DOI: https://doi.org/10.33197/justinfo.v2i1.1793 ISSN: 3031-3449

Data Breach of General Elections Commission: Causes and Prevention Efforts

[1]Muhamad Rizki, [2]Surgana

[1]Information Systems, Faculty of Engineering, Widyatama University, Bandung, Indonesia, rizki.1823@widyatama.ac.id

[2]Information Systems, Faculty of Engineering, Widyatama University, Bandung, Indonesia, surgana@widyatama.ac.id

ABSTRACT

The voter data breach of the General Elections Commission (KPU) on November 27, 2023, is a highly concerning event with potential negative impacts on society, including the misuse of voter data for political, criminal, or even terrorist purposes. This paper identifies the main factors causing the KPU data breach, including the complexity of the information system, software vulnerabilities, and user awareness issues. The complexity of the KPU voter data information system, which is integrated with various other systems, makes it vulnerable to cyber threats such as malware, phishing, and denial-of-service attacks. To mitigate this risk, regular security audits by independent information security experts are essential. Additionally, addressing software vulnerabilities requires timely software updates to fix identified security weaknesses. User awareness, particularly among KPU officials, is another critical factor. Enhancing user awareness through comprehensive training on information security principles, types of cyber attacks, and safe system usage practices is crucial. To prevent future data breaches, a holistic approach involving regular security audits, software updates, and strong user awareness programs is necessary to maintain the integrity of the election information system.

Keywords: Data Breach, Information Security, Privacy Violation, Data Misuse, General Election.

Corresponding Author:

Muhamad Rizki
Information Systems, Faculty of Engineering, Widyatama University
Bandung, Indonesia
rizki.1823@widyatama.ac.id

INTRODUCTION

The internet has become a necessity in modern society, encompassing various aspects such as communication, business, education, and entertainment. However, the rapid development of information technology and the internet also brings risks to information security, with serious threats such as cyber attacks, data misuse, and privacy violations.

In November 2023, the General Elections Commission (KPU) experienced a shocking data breach. Strongly suspected to be the result of a cyber attack, the breach included sensitive information such as National Identification Numbers (NIK), names, addresses, and voter phone numbers. The impact of this breach is significant, posing risks of data misuse by irresponsible parties, such as fraud, identity theft, and cyber attacks.

Additionally, psychological and social impacts also arise, with voter privacy being seriously compromised. Voters who fall victim to data breaches may experience emotional distress and social difficulties due to the insecurity of their personal information.

Furthermore, disruptions to the election process are also a risk that must be addressed. Voters whose personal data is leaked may face difficulties in exercising their voting rights, threatening the integrity and credibility of the democratic process.

The KPU data breach reflects the urgency of protecting personal information in this digital era. Preventive measures and enhanced cybersecurity are essential to protect the interests of society and the integrity of democratic institutions.

LITERATURE REVIEW

Information security has become a central issue in the current internet era, where technology continues to develop rapidly. Data breaches can result in serious risks, such as the misuse of personal information or political interests that harm society. One of the factors causing data breaches is the complexity of information systems. Modern information systems tend to become increasingly complex and integrated, making them vulnerable to cyber attacks that can be exploited by irresponsible parties.

Software vulnerabilities are also a crucial aspect of information security. Poorly protected software can be exploited by attackers to launch cyber attacks. User awareness about information security is also an important factor. Many internet users are not fully aware of the urgency of information security, leaving them vulnerable to cyber attacks such as phishing or malware.

To prevent data breaches, comprehensive efforts are needed. The implementation of security technologies, such as firewalls, antivirus, and antispam, is a proactive step in protecting information systems. Additionally, increasing user awareness through socialization and education about information security is a crucial step. Collaboration among stakeholders, including the government, private sector, and society, is also needed through law enforcement, the development of information security standards, and socialization to create a safe and trustworthy digital environment.

RESEARCH METHODS

This study adopts qualitative research methods as an approach to gain an in-depth understanding of the KPU voter data breach and the factors behind it. Qualitative research methods are considered appropriate because they provide space for researchers to explore the complexity of phenomena and the contexts involved. The inductive approach in this method allows researchers to develop theories or findings based on the data collected.

