International Journal Of Humanities Education And Social Sciences ***(IJHESS)*** *E-ISSN:* **2808-1765**
Volume 2, Number 6, June 2023, *Page. 2070 - 2077*
Email : editorijhess@gmail.com

Security Standard Recommendation of Teleworking in Government

Susilo Gumilang [1)], Rudy Sutanto [2)], Ahmad G. Dohamid [3)]*
[1,2,3)] Asymmetric Warfare Program, Faculty of Defense Strategy, Republic of Indonesia Defense University

***Corresponding Author
Email: gumigumigumi3@gmail.com

Abstract
Information technology and the internet are important factors in human life especially in works. Almost 70% of human works uses information technolgy, but since the restrictions on activities due to COVID-19 pandemic have caused people to be able to do work in office as before. Some companies and government sectors that still have to carry out their business processes require their employees to work remotely (teleworking) from home by utilizing the internet network. However, teleworking can pose a risk to the security of work data and personel data so there needs to be carrid out with minimal risk. This study uses a qualitative method with a literature approach to analyze the risks that arise from teleworking, classification of data that should not be disseminated, analyze the internet network, data protection and apply the theory of cyber security, network security, authentication and non-repudiation. Then apply these theories in a framework to develop security standards in teleworking. The final result of this research is a recommendation of regulatory standards for every government in conductiong teleworking.

Keywords: Data Security, Teleworking, Government

INTRODUCTION

The COVID-19 pandemic has caused various changes in human life due to restrictions on public activities such as school and work. Everyone is limited in going to work so it is necessary to do work remotely (remote working / teleworking) from home. According to Mouratidis and Papagiannakis in their research, they explained that there was a very significant increase in internet and social media use during the pandemic compared to before the pandemic took place. From this study, what illustrates the highest change is the use of teleconference from a value of 2.14 to 2.87, which is 34.11% and the second is the implementation of remote work (teleworking) with a pre-pandemic value of 2.68 to 3.50 with an increase in by 30.60% from before the pandemic took place (Mouratidis & Papagiannakis, 2021). Although now there are many companies and agencies that have allowed their employees to work in offices, there has not been a firm decision regarding the end of the pandemic and teleworking is increasingly becoming the choice of companies and agencies because it can save the cost of procuring a workplace and all the facilities included in it. The increasing use of online services in performance certainly provides new risks that arise, especially with regard to data security, network security and the threat of cyber attacks in the form of malware or cyber attacks in other forms. Based on the BSSN cyber security monitoring report, Indonesia experienced around 12 million cyber attacks in 2018, 98 million attacks in 2019, 316 million attacks in 2020 and 266 million in 2021. The highest increase occurred in 2020 during the COVID-19 pandemic takes place when the entire sector is "forced" to be implemented online. Cyber attacks that occurred in Indonesia varied, in 2018 dominated by malware attacks, while 2019 was dominated by Attempted Information Leak, 2020 was dominated by Trojan attacks and 2021 was dominated by Botnet attacks (BSSN, 2021).

Data leaks (Data Breaching) are one of the most frequent cyber attacks in Indonesia and are caused by various factors such as system security, network and the human factor itself. Given the impact of the pandemic and the rise in teleworking, there is an urgent need for

security standards for every agency, especially government agencies, to prevent data leaks and other security risks. It is crucial to implement proper data security measures, such as encryption, access control, and backup and recovery, as outlined by Denning (1982). Additionally, information security governance as defined by NIST-SP number 800-100 is essential to ensure that strategic information security aligns with and supports business processes and objectives, while complying with all applicable regulations (Bowen, Hash, & Wilson, 2006). By implementing these measures and standards, agencies can minimize the risks associated with teleworking and ensure that their sensitive information remains secure.

RESEARCH METHODS

The research method used in this study is a qualitative descriptive approach. This approach aims to understand phenomena holistically and describe them using various scientific methods. The study aims to describe the conditions of teleworking security risks associated with various security rules and standards for the implementation of teleworking.
The following are the steps involved in the research method:

a. Research question: The research question is formulated to identify the research problem and guide the study. In this case, the research question is "What are the teleworking security risks associated with various security rules and standards for the implementation of teleworking?"
b. Data collection: The data collection method is selected based on the research question and the nature of the study. Qualitative research often uses methods such as interviews, observation, and document analysis. In this study, data will be collected through interviews with teleworkers and teleworking managers, observation of teleworking practices, and analysis of teleworking policies and standards.
c. Data analysis: Data analysis is used to identify patterns, themes, and relationships in the data collected. In qualitative research, data analysis is often done through coding and categorizing data. In this study, the data will be analyzed using thematic analysis, which involves identifying patterns and themes in the data.
d. Validity and reliability: Validity and reliability are important considerations in qualitative research. Validity refers to the accuracy and credibility of the research findings, while reliability refers to the consistency and stability of the research findings. In this study, measures will be taken to ensure the validity and reliability of the findings, such as triangulation of data sources, member checking, and peer review.
e. Findings: The findings of the study will be presented in a descriptive and holistic manner, using various scientific methods to describe the teleworking security risks associated with various security rules and standards for the implementation of teleworking.
f. Conclusion: The conclusion will summarize the findings of the study, provide answers to the research question, and discuss the implications of the findings for teleworking practices and policies.

