ATLANTIS PRESS
Advances in Engineering Research, volume 166
3rd International Conference on Automation, Mechanical Control and Computational Engineering (AMCCE 2018)

Safety Protection Implementation for Automotive Repair Information Disclosure Service Platform

Guoliang DONG[a], Hong JIA[b], Haiying XIA[c]
Research Institute of Highway Ministry of Transport, Beijing, China
[a]email:GL.DONG@rioh.cn, [b]email:H.JIA@rioh.cn, [c]email:Hy.XIA@rioh.cn

Keywords: Information System, Safety Protection, Internet Security, Intrusion prevention, Server Security, Database Security

Abstract. Automotive repair information disclosure service platform is deployed on the internet which is open to the web users. The system's security should be seriously considered. The safety methods and technology applied in the process of deploying is discussed, such as institutional construction, server protection, database protection, system operation and maintenance. The platform is running normally after officially deployed. The protection methods and technology is proved to meet the security goal for the application and the database.

Introduction

The security of information system is very important for an application or system deployed on the web internet.

Automotive repair information disclosure service platform is deployed on the internet which is open to the internet users. The system is deployed on two physical servers. The web application is deployed on the application server which is open to the web internet, mainly facing to the automotive manufactures, repair works and others social users. Database is deployed on the data server which is unseen for normal users, hidden behind the application server. The system's topology diagram is shown in Fig.1.

Security technology must be seriously considered to protect the system running normally [1]. The strategy, methods and technology applied on the automotive repair service platform will be discussed.

Institutional Construction

A perfect security management system of a networks platform is the foundation for the management of the platform running and operating behavior [2]. It ensures the information system under security control according to the security system in the process of designing, developing, test running, security evaluating, officially running and operating maintenance.

Security Management System. Include the principle, construction, drawing, publishing, modifying and executing.

Operation Instruction. Include the instruction for system administrators, security administrators, operators, key equipment.

Security Management Organization. Setting up security management organization and configure necessary staff.

Staff Security Management. Include the regulations for employment offer, employee departure, employee evaluation, safety education training and outsiders. Some important posts should sign confidentiality agreements.

System Construction Management. Include the management regulations for the self-developed software, outsourcing software, platform test running [3].

System's Operation and Maintenance Management. Include the management system for computer room, network safety, system patch and version, system leak scanning, system updating

and publishing, data backup and restore, safety events report, events disposition and emergency plan for network security.

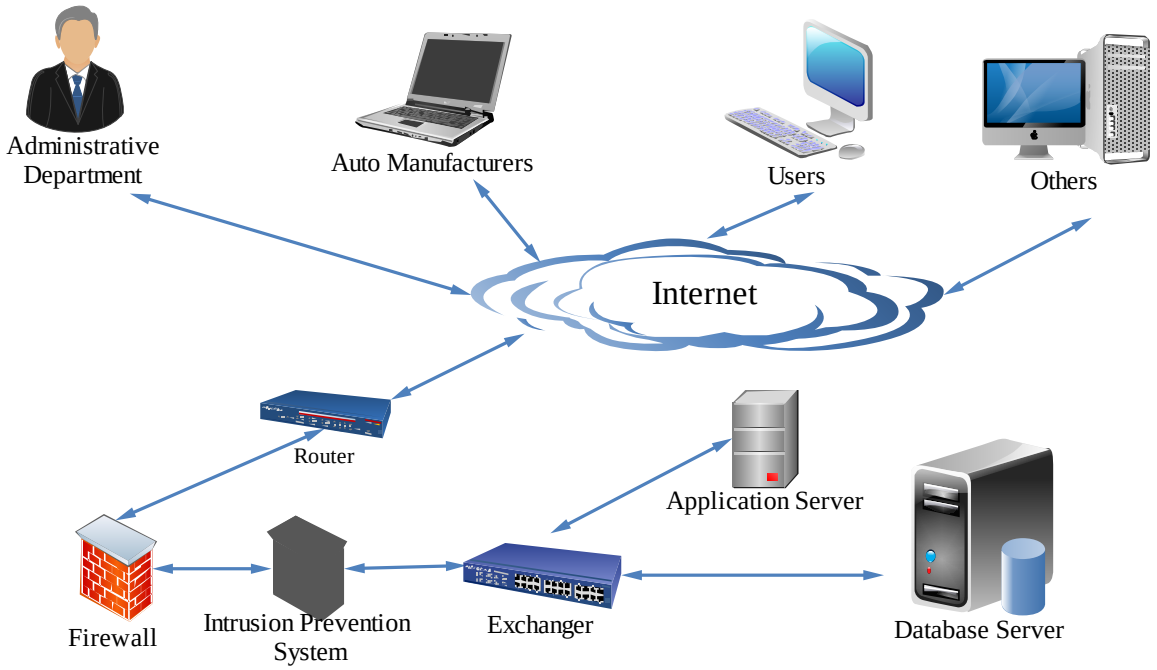

Fig.1. The system topology diagram

Hardware Protection Strategy

Hardware firewall and intrusion prevention system are important and protective barriers for the application server and the data server, which will monitor and filter virus, malicious attacks and other unusual access to the platform system.

Hardware Firewall. Support the function such as preventing external attack, intranet security, flow monitoring, junk mail filter, web filter, application filter. Use the ASPF(Application Specific Packet Filter)technology to detect the link status and unusual command or request. Supply many intelligent analysis and management means to monitor the network which will assist the webmaster to manage the system security.

