ERP security

ERP Security is a wide range of measures aimed at protecting Enterprise resource planning (ERP) systems from illicit access ensuring accessibility and integrity of system data. ERP system is a computer software that serves to unify the information intended to manage the organization including Production, Supply Chain Management, Financial Management, Human Resource Management, Customer Relationship Management, Enterprise Performance Management. Common ERP systems are SAP, Oracle E-Business Suite, Microsoft Dynamics.[1]

Contents

Review

ERP system integrates business processes enabling procurement, payment, transport, human resources management, product management, and financial planning.[2] As ERP system stores confidential information, the Information Systems Audit and Control Association (ISACA) recommends to regularly conduct a comprehensive assessment of ERP system security, checking ERP servers for software vulnerabilities, configuration errors, segregation of duties conflicts, compliance with relevant standards and recommendations, and recommendations of vendors.[3][4]

Causes for vulnerabilities in ERP systems

Complexity

ERP systems process transactions and implement procedures to ensure that users have different access privileges. There are hundreds of authorization objects in SAP permitting users to perform actions in the system. In case of 200 users of the company, there are approximately 800,000 (100*2*20*200) ways to customize security settings of ERP systems.[5] With the growth of complexity, the possibility of errors and segregation of duties conflicts increases.[3]

Specificity

Vendors fix vulnerabilities on the regular basis since hackers monitor business applications to find and exploit security issues. SAP releases patches monthly on Patch Tuesday, Oracle issues security fixes every quarter in Oracle Critical Patch Update (https://www.oracle.com/technetwork/topics/security/alerts-086861.html). Business applications are becoming more exposed to the Internet or migrate to the cloud.[6]

Lack of competent specialists

ERP Cybersecurity survey[7] revealed that organizations running ERP systems "lack both awareness and actions taken towards ERP security".[8] ISACA states that "there is a shortage of staff members trained in ERP security"[5] and security services have the superficial understanding of risks and threats associated with ERP systems. Consequently, security vulnerabilities complicate undertakings such as detecting and subsequent fixing.[6][9]

Lack of security auditing tools

ERP security audit is done manually as various tools with ERP packages do not provide means for system security auditing. Manual auditing is a complex and time-consuming process that increases the possibility of making a mistake.[3]

Large number of customized settings

The system includes thousands of parameters and fine settings including segregation of duties for transactions and tables, and the security parameters are set for every single system. ERP system settings are customized according to customers' requirements.

Security issues in ERP systems

Security issues occur in ERP systems at different levels.

Network layer

Traffic interception and modification

- Absence of data encryption

In 2011, Sensepost specialists analyzed DIAG protocol used in SAP ERP system for transferring data from the client to the SAP server. Two utilities were published that allowed to intercept, decrypt, and modify client-server requests containing critical information. This made attacks possible including Man-in-the-middle attack. The second utility operates like a Proxy and was created to identify new vulnerabilities. It allowed modifying requests coming to client and server.[10]

- Sending password in cleartext (SAP J2EE Telnet / Oracle listener old versions)

In the SAP ERP system, it is possible to perform administering functions via Telnet protocol, which encrypts passwords.

Vulnerabilities in encryption or authentication protocols'

- Authentication by hash
- XOR password encryption (SAP DIAG)
- Imposing the use of outdated authentication protocols
- Incorrect authentication protocols

Vulnerabilities in protocols (e.g. RFC in SAP ERP and Oracle Net in Oracle E-Business Suite). RFC protocol is used (Remote Function Call) to connect two systems by TCP/IP in SAP ERP. RFC call is a function that enables calling and running a functional module located in a system. The ABAP language that is used for writing business applications for SAP have functions to make RFC calls. Several critical vulnerabilities were found in SAP RFC Library versions 6.x and 7.x:[11]

- RFC function "RFC_SET_REG_SERVER_PROPERTY" allows determining an exclusive use of RFC server. Vulnerability exploits lead to a denial of access for the legitimate users. denial of service becomes possible.
- Error in RFC function "SYSTEM_CREATE_INSTANCE". Exploiting vulnerability allows executing arbitrary code.
- Error in RFC function "RFC_START_GUI". Exploiting vulnerability also allows executing arbitrary code.
- Error in RFC function "RFC_START_PROGRAM". Exploiting vulnerability allows executing arbitrary code or gain information about RFC server configuration.
- Error in RFC function "TRUSTED_SYSTEM_SECURITY". Exploiting vulnerability allows obtaining information about existing users and groups in RFC server.

