International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

Vol. 42 No. 2 January 2024, pp. 346-351

Optimization and Synergy of Backup and Restore Data Between BMKG Database Center and Regional Offices As Initial Mitigation Againts Ransomware Attacks

Heri Azhari Noor[1], Aulia Khamas H.[2], Tutun Juhana[3], Danang Rimbawa[4]

[1]Cyber Defense Engineering Study Program
Republic of Indonesia Defense University
Jakarta, Indonesia
gagahan09@gmail.com

[2]Faculty of Science and Defense Technology
Republic of Indonesia Defense University
Bogor, Indonesia
aulia.heikhmakhtiar@idu.ac.id

[3]School of Electrical Engineering and Informatics
Bandung Institute of Technology
Bandung, Indonesia
tutun@itb.ac.id

[4]Cyber Defense Engineering
Republic of Indonesia Defense University
Jakarta, Indonesia
hadr71@idu.ac.id

Abstract— In 2017 there were 99 countries, including Indonesia affected by the Wannacry ransomware cyber attack. This attack became one of the largest phenomenal cyberattacks ever to occur in the world. In just a short time, the malicious computer program inside this malware is then able to infect thousands of computer systems in hundreds of countries. Harapan Kita and Dharmais hospitals in Jakarta were successfully attacked by their information technology systems. Hundreds of PCs and servers were affected, making it difficult for patients to access services at both hospitals. BMKG as one of the entities of the Government of the Republic of Indonesia has invaluable assets in the form of data from observations and analysis in the fields of meteorology, climatology, air quality, and earthquakes. All of this data is obtained from observation points spread throughout Indonesia and has been going on for a very long period. From observation points then the data is centralized in the Database Center of the BMKG head office. Optimization and synergy in backing up data and restoring data between the head office and regions will be the intial mitigation to anticipate in the event of ransomware attacks in the future.

Keywords— Ransomware attack, backup and restore data

I. INTRODUCTION

Ransomware attacks have become increasingly sophisticated, targeting a broad spectrum of organizations, from small businesses to major corporations, and even governmental institutions. These attacks not only jeopardize the confidentiality, integrity, and availability of data but also inflict significant financial and reputational damage. Furthermore, they often undermine the trust that individuals and organizations place in digital systems.

Ransomware is a type of malware that attacks the victim by locking all files owned, then the attacker asks for a ransom against the victim, and the attacker will provide a key for the victim to use in opening the documents owned after the victim pays according to the rate given by the attacker. From the results of the annual cybersecurity monitoring report published by BSSN in 2021, Ransomware ranks second based on the types of attacks that are often reported to BSSN. [1]

In 2017 there were 99 countries, including Indonesia affected by the Wannacry ransomware cyber attack. This attack became one of the largest phenomenal cyberattacks ever to occur in the world. In just a short time, the malicious computer program inside this malware is then able to infect thousands of computer systems in hundreds of countries. Harapan Kita and Dharmais hospitals in Jakarta were successfully attacked by their information technology systems. Hundreds of PCs and servers were affected, making it difficult for patients to access services at both hospitals.

BMKG as one of the entities of the Government of the Republic of Indonesia has invaluable assets in the form of data from observations and analysis in the fields of meteorology, climatology, air quality, and earthquakes. All of this data is obtained from observation points spread throughout Indonesia and has been going on for a very long period. From observation points then the data is centralized in the Database Center of the BMKG head office. It is not impossible that in the future the BMKG could be targeted by hackers through a ransomware attack. If this were to happen, it would cause a huge loss to the organisation. this is because the data held by the BMKG is the result of direct observations that involve many resources, ranging from humans, expensive observation sensors and their communication networks.

Early anticipation is key to being able to minimise the impact of damage or losses from ransomware attacks. Optimization and synergy in backing up data and restoring data between the head office and regions will be the intial mitigation to anticipate in the event of ransomware attacks in the future for the BMKG organization.

II. LITERATUR REVIEW

Ransomware

Ransomware is a subset of malware, a collective term for all forms of malicious code, including computer viruses and worms. A ransomware attack can be defined as an attempt to extort an organization by denying it access to its data. Ransomware is probably one of the most serious cyberthreats the organization will face. In the past few years criminal gangs creating this type of malware and running ransomware as a service have been perfecting a different, more targeted approach to these kinds of attacks — for which metrics are much harder to obtain. Cybercriminals are also constantly coming up with new approaches to ensure that they receive the sum they ask for, usually by increasing the pressure on the victim.

