction? - Definition from WhatIs.com

Website title: SearchStorage

URL: <https://searchstorage.techtarget.com/definition/data-destruction> [4]

Author Poonamchand Soni

Article title: Creating and Usage of View in SQL

Website title: Codeproject.com

URL: <https://www.codeproject.com/Tips/639239/Creating-and-Usage-of-View-in-SQ> [5]

Author Difference sql

Article title: Difference between View and table in sql

Website title: Stack Overflow

URL: <https://stackoverflow.com/questions/6015175/difference-between-view-and-table-in-sql> [6]

Author What authorization?

Article title: What is the difference between authentication and authorization?

Website title: Server Fault

URL: <https://serverfault.com/questions/57077/what-is-the-difference-between-authentication-and-authorization> [7]

Article title: Backup and Recovery Overview

Website title: Docs.oracle.com

URL: https://docs.oracle.com/cd/B19306_01/backup.102/b14192/intro001.htm [8]

Article title: Back Up and Restore of SQL Server Databases - SQL Server

Website title: Docs.microsoft.com

URL: <https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/back-up-and-restore-of-sql-server-databases?view=sql-server-2017> [9]

Article title: Database User Roles and Permissions

Website title: Docs.plesk.com

URL: <https://docs.plesk.com/en-US/onyx/administrator-guide/database-servers/database-user-roles-and-permissions.74697/> [10]

Article title: SQL Constraints

Website title: www.tutorialspoint.com

URL: <https://www.tutorialspoint.com/sql/sql-constraints.htm> [11]

Author Md. Marufuzzaman

Article title: Overview of SQL Server database Triggers

Website title: Codeproject.com

URL: <https://www.codeproject.com/Articles/38808/Overview-of-SQL-Server-database-Triggers> [12]

Author Ashvin Kamaraju

Article title: Database encryption demystified: Four common misconceptions | ZDNet

Website title: ZDNet

URL: <https://www.zdnet.com/article/database-encryption-demystified-four-common-misconceptions/> [13]

Article title: What You Need to Do to Secure SQL Databases

Website title: Lifewire

URL: <https://www.lifewire.com/access-controls-in-sql-1019700> [14]

Author: Nesha Maric

Article title: Various techniques to audit SQL Server databases

Website title: SQL Shack - articles about database auditing, server performance, data recovery, and more

URL: <https://www.sqlshack.com/various-techniques-to-audit-sql-server-databases/> [15]

Article title: Transparent Data Encryption for the BIS workspace in SQL Server—ArcGIS Help | ArcGIS Desktop

Website title: Desktop.arcgis.com

URL: <https://desktop.arcgis.com/en/arcmap/10.5/extensions/maritime-bathymetry-guide/sql-server/transparent-data-encryption-tde-for-the-bis-workspace-in-sql-server.htm> [16]

Article title: Integrity Controls

Website title: WhiteHat Security Glossary

URL: <https://www.whitehatsec.com/glossary/content/integrity-controls> [17]

Appendix

[a]

```
/****** Permission *****/  
GRANT SELECT, INSERT, UPDATE  
ON suppliers  
TO DataEntry  
  
GRANT SELECT, INSERT, UPDATE  
ON customer  
TO DataEntry
```

[b]

```
REVOKE SELECT, INSERT, UPDATE  
ON customers  
FROM customer
```

[c]

```
CREATE TRIGGER customer  
ON customer  
AFTER INSERT  
AS  
    INSERT INTO dbo.customer (  
        TABLE_NAME,  
        TABLE_DML,  
        AUDIT_ACTION_ID,  
        MODYFIED_BY,  
        MODYFIED_DATE,  
        [CUSTOMER]  
    )  
    VALUES (  
        values(  
            'Person',  
            'Person',  
            'Insert',  
            SUSER_SNAME(),  
            GETDATE(),  
            1  
        )  
    )  
GO
```

```

/* Create master key */
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'R3NT4L@admin';
GO
/* Backup master key */
OPEN MASTER KEY DECRYPTION BY PASSWORD = 'R3NT4L@admin';
GO
BACKUP MASTER KEY TO FILE = 'E:\EquipmentRental V2 - Create EquipmentRental DB first.zip'
    ENCRYPTION BY PASSWORD = 'R3NT4L@admin';
GO

/* Create Certificate */
CREATE CERTIFICATE bis_cert WITH SUBJECT = 'BIS Server Certificate';
GO

/* Verify Certificate */
SELECT * FROM sys.certificates where [name] = 'bis_cert'
GO

/* Backup certificate */
BACKUP CERTIFICATE bis_cert TO FILE = 'E:\EquipmentRental V2 - Create EquipmentRental DB first.zip'
    WITH PRIVATE KEY (
        FILE = 'E:\EquipmentRental V2 - Create EquipmentRental DB first.zip',
        ENCRYPTION BY PASSWORD = 'R3NT4L@admin');
GO

--use bis database
USE bisdb
GO
/* Create Encryption key */
CREATE DATABASE ENCRYPTION KEY
    WITH ALGORITHM = AES_256
    ENCRYPTION BY SERVER CERTIFICATE bis_cert;
GO

/* Encrypt database */
ALTER DATABASE customer SET ENCRYPTION ON;
GO

/* Verify Encryption */
SELECT
    DB_NAME(database_id) AS DatabaseName
    ,Encryption_State AS EncryptionState
    ,key_algorithm AS Algorithm
    ,key_length AS KeyLength
FROM sys.dm_database_encryption_keys
GO
SELECT
    NAME AS DatabaseName
    ,IS_ENCRYPTED AS IsEncrypted
FROM sys.databases where name = 'customer'
GO

```

[d]

[E]

```

DBCC CHECKDB
    [ (CUSTOMER | CUSTOMER_ID | 0
        [ , NOINDEX
        | , { REPAIR_ALLOW_DATA_LOSS | REPAIR_FAST | REPAIR_REBUILD } ]
    ) ]
    [ WITH
        {
            [ ALL_ERRORMSG ]
            [ , EXTENDED_LOGICAL_CHECKS ]
            [ , NO_INFOMSGS ]
            [ , TABLOCK ]
            [ , ESTIMATEONLY ]
            [ , { PHYSICAL_ONLY | DATA_PURITY } ]
            [ , MAXDOP = number_of_processors ]
        }
    ]
]

```

[f]