TẠP CHÍ KHOA HỌC ĐẠI HỌC HẠ LONG
Scientific Journal of Ha Long University
http://uhl.edu.vn/

KHUNG BẢO MẬT ĐỂ ĐIỀU CHỈNH YÊU CẦU NGƯỜI DÙNG CHO NHIỀU CẤP ĐỘ ỨNG DỤNG

Ngô Hải Anh[1*], Lê Anh Tú[2]

[1]Viện Công nghệ thông tin, Viện Hàn lâm Khoa học và Công nghệ Việt Nam
[2]Phòng Đào tạo, Trường Đại học Hạ Long

** Email: ngohaianh@gmail.com*

Ngày nhận bài: 13/11/2023 *Ngày nhận bài sửa sau phản biện: 14/12/2023* *Ngày chấp nhận đăng: 22/12/2023*

TÓM TẮT

Các doanh nghiệp vừa và nhỏ (SME) có thể vận hành các dịch vụ mới nếu họ đáp ứng các tiêu chuẩn đánh giá bảo mật trước khi xây dựng và triển khai dịch vụ mới. Các nhà cung cấp dịch vụ, bao gồm cả các công ty SME, tiến hành đánh giá bảo mật của riêng họ trước khi mở dịch vụ, nhưng thực tế có những hạn chế trong việc đáp ứng các yêu cầu chi tiết của từng bộ phận trong tổ chức và các thay đổi môi trường khác nhau đối với tài sản của công ty như đám mây. Hầu hết các nghiên cứu hiện tại tập trung cải thiện các mục trong danh sách kiểm tra đánh giá bảo mật và xác minh tính hiệu quả, mà có ít nghiên cứu phân tích và tổng hợp các kết quả trường hợp thực tế. Vì vậy, bài viết này phân tích kết quả rà soát bảo mật cho toàn bộ quá trình từ lập kế hoạch đến vận hành hệ thống và dịch vụ đang vận hành, đồng thời đề xuất kế hoạch rà soát, tiến hành phù hợp theo quan điểm của người thực hiện bảo mật.

Từ khóa: *chính sách bảo mật, cấp độ bảo mật, đánh giá bảo mật, khung bảo mật*

SECURITY FRAMEWORK FOR ADAPTING USER REQUIREMENTS FOR MULTIPLE APPLICATION LEVELS

ABSTRACT

Small and medium-sized enterprises (SMEs) were able to operate new services if they met the standards after receiving security reviews before building new services and implementing services. Before launching services, service providers—including small and medium-sized enterprises—conduct their own security reviews. However, due to various environmental changes and practical constraints, it is not always possible to meet all of the specific requirements of every department within the company, including the cloud. Existing studies have been conducted to improve the items of the security review checklist and verify its effectiveness, but there are insufficient studies to analyze and synthesize actual case results. Therefore, this paper analyses the results of the security review for the entire process from planning to operation of the system and service in operation and proposes an appropriate review and proceeding plan from the security practitioner's point of view.

Keywords: *security policy, security framework, security levels, security review*

1. INTRODUCTION

Small and medium-sized enterprises (SMEs) had to undergo security deliberations from related agencies before establishing new electronic financial services and implementing related services. However, as the number of subjects to be deliberated increased due to the revitalization of the fintech business, the security review was changed to proceed with the company itself and maintain the security level on its own. Therefore, each company conducts its security review for new services, and if it is difficult to make its judgment, it contacts the relevant institution (the FSS – Financial Supervisory Service) for answers through a "non-action statement". However, changes in the internal environment as technology advances exist as a value that a company must continuously address and supplement, and there have been practical limitations in meeting various security requirements from the interests of each organization and from the perspective. In this regard, existing studies often changed or added checklists and important items to improve security review, and the effectiveness was reviewed, and the analysis and review of actual service cases were insufficient.

In this paper, we analyse the results of the security review of various systems and services in operation and define the process from initial planning to final service opening according to the work area of each department.

The composition of this paper briefly introduces the existing studies in Section 2, analyses the results of the security review of the actual operation service in Section 3, suggests an appropriate review plan, and concludes in Section 4.

2. SECURITY REVIEW ANALYSIS

2.1. Existing Research

Existing studies on security review can be broadly divided into the addition or improvement of review items, establishment of security level standards, and derivation of security requirements. In the study on the addition or improvement of review items, check items were suggested to solve the problem that it is difficult to conduct a security review realistically due to the lack of manpower and resources within the actual company. The effectiveness was verified through expert tests based on service security standards and OWASP Mobile TOP 10 (Yoo, 2017). In addition, to prevent accidents (personal information leakage) that occur through collaboration between malicious attackers and insiders, the item on preventing insider information leakage was presented as an in-house management plan (Jang-Su et al., 2014, 2015).

