PENGARUH SERANGAN SIBER *RANSOMWARE* YANG MENYERANG PUSAT DATA NASIONAL TERHADAP PERSEPSI DAN KEPERCAYAAN MASYARAKAT KOTA SEMARANG PADA KOMINFO

SKRIPSI

Diajukan untuk memenuhi persyaratan menyelesaikan program sarjana (S1)

Program Studi Ilmu Komunikasi

Fakultas Ilmu Komunikasi

Disusun oleh:

FAIZAL

32802100040

FAKULTAS ILMU KOMUNIKASI

PROGRAM STUDI ILMU KOMUNIKASI

UNIVERSITAS ISLAM SULTAN AGUNG SEMARANG

2025

SURAT PERNYATAAN KEASLIAN

Saya yang bertanda tangan di bawah ini:

Nama : Faizal

NIM : 32802100040

Fakultas Ilmu Komunikasi

Dengan ini menyatakan bahwa skripsi yang telah saya susun dengan judul : "Pengaruh Serangan Siber *Ransomware* Yang Menyerang Pusat Data Nasional Terhadap Persepsi Dan Kepercayaan Masyarakat Kota Semarang Pada Kominfo".

Adalah benar-benar hasil karya saya sendiri dan bukan merupakan plagiat dari skripsi atau karya ilmiah orang lain. Apabila demikian hari pernyataan saya tidak benar, maka saya bersedia menerima sanksi yang berlaku.

Demikian pernyataan ini saya buat dengan sebenar benarnya, untuk digunakan bilamana diperlukan.

Semarang, 2 Juni 2025

Penulis,

Faizal

32802100040

HALAMAN PENGESAHAN

Judul Skripsi	: **Pengaruh Serangan Siber *Ransomware* Yang Menyerang Pusat Data Nasional Terhadap Persepsi Dan Kepercayaan Masyarakat Kota Semarang Pada Kominfo**
Nama Penyusun	: Faizal
NIM	: 32802100040
Fakultas	: Fakultas Ilmu Komunikasi
Prodi	: Ilmu Komunikasi

Semarang, 2 Juni 2025

Dosen Pembimbing:	Penulis:
Made Dwi Adnjani, S.Sos., M.Si., M.I.Kom	Faizal
NIK.211109006	32802100040
(.....)	(.....)

Mengetahui,
Dekan Fakultas Ilmu Komunikasi

Trimanah, S.Sos., M.Si

NIK.211109008

HALAMAN PENGESAHAN SKRIPSI

Judul Skripsi	:	**Pengaruh Serangan Siber *Ransomware* Yang Menyerang Pusat Data Nasional Terhadap Persepsi Dan Kepercayaan Masyarakat Kota Semarang Pada Kominfo**
Nama Penyusun	:	Faizal
NIM	:	32802100040
Fakultas	:	Fakultas Ilmu Komunikasi
Prodi	:	Ilmu Komunikasi

Telah dinyatakan sah dan lulus dalam ujian skripsi Pendidikan Strata-1

Semarang, 2 Juni 2025

Penulis

Faizal

32802100040

Dosen Penguji:

1. Made Dwi Adnjani, S.Sos., M.Si., M.I.Kom (.....)
   NIK. 211109006
2. Mubarok S.Sos., M.Si (.....)
   NIK. 211121019
3. Iky Putri Aristhya, S.I.Kom, M.I.Kom (.....)
   NIK. 211121020

Mengetahui,

Dekan Fakultas Ilmu Komunikasi

Trimanah, S.Sos., M.Si

NIK.211109008

PERNYATAAN PERSETUJUAN UNGGAH KARYA ILMIAH

Saya yang bertanda di bawah ini

Nama	: Faizal
NIM	: 32802100040
Program Studi	: Ilmu Komunikasi
Fakultas	: Ilmu Komunikasi

Dengan ini menyerahkan karya ilmiah berupa skripsi dengan judul :

PENGARUH SERANGAN SIBER *RANSOMWARE* YANG MENYERANG PUSAT DATA NASIONAL TERHADAP PERSEPSI DAN KEPERCAYAAN MASYARAKAT KOTA SEMARANG PADA KOMINFO

dan menyetujuinya menjadi hak milik Universitas Islam Sultan Agung serta memberikan Hak Bebas Royalti Non-ekslusif untuk disimpan, dialih mediakan, dikelola dalam pangkalan data, dan dipublikasikannya di internet atau media lain untuk kepentingan akademis selama tetap mencantumkan nama penulis sebagai pemilik Hak Cipta. Pernyataan ini saya buat dengan sungguh-sungguh. Apabila dikemudian hari terbukti ada pelanggaran Hak Cipta/Plagiarisme dalam karya ilmiah ini, maka segala bentuk tuntutan hukum yang timbul akan saya tanggung secara pribadi tanpa melibatkan pihak Universitas Islam Sultan Agung.

Semarang, 10 Juni 2025

Yang menyatakan

Faizal

Motto

“Mulailah dengan apa yang benar, bukan dengan apa yang bisa diterima.”

-Franz Kafka-

HALAMAN PERSEMBAHAN

Dengan penuh rasa syukur ke hadirat Allah SWT yang senantiasa memberikan rahmat dan kemudahan, skripsi ini saya persembahkan kepada Ibu tercinta yang selalu menjadi sumber semangat dan kekuatan dalam hidup saya. Terima kasih atas doa, kasih sayang, dan dukungan yang tidak pernah henti mengiringi setiap langkah saya. Ucapan terima kasih juga saya sampaikan kepada teman-teman dan sahabat yang telah menemani perjalanan ini dengan kebersamaan, dukungan, serta motivasi yang sangat berarti. Tak lupa, saya juga mengucapkan terima kasih kepada diri saya sendiri yang telah bertahan dan berjuang hingga sampai pada tahap ini. Semoga skripsi ini dapat memberikan manfaat dan menjadi langkah awal untuk terus belajar dan berkarya demi masa depan yang lebih baik.

PENGARUH SERANGAN SIBER *RANSOMWARE* YANG MENYERANG PUSAT DATA NASIONAL TERHADAP PERSEPSI DAN KEPERCAYAAN MASYARAKAT KOTA SEMARANG PADA KOMINFO

Abstrak

Faizal

32802100040

Penelitian ini bertujuan untuk menganalisis pengaruh insiden serangan *ransomware* yang menyerang Pusat Data Nasional (PDN) terhadap persepsi dan kepercayaan masyarakat terhadap Kementerian Komunikasi dan Informatika (Kominfo). Latar belakang penelitian ini didasari oleh munculnya berbagai respons publik pasca insiden yang menyebabkan gangguan pada layanan digital pemerintah. Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei melalui kuesioner kepada 100 responden masyarakat Kota Semarang. Teknik analisis data menggunakan uji validitas, reliabilitas, dan regresi linier sederhana melalui bantuan software SPSS.

Hasil penelitian menunjukkan bahwa variabel serangan *ransomware* berpengaruh signifikan terhadap persepsi masyarakat, dengan nilai signifikansi 0,000 < 0,05 dan t hitung 6,310 > t tabel 1,984. Artinya, insiden tersebut secara langsung memengaruhi cara masyarakat memandang kinerja Kominfo. Namun, pada variabel kepercayaan masyarakat, pengaruh serangan *ransomware* tidak signifikan dengan nilai signifikansi 0,564 > 0,05 dan t hitung -0,579 < t tabel 1,984. Hal ini menunjukkan bahwa meskipun persepsi masyarakat terhadap Kominfo menurun, tingkat kepercayaan mereka belum sepenuhnya hilang. Penelitian ini selaras dengan teori kepercayaan (*trust theory*) yang menyatakan bahwa kepercayaan publik terbentuk dari akumulasi pengalaman dan tidak mudah berubah hanya karena satu peristiwa.

Kata Kunci: ***ransomware, persepsi masyarakat, kepercayaan, Kominfo, PDN, trust theory.***

THE IMPACT OF CYBER RANSOMWARE ATTACKS ON NATIONAL DATA CENTER ON SEMARANG CITY PUBLIC PERCEPTION AND TRUST IN KOMINFO

Abstract

Faizal

32802100040

This study aims to analyze the influence of the ransomware attack incident that attacked the National Data Center (PDN) on public perception and trust in the Ministry of Communication and Informatics (Kominfo). The background of this study is based on the emergence of various public responses after the incident that caused disruption to government digital services. This study uses a quantitative approach with a survey method through a questionnaire to 100 respondents from the Semarang City community. The data analysis technique uses validity, reliability, and simple linear regression tests through the help of SPSS software.

The results of the study show that the ransomware attack variable has a significant effect on public perception, with a significance value of 0.000 <0.05 and a t count of 6.310> t table 1.984. This means that the incident directly affects the way the public views the performance of Kominfo. However, on the public trust variable, the influence of the ransomware attack is not significant with a significance value of 0.564> 0.05 and a t count of -0.579 <t table 1.984. This shows that although public perception of Kominfo has decreased, their level of trust has not completely disappeared. This research is in line with the trust theory which states that public trust is formed from accumulated experience and is not easily changed by just one event.

Keywords: ransomware, persepsi masyarakat, kepercayaan, Kominfo, PDN, trust theory.

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat, taufik, dan hidayah-Nya sehingga penulis dapat menyelesaikan penyusunan skripsi yang berjudul "Pengaruh Insiden Serangan *Ransomware* yang Menyerang Data PDN terhadap Persepsi dan Kepercayaan Masyarakat terhadap Kominfo" ini dengan baik. Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana di Universitas Islam Sultan Agung Semarang.

Dalam penyusunan skripsi ini, penulis tidak terlepas dari dukungan, bimbingan, dan arahan dari berbagai pihak. Oleh karena itu, penulis ingin menyampaikan penghargaan dan rasa terima kasih yang mendalam kepada:

1. Ibu Trimanah, S.Sos., M.Si., selaku Dekan Fakultas Ilmu Komunikasi.
2. Bapak Urip Mulyadi, S.Sos., M.I.Kom., selaku Ketua Program Studi Ilmu Komunikasi.
3. Ibu Made Dwi Adnjani, S.Sos., M.Si., M.I.Kom., selaku dosen pembimbing magang yang memberikan kritik, saran, dan arahan yang sangat bermanfaat dalam penyusunan laporan ini.
4. Ibu yang selalu mendukung dalam hidup penulis.
5. Kepada teman saya, Majid, Maria, Aulia, Faisal, yang senantiasa banyak membantu pada waktu kuliah saya dan dalam keadaan darurat saya.
6. Teman-teman saya, Zaki, Bayu, Rizki, Anang, Nabil, Febri, Hatta, dan banyak lagi tidak bisa saya sebutkan satu-persatu.

7. Kepada diri saya yang sudah berjuang dan bertahan sejauh ini melalui proses yang panjang.

Penulis berharap Skripsi ini dapat memberikan manfaat, baik berupa wawasan maupun pengalaman, bagi siapa saja yang membacanya. Masukan berupa kritik dan saran juga sangat diharapkan demi penyempurnaan di masa mendatang.

Penulis

Faizal

DAFTAR ISI

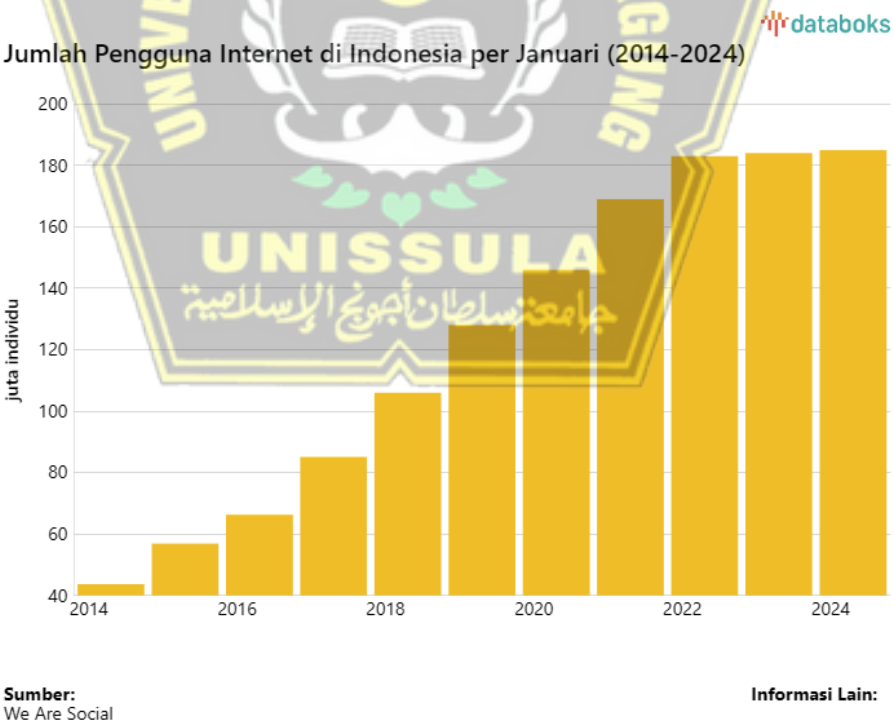
Daftar Gambar dan Tabel

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi membawa manusia kearah yang lebih baru seperti adanya internet, Internet merupakan sebuah jaringan yang berfungsi untuk menghubungkan antara satu media elektronik dengan media lainnya. Jaringan komunikasi inilah yang akan mentransfer data secara tepat dan cepat melalui frekuensi tertentu. Munculnya internet menjadikan kemudahan bagi semua orang untuk melakukan kegiatan seperti akses informasi, pekerjaan, hiburan, dan yang lain sebagainya.



Gambar 1. 1 Pertumbuhan jumlah pengguna internet di Indonesia tahun 2014-2024

Penggunaan internet di Indonesia telah mengalami pertumbuhan yang luar biasa dalam beberapa dekade terakhir. Menurut laporan We Are Social, pada Januari 2024 terdapat 185 juta individu pengguna internet di Indonesia, yang setara dengan 66,5% dari total populasi nasional yang mencapai 278,7 juta orang. Pengguna internet di Indonesia awal tahun ini meningkat sekitar 1,5 juta orang atau naik 0,8% dibandingkan dengan Januari 2023. Laporan tersebut juga menunjukkan bahwa jumlah pengguna internet di Indonesia terus meningkat selama satu dekade terakhir.

Jika dibandingkan dengan Januari 2014, jumlah pengguna internet saat ini telah bertambah sekitar 141,3 juta orang. Dalam 10 tahun terakhir, tingkat pertumbuhan tertinggi tercatat pada Januari 2017, di mana jumlah pengguna internet nasional melonjak sebesar 28,4%. Sebaliknya, pertumbuhan paling lambat tercatat pada Januari 2023, dengan peningkatan hanya sebesar 0,6%.

Peningkatan signifikan ini mencerminkan semakin pentingnya internet dalam kehidupan sehari-hari masyarakat Indonesia, baik untuk komunikasi, informasi, hiburan, hingga kegiatan ekonomi seperti belanja online dan perbankan digital.

Adanya perkembangan internet ini tentunya tidak hanya membawa kemudahan dan manfaat positif saja, tetapi juga menimbulkan tantangan baru, salah satunya adalah munculnya istilah baru yang dikenal sebagai cybercrime. Cybercrime mencakup berbagai aktivitas ilegal yang dilakukan

melalui jaringan internet, seperti pencurian identitas, penipuan online, peretasan sistem, dan penyebaran malware.

Aktivitas kejahatan siber ini tidak hanya mengancam individu, tetapi juga bisnis, lembaga pemerintah, dan infrastruktur kritis. Dengan semakin canggihnya teknologi, metode yang digunakan oleh pelaku kejahatan siber pun terus berkembang, membuat keamanan siber menjadi isu yang sangat penting. Oleh karena itu, upaya untuk meningkatkan keamanan siber harus dilakukan secara berkelanjutan, termasuk edukasi masyarakat tentang cara melindungi data pribadi, peningkatan sistem keamanan, dan kerjasama internasional dalam penegakan hukum terhadap kejahatan siber.

Keamanan siber kini menjadi isu yang sangat penting di era digital saat ini. Teknologi informasi telah merasuk ke dalam hampir setiap aspek kehidupan masyarakat modern, membuat ketergantungan kita pada sistem digital semakin besar. Akibatnya, insiden serangan siber telah mengalami peningkatan yang signifikan, baik dari segi frekuensi maupun tingkat keparahannya. Berdasarkan laporan yang diterbitkan oleh Global Cybersecurity Index (GCI), serangan siber di seluruh dunia mengalami kenaikan sebesar 17% pada tahun 2023 jika dibandingkan dengan tahun sebelumnya (ITU, 2023). Kenaikan ini menunjukkan betapa seriusnya ancaman keamanan siber di tingkat global.

