JICN: Jurnal Intelek dan Cendikiawan Nusantara
https://jicnusantara.com/index.php/jicn
Vol : 1 No: 3, Juni - Juli 2024
E-ISSN : 3046-4560

CRISIS MANAGEMENT AND INCIDENT RESPONSE: A NATIONAL DATA CENTER CASE STUDY

MANAJEMEN KRISIS DAN RESPONS INSIDEN: STUDI KASUS PUSAT DATA NASIONAL

Said Ma'ruf

Universitas Paramadina Indonesia

Email: said.maruf@students.paramadina.ac.id

Article Info

Article history :
Received : 02-07-2024
Revised : 04-07-2024
Accepted :06-07-2024
Published:10-07-2024

Abstract

This research aims to analyze crisis management and incident response related to the collapse of the National Data Center (PDN). Through these case studies, the research explores the steps taken by authorities to address the crisis, identifies the challenges faced, and evaluates the effectiveness of the incident response. Data was collected from secondary sources, including official reports, news articles, and interviews with cybersecurity experts. The results showed that despite rapid efforts to contain the incident, there were several weaknesses in preparedness and coordination that needed to be corrected to reduce future risks.

Keywords: ***National Data Center (PDN), Cyber Security, Crisis Management, Incident Response***

INTRODUCTION

The National Data Center (PDN) is a data center facility for the purposes of placing, storing and processing data, as well as data recovery which will later be used for data sharing by central agencies and regional governments, and is interconnected in Indonesia (Wikipedia). Data Center (Data Center) is a building facility used to place computer systems and related components, such as telecommunications systems and data storage. IT operations are very crucial, so this facility has backup power, redundant data communication connections, environmental controls (eg air conditioning, ventilation, fire prevention), and various data security devices. Large data center facilities operate on an industrial scale using as much electricity as a small city (Wikipedia).

The National Data Center (PDN) is a data center (server) where state data includes data owned by Ministries and Institutions. The National Data Center (PDN) is a very important state data center whose security and confidentiality must be maintained at all times. At this time the National Data Center (PDN) became the attention of the public, IT figures and the DPR when the National Data Center was attacked/hacked by hackers making the data center inaccessible.

The cyber attack that occurred since Thursday (20/6/2024) paralyzed a number of services,

including immigration services. Not only that, the attack also resulted in the data of 282 government agencies stored in PDN being locked and held hostage by hackers (Kompas.com, 26 June 2024). The National Data Center (PDN) breach incident highlighted the vulnerability of the Indonesian government's information technology infrastructure to cyber attacks. The National Data Center (PDN) is the backbone of various government digital services, so data leaks can have a serious impact on national security and public trust. Effective crisis management and incident response are critical to minimizing the impact of these incidents.

Based on the background above, this research aims to analyze crisis management and incident response related to the collapse of the National Data Center (PDN). The problem formulation is as follows: 1. How is crisis management implemented in dealing with the National Data Center collapse incident? 2. What incident response steps are taken by the authorities? 3. How effective was the incident response in mitigating the impact of the crisis?

The research objectives are: 1. Analyze crisis management in the context of the National Data Center breach incident. 2. Identify incident response steps taken. 3. Evaluate the effectiveness of incident response in overcoming the crisis. It is hoped that this research will provide insight into best practices in crisis management and incident response, as well as provide recommendations for improving preparedness for similar incidents in the future.

LITERATURE REVIEW

Crisis Management Theory

Crisis management is the process of dealing with unexpected events that can damage an organization. This involves effective planning, control and communication to reduce the negative impact of the crisis. Furthermore, crisis management is just one form of three forms of management response to changes that occur in the organization's external environment. Iriantara (2004). A "crisis" is an unexpected major event that has the potential to have a negative impact on the company and the public. This event is possibly quite significant damage to the organization, employees, products, services produced by the organization, financial condition and reputation of the company Putra (1999).

A crisis is an unexpected, dramatic, sometimes unprecedented event that pushes an organization into chaos and can destroy the organization without any real action. Powell (2005). In general, crisis management is an in-depth process of dealing with disruptive and unexpected events that will threaten and endanger organizations and companies. Crisis management has the responsibility to find solutions to crisis problems that arise using crisis management strategies.