RESULT AND DISCUSSION

Government Agencies

Government Agencies according to Law Number 20 of 197 concerning Non-Tax State Revenue Article 1 Number 4 are departments and non-departmental institutions. According to Law Number 36 of 1999 concerning Telecommunications Article 12 Number 3, Government Agencies are agencies that directly control, own, and or use land and or buildings. Government Agencies according to Law Number 4 of 2011 concerning Geospatial Information Article 1 Number 18 are ministries and non-ministerial government agencies. Based on the Law of the Republic of Indonesia Number 5 of 2014 concerning State Civil Apparatus Article 1 Number 15 Government Agencies are central agencies and regional agencies.

Government agencies referred to in this study are agencies in the form of ministries and non-ministerial, both central and regional which directly control, own and or use land and or buildings in carrying out their functions for state administration. Government agencies certainly have a variety of information that has various classifications, public, limited or excluded. According to the Regulation of the National Crypto Agency Number 10 of 2012 concerning Guidelines for the Management and Protection of Government-owned classified information, it is explained that classified information belonging to the government is a state asset that needs to be managed specifically as an effort to prevent leakage caused by own negligence or due to threats from other parties who do not have authority to utilize this information which has an impact on the survival of the state, the integrity and tranquility of the community (BSSN, 2012).

Data Security

Data Security according to Denning (1982) is the science of methods of protecting computer data and communication systems that apply various types of controls such as cryptography, access control, information flow paths and inference control, including backup and recovery (Denning, 1982). A collection of data contained in an agency can be classified as information, of course, it can also be in the form of classification information in the form of electronic data. This information certainly has a classification and can be in the form of excluded information, so the agency needs to manage this information with special governance. In the context of government agencies, a collection of data can be classified as information and may take the form of electronic data or classified information. This information has different levels of classification and may include excluded information that requires special governance to manage it effectively. This means that government agencies need to implement robust information security governance practices to ensure that their information is protected from internal and external threats.

NIST-SP number 800-100 defines information security governance as the process of building, maintaining and supporting management structures and processes to provide assurance that strategic information security is still aligned with and supports business processes, objectives and in line with applicable regulations by complying with all policies. and internal control as well as assigning responsibilities in order to manage risk (Bowen, Hash, & Wilson, 2006). The COVID-19 pandemic has brought significant changes in the way people work, resulting in an increase in teleworking among government agencies. This shift to remote work has created new challenges, including the need to implement safe teleworking practices that protect against various threats of cyber-attacks that may occur. Furthermore, vulnerabilities due to negligence on the part of employees or the agency itself may also put the teleworking

environment at risk. Therefore, it is crucial for government agencies to implement strong information security governance practices to mitigate these risks and ensure safe teleworking.

Teleworking Risk

NIST SP 800-46 Rev. 2 explains that the risks of teleworking include:

1. Lack of Physical Security Controls . Agencies cannot easily control the use of each employee's device at work.
2. Unsecured Networks , agencies must see that the internet network used by their employees during teleworking is not safe so they must establish appropriate policies.
3. Infected Devices on Internal Networks , agencies cannot ensure that the devices used by their employees have been infected with malware or not and are then used to access government agencies' internal networks. If the device used by the employee is infected, it can spread the malware through the office's internal network.
4. External Access to Internal Resources , the ease of remote access will create new threats from unverified devices or networks and increase the possibility that these devices have been infiltrated by malware.

Teleworking makes employees highly vulnerable to a variety of challenges and threats that can compromise critical data and/or compromise their own identities. Some of the possible threats include eavesdropping, malware attacks, data theft, system failures and unauthorized access to personal data (Deloitte, 2020).

During the COVID-19 pandemic, the number of Distributed Denial of Services (DDoS) attacks increased. Criminals also often use various domains and websites to spread malware, spyware or Trojans, sending spam e-mails using the keyword "coronavirus". The COVID-19 pandemic is an opportunity for criminals to take advantage of the situation to send malware, spyware or Trojans via e-mail that attacks employee weaknesses and security system vulnerabilities by using the coronavirus outbreak as bait (Crossland, Ertan, Michaelides, & Pappenheim, 2021).