Di Indonesia, situasinya tidak jauh berbeda. Serangan siber tidak hanya menargetkan sektor swasta seperti perusahaan teknologi dan

perbankan, tetapi juga institusi pemerintah yang menyimpan data publik yang sangat sensitif. Serangan-serangan ini menimbulkan kekhawatiran besar mengenai keamanan data publik dan kemampuan pemerintah dalam melindungi informasi penting dari akses yang tidak sah. Sebagai contoh, serangan yang terjadi di Kementerian Komunikasi dan Informatika (Kominfo) Indonesia menjadi bukti nyata bahwa ancaman siber dapat menyerang berbagai sektor, termasuk lembaga pemerintahan yang seharusnya memiliki sistem keamanan yang kuat.

Serangan *ransomware* yang menyerang Pusat Data Nasional (PDN) Kementerian Komunikasi dan Informatika (Kominfo) Indonesia pada Juni 2024 adalah salah satu contoh nyata dari ancaman siber yang dapat berdampak luas. Serangan ini tidak hanya mengganggu layanan penting seperti sistem keimigrasian tetapi juga menimbulkan kekhawatiran tentang keamanan data publik.

Menteri Komunikasi dan Informatika, Budi Arie Setiadi, mengungkapkan bahwa Pusat Data Nasional mengalami enkripsi oleh *ransomware*. Namun menurutnya data yang berdampak pada insiden yang merugikan ini adalah data PDN sementara yang mana tersedia di Surabaya, serangan ini dilakukan dengan cara randomware yang mengenskripsi data sehingga tidak dapat digunakan dan dibuka datanya. Serangan ini berdampak pada 210 instansi pemerintah, termasuk instansi di pusat dan

daerah, yang menunjukkan betapa luasnya cakupan dan dampak dari serangan tersebut.

Gambar 1. 2 Breaking News dari kominfo tentang PDN yang down

Menurut Samuel A. Pangerapan selaku Dirjen Aplikasi Informatika mengatakan merasa ada indikasi serangan *ransomware* ini pada waktu subuh dan setelah ditelusuri ada pelayanan yang down dan sedang dilakukan investigasi, *ransomware* ini menggunakan teknologi Brainchipper yang merupakan mutase dari Lockbit 3.0 dan data sudah dilakukan karantina, menurutnya kerugian dalam insiden ini adalah layanan imigrasi yang paling parah berdampak.

Pihak Telkom juga menambahkan dari insiden *ransomware* yang terjadi ini, pelaku yang meretas data PDN meminta tebusan sejumlah 8 juta USD atau setara dengan 131 Milyar Rupiah dan pihak Telkom mengatakan

bahwa saat ini timnya sudah memiliki jaringan untuk mengakses dan menghunungi pelaku peretas PDN ini dan mengaku akan membereskan masalah ini secepatnya agar layanan publik cepat pulih Kembali dan Masyarakat tidak khawatir akan data yang tersebar di Blackmarket.

Tanggapan pemerintah terhadap serangan ini melibatkan berbagai pihak, termasuk Kementerian Kominfo, Badan Siber dan Sandi Negara (BSSN), Cyber Crime Polri, dan Telkom. Mereka berupaya melakukan pemulihan sistem serta investigasi untuk mengetahui penyebab dan pelaku serangan.

Kejadian ini menyoroti pentingnya keamanan siber yang kuat, terutama dalam mengelola data sensitif yang dimiliki oleh instansi pemerintah. Kerentanan terhadap serangan *ransomware* menimbulkan risiko besar bagi masyarakat, terutama jika data pribadi mereka dieksploitasi oleh peretas.

Kepercayaan masyarakat terhadap institusi pemerintah sangat bergantung pada persepsi mereka tentang keamanan dan privasi data. Studi menunjukkan bahwa insiden keamanan siber dapat mengakibatkan penurunan signifikan dalam kepercayaan publik (Ponemon Institute, 2022). Dalam konteks yang lebih luas, kepercayaan publik adalah pondasi bagi keberlangsungan dan efektivitas layanan pemerintah. Kepercayaan ini mencakup keyakinan bahwa pemerintah mampu melindungi data pribadi mereka dari ancaman siber, yang semakin kompleks dan beragam.

Kasus pembobolan data di Kementerian Komunikasi dan Informatika (Kominfo) Indonesia bukan hanya menjadi masalah teknis yang memerlukan solusi segera, tetapi juga menjadi krisis kepercayaan yang mendalam. Ketika insiden seperti ini terjadi, masyarakat cenderung meragukan kemampuan pemerintah untuk menjaga keamanan data mereka. Hal ini tidak hanya mempengaruhi persepsi terhadap satu instansi, tetapi juga bisa meluas ke seluruh ekosistem digital yang dikelola oleh pemerintah. Rasa ketidakamanan ini dapat menyebabkan masyarakat menjadi enggan menggunakan layanan digital yang disediakan oleh pemerintah, meskipun layanan tersebut dirancang untuk meningkatkan efisiensi dan kemudahan dalam berbagai aspek kehidupan.

Oleh karena itu, penelitian ini akan menganalisis pengaruh serangan siber *ransomware* yang menyerang pusat data nasional terhadap persepsi dan kepercayaan masyarakat kota semarang pada kominfo. Penelitian ini diharapkan dapat memberikan wawasan yang lebih dalam tentang dampak serangan siber terhadap persepsi publik serta rekomendasi untuk meningkatkan kebijakan keamanan siber dan strategi komunikasi pemerintah.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan di atas, maka rumusan masalah yang menjadi fokus penelitian ini adalah sebagai berikut:

1.2.1 Bagaimanakah pengaruh serangan siber *ransomware* yang menyerang Pusat Data Nasional terhadap persepsi Masyarakat Kota Semarang pada Kominfo

1.2.2 Bagaimanakah pengaruh serangan siber *ransomware* yang menyerang Pusat Data Nasional terhadap kepercayaan Masyarakat Kota Semarang pada Kominfo

1.3 Tujuan Penelitian

Berdasarkan Rumusan masalah yang telah dijelaskan di atas, maka tujuan penelitian ini adalah sebagai berikut:

1.3.1 Untuk mengetahui pengaruh serangan siber *ransomware* yang menyerang Pusat Data Nasional terhadap persepsi Masyarakat Kota Semarang pada Kominfo

1.3.2 Untuk mengetahui pengaruh serangan siber *ransomware* yang menyerang Pusat Data Nasional terhadap kepercayaan Masyarakat Kota Semarang pada Kominfo

1.4 Manfaat Penelitian

1.4.1 Secara Akademis

Penelitian ini diharapkan dapat memperkaya bahan referensi penelitian dan menjadi sumber bacaan di lingkungan program studi Ilmu Komunikasi, khususnya dalam memahami dampak insiden keamanan siber terhadap persepsi dan kepercayaan masyarakat.

1.4.2 Secara Teoritis

Hasil dari penelitian ini diharapkan nantinya dapat memberikan pengetahuan yang lebih mendalam mengenai bagaimana insiden *ransomware* mempengaruhi kepercayaan masyarakat. Penelitian ini juga diharapkan dapat menjadi sumber informasi untuk pengembangan penelitian sejenis di masa yang akan datang.

1.4.3 Secara Praktis

a. Bagi Pemerintah dan Instansi Terkait:

Penelitian ini nantinya dapat dijadikan sebagai informasi dan dasar pertimbangan dalam memperkuat kebijakan keamanan siber dan pengelolaan data. Pemerintah dan instansi terkait dapat menggunakan hasil penelitian ini untuk meningkatkan sistem keamanan dan transparansi dalam penanganan data publik.

b. Bagi Masyarakat:

Penelitian ini diharapkan dapat menjadi masukan berharga bagi masyarakat dalam memahami pentingnya keamanan data pribadi. Selain itu, penelitian ini dapat membantu masyarakat untuk lebih kritis dan waspada terhadap risiko keamanan siber, sehingga mereka dapat lebih percaya dan nyaman dalam menggunakan layanan digital pemerintah.

c. Bagi Akademisi dan Peneliti:

Penelitian ini dapat menjadi dasar bagi penelitian lanjutan yang ingin mengkaji lebih dalam mengenai hubungan antara insiden keamanan siber dan kepercayaan publik. Peneliti lain dapat menggunakan temuan penelitian ini sebagai acuan untuk memperluas studi di bidang keamanan siber dan kepercayaan masyarakat terhadap institusi pemerintah.

1.5 Kerangka Teori

1.5.1 Paradigma Penelitian

Bogdan dan Biklen (dalam Edi Suryadi, 2019:22) mendefinisikan paradigma sebagai pengelompokan longgar dari asumsi yang dihubungkan bersama oleh ide atau klaim yang memandu penelitian dan penalaran. Paradigma merujuk pada gaya berpikir, sudut pandang, atau cara pandang seseorang terhadap dunia. Menurut Khun (dalam Kriyantono, 2016:14), paradigma adalah kumpulan praduga, ide, pendekatan, dan contoh ideal dari solusi masalah penelitian.

Penelitian ini menggunakan paradigma positivis. Paradigma ini memandang realitas sosial sebagai entitas asli dan/atau konkrit yang dapat diamati dan diukur dengan cermat (Edi Suryadi, 2019:23). Filsafat positivisme menganggap bahwa realitas/gejala/fenomena dapat diklasifikasikan, relatif tetap, konkrit, teramati, terukur, dan hubungan gejala bersifat sebab-akibat

(Sugiyono, 2016:8). Paradigma ini mencakup ciri-ciri ilmu, yang mengandung berbagai hipotesis yang dapat divalidasi di masa depan dan diakui sebagai fakta atau hukum. Paradigma ini telah berkembang dari waktu ke waktu, dengan setiap informasi berfungsi sebagai jenis blok bangunan yang, ketika dirakit dalam urutan yang benar, melengkapi "konstruksi pengetahuan" yang memungkinkan generalisasi dibuat untuk populasi tertentu (Denzin dan Lincoln, 2009:140).

Paradigma positivisme ini sangat cocok dengan penelitian yang akan dilakukan untuk mengetahui pengaruh insiden *ransomware* yang menyerang Pusat Data Nasional terhadap persepsi dan kepercayaan masyarakat Kota Semarang terhadap institusi pemerintah. Paradigma ini memungkinkan peneliti untuk mengukur dan mengamati fenomena secara objektif serta menganalisis hubungan sebab-akibat antara insiden *ransomware* dengan perubahan persepsi dan kepercayaan masyarakat.

1.5.2 State of Art

Heny Triyaningsih (2020), dengan judul *"Efek Pemberitaan Media Massa Terhadap Persepsi Masyarakat Tentang Virus Corona (Studi Kasus; Masyarakat di Pamekasan)"*. Hasil survei menunjukkan bahwa media terutama media sosial menjadi rujukan bagi masyarakat untuk mendapat informasi mengenai virus Corona. Adapun efek media kepada masyarakat menunjukkan strong effect

bahkan mampu membentuk persepsi masyarakat Pamekasan tentang pencegahan penularan Virus Corona kepada individu. Hasil survei tersebut menyiratkan betapa pentingnya bagi individu maupun instansi media membuat dan menyebar berita/informasi yang benar dan valid. Sekaligus kebutuhan pembenahan Undang Undang terkait dalam ranah Sistem Komunikasi Indonesia.

Hutomo Rusdianto, Chanafi Ibrahim (2016), dengan judul *"PENGARUH PRODUK BANK SYARIAH TERHADAP MINAT MENABUNG DENGAN PERSEPSI MASYARAKAT SEBAGAI VARIABEL MODERATING DI PATI".* Hasil kajian menunjukkan bahwa produk-produk bank syariah yang ada di lembaga keuangan mikro khususnya di kecamatan Kota Pati mempunyai dampak bagi masyarakat, hal ini membuktikan bahwa produk-produk (tabungan) lembaga keuangan mikro mempunyai manfaat bagi nasabah atau masyarakat. Sedangkan persepsi masyarakat dapat menjadi variabel moderating, karena Bank Umum mampu memberikan edukasi kepada masyarakat bahwa produknya terbebas dari unsur riba.

Tri Inda Fadhila Rahma (2018), dengan judul "*PERSEPSI MASYARAKAT KOTA MEDAN TERHADAP PENGGUNAAN FINANCIAL TECHNOLOGY (FINTECH)".* Hasil penelitian menunjukkan bahwa persepsi masyarakat terhadap penggunaan financial technology (fintech) meliputi sikap, minat, pemahaman, motivasi, dan harapan. Dimana sikap masyarakat terhadap

penggunaan fintech, memberikan dukungan kepada kemajuan inovasi teknologi keuangan di Indonesia yang sangat membantu masyarakat, sedangkan minat masyarakat untuk menggunakan fintech sudah terbukti dari hasil wawancara 9 dari 10 responden sudah berminat menggunakannya. Masyarakat sudah begitu memahami manfaat dan penggunaan fintech karena penggunaan fintech lebih efisien dan efektif dibandingkan jasa keuangan lainnya sehingga masyarakat termotivasi untuk menggunakan fintech. Dan harapan masyarakat kepada penyelenggara fintech agar memberikan sosialisasi kepada masyarakat dan kemudahaan atau kepraktisan dalam menggunakan layanan, sehingga masyarakat yang kurang memahami teknologi dapat menggunakannya dengan mudah.

Penelitian ini menggunakan State of Art sebagai acuan selama proses penulisan. Dari State of the Art diatas, perbedaan dan keunikan dari penelitian ini dengan yang diatas adalah terdapat di tema penelitian, objek penelitian, populasi penelitian dan tujuan penelitian.

1.5.3 Teori Penelitian

1. Trust Theory

Teori kepercayaan telah menjadi fokus penelitian sejak awal tahun 1950-an ketika Deutsch memulai penelitian kepercayaan dalam psikologi sosial. Deutsch (1958)

mendefinisikan *trust* sebagai keyakinan individu terhadap niat dan kemampuan mitra yang terlibat, serta keyakinan bahwa mitra tersebut akan bertindak sesuai keinginan individu.

Teori Kepercayaan (*Trust Theory*) adalah pendekatan penting dalam memahami dampak insiden *ransomware* terhadap kepercayaan masyarakat terhadap institusi pemerintah. Teori ini mengeksplorasi faktor-faktor yang mempengaruhi kepercayaan seseorang atau kelompok terhadap entitas lain, dalam hal ini institusi pemerintah yang bertanggung jawab atas keamanan data publik.

Faktor-faktor lain yang mempengaruhi kepercayaan termasuk transparansi dalam komunikasi dan respons cepat serta efektif terhadap insiden. Ketika pemerintah menunjukkan bahwa mereka memiliki langkah-langkah keamanan yang kuat dan dapat merespons ancaman dengan cepat, tingkat kepercayaan masyarakat cenderung meningkat. Sebaliknya, kurangnya komunikasi yang jelas dan respons yang lambat dapat merusak kepercayaan masyarakat secara signifikan.

Oleh karena itu, teori kepercayaan menyediakan kerangka yang sangat berguna untuk menganalisis bagaimana insiden *ransomware* mempengaruhi kepercayaan masyarakat terhadap institusi pemerintah. Dengan memahami komponen-komponen

kepercayaan dan faktor-faktor yang mempengaruhinya, penelitian ini dapat memberikan wawasan mendalam tentang cara mengelola dan memulihkan kepercayaan publik setelah insiden keamanan siber.

2. Teori Elaboration Likelihood Model

Teori yang digunakan dalam penelitian ini adalah Elaboration Likelihood Model Theory. Teori ini ditemukan oleh Richard E. Petty dan John Cacioppo pada tahun 1980 di Ohio State University Amerika Serikat. Keduanya adalah ahli komunikasi persuasif. Elaboration Likelihood Model Theory berupaya menjelaskan bagaimana dan kapan seseorang dapat dipengaruhi atau justru tidak terpengaruh oleh suatu pesan yang diterimanya (Littlejohn, Foss, & Oetzel, 2017)

ELM menggambarkan bahwa proses penerimaan pesan tidak terjadi secara tunggal, melainkan melalui dua jalur utama, yaitu jalur sentral (central route) dan jalur periferal (peripheral route).

