Identifikasi Tren Cyber Threats Menggunakan Next Generation Firewall Pada Dinas Komunikasi Dan Informatika Kabupaten Boyolali

Heriyanto Agus Prihatin, hproj50@gmail.com, Universitas Surakarta
Jani Kusanti, jani_kusanti@unsa.ac.id, Universitas Surakarta
Sukoco, sukoco@unsa.ac.id, Universitas Surakarta

ABSTRAKSI

Keamanan siber dinilai semakin penting seiring bertambahnya jumlah pengguna internet dan merupakan bentuk perlindungan terhadap ancaman siber di dunia maya. Keamanan jaringan merupakan faktor penting dalam mencegah adanya ancaman siber atau biasa disebut cyber threats. Melindungi sistem dari ancaman siber memerlukan perangkat yang dapat membatasi akses antara jaringan yang dilindungi dan Internet serta dapat mendeteksi adanya aktivitas yang mencurigakan. Next Generation Firewall merupakan sistem keamanan yang digunakan untuk meningkatkan keamanan jaringan terhadap berbagai jenis ancaman siber seperti Denial of Service, malware, dan sebagainya. Perangkat keamanan jaringan ini memantau trafik jaringan, mendeteksi aktivitas yang mencurigakan, dan mencegah intrusi atau peristiwa yang dapat menyebabkan jaringan berfungsi tidak sebagaimana mestinya. Dalam upaya untuk melindungi sistem diperlukan identifikasi terhadap adanya ancaman siber menggunakan perangkat yang mampu membatasi akses antara sebuah jaringan yang diproteksi dan internet.

Kata kunci : Cyber Threats, Firewall, Keamanan Jaringan, Internet, Keamanan Siber

1. LATAR BELAKANG MASALAH

Pesatnya perkembangan teknologi informasi dan komunikasi dapat mempengaruhi kerentanan terhadap kebocoran dan penyalahgunaan informasi. Layanan yang ditujukan untuk masyarakat umum tidak dapat dibuat hanya dengan berinvestasi pada perangkat atau sistem elektronik. Namun, keamanan data melibatkan beberapa hal, termasuk jaminan Kerahasiaan (Confidentiality), Keutuhan (Integrity), Ketersediaan (Availability), Keaslian (Authentication), dan Kenirsangkalan (non-repudiation).

Badan Siber dan Sandi Negara menyatakan ada 495.337.202 anomali trafik jaringan di Indonesia pada tahun 2020. Pada tahun 2021, jumlahnya meningkat secara signifikan yaitu 1.637.973.022 anomali trafik. Pada tahun 2021, botnet MyloBot mengendalikan setidaknya 44,62 persen insiden trafik (BSSN, 2021). Tidak hanya botnet MyloBot, beberapa anomali dalam kategori Top 10 anomali juga memiliki link ke botnet lain seperti ZeroAccess dan Discover Using Socks Agent dalam serangannya. Botnet adalah jaringan komputer yang terinfeksi malware yang dikendalikan oleh satu penyerang. Botnet dapat dirancang untuk mengirim spam, pencurian data, ransomware, click jacking, penolakan layanan (Denial of Service), dan masih banyak lagi.

Keamanan jaringan merupakan upaya untuk melindungi jaringan komputer dan sistem informasi sebuah instansi dari ancaman keamanan siber. Dalam upaya untuk melindungi jaringan komputer dan sistem informasi tersebut diperlukan adanya identifikasi terhadap adanya cyber threats menggunakan perangkat yang mampu membatasi akses antara sebuah jaringan yang diproteksi dan internet.

2. RUMUSAN MASALAH

Berdasarkan latar belakang di atas, maka dapat dirumuskan masalah yaitu banyaknya cyber threats pada Dinas Komunikasi dan Informatika Kabupaten Boyolali yang belum teridentifikasi.

Pada karya tulis ini hanya berfokus pada identifikasi terhadap cyber threats yang terjadi pada sistem yang terkena serangan siber dalam periode waktu tertentu

3. METODE PENELITIAN

Dalam penelitian ini data primer diperoleh dari wawancara yang dilakukan dengan pejabat yang bertugas pada Bidang Persandian dan Pengamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Boyolali untuk

mendapatkan data atau informasi terkait kebijakan keamanan informasi yang sudah diterapkan.