National Data Center (PDN)

The National Data Center (PDN) is a data center facility for the purposes of placing, storing and processing data, as well as data recovery which will later be used for data sharing by central agencies and regional governments, and is interconnected in Indonesia (Wikipedia).

Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions (PP PSTE) states: Article 27 paragraph (5). The National Data Center as

referred to in paragraph (21) letter a consists of a data center organized by the minister who carries out government affairs in the field of communications and informatics and/or a data center for central agencies and regional governments that meets certain requirements. This Government Regulation regulates the implementation of electronic systems and transactions, including the implementation of data centers and disaster recovery centers to ensure the security, integrity and availability of data managed by central and regional government agencies.

Cybersecurity

Cybersecurity is the practice of protecting computers, networks, software applications, systems critical, and data on potential digital threats. Cybersecurity (cybersecurity) is a practice protect systems, networks, and programs from digital attacks. These attacks are usually targeted to access, change, or destroy sensitive information, extort money from users, or disrupt business operations. Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE). The ITE Law is the governing legal basis regarding information and electronic transactions. One of the important points in this law is about sanctions for cybercriminals. Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions (PP 71/2019). PP 71/2019 regulates further regarding the implementation of electronic systems and transactions. One of the goals is to increase public confidence in electronic transactions that are safe and legal in the judgements of the law.

Incident Response

Incident response is a systematic approach to addressing and managing the consequences of a cybersecurity incident. This includes detection, analysis, containment, eradication, and recovery. Incident response is the action that organizations take when they believe that IT systems or data may have been breached. For example, security professionals will act if they see evidence of unauthorized users, malware, or failed security measures (Microsoft Security).

Previous Research

No	Title	Writer	Year	Comparison
1	Analisis Manajemen Krisis: Studi Kasus PT Garuda Indonesia	Ibnu Nur Aziiz Ibnu Aziiz Walisongo State Islamic University	2023	Crisis management and crisis communication have a crucial role in the field of Public Relations
2	Analisis Manajemen Krisis (Studi Kasus : Perusahaan Shopee Indonesia)	Teguh Hadi Prasety Fakultas Daakwah dan Komunikasi ,	2022	Crisis management is one method that can be used to overcome a

		UIN Walisongo Semarang		crisis that befalls a company
3	Strategi Manajemen Krisis Public Relations PT Blue Bird Group	Ita Suryani, Asriyani Sagiyanto Akademi Komunikasi Bina Sarana Informatika	2018	Public relations is a communication function for develop public institution communication.
4	Analisis Manajemen Krisis Dan Manajemen Isu PT Sariwangi Terhadap Peningkatan Citra Perusahaan	Nabilla Luthfyana Azhaar Universitas Islam Negeri Walisongo Semarang	2023	Analyzing the crisis stages of the crisis experienced by PT Sariwangi and the strategies that should be implemented to improve it
5	Analisis Faktor Yang Mempengaruhi Pelaporan Insiden Keselamatan Pasien pada Perawat	Maria Yuventa, Nursalam Nursalam, Andri Setiya Wahyudi Airlangga University, Fundamental and Management Nursing Journal 3(1):15	2020	Reporting incidents is an important first step to improving patient safety

RESEARCH METHODOLOGY

Types of Research and Research Design

This research uses a qualitative method with a case study method to gain an in-depth understanding of crisis management and incident response at the National Data Center. According to Wikipedia, Qualitative Research is research that is descriptive and tends to use analysis. Process and meaning (subject perspective) are more emphasized in qualitative research. The theoretical basis is used as a guide so that the research focus is in accordance with the facts in the field. Apart from that, this theoretical basis is also useful for providing a general overview of the research setting and as material for discussing research results.

From the perspective that qualitative research does not require theory, there are several points to focus on, namely: Qualitative research is exploratory and/or descriptive, not explanatory

(Creswell in Poerwandari, 2017). The type of research used in solving the problem formulation in this research is using qualitative research methods with a case study approach. Case study research is qualitative research that seeks to find meaning, investigate processes and gain in-depth understanding and understanding of individuals or situations (Emzir, 2016).

To begin a case study, the researcher first identifies the problem or question to be researched and develops a rationale for why a case study is an appropriate method to use in the study. In addition to the research question being clear, the selection of participants must be clearly based on their ability to contribute to the understanding of the phenomenon to be studied (Emzir, 2016).