Jalur sentral terjadi ketika individu secara aktif dan kritis memproses isi pesan, biasanya ketika mereka memiliki motivasi dan kemampuan tinggi untuk memperhatikan informasi secara mendalam. Sebaliknya, jalur periferal terjadi ketika individu kurang berminat atau tidak memiliki kapasitas untuk mencerna

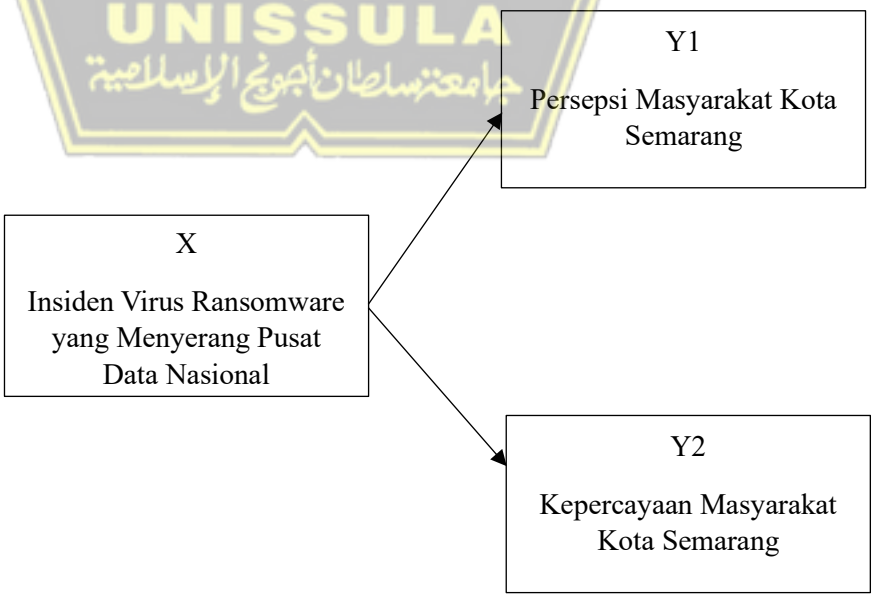
pesan secara mendalam, sehingga mereka cenderung dipengaruhi oleh faktor-faktor luar seperti kredibilitas sumber, daya tarik visual, atau emosi sesaat.

Dalam konteks komunikasi publik, termasuk dalam isu-isu seperti serangan siber terhadap PDN, ELM dapat digunakan untuk menganalisis bagaimana masyarakat membentuk persepsi dan kepercayaannya. Apakah masyarakat menilai berdasarkan isi informasi yang mendalam, atau hanya sekadar berdasarkan simbol, citra, atau pernyataan sepihak yang disampaikan oleh otoritas.

1.5.4 Kerangka Empiris Penelitian

Kerangka empiris dalam penelitian ini yaitu:

Kerangka penelitian



Keterangan:

X : Variabel Independen merupakan variabel yang bersifat bebas yang memengaruhi dan menyebabkan perubahan atau munculnya variabel dependen (terikat). Pengaruh insiden virus *ransomware* yang menyerang pusat data nasional adalah variabel dalam penelitian ini.

Y1 : Variabel dependen merupakan variabel yang bersifat terikat, yang dipengaruhi atau yang menjadi akibat dari adanya variabel independent (bebas). Persepsi Masyarakat Kota Semarang merupakan variabel dependen (Y1) dalam penelitian ini.

Y2 : Variabel dependen merupakan variabel yang bersifat terikat, yang dipengaruhi atau yang menjadi akibat dari adanya variabel independent (bebas). Kepercayaan Masyarakat Kota Semarang merupakan variabel dependen (Y2) dalam penelitian ini.

1.5.5 Hipotesis

Menurut Creswell & Creswell (2018), "Hipotesis adalah pernyataan formal yang menyajikan hubungan yang diharapkan antara variabel independen dan variabel dependen". Hipotesis berfungsi sebagai prediksi atau dugaan awal yang diuji melalui penelitian ilmiah. Dalam konteks penelitian kuantitatif, hipotesis biasanya dirumuskan

berdasarkan teori yang ada dan kemudian diuji melalui analisis statistik untuk menentukan validitasnya. Dengan kata lain, hipotesis membantu peneliti mengarahkan fokus penelitiannya dan menyediakan kerangka kerja untuk interpretasi data yang dikumpulkan.

Hipotesis juga berperan penting dalam menentukan desain penelitian dan metode analisis data. Sebuah hipotesis yang jelas dan terukur memungkinkan peneliti untuk merancang eksperimen atau studi yang dapat menguji hubungan antara variabel secara efektif.

Terdapat beberapa jenis situasi yang akan menjawab penelitian ini, berikut beberapa hipotesis dalam penelitian ini:

$H_0$1: Tidak terdapat pengaruh Insiden Virus *Ransomware* yang menyerang PDN terhadap Persepsi Masyarakat Kota Semarang

H_a1: Terdapat pengaruh Insiden Virus *Ransomware* yang menyerang PDN terhadap Persepsi Masyarakat Kota Semarang.

$H_0$2: Tidak terdapat pengaruh Insiden Virus *Ransomware* yang menyerang PDN terhadap Kepercayaan Masyarakat Kota Semarang

H_a2: Terdapat pengaruh Insiden Virus *Ransomware* yang menyerang PDN terhadap Kepercayaan Masyarakat Kota Semarang. Semakin tingginya keparahan insiden ini, maka semakin tinggi

pula pengaruhnya terhadap kepercayaan Masyarakat yang semakin tidak percaya Instansi pemerintah.

1.6 Definisi Konseptual dan Operasional Variabel

1.6.1 Definisi Konseptual

1. Serangan Siber *Ransomware*

Ransomware merupakan jenis malware yang diciptakan untuk mengenkripsi data pada sistem komputer atau perangkat lain, dan kemudian meminta pembayaran tebusan kepada korban agar data tersebut dapat dipulihkan atau didekripsi (Budi Hartono, 2023). Serangan ini dapat mempengaruhi berbagai aspek, termasuk operasional, finansial, dan reputasi dari entitas yang diserang.

Operasional perusahaan atau institusi yang terkena serangan *ransomware* seringkali terhenti total atau mengalami gangguan besar, karena akses ke data penting menjadi terbatas atau tidak mungkin sama sekali. Ketika sistem yang terganggu adalah bagian dari infrastruktur kritis, seperti sistem kesehatan, transportasi, atau layanan publik, dampaknya bisa meluas ke masyarakat umum, menyebabkan gangguan layanan yang signifikan.

Dari sisi finansial, dampak *ransomware* sangat merugikan. Selain biaya tebusan yang diminta oleh pelaku serangan, yang seringkali sangat tinggi, korban juga harus menanggung biaya pemulihan sistem, peningkatan keamanan, kehilangan pendapatan

selama sistem tidak berfungsi, serta potensi denda dan sanksi jika data yang dilindungi undang-undang terlibat dalam pelanggaran tersebut. Sebuah laporan dari Cybersecurity Ventures memperkirakan bahwa kerugian global akibat *ransomware* mencapai miliaran dolar setiap tahunnya.

Reputasi organisasi yang diserang *ransomware* juga dapat mengalami kerusakan serius. Kepercayaan pelanggan dan mitra bisnis bisa menurun drastis jika dianggap tidak mampu melindungi data dengan baik. Ini bisa berdampak jangka panjang, mengurangi nilai saham, menghambat kerjasama bisnis, dan merusak hubungan dengan pelanggan. Studi oleh Ponemon Institute menunjukkan bahwa pemulihan reputasi setelah insiden keamanan siber bisa memakan waktu bertahun-tahun dan biaya yang sangat besar.

Selain itu, serangan *ransomware* sering kali memaksa organisasi untuk meningkatkan kebijakan dan prosedur keamanan mereka, yang dapat memerlukan investasi signifikan dalam teknologi, pelatihan karyawan, dan penilaian risiko berkelanjutan. Organisasi mungkin juga harus berurusan dengan investigasi dari regulator dan pihak penegak hukum, serta tuntutan hukum dari pihak yang merasa dirugikan.

Dalam konteks yang lebih luas, serangan *ransomware* juga mendorong perubahan dalam kebijakan keamanan siber di tingkat

nasional dan internasional. Pemerintah dan lembaga regulasi sering kali merespons serangan besar dengan memperketat undang-undang perlindungan data dan meningkatkan kolaborasi internasional untuk melacak dan menangkap pelaku kejahatan siber.

2. Persepsi Masyarakat

Menurut William Fish (2021) Persepsi adalah proses yang melibatkan penginderaan dan pemahaman terhadap dunia di sekitar kita melalui panca indera. Fish mengeksplorasi beberapa teori utama dalam filsafat persepsi, termasuk representasionalisme, realisme langsung, dan fenomenalisme, serta bagaimana masing-masing teori ini berusaha menjelaskan cara kita mengalami dan memahami realitas.

Representasionalisme sebagai pandangan bahwa persepsi adalah tentang representasi mental dari dunia luar. Menurut teori ini, ketika kita melihat objek, kita tidak berhubungan langsung dengan objek tersebut, melainkan dengan representasi mental dari objek itu. Representasi ini mencakup informasi tentang objek, seperti bentuk, warna, dan posisi, yang diproses oleh otak kita.

Sebagai kontras dari representasionalisme, realisme langsung (atau naif) menyatakan bahwa kita memiliki akses langsung ke dunia nyata melalui persepsi kita. menurut teori ini, ketika kita melihat sebuah objek, kita sebenarnya sedang

berinteraksi langsung dengan objek tersebut tanpa perantara representasi mental. Realisme langsung menekankan hubungan yang tidak terputus antara pengamat dan dunia (William Fish, 2021).

Menurut William Fish (2021) fenomenalisme, yang berpendapat bahwa persepsi kita hanya berkaitan dengan fenomena atau penampakan dunia, bukan dengan objek itu sendiri. Menurut fenomenalisme, apa yang kita persepsikan adalah rangkaian sensasi yang disusun oleh pikiran kita menjadi pengalaman kohesif dari dunia luar.

3. Kepercayaan Masyarakat

Kepercayaan masyarakat merujuk pada keyakinan dan keyakinan masyarakat terhadap integritas, kompetensi, dan niat baik dari sebuah institusi atau entitas.

Menurut Flew dan Mcwaters (2020) kepercayaan dapat dipahami dari berbagai sudut pandang filosofis dan sosiologis yang saling melengkapi. Dari sudut pandang filosofis, kepercayaan dapat diartikan sebagai hubungan tiga pihak di mana A mempercayai B untuk melakukan tindakan X. Hubungan ini memiliki dimensi objektif dan subjektif yang didasarkan pada kapasitas institusional, kewajiban kontraktual, atau sejarah efektivitas dan keandalan. Selain itu, kepercayaan juga bergantung

pada karakter etis individu dan institusi yang dinamis dan kontekstual.

Sosiolog Niklas Luhmann menganggap kepercayaan sebagai salah satu sumber utama yang digunakan individu untuk mengelola kompleksitas kehidupan sosial, memungkinkan manajemen risiko masa depan yang lebih baik berdasarkan pemahaman dari pengalaman masa lalu. Sementara itu, Anthony Giddens menambahkan bahwa kepercayaan tidak hanya sekadar keyakinan individu bahwa tindakan tertentu akan menghasilkan konsekuensi tertentu, tetapi juga memerlukan "kualitas keyakinan" yang cenderung menolak pengambilan keputusan yang kalkulatif.

Menurut Flew dan Mcwaters (2020) sosiolog seperti Georg Simmel dan Max Weber menekankan bahwa kepercayaan tidak hanya ditempatkan pada individu tetapi juga pada institusi sosial. Kepercayaan dalam institusi memainkan peran penting dalam legitimasi berkelanjutan dari lembaga-lembaga tersebut dan interdependensi dalam hubungan kepercayaan antara individu, institusi, dan masyarakat secara keseluruhan

Dalam konteks ini, kepercayaan masyarakat terhadap institusi pemerintah adalah bagaimana masyarakat melihat kemampuan dan kejujuran pemerintah dalam melindungi data mereka dan menangani insiden siber.

1.6.2 Definisi Operasional

Definisi operasional adalah penetapan makna bagi suatu variabel melalui spesifikasi kegiatan atau prosedur yang diperlukan untuk mengukur, mengkategorisasi, atau memanipulasi variabel tersebut. Definisi ini menjelaskan kepada pembaca laporan penelitian apa saja yang perlu dilakukan untuk menjawab pertanyaan penelitian atau menguji hipotesis yang diajukan (Sutama 2016:52). Variabel dalam penelitian ini adalah Variabel bebas (X) dan terikat (Y1 dan Y2).

1. Variabel X: Serangan Siber Ransomware pada Pusat Data Nasional

   Variabel: Serangan Siber Ransomware pada PDN

   Indikator:

   a. Tingkat Ancaman

      Pengetahuan masyarakat tentang tingkat bahaya serangan siber terhadap keamanan nasional.

   b. Kegentingan

      Penilaian masyarakat tentang urgensi pemerintah dalam menangani insiden.

   c. Kegagalan Sistem

      Penilaian masyarakat terhadap kelemahan sistem keamanan pemerintah sebelum serangan.

   d. Dampak Layanan

Tingkat kekhawatiran masyarakat terhadap dampak insiden pada layanan publik.

2. Variabel Y1: Persepsi Masyarakat Kota Semarang

   Indikator:

   a. Kualitas Informasi

      Persepsi masyarakat tentang logika dan kejelasan informasi yang disampaikan pemerintah.

   b. Pemrosesan Pesan

      Sejauh mana masyarakat memproses dan menganalisis informasi yang diterima.

   c. Pengaruh Sosial

      Pengaruh opini publik atau media sosial terhadap persepsi masyarakat.

   d. Kredibilitas Sumber

      Kepercayaan terhadap lembaga yang menyampaikan informasi.

3. Variabel Y2: Kepercayaan Masyarakat Kota Semarang

   Indikator:

   a. Kemampuan Teknis (Ability)

      Keyakinan masyarakat terhadap kapasitas teknis pemerintah.

   b. Integritas (Integrity)

      Persepsi masyarakat terhadap kejujuran dan komitmen pemerintah.

c. Transparansi

Tingkat keterbukaan informasi dari pemerintah kepada publik.

d. Kolaborasi (Benevolence)

Kepercayaan masyarakat terhadap niat baik pemerintah dalam bekerja sama memperbaiki sistem.

1.7 Metode Penelitian

Sugiyono (2016) mendefinisikan metode penelitian sebagai cara ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu. Cara ilmiah berarti kegiatan penelitian didasarkan pada ciri-ciri keilmuan yaitu rasional, empiris, dan sistematis. Rasional berarti kegiatan penelitian dilakukan dengan cara-cara yang masuk akal sehingga dapat dijangkau oleh penalaran manusia. Empiris berarti cara-cara yang digunakan dapat diamati oleh indra manusia sehingga orang lain dapat mengamati dan mengetahui cara-cara yang digunakan. Sistematis berarti proses yang digunakan dalam penelitian itu menggunakan langkah-langkah tertentu yang bersifat logis.

1.7.1 Jenis Penelitian

Penelitian ini menggunakan metode pendekatan kuantitatif, yang bertujuan untuk mengukur dan menganalisis data numerik secara objektif (Sugiyono, 2016). Data numerik yang diperoleh lalu dianalisis lebih lanjut dan menghasilkan hasil. Penelitian ini memiliki Variabel X1, Y1, dan Y2.

1.7.2 Sumber Data

Sumber data dalam penelitian ini adalah:

1) Data Primer

Data yang diperoleh langsung dari responden melalui survei atau kuesioner yang disebarkan kepada masyarakat Kota Semarang. Responden dalam penelitian ini adalah individu-individu yang terpengaruh atau memiliki persepsi mengenai insiden *ransomware* yang menyerang Pusat Data Nasional. Pengumpulan data primer memungkinkan peneliti untuk mendapatkan informasi yang spesifik dan relevan terkait persepsi dan kepercayaan masyarakat terhadap pemerintah setelah insiden *ransomware* tersebut.

2) Data Sekunder

Data yang diperoleh dari sumber-sumber yang telah ada sebelumnya, seperti laporan pemerintah, publikasi ilmiah, artikel jurnal, buku, dan laporan dari institusi keamanan siber. Data sekunder ini digunakan untuk melengkapi dan mendukung analisis data primer, serta memberikan konteks lebih luas mengenai insiden *ransomware* dan dampaknya terhadap persepsi dan kepercayaan masyarakat.

Data primer dan sekunder akan dianalisis secara komprehensif untuk mendapatkan gambaran yang holistik mengenai pengaruh insiden

ransomware terhadap persepsi dan kepercayaan masyarakat di Kota Semarang. Analisis data ini akan membantu dalam mengidentifikasi faktor-faktor yang mempengaruhi kepercayaan masyarakat dan memberikan rekomendasi yang dapat digunakan oleh pemerintah untuk meningkatkan keamanan data serta mengembalikan kepercayaan publik.

1.7.3 Populasi dan Sampel

1) Populasi

Populasi dalam penelitian ini adalah seluruh masyarakat Kota Semarang yang berusia 18 tahun sampai dengan 45 tahun, dalam hal ini jumlahnya adalah 913.907 jiwa menurut BPS Kota Semarang pada data yang diperbarui bulan Februari 2024 (diambil pada bulan juni 2024). Populasi ini dipilih karena representatif dalam menggambarkan persepsi dan kepercayaan masyarakat terhadap insiden *ransomware* yang menyerang Pusat Data Nasional. Selain itu, populasi ini dianggap cukup dewasa dan memiliki pemahaman yang cukup mengenai isu-isu keamanan data dan dampaknya terhadap kehidupan sehari-hari. Dengan memilih populasi yang luas ini, penelitian dapat memperoleh gambaran yang lebih komprehensif dan akurat tentang bagaimana insiden *ransomware* mempengaruhi masyarakat secara umum.