In 2019, they started to rely on double extortion, which combines the “usual” data encryption with data exfiltration. In this way, they not only prevented access to the victim’s valuable, critical, or otherwise sensitive files, but could also leak or sell them to other malicious actors. Upping the ante further, some ransomware operators have adopted triple extortion, adding the further step of contacting business partners or customers of victims that have not paid the ransom demand. The cybercriminals inform the victim’s partners/customers that their sensitive data has been accessed as part of the ransomware attack, suggesting these partners/customers pressure the ransomware victim to pay up to prevent this data being released. In some cases, the attackers even demand payment from these partners/customers. Recent years have seen a shift away from victimizing large numbers of random people while requesting ransom demands of modest sums, toward a targeted approach making much larger ransom demands from a smaller victim pool. That group features deeper pockets and members who can ill afford to lose access to their data or control over it. [2]

One of the most phenomenal ransomware attacks ever was the Ransomware WannaCry attack. This ransomware exploits a vulnerability that exists in older Windows. Although Microsoft has patched the vulnerability quickly, most companies are still

infected because they do not update the systems they use. In other words, many companies are still using older versions of Windows. Once the WannaCry ransomware infects your device, it will start infecting your computer and encrypting all data. After that, the programme will display a screen asking the victim to pay a sum of money to regain access. Typically, the asking price will get higher over time until the files will be destroyed.

The WannaCry ransomware attack started on 12 May 2017 and occurred first in Asia. It quickly infected as many as 10,000 people every hour and was finally stopped after 4 days. The attack then caused a lot of chaos. Many businesses lost data and hospitals reported many cancelled surgeries because patient files had been lost. Although not 100% sure, the cybersecurity community attributes the attack to North Korea. Although WannaCry did not appear to target anyone specifically, it spread rapidly to 150 countries. The most attacks occurred in Russia, China, Ukraine, Taiwan, India, and Brazil. [3]

BMKG Database Center

The Database Center of the Meteorology, Climatology and Geophysics Agency (BMKG) is one of the critical components of the information technology infrastructure that supports the agency's operations and research. BMKG, as the institution responsible for monitoring weather, climate and earthquakes in Indonesia, collects and manages a large amount of data every day. The BMKG Database Center is the lifeblood of integrating, storing and managing all this data so that it can be used for analysis, prediction and research related to meteorology, climatology and geophysics in Indonesia.

One of the things that makes the BMKG Database Center so important is the variety of data it holds. They collect weather data from observation stations across Indonesia, long-term climate data, as well as seismic data related to earthquakes. All of this data is stored in various formats, including real-time, time series and spatial data, which requires a robust and scalable database management system to manage. The BMKG Database Center is not only a data repository but also the heart that drives various aspects of the BMKG's work. The success of operations and research at BMKG is highly dependent on the quality of data management.

BMKGSoft

In order to support the implementation of the main tasks and functions as a data center, the BMKG database center created a single data entry application called BMKGSoft. BMKG SOFT is the single data entry system that acts as the gateway for all incoming data. It serves as a critical interface between the real world and the digital realm, enabling BMKG to ingest, process, and store vast amounts of data. This system allows for the seamless transfer of data from various observation points, such as weather stations and seismograph networks, into a structured and accessible format within BMKG's database.

BMKGSoft was put into operation at the end of 2013. BMKGSoft is the software and hardware used in the management of meteorological, climatological and geophysical data online and centrally. BMKGSoft is an implementation of the goal of realising a single data entry system in a single system. Another goal is to uniform data in various formats owned by Stations (Technical Implementation Units/ UPT) in the regions and integrate them into one system. [4]

Mitigatian and Incident Response

In NIST SP 800-61, the incident handling process is also called the incident response life cycle. The process is also referred to as the incident response life cycle. This is because the incident team will use the results of incident handling to fix problems that arise in the previous incident handling process or develop new procedures to shorten the incident handling time. incident handling time.

Fig 1: NIST SP 800-61 (rev 2) Computer Security Incident Handling Guide

Incident handling consists of 4 processes as follows:

1. Preparation

   This stage is the preparation stage for incident handling. At this stage it is possible to reduce the probability of an incident occurs.

2. Detection and analysis

   At this stage, the incident response team detects symptoms that may indicate the occurrence of an incident and ascertain whether it is an incident or not.

3. Containment, Eradiction and Recovery

   This stage is where the incident response team seeks to control the incident until the recovery process from the incident.

4. Post-incident Activity

   At this stage, the incident that occurred and the handling process are analysed with the aim of reduce the probability of the same incident occurring and increase the effectiveness of the incident handling procedure. [5]

III. Research Method

The methodology used in this research is a literature study by collecting some literature sourced from books, journals, scientific papers, and researches on the threat of ransomware cyberattacks and mitigation of response incidents.