In the study on the establishment of security level standards, the CIAPP security level was proposed by adding the authentication (P) and personal information (P) indicators to the CIA-based security level to prepare the security level and standards for electronic financial transactions (Kil-Young & In-Seok, 2018). In particular, for the addition of security level indicators, the importance of authentication and personal information, the necessity of introduction, and actual cases are shown. In the case of personal information, the indicators are divided into economic aspects and privacy protection aspects.

In the study on deriving security requirements, we analysed actual attack vulnerabilities to ensure vehicle cyber security, identified asset threats, derived security goals, and derived security requirements that must be applied to vehicles based on risk assessment (Yun et al., 2019). In order to prevent the leakage of internal information, by having the user explain the security violation caused by an insider's mistake while the security solution is being operated, clearly explain what purpose or task the user violated the security behaviour for within the company and request approval from the superior By doing so, the facts of access to information and the basis for risky behaviour were also prepared (Irdin et al, 2023; Jouini & Rabai, 2019).

Table 1. Security review actual case analysis and summary

No	Main field	Key review items
1	Server configuration	Network: AD server zone separately configured Communication Control: IP and Port Control through Firewall
2	Sales purpose Product information transmission	External communications: outbound restrictions, specific IP restrictions Transmission interval security: encryption, using SFT
3	Other Service Interworking APIs	External communication: Outbound restrictions Transmission interval encryption
4	Data Pipeline Improvement (IDC → Cloud)	Network: Configure a separate security area, An AWS Direct connection, VPC Peering
5	Build and improve business messengers	Communication: Restricting access to internal systems from external devices Terminal: External device (cell phone and mobile device)
6	Consignment of business to an external company	Documentation of consignment work (personal information) Specifying legal liability for Damages
7	Provide member information of affiliated company	Purpose and consent of personal information collection Security when providing personal information: encryption
8	Evidence functions to prevent service cancellation fee deduction	Contract confirmation, consent to personal information: collection of documentation evidence Encrypting Personal Information Files: A Secure Meth
9	Expansion of non-membership purchases	Destruction and separate storage of personal information Consignment of personal information and provision to third parties Encrypt personal information
10	Access to internal system of external Dispatched workers	Secure connection: VPN Enable device security and static IP Accountability tracking: Access record storage and review Apply additional authentication methods (OTP) File security check and personal information retention check Limit usage and server connection time Delete Unnecessary Files

2.2. Security review real case analysis and arrangement

In this section, based on the results of conducting security reviews of systems and services operated by various companies, core review areas are summarized into a total of 10 cases as shown in Table 1. In the field of review, various departments, such as service planning, development, operation, and legal affairs, requested review from the security department for the past 3 years, checked security issues, and selected from about 50 cases that drew results. Duplicate cases due to similarities were excluded. In addition, cases in which results were derived but were not constructed or given up in the middle were excluded.

Major items derived from the review results include network and communication, terminal and system, responsibility tracking, personal information, compliance and contract, data security, and assignment of responsibility in case of violation.

Some of the main review items are as follows.

In the server configuration, it is necessary to review the network, communication control, system security, access control, access history, and access restriction to important information.

In the case of product information transmission, external communication is restricted and encrypted communication is made to maintain security in the transmission section (Chauhan & Stavros, 2023).

In interworking with other services, communication to the outside is restricted, consent from the information subject is required when providing personal information (members), and vulnerabilities of APIs built to prevent direct communication with external systems are checked.

In the data transfer from IDC to AWS, a dedicated line (AWS Direct Connect) and cleaning of important information (personal information) are required to secure the communication section.

In the business messenger development, files were shared only for business purposes, such as prohibiting file downloads from personal mobile devices other than the in-house PC, and external exposure was restricted.

In consignment and provision of personal information, when entrusting a member's (user) personal information to a third party for business purposes, the contract is concluded through a separate document for personal information protection other than the original contract. In the case of transmitting personal information to the outside, the information of the information subject is protected (encryption, etc.).

In the case of evidence for the prevention of fee deduction, if the service cannot be used due to company circumstances after payment, in order to prevent disadvantages to the member (user), the consent of the information subject is obtained and encryption is obtained in the process of collecting the documentary evidence.

In the case of non-member purchases, only members previously used the service, but when the purpose of the service was achieved while expanding to non-members, it was guided to delete the information of non-members or keep them separately in a separate system.

