THE ROLE OF THE HUMAN FACTOR IN IMPLEMENTING SECURITY CULTURE POLICIES IN ONLINE CARD PAYMENTS

Pavel Kaminsky[1], Yordanka Anastasova[2], Nikolay Yanev[2]

[1] University of Mining and Geology “St. Ivan Rilski”, 1700 Sofia; 7Security Ltd, 1407 Sofia, E-mail: p.kaminsky@7sec.com
[2] University of Mining and Geology “St. Ivan Rilski”, 1700 Sofia; E-mail: yordanka.anastasova@mgu.bg, nikolay.yanev@mgu.bg

ABSTRACT. Within the past year, card payments have become an integral part of our daily routine. The number of people using card payments on various digital devices grows every day for both business-related and personal needs.
The transition from a traditional to an electronic market in many areas of our lives, and the increased offering of goods and services which were not present at all on the Internet a year ago, have also contributed to the extremely rapid development of this sector., When it comes to online card payments, the safety issue is of high importance for all users; yet, many are still unaware of the possible risks and dangers.
This article examines the ways of developing and implementing corporate policies and user requirements in order to create a lasting culture that guarantees maximum security when using card payments. For the successful implementation of these policies and requirements, the role of the human factor is of particular importance, which is the focus of the article.

Keywords: Online card payments, Security culture, Human factor

РОЛЯТА НА ЧОВЕШКИЯ ФАКТОР ПРИ ПРИЛОЖЕНИЕ ПОЛИТИКИТЕ ЗА ИЗГРАЖДАНЕ КУЛТУРА НА СИГУРНОСТ ПРИ ОНЛАЙН ПЛАЩАНИЯ С КАРТИ

Павел Каминский[1], Йорданка Анастасова[2], Николай Янев[2]

[1] Минно-геоложки университет „Св. Иван Рилски“, 1700 София, 7Секюрити ООД, 1407 София
[2] Минно-геоложки университет „Св. Иван Рилски“, 1700 София, България

РЕЗЮМЕ. През последната година разплащанията с карти станаха неотменна част от ежедневието ни. Броят на потребителите, които ползват плащане с карти чрез различни дигитални устройства, нараства ежедневно както при бизнеса, така и при индивидуални потребители.
За екстремно бързото развитие на този сектор допринесе и прехода от традиционен към електронен пазар в много сфери на живота ни и предлагането на продукти и услуги, които преди година не присъстваха въобще в Интернет пространството. За всички потребители на преден план излезе въпросът за сигурността при онлайн разплащанията с карти, но все още повечето от тях не са запознати с възможните рискове и опасности.
Статията разглежда начините за разработване и прилагане на корпоративни политики и изисквания към потребителите с цел създаване на трайна култура за гарантиране максимална сигурност при използване на онлайн картови плащания. За успешното реализиране на тези политики и изисквания от особено значение е ролята на ролята на човешкия фактор, върху което се акцентира в статията.

Ключови думи: Онлайн плащания с карти, Култура на сигурност, Човешки фактор

Introduction

Each company and every individual strive for maximum security when using card payments. The Internet community, where hacker attacks have become a daily routine, cannot readily find the best solutions to this issue.

To answer all questions concerning the security of card payments is a challenging task, but the most important ones we raise are:

- What is the highest security level that we can achieve?
- Are we adequately protected at the moment and will we continue to be protected in the future?
- What are the best security technologies and have we properly implemented them?

Within the past decades, the major focus has been put on in-depth protection which has limited the damage from hacker attacks. Today, with the advancement of technology and the enforcement of card payment standards, the focus for the implementation of good security is on developing the right corporate policy and the role of the human factor in that.

PCI DSS and its application

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all organisations which store, process, or transmit cardholder data do so in a secure environment. It is based on “five global payment brands - American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. that have agreed to include PCI DSS as a technical requirement for compliance with each of their data security programs” (7Security, n.d.). The standards “are developed specifically to protect payment account data throughout the

payment lifecycle and to enable technology solutions which devalue this data and remove the incentive for criminals to steal it. They include standards for merchants, service providers, and financial institutions on security practices technologies and processes, and standards for developers and vendors for creating secure payment products and solutions.” (PCI Security Standards Council, n.d.)