2) Sampel

Teknik pengambilan sampel menggunakan rumus slovin sebagai berikut:

$$n = \frac{N}{Ne^2} + 1$$

Keterangan:

n = jumlah sampel N = Populasi

e = tingkat kesalahan (margin of errors) untuk penelitian kuantitatif 10%

Berdasarkan rumus tersebut maka:

$$n = \frac{1.113.629}{1.113.629\ (0{,}01)} + 1$$

$$n = 99{,}99$$

Dibulatkan menjadi 100, maka responden yang digunakan untuk sampling adalah 100 orang.

1.7.4 Teknik Pengambilan Sampel

Teknik pengambilan sampel yang digunakan dalam penelitian ini adalah purposive sampling. Dalam teknik ini, responden dipilih berdasarkan kriteria tertentu yang relevan dengan penelitian. Kriteria utama yang digunakan dalam pemilihan sampel adalah bahwa responden harus pernah mendengar atau mengetahui tentang insiden *ransomware* yang menyerang Pusat Data Nasional. Teknik purposive

sampling dipilih karena memungkinkan peneliti untuk fokus pada subjek yang memiliki informasi atau pengalaman yang relevan dengan topik penelitian. Dengan demikian, hasil penelitian diharapkan lebih valid dan dapat memberikan wawasan yang lebih mendalam mengenai persepsi dan kepercayaan masyarakat terhadap pemerintah setelah terjadinya insiden *ransomware*.

1.7.5 Metode Pengambilan Data

Metode pengambilan data dalam penelitian ini menggunakan pendekatan kuantitatif melalui survei. Metode ini dipilih karena dapat mengumpulkan data dari banyak responden secara efisien, serta memungkinkan analisis statistik yang memberikan gambaran umum tentang persepsi dan kepercayaan masyarakat terhadap insiden *ransomware* yang menyerang Pusat Data Nasional. Penelitian ini menggunakan skala likert, Menurut Sugiyono (2016), skala Likert adalah metode pengukuran yang digunakan untuk mengukur sikap, pendapat, dan persepsi seseorang atau sekelompok orang tentang fenomena sosial. Dalam skala Likert, responden diminta untuk menunjukkan tingkat persetujuan atau ketidaksetujuan mereka terhadap serangkaian pernyataan yang terkait dengan variabel yang diukur. Skala ini biasanya memiliki lima pilihan jawaban, yaitu:

1. Sangat setuju
2. Setuju
3. Netral/tidak tahu

4. Tidak setuju
5. Sangat tidak setuju

Setiap jawaban diberi skor yang berbeda, dengan nilai tertinggi menunjukkan tingkat persetujuan atau sikap yang paling kuat. Misalnya, "sangat setuju" mungkin diberi skor 5, sedangkan "sangat tidak setuju" diberi skor 1. Skor total dari semua item kemudian dihitung untuk menentukan sikap keseluruhan responden terhadap variabel yang diukur. Skala Likert memungkinkan pengukuran yang lebih halus dan lebih tepat terhadap sikap dan persepsi dibandingkan metode pengukuran lainnya.

1.7.6 Teknik Pengambilan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini meliputi kuesioner dan dokumentasi.

a. Kuesioner/Angket

Kuesioner adalah metode pengumpulan data dengan cara memberikan pertanyaan tertulis kepada responden untuk dijawab. Dalam penelitian ini, peneliti menyebarkan kuesioner kepada masyarakat Kota Semarang yang berusia 18 tahun ke atas dan pernah mendengar atau mengetahui tentang insiden *ransomware* yang menyerang Pusat Data Nasional.

b. Dokumentasi

Dokumentasi adalah metode pengumpulan data yang diperoleh melalui buku, arsip, dokumen, tulisan, angka, dan gambar

yang berisi laporan serta informasi yang mendukung penelitian. Dokumentasi ini akan membantu memperkuat data yang dikumpulkan melalui kuesioner dengan menyediakan bukti tambahan dan konteks yang relevan mengenai insiden *ransomware* dan respons pemerintah. (Sugiyono, 2016)

1.7.7 Analisis Data

Analisis deskriptif adalah metode yang digunakan untuk menggambarkan data yang telah dikumpulkan secara objektif, tanpa membuat kesimpulan umum. Teknik ini melibatkan penyajian data dalam bentuk tabel, grafik, atau diagram untuk menunjukkan bagaimana distribusi frekuensi terjadi, serta nilai-nilai statistik seperti rata-rata, median, modus, dan ukuran-ukuran deskriptif lainnya. Dengan menggunakan analisis ini, kita dapat memahami pola dan karakteristik utama dari data tanpa melakukan inferensi lebih lanjut.

1.7.8 Uji Instrumen

Uji instrumen merupakan langkah penting dalam penelitian untuk memastikan bahwa instrumen pengumpulan data yang digunakan valid dan reliabel. Validitas dan reliabilitas adalah dua komponen utama yang menentukan kualitas instrumen penelitian. Validitas mengukur sejauh mana instrumen benar-benar mengukur apa yang seharusnya diukur, sedangkan reliabilitas mengukur konsistensi instrumen dalam menghasilkan hasil yang sama pada berbagai kesempatan.

1) Uji Validitas

Validitas isi menilai sejauh mana isi dari suatu instrumen mencakup seluruh aspek konsep yang diukur. Proses validasi isi dilakukan dengan meminta pendapat dari ahli atau pakar dalam bidang yang relevan untuk menilai apakah setiap item dalam instrumen sudah sesuai dengan tujuan penelitian. Menurut Sugiyono (2016), Valid berarti menunjukkan derajat ketepatan antara data yang benar terjadi pda objek data.

2) Uji Reliabilitas

Menurut Sugiyono (2016), hasil penelitian dianggap reliabel apabila data yang diperoleh konsisten dalam berbagai waktu yang berbeda. Sebuah instrumen dikatakan reliabel jika ketika digunakan berulang kali untuk mengukur objek yang sama, hasilnya tetap konsisten dan tidak berubah.

Dalam pengujian validitas terhadap kuesioner, terdapat dua jenis validitas, yaitu validitas faktor dan validitas item. Validitas faktor diukur jika item yang disusun menggunakan lebih dari satu faktor yang memiliki kesamaan antar faktor. Pengukuran validitas faktor dilakukan dengan cara mengkorelasikan skor faktor (penjumlahan item dalam satu faktor) dengan skor total faktor (total keseluruhan faktor).

Validitas item diindikasikan oleh adanya korelasi atau dukungan terhadap item total (skor total). Perhitungan ini

dilakukan dengan mengkorelasikan skor item dengan skor total item. Jika lebih dari satu faktor digunakan, maka validitas item diuji dengan cara mengkorelasikan skor item dengan skor faktor, kemudian dilanjutkan dengan mengkorelasikan skor item dengan skor total faktor (penjumlahan dari beberapa faktor).

Hasil perhitungan korelasi akan menghasilkan suatu koefisien korelasi yang digunakan untuk mengukur tingkat validitas suatu item dan menentukan apakah suatu item layak digunakan atau tidak. Penentuan kelayakan item biasanya dilakukan melalui uji signifikansi koefisien korelasi pada taraf signifikansi 0,05. Artinya, suatu item dianggap valid jika berkorelasi signifikan terhadap skor total.

Untuk melakukan uji validitas ini, menggunakan program SPSS. Teknik pengujian yang digunakan adalah menggunakan korelasi Bivariate Pearson (Produk Momen Pearson). Analisis ini dilakukan dengan mengkorelasikan masing-masing skor item dengan skor total. Skor total adalah penjumlahan dari keseluruhan item. Item-item pertanyaan yang berkorelasi signifikan dengan skor total menunjukkan bahwa item-item tersebut mampu memberikan dukungan dalam mengungkap apa yang ingin diungkap, sehingga dinyatakan valid. Jika r hitung ≥ r tabel (uji 2 sisi dengan sig. 0,05), maka instrumen atau item-item pertanyaan tersebut berkorelasi signifikan terhadap skor total dan dinyatakan valid.

1.7.9 Uji Asumsi Klasik

Uji asumsi klasik merupakan syarat statistik yang harus dipenuhi dalam analisis regresi linear berganda berbasis Ordinary Least Squares (OLS). Untuk memastikan bahwa model regresi yang dihasilkan adalah model terbaik, yang akurat dalam estimasi, tidak bias, dan konsisten, maka perlu dilakukan pengujian asumsi klasik (Juliandi et al., 2016). Pengujian ini dilakukan untuk memastikan bahwa koefisien regresi tidak bias, konsisten, dan memiliki ketepatan dalam estimasi. Uji asumsi klasik memastikan bahwa analisis telah lolos dari uji normalitas, multikolinearitas, dan heteroskedastisitas, sehingga analisis regresi linear dapat dilakukan dengan valid. Berikut adalah penjelasan dari masing-masing uji asumsi klasik yang dilakukan dalam penelitian ini:

a. Uji Normalitas

Uji normalitas bertujuan untuk memeriksa apakah data residual dalam model regresi berdistribusi normal. Distribusi normal pada data residual adalah asumsi penting dalam analisis regresi klasik karena mempengaruhi validitas inferensi statistik.

Menurut Ghozali (2016), uji normalitas bertujuan untuk mengevaluasi apakah dalam suatu model regresi, variabel independen dan dependen, atau keduanya, memiliki distribusi normal atau tidak. Jika suatu variabel tidak berdistribusi secara normal, maka hasil uji statistik akan mengalami penurunan kualitas. Uji normalitas data dapat dilakukan menggunakan uji

One Sample Kolmogorov-Smirnov. Ketentuannya adalah jika nilai signifikansi di atas 5% atau 0,05, maka data tersebut memiliki distribusi normal. Sebaliknya, jika hasil uji One Sample Kolmogorov-Smirnov menunjukkan nilai signifikansi di bawah 5% atau 0,05, maka data tersebut tidak memiliki distribusi normal. Hipotesis dalam uji normalitas Kolmogorov-Smirnov adalah sebagai berikut:

H0: Data residual memiliki distribusi normal.

Ha: Data residual tidak memiliki distribusi normal.

Pengambilan keputusan didasarkan pada nilai signifikansi (Sig.):

3) Jika Sig. (2-tailed) < 0,05, maka H0 ditolak, yang berarti data residual tidak berdistribusi normal.
4) Jika Sig. (2-tailed) > 0,05, maka H0 tidak ditolak, yang berarti data residual berdistribusi normal.

1.7.10 Uji Hipotesis

Menurut Neuman, W. L. (2019) Hipotesis adalah pernyataan tentang hubungan antara dua atau lebih variabel yang diuji dalam sebuah penelitian. Hipotesis digunakan untuk mengarahkan proses pengumpulan data dan untuk menentukan apakah hasil penelitian mendukung atau menolak hubungan yang diusulkan.

a) Analisis regresi linier sederhana

Analisis regresi linier sederhana bertujuan untuk menilai sejauh mana variabel independen mempengaruhi variabel dependen. Teknik ini digunakan untuk mengukur seberapa besar hubungan antara variabel bebas dan variabel terikat, serta untuk memproyeksikan nilai variabel terikat berdasarkan variabel bebas yang diberikan. Menurut Ghozali (2021), regresi ini dimaksudkan untuk mengevaluasi dampak langsung variabel independen terhadap variabel dependen dalam konteks penelitian.

b) Uji T

Menurut Ghozali (2016) Uji T adalah metode yang digunakan untuk menguji signifikansi dari perbedaan antara dua rata-rata sampel. Ini sering digunakan dalam analisis data untuk menentukan apakah perbedaan yang diamati antara dua kelompok sampel adalah signifikan secara statistik atau hanya terjadi secara kebetulan.

T-statistics adalah nilai yang digunakan untuk menilai tingkat signifikansi dalam pengujian hipotesis melalui prosedur bootstrapping. Dalam konteks ini, signifikansi dianggap tercapai jika nilai T-statistics melebihi ambang 1,96, sedangkan jika nilainya kurang dari 1,96, signifikansi tidak tercapai (Ghozali, 2016).

Dalam konteks pengambilan keputusan berdasarkan uji t, seperti yang dijelaskan oleh Ghozali (2016), kriteria berikut berlaku:

Jika nilai signifikansi uji t > 0,05, maka hipotesis nol (H_0) diterima dan hipotesis alternatif (Ha) ditolak. Ini mengindikasikan bahwa tidak ada bukti yang cukup untuk menolak bahwa tidak ada pengaruh antara variabel independen terhadap variabel dependen.

Jika nilai signifikansi uji t < 0,05, maka hipotesis nol (H_0) ditolak dan hipotesis alternatif (Ha) diterima. Hal ini menunjukkan bahwa terdapat bukti yang cukup untuk menolak bahwa tidak ada pengaruh antara variabel independen terhadap variabel dependen.

Dengan tingkat kepercayaan sebesar 95% atau taraf signifikansi sebesar 5% ($\alpha = 0,05$), batasan ini digunakan untuk menentukan apakah hasil regresi secara statistik signifikan atau tidak.

BAB II

GAMBARAN UMUM OBJEK PENELITIAN

2.1 Kementerian Komunikasi dan Informatika (Kominfo)

2.1.1 Sejarah dan Latar Belakang Pembentukan Kominfo

Kementerian Komunikasi dan Informatika (Kominfo) merupakan lembaga pemerintah yang memiliki peran strategis dalam mengelola urusan komunikasi, informatika, dan penyiaran di Indonesia. Lembaga ini dibentuk sebagai jawaban atas perkembangan pesat teknologi informasi serta kebutuhan akan tata kelola informasi dan komunikasi yang terpusat. Berdiri secara resmi melalui Keputusan Presiden Nomor 9 Tahun 2005 dan Peraturan Presiden Nomor 22 Tahun 2005, Kominfo menyatukan berbagai fungsi yang sebelumnya tersebar di sejumlah lembaga, seperti Departemen Penerangan dan Direktorat Jenderal Pos dan Telekomunikasi. Kominfo lahir sebagai bentuk adaptasi pemerintah terhadap realitas globalisasi dan digitalisasi yang menuntut efisiensi serta perlindungan terhadap informasi publik dan sistem komunikasi negara.

2.1.2 Tugas dan Fungsi Kominfo

Kominfo memiliki mandat untuk mengatur dan mengawasi sektor komunikasi dan informatika secara nasional. Tugas-tugas tersebut meliputi pengaturan penyiaran, pengelolaan telekomunikasi, penyebaran informasi publik, perlindungan data pribadi, serta pengawasan terhadap konten digital. Lembaga ini juga menjalankan fungsi edukatif melalui peningkatan literasi digital masyarakat, serta membangun infrastruktur TIK yang merata di seluruh wilayah Indonesia. Unit-unit penting di bawah Kominfo seperti Direktorat Jenderal Aplikasi

Informatika (Ditjen Aptika), Direktorat Jenderal Informasi dan Komunikasi Publik, dan Badan Aksesibilitas Telekomunikasi dan Informasi (BAKTI) menjalankan berbagai program yang bertujuan untuk memperkuat posisi Indonesia dalam era digital.

2.1.3 Peran Kominfo dalam Era Digital dan Keamanan Siber

Di tengah transformasi digital, Kominfo juga dihadapkan pada tantangan serius terkait keamanan siber. Salah satu langkah strategis pemerintah adalah pembangunan Pusat Data Nasional (PDN) sebagai pusat penyimpanan data milik instansi pemerintah. Namun, insiden peretasan terhadap PDN yang terjadi pada pertengahan 2024 menjadi bukti nyata bahwa keamanan data nasional masih rentan terhadap serangan siber, seperti *ransomware*. Kejadian tersebut menimbulkan gangguan terhadap sejumlah layanan publik dan memunculkan kekhawatiran masyarakat terkait keamanan data pribadi serta kemampuan pemerintah dalam mengatasi krisis digital. Kominfo, sebagai lembaga yang bertanggung jawab di bidang ini, menjadi sorotan utama publik. Tidak hanya dalam hal teknis penanganan, tetapi juga dalam aspek komunikasi krisis dan transparansi informasi yang disampaikan ke masyarakat.