The object of research in this research is: Crisis Management and Incident Response "National Data Center Case Study". The media used for research are mainstream media newspapers. This research uses a qualitative approach with a case study method to gain an in-depth understanding of crisis management and incident response at the National Data Center.

Research Instruments

Experts provide different views regarding understanding the definition of qualitative research instruments. Creswell (2014) states that qualitative research instruments are tools used to collect data in qualitative research which includes interviews, observations and case studies. Miles, Huberman, and Saldaña (2014) explained that qualitative research instruments are tools used to collect data in qualitative research which includes interviews, observation, and documentation. Bogdan and Biklen (2014) state that qualitative research instruments are tools or techniques used to collect data in qualitative research, which includes interviews, observations, case studies, focus group discussions (FGD), and documentation.

From the definitions presented by several experts, it can be concluded that qualitative research instruments are tools or techniques used to collect data in qualitative research which includes various types, including interviews, observations, case studies, FGDs, and documentation of activities.

Data Collection Techniques

Documentation - Newspaper Media

Data was collected from official reports, news articles, government documents, and interviews with cybersecurity experts.

Data Analysis Techniques

Data were analyzed using thematic analysis techniques to identify main themes related to crisis management and incident response.

Data analysis techniques are the process of systematically searching and compiling data obtained from interviews, field notes and documentation, by organizing data into categories, describing it into units, synthesizing it, arranging it into patterns, choose what is important and what will be studied, and make conclusions so that they are easily understood by yourself and others (Sugiyono,

2017: 147).

DISCUSSION

The National Data Center (PDN) was attacked by Ransomware which is software. Ransomware actively blocks access and content of data to the data owner. The implications can be seen when the data owner cannot access his own data. This cyber attack on PDN used a new type of ransomware virus known as Lockbit 3.0. As a result, around 210 databases belonging to ministries, institutions and local governments were affected, causing disruption to various public services. (6.com coverage, 27 June 2024).

Gadjah Mada University Faculty of Engineering lecturer, Ridi Ferdiana, regrets the cyber attack on the Temporary National Data Center Server (PDNS) managed by the Ministry of Communication and Information (Kominfo). The hack on Thursday, June 20 2024 had an impact on government agencies and services. (nasional.tempo.co- Saturday, 29 June 2024).

The following are a number of facts about National Data Center (PDN) disruptions compiled by kompas.com, 25 June 2024.

1. Consequences of Cyber Attacks on the Surabaya Server

   Head of the National Cyber and Crypto Agency (BSSN) Hinsa Siburian said the disruption to PDNS was caused by a cyber attack via ransomware on a server in Surabaya. "We need to convey that this temporary data center incident was a cyber attack in the form of ransomware with the name brain cipher ransomware," he said, quoted from the official BSSN website. Hinsa explained that brain cipher ransomware is the newest type of ransomware in cyber attacks. Hinsa explained that brain cipher ransomware is the newest type of ransomware in cyber attacks. The attack carried out infected the PDNS server and encrypted the data in it.

2. Disrupting Services in 210 Agencies

   As a result of the attack on PDNS, public services in 210 government agencies were disrupted. "From the data that was affected, there were 210 agencies that had an impact from both the central and regional levels," said Director General of Informatics Applications for Communications and Information, Semuel Abrijani Pangerapan, as reported by Kompas.com, Monday (24/6/2024). Of the 210 agencies affected, the most severe disruption occurred in the Ministry of Law and Human Rights' immigration services. Meanwhile, the Ministry of Education and Culture announced that important applications such as SINDE, KIP-Kuliah, Forms, PPKS Portal, Kemdikbudristek Scholarships, Cloud Drive, and other services were also affected by PDNS disruption.

3. Attack Windows Defender Security Features

   Head of BSSN Hinsa Siburian added that his party discovered a ransomware attack which resulted in an attempt to deactivate the Windows Defender security feature on PDNS which occurred starting June 17 2024 at 23.15 WIB.

This incident caused unwanted activity to occur at PDNS since June 20 2024 at 00.54 WIB. These activities include installing malicious files, deleting important system files, and disabling running services. Files related to storage, such as VSS, HyperV Volume, VirtualDisk, and Veaam vPower NFS are also inactive and damaged. "It was discovered that on June 20 2024, at 00.55 WIB, Windows Defender experienced a crash and could not operate," said Hinsa, quoted from the official BSSN page. Once it is known that there has been a cyber attack, the ransomware samples that attack will be subjected to further analysis involving other cyber security entities.

