ICTN 4040

Section 001

Enterprise Information Security

Enterprise Database Security Issues and Solutions

Roger Brenton Huff

East Carolina University

Abstract

This paper will review some of the key security issues that databases succumb to as well as some solutions and preventions to these problems. Specifically, it will focus on several key issues such as platform vulnerabilities, which can cause issues with software updates and could cause an attack on the database by gaining access and corrupting the databases data. It will also focus on SQL injections and how an attacker may gain access by inserting a line of code into a database channel, which can allow them to gain access to the database and its information. Other areas of focus will be Denial of Service attacks and Data exposure through backups. Although these security breaches can occur and are the most used to attack databases, there are ways to prevent these attacks from happening or mitigate the attack. This paper will bring forward ways that all these issues can be prevented and help keep the databases security and credentials as strong as they can be.

Introduction

Today, most enterprises and corporations have many different employees, clients, subscribers, documents, descriptions, objects, and many other important resources that they need to keep track of as well as keep their information safe. When corporations or businesses need to keep their compiled data together and in a secured area for access they turn to database systems to store their company's important information. These databases can contain salaries, names, addresses, confidential information and much more information that is highly valuable. With these increase of credentials and high leveled information and data, there comes a great threat to the company as well, because there are always individuals who want access the credentials and important

data of a company so that they may gain the company's secrets, information or even steal from the company. Although the threats on database systems are increasing and there are multiple ways to infiltrate the system, there are also many lines of defense that corporations may partake in that will hinder these hackers from stealing or accessing information from the company.

Database Systems

Database systems are just a collection of relative data within a company and are widely used by many companies, schools, businesses, etc. They are structured to lists and inventories of names, addresses, salaries, position titles and almost anything else that can be listed into a relative group for storing purposes. The most widely used language for constructing databases is known as SQL which stands for Structured Query Language, which is an international standardized language within databases. For example, if there is a company that requires you to create a user account to access their website and use their resources, when the user creates the account with the required information (username, password, email, address, name, etc.), that information is stored within a database on a company server, which can be referenced and accessed to for later purposes. Most companies will use a Database Management System (DBMS) to help manage their data within the databases. The DBMS is a software application that is used to do manipulative actions to the data such as controlling, moving, retrieving, maintenance and definitions of the data. These applications make it much easier for end users to sufficiently manage databases while still ensuring the data's independence and accuracy. Another positive feature of DBMS is that they increase the security of the databases and help recover data from crashes.

Security Issues and Threats

Since databases are used widely to conceal and harbor confidential, important and even personal information, they are at a great risk to threats and people that wish to get a hold of the information that they hold. Security issues can occur not only outside of the company but even within the organization's staff itself. Threats that can attack a company's database are not just limited to hacking or just one type of threat, there are actually many ways to access and compromise a database, but for the sake of time, we will focus on the most popular. The most popular threat to a database is actually going to occur within the company, because the number one cause to security threats is giving employees too many privileges over a system that they don't use or people abusing their privileges once gaining access to the database system. When privilege control is not maintained or well managed, individuals can end up with too many privileges that are not required for their job and will allow them to alter or change data, sometimes undetected, for a personal gain. Mostly, if an individual who has many privileges leaves from an organization, most of time their credentials and rights do not change, so they are still able to access and, if willing, alter the company's data. This creates an unnecessary risk for the company and can easily be avoided.

Another popular threat that occurs often and typically outside of the company itself is known as SQL injection. SQL injection is a very popular attack technique that allows an attacker to gain access to a company's database information and use it for their advantage. This method takes advantage of poorly secured web applications and stored procedures by connecting to a database through an unsecured data channel. To complete this task and gain access to the database, the attacker inputs a malicious SQL

command into an input field for a web application. If the command finds an “injection hole” and passes through to the database, the attacker then has the ability to explore, copy and even alter the database and the information that is displayed to them. This presents a threat to the company and their clients, users and employees because now confidential information has been exposed and taken, which can now be used to corrupt or steal from the company. This issue, because it is so widely changing and hard to pinpoint every possible SQL command attack that will take place, can still be somewhat inhibited or prevented. SQL injections are mostly searching for a security vulnerability within the application or program so that they may access this point and gain information within the application’s database so that they may use it for their own benefit whether it be publicity, money, etc. SQL is not an easily recognized or detected attack, some go unrecognized for some time, which can make it hard to prevent attackers from gaining access to the database information and stealing credentials, passwords and other confidential information of use.