2.1.4 Kominfo di Tingkat Daerah: Peran Diskominfo

Di level daerah, Kominfo diwakili oleh Dinas Komunikasi dan Informatika (Diskominfo) yang berada di tiap provinsi, kabupaten, dan kota, termasuk di Kota Semarang. Diskominfo Kota Semarang memiliki peran dalam menyebarluaskan informasi publik daerah, mengelola sistem komunikasi pemerintahan lokal, dan

mendukung infrastruktur digital daerah. Namun, dalam konteks insiden serangan PDN yang berdampak secara nasional, kewenangan daerah terbatas dalam penanganan langsung. Diskominfo tidak memiliki akses penuh terhadap sistem pusat yang diretas, sehingga tidak dapat sepenuhnya mencegah atau memperbaiki dampak yang ditimbulkan. Hal ini menimbulkan keresahan dan pertanyaan di masyarakat lokal, khususnya terkait perlindungan data mereka dan sejauh mana pemerintah pusat maupun daerah mampu menjamin keamanan informasi di era digital. Oleh karena itu, persepsi dan kepercayaan masyarakat terhadap Kominfo menjadi penting untuk dikaji, khususnya di tengah krisis seperti insiden *ransomware* yang menyerang sistem nasional. 2.2 Gambaran Umum Kota Semarang

2.2 Kota Semarang

2.2.1 Sejarah dan Letak Geografis

Kota Semarang merupakan ibu kota Provinsi Jawa Tengah yang memiliki posisi strategis di jalur pantai utara Pulau Jawa. Secara geografis, kota ini terletak antara 6°50' – 7°10' Lintang Selatan dan 109°35' – 110°50' Bujur Timur. Wilayahnya terbentang dari kawasan dataran rendah di sisi utara hingga perbukitan di sisi selatan. Semarang tidak hanya menjadi pusat pemerintahan provinsi, tetapi juga berperan sebagai simpul ekonomi, pendidikan, budaya, dan transportasi di wilayah Jawa Tengah. Secara historis, Semarang berkembang sejak masa kolonial sebagai pelabuhan perdagangan penting, dan kini terus bertransformasi menjadi kota metropolitan yang modern namun tetap mempertahankan nilai-nilai kulturalnya.

2.2.2 Kondisi Demografi dan Sosial

Berdasarkan data Badan Pusat Statistik (BPS) Kota Semarang, jumlah penduduk pada tahun terakhir tercatat lebih dari 1,6 juta jiwa, dengan komposisi usia produktif yang dominan. Masyarakat Kota Semarang dikenal heterogen, terdiri dari berbagai latar belakang suku, agama, dan budaya, yang hidup berdampingan secara harmonis. Tingkat pendidikan penduduk juga cukup tinggi, dengan akses terhadap informasi dan teknologi digital yang semakin luas. Hal ini membuat masyarakat Semarang menjadi salah satu komunitas urban yang cukup responsif terhadap isu-isu sosial maupun kebijakan publik, termasuk dalam hal pelayanan digital dan keamanan informasi.

2.2.3 Perkembangan Digitalisasi dan Layanan Publik

Sebagai kota besar yang tengah bertransformasi menuju smart city, Semarang telah mengembangkan berbagai layanan publik berbasis digital, seperti sistem perizinan online, pelaporan masyarakat melalui aplikasi, serta integrasi data antar-instansi daerah. Pemerintah Kota Semarang, melalui Dinas Komunikasi dan Informatika (Diskominfo), berperan aktif dalam mengembangkan infrastruktur teknologi informasi dan komunikasi guna meningkatkan kualitas pelayanan publik. Penerapan sistem informasi terintegrasi juga menjadikan data sebagai aset penting dalam pengambilan kebijakan. Namun, di balik kemajuan ini, tantangan dalam hal keamanan siber juga meningkat. Ketergantungan pada sistem digital membuat Kota Semarang turut terdampak secara tidak langsung ketika sistem pusat seperti Pusat Data Nasional mengalami gangguan akibat serangan siber.

2.2.4 Signifikansi Penelitian di Kota Semarang

Kota Semarang menjadi wilayah yang relevan untuk diteliti dalam konteks persepsi dan kepercayaan masyarakat terhadap keamanan data digital. Sebagai kota dengan populasi besar, tingkat digitalisasi yang tinggi, serta keberadaan Diskominfo yang aktif, masyarakatnya memiliki ekspektasi terhadap keamanan dan keandalan sistem layanan publik. Insiden peretasan terhadap PDN pada tahun 2024 memicu keresahan, terutama karena sejumlah layanan yang menggunakan sistem nasional mengalami gangguan. Oleh karena itu, penelitian mengenai bagaimana masyarakat Kota Semarang memandang kemampuan pemerintah dalam menangani insiden ini, serta sejauh mana kepercayaan mereka terhadap Kominfo, menjadi penting sebagai cerminan kepercayaan publik di tingkat kota besar.

2.3 Serangan Siber *Ransomware*

2.3.1 Definisi dan Karakteristik Umum

Ransomware merupakan salah satu jenis malware yang bertujuan untuk mengenkripsi atau membatasi akses ke data maupun sistem komputer milik korban. Pelaku di balik serangan ini biasanya meminta tebusan dalam bentuk mata uang digital sebagai syarat untuk mengembalikan akses atau data kepada pemiliknya. (Simorangkir, Sihombing, Intani, & Parhusip, 2024)

2.3.2 Mekanisme Serangan

Serangan *ransomware* biasanya dimulai dengan penyusupan malware ke dalam sistem target melalui berbagai metode, seperti email phishing, situs web berbahaya, atau eksploitasi kerentanan sistem. Setelah berhasil masuk, *ransomware*

akan mengenkripsi data penting dan menampilkan pesan yang meminta pembayaran tebusan untuk mendapatkan kunci dekripsi.

BAB III

TEMUAN PENELITIAN

Pada bab ini akan diuraikan temuan data yang diperoleh langsung peneliti dari hasil penelitian lapangan. Temuan penelitian ini adalah informasi yang diperoleh dari pengumpulan informasi dari tanggapan responden melalui berbagai pendapat yang dilakukan oleh peneliti terkait temuan penelitian mengenai "**Pengaruh Serangan Siber *Ransomware* Yang Menyerang Pusat Data Nasional Terhadap Persepsi Dan Kepercayaan Masyarakat Kota Semarang Pada Kominfo."** Hasil penyebaran kuisioner dapat dilihat lengkap sebagai berikut:

3.1 Karakteristik Responden

Responden dalam penelitian ini merupakan masyarakat Kota Semarang yang berusia antara 18 hingga 45 tahun. Rentang usia ini dipilih dengan pertimbangan bahwa kelompok usia tersebut dinilai lebih relevan dan responsif terhadap isu-isu digital, khususnya terkait keamanan data dan serangan siber *ransomware*. Selain itu, individu dalam kelompok usia ini umumnya memiliki tingkat literasi digital yang memadai, serta lebih aktif menggunakan layanan berbasis teknologi informasi. Sementara itu, kelompok usia lanjut tidak dijadikan fokus utama dalam penelitian ini karena terdapat kecenderungan kurangnya pemahaman atau ketertarikan terhadap isu teknis seperti serangan pada Pusat Data Nasional (PDN), yang dapat memengaruhi keakuratan data yang diperoleh dalam penelitian ini.

3.1.1 Jenis Kelamin

Berdasarkan hasil survei yang dilakukan terhadap 100 responden, diketahui bahwa sebanyak 53 orang (53%) adalah laki-laki, sedangkan 47 orang (47%) adalah perempuan. Hal ini menunjukkan bahwa partisipasi dalam penelitian ini cukup seimbang antara kedua jenis kelamin. Perbedaan proporsi yang tidak terlalu signifikan ini juga menunjukkan bahwa baik laki-laki maupun perempuan memiliki tingkat kepedulian yang relatif sama terhadap isu keamanan data pribadi dan serangan siber.

Keseimbangan ini penting untuk menghasilkan data yang tidak bias gender, terutama dalam konteks persepsi dan kepercayaan masyarakat terhadap penanganan pemerintah dalam menghadapi krisis siber. Baik laki-laki maupun perempuan dalam rentang usia tersebut kemungkinan besar memiliki pengalaman langsung atau tidak langsung dalam menggunakan layanan digital pemerintah yang terintegrasi dengan PDN.

Tabel 3. 1

Kelompok Jenis Kelamin

Jenis Kelamin	Frekuensi	Persen	Valid Percent	Cumulative Percent
Laki-laki	53	53.0	53.0	53.0
Perempuan	47	47.0	47.0	100.0
Total	100	100.0	100.0	

3.1.2 Kelompok Usia

Dalam hal distribusi usia, responden terbagi ke dalam tiga kelompok besar. Kelompok usia 18–25 tahun mencakup 37 orang (37%), yang terdiri dari kalangan remaja akhir hingga dewasa awal. Kelompok ini cenderung merupakan mahasiswa, pelajar, atau pekerja pemula yang aktif menggunakan layanan digital dan media sosial.

Kelompok berikutnya adalah usia 26–35 tahun yang mendominasi jumlah responden dengan total 43 orang (43%). Mereka merupakan generasi dewasa muda yang umumnya telah bekerja dan bergantung pada sistem digital untuk menunjang aktivitas sehari-hari, baik secara profesional maupun personal. Persepsi dari kelompok usia ini sangat penting karena mereka berada pada masa pengambilan keputusan ekonomi dan sosial yang aktif.

Tabel 3. 2

Kelompok Umur

Kelompok Usia	Frekuensi	Persen	Valid Percent	Cumulative Percent
18 - 25 tahun	37	37.0	37.0	37.0
26 - 35 tahun	43	43.0	43.0	80.0
36 - 45 tahun	20	20.0	20.0	100.0
Total	100	100.0	100.0	

Sedangkan kelompok usia 36–45 tahun terdiri dari 20 orang (20%). Distribusi usia ini memberikan cakupan yang cukup representatif dan komprehensif dalam memahami persepsi serta tingkat kepercayaan masyarakat lintas generasi,

khususnya yang memiliki akses dan ketergantungan tinggi terhadap teknologi informasi.

3.1.3 Domisili

Sebaran wilayah tempat tinggal para responden juga menjadi salah satu faktor penting dalam menilai keragaman sudut pandang terhadap isu yang diteliti. Dalam penelitian ini, responden berasal dari berbagai kecamatan yang ada di Kota Semarang. Wilayah Genuk merupakan yang paling banyak menyumbang responden, yaitu sebanyak 21 orang (21%). Hal ini bisa disebabkan oleh karakter wilayah tersebut yang padat penduduk atau mudah dijangkau secara komunikasi.

Selain Genuk, beberapa wilayah dengan jumlah responden cukup tinggi antara lain Candisari dan Tembalang masing-masing dengan 8 responden (8%), serta Pedurungan dan Semarang Selatan masing-masing 6 responden (6%). Wilayah lainnya seperti Banyumanik, Gajahmungkur, Gayamsari, Gunungpati, Mijen, Ngaliyan, Semarang Barat, Semarang Tengah, Semarang Timur, Semarang Utara, dan Tugu memiliki kontribusi responden antara 2 hingga 5 orang.

Penyebaran ini menunjukkan bahwa pengumpulan data dilakukan dengan mempertimbangkan keterwakilan dari seluruh kecamatan di Kota Semarang. Dengan begitu, hasil penelitian ini diharapkan mampu menggambarkan persepsi dan kepercayaan masyarakat secara lebih menyeluruh, tidak hanya terfokus pada satu wilayah tertentu saja.

Tabel 3. 3

Domisili

Domisili	Frekuensi	Persen	Valid Percent	Cumulative Percent
Banyumanik	6	6.0	6.0	6.0
Candisari	8	8.0	8.0	14.0
Gajahmungkur	5	5.0	5.0	19.0
Gayamsari	4	4.0	4.0	23.0
Genuk	21	21.0	21.0	44.0
Gunungpati	4	4.0	4.0	48.0
Mijen	5	5.0	5.0	53.0
Ngaliyan	6	6.0	6.0	59.0
Pedurungan	6	6.0	6.0	65.0
Semarang Barat	4	4.0	4.0	69.0
Semarang Selatan	6	6.0	6.0	75.0
Semarang Tengah	2	2.0	2.0	77.0
Semarang Timur	8	8.0	8.0	85.0
Semarang Utara	4	4.0	4.0	89.0
Tembalang	8	8.0	8.0	97.0
Tugu	3	3.0	3.0	100.0
Total	100	100.0	100.0	

3.2 Deskripsi Variabel Penelitian

Penelitian ini menggunakan tiga variabel utama, yaitu Serangan *Ransomware* terhadap Pusat Data Nasional (PDN) sebagai variabel independen (X), serta dua variabel dependen yaitu Persepsi Masyarakat (Y1) dan Kepercayaan Masyarakat (Y2). Masing-masing variabel dijelaskan melalui sejumlah indikator yang disusun dalam bentuk pernyataan dan diukur dengan skala Likert.

3.2.1 Deskripsi Variabel Serangan *Ransomware* yang menyerang PDN (X)

Variabel Serangan *Ransomware* terhadap PDN sebagai variabel independen mengacu pada sejauh mana masyarakat mengetahui, memahami, serta merasakan dampak dari peristiwa serangan siber yang menargetkan pusat data milik pemerintah. Insiden ini menyebabkan terganggunya berbagai layanan publik yang bergantung pada sistem digital. Dalam penelitian ini, variabel tersebut mencerminkan tingkat pengetahuan masyarakat terhadap insiden tersebut, tingkat kewaspadaan mereka terhadap ancaman siber, serta penilaian mereka terhadap dampak serangan terhadap pelayanan publik dan respon awal pemerintah dalam menangani krisis. Hasil kuisioner X1 dengan 4 pertanyaan sebagai berikut :

Tabel 3. 4 Hasil distribusi jawaban terhadap pernyataan "Saya menilai insiden serangan ransomware pada PDN sebagai hal yang sangat serius"

Valid	Jawaban	Frequency	Percent	Cumulative Percent	Mayoritas
Valid	Sangat Tidak Setuju	1	1.0%	1.0%	Setuju
Valid	Tidak Setuju	0	0.0%	1.0%	
Valid	Netral	7	7.0%	8.0%	
Valid	**Setuju**	**61**	**61.0%**	**69.0%**	
Valid	Sangat Setuju	31	31.0%	100.0%	
	Total	100	100.0%	100.0%	

Berdasarkan hasil distribusi jawaban terhadap pernyataan "Saya menilai insiden serangan *ransomware* pada PDN sebagai hal yang sangat serius", mayoritas responden menunjukkan sikap yang serius dan peduli terhadap kejadian tersebut. Sebanyak 61 responden (61%) menyatakan setuju, dan 31 responden (31%) sangat setuju, yang secara keseluruhan mencerminkan bahwa 92% responden menilai insiden ini sebagai permasalahan serius yang perlu mendapat perhatian.

Sementara itu, hanya 7 responden (7%) yang bersikap netral, dan 1 responden (1%) yang sangat tidak setuju terhadap pernyataan tersebut. Hal ini menunjukkan bahwa hanya sebagian sangat kecil dari responden yang tidak melihat insiden ini sebagai isu yang penting.

Secara keseluruhan, data ini memperkuat pemahaman bahwa masyarakat Kota Semarang, khususnya dalam rentang usia produktif, memiliki tingkat kesadaran yang cukup tinggi terhadap dampak dan urgensi dari insiden serangan siber pada Pusat Data Nasional.

Tabel 3. 5 Hasil distribusi jawaban terhadap pernyataan "Serangan Ransomware ini perlu segera ditangani oleh pemerintah"

Valid	Jawaban	Frequency	Percent	Cumulative Percent	Mayoritas
Valid	Sangat Tidak Setuju	0	0.0%	0.0%	Sangat Setuju
Valid	Tidak Setuju	0	0.0%	0.0%	
Valid	Netral	1	1.0%	1.0%	
Valid	Setuju	35	35.0%	36.0%	
Valid	**Sangat Setuju**	**64**	**64.0%**	**100.0%**	
	Total	100	100.0%	100.0%	

Berdasarkan data diatas, mayoritas responden menunjukkan kepedulian yang sangat tinggi terhadap insiden serangan *ransomware* yang menyerang Pusat Data Nasional. Hal ini terlihat dari jawaban responden atas pernyataan "Serangan *ransomware* ini perlu segera ditangani oleh pemerintah", di mana sebanyak 64 responden (64,0%) menjawab sangat setuju, dan 35 responden (35,0%) menjawab setuju. Sementara itu, hanya 1 responden (1,0%) yang memilih netral, dan tidak ada responden yang menyatakan tidak setuju atau sangat tidak setuju. Dengan demikian, total 99% responden sepakat bahwa penanganan terhadap serangan ini merupakan hal yang sangat penting dan mendesak. Temuan ini memperkuat pandangan bahwa

masyarakat Kota Semarang memiliki harapan besar terhadap peran aktif pemerintah dalam mengatasi krisis siber tersebut secara cepat dan transparan.

Tabel 3. 6 Hasil distribusi jawaban terhadap pernyataan "Menurut saya, sistem keamanan data pemerintah sebelum insiden ini belum cukup kuat."

Valid	Jawaban	Frequency	Percent	Cumulative Percent	Mayoritas
Valid	Sangat Tidak Setuju	1	1.0%	1.0%	Sangat Setuju
Valid	Tidak Setuju	0	0.0%	1.0%	
Valid	Netral	7	7.0%	8.0%	
Valid	Setuju	12	12.0%	20.0%	
Valid	**Sangat Setuju**	**80**	**80.0%**	**100.0%**	
	Total	100	100.0%	100.0%	

Berdasarkan data dari penyebaran kuesioner, tampak bahwa mayoritas responden memiliki pandangan kritis terhadap kesiapan sistem keamanan data pemerintah sebelum terjadinya insiden serangan *ransomware* pada Pusat Data Nasional. Sebanyak 80 responden (80,0%) menyatakan sangat setuju, dan 12 responden (12,0%) menyatakan setuju. Sementara itu, 7 responden (7,0%) memilih netral, hanya 1 responden (1,0%) yang sangat tidak setuju, dan tidak ada responden yang menjawab tidak setuju. Temuan ini menunjukkan bahwa secara keseluruhan, 92% responden menilai sistem keamanan data pemerintah sebelum insiden belum memadai. Hal ini mencerminkan adanya persepsi publik yang menuntut perbaikan mendasar terhadap sistem keamanan informasi negara, terutama dalam menghadapi potensi serangan siber di masa mendatang.