4. Lockbit 3.0 offender

According to BSSN's explanation, the ransomware that attacked PDNS was the latest version of the Lockbit 3.0 ransomware.

Kompas.id reported, Tuesday (25/6/2024), Lockbit is the most active ransomware syndicate in the world for the last three years. In 2022, Lockbit attacked 147 victims. This number is twice as many as the cyber criminal gangs which are in the second and third most active positions, BlackCat with 77 victims and Royal with 71 victims. Although the mastermind behind the hacking has not been revealed, from hacking incidents that have occurred in many countries, the ransomware gang is suspected to have come from Russia and North Korea.

5. The intruder demanded a ransom of 8 million US dollars

Minister of Communication and Information Budi Arie revealed that the PDNS system attacker demanded a ransom to return the taken data. "Yes (the ransom request) according to the team is 8 million US dollars," he said, as reported by Kompas.com, Monday. The ransom must be paid so that the perpetrator of the cyber attack will open the encryption of the infected PDNS data system. However, the government emphasized that it would not immediately agree to the request. The joint BSSN, Kominfo and Polri team will still investigate this attack.

6. Citizen data is not safe

With this attack, Hansa said that Indonesian citizens' data was not safe. "Earlier, I said the data was encrypted. If it's encrypted, it's actually not safe," said Hinsa. This malware works by taking control of data access, then locking it with a password that can only be opened if the victim pays a ransom of the amount specified by the perpetrator. Even so, it is very likely that the perpetrator first copied the data in PDNS before it was locked. Public data in the hands of perpetrators has the potential to be traded via special hacker sites. Hinsa said, BSSN together with the Ministry of Communication and Information, The National Police's Cyber Crime Team, and Telkomsigma Operational Cooperation as PDN managers will temporarily handle this problem.

The agencies or institutions responsible for the National Data Center (PDN) are the Ministry of Communication and Information (Kemenkominfo) and the National Cyber

Crypto Agency (BSSN). As the person responsible for the National Data Center (PDN), the two institutions must synergize and work well together. When a problem occurred when the National Data Center (PDN) was hacked by hackers and could not be accessed, the two institutions actually shifted responsibility to each other. This was revealed during a Hearing Meeting (RDP) at the DPR on June 27 2024. The National Data Center (PDN) as the center for all national data (data center) actually does not have data back up. A large budget should have allocated funds to purchase backup data devices (back up servers). When the National Data Center (PDN) was hacked, the two institutions were not ready to face Crisis Management and Incident Response even though the existence of the National Data Center (PDN) was covered by Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions (PP PSTE) and a large budget, but do not have good capabilities in mitigating unexpected incidents (force majeure).

The main problem is governance. "This is the result of our checks and there is no back up," said Head of BSSN, Lt. Gen. (Ret.) Hinsa Siburian, in a meeting between Commission I DPR, Ministry of Communication and Information, and BSSN at the DPR Building, Senayan, Jakarta, Thursday (27/6/2024). kompas.com, 28 June 2024. The House of Representatives or DPR questioned the performance and responsibility of the Ministry of Communication and Information, as well as the National Cyber and Crypto Agency (BSSN) in the event of a ransomware cyber attack targeting the Temporary National Data Center (PDNS) II Surabaya (. national.tempo.co- Saturday, 29 June 2024).

The following is a series of incident response steps taken to deal with hackers at the National Data Center (PDN):

a. Usman Kansong, Director General of Information and Public Communication, Kominfo, revealed that Kominfo together with the National Cyber and Crypto Agency or BSSN, and Telkom Sigma as the vendor have isolated data from PDNS 2 in Surabaya. Because of this, he claimed that the data in the data center could not be retrieved by the hacker, even though the server was successfully paralyzed. (6.com coverage, 27 June 2024).

b. Hearing Meeting (RDP) of the Ministry of Coordination of Information & BSSN on Thursday, 27 June 2025

c. Member of the DPR Defense Commission, Sukamta, encouraged the formation of a special committee or Special Committee to explore and resolve the issue of cyber attacks that

often occurs and targets government institutions. (nasional.tempo.co- Saturday, 29 June 2024).

d. A week after PDNS was hacked, the President summoned the Minister of Communication and Information and the Head of BSSN (Kompas 28 June 2024).