Dalam penelitian ini data sekunder diperoleh dari informasi tertulis atau hasil dokumentasi pada instansi berupa jenis maupun seri perangkat keamanan jaringan yang dipakai, dan lain sebagianya.

a) Analisis

Identifikasi cyber threats perlu dilakukan dalam melindungi jaringan dan sistem informasi dari serangan keamanan siber. Dengan mengidentifikasi cyber threats, instansi dapat mengetahui jenis serangan yang mungkin terjadi dan cara terbaik untuk mencegahnya. Hal ini membantu meningkatkan keamanan jaringan secara keseluruhan dan melindungi aset informasi dari ancaman keamanan siber.

b) Perancangan

Proses perencanaan dan implementasi teknologi serta strategi untuk mendeteksi, menganalisis, dan merespons ancaman keamanan siber yang dapat mengancam jaringan dan sistem informasi. Tujuan dari perancangan sistem identifikasi cyber threat adalah untuk memastikan bahwa intansi memiliki kemampuan untuk mengidentifikasi ancaman keamanan siber dengan cepat dan mengambil tindakan yang diperlukan untuk melindungi aset informasi mereka. Perancangan sistem identifikasi cyber threats melibatkan teknologi keamanan, pemantauan jaringan, dan analisis data untuk mendeteksi aktivitas aneh dan potensi serangan keamanan siber.

c) Pembuatan

Berikut ini merupakan alur proses pembuatan dimulai dari identifikasi asset yang bertujuan untuk melakukan pendataan aplikasi yang ada di server instansi, kemudian dilakukan konfigurasi perangkat untuk menentukan aplikasi yang akan diproteksi oleh perangkat. Pada proses selanjutnya dilakukan monitoring fitur pada perangkat Next Generation Firewall (NGFW) yang dibutuhkan pada saat penelitian. Dalam hal ini akan dilakukan monitoring pada fitur network & threats.

Analisis tren cyber threats merupakan tahapan berikutnya untuk mendapatkan data dan informasi mengenai tren cyber threats pada instansi.

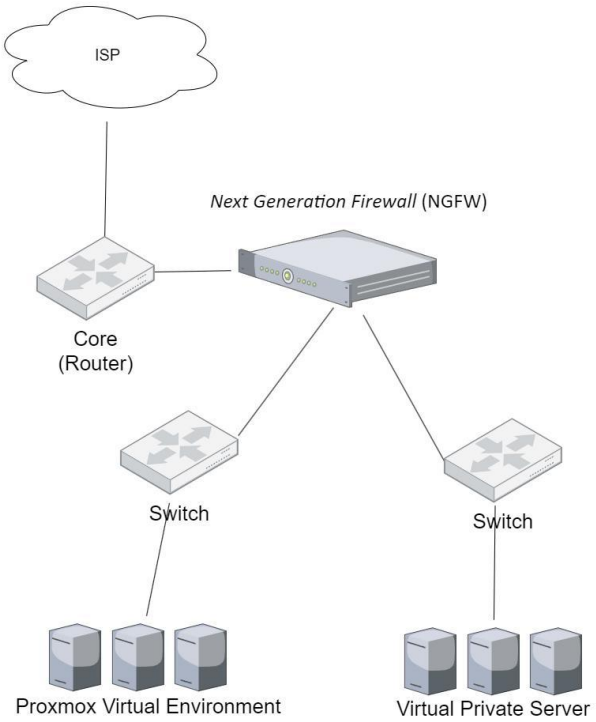
d) Pengujian

Pada tahap pengujian akan dilakukan monitoring penggunaan perangkat guna mengidentifikasi tren cyber threats yang terdeteksi dalam periode tertentu. Dari hasil monitoring akan diketahui jenis ancaman siber, maupun informasi lainnya dari penyerang

