Enterprise Systems and Threats

Dr. Risa Blair
Instructional Associates, LLC
Miami Shores, FL, 33150/EST, United States

ABSTRACT[1]

The scenario included a medium-sized international company. The guidelines were to select and include three enterprise systems that were based on databases, one cloud-based and one that was not SQL-based. Systems were accessible via a browser and included mobile applications. Of key importance for this project was to research potential and known vulnerabilities for these three enterprise systems. The systems selected were ADP Streamline Payroll, Salesforce, and MongoDB. There are numerous threats described in this project, including excessive privileges, SQLi attacks, weak auditing, storage media exposure, unnecessary features enabled, broken configurations, and buffer overflows. Enterprise systems are a potential magnet for hackers on the black market and the Dark Web, as they provide extensive confidential data, particularly in the technology, finance, government, education, healthcare, and retail sectors. It was impressive to see how both ADP and Salesforce provided up-to-date known and potential vulnerabilities. What was the most interesting throughout the research was uncovering the Mongo Lock ransomware and the Salesforce Meatpistol malware. What is worse is that the Salesforce team provided a talk in Las Vegas in July of 2017, where they explained how Salesforce attacked its own system to see how well it would hold up against cyber attacks. The talk focused on Meat pistol, a malware too for making it easier to conduct the attacks from the standpoint of infrastructure automation, implant creating, and interaction. The intent was to make it easier for the Salesforce teams to conduct their attacks. They utilized the methodology of the well-known tool, Metasploit, which does not exploit systems or launch attacks. It just provides the framework for hackers to control systems after they have been able to access what they choose. The duo of "red team" inside hackers explained their process for access the system through the utilization of Meatpistol, against the advice of their superiors. Immediately after the presentation, they were fired.

Keywords: SQLi attacks, storage media, Dark Web, Salesforce, Meatpistol, malware, cyber attacks.

1. INTRODUCTION

Three enterprise systems for this presentation regarding the medium-sized global company described in the scenario include ADP Streamline Payroll, Salesforce, and MongoDB. The first enterprise system, ADP Streamline Payroll, is cloud-based software and designed for managing human resources and global payroll. The embedded data hub functionality allows users to review HR data and to manage payroll. The software effectively handles global payroll, as in-country specialists with localized knowledge utilize best practices for HR. Sensitive data, including tax identification numbers, demographics, and social security numbers are stored within the system.

The second enterprise system, Salesforce, is a cloud-based customer relationship management (CRM) tool designed for managing relationships with current customers and potential customers. CRM's facilitate communication with clients (internal and external), facilitate procedures, and increase profitability. CRM's are laser-focused on building and maintaining relationships throughout the lifecycle process, as well as providing additional products and services to existing customers. Salesforce provides a complete record of customer communications, sales, invoicing, accounting, marketing, commerce, engagement, integration, advanced analytics, artificial intelligence, and surveys (Salesforce, 2019).

[1] The paper "Enterprise Systems and Threats" was edited by Dr. Lyndon Godsall. I would like to express my deeply felt gratefulness to Dr. Godsall for his comprehensive and detailed peer-editing of this document.

The third enterprise system, MongoDB, uses a nonrelational database model, is open source, and uses a database model that relies on a document orientation. This database model is nearly 20 years old, and uses the NoSQL technology to manage big data and other data that does not fit within a relational database model. MongoDB relies on documents and collections rather than rows and tables, as one would find in relational databases. MongoDB is designed to support big data applications through the core design functionality based on horizontal scalability. This enterprise system also provides Application Programming Interfaces (APIs) to connect with third-party tools and storage engines. There are some restrictions with MongoDB, as the architecture does not support data sharing among different databases (Botelho & Vaughan, August 2018).

2. DATA & DATABASE ENTERPRISE SYSTEM THREATS

There are data and database enterprise threats that IT security professionals need to keep in the forefront while implementing and maintaining database systems and data. There may be unused or excessive privileges assigned by default. Clear control mechanisms need to put into place to provide employees with the privileges they need, but no extended privileges. These extended privileges may lead to system abuse (Fletcher, 28 March 2017).

Web Shell and SQL Injection (SQLi) attacks may be categorized as a web application security threat. Malicious code may be entered into web application fields or added to Big Data components. The lack of web application security provides a potentially open backdoor to hackers to gain unrestricted database access (Fletcher, 28 March 2017).
Data and database applications may also suffer from the threat of a weak audit. This shortcoming involves the lack of automated monitoring for databases. In this case, compliance anomalies and security details, along with audit logs containing contextual details are not set up or maintained by the IT security professionals. These detailed logs are essential for investigating incidents and warding off potential hacker attacks at multiple levels (Fletcher, 28 March 2017).

Another somewhat obvious threat to data and databases is storage media exposure. If the media is left exposed and unprotected, and not locked up, it is possible that backup discs or tapes make be taken – from an insider or an outsider (Fletcher, 28 March 2017).