Tabel 3. 7 Saya khawatir layanan publik seperti administrasi kependudukan dapat terganggu akibat insiden ini.

Valid	Jawaban	Frequency	Percent	Cumulative Percent	Mayoritas
Valid	Sangat Tidak Setuju	0	0.0%	0.0%	Sangat Setuju
Valid	Tidak Setuju	0	0.0%	0.0%	
Valid	Netral	3	3.0%	3.0%	
Valid	Setuju	33	33.0%	36.0%	
Valid	**Sangat Setuju**	**64**	**64.0%**	**100.0%**	
	Total	100	100.0%	100.0%	

Hasil tanggapan responden terhadap pernyataan ini menunjukkan adanya kekhawatiran yang besar dari masyarakat terhadap potensi gangguan layanan publik akibat serangan *ransomware* pada Pusat Data Nasional. Sebanyak 64 responden (64,0%) menyatakan sangat setuju, dan 33 responden (33,0%) menyatakan setuju. Sementara itu, hanya 3 responden (3,0%) memilih netral, dan tidak ada yang menjawab tidak setuju maupun sangat tidak setuju. Secara kumulatif, 97% responden mengungkapkan kekhawatiran mereka terhadap terganggunya layanan publik penting, seperti administrasi kependudukan. Temuan ini menegaskan bahwa insiden keamanan siber tidak hanya dipandang sebagai masalah teknis, tetapi juga berimplikasi langsung terhadap pelayanan masyarakat yang bersifat vital dan sehari-hari.

3.2.2 Deskripsi Variabel Persepsi Masyarakat Kota Semarang (Y_1)

Persepsi Masyarakat sebagai variabel pertama yang dipengaruhi (Y1) menggambarkan bagaimana masyarakat Kota Semarang memandang peristiwa serangan *ransomware* terhadap PDN. Persepsi ini mencakup sejauh mana masyarakat memahami isu yang terjadi, reaksi emosional mereka terhadap insiden, pandangan terhadap transparansi informasi dari pemerintah, dan bagaimana mereka

menyikapi ancaman serupa di masa mendatang. Variabel ini penting untuk mengetahui sejauh mana masyarakat merasa dilibatkan atau terinformasi dalam konteks gangguan layanan publik akibat serangan siber.

Tabel 3. 8 Saya menilai insiden ini berdasarkan berita dan data yang saya baca.

Valid	Jawaban	Frequency	Percent	Cumulative Percent	Mayoritas
Valid	Sangat Tidak Setuju	0	0.0%	0.0%	Setuju
Valid	Tidak Setuju	0	0.0%	0.0%	
Valid	Netral	4	4.0%	4.0%	
Valid	**Setuju**	**62**	**62.0%**	**66.0%**	
Valid	Sangat Setuju	34	34.0%	100.0%	
	Total	100	100.0%	100.0%	

Berdasarkan hasil kuesioner, dapat diketahui bahwa sebagian besar responden dalam penelitian ini membentuk penilaiannya terhadap insiden serangan *ransomware* pada Pusat Data Nasional berdasarkan sumber berita dan data yang mereka baca. Hal ini terlihat dari 62 responden (62,0%) yang menjawab setuju dan 34 responden (34,0%) yang menjawab sangat setuju. Hanya 4 responden (4,0%) yang memilih netral, sementara tidak ada responden yang menyatakan tidak setuju atau sangat tidak setuju. Temuan ini menunjukkan bahwa masyarakat Kota Semarang umumnya cukup aktif dalam mengakses informasi seputar isu nasional melalui media, baik itu media daring maupun cetak. Hal ini penting, karena persepsi yang terbentuk dari sumber informasi yang akurat dapat mencerminkan tingkat literasi digital dan kewaspadaan masyarakat terhadap isu-isu siber yang berkembang.

Tabel 3. 9 Saya merasa data pribadi saya tidak lagi aman setelah insiden ini.

Valid	Jawaban	Frequency	Percent	Cumulative Percent	Mayoritas
Valid	Sangat Tidak Setuju	1	1.0%	1.0%	Setuju
Valid	Tidak Setuju	0	0.0%	1.0%	
Valid	Netral	3	3.0%	4.0%	
Valid	**Setuju**	**49**	**49.0%**	**53.0%**	
Valid	Sangat Setuju	47	47.0%	100.0%	
	Total	100	100.0%	100.0%	

Hasil penyebaran kuesioner menunjukkan bahwa sebagian besar masyarakat Kota Semarang memiliki kekhawatiran terhadap keamanan data pribadi mereka pasca insiden serangan *ransomware* pada Pusat Data Nasional. Sebanyak 49 responden (49,0%) menyatakan setuju dan 47 responden (47,0%) menyatakan sangat setuju. Hanya 3 responden (3,0%) yang bersikap netral, dan 1 responden (1,0%) menyatakan sangat tidak setuju. Tidak ada responden yang menjawab tidak setuju. Dengan demikian, sebanyak 96% responden menunjukkan adanya kekhawatiran atau hilangnya rasa aman terhadap perlindungan data pribadi mereka. Temuan ini menggambarkan bahwa insiden tersebut telah menurunkan rasa percaya publik terhadap sistem keamanan data yang dikelola pemerintah dan menimbulkan ketidakpastian dalam hal perlindungan informasi pribadi warga.

Tabel 3. 10 Saya semakin khawatir data saya bisa bocor setelah serangan ini.

Valid	Jawaban	Frequency	Percent	Cumulative Percent	Mayoritas
Valid	Sangat Tidak Setuju	1	1.0%	1.0%	Sangat Setuju
Valid	Tidak Setuju	0	0.0%	0.0%	
Valid	Netral	5	5.0%	6.0%	
Valid	Setuju	33	33.0%	39.0%	
Valid	**Sangat Setuju**	**61**	**61.0%**	**100.0%**	
	Total	100	100.0%	100.0%	

Berdasarkan data yang diperoleh dari kuesioner, terlihat bahwa tingkat kekhawatiran masyarakat Kota Semarang terhadap kemungkinan kebocoran data pribadi pasca serangan *ransomware* pada Pusat Data Nasional sangat tinggi. Hal ini ditunjukkan oleh 61 responden (61,0%) yang sangat setuju dan 33 responden (33,0%) yang setuju terhadap pernyataan ini. Sementara itu, hanya 5 responden (5,0%) yang memilih netral, dan hanya 1 responden (1,0%) yang sangat tidak setuju. Tidak ada responden yang menyatakan tidak setuju. Dengan demikian, sebanyak 94% responden menunjukkan tingkat kekhawatiran yang signifikan terhadap potensi kebocoran data mereka. Angka ini menunjukkan bahwa insiden tersebut benar-benar memberikan dampak psikologis dan persepsi negatif terhadap sistem pengamanan data yang dikelola oleh pemerintah.

Tabel 3. 11 Saya merasa pemerintah belum cukup siap secara teknis dalam menghadapi serangan seperti ini.

Valid	Jawaban	Frequency	Percent	Cumulative Percent	Mayoritas
Valid	Sangat Tidak Setuju	2	2.0%	2.0%	Sangat Setuju
Valid	Tidak Setuju	0	0.0%	2.0%	
Valid	Netral	5	5.0%	7.0%	
Valid	Setuju	44	44.0%	51.0%	
Valid	**Sangat Setuju**	**49**	**49.0%**	**100.0%**	
	Total	100	100.0%	100.0%	

Hasil kuesioner menunjukkan bahwa sebagian besar masyarakat Kota Semarang meragukan kesiapan teknis pemerintah dalam menghadapi serangan siber seperti *ransomware* yang menyerang Pusat Data Nasional. Tercatat 49 responden (49,0%) menyatakan sangat setuju dan 44 responden (44,0%) setuju dengan pernyataan tersebut, sehingga secara keseluruhan 93% responden memiliki pandangan kritis terhadap kesiapan pemerintah. Sementara itu, hanya 5 responden (5,0%) yang bersikap netral dan 2 responden (2,0%) yang sangat tidak setuju. Tidak ada responden yang menyatakan tidak setuju. Data ini menggambarkan bahwa kepercayaan masyarakat terhadap kemampuan teknis pemerintah dalam menangani insiden siber masih perlu ditingkatkan. Ketidaksiapan yang dirasakan ini juga dapat memperbesar kekhawatiran masyarakat atas pengelolaan data digital oleh negara.

3.2.3 Deskripsi Variabel Kepercayaan Masyarakat Kota Semarang (Y_2)

Variabel kedua yang dipengaruhi (Y2) adalah Kepercayaan Masyarakat. Kepercayaan ini mencerminkan keyakinan masyarakat terhadap kemampuan pemerintah, khususnya Kementerian Komunikasi dan Informatika (Kominfo), dalam menangani insiden serta menjaga keamanan data publik di masa mendatang. Dalam hal ini, kepercayaan masyarakat diukur melalui keyakinan mereka

terhadap kapasitas pemerintah dalam mengatasi serangan siber, perlindungan terhadap data pribadi, serta harapan akan peningkatan sistem keamanan digital nasional.

Tabel 3. 12 Saya percaya pemerintah bisa mengatasi serangan siber semacam ini di masa depan.

Valid	Jawaban	Frequency	Percent	Cumulative Percent	Mayoritas
Valid	Sangat Tidak Setuju	4	4.0%	4.0%	Setuju
Valid	Tidak Setuju	17	17.0%	21.0%	
Valid	Netral	13	13.0%	34.0%	
Valid	**Setuju**	**43**	**43.0%**	**77.0%**	
Valid	Sangat Setuju	23	23.0%	100.0%	
	Total	100	100.0%	100.0%	

Data hasil kuesioner menunjukkan bahwa masyarakat Kota Semarang memiliki tingkat kepercayaan yang cukup beragam terhadap kemampuan pemerintah dalam mengatasi serangan siber di masa depan. Mayoritas responden, yaitu 43 orang (43,0%), menyatakan setuju, dan 23 orang (23,0%) sangat setuju, sehingga total 66% responden memiliki optimisme terhadap pemerintah. Namun demikian, terdapat juga 13 responden (13,0%) yang bersikap netral, serta 17 responden (17,0%) yang tidak setuju dan 4 responden (4,0%) yang sangat tidak setuju. Meskipun mayoritas bersikap positif, data ini juga mengindikasikan adanya keraguan dari sebagian masyarakat terhadap kesiapan dan komitmen pemerintah dalam menangani ancaman serangan siber secara berkelanjutan di masa mendatang. Keberagaman persepsi ini menandakan bahwa pemerintah perlu meningkatkan kepercayaan publik melalui langkah konkret dan transparan dalam penguatan sistem keamanan siber.

Tabel 3. 13 Pemerintah cukup transparan dalam memberikan informasi terkait serangan ini.

Valid	Jawaban	Frequency	Percent	Cumulative Percent	Mayoritas
Valid	Sangat Tidak Setuju	14	14.0%	14.0%	Setuju
Valid	Tidak Setuju	9	9.0%	23.0%	
Valid	Netral	16	16.0%	39.0%	
Valid	**Setuju**	**35**	**35.0%**	**74.0%**	
Valid	Sangat Setuju	26	26.0%	100.0%	
	Total	100	100.0%	100.0%	

Berdasarkan hasil kuesioner, persepsi masyarakat Kota Semarang terhadap transparansi pemerintah dalam menyampaikan informasi terkait insiden serangan *ransomware* terhadap PDN menunjukkan beragam tanggapan. Sebanyak 35 responden (35,0%) menyatakan setuju dan 26 responden (26,0%) sangat setuju, menunjukkan bahwa 61% responden menganggap pemerintah telah bersikap cukup terbuka. Namun, masih terdapat 16 responden (16,0%) yang bersikap netral, serta 9 responden (9,0%) yang tidak setuju dan 14 responden (14,0%) yang sangat tidak setuju, sehingga 23% dari responden merasakan kurangnya transparansi. Data ini mencerminkan bahwa meskipun mayoritas publik menilai pemerintah cukup transparan, masih ada sekelompok masyarakat yang merasa informasi yang disampaikan belum maksimal. Hal ini menunjukkan perlunya peningkatan komunikasi yang lebih jelas, terbuka, dan terstruktur dari pemerintah kepada publik untuk membangun kepercayaan dan mencegah spekulasi negatif.

Tabel 3. 14 Saya percaya pemerintah menangani krisis ini dengan jujur dan bertanggung jawab.

Valid	Jawaban	Frequency	Percent	Cumulative Percent	Mayoritas
Valid	Sangat Tidak Setuju	15	15.0%	15.0%	Sangat Setuju
Valid	Tidak Setuju	8	8.0%	23.0%	
Valid	Netral	13	13.0%	36.0%	
Valid	Setuju	31	31.0%	67.0%	
Valid	**Sangat Setuju**	**33**	**33.0%**	**100.0%**	
	Total	100	100.0%	100.0%	

Hasil tanggapan responden menunjukkan bahwa persepsi masyarakat Kota Semarang terhadap integritas dan tanggung jawab pemerintah dalam menangani insiden serangan *ransomware* cukup positif, meskipun tidak mutlak. Dari total 100 responden, 31% menyatakan setuju dan 33% sangat setuju, sehingga mayoritas atau 64% percaya bahwa pemerintah menangani krisis ini secara jujur dan bertanggung jawab. Namun demikian, terdapat 13% responden yang bersikap netral, serta 8% tidak setuju dan 15% sangat tidak setuju, yang jika digabungkan mencapai 23% yang meragukan integritas penanganan pemerintah. Hal ini menunjukkan bahwa meskipun kepercayaan publik cukup tinggi, pemerintah tetap perlu memperkuat akuntabilitas dan komunikasi publik agar persepsi negatif yang masih ada bisa ditekan secara maksimal. Keterbukaan dalam menyampaikan fakta dan langkah-langkah penanganan secara konsisten sangat berpengaruh dalam menjaga dan meningkatkan kepercayaan masyarakat.

Tabel 3. 15 Saya yakin pemerintah bisa bekerja sama dengan instansi lain untuk memperbaiki keamanan data.

Valid	Jawaban	Frequency	Percent	Cumulative Percent	Mayoritas
Valid	Sangat Tidak Setuju	4	4.0%	4.0%	Setuju
Valid	Tidak Setuju	15	15.0%	19.0%	
Valid	Netral	7	7.0%	26.0%	
Valid	**Setuju**	**38**	**38.0%**	**64.0%**	
Valid	Sangat Setuju	36	36.0%	100.0%	
	Total	100	100.0%	100.0%	

Tanggapan responden terhadap kemampuan pemerintah dalam menjalin kerja sama lintas instansi untuk memperbaiki keamanan data menunjukkan tingkat optimisme yang cukup tinggi. Dari 100 responden, mayoritas yaitu 38% menyatakan setuju dan 36% sangat setuju, sehingga total 74% meyakini adanya potensi kerja sama yang baik antar lembaga. Sementara itu, 7% responden bersikap netral, dan sisanya yaitu 15% tidak setuju serta 4% sangat tidak setuju, mengindikasikan bahwa masih terdapat keraguan dari sebagian kecil masyarakat terhadap efektivitas kolaborasi antarinstansi. Secara keseluruhan, hasil ini mencerminkan bahwa kepercayaan masyarakat terhadap kolaborasi pemerintah cukup kuat, namun pemerintah tetap perlu menunjukkan komitmen nyata melalui koordinasi dan aksi kolektif yang transparan dalam meningkatkan sistem keamanan data nasional.

3.3 Interval Kelas

Berdasarkan hasil kuisioner yang disebar kepada 100 responden, dapat ditarik kesimpulan mengenai “Pengaruh Serangan Siber *Ransomware* Yang Menyerang Pusat Data Nasional Terhadap Persepsi Dan Kepercayaan Masyarakat Kota Semarang Pada Kominfo.” Maka akan digunakan rumus untuk menghitung

interval sebagai berikut:

$$I = \frac{(A - B) + 1}{K}$$

Keterangan :

I : Interval Kelas

A : Skor Tertinggi

B : Skor Terendah

K : Jumlah Kelas

3.3.1 Interval Kelas Variabel Serangan *Ransomware* yang menyerang PDN (X)

Variabel Serangan *Ransomware* yang menyerang PDN terbagi menjadi nilai terendah 1 dan skor tertinggi 5, berdasarkan jumlah total hasil perhitungan skala likert pada 4 pertanyaan dari 100 responden didapatkan hasil olah data pada table sebagai berikut:

Tabel 3. 16 Kategori Interval

Kategori	Rentang Skor Total	Keterangan
Rendah	4 – 9	Pemahaman masalah kurang
Sedang	10 – 14	Pemahaman masalah sedang
Tinggi	15 – 20	Pemahaman masalah tinggi

Tabel 3. 17 Interval Kelas X

Kategori Skor	Rentang Skor	Frekuensi	Persentase
Rendah	4 – 8	0	0.0%
Sedang	9 – 13	2	2.0%
Tinggi	14 – 20	98	98.0%
Total	-	100	100%

Sebagian besar responden (98%) menilai bahwa serangan *ransomware* terhadap PDN merupakan persoalan yang sangat serius dan memiliki urgensi tinggi. Hanya sebagian kecil (2%) yang menilai masalah ini dalam tingkat sedang. Tidak ada responden yang menganggap persoalan ini berada di tingkat rendah.