IV. Result And Discussions

BMKGSoft is a database integration system consisting of station and regional offices, head office, and users. The station and regional offices will enter observation data and weather forecasts, which will be simultaneously monitored and QC by the BMKG Database Center. Data that has been inputted will be stored on the cluster server and shared storage, which through the BMKG communication network can be accessed by users. These users consist of internal users for the benefit of BMKG data and external users for academics, research, individuals, companies and institutions. The display depicts as follows :

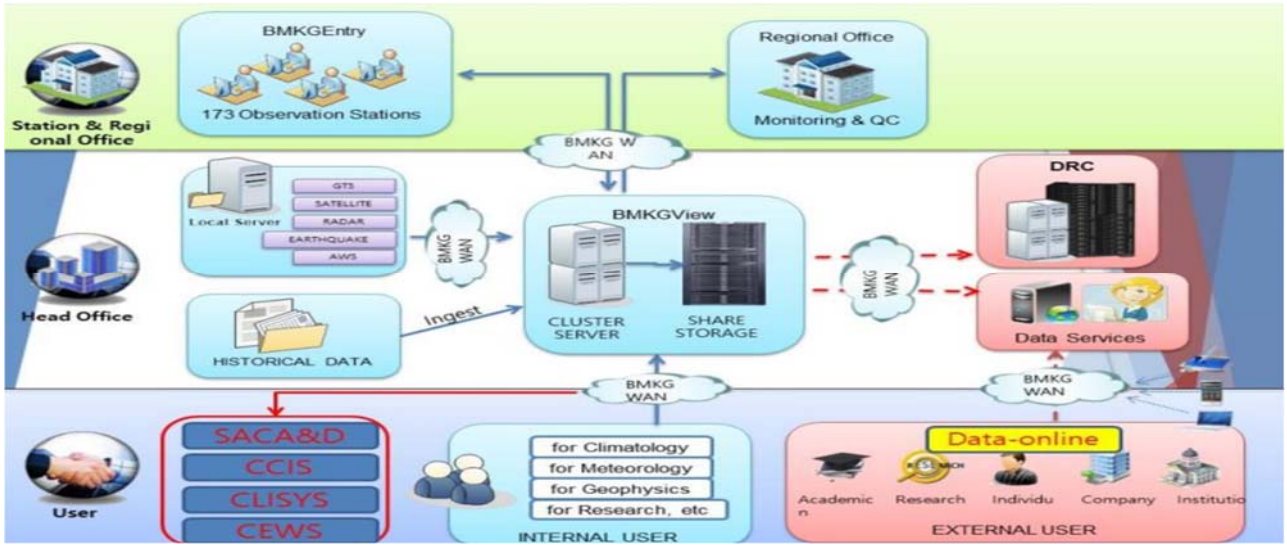

Fig 2: BMKGSoft Integration system

According to the Inter Vision, " Data backups don't prevent ransomware attacks from happening, but they can help mitigate the damage. The point of a ransomware attack is to infiltrate your data, encrypt or lock it, and then hold it hostage until you pay the ransom. Think kidnapping plots from your favorite action movies–that's what ransomware does with your data. Once your data is encrypted, it is essentially impossible for you to access it or use, let alone ensure its safety.

However, if your data is backed up, or stored in more than one location, then the ransomware is essentially ineffective because you still have your data. The next step requires having a plan to access and use that data. Think of it like this. Let's say you needed a house key to get in your home. Then someone steals your house key and says they will sell it back to you for S100. That's a pretty steep price for a key, but if that's your only one you might be tempted to buy it back. If you have a spare key somewhere else, however, then you can still get in your house without buying the original key back, and then take additional security measures after the fact. That is why backups are one of best ways to protect against ransomware. [6]

Having a data backup is great, unless it too falls victim to ransomware. So, in order to protect our backups from ransomware attacks, follow some of these ransomware backup best practices, they are :

- Have at least three copies of your data, or in other words, backup your backup.
- Store your backups on different media, including at least one off-site copy.
- Have at least one backup stored off-line.
- Back up your data early and often, avoiding long lapses in backup cycles.

Data backup is the first step to anticipate a ransomware attack. The BMKG database center must ensure consistent and regular data backups. The ability to restore data affected by a ransomware attack is key to minimizing losses. The BMKG database center must have an effective recovery plan in place. Strong cooperation between BMKG and regional offices is important in ensuring optimal data backup and recovery.

The BMKG database center should consider using the latest technology such as intrusion detection systems, security monitoring and advanced cybersecurity solutions. Equally important is raising information security awareness among BMKG staff and regional offices so that they can identify cyber threats quickly. Regular training on cybersecurity is a proactive measure that can help reduce the risk of ransomware attacks. BMKG database centers and regional offices should have strict data security policies and implement appropriate access controls. Real-time security monitoring can help detect ransomware attacks early and

reduce their impact. BMKG should have a tested emergency response plan to deal with a ransomware attack and manage the crisis effectively.

REFERENCES

[1] O. Kubovič, "RANSOMWARE: A look at the criminal art, of malicious code, pressure, and manipulation," *ESET Research white papers,* 2021.

[2] Feradhita, "https://www.logique.co.id/blog/2020/08/13/ransomware-wannacry/," 13 August 2020. [Online].

[3] Admin, "https://bmkg.go.id," 6 september 2023. [Online].

[4] B. Rahardjo, Incident Response, Jakarta, 2023.

[5] i. vision, "https://intervision.com," 13 may 2022. [Online].