Security incident

Nowadays, many software companies become successful and profitable overnight because the software has practical and easy handling features. Moreover, cloud services give another opportunity to let companies run at low cost and provides many non-functional advantages. This article will describe a security event that happened in Feb, 2015, analyse distributed Database security concerns and SaaS security considerations.

Feature of Slack

Enterprise chat software *Slack* is a platform for team communications which integrates with tools like Dropbox, Twitter, Hangouts, Github, etc, and provides real-time messaging, file sharing, etc. It provides single points login and third-party tools connecting authorization.

Incident Description

Four days in February, Slack suffered database breach due to unauthorized access, exposing sensitive information to malicious hackers including user name, email address, Skype ID, phone numbers and one-way hashing passwords which adopted randomly generated salt per-password. But no financial information and chat logs were accessed in the attack even though searchable chat logs have not encrypted.

Influence and why it is significant

The influence may be worse than the official analysis. Slack has 60,000 clients, like Apple, Google, Amazon, etc. Besides, many sensitive logs without encryption may threat the operation of many companies.

Measures taken

The company takes many measures to face the security event. The most important is two-factor authentication, which allows users to receive a one-time use code on phone to enter with other account credentials. Besides, it offered team leaders a “password kill switch” to automatically reset passwords for every team members, which terminate user sessions.

Possible Reasons for the incident and analysis

Slack has many security threats. Firstly, enterprise-oriented, means it needs user identity authentication and access control when retrieving shared files and messages logs. Another is about encryptions, encrypting user profile, relationship and meeting logs. Lastly, when integrating with many third party tools, these third-parties provide different connection protocol and ways of data exposing.

Database

However, it was after four days that Slack realised the compromised database, and more problems about database security reveals. It must lack authentication. It may use cloud database while some distributed Database like MongoDB had some security incidents last year because of bugs in access control and authentication. Besides, four days without tracing usage probably means that the database system lacked audits and analysis. Firewall can be effective in this situation to provide Asym/sym authentication, and PKI with certificate authority, which ensures internal data secure. The database security can be enhanced by segmenting data and update database system regularly.

Data from connecting applications may be comprised in the future or right now. For example, user lists from Google+. SaaS provides many benefits but also security risks. One compromised data triggered series of leaked information. Some providers provide good security protocols like encrypted connector provided by Google.

References

[1] Ben-Natan, Ron. *Implementing Database Security And Auditing*. Burlington, MA: Elsevier Digital Press, 2005. Print.

[2] Brodkin, Jon. '5 Problems With Saas Security'. *Network World*. N.p., 2015. Web. 29 Mar. 2015.

[3] Cnodejs.org,. 'Limbo: 简单访问远程数据库 - Cnode'. N.p., 2015. Web. 29 Mar. 2015.

[4] 'March 2015 Security Incident And The Launch Of Two Factor Authentication'. N.p., 2015. Web. 29 Mar. 2015.

[5] Salesforce.com,. 'Saas (Software As A Service) Security & Performance Information - Salesforce.Com'. N.p., 2015. Web. 29 Mar. 2015.

[6] Slack,. 'Slack: Be less busy'. N.p., 2015. Web. 29 Mar.2015.

[7] The Verge,. 'Slack Enables Two-Factor Authentication Following Security Breach'. N.p., 2015. Web. 29 Mar. 2015.