3.3.2 Interval Kelas Variabel Persepsi Masyarakat Kota Semarang

Tabel 3. 18 Interval Kelas Y1

Kategori Skor	Rentang Skor	Frekuensi	Persentase
Rendah	4 – 8	0	0.0%
Sedang	9 – 13	6	6.0%
Tinggi	14 – 20	94	94.0%
Total	-	100	100.0%

Sebagian besar responden (94%) memiliki persepsi yang tinggi terhadap keseriusan dan dampak insiden serangan *ransomware* pada Pusat Data Nasional (PDN). Artinya, masyarakat Kota Semarang menyadari bahwa insiden ini merupakan masalah yang penting dan perlu perhatian serius. Hanya 6% yang berada di kategori persepsi sedang, dan tidak ada yang menilai rendah.

3.3.3 Interval Kelas Variabel Kepercayaan Masyarakat Kota Semarang

Tabel 3. 19 Interval Kelas Y2

Kategori Skor	Rentang Skor	Frekuensi	Persentase
Rendah	4 – 8	19	19.0%
Sedang	9 – 13	10	10.0%
Tinggi	14 – 20	71	71.0%
Total	-	100	100.0%

Sebanyak 71% responden memiliki tingkat kepercayaan yang tinggi terhadap kemampuan pemerintah dalam menangani insiden serangan *ransomware* pada PDN. Sementara itu, 10% berada pada tingkat sedang, dan 19% lainnya menunjukkan tingkat kepercayaan yang rendah.

Data ini menunjukkan bahwa meskipun sebagian besar masyarakat optimis terhadap kemampuan pemerintah, masih ada segmen yang meragukan atau belum sepenuhnya yakin terhadap langkah-langkah penanganan yang dilakukan.

BAB IV

HASIL DAN PEMBAHASAN

Penelitian ini merupakan penelitian kuantitatif yang bertujuan untuk mengetahui Pengaruh serangan *ransomware* yang menyerang PDN terhadap Persepsi dan Kepercayaan Masyarakat Kota Semarang terhadap Kominfo. Data diperoleh melalui penyebaran kuesioner kepada 100 responden masyarakat Kota Semarang, yang kemudian dianalisis menggunakan perangkat lunak SPSS versi 22. Penilaian pada kuesioner menggunakan skala Likert dengan rentang skor 1 sampai 5, yaitu:

1. Sangat Tidak Setuju
2. Tidak Setuju
3. Netral
4. Setuju
5. Sangat Setuju

Kuesioner yang disusun terdiri dari tiga variabel:

X: Pengaruh serangan *ransomware* pada Pusat Data Nasional (PDN).

Y1: Persepsi masyarakat Kota Semarang.

Y2: Kepercayaan masyarakat Kota Semarang.

4.1 Hasil

4.1.1 Uji Validitas

Menurut Sugiyono (2016), uji validitas dilakukan untuk mengetahui sejauh mana setiap item pertanyaan dalam kuesioner mampu mengukur apa yang seharusnya diukur, sesuai dengan tujuan penelitian. Validitas berhubungan dengan ketepatan dan ketelitian suatu alat ukur dalam melakukan fungsinya, yaitu mengungkap data dari variabel yang dimaksud secara tepat. Dalam konteks penelitian ini, uji validitas dilakukan untuk memastikan bahwa instrumen yang digunakan dalam bentuk kuesioner benar-benar mampu mengukur persepsi masyarakat terhadap insiden serangan *ransomware* serta dampaknya terhadap kepercayaan terhadap Kominfo.

Uji validitas dalam penelitian ini dilakukan terhadap data yang diperoleh dari 100 responden. Metode analisis yang digunakan untuk menguji validitas adalah korelasi Pearson Product Moment (Bivariate Pearson), yang digunakan untuk mengukur hubungan antara skor masing-masing item pertanyaan dengan total skor dari keseluruhan item pada variabel tersebut. Jika suatu item memiliki nilai signifikansi (Sig. 2-tailed) kurang dari 0,05 dan nilai korelasi positif yang cukup tinggi terhadap skor total, maka item tersebut dinyatakan valid, karena menunjukkan bahwa item tersebut memiliki hubungan yang signifikan dan searah dengan konstruk yang dibentuk oleh keseluruhan item.

Tabel 4. 1

Uji Validitas X

No.	Pernyataan	N	R Tabel (5%)	R Hitung	Sig. (2-Tailed)	Keterangan
1	X1	100	0.197	0.621	0.000	Valid
2	X2	100	0.197	0.390	0.000	Valid
3	X3	100	0.197	0.660	0.000	Valid
4	X4	100	0.197	0.638	0.000	Valid

Dari tabel di atas, hasil uji validitas variabel serangan *ransomware* yang menyerang PDN menunjukkan bahwa seluruh pernyataan memiliki nilai signifikansi di bawah 0,05 dan nilai r hitung lebih besar dari r tabel (5%) yaitu sebesar 0,197. Hal ini menunjukkan bahwa seluruh item pernyataan pada variabel tersebut dinyatakan valid. Nilai r hitung tertinggi terdapat pada pernyataan ketiga (X3) dengan nilai sebesar 0,660, yang menunjukkan korelasi paling kuat terhadap total skor. Dengan demikian, seluruh item pada instrumen variabel ini dapat digunakan dalam analisis lebih lanjut karena telah memenuhi syarat validitas.

Tabel 4. 2

Uji Validitas Y1

No.	Pernyataan	N	R Tabel (5%)	R Hitung	Sig. (2-Tailed)	Keterangan
1	Y1 Pernyataan 1	100	0.197	0.577	0.000	Valid
2	Y1 Pernyataan 2	100	0.197	0.620	0.000	Valid
3	Y1 Pernyataan 3	100	0.197	0.699	0.000	Valid
4	Y1 Pernyataan 4	100	0.197	0.609	0.000	Valid

Dari tabel di atas, uji validitas variabel Persepsi Masyarakat Kota Semarang menunjukkan bahwa seluruh item pernyataan memiliki nilai signifikansi di bawah

0,05 dan nilai r hitung lebih besar dari r tabel sebesar 0,197. Hal ini menandakan bahwa seluruh pernyataan dinyatakan valid. Nilai r hitung tertinggi terdapat pada pernyataan ketiga (Y1_3) dengan nilai 0,699, menunjukkan korelasi paling kuat terhadap total skor variabel persepsi masyarakat. Dengan demikian, seluruh butir pertanyaan pada variabel ini dapat digunakan dalam analisis selanjutnya karena telah memenuhi syarat validitas.

Tabel 4. 3

Uji Validitas Y2

No.	Pernyataan	N	R Tabel (5%)	R Hitung	Sig. (2-Tailed)	Keterangan
1	Y2 Pernyataan 1	100	0.197	0.886	0.000	Valid
2	Y2 Pernyataan 2	100	0.197	0.904	0.000	Valid
3	Y2 Pernyataan 3	100	0.197	0.931	0.000	Valid
4	Y2 Pernyataan 4	100	0.197	0.860	0.000	Valid

Dari tabel di atas, dapat diketahui bahwa seluruh pernyataan dalam variabel Kepercayaan Masyarakat Kota Semarang (Y2) memiliki nilai signifikansi (Sig. 2-tailed) di bawah 0,05 dan nilai r hitung lebih besar dari r tabel sebesar 0,197. Nilai r hitung tertinggi terdapat pada pernyataan ke-3 dengan nilai sebesar 0,931, sedangkan yang terendah berada pada pernyataan ke-1 dengan nilai 0,886.

Dengan demikian, dapat disimpulkan bahwa keempat butir pernyataan pada variabel Y2 valid dan layak digunakan untuk pengukuran dalam penelitian ini. Validitas ini menunjukkan bahwa setiap pernyataan mampu mengukur aspek

kepercayaan masyarakat terhadap pemerintah pasca-insiden serangan *ransomware* yang menyerang PDN.

4.2 Uji Reliabilitas

Dalam penelitian ini, uji reliabilitas dilakukan dengan menggunakan rumus koefisien Cronbach's Alpha. Pemilihan metode ini didasarkan pada kemampuannya dalam mengukur konsistensi internal, yaitu sejauh mana butir-butir pertanyaan dalam kuesioner memberikan hasil yang stabil dan konsisten dalam mengukur konstruk atau variabel yang dimaksud. Dengan kata lain, Cronbach's Alpha digunakan untuk mengetahui apakah setiap item dalam suatu variabel saling berkorelasi dan dapat dikatakan homogen atau tidak.

Penggunaan metode ini sangat relevan dalam penelitian kuantitatif karena mampu memberikan gambaran sejauh mana instrumen pengukuran (kuesioner) dapat diandalkan dalam berbagai situasi atau pada kelompok responden yang berbeda.

Sebagai dasar dalam pengambilan keputusan, nilai koefisien Cronbach's Alpha yang digunakan sebagai acuan minimal adalah 0,60. Apabila nilai yang diperoleh lebih tinggi dari angka tersebut, maka kuesioner dianggap memiliki tingkat reliabilitas yang baik dan dapat dipercaya untuk digunakan dalam pengumpulan data. Sebaliknya, jika nilai yang diperoleh berada di bawah angka tersebut, maka kuesioner dinilai kurang konsisten dan perlu dilakukan evaluasi ulang terhadap item-item pertanyaannya.

Tabel 4. 4

Uji Reliabilitas

No	Variabel	Nilai Alpha	Keterangan
1	Serangan *Ransomware* pada PDN	0,709	Reliabel
2	Persepsi	0,727	Reliabel
3	Kepercayaan	0,916	Reliabel

Berdasarkan hasil uji reliabilitas yang ditampilkan dalam tabel, seluruh variabel dalam penelitian ini menunjukkan nilai Cronbach's Alpha di atas 0,60. Hal ini berarti bahwa setiap instrumen kuesioner yang digunakan dinyatakan reliabel atau memiliki konsistensi internal yang baik dalam mengukur masing-masing variabel.

Variabel Serangan *Ransomware* pada PDN memperoleh nilai alpha sebesar 0,709. Nilai ini menunjukkan bahwa item-item pernyataan dalam variabel tersebut memiliki tingkat konsistensi yang memadai, sehingga dapat dipercaya untuk merepresentasikan tanggapan responden terhadap insiden serangan *ransomware* yang menyerang Pusat Data Nasional.

Selanjutnya, variabel Persepsi Masyarakat menunjukkan nilai alpha sebesar 0,727, yang mengindikasikan bahwa pernyataan-pernyataan dalam kuesioner mampu mengukur persepsi masyarakat secara konsisten dan andal. Artinya,

instrumen yang digunakan untuk menggali persepsi masyarakat dapat dikatakan baik secara statistik.

Adapun variabel Kepercayaan Masyarakat menghasilkan nilai reliabilitas tertinggi, yaitu 0,916. Nilai ini menunjukkan bahwa seluruh item dalam variabel tersebut sangat konsisten satu sama lain dan sangat layak digunakan sebagai alat ukur untuk menilai tingkat kepercayaan masyarakat terhadap Kominfo setelah terjadinya serangan.

4.3 Analisis Regresi Linier Sederhana

Model persamaan regresi linier sederhana dalam penelitian ini adalah:

Y + a + bx

Keterangan:

1. Y = Variabel independent
2. X = Variabel Independen yang memiliki nilai tertentu
3. a = Nilai Intercept (konstan)
4. b = Nilai Variabel Independen

4.3.1 Analisis Regresi Linier Sederhana Variabel Serangan *Ransomware* yang menyerang PDN (X) terhadap variabel Persepsi Masyarakat Kota Semarang (Y1)

Tabel 4. 5

Uji Regresi Linier Sederhana X

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	10.118	1.278		7.914	.000
	Persepsi Masyarakat Kota Semarang	.456	.072	.538	6.310	.000

a. Dependent Variable: Serangan Ransomeware yang menyerang PDN

Hasil perhitungan menunjukkan bahwa persamaan regresi yang terbentuk adalah:

$$Y=10,118+0,456X$$

Nilai konstanta sebesar 10,118 menunjukkan bahwa jika tidak terdapat persepsi dari masyarakat terhadap insiden serangan *ransomware*, maka skor yang berkaitan dengan persepsi dasar terhadap serangan tetap berada pada angka 10,118. Sementara itu, koefisien regresi sebesar 0,456 menunjukkan bahwa setiap peningkatan satu satuan dalam persepsi masyarakat akan meningkatkan skor persepsi terhadap serangan *ransomware* sebesar 0,456 satuan.

Hasil uji signifikansi pada tabel menunjukkan bahwa nilai significance (Sig.) sebesar 0,000, yang berarti lebih kecil dari 0,05. Hal ini menunjukkan bahwa pengaruh variabel persepsi masyarakat terhadap insiden serangan *ransomware* adalah signifikan secara statistik.

Dengan demikian, dapat disimpulkan bahwa semakin tinggi persepsi masyarakat terhadap insiden serangan *ransomware* pada PDN, maka semakin tinggi pula perhatian atau penilaian mereka terhadap isu tersebut. Persepsi masyarakat berperan penting dalam membentuk respons publik terhadap kejadian keamanan siber seperti serangan *ransomware* ini.

4.3.2 Analisis Regresi Linier Sederhana Variabel Serangan *Ransomware* yang menyerang PDN (X) terhadap variabel Kepercayaan Masyarakat Kota Semarang (Y2)

Tabel 4. 6

Uji Regresi Linier Sederhana Y1

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	18.414	.478		38.508	.000
	Kepercayaan Masyarakat Kota Semarang	-.018	.031	-.058	-.579	.564

a. Dependent Variable: Serangan Ransomeware yang menyerang PDN

Berdasarkan hasil pengolahan data menggunakan program SPSS, diperoleh persamaan regresi linier sederhana sebagai berikut:

$$Y=18{,}414-0{,}018X$$

Dari persamaan tersebut, nilai konstanta sebesar 18,414 mengindikasikan bahwa ketika tidak terdapat pengaruh dari variabel serangan *ransomware* (X = 0), maka tingkat kepercayaan masyarakat tetap berada pada nilai 18,414. Sementara itu, nilai koefisien regresi sebesar -0,018 menunjukkan bahwa setiap peningkatan

satu satuan dalam persepsi terhadap serangan *ransomware*, justru menyebabkan penurunan kepercayaan masyarakat sebesar 0,018 satuan.

Namun demikian, hasil uji signifikansi menunjukkan bahwa nilai signifikansi (Sig.) sebesar 0,564 jauh lebih besar dari batas signifikansi 0,05. Artinya, secara statistik, tidak terdapat pengaruh yang signifikan antara persepsi masyarakat terhadap serangan *ransomware* dan tingkat kepercayaan mereka kepada pemerintah dalam konteks penelitian ini.

Dengan kata lain, meskipun serangan *ransomware* menjadi isu penting di tingkat nasional, dalam penelitian ini tidak terbukti bahwa hal tersebut secara langsung berdampak pada menurunnya kepercayaan masyarakat Kota Semarang. Hal ini bisa disebabkan oleh berbagai faktor lain seperti penanganan krisis oleh pemerintah, komunikasi publik, atau tingkat paparan informasi masyarakat terhadap isu tersebut.

Pada penelitian ini terdapat satu variabel bebas (X) yaitu Serangan *Ransomware* yang Menyerang PDN, dan dua variabel terikat, yaitu:

Y1: Persepsi Masyarakat Kota Semarang

Y2: Kepercayaan Masyarakat Kota Semarang

Dengan demikian, hipotesis yang diajukan dalam penelitian ini adalah sebagai berikut:

H1: “Terdapat pengaruh yang signifikan ke arah negatif antara serangan *ransomware* yang menyerang PDN terhadap persepsi masyarakat Kota Semarang.”

H2: “Tidak Terdapat pengaruh yang signifikan antara serangan *ransomware* yang menyerang PDN terhadap kepercayaan masyarakat Kota Semarang, namun tetap ada indikasi pengaruh emosional atau persepsi negatif.”