Teleworking vulnerabilities do not only come from physical attacks but also psychologically have an impact on increasing cybercrimes. Government employees who are unfamiliar with teleworking and are under pressure due to the COVID-19 pandemic are easy targets for phishing and social engineering attacks. In the weeks since the COVID-19 pandemic began, a high increase in cyber attacks has triggered a rapid response by exploiting sensitive information about COVID-19, for example clicking on a malicious link, downloading an attachment or an application about COVID-19 that has been infected with malware (Adelmann & Gaidosch, 2020).

Based on the results of the Honeynet report from BSSN in 2020, TrojanDownloader:Win32/Small malware attacks were the most common attacks in 2020 (BSSN, 2020).

Teleworking Framework

NIST SP 800-46 Revision 2 has provided remote access security guidelines which can be divided into 4 (four) main parts, namely:

1. The method used in teleworking .

   In securing data and information in government, there are various methods of securing teleworking, namely:

   a) VPN

Virtual Private Network is a path that provides protection of the client (employee) relationship with the server being accessed. VPN provides authentication and access control services for employees when doing remote access.

b) Application Portal
This application portal connects the client with the server using an application that has the same authentication and access control functions as a VPN, except that the data accessed is on the portal server.

2. Security on Remote Access
   a) Remote access server security.
   Remote access servers must be fully patched operated using security settings from government agencies and managed by authorized and trustworthy personnel.
   b) Placement of remote access server.
   In placing a server, government agencies must consider server capabilities, traffic checks
   c) Authentication, authorization and remote access control access.
      1) Authentication
      Many kinds of authentication can be passwords, digital certificates, tokens, biometrics. Implement two-factor authentication, as well as re-authenticate if during a specified periodic time there is no remote working activity.
      2) Authorization
      Agencies check the equipment used by their employees, this is often referred to as health, suitability, screening or assessment check.
      3) Access control
      Agencies are required to protect data content by applying cryptography when teleworking.
   d) Remote access software.
   The software used by employees in teleworking must meet security standards that can be regulated by the agency.
3. Employee device security
   a) Security on PC
   Devices used by employees must activate the firewall and activate security updates for applications and operating systems on a regular basis.
   b) Security on mobile devices.
   Implementing Mobile Device Management (MDM) on every employee's mobile device used for teleworking.
   c) Data protection on employee devices.
   Sensitive/classified data stored in employees during teleworking must be encrypted using a secure cryptographic key determined by the agency. Using a Virtual Machine (VM) in accessing data by teleworking, as well as implementing back-up data during teleworking.
4. Remote access cycle
   Government agencies are required to carry out security checks for teleworking systems that will be implemented.

a) Initiation, in the form of security requirements needed for teleworking;
b) Development, containing the necessary technical characteristics such as authentication methods, cryptography, firewalls and secure access control as various threats develop;
c) Implementation, consisting of combining various security control configurations such as event logging, network management and integrated server authentication;
d) Operations and maintenance, security systems carried out by agencies in the form of operations, log reviews, attack detection, incident response and recovery, and must be documented in the form of configuration management policies;
e) Deactivation, in the form of turning off or deactivating the teleworking system that is run if the system is not being used again, or replacing it with a new, more up-to-date system.

The IMF provides several recommendations in dealing with risks in the implementation of teleworking as follows:

1. Government agencies must implement the use of teleworking in accordance with internationally applicable remote working security standards;
2. Teleworking services can only be accessed if necessary;
3. Cloud utilization must pass a thorough risk test;
4. Teleconferencing must be used using a platform authorized by a government agency;
5. There is a cyber security awareness campaign for all employees;
6. Implementation of strong control over the security configuration of both end-user and server during teleworking to prevent harmful use;
7. Agencies must implement additional security controls on critical functions that previously could not be performed remotely;

There must be strict supervision that teleworking increases cybersecurity risks.

CONCLUSION

In implementing teleworking, government agencies are required to implement several standards that must be met to protect the security of government data and information which are classified as follows:

1. Planning a teleworking security policy based on the assumption that an external environment has a high threat risk;
2. Implement security controls during teleworking in the form of protection from eavesdropping, interception and modification;
3. Making assumptions that employee devices have a high risk of being infiltrated by malware;
4. Develop teleworking security policies, remote access and security requirements on personal mobile devices;
5. Making teleworking risk mitigation policies regarding what is allowed and not as long as employees teleworking with the devices used.
6. Create security policies and implement effective security on remote access servers;
7. Determine the placement of remote access servers with effective security standards determined by the agency;
8. Provide security for each employee's teleworking device that can be controlled by the

agency and update security controls regularly;

9. Conduct periodic checks on all devices used by employees during teleworking, including PCs, tablets and smartphones. And does not provide teleworking access to unknown devices.