Additional database threats include unnecessarily enabled database features. Database administrators should disable or uninstall these unused features. Broken configuration management is a challenge and needs to be dealt with when the system is installed. These elements need to be disabled or turned off. Buffer overflows provide opportunities for hackers to flood input sources, for instance. Database vendors generally distribute patches to deal with such issues. This is one reason why routinely running patches is so very important. Finally, all database data should be encrypted, whether at rest or in motion (Dark Reading, 1 November 2010).

Cloud-based enterprise systems have some unique threats and vulnerabilities. With cloud services, there is a shared responsibility for management and data security between the client and the provider. Such a partnership requires both parties to be proactive in protecting their data. Although key providers, including Google, Microsoft, Box, and Dropbox have fundamental security practices in place, it is up to the client to provide fine grain control related to password security, access restrictions, and authentication. Data loss on the cloud is a risk, as exhibited by Amazon and Google. Both companies suffered severe losses by destroying data (Amazon) and natural disaster (Google). The onus is on the client to review the provider's back up policies and procedures as they relate to physical storage, access, and disaster recovery (Application Security, 14 December 2015).

3. REASONS FOR ENTERPRISE SYSTEM THREATS

Enterprise system threats exist since an organization's confidential employee, and customer data are maintained in these systems. Industries in the technology, finance, government, education, healthcare, and retail sectors are all active targets for hackers. The data can be extremely valuable on the black market. Data breaches can be equally devastating to individuals and organizations (Fletcher, 28 March 2017).

Hackers choose to access data for the purpose of stealing or leaking information about employees,

customers, or other proprietary and confidential data specific to the organization. Threat actors may go after major targets to make the biggest impact and draw the most attention. Such companies include Equifax, eBay, Home Depot, Adobe, Yahoo, Target, and Sony. Hackers may choose to embarrass users, as they did with penetrating the Ashley Madison site and the exposure of people's private information.

Threat actors also have other reasons for hacking, like taking systems down through a DoS or a DDoS, to cause even more impact. They may choose to steal customer confidential information or data and hold it for ransom, with the ultimate goal of making money. Finally, hackers may have an alternate purpose in mind – for taking down a government, targeting a religious group, or promoting an agenda. Regardless, enterprise systems running in an organization may be impacted by such a hacking attempt. It is the job of the IT security professionals and database administrators to secure data, systems, hardware, software, the cloud, and third-party tools, as well (Appknox, n.d.).
are performed.

4. VULNERABILITIES – DATA, DATABASES, AND INFRASTRUCTURES

A known vulnerability for ADP systems was the Drupal core vulnerability (CVE-2018-7600), which could allow hackers to remotely execute code on affected systems. ADP indicated that after close inspection of their systems, that this specific vulnerability impacted no client-facing systems, but that the company would continue to monitor the situation (ADP, 23 April 2018). Another vulnerability reported by ADP was the Apache Struts vulnerability (CVE-2018-117766), which would potentially allow threat actors to remotely execute code on ADP systems. Again, upon a close investigation of its systems, ADP determined that such a threat was prevented through their layered defense strategy of using technologies and controls to ward off such threats, through implementing protection and detection controls (ADP, 29 August 2018).

Some common vulnerabilities for Salesforce data include authorization bypass, SOQL injection, and stored cross-site scripting. Access control, or authorization, serves as a key security control for multi-users within a shared database setting. If the IT security professional established the correct roles for users in the system, each user would access only the intended functions, resources, and data, necessary to complete their work. When roles and authorization schemas are not properly structured, the data and database are vulnerable, as the backdoor is open for hackers (Wolf, 22 May 2018).

Salesforce Object Query Language (SOQL) is the programming language which supports the storage and retrieval of information in Salesforce databases. SOQL, which is a stripped-down version of SQL, is the Salesforce version of the program. SOQL injection allows hackers to input characters in a form to modify queries. This can occur if the IT security professional fails to establish user input validation methods. Without these user input validation methods in place, Salesforce depends on the users and their input to ensure integrity. Hackers are able to find a backdoor to access the data (Wolf, 22 May 2018).

Another known issue with Salesforce is Cross-site scripting (XSS), which refers to information that is stored as XSS. XSS does not necessitate that a malicious link is utilized. XSS can be hidden anywhere, on any page of a web application where data is gathered and stored from users for future use. If malicious data is entered by a user, it does not get filtered out by the system. That user input becomes part of the website and runs in the browser, exactly like the web application, with the identical permissions. The threat actor can hijack a user's browser, collect others' confidential information, deface the application, and even port scan hosts (Wolf, 22 May 2018).

MongoDB also contains some known vulnerabilities. The first vulnerability is the automatic failover strategy. When a database developer structures the database, it is only required that one master node be established. The design of MongoDB is structured such that if the original database master fails, it will automatically move to the slave node. That same slave node will become the new master. Although this switch does occur, it may take up to one minute, so there is not direct continuity. Data could be damaged, corrupted, or impacted during the wait time (Botelho & Vaughan, August 2018).

