Databases are important in today's digital age society. Everything uses databases to store information, from video games, to banks, and even the government. Therefore, it is important to protect them from attackers (hackers)who seek to gain through stolen data from multiple sources to increase their profit. As well as understand what risks and prevention is available.

Since databases have become exceedingly important to the infrastructure of the information technology driven society of today, it is important to understand what they are and what their function is. A database is a collection of information that is organized so that it can be easily accessed, as well as easily managed and updated (Rouse, 2017). The data is stored in organized rows, columns, and tables that are indexed to ensure that relevant information is easier to locate. The data can be updated, expanded and removed as new information become available and is added. Databases process workloads to create and update themselves through querying the data they contain and running applications against it (Rouse, 2017). Databases are common in large mainframe systems, however, they are also present in smaller distributions, such as workstations and midrange systems, like that of IBM’s AS/400 and personal computers (Rouse, 2017). Sales transactions, product catalogs and inventories, and customer profiles are examples of aggregations of files that computer databases typically contain. The database manager usually provides users with the ability to control read/write access, specify report generation and analyze usage. Some databases are equipped with ACID compliance, which stands for atomicity, consistency, isolation, and durability. These guarantee that data is consistent and that transactions are complete.

Databases have continued to evolve since their beginnings in the 1960’s. Thus, over time many different types of databases with different features have been developed. Databases have evolved from hierarchical and network databases to object-oriented, and now to today with SQL and NoSQL databases and cloud databases(Rouse, 2017). Database types are categorized by content type or organizational approach. E.F. Codd at IBM invented the relational database in 1970. It is a tabular database in which data is defined so that it can be reorganized and accessed in many differing ways(Rouse, 2017). They are made up of a set of tables with data that fits into a predefined category, while each table has a least one data category in a column, and each row has a certain data instance for the categories which are defined in the columns (Rouse, 2017). The SQL (Structured Query Language) is the application program interface for relational databases. Thus, they can be easily extended without having to modify all the existing applications (Rouse, 2017). Object-oriented databases can also be used to house items created using object-oriented programming languages (they are typically stored in relational databases). These databases are organized around objects and data rather than actions and logic.

Another type of database is a distributed database, in which portions of the database are stored in multiple physical locations as well as dispersing or replicating the processing among different points in a network (Rouse, 2017). They can also be homogeneous or heterogeneous. The physical locations in a homogeneous system will have the same underlying hardware and the same operating systems and database applications (Rouse, 2017). While in heterogeneous systems the hardware and operating systems may be different at each location.

Cloud databases are databases that have been optimized or built or a virtualized environment. They can be a part of a hybrid, public, or private cloud. Cloud databases provide benefits that other databases do not. They can allow the user to be able to pay for storage and bandwidth on a peruse basis along with also providing scalability on demand (Rouse, 2017). They also provide businesses with the opportunity to support their applications in a software-as-a-service deployment (Rouse, 2017).

When dealing with large sets of distributed data NoSQL databases are useful. NoSQL databases are effective for big data performance issues and perform increasingly well when analyzing large chunks of unstructured data (Rouse, 2017). As well as data that is stored across multiple virtual servers in the cloud. Graph databases are a type of NoSQL database that uses graph theory to store, map, and query relationships (Rouse, 2017). They are essentially collections of nodes and edges, in which each node represents an entity, and each edge represents a connection between nodes. They are growing in popularity or determining and analyzing interconnections, like data mining about customers form social media for example (Rouse, 2017).

Accessing database also provides differences in each type of database. A database management system (DBMS) is a what allows the user to define, manipulate, retrieve, and manage data stored within a database. The relational database management system (RDBMS) is the most popular way to manage a database. Microsoft SQL Server, Oracle Database, IBM DB2 and MySQL are the top RDBMS products available for enterprise users(Rouse, 2017).

Seeing as databases store and organize much information for many enterprises, they are to in a way be considered the “crown jewels” of an organization. Thus, they are subject to a wide variety of attacks. Some of the most commonly used attacks include excessive privileges, privilege abuse, unauthorized privilege elevation, platform vulnerabilities, SQL injection, denial of service, database protocol vulnerabilities, weak authentication, and exposure of backup data. Every organization should be aware of these and know hold to combat them.