A week after the Lockbit ransomware variant attack on the Temporary National Data Center

or PDNS 2 occurred, President Joko Widodo summoned a number of ministers and heads of institutions to the Merdeka Palace, Jakarta, Friday (28/6/2024). The closed meeting discussed handling the attack on PDNS.

e. President Jokowi asked BPKP to audit the governance of the Temporary National Data Center (PDNS) 2 in Surabaya. (Kompas 28 June 2024).

President Joko Widodo asked for the management of the Temporary National Data Center 2 Surabaya to be audited while continuing efforts to recover from the paralysis caused by the ransomware attack. In the future, there must be improvements to the database system and comprehensive improvements.

Located at the Merdeka Palace, Jakarta, Friday (28/6/2024), President Joko Widodo summoned ministers and heads of institutions to attend a meeting. The meeting, which took place behind closed doors and started at 14.00 WIB, discussed the handling of the Temporary National Data Center (PDNS) attack which occurred since Thursday (20/6/2024).

Present, among others, were the Minister of Communication and Information, Budi Arie Setiadi, the Minister for Civil Service Empowerment and Bureaucratic Reform (PAN RB) Azwar Anas, the Minister of Home Affairs Tito Karnavian, and the Minister of State-Owned Enterprises Erick Thohir.

Apart from that, the Minister of National Development Planning/National Development Planning Agency Suharso Monoarfa, the Minister of Finance Sri Mulyani Indrawati, the Head of the National Cyber and Crypto Agency Hinsa Siburian, and the Head of the Financial and Development Supervisory Agency (BPKP) Yusuf Ateh.

f. The government announced a data migration recovery scheme in response to the ransomware cyber attack incident that occurred at the Temporary National Data Center (PDNS) 2 in Surabaya, East Java (Kompas TV 26 June 2024)

Director of Network and IT Solutions Telkom Indonesia, Herlan Wijarnako, explained that there are two stages of the data recovery process.

"The first stage is carried out on services that have data backups, while the second stage is for data owners who do not have data backups," explained Herlan in

press conference at the Ministry of Communication and Information, Central Jakarta, Wednesday (26/6/2024). Quoted from the KompasTV broadcast.

For the first stage, 44 tenants who have data backups in Surabaya and Batam locations have been identified.

1) The tenant has been contacted to help reactivate its public services through a temporary medium supported by PDNS 1 in Serpong, South Tangerang, and a backup data center in the Riau Islands.

2) This explanation confirms the statement by the Deputy Minister of Communications and Information, Nezar Patria, who previously stated that 44 agencies had migrated data to restore their public services.

The following is the Crisis Management carried out regarding the ransomware attack on the National Data Center (PDN):

a) Threat Identification and Isolation

Data Isolation: Kominfo, BSSN, and Telkom Sigma immediately isolated data from PDNS 2 in Surabaya to prevent further data theft.

Security Feature Disablement: Attackers disable Windows Defender security features, indicating that basic protection measures should be evaluated and strengthened.

b) Crisis Communication

Hearing Meeting (RDP): Meeting between Commission I DPR, Kemenkominfo, and BSSN to discuss the incident and the steps taken.

Public Statement: High-ranking officials provide information to the public regarding the incident and mitigation measures taken.

c) Early Remedial Actions

Governance Audit: President Jokowi asked BPKP to audit PDNS governance to identify deficiencies and improve them.

Public Service Recovery: Identify tenants with data backup and migrate public services to temporary data centers in Serpong and the Riau Islands.

d) Research and Analysis

Ransomware Analysis: Ransomware samples are further analyzed involving other cybersecurity entities to understand the attack mechanism and prevent similar attacks in the future.

Collaboration with Security Entities: BSSN is collaborating with the National Police's Cyber Crime team and Telkomsigma Operational Cooperation for further investigations.

e) Impact Mitigation

Data Migration: The data migration process for affected tenants with data backup has been carried out.

Recovery Scheme: A two-stage data recovery scheme for tenants with and without data backup is implemented.

f) Improved Security and Policies

Security Protocol Review: Review and enhancement of existing security protocols, including protection measures to prevent disabling security features such as Windows Defender.

Data Backup Policy: Implementation of stricter policies for regular data backup and storage of backup data in different locations.

g) Responsibility and Accountability

DPR Special Committee: Proposal to form a Special Committee (Pansus) to investigate and resolve the issue of frequent cyber attacks.

