ANALISIS KEAMANAN JARINGAN PADA RUMAH MENGGUNAKAN METODE NIST

Arya Maulana Kurniawan, Diki Gita Purnama, Bilal Al Ghiffari
Teknik Informatika, Universitas Paramadina
Jl. Mabes Hankam Kav.9 Setu, Cipayung, Jakarta Timur
arya.kurniawan@students.paramadina.ac.id

ABSTRAK

Perkembangan internet di Indonesia setiap tahunnya selalu mengalami peningkatan yang signifikan, pada tahun 2023 terjadi peningkatan pengguna dengan penambahan sekitar 599.387 pengguna. Peningkatan pengguna internet di Indonesia juga berdampak pada kenaikan pengguna jaringan WiFi di rumah. Keamanan jaringan dirumah seringkali diabaikan oleh banyak individu, meskipun ancaman siber yang beragam, seperti malware, virus, brute force, phising, dan lain-lain. Permasalahan yang menjadi fokus penelitian ini melibatkan tingkat kesadaran dan pemahaman pengguna internet rumah terhadap keamanan jaringan, faktor-faktor yang mempengaruhi keamanan jaringan di rumahh, serta langkah-langkah yang dapat diambil untuk melindungi keamanan jaringan tersebut. Penelitian ini bertujuan untuk melakukan analisis keamanan jaringan pada rumah dengan menggunakan framework NIST cybersecurity, tujuan utama dari penelitian ini adalah untuk melinai tingkat kesadaran dan pemahaman pengguna internet rumah terhadap keamanan jaringan, mengidentifikasi faktor-faktor yang mempengaruhi keamanan jaringan di rumah, dan mengevaluasi langkah-langkah yang dapat diambil untuk melindungi keamanan jaringan tersebut. Penelitian ini menggunakan metode kuantitatif dengan menyebar kuesioner kepada pengguna internet rumah. Hasil dari penelitian menunjukan bahwa responden memiliki kesadaran yang baik terhadap keamanan jaringan, tetapi terdapat beberapa hal yang perlu ditingkatkan, seperti rutinitas pengecekan perangkat dan file, penggantian password, perlindungan data, pemantauan aktivitas jaringan, rencana tanggapan, dan rencana pemulihan.

Kata kunci : *keamanan jaringan, WiFi, NIST Cybersecurity, internet*

1. PENDAHULUAN

Pengguna internet di Indonesia setiap tahunnya terus mengalami peningkatan yang signifikan, menurut hasil survey yang telah dilakukan oleh APJII. Pada tahun 2022, jumlah pengguna internet di Indonesia mencapai 210.026.769. Tahun 2023 terjadi peningkatan mencapai 5.599.387 pengguna, dengan jumlah total pengguna internet di Indonesia menjadi sekitar 215.626.156 dari total populasi penduduk sebanyak 275.773.901 jiwa [1].

Peningkatan pengguna internet di Indonesia juga berdampak pada kenaikan pengguna jaringan *WiFi* di rumah, dengan kenaikan sekitar 0,15% dibandingkan tahun sebelumnya [1]. Dengan meningkatnya pengguna internet, keamanan jaringan perlu diperhatikan agar pengguna dapat terlindungi dari pihak-pihak yang tidak bertanggung jawab. Namun, keamanan jaringan di lingkungan rumah seringkali diabaikan oleh banyak individu, meskipun ancaman siber yang beragam, termasuk serangan *malware, virus, brute force, phising, rasomware*, hingga *web defacement*, yang dapat mengintai jaringan dirumah [2]. Tidak hanya itu, serangan *Distribute Denial of Service* (DDOS) juga menjadi ancaman serius, dengan berbagai serangan yang sering kali dihadapi, seperti *HTTP flood attack, UDP flood attack*, dan serangan *DDoS Zero-day* [3].