Intrusion Prevention System. Intrusion prevention system is the important barrier to detect and block the threat from malicious attack to the system. The following technology is used in the intrusion prevention system for automotive repair platform.

Defense for Advanced Threats. Integrate sandbox function which will defend the APT attacks. Detect exploits and unknown malware. Detect and defend the known and unknown attacks.

Flow Scanning Virus Technology. Track the hot virus in real time. Update the hot virus library within hours.

Sensitive Data Protection. Detect and block some documents from sending out. Check sensitive data and warn the webmaster, block the documents from leaking out.

Botnets Protection. Detect malicious URL and botnets based on the real-time creditability mechanism and intercept the threats.

Software Protection Strategy (Servers Protection Strategy)

General Server Protection Strategy (Intrusion Prevention). The following strategy is applied on application server and data server to protect the system [4].

Account Management. Close the default administrator account. Create a new administrator account. Close guest account. Set up complex passwords. Set up account lock time, account lock threshold, reset account lock counter to strengthen the security of the system.

Software Firewall. Set the software firewall active. Close unused services such as telnet, terminal. Close vulnerable ports such as 135,136,137,138,139,445 [5].

System Log. Set system log active to record the user behavior logging on the server including date, time, user, event description and event status [6].

Operation System Update. Set the system update mode as "Automatic Updates" to fix the bugs to be updated [7] .

Bugs Fix. Fix bugs of the development environment or structure which the application is based on such as MySQL, Struts, Apache tomcat.

Auditor Role. Set up auditor role to audit the logins log, error log and warning message.

Remote desktop. Forbid the default port for remote desktop access. Open a new and specific port for it which will reduce the attacked probability.

Safety Protection Software. A professional protection software is installed which can kill the virus and protect the system. Scanning the system files based on the newly anti-virus engine to check the virus and Trojan, clean threat efficiently [8]. Detect the network, application and application services in real time to monitor the ports, applications and processes. Once a threat is detected, it will be intercepted timely to avoid harming to the computer and the system.

Communication Security. Encryption method is applied in authentication communication to prevent the user name or password is intercepted (if in the clear text).

Application Server Protection Strategy. The authentication strategy for application users is applied only on application server.

Assigned Account. Submit an account application offline with necessary application materials. After approval, a new account is assigned to the applicant. The unwanted is forbidden to access the platform system to reduce the potential risks.

Login Failure Security Strategy. Set the account login failure strategy such as end session, limiting the failed log-in attempts number before the account is locked, locking the account temporarily, prompting fuzzy failure message which will avoid the account and the password being guessed or exploited.

Mandatory Complex Password. Force using complex password to avoid the password is guessed or exploited.

Data Server Protection Strategy. Database is the root of the system. Data security is very important [9]. The authentication strategy for application users is applied only on data server.

Assigned Accounts. Assign account to the necessary applicant. The account is unique and partial access.

Specific IP access. Limit the IP range. Only specific intranet IP could access the data server to reduce the attack probability from the internet.

Data Security. Many methods are used to protect the data security The following strategy is applied to the platform.

Functionally-separate Servers. Application server and data server are separate. Application and data is deployed and saved independently. Once the application server is attacked, the application database will not be destroyed.

Data Server Access Management. Only specific intranet IP could access the data server. Communicate with the application server by specific port (not default port).

Port Limit. Close some high-risk default port to reduce the security risk.

Database Security. Access the database in complex password. Close the default database administrator account. Create a specific administrator account. Set up the minimum access for each account to prohibit the privilege abuse.

Data Backup and Restore. Apply Cloud backup and manual backup for database [10]. Two backup methods ensure the data security.

Conclusion

The platform is running normally up to now after officially deploying the discussed security methods. The protection methods and technology is proved to meet the security goal for the application and the database.

References

[1] Min LEI, Xiao-ming LIU, Hong ZHANG, Mian WANG and Yu YANG. Research on Security Threats and Risk Assessment of Web Information System [J]. Journal of Beijing University of Posts and Telecommunications, 2016 39(b06) 87-93.

[2] Da-zhe YANG and Rui-hao SUN. Practice of Classified-protection-based Oracle Database Security Reinforcement in Electric Power Information Systems [J]. Shanxi Electric Power, 2015(5) 38-40.

[3] Xiang-fei CHE. Study on the Security Evaluation Scheme before the Information System Go Online [J]. Software Engineer, 2015(11) 15-17.

[4] Shu-wen LI. Security Management Study for Information System Operation and Maintenance [J]. Economic & Trade, 2016(17).

[5] Yin-min JIN. Information Port and Security Strategy [J]. Network Security Technology & pplication , 2015 (11) 77-77.

[6] Peng-cheng HE and Yong FANG. A Risk Assessment Model of Intrusion Detection for Web Applications Based on Web Server Logs and Website Parameters [J]. Netinfo Security, 2015 (1) 61-65.

[7] Chao LI. Analysis of Trojan Virus Stealth Mode and Security Protection [J]. Information & Communications, 2014(3) 148-149.

[8] Tian-yan GUO. Analysis for Hazard Protection Method of Multi-stage Attack [J]. Network Security Technology & Application, 2016 (4) 21-22.

[9] Yan ZHANG. Analysis and Resolution of Database Security in Information System [J]. Computer Knowledge and Technology, 2014(15) 3468-3470.

[10] Ji-bin WANG and Huan-peng LIU. Research on Management Information System Data Backup and Recovery in the Operation and Maintenance Services [J]. Information Technology, 2016(7) 192-194.