Inter-Agency Coordination: Improve coordination between the Ministry of Communication and Information and BSSN to ensure clear responsibilities and synergy in handling incidents.

Pointing out the Crisis Management & Incident Response steps that have been taken by Institutions, Ministries including the President regarding the National Data Center (PDN) which was hacked by hackers, so far they have not been able to show maximum results. The government's credibility looks very weak, especially since hackers are asking for a ransom of 8 million US$. The government fails to protect important and confidential data. Until now, the National Data Center (PDN) still cannot be restored. The government admits it has failed to fight hackers who carried out ransomware attacks on the National Data Center (PDN). kompas.com/tren/read/2024/06/28. The institution/institution that is best prepared for Crisis Management and Incident Response is the Directorate General of Immigration, as written by the business. tempo. co (June 29, 2024).

Director General of Immigration at the Ministry of Law and Human Rights, Silmy Karim, confirmed that crossing, visa, residence permit and passport services were operating normally on Friday, June 28. Previously, immigration services were hampered after the National Data Center (PDN) was hacked last Thursday. "Since the disturbance at the Ministry of Communication and Information's PDN occurred on Thursday last week,

"We are taking steps to deal with it, starting from issuing responsive and adaptive policies to deal with the impact of this cyber attack," said Silmy Karim in a written statement on Saturday, June 29 2024.

The crossing system has been restored and has been operating since Saturday evening, 22 June 2024. Autogate, visa and residence permit applications have returned to normal on Sunday, 23 June 2024. The M-Paspor and Cekal Online applications are operational again on Sunday, 23 June 2024, and the passport issuance system fully recovered last Friday. Silmy explained that his team had checked manually and documented it as the earliest form of handling of the crossing system at immigration crossing points (TPI) at airports and ports. Even though the airport entry and exit process was disrupted, Silmy said Immigration still had a crossing record.

"The decision to move the data center was made after 12 hours since the technical problem

at the Ministry of Communications and Information's national data center (PDN) occurred. We observed the development of PDN recovery which did not show anything positive on the first day of disruption. To handle system problems, the first step taken by the Directorate General of Immigration's IT Team was to ensure the status of the Immigration database at PDN. "Furthermore, the team prepared an Application Recovery Plan, formed an Immigration Services Recovery Task Force and carried out an inventory of technical needs," he said.

Not only that, Silmy said that since Thursday, June 20 last week, the Directorate General of Immigration's IT Team moved and integrated Immigration back-up data to a new data center. On Friday, June 21, the next day the system recovery showed positive signs.

The gradual restoration of immigration services starts with Cekal Online, Interpol, Immigration Crossing Application and Autogate. Once stable, recovery continues to Visa Services, Residence Permits and Passport Services. The progress of system recovery has shown significant results since Thursday, June 27. Silmy said 60 percent of all immigration service points in Indonesia and abroad had recovered. Meanwhile, last Friday the system had recovered 100 percent or perfectly.

"The Directorate General of Immigration's IT team works 24 hours to resolve problems with the Immigration service system. "When we received information that the application system was gradually recovering, officers in the visa and passport section came to work on holidays (Saturday-Sunday) to be able to serve the visa and passport issuance process which had been hampered," he said.

"The decision to move the data center was made after 12 hours since the technical problem at the Ministry of Communication and Information's PDN occurred. We observed the development of PDN recovery which did not show anything positive on the first day of disruption. To deal with system problems, the initial step taken by the Directorate General of Immigration's IT Team was to ensure the status of the Immigration database at PDN. "Furthermore, the team prepared an Application Recovery Plan to form an Immigration Services Recovery Task Force and carried out an inventory of technical needs," he said.

Not only that, Silmy said that since Thursday, June 20 last week, the Directorate General of Immigration's IT Team moved and integrated Immigration back-up data to a new data center. On Friday, June 21, the next day the system recovery showed positive signs.

CONCLUSION

1. Crisis Management implemented in dealing with the National Data Center collapse incident is as follows:
   a. Threat Identification and Isolation
   b. Data Isolation: Kominfo, BSSN, and Telkom Sigma isolated data from PDNS 2 in Surabaya to prevent further data theft.