In accessing the internal system of dispatched workers, internal employees must maintain their work through the company system when dispatched overseas, so they use a terminal to which security policy has been applied to access through a secure means of access.

As a result of analysing actual cases of security review, the subject of security review is as shown in Table 2 when developing new services, adding or changing functions to existing services, linking with external services, and personal information There were a total of 4 cases of collecting or changing exposure.

Table 2. Classification of security review targets

No.	Target	Contents
I	New service development	In case of new development other than the existing service
II	Additions and changes to major service functions	When it takes a long time to develop or add functions to an existing service
III	External service linkage	When internal information such as personal information, financial information, and sensitive information is linked with third-party services
IV	Collection, alteration, and disclosure of personal information	When personal information is collected (initially, changed, expanded) or the method of use is changed

Table 3. Main categories and review contents of security review

No.	Target	Contents
A	Network and Communication	External communication, transmission section, zone configuration and separation, connection means, manganese communication
B	Terminals and systems	Vulnerability, vaccine, security setting, access control, additional authentication
C	Accountability	Saving Access and Behaviour Logs
D	Privacy	Collection, Save, use, provision, destruction
E	Compliance and Contracts	Service Contracts, Damages Compensation
F	Data Security	Encryption, access restriction
G	Grant responsibility for violations	Information Protection Pledge, Agreement, Audit

In addition, as shown in Table 3, the main categories that security practitioners should review were derived from a total of 7 categories: network and communication, terminal and system, responsibility tracking, personal information, compliance and contract, data security, and assignment of responsibility in case of violation. The main contents to be reviewed for each category are as follows.

In network and communication (A), it is checked whether there is communication with an external system, communication direction (unidirectional or bidirectional), and security (encrypted communication) in the communication section is guaranteed. In the terminal and system (B), it is checked whether there are any vulnerabilities in the terminal itself or whether the security settings such as the host firewall are appropriate. In accountability tracking (C), it is checked whether the authorized user performed work activities at the permitted location and at the appropriate time.

In the case of personal information (D), according to the personal information life cycle (collection, storage, use, provision, and destruction), the consent of the information subject, storage and use are matched with the initial purpose of collection, and destruction is checked when the purpose is achieved. In compliance and contract (E), it is checked whether the contents of the contract include reviewing whether the business scope is clear before the security check.

In data security (F), it is checked whether appropriate measures are taken to prevent leakage or exposure of confidential and important information within the company.

In case of violation (G), the responsibility of the company's executives and employees or subcontractors' employees in case of breach of contract, negligence, or violation of security regulations is made clear.

In the case of personal information (D), according to the personal information life cycle (collection, storage, use, provision, and destruction), the consent of the information

subject, storage and use are matched with the initial purpose of collection, and destruction is checked when the purpose is achieved.

In compliance and contract (E), it is checked whether the contents of the contract include reviewing whether the business scope is clear before the security check.

In data security (F), it is checked whether appropriate measures are taken to prevent leakage or exposure of confidential and important information within the company.

In case of violation (G), the responsibility of the company's executives and employees or subcontractors' employees in case of breach of contract, negligence, or violation of security regulations is made clear.

Based on the review results, the category is related to work by department and requires cooperation to take supplementary measures (A, B, E, G). It can be divided into repeated cases (C, D, F) and cases in which complementary activities are continuously required in the management aspect (E, G).

Table 4 is the combined result of the above review, and it provides a comprehensive overview of Security Review Actual Case Analysis and Summary in Table 1, Classification of Security Review Targets in Table 2, and Security Review Main Categories and Review Contents in Table 3.

Table 4. Integration of real case result analysis in security review

No.	Classification of Security Review Targets [Table 2]				Main Categories and Review Contents of Security Review [Table 3]						
[Table 1]	I	II	III	IV	A	B	C	D	E	F	G
7		●		●				○			
8		●		●				○	○	○	
9		●		●	○				○	○	
10	●				○	○	○	○			

For example, item 5 in Table 4 is the field of business messenger construction and improvement. As for the security review target, it is a new construction related to personal information and falls into I and IV. Network and Communication (A), Terminals and systems (B), Accountability (C), and Grant responsibility for violations (G) are applicable. From the results of the existing case analysis, it was found that the classification of security review targets involves adding functions to existing services or reviewing personal information-related services, and the main categories of security review are Network and Communication (A) and Privacy (D).

