**Assignment 5 Database Administration**

Total points: 50

**This assignment should be completed individually.**

**Transactions and Concurrency Control (14 pts)**

**Suppose you are a manufacturer of product QER123, which is composed of parts Q11, Q12, and Q13. Each time a new product is created, it must be added to the product inventory, using the PROD\_QOH in a table named PRODUCT. And each time the product QER123 is created, the parts inventory, using PART\_QOH in a table named PART, must be reduced by one each of parts Q11, Q12, and Q13. The sample database contents are shown below.**

**Table name: PRODUCT Table name: PART**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PROD\_CODE** | **PROD\_QOH** |  | **PART\_CODE** | **PART\_QOH** |
| **QER123** | 1,205 |  | Q11 | 567 |
|  |  |  | Q12 | 98 |
|  |  |  | Q13 | 549 |

**Given that information, answer the questions.**

* 1. **How many database requests can you identify for an inventory update for both PRODUCT and PART (a new product QER123 being created)? Using SQL, write the complete transaction(s) showing each database request. (6 pts)**

1. **Situation #1**
   1. **2 database requests**

**update product**

**set prod\_qoh = prod\_qoh + 1**

**where prod\_code = ‘QER123’**

**update part**

**set part\_qoh = part\_qoh - 1**

**where part\_code in (‘Q11’, ‘Q12’, ‘Q13’)**

**commit**

1. **Situation #2**
   1. **4 database requests**

**update product**

**set prod\_qoh = prod\_qoh + 1**

**where prod\_code = ‘QER123’**

**update part**

**set part\_qoh = part\_qoh - 1**

**where part\_code = ‘Q11’**

**update part**

**set part\_qoh = part\_qoh - 1**

**where part\_code = ‘Q12’**

**update part**

**set part\_qoh = part\_qoh - 1**

**where part\_code = ‘Q13’**

**commit**

* 1. **Write the transaction log, using the Table below as your template. (8 pts)**

Assume that product ‘**QER123**’ has a PROD\_QOH = 23 at the start of the transaction and that the transaction is representing the addition of 1 new product. Also assume that PART components “Q11”, “Q12” and “Q13” have a PROD\_QOH equal to 56, 12, and 45 respectively.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **TRL**  **ID** | **TRX**  **NUM** | **PREV**  **PTR** | **NEXT**  **PTR** | **OPERATION** | **TABLE** | **ROW**  **ID** | **ATTRIBUTE** | **BEFORE**  **VALUE** | **AFTER**  **VALUE** |
| 1 | 1A3 | NULL | 2 | START | \*\*START TRANSACTION |  |  |  |  |
| 2 | 1A3 | 1 | 3 | UPDATE | PRODUCT | ‘QER123’ | PROD\_QOH | 23 | 24 |
| 3 | 1A3 | 2 | 4 | UPDATE | PART | ‘Q11’ | PART\_QOH | 56 | 55 |
| 4 | 1A3 | 3 | 5 | UPDATE | PART | ‘Q12’ | PART\_QOH | 12 | 11 |
| 5 | 1A3 | 4 | 6 | UPDATE | PART | ‘Q13’ | PART\_QOH | 45 | 44 |
| 6 | 1A3 | 5 | NULL | COMMIT | \*\*END OF TRANSACTION |  |  |  |  |

**Database Administration (20 pts)**

The user of cloud-based data services does not signal the end of DBAs, but it does have a significant impact on their role and can also impact the security of the data. Answer the following questions.

**2.1 Discuss how the role of the DBA has transformed with the introduction of cloud computing. Be sure to use external sources to support your position.**

* **Cloud computing allows users to access data files and use applications through the Internet from any device.**
* **There is less work for the DBA to install, configure, and maintain hardware and software as the company can just pay a cloud computing service provider (e.g. Amazon – AWS, Microsoft - Azure) to receive these services.**
* **The DBA doesn’t have to worry about backup as the cloud computing service provider can handle that. However, the DBA will still have to be involved in database recovery management tasks and troubleshooting when situations such as natural disasters cause failures.**
* **Database-as-a-Service (DBaaS) providers will remove some of the work from the DBA, but the DBA should still work with these providers in understanding the services being provided and making sure that the services can help fulfill the company’s needs and goals.**
* **According to the article “THE CHANGING ROLE OF THE DBA IN THE NEW CLOUD ERA” by Joyce Wells, the DBA will be more involved in understanding “what businesses do with data rather than just the mechanics of keeping the database healthy and running”. The DBA will be more responsible for “data modeling [and] data security” (Wells).**
* **According to the article “THE CHANGING ROLE of the DBA in the NEW CLOUD WORLD” by Joe McKendrick, cloud computing will help the DBA focus more on “taking advantage of things like blockchain” and helping with strategic data and performance management tasks such as database design and performance tuning.**