Serangan siber terhadap pengguna internet baik individu, perusahaan, dan rumah merupakan ancaman yang perlu dipahami dan ditangani dengan serius. Di Indonesia ada beberapa serangan siber yang paling sering dialami, yaitu *Malware, virus, brute force, phising, rasomware, web deface*, dan masih banyak serangan lainnya [2]. Selain karena factor-factor orang luar, serangan siber di Indonesia sering terjadi karena tidak mengetahui/tidak pernah melakukan tindakan untuk menjaga keamanan data dan pengguna internet masih banyak yang mengabaikan pentingnya periode pergantian password [1].

Penelitian ini bertujuan untuk melakukan analisa keamanan jaringan dan membahas pentingnya menjaga keamanan jaringan pada rumah. Penulis akan menjelaskan jenis-jenis ancaman siber yang mungkin mengintai jaringan pada rumah. Selain itu, penelitian ini juga akan memberikan Langkah-langkah yang dapat diterapkan pada jaringan rumah untuk melindungi keamanan jaringan pada rumah.

Pada proses analisis keamanan jaringan pada rumah, dalam penelitian ini akan menggunakan *framework* NIST. *Framework* NIST *Cybersecurity* diorganisir berdasarkan lima fungsi kunci, yaitu Identifikasi, Perlindungan, Deteksi, Respons, dan Pemulihan. Dengan menggunakan framework ini dapat memberikan pandangan komprehensif mengenai siklus manajemen risiko keamanan siber dari waktu ke waktu[4].

2. TINJAUAN PUSTAKA

2.1. Penelitian terdahulu

Pada Penelitian karya Rajesh Yadav dengan judul "Cyber security Threats during covid-19 pandemic", menjelaskan para pelaku penyerangan siber sering menargetkan celah yang memiliki kerentanan dan mengambil keuntungan dari segala hal

darurat diberbagai kalangan masyarakat seperti finansial, kesehatan, dan sebagainya. Pada penelitian ini juga menjelaskan spam email yang memiliki link URL berbahaya meningkat sebanyak 300%, selain itu masih banyak serangan-serangan siber yang mengalami peningkatan seperti DDOS Attack, Website berbahaya, Malware, Rasomware, dan lain-lain [5].

Pada penelitian karya Md. Waliullah dan Diane Gan dengan judul "Wireless LAN Security threats & Vulnerabilities: A Literature Review", menjelaskan bahwa mengamankan jaringan nirkabel memiliki proses yang berkelanjutan. Pada penelitian tersebut juga menjelaskan belum ada langkah keamanan tunggal yang benar-benar aman. Ketika teknologi baru pertama kali diperkenalkan, para peretas mempelajari protocolnya, mencari kerentanannya, dan kemudian membuat beberapa program dan skrip untuk mencoba mengeksploitasi kerentanannya [6].

Pada penelitian karya Geerten van de kaa, Frank den Hartog, dan Henk J. de Vries dengan judul "Mapping standards for home networking", menjelaskan bahwa jaringan rumah sangat beragam dan belum ada yang dominan. Pada penelitian ini juga membahas tentang standar-standar yang digunakan untk jaringan rumah, yaitu sistem konikasi antara berbagai perangkat di lingkungan rumah [7].

2.2. Jaringan Nirkabel

Jaringan nirkabel adalah gabungan dari berbagai jaringan yang memungkinkan satu komputer mengakses komputer lain tanpa menggunakan koneksi kabel secara fisik [8].

2.3. *Firewall*

Firewall merupakan perangkat perlindungan pertama dari batas dalam dan luar. *Firewall* mengatur data yang masuk dan keluar dalam teknologi informasi dan komunikasi (TIK) dan memberikan perlindungan TIK dengan menyaring data, melakukan verifikasi informasi berdasarkan kriteria yang telah ditetapkan, dan memutuskan apakah paket-paket tersebut boleh masuk ke dalam sistem [9].

2.4. Serangan Siber

Serangan siber yang biasa dikenal sebagai serangan jaringan komputer adalah eksploitasi yang disengaja terhadap sistem komputer, perusahaan, dan jaringan yang bergantung pada teknologi. Para penyerang menggunakan kode berhaya untuk mengubah kode, logika, atau data komputer yang menghasilkan konsekuensi yang mengganggu yang dapat membahayakan data dan mengarah pada kejahatan siber, seperti pencurian informasi dan identitas [10].