The next most popular and rising attack on databases that have been present within the last few years is malware attacks. Lately, malware has played an extensive role in gaining access to databases and stealing confidential information from the database servers and returning it back to the attacker who set the malware in place. How these installed malwares work is they are run onto the system, in which the programs begin to search for database locations on the machine by accessing and reading the registry keys or even just analyzing packets on the network. Once the program has discovered a database or databases, it uses an embedded or Linked SQL library, in which it uses to send commands to the database in order to gain access and

even gain high privileges or root to the databases information itself. Once the malware program has gained access to the databases, it now has the ability to mine, copy or even destroy the information. While mining for the data the program begins to send what it receives back to the attacker who implemented the malware. The data is simply sent back by a few ways, one of which is through HTTP, email or FTP servers. However, another more interactive process is the program can grant the attacker an interactive connection to the database itself, where they can run malicious commands to retrieve the data on the database. Once the program has finished its process it may implement a self-destruct sequence in which it erases the any files relating to it, making it undetectable that it was ever on the machine, unless database administrators who are monitoring the servers see the malicious activities. As seen, Malware has become an increasing threat to daily enterprise operations and can cause a lot of damage to its systems, especially stored database information. Network and database administrators should continuously research and find ways in which they can prevent malware from gaining access and the ability to steal information from their systems.

Preventative measures against database attacks

Although attacks on enterprise networks and their information is inevitable does not mean there is no way for a company to protect its most valuable data and assets. With every attack and issue there is against technology, there is a solution that, if not can completely eliminate the issue, can help prevent or diminish it. In this section, we will focus on ways in which an enterprise can help defend against the attacks we discussed earlier and prevent their information from being stolen or compromised.

The first issue which should be discussed on how to prevent is the issue of privilege abuse. Imperva, a data center security solutions company, states that there are a few practices a database administrator can partake in to help protect their company from inside attacks or privilege abuse. The most widely used and effective approach is using a process known as Query-Level Access Control. Query-level access control allows a database administrator to enter rules to restrict users from using specific SQL operations when accessing a database on the network. This mechanism also logs the user's operations and sends an alert to the administrator when the user attempts to use an operation they were not granted and also block the command from running. A query-level access control program is highly effective in detecting privilege abuse within the company as well as preventing the issue from getting worse or taking place. Query-level access control lists are also used in many other forms of prevention against other attacks on databases as well. As shown, privilege abuse is not a difficult attack that can be prevented; unfortunately it is the top threat to database security because many companies don't monitor their employees' privileges as closely as they should, but with the implementation of query-level access control list and monitoring their employees' privileges and policies, privilege abuse can be easily avoided.

The second issue that has been a horrendous headache and continuous problem for network administrators is the SQL injection. Although it is a much harder process to detain because it occurs outside of the company walls, it is still possible to prevent these malicious codes from entering and depleting your valuable information. There are three specific approaches that when combined can effectively help in the prevention of SQL injections. The first is the Intrusion Prevention System (IPS), which is used to

identify the weaknesses in the stored procedures used to create the databases. Alas, SQL strings are typically prone to a false positive, which means the alert system is sometimes overwhelmed with “possible” SQL injections. This makes IPS an unreliable solution by itself. However, if IPS is implemented with the corresponding protection of query-level access and correlated attack validation, then it is a higher possibility of the database being protected from the treacherous hands that of SQL injections. Query-level access is used to create profiles with preexisting commands that they run in the database and if a query is run that is unrecognized and not linked to the user, then it is identified and logged. The correlated attack validation is used to correlate multiple and consistent violations that are used to query a database, which is then identified as an attack in real time and with extreme accuracy. Although SQL injections are everlasting issue in the database security and seems to be difficult to prevent, with these three techniques, it is possible for an enterprise to establish a strong and accurate defense against the malicious content that is constantly finding its way in and apprehending confidential and valuable data.