The standard has six main sections, which include a total of 12 requirements, namely:

Build and maintain a secure network and systems:

1. Install and maintain a firewall configuration to protect cardholder data;
2. Do not use vendor-supplied defaults for system passwords and other security parameters;

Protect the cardholder data:

3. Protect stored cardholder data;
4. Encrypt transmissions of cardholder data across open, public networks;

Develop and maintain a vulnerability management program:

5. Use and regularly update anti-virus software on all systems commonly affected by malware;
6. Develop and maintain secure systems and applications;

Implement strong access control measures:

7. Restrict access to cardholder data by business need-to-know;
8. Assign a unique ID to each person with computer access;
9. Restrict physical access to cardholder data;

Regularly monitor and test networks:

10. Track and monitor all access to network resources and cardholder data;
11. Regularly test security systems and processes;

Maintain an information security policy:

12. Maintain a policy that addresses information security – a cornerstone of every information security program.

The role of the human factor in observing the requirements of PCI DSS

Today, we are increasingly talking about the Business-As-Usual (BAU) concept. The concept requires security to be organised as a continuous process. The only way we can ever feel secure is to incorporate security controls into our daily business operations and make sure that we periodically evaluate that these controls work effectively.

According to a study by the Ponemon Institute (Ponemon Institute 2018) among companies from different countries, the main reasons for compromising the data in terms of their security are (Fig. 1):

- Crime, malicious attacks - 48%;
- Human factor (negligence and incompetence of employees) - 27%;
- Gaps in the design and development of information systems - 25%.

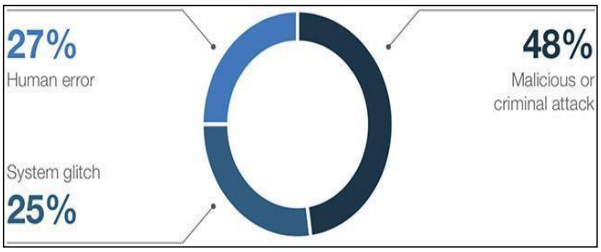

Figure 1: Cost of a Data Breach Study

It is clear from the data that even if clear and rigorous policies, with clear sanctions, are in place, employees are still considered to be vulnerability in terms of information security.

We can install all possible security systems and still be unprotected because our security team is not well-trained and prepared, does not review logs, does not update our systems, and so on. Good communication among the departments is also essential, as “security is about co-operation and communication; if teams are divided up to the point that interaction is discouraged, then bugs, including security-related ones, will fall between the cracks and eventually they will be exploited” (Williams, 2017). Various issues can also be found at the psychological and cultural levels.

The human factor is of high importance when we want to be confident in our security, and, according to PCI DSS, information security professionals are required to periodically perform the following actions:

Daily activities:

- Reviewing of all security-related events;
- Reviewing logs of all system components that store, process or transmit Cardholder Data (CHD) and/or Sensitive Authentication Data (SAD);
- Reviewing logs of all critical components;
- Reviewing logs of all servers and system components that perform security features (such as firewalls, intrusion detection systems/intrusion prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

To ensure that all these measures are effective and to facilitate the actions of the responsible personnel, it is necessary to install different mechanisms for detecting changes (e.g. file integrity monitoring tools). This installment is imperative so staff is promptly warned of unauthorised actions (including changes, additions, and deletions) of critical system files, configuration files, or content files.

It is recommended that at least **once a week** the software be configured to perform critical file comparisons.

At least on a **quarterly** basis**,** the responsible personnel are expected to take the following actions:

* Execution of data retention procedures for the purpose of minimum storage of cardholder data. This implies a secure deletion of the stored data that exceeds a defined retention period;
* Implementation of processes that test the availability of wireless access points (802.11), detect and identify all authorised and unauthorised wireless access points;
* Running of internal and external network vulnerability scans and after any significant change in networks;
* Performing reviews to confirm that the personnel follow security policies and operational procedures.

Every **six months**, employees need to:

- Review the firewall and router rule sets;
- Perform penetration testing on segmentation controls if segmentation is used for scope reduction.

At least **once a year**, it is necessary to:

- Train developers in secure coding;
- Conduct general security awareness training for all personnel;
- Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures;
- Carry out a risk assessment and treatment;
- Review and update the security policy;
- Assess public-facing web applications for vulnerabilities;
- Maintain inventory logs of all media and conduct media inventories;
- Review the security of stored media location;
- Perform external, internal, and segmentation penetration testing;
- Review and test the Incident Response Plan;
- Maintain a program to monitor service providers' PCI DSS compliance status.