2.5. *Distributed Denial of Service*

DDoS adalah serangan yang menargetkan ketersediaan *server* dengan membajiri saluran komunikasi dengan permintaan palsu yang berasal dari perangkat terdistribusi [3].

2.6. *Malware*

Malware merupakan perangkat lunak jahat yang dirancang untuk merusak sumber daya komputer dengan mencuri informasi penting dan mengakses perangkat target dengan jarak jauh. *Malware* juga dapat berupa .exe, *script, file, makro* [11].

2.7. *Virus*

Virus komputer merupakan program yang memiliki kemampuan untuk menggandakan diri dan menyebar dengan cepat. *Virus* dapat berkembang dengan cepat sehingga mengganggu jaringan dan membuatnya tidak berfungsi sementara [12].

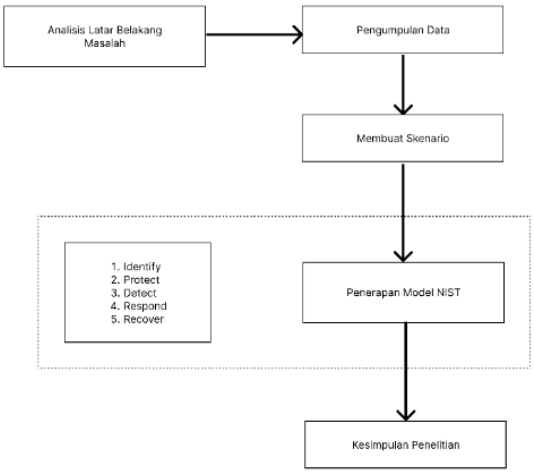
2.8. *Spyware*

Spyware merupakan perangkat lunak yang digunakan untk memata-matai aktivitas pengguna pada komputer. Ini bisa mencakup *keylogger* yang mencatat setiap tindakan ketik atau mengambil tangkapan layar. *Spyware* memerlukan pengetahuan teknis yang lebih tinggi dan digunakan untuk mencuri informasi pengguna seperti *username* dan *password* [12].

2.9. *Phising*

Phising merupakan teknik yang biasa digunakan untuk mencuri identitas dengan cara mengirim *email* palsu yang mengarahkan target untuk memasukkan informasi pribadi mereka ke situs web palsu yang dikendalikan oleh penyerang [12].

3. METODE PENELITIAN



Gambar 1. Alur penelitian

Analisis keamanan jaringan pada rumah dalam penelitian ini, pengumpulan data akan menggunakan metode kuantitatif dan metode untuk menganalisis keamanan jaringan pada penelitian ini akan menggunakan framework NIST *Cybersecurity*. Proses pengumpulan data akan dilakukan dengan cara menyebar kuesioner kepada pengguna internet rumah dan untuk analisis keamanan jaringan akan melakukan beberapa tahapan yaitu tahapan membuat skenario,

tahapan identifikasi, tahapan *protect*, tahapan *detect*, tahapan *respon*, dan tahapan *recover*. Berikut pada gambar 1 dibawah ini merupakan tahapan kerangka penelitian yang dilakukan untuk menganalisis keamanan jaringan pada rumah.

Keterangan untuk gambar 1 akan dijelaskan sebagai berikut:

3.1. Analisis Latar Belakang Masalah

Penelitian ini bertujuan untuk menganalisis keamanan jaringan dan membahas pentingnya menjaga keamanan jaringan pada rumah. Penulis akan menjelaskan jenis-jenis ancaman siber yang mungkin mengintai jaringan pada rumah.

3.2. Pengumpulan Data

Pada penelitian ini, pengumpulan data akan menggunakan metode kuantitatif dengan cara menyebarkan kuisioner pada pengguna internet di rumah. Penelitian ini juga akan menggunakan studi literatur sebagai data tambahan.