**2.2 Discuss how the move to cloud computing can impact database security. What are the risks and advantages of moving to the cloud? Offer some guidelines for protecting your data in the cloud.**

* **How move to cloud computing can impact database security**
  + **Potential data breaches**
    - **Hackers can attack databases to access personal data such as healthcare or credit card information**
    - **Breaches occur more often when the database is centralized.**
  + **Potential account hacks**
    - **Hackers can use holes in database security systems to get access to users’ login information. They can then lock out the user by changing the password and access files and information stored in the user’s account (“What are the Security Risks of Cloud Computing?”).**
  + **Potential loss of data**
    - **Hackers could tamper user data in databases and if the company doesn’t perform up-to-date backups frequently, there could be a loss of updated data.**
  + **Potential Distributed Denial-of-Service (DDoS) attacks** 
    - **Hackers can make online services unavailable by overwhelming them with traffic (“Digital Attack Map”)**
  + **According to the article “12 Risks, Threats, & Vulnerabilities in Moving to the Cloud” by Timothy Morrow, with the cloud computing service provider supplying resources, the company has less control and visibility, which can have vulnerabilities in security.**
* **Risks of moving to the cloud**
  + **Potential data breaches**
  + **Potential account hacks**
  + **Potential loss of data**
  + **Potential DDoS attacks**
* **Advantages of moving to the cloud**
  + **Cost efficient**
    - **“Pay-as-you-go” vs. purchasing & installation costs of hardware & software**
  + **Less work for the client (the company requesting service) in database administration and management**
  + **Promotes collaboration between provider and client (the company requesting service) in providing services that align with the company’s needs (Walker)**
  + **Flexibility in scaling database security**
    - **The company can request the provider to scale up database security when the company is involved in operations where the number of potential threats is high (Walker). The company can request the provider to scale down database security to reduce costs when there is not much risk in operations (Walker).**
* **Guidelines for protecting data in the cloud**
  + **Cloud encryption of data**
    - **Encryption can help make data unreadable and only accessible with a decryption key.**
  + **Using economies of scale**
    - **According to the article “What are the Security Risks of Cloud Computing?”, replicating data across multiple data centers in multiple regions helps reduce the risk of losing data.**
  + **Having frequent up-to-date database backups can lead to less risk of losing data.**
  + **Not storing a lot private and sensitive information on the cloud can lead to less data leakage and identity thefts.**
  + **Having stronger passwords when logging into accounts can lead to less identity thefts.**

**Works Cited**

Digital Attack Map. (n.d.). Retrieved from https://www.digitalattackmap.com/understanding-ddos/.

Morrow, T. (2018, March 5). 12 Risks, Threats, & Vulnerabilities in Moving to the Cloud. Retrieved from https://insights.sei.cmu.edu/sei\_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html.

McKendrick, J. (2019). THE CHANGING ROLE of the DBA in the NEW CLOUD WORLD.*Big Data Quarterly, 5*(1), 8-12. Retrieved from <http://libproxy.utdallas.edu/login?url=https://search.proquest.com/docview/2216728737?accountid=7120>

Walker, S. (n.d.). 5 Benefits of a Cloud Computing Security Solution. Retrieved from https://blog.tbconsulting.com/5-benefits-of-a-cloud-computing-security-solution.

Wells, J. (2017). THE CHANGING ROLE OF THE DBA IN THE NEW CLOUD ERA.*Big Data Quarterly, 3*(3), 4-5. Retrieved from <http://libproxy.utdallas.edu/login?url=https://search.proquest.com/docview/2014890918?accountid=7120>

What are the Security Risks of Cloud Computing? (n.d.). Retrieved from <https://www.akamai.com/us/en/resources/data-security-in-cloud-computing.jsp>.

**DATABASE SECURITY (16 pts)**

**Using the following website -** <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/> - **choose 2 different incidents and read about them. Then provide a brief synopsis of each that includes a clear description of how the breech happened. In your discussion answer the following - which security measures were not in place and thus led to the issue? What security policies should be implemented or have been implemented as a result of the breech?**

**For *each* scenario provide a *minimum* 350 word synopsis. (8 points each)**

**Facebook Breach**

In September 2019, there was a leak of more than 419 million Facebook users’ phone numbers. Records of 133 million users in the U.S. were exposed (Grothaus, 2019). Each record in the databases has the phone number listed on the account. Some records even have the user’s name, gender, and country of residence. How did the breach happen? The databases were found on a server with no password protections. This allowed anyone with an internet connection to access these databases. After Facebook was notified of this breach, the databases were immediately taken down and the company stated that the dataset is “old” and had “duplicated records”, which is better than what other articles had stated but shows vulnerabilities in security for users (Grothaus, 2019).