Security Feature Disablement: Attackers disable Windows Defender security features, indicating that basic protection measures should be evaluated and strengthened.

c. Crisis Communication

Hearing Meeting (RDP): Commission I DPR, Ministry of Communication and Information, and BSSN

d. Initial Recovery Actions

1) Governance Audit: In accordance with Presidential Instructions, BPKP will audit the governance of the Temporary National Data Center (PDNS) 2 in Surabaya.

2) Public Service Recovery: Identify tenants with data backup and migrate public services to temporary data centers in Serpong and the Riau Islands.

e. Research and Analysis

Ransomware Analysis: Ransomware samples are further analyzed involving other cybersecurity entities to understand the attack mechanism and prevent similar attacks in the future. Collaboration with Security Entities: BSSN is collaborating with the National Police's Cyber Crime team and Telkom Sigma Operational Cooperation for further investigations.

f. Impact Mitigation

Data Migration: The data migration process for affected tenants with data backup has been carried out. Recovery Scheme: A two-stage data recovery scheme for tenants with and without data backup is implemented.

g. Security and Policy Improvements

Security Protocol Review: Review and enhancement of existing security protocols, including protection measures to prevent disabling security features such as Windows Defender.

Data Backup Policy: Implementation of stricter policies for regular data backup and storage of backup data in different locations.

h. Responsibility and Accountability

1) DPR Special Committee

2) Inter-Agency Coordination

2. Incident response steps taken by authorities/institutions:

a. Ministry of Communication and Information, National Cyber Crypto Agency (BSSN) & Telkom Sigma isolate data from PDNS 2 in Surabaya

b. Hearing Meeting (RDP) at the Ministry of Coordination of Information & BSSN at the

DPR

c. The DPR Defense Sector Commission is encouraging the formation of a special committee to explore and resolve the issue of cyber attacks that frequently occur and target government institutions.

d. The President Summons the Minister of Communication and Information and the Head of BSSN

e. President Jokowi asked BPKP to audit the governance of the Temporary National Data Center (PDNS) 2 in Surabaya

f. The government announced a data migration recovery scheme in response to ransomware cyberattack incidents.

3. The incident response carried out by institutions, ministries including the President regarding the National Data Center (PDN) which was hacked by hackers, has so far not been able to show an effective incident response. The National Data Center (PDN) still cannot be restored.

BIBLIOGRAPHY

Creswell, J. W. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. Sage Publications, Los Angeles.

Emzir. (2016). Metodologi Penelitian Kualitatif: Analisis Data. Rajawali Pers, Jakarta.Microsoft Security

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). Qualitative Data Analysis: A Methods Sourcebook. Sage Publications, Los Angeles.

Putra, A. Y. (1999). Manajemen Krisis dalam Organisasi. Gramedia Pustaka Utama, Jakarta.

Powell, G. (2005). Crisis Management: Leading in the New Strategy Landscape. Sage Publications, Los Angeles.Wikipedia

Yosal, Iriantara, 2004. Manajemen Krisis dan Respons Insiden:Studi Kasus dan Teori.Bandung : Unpad Press

Sugiyono. (2017). Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Alfabeta, Bandung.

"Pemerintah Gagal Lawan Peretas PDN, Siapa yang Harus Bertanggung Jawab?", Klik untuk baca: https://www.kompas.com/tren/read/2024/06/28/160000765/pemerintah-gagal-lawan-peretas-pdn-siapa-yang-harus-bertanggung-jawab-.

https://nasional.tempo.co/read/1885484/dpr-dorong-pembentukan-pansus-dalami-insiden-peretasan-pdns?tracking_page_direct

https://bisnis.tempo.co/read/1885525/ada-60-ribu-paspor-telat-terbit-saat-pusat-data-nasional-diretas-pekan-lalu?tracking_page_direct

https://www.kompas.com/tren/read/2024/06/25/153000565/6-fakta-gangguan-pusat-data-nasional-pelaku-minta-tebusan-8-juta-dollar-as

Artikel ini telah tayang di Kompas.com dengan judul "6 Fakta Gangguan Pusat Data Nasional, Pelaku Minta Tebusan 8 Juta Dollar AS", Klik untuk baca: https://www.kompas.com/tren/read/2024/06/25/153000565/6-fakta-gangguan-pusat-data-nasional-pelaku-minta-tebusan-8-juta-dollar-as.

https://www.kompas.id/baca/polhuk/2024/06/28/presiden-jokowi-minta-audit-tata-kelola-pdn