3.3. Membuat Skenario

Pada tahapan ini peneliti akan membuat scenario jaringan pada rumah yang akan nantinya akan digunakan sebagai contoh penerapan keamanan jaringan pada rumah.

3.4. Merapkan Metode NIST

3.4.1. Identify

Pada tahapan ini akan dilakukan asset yang perlu dilindungi, ancaman yang mungkin terjadi, dan kerentanan yang mungkin ada pada jaringan rumah dari hasil kuesioner dan studi literatur yang telah dilakukan.

3.4.2. Protect

Tahapan ini akan melakukan analisis kontrol keamanan siber yang sesuai untuk melindungi aset dari ancaman yang telah diidentifikasi.

3.4.3. Detect

Pada tahapan ini akan dilakukan analisis kontrol keamanan siber untuk mendeteksi ancaman keamanan siber yang mungkin terjadi pada jaringan rumah.

3.4.4. Respond

Pada tahapan ini akan menganalisis rencana respon keamanan siber untuk menangani insiden keamanan siber yang mungkin terjadi pada jaringan rumah.

3.4.5. Recover

Pada tahapan yang terakhir akan melakukan analisis rencana pemulihan untuk memulihkan system setelah insider keamanan siber terjadi pada jaringan rumah.

3.5. Membuat Kesimpulan

Membuat kesimpulan secara lengkap dari uraian tahapan NIST yang telah diterapkan untuk analisis keamanan jaringan pada rumah.

4. HASIL DAN PEMBAHASAN

Setelah melakukan pengumpulan data pada pengguna internet rumah, dari 60 responden terdapat 52 responden yang menggunakan *WiFi* pada jaringan rumahnya. Penerapan metode NIST dilakukan kepada 52 responden tersebut, berikut adalah hasil dari analisis penerapan metode NIST:

4.1. *Identify*

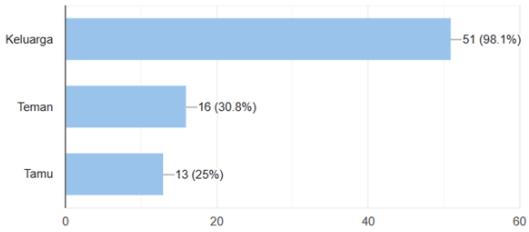
Pada tahapan ini peneliti menganalisis perangkat apa saja yang responden pada jaringan rumahnya, siapa saja yang biasa terhubung pada jaringan tersebut, bagaimana kebiasaan responden dalam menggunakan internet pada jaringan tersebut, dan pengetahuan responden terhadap keamanan jaringan.

Tabel 1. Jenis-jenis perangkat

No	Jenis perangkat yang terhubun	Jumlah pengguna
1	*Smartphone*	50
2	*Smart TV*	30
3	*Laptop*	43
4	*Computer Tower*	6
5	*Smart Device*	10
6	*PlayStation*	1
7	*Printer*	1

Pada table 1 menampilkan perangkat-perangkat milik responden yang biasa terhubung ke jaringan internet rumah, dari list-list tersebut smartphone dan *laptop* merupakan perangkat yang paling banyak digunakan oleh responden.

Dari hasil penelitian yang telah dilakukan, sebanyak 98,1% dari responden yang hanya memberikan akses terhadap jaringan internet dirumahnya kepada anggota keluarga saja, sedangkan sisanya memberikan akses juga kepada orang luar seperti teman atau tamu seperti yang ditampilkan pada gambar 2 dibawah ini.

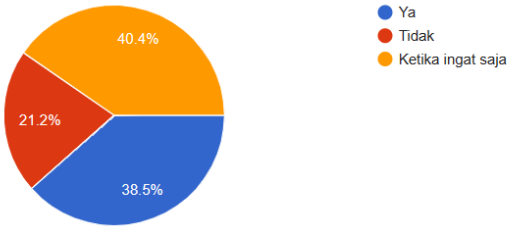


Gambar 2. Diagram pengguna jaringan rumah

Pada tahapan ini juga mengidentifikasi bagaimana kebiasaan responden ketika menggunakan jaringan internet dirumahnya, sebanyak 44,2% dari responden hanya melakukan pengecekan website yang dituju ketika waktu tertentu saja. Tahapan ini juga mengidentifikasi apakah responden memastikan terlebih dahulu data yang diunduh merupakan data yang sesungguhnya, pada gambar 1 akan menjelaskan bagaimana user mengidentifikasi data yang telah diunduh.