Operating system level

OS software vulnerabilities

- Any remote vulnerability in OS is used to gain access to applications

Weak OS passwords

- Remote password brute-forcing
- Empty passwords for remote management tools like Radmin and VNC

Insecure OS settings

- NFS and SMB. SAP data becomes accessible to remote users via NFS an SMB

- File access rights. Critical SAP and DBMS Oracle data files have insecure access rights such as 755 and 777
- Insecure hosts settings. In the trusted hosts, servers can be listed and an attacker easily accesses them

Application vulnerabilities

ERP systems transfer more functionality on the web applications level with a lot of vulnerabilities:

- Web application vulnerabilities (XSS, XSRF, SQL Injection, Response Splitting, Code Execution)
- Buffer overflow and format string in web-servers and application-servers (SAP IGS, SAP Netweaver, Oracle BEA Weblogic)
- Insecure privileges for access (SAP Netweaver, SAP CRM, Oracle E-Business Suite)

Role-based access control

In ERP systems, RBAC (Role-Based Access Control) model is applied for users to perform transactions and gain access to business objects.[12] In the model, the decision to grant access to a user is made based on the functions of users, or roles. Roles are a multitude of transactions the user or a group of users performs in the company. Transaction is a procedure of transforming system data, which helps perform this transaction. For any role, there is a number of corresponding users with one or multiple roles. Roles can be hierarchical. After the roles are implemented in the system, transactions corresponding to each role rarely change. The administrator needs to add or delete users from roles. The administrator provides a new user with a membership in one or more roles. When employees leave the organization, the administrator removes them from all the roles.[13]

Segregation of Duties

Segregation or Separation of duties, also known as SoD, is the concept according to which a user cannot make a transaction without other users (e.g. a user cannot add a new supplier, write out a cheque or pay to a supplier)[14] and a risk of fraud is much lower.[15] SoD can be implemented by RBAC mechanisms, and a notion of mutually exclusive roles is introduced. For instance, to pay a supplier, one user initiates payment procedure and another accepts it.[16] In this case, initiating payment and accepting are mutually exclusive roles. Segregation of duties can be either static or dynamic. With static SoD (SSoD), a user cannot belong to two mutually exclusive roles. With dynamic SoD (DSoD), a user does but cannot perform them within one transaction. Both of them have their own advantages. SSoD is simple, while DSoD is flexible.[17] Segregation of Duties is explained in SoD matrix. X and Y matrixes describe system roles. If the two roles are mutually exclusive, there is a flag at the interception of the corresponding rows and columns. The examples of Segregation of Duties software:

- Appsian Security Platform (http://www.appsian.com) for Oracle E-Business Suite and SAP ECC/S4HANA

ERP Security scanners

ERP Security scanner is a software intended to search for vulnerabilities in ERP systems. Scanner analyzes configurations of ERP system, searches for misconfigurations, access control and encryption conflicts, insecure components, and checks for updates. The scanner checks system parameters for compliance with

the manufacturer's recommendations and auditing procedures ISACA. ERP Security scanners produce reports with the vulnerabilities listed according to their criticality. The examples of scanners:

- SecurityBridge (https://securitybridge.com/) Holistic Cybersecurity Platform for SAP ERP
- ERPScan (https://erpscan.io/) for SAP ERP
- Onapsis (https://www.onapsis.com/) for SAP ERP
- Safe O'Clock (https://safeoclock.com/) for SAP ERP
- AppSentry (http://www.integrigy.com/products/appsentry) for Oracle E-Business Suite
- Appsian Security Platform (http://www.appsian.com) for Oracle E-Business Suite and Oracle PeopleSoft
- MaxPatrol (http://www.ptsecurity.ru) for SAP ERP

ERP Data Security

ERP Data Security is software intended to provide fine-grained access controls and visibility to specific transactions and data fields within an ERP application. The intention of ERP Data Security is to ensure that access to data is dynamically enforced based on the context of a user's access versus pre-defined roles and privileges. Both of which can be corrupted or exploited. ERP Data Security software is intended to work in conjunction with an organizations' existing ERP security and identity & access management controls, but provides granular, fine-grained levels of protection for particularly sensitive financial and PII data fields.