There are some key security standards that should be followed when implementing teleworking in government:

a. Strong Passwords: Government agencies should require employees to create strong passwords and regularly change them. Passwords should be a combination of letters, numbers, and symbols, and should be at least 12 characters long.
b. Multi-Factor Authentication: Multi-factor authentication should be used to provide an additional layer of security beyond passwords. This can include using a smart card, token, or biometric identifier in addition to a password.
c. Encryption: All sensitive data should be encrypted both in transit and at rest. This helps to protect the data from unauthorized access, interception, or theft.
d. Virtual Private Network (VPN): A VPN should be used to provide a secure connection between the employee's computer and the government's network. This helps to protect against unauthorized access and eavesdropping.
e. Anti-Virus and Firewall: All computers used for teleworking should have up-to-date anti-virus software and firewall protection to prevent malware and other malicious attacks.
f. Regular Updates and Patches: All software and operating systems used for teleworking should be kept up-to-date with the latest security updates and patches.
g. Data Backup and Recovery: Regular data backups should be performed to ensure that important data is not lost in the event of a system failure, data breach, or other disaster.
h. Training and Awareness: Government employees should receive regular training on teleworking security best practices, as well as be made aware of potential security threats and how to respond to them

REFERENCES

Adelmann, F., & Gaidosch, T. (2020). *Cybersecurity of Remote Work During the Pandemic*. Monetary and Capital Markets, International Meonetary Fund.Bodsberg, L., Grøtan, T. O., Jaatun, M. G., & Wærø, I. (2021). HSE and Cyber Security in Remote Work. *Cyber Science 2021*.

Bowen, P., Hash, J., & Wilson, M. (2006). *Information Security Handbook: A Guide for Managers, Recommendations of the National Institute of Standards and Technology* . Gaithersburg: National Institute of Standards and Technology.

BSSN. (2020). *LAPORAN TAHUNAN 2020 HONEYNET PROJECT BSSN - IHP*. Jakarta: Badan Siber dan Sandi Negara.

BSSN. (2012). *Peraturan Kepala Lembaga Sandi Negara Nomor 10 Tahun 2012 Tentang Pedoman Pengelolaan dan Perlindungan Informasi Berklasifikasi Milik Pemerintah.* Jakarta: Badan Siber dan Sandi Negara.

Crossland, G., Ertan, A., Michaelides, N., & Pappenheim, B. (2021). *Remote Working and Cyber Security Literature Review.* London: Research Institute for Sociotechnical Cyber Security.

Deloitte. (2020). *Organisational and personnel vigilance Combating risks of remote working amidst the COVID-19 crisis.* Deloitte.

Denning, D. E. (1982). *Cryptography and Data Security.* Monterey: Addison-Wesley Publishing Company.

INSA's Insider Threat Committee. (2021). *Managing Insider Threats in a Remote Work Environment: Lessons from the Pandemic.* Intelligence and National Security Alliance.

Mouratidis, K., & Papagiannakis, A. (2021). COVID-19, internet, and mobility: The rise of telework, telehealth, e-learning, and e-shopping. *Sustainable Cities and Society 74*, 1-11.

Nurse, J. R., Williams, N., Collins, E., Panteli, N., Blythe, J., & Koppelman, B. (2021). Remote Working Pre- and Post-COVID-19 : An Analysis of New Threats and Risks to Security and Privacy. *Communications in Comuter and Information Science, vol 1421*.

Ponemon Institute. (2020). *Cybersecurity in the Remote Work : A Global Risk Report.* Keeper.

Puspitarini, A., Purnama, P. A., & dewi, I. R. (2021). Fraud risk and Trust on the Intention to buy of e-commerce. *Journal of Contemporary Accounting Volume 3 Issue 1*, 45-52.

Souppaya, M., & Scarfone, K. (2016). *User's Guide to Telework and Bring Your Own Device (BYOD) Security.* Gaithersburg: National Institute of Standards and Technology.

SECURE, C. (2020). *Future of Secure Remote Work Report.* CISCO .

Yazdanifard, R., Edres, N. A.-H., & Seyedi, A. P. (2011). Security and Privacy Issues as a Potential Risk for Further Ecommerce Development. *2011 International conference on Information Communication and Management*, 23-27