Research data were obtained through two main sources, namely literature studies and interviews with information security experts. Through literature reviews, researchers gathered relevant information to understand the landscape of information security, system vulnerabilities, and best practices in preventing data breaches. Interviews with information security experts became a key element in exploring the views and insights directly from experts who have experience and in-depth understanding of information security issues.

By using qualitative research methods, this study does not only focus on numbers or statistics but also considers context, subjective views, and interactions between factors. This approach is expected to produce a deeper and more contextual understanding of the factors causing the KPU voter data breach and provide a basis for developing more effective prevention recommendations.

RESULTS AND DISCUSSION

Based on the literature review and interviews, it can be concluded that the KPU data breach is influenced by several critical factors. First, the complexity of the KPU voter data information system becomes a potential gap, considering that the system is integrated with various other information systems. This diversity makes the system more vulnerable to cyber attacks, such as malware, phishing, and denial-of-service.

The second factor is the vulnerability of the software used in the information system. This vulnerability can be exploited by irresponsible parties to launch cyber attacks. For example, design, coding, or software configuration errors can become entry points for attackers.

Additionally, the lack of user awareness, especially KPU officials, about information security is another contributing factor. The lack of understanding of security risks makes users more vulnerable to cyber attacks, such as credential loss or phishing traps.

To prevent future data breaches, several efforts need to be made. First, regular security audits on the KPU voter data information system need to be conducted to identify and address potential security vulnerabilities. The second effort is to increase user awareness through training and education. This training includes understanding security risks, preventive actions, and responses to security incidents.

Finally, the protection of the network infrastructure used to access the information system needs to be strengthened with security methods such as firewalls and intrusion detection systems. This approach will form an additional layer of defense to prevent cyber attacks that can harm the integrity of the KPU voter data.

CONCLUSION

In conclusion, the data breach at the General Elections Commission (KPU) on November 27, 2023, shows serious vulnerabilities in information security. The potentially harmful impacts, particularly related to the misuse of voter data for political, criminal, and even terrorist purposes, underscore the urgency of identifying causes and taking appropriate preventive measures.

Factors such as the complexity of integrated information systems, software vulnerabilities, and lack of user awareness, especially KPU officials, are key points that need to be addressed. The complexity of information systems creates various gaps that can be exploited by cyber attacks, while software vulnerabilities reinforce this risk. The lack of user awareness adds a layer of vulnerability, given their significant role in managing the system.

Proposed preventive efforts, such as regular security audits, increasing user awareness through training, and strengthening network infrastructure, are key to mitigating the risk of future data breaches. These steps need to be implemented earnestly and continuously. Awareness of information security must be instilled in the organizational culture, and relevant parties need to work together to create a robust defense layer against evolving cyber threats.

This conclusion highlights the importance of holistic and collaborative preventive actions in maintaining data security, a crucial step to ensure the integrity of elections and the protection of citizens' personal data.

REFERENCES

[1] A. Maulana, "Regulation of the Use of Personal Data for the Implementation of Democracy in General Elections in Indonesia," Thesis, Sriwijaya University, 2023.

[2] M. Fauzan, "Analysis of Factors Causing KPU Data Breach," ICT Journal, University of Indonesia, 2023.

[3] M. Putri, "Minimizing the Risk of Voter Data Breach in Indonesia," Tempo, Nov. 27, 2023.

[4] M. Iqbal, "Efforts to Prevent Voter Data Breach," CNN Indonesia, Nov. 27, 2023.

[5] P. Persada, "KPU Admits Voter Data Breach, This is What Cybersecurity Experts Say," CNBC Indonesia, Nov. 27, 2023.

[6] A. Tanujaya, "KPU Voter Data Breach, Experts: Security Audit Needed," detikINET, Nov. 27, 2023.

[7] H. Asy'ari, "KPU Voter Data Breach, KPU: We Have Conducted Security Audits," CNN

Indonesia, Nov. 27, 2023.

[8] A. Kharis, "KPU Voter Data Breach, DPR Requests KPU to Tighten Security," Kompas, Nov. 27, 2023.

[9] S. Susanto, "KPU Voter Data Breach, KPAI: Don't Hand Over Data to Third Parties," CNN Indonesia, Nov. 27, 2023.

[10] D. Lestari, "KPU Voter Data Breach, There Needs to be Data Security Regulations," Bisnis, Nov. 27, 2023.