Gambar 3. Diagram bagaimana user mengecek file yang telah diunduh

Pada gambar 3 menjelaskan sebanyak 38,5% dari responden hanya melakukan pengecekan dengan cara memperhatikan ukuran, nama, dan ekstensi dari file yang telah diunduh saja, dan sebanyak 34,6% responden menggunakan *antivirus* untuk mengecek data yang telah diunduh terbebas dari *malware* atau *virus*.



Gambar 4. Diagram rutinitas user melakukan pengecekan perangkat

Pada gambar 4 menjelaskan apakah responden secara teratur melakukan pengecekan perangkat - perangkatnya terbebas dari *malware*, *virus*, atau *spyware*. Gambar 4 menampilkan bahwa sebanyak 40,4% responden hanya melakukan pengecekan perangkat - perangkatnya ketika mengingatnya saja.

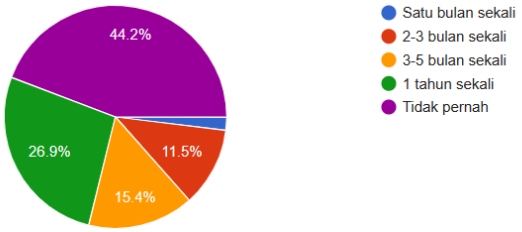
Quesioner ini juga memberikan hasil yaitu 63,5% dari responden menyadari adanya ancaman keamanan jaringan. Ancaman keamanan jaringan yang diketahui antara lain, serangan *phising*, serangan *malware*, dan serangan *rasomware*. Sebanyak 30,8% dari responden juga tidak mengetahui apakah mereka telah mengalami serangan siber.

4.2. *Protect*

Pada tahapan ini, peneliti menganalisis bagaimana pemahaman responden terhadap keamanan jaringan, apa cara yang dilakukan responden untuk mengamankan jaringannya, dan bagaimana cara menjegah serangan siber. Dari hasil quesioner yang telah disebar sebanyak 38,5% familiar dengan konsep keamanan siber serta 17,3 persen tidak familiar dengan konsep keamanan siber, tetapi sebanyak 50% dari responden menganggap menjaga keamanan siber itu penting, oleh karena itu berikut beberapa hasil quesioner lain berkaitan dengan tahapan *protect* pada NIST *cybersecurity*.

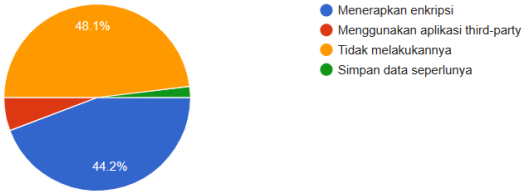
Pada proses autentikasi, kata sandi berfungsi sebagai alat berbasis pengetahuan dan berfungsi sebagai perantara untuk mengidentifikasi pengguna dalam sistem. Ini dimaksudkan untuk mengatur akses pengguna ke berbagai sumber daya atau sistem [13].

Dari hasil quesioner yang telah disebar, sebanyak 94,2% responden menggunakan *password* yang kuat untuk melindungi perangkat-perangkat yang terhubung kejaringan rumahnya. Selain itu, 65,4% responden menggunakan *password* yang berbeda untuk setiap perangkat mereka. Tetapi sebanyak 44,2% reponden tidak pernah mengganti *password* mereka, dan sekitar 26,9% reponden mengubah passwordnya hanya sebanyak 1 tahun sekali seperti yang ditampilkan pada gambar 5 dibawah ini.