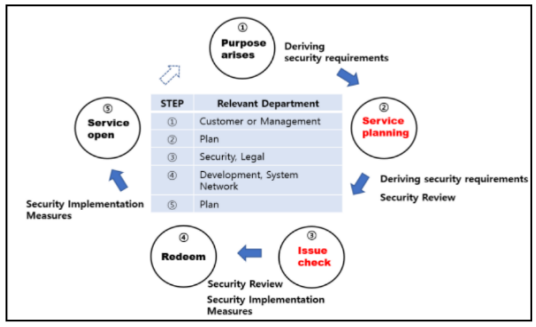

Figure 1. Service and Security Review Process

3. SECURITY REVIEW PLAN

This section suggests a plan for more effective security review from the perspective of security practitioners. First, in order to effectively conduct a security review, it is necessary to clarify the role with the relevant departments in the field and secure a process from the beginning of the initial review to the end of the review.

Figure 1 summarizes the general security review process. First, when the purpose of building or changing a new system for service improvement arises from a customer or management, the service planning department devises a specific plan according to the purpose. . In addition, from the prepared plan, the security department guides the reviewed issues to the relevant departments such as development and system, and based on this, security implementation measures are completed before the service is opened. Finally, make sure it has been removed.

Next, after establishing the security review process, the security practitioner checks the main categories and contents of the security review to see if there is anything to review, and checks the main items of the corresponding category.

For example, the security review of customer service through the linkage of third-party services in Figure 2 is as follows. The security practitioner first checks the direction of communication between the external system and the internal system and restricts unnecessary access. Currently, it prevents outsiders from directly accessing the internal system and prepares supplementary measures such as additional authentication means. When major information such as customer information of another company is stored in the internal system, the data is encrypted, and a security pledge for the fulfilment of responsibilities and obligations is requested. In addition, a system should be established so that personnel participating in development and operation can check when and what actions were performed, and security matters such as blocking malicious codes and blocking harmful sites should be maintained.

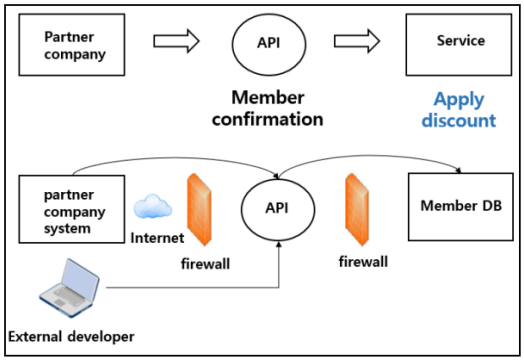

Figure 2. Customer service through interworking with other companies

4. CONCLUSIONS

In this paper, the contents of the review conducted on the systems and services in operation regarding the security review were analysed. As a result of the review based on the entire service process, the security review target often added functions to existing services, and the contents of the security review were prominent in terms of network, communication, and personal information. It is also suggested that security issues should be managed continuously while establishing the entire process from the beginning to the end of the service construction with the relevant departments, and that the security practitioner should respond appropriately to the current organization and situation.

ACKNOWLEDGEMENT

The Vietnam Academy of Science (VAST) supported this research under the project numbered "VAST01.09/22-23".

REFERENCES

Chauhan, M., & Stavros, S. (2023). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. *Network 3, No.3*, 422-450.

Irdin, P., Raffaela, G., Thomas, W., Jubril, G., A., Alexander, R., Michael, F., & Matthias, T. (2023). A systematic review on security and safety of self-adaptive systems. *Journal of Systems and Software, Volume 203*, 2023, 111716.

Jang-Su, P., Yong-Suk, K., & Im-Yeong, L. (2014). A Study on The Management Plan for Prevention of Information Leak by Using Call-out. *Korea Information Processing Society 2014 Spring academic presentation Competition, 2014*, 431-434.

Jang-Su, P., Su-Hyun, K., & Im-Yeong, L. (2015). A Study on a Methodology of the Internal Security Management. *Korea Information Processing Society 2015 Fall Conference, 2015*, 726-729.

Jouini, M. & Rabai, L. B. (2019). A Security Framework for Secure Cloud Computing Environments. In *I. Management Association (Ed.), Cloud Security: Concepts, Methodologies, Tools, and Applications* (pp.249-263). IGI Global.

Kil-Young, J., & In-Seok, K. (2018). Establishing Security Level Standards and Case Studies for Safe Electronic Financial Transactions. *Korea Information Security Association*, 729-741, 2018.

Yoo, H., S. (2017). *A study on developed security check items for assessing mobile financial service security.* Chung-Ang University Graduate School.

Yun, K., S., Samuel, W., Jungho, L., & You, S., L. (2019). Deriving Essential Security Requirements of IVN through Case Analysis. *The Journal of the Korea Institute of Intelligent Transport Systems*, 144-155.