Excessive privileges occur when someone is given database privileges that exceed the requirements of their job function and they use those privileges to exploit and access potentially confidential information. A solution is to control query-level access, which restricts privileges to minimum-required operations and data (Schulman, 2007). Privilege abuse is also a cause for concern. This is when a user who has legitimate data access privileges uses it for unauthorized purposes. Through the enforcement of policies that apply to what data is accessible and how the data is accessed, users that are abusing their power can be identified. Attackers could also use vulnerabilities in database management software to elevate and distort privileges (Schulman, 2007). For example, an attacker might take advantage of a database buffer to overflow vulnerability to gain administrative privileges. These exploits can be defeated with both query-level access control and intrusion prevention systems (Schulman, 2007).

Intrusion prevention systems are also a good way to combat against platform vulnerabilities. Platform vulnerabilities are vulnerabilities in underlying operating systems that could lead to unauthorized data access and corruption. The Blaster worm that took advantage of a Windows 2000 vulnerability to take down targeted servers is an example of such attack (Schulman, 2007). SQL injection attacks are arguably one of the most commonly used attacks. SQL injection attacks involves a user who takes advantage of weaknesses in front-end web application and stored procedure to send unauthorized database queries, usually with elevated privileges (Schulman, 2007). Attackers even have the potential to gain access to entire database, unrestricted through using SQL injection (Schulman, 2007). Query-level access control detects unauthorized queries injected through the web applications and/or stored procedures. Denial of service is also invoked through many techniques. Buffer overflow, data corruption, network flooding, and resource consumption are all common ways to pull of these attacks (Schulman, 2007). Prevention occurs on many levels with IPS and connection rate controls to prevent individual users from consuming database server resources.

Lastly database protocol vulnerabilities, weak authentication, and exposure of backup data are all also on the list of dangers to databases. Vulnerabilities in protocols may allow unauthorized data access, corruption, or availability. Like the SQL Slammer worm that took advantage of a Microsoft SQL server protocol vulnerability to execute attack code on target database servers (Schulman, 2007). SQL communications should be parsed and validated to ensure that they are not malformed and prevent against protocol vulnerabilities. Weak authentication schemes also are threats to database security. These schemes allow attackers to assume the identity of a real database user (Schulman, 2007). Typically, these attacks are brute force or social engineering attacks. Using passwords or two-factor authentication is a must, however, authentication mechanisms should be integrated with enterprise directory/user management infrastructures to prevent such attacks from being successful (Schulman, 2007). In more recent high-profile attacks theft of database backup tapes and hard disks have occurred. All backups should always be encrypted which will combat the issue of exposure of an organization's backup data (Schulman, 2007). All threats to databases need to be considered and dealt with to bring the attack vectors to near zero, especially in our digital age of society.

Due to all of the data and activities today that use databases in some way they are considered to be very valuable to attackers. Cyberspace is the Wild West of the 21st century. Governments have not agreed on legislation or “rules” that should apply to cyberspace or how to apply existing “rules” for espionage, crime, and warfare. Thus , attackers take advantage of the borders and the internet’s ability to cross them with ease. They even have the ability to combine database contents from multiple sources to increase the value of their harvest. This makes protection of information like that stored in databases exceedingly important.

Attackers need information from multiple sources to gain enough important data to be worth their profit. First they perform research on their target. They look for weaknesses in the organization's security either through people, systems, or the network (Micro, 2010). Once that is complete they perform their attack either through a network or social attack. A network attack occurs when they use the infrastructure, system and application weaknesses to infiltrate an organization's network (Micro, 2010). Social attacks involve tricking employees into giving access to the organization's network. Typically, a malicious attachment through an email can fool an employee into giving their login credentials to the attacker. The final step is exfiltration, once they are in they can attack the network and tunnel into and out of confidential data (Micro, 2010). Once the data is extracted, the attack is considered successful.

Attackers want to maximize potential profits, thus reasoning for sealing information in bulk quantities. However, this also means that they check out avenues to gain more data or valuable information from what they have already stolen. For example, if they have access to emails and the password associated with them then an attacker could perform some research and see what other sites the user may have also used that email address and the same password for to then gain access to more personal accounts. They could also read and write emails and potential change passwords to user’s other accounts to lock the user out of and use their account and exploit to gain more information or sell the accounts and what information they receive. Therefore, attackers inventory their stolen data, they look through for authentication credentials, personal information like names, addresses, and phone numbers, and financial information like credit card details. Attackers will package up personal information and sell them, in bulk (Editor, 2017). The more recent the more valuable. According to Quartz, a full set of someone’s personal information including identification number, address, birthdate, and possibly credit card info costs between $1 and $450 with a media cost of $21.35 (Editor, 2017). Then attackers will inventory authentication credentials further and look for lucrative accounts. Government and military addresses are very valuable, along with company email addresses and passwords for large corporations (Editor, 2017). Since people often re-use their passwords, hackers can often use credentials for military or corporate accounts to target other companies. For example, Dropbox was breached in 2012 using credentials stolen in the LinkedIn data breach earlier that year (Editor, 2017). An attacker may plan an attack themselves or they may sell the information to others on the dark web for a much higher price.