Gambar 5. Diagram periode pergantian *password* responden

Melindungi data termasuk kedalam tahap protect pada NIST *cybersecurity*, dari quesioner yang telah disebar sebanyak 48,1% tidak melindungi data sensitif yang berada pada perangkat yang terhubung kejaringan rumahnya dan sebanyak 44,2% dari responden menerapkan enkripsi untuk melindungi data-data mereka yang bisa dilihat pada gambar 6 dibawah ini.



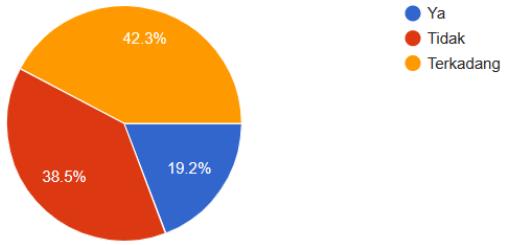
Gambar 6. Diagram cara responden melindungi data *sensitive*

Selain melindungi data, mencadangkan file-file merupakan hal yang penting agar ketika serangan terjadi data tersebut bisa dikembalikan. Dari quesioner yang telah disebar, sebanyak 69,2% responden secara teratur mencadangkan file-file penting yang ada pada perangkat-perangkat mereka. Mencadangkan file menggunakan layanan cloud merupakan cara yang paling banyak dipilih oleh responden, sedankan hanya sekitar 31% yang menggunakan penyimpanan ekternal untuk mencadangkan file-file penting.

4.3. *Detect*

Pada tahapan ini, peneliti menganalisis bagaimana cara responden mendeteksi ancaman-ancaman yang ada pada jaringan dirumah mereka. Sebanyak 55,8% responden menggunakan sistem keamanan untuk mendeteksi ancaman pada jaringan rumah mereka, 89% dari responden menggunakan antivirus untuk mendeteksi ancaman sedangkan

sisanya menggunakan *antimalware*, ID/IPS, dan tidak menggunakan sama sekali.



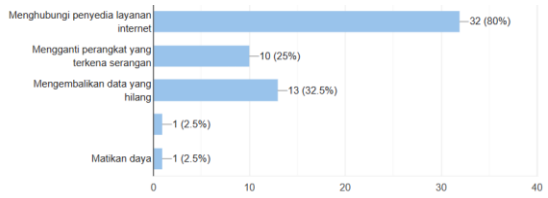
Gambar 7. Diagram pemantauan aktivitas jaringan

Pada gambar 7 menampilkan bahwa 42,3% responden hanya ketika waktu tertentu saja melakukan pemantauan aktivitas pada jaringan rumah mereka dan hanya 19,2% yang melakukan pemantauan aktivitas secara berkala.

Penelitian ini juga menampilkan tingkat kesulitan reponden dalam mendeteksi adanya anomali atau aktivitas mencurigakan pada jaringan rumah mereka, sebanyak 46,2% responden mudah dalam mendeteksi adanya anomali atau aktivitas yang mencurigakan pada jaringan rumah mereka.

4.4. *Respond*

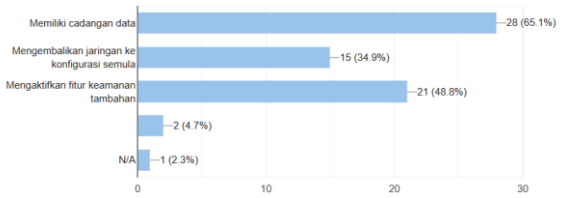
Pada tahap selanjutnya, peneliti juga menganalisis bagaimana cara tanggapan responden ketika terjadi pada jaringan dirumahnya, sebanyak 53,8% responden memiliki rencana tanggapan ketika terjadi serangan keamanan jaringan. Sebanyak 80% responden memiliki rencana yaitu dengan menghubungi penyedia layanan jaringan saja, dan sisanya akan ditampilkan pada gambar 8 dibawah ini.