The periodic activities that each company determines **depending on the degree of risk** are**:**

- Review logs of all other system components based on the organisation's policies and risk management strategy as determined by the organisation's annual risk assessment;
- For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software;
- Periodically inspect device surfaces to detect tampering or substitution.

Examples of how to incorporate PCI DSS into BAU activities include:

- Monitoring of security controls (firewalls, IDS/IPS, File Integrity Monitoring (FIM), Anti-Virus, Access controls)
- Ensuring that failures in security controls be detected and responded to:
  - Restoring the security control;
  - Identifying the cause of failure;
  - Identifying and addressing any security issues that arose during the failure;
  - Implementing mitigation to prevent reoccurring;
  - Resuming monitoring of the security control.
- Reviewing changes to the environment:
  - Addition of new systems, changes in the system or network configurations, or organisational structure;
  - Potential impact to PCI DSS scope;
  - Requirement applicable to new scope;
  - Updating PCI DSS scope and implementing security controls as appropriate.
- Implementing periodic reviews to verify the following:
  - PCI DSS requirements continue to be in place (e.g., configuration standards have been applied, patches and AV are up to date, audit logs are reviewed, and so on);
    - Personnel follow secure processes;
  - All facilities and locations are covered;
    - Appropriate evidence is maintained (audit logs, vulnerability scan reports, firewall reviews, etc.)

In addition to the above practices, consideration may also be given to implementing segregation of duties related to security functions in order to separate security and/or audit functions from operational functions. In environments where one individual performs multiple roles (for example, administration and security operations), duties may be assigned such that no single individual has end-to-end control of a process without an independent checkpoint. For example, responsibility for configuration and responsibility for approving changes could be assigned to separate individuals.

Conclusion

All organisations and individuals that use online card payments have issues with security control. Integrating PCI DSS into BAU operations provides a mechanism that identifies those issues before they become damaging, and fixes them before too many controls fail and result in a breach. This is what makes the human factor so essential - if the breach analysis reports are often checked, the problems caused by non-functioning control mechanisms or security malfunctions can be prevented to a large extent. In fact, a quick reaction from the personnel is more vital to prevent breach and losses than we might imagine, as “the average time for companies to detect any data breach is 197 days” (Ponemon Institute, 2018), resulting in more time to contain the breach and, in turn, leading to large material damages, with an average total cost of a data breach being $3.86 million (Ponemon Institute 2018).

Nowadays, the industry offers different software and hardware security solutions in all possible forms, which suggests we can obtain the required ones to guarantee security. But what happens after their installation?

Hackers expect to see such technology in the environments they target. What they don't expect is to find them updated, or to get caught by staff during security log reviews, or to find that the vulnerabilities are mitigated during scanning and penetration testing sessions. As a 2018 research concludes, “‘no organisation affected by a payment card data breach was in full compliance with the PCI DSS requirements. This is a testament to the need for compliance to be taken more seriously” (Damour, 2019).

It is necessary to constantly monitor and update these solutions in which the human factor plays a major role. To guarantee the security of the card payment environments, it is important to constantly invest in the vulnerability mitigation of the human factor, which will make us confident that we have secured the payment processes and the cardholders to the possible maximum.

References

7Security. (n.d.). 2021. *PCI DSS Compliance and Certification - 7Security*. 7Security. Retrieved April 27, from https://www.7sec.com/compliance/pci-dss/

Damour, C. 2019, June 21. What is PCI DSS? *Payments Journal.* https://www.paymentsjournal.com/what-is-pci-dss/

Kaminsky, P. 2019. *PCI DSS: Building a Culture of Security*, ISACA Day, Sofia.

PCI Security Standards Council. (n.d.). *Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards*. PCI Security Standards. Retrieved April 27, 2021, from https://www.pcisecuritystandards.org/pci_security/standards_overview

Ponemon Institute LLC. (2018, July). *2018 Cost of a Data Breach Study: Global Overview.* https://www.intlxsolutions.com/hubfs/2018_Global_Cost_of_a_Data_Breach_Report.pdf.

Williams, G. (2017, November 1). *Looking at the human factors in security breaches*. StarWind. https://www.starwindsoftware.com/blog/looking-at-the-human-factors-in-security-breaches