4.4 Uji Parsial (Uji t)

Untuk mengetahui ada tidaknya pengaruh antara variabel bebas terhadap variabel terikat, maka dilakukan uji t dengan ketentuan sebagai berikut:

a. jika t hitung > t tabel, maka H0 ditolak dan H1 diterima
b. jika t hitung < t tabel, maka H0 diterima dan H0 ditolak

Rumus t tabel dalam penelitian ini adalah sebagai berikut:

$$df = n-k$$

Keterangan:

df = degree freedom

n = sampel

k = jumlah variabel

$$df = 100-3$$

$$= 97$$

4.4.1 Uji t Variabel Serangan *Ransomware* yang menyerang PDN (X) terhadap variabel Persepsi Masyarakat Kota Semarang (Y1)

Tabel 4. 7

Uji T X terhadap Y1

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	10.118	1.278		7.914	.000
	Persepsi Masyarakat Kota Semarang	.456	.072	.538	6.310	.000

a. Dependent Variable: Serangan Ransomeware yang menyerang PDN

Berdasarkan tabel di atas, diperoleh nilai t hitung sebesar 6,310 dan nilai signifikansi (Sig.) sebesar 0,000, yang berarti lebih kecil dari nilai alpha (0,05). Jika dibandingkan dengan nilai t tabel sebesar 1,984, maka t hitung > t tabel.

Dengan demikian, H0 ditolak dan H1 diterima, yang berarti terdapat pengaruh yang signifikan antara Persepsi Masyarakat Kota Semarang (Y1) terhadap Serangan *Ransomware* yang Menyerang PDN (X).

Artinya, semakin tinggi persepsi masyarakat terhadap isu keamanan data dan peran pemerintah, maka semakin besar pengaruhnya terhadap bagaimana masyarakat memandang dan merespons insiden serangan *ransomware* yang terjadi pada Pusat Data Nasional. Hal ini menunjukkan pentingnya membangun persepsi publik yang baik dalam menangani insiden digital yang bersifat masif dan berdampak luas.

4.4.2 Uji t Variabel Serangan *Ransomware* yang menyerang PDN (X) terhadap variabel Kepercayaan Masyarakat Kota Semarang (Y2)

Tabel 4. 8

Uji T X Terhadap Y2

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	18.414	.478		38.508	.000
	Kepercayaan Masyarakat Kota Semarang	-.018	.031	-.058	-.579	.564

a. Dependent Variable: Serangan Ransomeware yang menyerang PDN

Berdasarkan tabel di atas, diketahui bahwa nilai t hitung sebesar -0,579, sedangkan nilai signifikansi sebesar 0,564. Nilai signifikansi tersebut lebih besar dari 0,05, dan nilai t hitung juga lebih kecil dari t tabel sebesar 1,984. Dengan demikian, H_0 diterima dan H_1 ditolak, yang berarti tidak terdapat pengaruh yang signifikan antara variabel Kepercayaan Masyarakat Kota Semarang (X) terhadap variabel Serangan *Ransomware* yang Menyerang PDN (Y2).

Nilai koefisien regresi sebesar -0,018 menunjukkan arah hubungan negatif yang sangat lemah. Namun, karena hubungan ini tidak signifikan, maka kepercayaan masyarakat tidak dapat dijadikan dasar untuk memprediksi atau menjelaskan tingkat serangan *ransomware* pada Pusat Data Nasional berdasarkan hasil analisis ini.

4.5 Pembahasan

Berdasarkan penelitian yang dilakukan dengan mendistribusikan kuesioner kepada 100 responden sebagai metode pengumpulan data dan menggunakan SPSS

22 untuk analisis data, peneliti selanjutnya akan menghubungkan hasil yang telah dianalisis dengan teori yang telah ditetapkan untuk mencapai tujuan penelitian ini.

Penelitian ini mengkaji pengaruh insiden serangan *ransomware* yang menyerang Pusat Data Nasional (PDN) terhadap persepsi dan kepercayaan masyarakat Kota Semarang terhadap Kementerian Komunikasi dan Informatika (Kominfo). Penelitian ini didasari oleh urgensi keamanan data nasional dan bagaimana hal tersebut memengaruhi hubungan antara pemerintah dan publik, khususnya dalam konteks kepercayaan dan persepsi terhadap lembaga penyelenggara komunikasi dan data.

Hasil uji regresi linier sederhana menunjukkan bahwa terdapat pengaruh yang signifikan antara serangan *ransomware* terhadap persepsi masyarakat, dibuktikan dengan nilai t hitung sebesar 6,310 lebih besar dari t tabel 1,984 dan nilai signifikansi sebesar 0,000 < 0,05. Hal ini mengindikasikan bahwa masyarakat merespons peristiwa ini dengan munculnya persepsi tertentu, yang bisa mencakup pandangan negatif terhadap performa, transparansi, atau kesiapan Kominfo dalam menangani insiden keamanan siber.

Namun, hasil berbeda ditunjukkan pada variabel kepercayaan masyarakat, di mana hasil analisis regresi menunjukkan bahwa serangan *ransomware* tidak memiliki pengaruh yang signifikan terhadap tingkat kepercayaan masyarakat, dengan nilai t hitung -0,579 < t tabel dan signifikansi 0,564 > 0,05. Hal ini menunjukkan bahwa walaupun persepsi masyarakat terhadap Kominfo mungkin berubah atau terdampak, namun kepercayaan mereka belum sepenuhnya luntur.

4.5.1 Pembahasan Berdasarkan *Trust Theory*

Hasil penelitian menunjukkan bahwa serangan *ransomware* secara signifikan memengaruhi persepsi masyarakat terhadap Kominfo, tetapi tidak memiliki pengaruh yang signifikan terhadap kepercayaan masyarakat. Jika dilihat dari kaca mata *Trust Theory* oleh Deutsch (1958), hal ini mungkin terjadi karena kepercayaan terbentuk dari akumulasi pengalaman dan ekspektasi, bukan hanya satu insiden saja.

Namun demikian, realitas di lapangan menunjukkan bahwa sebagian masyarakat mulai kehilangan kepercayaan terhadap Kominfo, yang ditunjukkan melalui respons di media sosial, kritik dari tokoh publik, hingga beredarnya meme atau sindiran terhadap kinerja Kominfo. Hal ini mengindikasikan adanya gap antara hasil data kuantitatif dan dinamika sosial yang terjadi di masyarakat.

Meskipun data menunjukkan tidak ada pengaruh signifikan terhadap kepercayaan secara statistik, hal ini tidak bisa diabaikan begitu saja. Kemungkinan besar, kepercayaan masyarakat mulai mengalami degradasi, namun belum pada titik yang cukup kuat untuk terdeteksi secara signifikan melalui kuesioner, atau masyarakat masih memiliki harapan bahwa pemerintah akan melakukan perbaikan.

Dengan kata lain, kepercayaan mungkin belum sepenuhnya hilang, tetapi sudah terguncang, dan ini menjadi sinyal penting bagi lembaga pemerintah seperti Kominfo untuk segera melakukan tindakan pemulihan citra dan peningkatan keamanan data yang nyata dan transparan.

4.5.2 Pembahasan Berdasarkan Teori *Elaboration Likelihood Model (ELM)*

Berdasarkan hasil penelitian mengenai persepsi masyarakat Kota Semarang terhadap penanganan insiden ransomware yang menyerang Pusat Data Nasional (PDN), ditemukan bahwa pembentukan persepsi masyarakat terjadi melalui dua jalur utama sesuai dengan kerangka Teori Kemungkinan Elaborasi (Elaboration Likelihood Model/ELM). Teori ini menyatakan bahwa seseorang memproses pesan persuasif melalui dua jalur, yaitu central route (jalur pusat) dan peripheral route (jalur pinggiran), tergantung pada tingkat keterlibatan kognitif individu terhadap isu yang disampaikan.

Hasil kuesioner menunjukkan bahwa sebagian besar responden menilai informasi yang disampaikan oleh pemerintah mengenai insiden ini cukup jelas, logis, dan masuk akal. Hal ini terlihat dari skor tinggi pada indikator kualitas informasi dan pemrosesan pesan. Dengan demikian, masyarakat dapat dikatakan menggunakan jalur pusat dalam memproses pesan, karena mereka memperhatikan isi pesan, memahami informasi, dan mengevaluasinya secara kritis sebelum membentuk persepsi. Responden juga menyatakan bahwa mereka menganalisis terlebih dahulu kebenaran informasi sebelum mempercayainya, yang mencerminkan keterlibatan elaboratif yang tinggi dalam menyikapi isu tersebut.

Namun demikian, tidak semua responden menunjukkan elaborasi tinggi. Sebagian lainnya menyatakan bahwa kepercayaan mereka terhadap informasi didasarkan pada siapa yang menyampaikan pesan, seperti Kominfo atau media resmi pemerintah. Hal ini mengindikasikan bahwa masyarakat juga menggunakan

jalur periferal, yaitu membentuk persepsi berdasarkan isyarat non-substantif, seperti kredibilitas sumber atau pengaruh sosial. Pengaruh media sosial, opini lingkungan sekitar, dan reputasi lembaga penyampai pesan menjadi faktor yang memperkuat kecenderungan responden dalam menerima pesan tanpa elaborasi mendalam.

Dengan demikian, hasil penelitian ini menunjukkan bahwa persepsi masyarakat terhadap penanganan insiden ransomware oleh pemerintah terbentuk melalui gabungan kedua jalur dalam ELM. Masyarakat dengan minat tinggi terhadap isu keamanan digital dan akses informasi yang baik cenderung memproses pesan melalui jalur pusat, sementara masyarakat yang kurang memiliki ketertarikan atau kapasitas kognitif yang memadai cenderung menggunakan jalur periferal. Temuan ini menegaskan pentingnya pemerintah dalam menyampaikan pesan yang tidak hanya kuat secara substansi, tetapi juga meyakinkan secara kredibilitas sumber, agar dapat diterima oleh berbagai lapisan masyarakat.

BAB V

PENUTUP

5.1 Kesimpulan

Penelitian ini bertujuan untuk mengetahui pengaruh insiden serangan *ransomware* yang menyerang Pusat Data Nasional (PDN) terhadap persepsi dan kepercayaan masyarakat terhadap Kementerian Komunikasi dan Informatika (Kominfo). Berdasarkan hasil penyebaran kuesioner kepada 100 responden masyarakat Kota Semarang dan analisis data menggunakan regresi linier sederhana melalui SPSS, maka dapat disimpulkan hal-hal sebagai berikut:

Persepsi masyarakat terhadap Kominfo dipengaruhi secara signifikan oleh insiden serangan *ransomware*. Hasil uji t menunjukkan nilai signifikansi sebesar 0,000 < 0,05 dan nilai t hitung sebesar 6,310 > t tabel 1,984. Hal ini menunjukkan bahwa insiden tersebut telah memberikan dampak terhadap cara masyarakat memandang kinerja dan citra Kominfo, yang secara umum cenderung negatif, karena Kominfo dianggap lalai atau kurang mampu melindungi data publik secara maksimal.

Kepercayaan masyarakat terhadap Kominfo tidak dipengaruhi secara signifikan oleh insiden serangan *ransomware*. Hasil uji t menunjukkan nilai signifikansi sebesar 0,564 > 0,05 dan nilai t hitung -0,579 < t tabel 1,984. Dengan demikian, kepercayaan masyarakat tidak terganggu secara langsung meskipun persepsinya terhadap Kominfo menurun. Hal ini menunjukkan bahwa kepercayaan masyarakat masih relatif stabil, kemungkinan karena ketiadaan alternatif lembaga

lain atau karena adanya harapan bahwa pemerintah mampu memperbaiki sistem keamanan ke depannya.

Dengan mengacu pada teori ELM, dapat disimpulkan bahwa efektivitas komunikasi pemerintah dalam menangani krisis serangan siber sangat dipengaruhi oleh substansi pesan dan kredibilitas sumber. Oleh karena itu, strategi komunikasi publik sebaiknya disusun dengan memperhatikan kedua jalur elaborasi agar dapat menjangkau semua segmen masyarakat, baik yang memproses pesan secara rasional maupun secara intuitif.

Secara keseluruhan, insiden serangan *ransomware* yang terjadi telah berdampak terhadap persepsi masyarakat namun belum cukup kuat untuk menggoyahkan kepercayaan masyarakat terhadap Kominfo. Fakta ini memberikan sinyal bahwa Kominfo perlu segera melakukan pemulihan citra dan penguatan kepercayaan publik melalui transparansi, perbaikan sistem, dan komunikasi krisis yang efektif.

5.2 Saran

Berdasarkan hasil penelitian dan kesimpulan yang diperoleh, peneliti memberikan beberapa saran sebagai berikut:

1. Bagi Kominfo, disarankan untuk meningkatkan komunikasi publik yang lebih terbuka, jujur, dan tepat waktu dalam menangani insiden keamanan data. Membangun kembali persepsi dan menjaga kepercayaan masyarakat harus menjadi prioritas utama melalui langkah-langkah strategis, seperti audit

keamanan data terbuka, pelibatan pihak independen, dan pelatihan literasi digital bagi masyarakat.

2. Bagi Pemerintah, diperlukan evaluasi menyeluruh terhadap sistem pengelolaan dan infrastruktur Pusat Data Nasional (PDN), termasuk penguatan kebijakan dan regulasi di bidang keamanan siber. Pemerintah juga perlu mempertimbangkan untuk melibatkan komunitas keamanan digital dalam proses pengawasan sebagai bentuk partisipasi publik.
3. Bagi Peneliti Selanjutnya, disarankan untuk memperluas ruang lingkup penelitian dengan menggunakan metode campuran (mixed methods) agar dapat menangkap nuansa emosi, ketidakpercayaan, atau ketidakpuasan masyarakat yang tidak terdeteksi secara kuantitatif. Pendekatan kualitatif seperti wawancara atau analisis media sosial dapat memperkaya pemahaman terhadap perubahan persepsi dan kepercayaan masyarakat secara lebih mendalam.

DAFTAR PUSTAKA

Assiddiq, Alif Akbar (2021) Pengaruh Kepercayaan,Kemudahan Dan Kualitas Informasi Terhadap Keputusan Pembelian. Other thesis, Universitas Komputer Indonesia.

Bogdan, R., & Biklen, S. (2019). *Qualitative Research for Education: An Introduction to Theories and Methods.* Edi Suryadi (Ed.).

Creswell, J., W. & Creswell, J.,D. (2018). *Research design: Qualitative, Quantitative, and Mixed Methods Approaches. 5th ed*., SAGE Publications

Denzin, N. K., & Lincoln, Y. S. (2018). *Handbook of Qualitative Research.*

Donni Juni. 2017. Perilaku Konsumen: Dalam Persaingan Bisnis Kontemporer. Bandung: CV Alfabeta

Fish, William. (2021). *Philosophy of Perception: A Contemporary Introduction.* New York: Routledge

Flew, Terry and McWaters, Callum, *Trust in Communication Research: A Systematic Literature Review of Trust Studies in Leading Communication Journals* (January 22, 2020).

Ghozali, I. (2016) Aplikasi Analisis Multivariete Dengan Program IBM SPSS 23. Edisi 8. Semarang: Badan Penerbit Universitas Diponegoro.

Ghozali, I. (2021). Aplikasi Analisis Multivariate Dengan Program IBM SPSS 26. Edisi 10. Badan Penerbit Universitas Diponegoro.

Hartono, Budi. (2023). *Ransomware*: Memahami Ancaman keamanan digital. Jakarta: Amartaraya Solusi Utama

Juliandi A, Irfan, Manurung S. 2016. Metodologi Penelitian Bisnis: Konsep dan Aplikasi. Medan: UMSU Press.

Khun, T. (2016). *The Structure of Scientific Revolutions*. Dalam Kriyantono.

Littlejohn, Foss, & Oetzel. (2017). Teori Komunikasi Manusia. Illinois: Waveland Press.

M. Deutsch. 1958. *Trust and suspicion*. *Journal of Conflict Resolution* 2, 4 (1958)

Newbold, P., Carlson, W. L., & Thorne, B. (2020). *Statistics for Business and Economics.* Pearson Education.

Neuman, W. L. (2019*). Social research methods: Qualitative and quantitative approaches (8th ed.).* Pearson Education.

Ponemon Institute. (2022). *The Impact of Data Breaches on Consumer Trust.* Ponemon Institute.

Sugiyono. (2016). Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung: Alfabeta.

Sutama (2016). Metode Penelitian Pendidikan Kuantitatif, Kualitatif, PTK, dan R&D. Surakarta: Fairus Media.

Institute, P. (2022). *The Impact of Data Breaches on Consumer Trust*. *Ponemon Institute*.

Simorangkir, A., Sihombing, H., Intani, P., & Parhusip, J. (2024). *Ransomware* pada Data PDN: Implikasi Etis dan Tanggung Jawab Profesional dalam Pengelolaan Keamanan Siber. *Jurnal Sains Student Research Vol.2, No.6*.

Suryadi, E. (2019). *Qualitative Research for Education: An Introduction to Theories and Methods.*

Union, I. T. (2023). *Global Cybersecurity Index (GCI)*.