Database Security

ICTN 4040- Term Paper

Rodney Compton

As technology has advanced within the past century, there has been an increase emphasis not only on device development, but the storage of information from these devices. In today's world, technology relies heavily upon databases. Further, how we keep those databases secure, themselves, is critical. Databases encounter many security obstacles to stay protected. Thus, businesses must take the necessary precautions to make ensure that their databases are secure from any type of threat. As you read along you will learn much about the process in securing a database and all the elements or encounters you can and will face. The process in securing a database is complex; however, the potential harm from not properly securing a database is far greater.

In general, Database Security refers to the processes used to protect and secure a database from malicious threats and/or attacks. To aid in this process, many programs have been developed. These programs include, but are not limited to MySQL, Oracle, and Microsoft SQL Server. These three programs offer a variety of utilizations for database security. MySQL, for example, is by far the most used program. This is due to its open source ability, the greatest aspect of this program. Open source ability allows the user to both download and modify the software. The malleability of this program allows for more individualized database protection. In another instance, Oracle database is known as the first database to be designed for enterprise grid computing. Comparatively, Oracle is not open source. However, among other purchasable programs, it is considered the most flexible and cost effective way to manage information and applications (Oracle Enterprise Performance Management System Supporting Documentation Backup and Recovery Guide, 2017). Microsoft SQL Server works as a two-part system known as a relational database management system (RDMS). First the data is stored in the server as a

relational database; whereas, the entire server is your management system (MySQL 5.7 Reference Manual, 2017).

A common misconception pertains to the extent of a database. In many circumstances, the public relates databases to a large company. However, a database is far greater than that. Databases can range from simple to complex. For instance, databases may include a simple shopping list or a picture gallery or even the vast amounts of information in a corporate network (MySQL 5.7 Reference Manual, 2017). And so, all individuals interacting with technology are essentially interacting with some form of a database. In the case of individual users, their interaction is certainly present in today's times. Unlike the complex databases of large companies, individual users are not tasked with securing databases (Bertino, 2005). The vast majority of web developers and industry leaders such as Amazon, Yahoo, and Google have the most to worry about within database security. Being an industry leader brings excessive amounts of attention towards the company. Unfortunately, not all of that attention is safe. Hackers today are well advanced in knowing the loopholes and the tactics to intrude a company's database. Amazon leads with the world's largest retail store and maintains over 59 million active customers (Bertino, 2005). Their databases are comprised of personal data such as name, phone number, addresses, and payment information. Maintaining the security of this information is not only critical for the consumer, but the company itself (Schlichting, 2008).

As the threat to maintain database security has increased, so have the procedures to effectively secure a database. There are a multitude of procedures every company goes through to ensure their database is as secure as possible. The first layer of database security is physical. The database for a company is stored on a server. These servers can be located in a dedicated place around the world or in most cases, companies have their own data centers where all servers

are stored. The process of physical security is very important and needs to be addressed very often. In addition to the physical location of servers, physical security includes determining access to these servers. Specific personnel need to be identified as authorized individuals with access to the server rooms. Many companies choose to lock and secure their server rooms with a key and lock system. Though some companies are adopting finger print scanners at the doors to gain access to the room. In addition to identified the proper personnel, there needs to be a procedure to ensure the identity of these authorized individuals. A good recommendation for added security, would be to implement security cameras into the server rooms. Should an incident occur, the security cameras would serve to properly document any altercation that took place.

The second layer of database security is software. Firewalls are labeled the best software protection to determining the information traffic encountered on a server. The firewall filters all the connections that are needed to gain access to the database server such as specific application or web servers that need access to the database information (Bamrara, 2015). The firewall will block and ignore all other traffic that is not approved. Along with Firewalls, Encryption is a part of the second layer of database security. Encrypting database information is crucial, in the regards, to keeping a database secure. When encrypting data, the information is being converting into a code that can prevent unwanted access from users (Schlichting, 2008). In a similar fashion, encrypting all recovery or backup data is important. Maintaining the decryption keys separate from the encrypted data is also vital.

With these two layers in place, any database could confidently be described as secure. Regardless, there are additional procedures that need to be completed. All database activity needs to be monitored on a regular basis. This mainly refers to a user's account. Individual users

need to be conscientious of invalid logins and also the location in which the accounts are being logged in from. Checking location of account logins can be a good assumption of a shared or hacked account.

Threats are the biggest concern when it comes to database security and they come in many forms. One form includes excessive and unused privileges. Authorized personnel need to have the appropriate amount of access to a database. Allowing too much access to the wrong individual can be dangerous. A basic user who has more rights than their position holds is one way the database can be compromised and breached (Bamrara, 2015). Also, employees with advanced privileges can use the information they see and abuse it by giving it to other people or other competitors. Unlike the previously described threat, Malware presents a completely different threat to a database's security. Malware can be a persistent occurrence. A common source of this threat includes individual devices that are allowed access to a company's network. Further, these individual devices are prone to phishing schemes. Once a computer is infected from a phishing email, the Malware then replicates itself. From here, the Malware begins sending to other users on the emails contact list to find more suppliers. Similarly, other tasks can render a database vulnerable to threats. During an audit, proper tracking of all information from the database is crucial. Databases may contain transaction history or any other sensitive information. Failing to properly track during an audit can lead to a very high risk database breach. Of all the threats mentioned, the most common attack on a database is Denial of Service (DDOS). Essentially, when a server becomes flooded by a well-crafted number of query's, the server resources are utilized to quickly. The result of this includes limited user access and potential downtime usage of database information (Bamrara, 2015).