The final most widely talked about and uprising threat that has been making waves in database security is malware attacks which needs to be heavily assessed and a solution is needed. According to an Imperva source, there are a few general practices that can be used to help prevent malware from gaining access into the databases, which usually starts with the end users. It is suggested that vulnerability assessment tools should be implemented to recognize any vulnerabilities in the database that may be accessed and any malware-infected hosts that are on the network so they can be disconnected or blocked from gaining access to any of the confidential information on

the databases. Other ways to effectively prevent malware programs from gaining access to your systems are the general practices that are used to prevent malwares. The practice that should be implemented against malware attacks are running an up to date security software and a firewall, which will recognize unwanted and malicious software and prevent them from being installed or run of the users systems. Although vulnerabilities and threats are hard to detect and can be detrimental to a company's systems and databases, there are many practices and techniques that can be implemented to protect the enterprises most valuable data from being compromised.

Hardware Database Protective Devices (DB Networks ADF-4200)

Now, the suggested practices above are proven to be effective tools in the defense against database vulnerabilities and attacks, however many professionals suggest that there be another line of defense that should be focused on and implemented for a bit more protection to an enterprises' databases, I mean you can never have enough security, right? There are many advanced hardware platforms in informational security industry that can help prevent attacks and failures. The main focus of this section will be discussing how the implementation of an adaptive firewall known as ADF-4200 can help an industry in protecting their databases information.

DB networks are an information security company who specializes in database security solutions and firewall devices. They have developed a physical firewall that can be implemented on to a company's network and help prevent their information from being compromised or stolen. This firewall is known as ADF-4200, which was built off the Adaptive Database Firewall platform, using its technology to track, learn and adapt to each applications behavior and SQL query behavior on its network and is analyzed

heavily. If an unrecognized SQL statement is attempting to find its way into a database, it is quickly identified, blocked and an alarm is sent to warn the administrator about the issue. This can be very beneficial because it has the ability to identify threats and unauthorized SQL traffic in real time. The ADF-4200 is able to support both Oracle and Microsoft SQL server products, which allows it to be almost universally used within companies. This firewall can also be easily deployed onto a company's network without altering or changing any existing applications or databases, which allows it to be flexible with its implementation and learning abilities of the networks behavior. The ADF-4200 would be a valuable implementation to an enterprises' network to help efficiently defend against many different attacks that attempt to gain access and steal their information.

Conclusion

As stated before, database threats and security are an ongoing issue for enterprises and companies. There are many attacks that have the ability to strike mayhem onto a company's network and compromise their most valuable data. These attacks can vary from within the company walls to someone who is across the world. In this report, we only touched base on a few of the many attacks that are used against databases to steal confidential and valuable data, which can compromise the integrity of the company itself. Although there are so many attacks which can inflict severe damage to a company, there are also many practices, software tools and devices that can be used to help prevent these attacks and effectively protect a company from attacks and losing their valuable information. If these practices are followed precisely and consistently, it is possible for a company to go without any major damage to their reputation or data storage systems.

Work Cited

***Cerrudo, C. (n.d.). *Data0: Next generation malware for stealing databases*. Retrieved from http://www.argeniss.com/research/Data0.pdf**

Alechina, N. (n.d.). *Introduction to database systems*. Retrieved from http://www.cs.nott.ac.uk/~nza/G51DBS09/dbs1-slides.pdf

***Ogbolumani, D. (2008). *Security and control issues within relational databases*. Retrieved from http://www.cpd.iit.edu/netsecure08/DAVID_OGBOLUMANI.pdf**

***Shulman, A. (2006). *Top ten database security threats*. Retrieved from http://www.schell.com/Top_Ten_Database_Threats.pdf**

****Top ten database security threats the most significant risks and how to mitigate them*. (2013). Retrieved from http://www.imperva.com/docs/WP_TopTen_Database_Threats.pdf**

****Hacker Intelligence initiative, Monthly Trend Report #18.* (2013). Retrieved from http://www.imperva.com/docs/HII_Assessing_the_Threat_Landscape_of_DBaaS.pdf**

***Help prevent malware infection on your pc*. (2014). Retrieved from https://www.microsoft.com/security/portal/mmpc/shared/prevention.aspx**

***How to protect yourself from malware*. (2013). Retrieved from http://safeandsavvy.f-secure.com/2011/01/20/how-to-protect-from-malware/**

***Db networks introduces first adaptive database firewall into general availability*. (2013, February 21). Retrieved from http://www.prweb.com/releases/2013/2/prweb10449244.htm**