ERP Data Security Use Cases:

- Securing remote users
- Enforcing zero trust and least privilege
- Preventing data exfiltration
- Privileged access management
- Segregation of Duties
- Limiting risk exposure in financial transactions
- Threat detection, response & forensics
- Custom code vulnerability detection

The examples of ERP data security software:

- Appsian Security Platform (http://www.appsian.com) for Oracle E-Business Suite, Oracle PeopleSoft, and SAP ECC/S4HANA

References

1. "ERP (enterprise resource planning)" (https://searcherp.techtarget.com/definition/ERP-enterprise-resource-planning). *SearchERP TechTarget*. May 2017. Retrieved 6 April 2018.
2. "What Is ERP?" (https://www.oracle.com/applications/erp/what-is-erp.html). Retrieved 6 April 2018.
3. Security issues in ERP http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/sap-erp.aspx
4. "Why security should be a priority for an ERP ecosystem" (http://www.information-age.com/security-priority-erp-ecosystem-123468295/). *Information Age*. 31 August 2017. Retrieved 6 April 2018.

5. ERP Security and Segregation of Duties Audit: A Framework for Building an Automated Solution https://csbweb01.uncw.edu/people/ivancevichd/classes/MSA%20516/Extra%20Readings%20
6. "ERP Security Deserves Our Attention Now More Than Ever" (https://www.forbes.com/sites/forbestechcouncil/2017/07/07/erp-security-deserves-our-attention-now-more-than-ever/). *Forbes*. 7 July 2017. Retrieved 6 April 2018.
7. ERP Cybersecurity survey 2017 https://erpscan.com/research/white-papers/erp-cybersecurity-survey-2017/
8. "Survey reveals the damage of fraud attacks against SAP system is estimated at $10m" (https://www.cso.com.au/article/621185/survey-reveals-damage-fraud-attacks-against-sap-system-estimated-10m/). *CSO from IDG*. 27 June 2017. Retrieved 6 April 2018.
9. "Six classic ERP system security problems – and how to avoid them" (https://www.cloudcomputing-news.net/news/2017/may/10/six-classic-erp-system-security-problems-and-how-avoid-them/). *CloudTech*. 10 May 2017. Retrieved 6 April 2018.
10. ERPScan warns about new vulnerabilities of DIAG protocol in SAP (https://archive.today/20130416172959/http://erpscan.ru/press-center/press-release/erpscan-warns-about-new-vulnerabilities-of-diag-protocol-in-sap/)
11. SAP RFC Library Multiple Vulnerabilities http://www.cnet.com/forums/post/7986898c-0a03-43d4-af70-b8427164c8e2
12. Security for Enterprise Resource Planning Systems http://www.utdallas.edu/~bxt043000/Publications/Journal-Papers/DAS/J46_Security_for_Enterprise_Resource_Planning_Systems.pdf
13. Role-Based Access Controls http://csrc.nist.gov/rbac/ferraiolo-kuhn-92.pdf
14. ISACA Glossary Terms http://www.isaca.org/Knowledge-Center/Lists/ISACA%20Glossary%20Terms/DispForm.aspx?ID=1700
15. A risk-based approach to segregation of duties http://www.ey.com/Publication/vwLUAssets/EY_Segregation_of_duties/$FILE/EY_Segregatio
16. R. A. Botha and J. H. P. Eloff Separation of Duties for Access Control Enforcement in Workflow Environments (http://www.research.ibm.com/journal/sj/403/botha.html)
17. Simple Search http://www.bth.se/fou/cuppsats.nsf/all/52d12689b4758c84c12572a600386f1d/$file/mcs-2006-16.pdf Archived (https://web.archive.org/web/20150226025612/http://www.bth.se/fou/cuppsats.nsf/all/52d12689b4758c84c12572a600386f1d/$file/MCS-2006-16.pdf) 2015-02-26 at the Wayback Machine

ERP Security