Financial information such as credit card numbers are packaged and sold in bundles as well. Usually a “broker buys the card information then sells it to a “carder” who goes through a shell game of purchases to avoid detection (Editor, 2017). The “carders” use the stolen credit card to buy gift cards to stores or to Amazon, then use those to buy physical items and then sell the items through channels like eBay, or on the dark web (Editor, 2017).

Therefore, attackers can combine information they steal through multiple channels for from multiple databases and use the information to make more profit. Just one password can give an attacker access to so much more. Some examples of data breaches in 2017 include that Equifax in which 145.5 million US citizens and 15.2 million in the UK had personal record exposed (Micro, 2018). Their name, date of birth, social security number, address, gender, phone number, driver’s license number, email, payment card number and expiration date, tax ID , and driver’s license state were all exposed. The breach was raced back to a security program vulnerability the Equifax had failed to patch (Micro, 2018). Even if just basic information was gained attackers could still use it to exploit from other positions.

Individual users are also not the group at risk, companies and organizations have much to protect, especially intellectual property. Uber was hacked in 2016, two outsiders gained access to user data that was stored on a third-party cloud-based service (Micro, 2017). The stolen information included names and driver’s license numbers of 600,000 Uber drivers, but they did not stop there. The attackers were able to gain access to the information after the company uploaded code on to GitHub, but they had failed to remove the credentials that could be used to log into special accounts on Uber’s network (Micro, 2017). The network contained the sensitive data, which was hosed on Amazon Web Service servers (Micro, 2017). Everyone needs to take steps to prevent personal information and data to be breached and know the risks of what could happen if you do not take those steps.

Attackers look for every way to gain access to information and build up their profits, even if that means going through multiple sources and using many different methods. As our society continues evolve into a digital controlled era it is important for prevention and protection of information, especially databases. Being informed on risks, staying up-to-date with patches, updates, and fixes, as well as using good password generation techniques information can be more secure. More dedication and protection should be directed toward databases within our society today, to ensure that the digital era does not cause the economy as well as society to crumble.

Work Cited

“2017 Data Breaches - The Worst Breaches, So Far | IdentityForce®.” *We Aren't Just Protecting You From Identity Theft. We Protect Who You Are.*, 11 Sept. 2018, www.identityforce.com/blog/2017-data-breaches.

Editor. “Once Stolen, What Do Hackers Do With Your Data?” *Secplicity - Security Simplified*, Secplicity, 18 May 2017, www.secplicity.org/2017/05/18/stolen-hackers-data/.

Micro, Trend. “Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes.” *Security News - Trend Micro USA*, 2010, www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101.

Micro, Trend. “Equifax Reveals Extent of 2017 Data Breach, Details Number of Stolen Records.” *Security News - Trend Micro USA*, May 2018, www.trendmicro.com/vinfo/us/security/news/cyber-attacks/equifax-reveals-extent-of-2017-data-breach-number-of-stolen-records.

Micro, Trend. “Uber Breach Exposes the Data of 57 Million Drivers and Users.” *Security News - Trend Micro USA*, Nov. 2017, www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/uber-breach-exposes-the-data-of-57-million-drivers-and-users.

Rouse, Margret. “What Is Database (DB)? - Definition from WhatIs.com.” *SearchSQLServer*, Feb. 2017, searchsqlserver.techtarget.com/definition/database.

Schulman, Amichai. “Top 10 Database Attacks.” *Top 10 Database Attacks | Security, Data and Privacy | Subject Areas | Publishing and Editorial | BCS - The Chartered Institute for IT*, 2007, www.bcs.org/content/ConWebDoc/8852.

Zurier, Steve. “8 Ways Hackers Monetize Stolen Data.” *Dark Reading*, Apr. 2018, www.darkreading.com/attacks-breaches/8-ways-hackers-monetize-stolen-data-----------/d/d-id/1331560.