Gambar 8. Diagram rencana tanggapan Ketika terkena serangan

4.5. *Recover*

Pada tahapan terakhir ini, peneliti melakukan analisis rencana apa saja yang dimiliki responden untuk pemulihan pasca terjadinya serangan keamanan jaringan yang terjadi pada jaringan rumah mereka. Sebanyak 76,9% responden memiliki rencana pemulihan pasca terjadinya serangan keamanan jaringan, sebanyak 65,1% responden memiliki cadangan data dan rencana-rencana lainnya akan ditampilkan pada gambar 9 dibawah ini.



Gambar 9. Diagram rencana pemulihan pasca terjadinya serangan

5. KESIMPULAN DAN SARAN

Berdasarkan hasil analisis penerapa metode NIST pada jaringan internet rumah, dapat disimpulkan bahwa responden memiliki kesadaran yang baik terhadap keamanan jaringan. Tetapi terdapat beberapa hal yang perlu ditingkatkan, seperti rutinitas pengecekan perangkat dan file yang diunduh. Hal ini bertujuan untuk memastikan bahwa perangkat dan file yang terhubung ke jaringan rumah aman dari ancaman *malware, virus, dan spyware*. Penggantian *password* secara berkala. Hal ini bertujuan untuk mencegah peretasan yang memanfaatkan password yang lemah atau sudah pernah bocor. Perlindungan data *sensitive* dengan enkripsi, hal ini bertujuan untuk melindungi data-data penting dari pihak yang tidak bertanggung jawab. Pemantauan aktivitas jaringan secara berkala, hal ini bertujuan untuk mendeteksi adanya *anomaly* atau aktivitas mencurigakan yang dapat menjadi tanda serangan siber. Peningkatan kemampuan untuk mendeteksi *anomaly* atau aktivitas mencurigakan, hal ini dapat dilakukan dengan mengikuti pelatihan keamanan siber atau menggunakan perangkat lunak keamanan yang canggih. Pembuatan rencana tanggapan dan pemulihan yang lebih baik, hal ini bertujuan untuk mengirangi dampak dari serangan siber yang terjadi.

DAFTAR PUSTAKA

[1] APJII, “Survei Penetrasi & Perilaku Internet di Indonesia,” 2023.

[2] APJII, “Survei Internet Service Provider Industry & Market Profile,” 2023.

[3] R. Vishwakarma and A. Kumar Jain, “A survey of DDoS attacking techniques and defence mechanisms in the IoT network,” 2019.

[4] A. Mahn, J. Marron, S. Quinn, and D. Topper, “Getting started with the NIST Cybersecurity Framework : A Quick Start Guide,” Aug. 2021. doi: 10.6028/NIST.SP.1271.

[5] R. Yadav, “Cyber Security Threats During Covid-19 Pandemic,” 2020.

[6] M. Waliullah and D. Gan, “Wireless LAN Security Threats & Vulnerabilities,” 2014.

[7] G. van de Kaa, F. den Hartog, and H. J. de Vries, “Mapping standards for home networking,” *Comput Stand Interfaces*, vol. 31, no. 6, pp. 1175–1181, Nov. 2009, doi: 10.1016/j.csi.2009.04.002.

[8] R. Nazir, A. Ali Laghari, K. Kumar, S. David, and M. Ali, “Survey on Wireless Network Security,” 2021.

[9] Z. D.A and M. A. Abdurakhmon Ugli, "Network security issues and effective protection against network attacks," 2021.

[10] R. Adlakha, S. Sharma, A. Rawat, and K. Sharma, "Cyber Security Goal's, Issue's, Categorization & Data Breaches," 2019.

[11] S. Sibi Chakkaravarthy, D. Sangeetha, and V. Vaidehi, "A Survey on malware analysis and mitigation techniques," *Computer Science Review*, vol. 32. Elsevier Ireland Ltd, pp. 1–23, May 01, 2019. doi: 10.1016/j.cosrev.2019.01.002.

[12] Chuck. Easttom, *Computer security fundamentals*. Pearson, 2011.

[13] B. Frischmann and A. Johnson, "Common nonsense about password security and the expert-layperson knowledge gap." [Online]. Available: https://ssrn.com/abstract=4345028