Another issue with MongoDB is that it does not offer complete referential integrity by virtue of using foreign key constraints. This issue can impact

the consistency of the data. On other vulnerability of MongoDB is that the default settings do not include user authentication. The database administrator needs to change the settings. Without user authentication enabled, hackers are able to attack the system and have been able to carry out numerous ransom attacks (Botelho & Vaughan, August 2018).

Critically important weaknesses in MongoDB are the lack of user authorization and the lack of administrator authorization. All users have instant read-only access to the entire database. This does not provide for optimal security. Additionally, anyone with administrative user access to the database has full read and write access to everything. Administrators do not have required passwords, so there is little control or granularity designating who has access to what (Kirkpatrick, 21 March 2013).

5. SUMMARY

MongoDB experienced a difficult ransom attack via the deployment of Mongo Lock ransomware. The way Mongo Lock worked was that attackers scanned the Internet or used Shodan.io to find unprotected servers running MongoDB. Once hackers connected with the servers, they opted to export and delete the database. Then, they deployed the ransom note, which explained that the database was encrypted and that if the owner wanted access to the data, he or she would need to send the ransom via BTC (.1 BTC). The owner was also instructed to save a unique key and email it to a particular email for decryption service. There were different versions of this ransom attack, with the most expensive equating to about USD $11,000 (Abrams, 11 September 2018).

Another fascinating incident related to malicious software (pen testing) was revealed by Salesforce. Two senior security engineers developed MEATPISTOL, an anagram of Metasploit for the purpose of deploying malware to attack Salesforce. They developed Meatpistol in-house, with the intention of the tool being used as an open-source tool for exploiting weaknesses and strengthening network security. These two engineers presented their project at DEF CON, one of the largest hacker conferences to their audience. A Salesforce executive texted the engineers not to go on stage and present. However, they missed the text. Upon the conclusion of their presentation, they were told they no longer worked for Salesforce (Quach, 10 August 2017).

6. REFERENCES

[1] Abrams, L. (2018, September 11). **Mongo Lock attack ransoming deleted MongoDB databases.** Retrieved from https://www.bleepingcomputer.com/news/security/mongo-lock-attack-ransoming-deleted-mongodb-databases/

[2] ADP. (2018, April 23). **Drupal core vulnerability.** Retrieved from https://www.adp.com/about-adp/data-security/alerts/information-regarding-drupal-core-vulnerability.aspx

[3] ADP. (2018, August 29). **Apache Struts vulnerability.** Retrieved from https://www.adp.com/about-adp/data-security/alerts/information-regarding-apache-struts-vulnerability.aspx

[4] ADP. (2019a). **ADP Streamline Payroll.** Retrieved from https://www.softwareadvice.com/hr/adp-streamline-profile/

[5] ADP. (2019b). **ADP Streamline Payroll screenshot.** Retrieved from https://www.getapp.com/hr-employee-management-software/a/adp-streamline/

[6] Appknox. (n.d.). **Why do hackers hack – five big reasons explained.** Retrieved from https://blog.appknox.com/why-do-hackers-hack/

[7] Application Security. (2015, December 2014). **Top 10 security concerns for cloud-based systems.** Retrieved from https://www.imperva.com/blog/top-10-cloud-security-concerns/?utm_campaign=Incapsula-moved

[8] Botelho, B., & Vaughan, J. (2018, August). **MongoDB.** Retrieved from https://searchdatamanagement.techtarget.com/definition/MongoDB

[9] Dark Reading. (2010, November 1). **The 10 most common database vulnerabilities.** Retrieved from https://www.darkreading.com/vulnerabilities---threats/the-10-most-common-database-vulnerabilities/d/d-id/1134676

[10] Fletcher, D. (2017, March 28). History repeating: Top five database threats. Retrieved from https://www.infosecurity-magazine.com/opinions/history-repeating-top-five/

[11] Kirkpatrick, D. (2013, March 21). MongoDB – security weaknesses in a typical NoSQL database. Retrieved from https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog-mongodb-security-weaknesses-in-a-typical-nosql-database/

[12] Quach, K. (2017, August 10). **Salesforce sacks two top security engineers for their DEF CON talk.** Retrieved from https://www.theregister.co.uk/2017/08/10/salesforce_fires_its_senior_security_engineers_after_defcon_talk/

[13] Salesforce. (2019). **Explore the CRM software features that can help you grow sales faster.** Retrieved from https://www.salesforce.com/products/sales-cloud/features/

[14] Whittaker, Z. (2017, August 9**). Salesforce fires red team staffers who gave Defcon talk.** Retrieved from Salesforce fires red team staffers who gave Defcon talk | ZDNet

[15] Wolf, A. (2018, May 22). **Common risks to your Salesforce data – and how you can prevent them.** Retrieved from https://222.salesforceben.com/common-risks-salesforce-data/