According to the article “Facebook security breach exposed the phone numbers of over 400 million users” by Adrian Potoroaca, it was revealed that “the company's two-factor authentication system could be used by almost anyone to find [people’s] phone number[s]”. According to the article “Facebook's two-factor authentication puts security and privacy at odds”, James Martin states that hackers can “intercept text messages containing [people’s] PIN code[s] when [people] try logging in, through methods like SIM hijacking”.

This leak could also have led to the occurence of SIM swap attacks, where hackers can trick phone carriers to switch phone numbers over to SIM cards they own (Grothaus, 2019). In addition, hackers can reset passwords and prevent users from logging in by just using their phone numbers. Another possibility is that users could have gotten more spam phone calls. After this leak, Facebook has taken away developers’ access to users’ phone numbers and removed people’s ability to find others using phone numbers (Grothaus, 2019).

One way that Facebook can further improve its security is putting a login requirement with strong passwords for access to these databases. Facebook should also set access-level permissions by allowing only a certain number of people to access these databases. Facebook also “added the option to set up two-factor authentication for your account without registering a phone number” (Martin, 2019). Instead, users can now use authenticator apps like Google Authenticator or Microsoft authenticator to receive the same benefits of this privacy feature.

**Marriott Hotels Breach**

In November 2018, Marriott International reported that personal data of about 500 million people who made reservations through Marriott’s Starwood reservation system from 2014 to September 2018 was stolen. The data stolen included names, addresses, phone numbers, birth dates, email addresses, credit card details, and even travel histories and passport numbers. Marriott came across an unauthorized attempt to access the guest reservation database in September 2018 and later discovered that hackers had started the infiltration back in 2014.

Surprisingly, according to an article “Marriott data breach FAQ: How did it happen and what was the impact?” by Josh Fruhlinger, in December 2018, articles from the New York Times and the Washington Post mentioned that the hackers might have been employed by Chinese intelligence services. One reason was that none of the data stolen was for sale on the dark web, which is a collection of encrypted websites. James A. Lewis, a cybersecurity expert at the Center for Strategic Studies in Washington, stated that “usually when stolen data doesn’t appear, it’s a state actor collecting it for intelligence purposes” (Perlroth, 2018). The stolen information can be analyzed and from this, countries can learn about people’s, including intelligence agents’, comings and goings (Perlroth, 2018). Another reason was that “the code and attack patterns used [matched] up with techniques employed by state-sponsored Chinese hackers” (Fruhlinger, 2019).

There was a lack of security defense, which allowed hackers to access and breach the system for 4 years. Fruhlinger also stated that the passport numbers were not all encrypted (Fruhlinger, 2019). In addition, encrypted credit card numbers and keys were stored on the same server, which led to a huge gap in protection. For example, leaving your keys in the lock is way riskier than keeping your keys in another location.

After the breach, Marriott set up a website and call center to reach out to and inform people who had been affected about the breach. The company is also offering 1 year of free service called Web Watcher for guests, where it monitors websites and alerts people when hackers swap and sell personal information on these sites. Another policy that could be implemented is to store encrypted data and encrypted keys on different servers.

**Works Cited**

Grothaus, M. (2019, September 5). The phone numbers of 419 million Facebook accounts have

been leaked. Retrieved from https://www.fastcompany.com/90399734/the-phone-numbers-of-419-million-facebook-accounts-have-been-leaked.

Fruhlinger, J. (2019, September 30). Marriott data breach FAQ: How did it happen and what was

the impact? Retrieved from https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html.

Ng, A. (2019, March 5). Facebook's two-factor authentication puts security and privacy at odds.

Retrieved from https://www.cnet.com/news/facebooks-two-factor-authentication-with-phone-numbers-puts-security-and-privacy-at-odds/.

Perlroth, N., Tsang, A., & Satariano, A. (2018, November 30). Marriott Hacking Exposes Data of

Up to 500 Million Guests. Retrieved from https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html.

Potoroaca, A. (2019, September 4). Facebook security breach exposed the phone numbers of

over 400 million users. Retrieved from https://www.techspot.com/news/81752-hundreds-millions-phone-numbers-facebook-accounts-leaked-online.html.