Despite all efforts put forth, security breaches are a common occurrence. One particular incidence pertained to a breach in Verizon's Database Servers. Such a breach caused an uproar for not only Verizon, but Google as well. Google has many procedures in place to ensure the security of user accounts. One of these ways is through two-factor authentication. Two-factor authentication entails linking an activate phone line to the users account. This was a great implementation for google to have to secure their users accounts. Of Googles popular platforms, YouTube is a place where millions of information traffic occurs every day. As a result, YouTube content creators can make a substantial amount of money. That is to say, some creators have chosen YouTube as their career and make millions annually. Unfortunately, this type of lifestyle makes them great targets from hackers. In the summer of 2016, Verizon experienced a database security breach. This breach caused many YouTubers to lose access to all their accounts including their Gmail email address accounts. By losing access to these accounts, any associated accounts were then hacked. Commonly associated accounts included bank accounts and PayPal accounts. As hackers gained access to these accounts, money and valuable information was stolen. In this case, the Verizon database was breached from a procedure called social engineering. Social Engineering occurs where an individual manipulates other people to give up confidential information. Anonymous users would call into Verizon support claiming to be sales agents setting up a new phone for their client; which in fact, they were not. They then proceeded to claim they needed to have their sim card resent to this customer. As a result, these anonymous callers would gain access to top end YouTubers sim cards and have access to all their information such as text messages, email and web search history. By gaining access from the sim card, the hackers would not be able to use two-factor authentication to gain access to their Gmail or YouTube account and therefore gaining all access to personal information.

Backup and Recovery is a key process to ensure all data is secure. Backing up database information is a process that needs to be completed on a regular basis. Because modern day servers are still running on mechanical hard drives, they can go bad at any time. Thus, any data could and can be lost without a backup. When backing up data, any company needs to ensure they have a proper procedure (Database Concepts, 2005).

To start, different data needs to be prioritized as a necessity for being backed up. Next, the company needs to determine what method of backing up is to be used. There are three major types of backup procedures: Logical Backups, Physical offline backup, and Physical Online Backup. Logical backups apply to the Oracle database sequence where the data is backed up, but not physical files, from one location to another (Oracle Enterprise Performance Management System Supporting Documentation Backup and Recovery Guide, 2017).

Physical offline backup or Cold Backup is a backup where the database is offline and is not accessible to update. This backup is the fastest way to backup data because there is no copying any data that would have been in the process of updating during an online backup (Database Concepts, 2005). Physical online backups, also known as Hot backups, are the process when the data is backed up while the database is online. When doing physical online backups, there is a risk of not copying data in the process of updating(Database Concepts, 2005). This should be taken into account when selecting a backup procedure. Not to mention, Also, when completing online backups, there is also an option of using automatic backups. This tool is provided by the servers OEM. Once a backup is complete, maintenance should be schedule for specific times and days. During maintenance, backups are tested to verify they are working as intended (Database Concepts, 2005).

In conclusion, the end goal is to keep a database server secure. Protection for these database servers start at the physical level. Having a secured server room where only authorized individuals may access the room is key. In addition, all software such as firewalls should be running at all times. With this being said, all user accounts should have confirmed authorization for the correct permissions and can only access the data they are approved to see. Monitor the database for any out of the ordinary sequences and complete audits when necessary. Keep the server and backups encrypted and ensure that the decryption key is keep separated from its source. Lastly, make sure that all backup and recovery procedure are well suited if anything is to go extremely wrong. In the end there is no solution to database security, but running good practices in order to maintain a clean and safe environment is key to staying ahead. Attacks are happening every day and as long as we are staying up to date with security issues, we should have a better chance to combat any database breach that comes our way.

Works Cited

A, Bamrara. "Evaluating Database Security and Cyber Attacks: A Relational Approach." The Journal of Internet Banking and Commerce 20.2 (2015): n. pag. Web.

Bertino, E., and R. Sandhu. "Database security - concepts, approaches, and challenges." IEEE Transactions on Dependable and Secure Computing 2.1 (2005): 2-19. Web.

Database Concepts." Introduction to the Oracle Database. N.p., 10 Oct. 2005. Web. 10 Apr. 2017.

MySQL 5.7 Reference Manual :: 1.3.1 What is MySQL?" MySQL. N.p., n.d. Web. 10 Apr. 2017.

Oracle Enterprise Performance Management System Supporting Documentation Backup and Recovery Guide." Moved. N.p., n.d. Web. 10 Apr. 2017

Schlichting, Don. "What is SQL Server." Database Journal. N.p., 05 Sept. 2008. Web. 10 Apr. 2017