4. IMPLEMENTASI

a) Jaringan Usulan

Pada topologi jaringan usulan, perangkat Next Generation Firewall (NGFW) diposisikan antara perangkat Switch dengan perangkat Core (Router) yang terhubung ke Internet Service Provider. Dari perangkat Next Generation Firewall (NGFW), didistribusikan pada 2 perangkat Switch yang terhubung ke Virtual Environment dan Server Virtual Private Server pada Data Center. Berikut ini merupakan gambar topologi jaringan yang diusulkan :



Gambar 2. Topologi jaringan

Aturan firewall bertujuan untuk mengizinkan atau melarang arus lalu lintas antara zona dan jaringan serta menerapkan kebijakan dan tindakan keamanan. Konfigurasi tersebut berlaku untuk jaringan IPv4 dengan mengatur kriteria diantaranya seperti sumber, tujuan, layanan, dan pengguna selama jangka waktu tertentu. Pada firewall rules ini mengatur antara zona DMZ (demilitarized one) , WAN serta LAN. Zona DMZ demilitarized zone) atau biasa disebut dengan zona demiliterisasi yang merupakan sebuah pengaman jaringan dari trafik yang tidak tepercaya.

b) Pengujian Jaringan

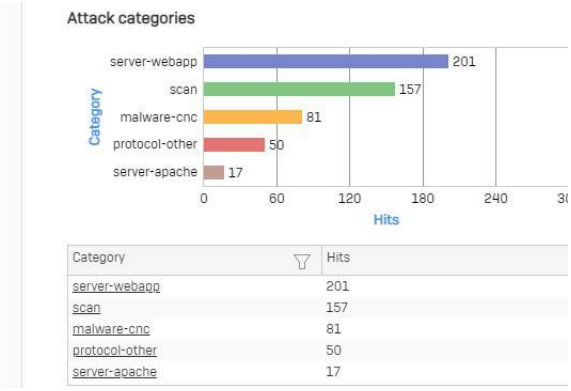
Tujuan dari ujicoba ini adalah untuk memastikan apakah perangkat Next Generation Firewall (NGFW) mampu mendeteksi adanya lalu lintas jaringan yang mencurigakan berkaitan dengan adanya serangan web defacement.

Identifikasi tren cyber threats dilakukan berdasarkan studi kasus yang terjadi pada instansi. Dengan identifikasi tersebut diharapkan dapat diketahui tren ancaman yang terjadi hingga menimbulkan adanya serangan web defacement pada web. Web defacement merupakan serangan yg dapat mengubah konten situs web yang dirusak dengan gambar atau pesan pilihan dari penyerang. Penyerang melakukan web defacement dengan mengubah tampilan web menjadi halaman yang menampilkan logo dan nama penyerang beserta tulisan lainnya.

Gambar 3. Serangan web defacement

Pada identifikasi tren cyber threats ini akan dilakukan analisis menggunakan data yang terdeteksi oleh perangkat Next Generation Firewall (NGFW). Attack categories merupakan hasil identifikasi untuk mengetahui kategori serangan yg terjadi. Berikut ini merupakan hasil identifikasi attack categories menggunakan perangkat Next Generation Firewall (NGFW).

Pada gambar 3. menunjukkan bahwa kategori serangan paling banyak yaitu server-webapp. Metodologi serangan server-webapp merupakan upaya menemukan sebanyak mungkin informasi tentang server target. Setelah mengumpulkan informasi, penyerang melakukan analisis untuk menemukan kelemahan dalam mekanisme keamanan dengan menemukan lebih banyak informasi tentang server web, seperti port dan layanan, aspek keamanan, dll.



Category	Hits
server-webapp	201
scan	157
malware-cnc	81
protocol-other	50
server-apache	17

Gambar 4. Identifikasi *attack categories*

Ini membantu peretas untuk mengetahui tentang kemampuan akses jarak jauh dari server. Kemudian dilakukan proses menyalin situs web dan kontennya ke server baru untuk menjelajahinya secara online. Pencerminan situs web membantu penyerang untuk melihat struktur situs web secara mendalam. Alat pemindaian kerentanan digunakan untuk mendeteksi kerentanan dan kesalahan konfigurasi di server. Peretas dapat mengambil alih sesi pengguna dan mendapatkan kendali penuh menggunakan pembajakan sesi. Peretas juga menggunakan beberapa metode peretasan kata sandi untuk menyusupi server.

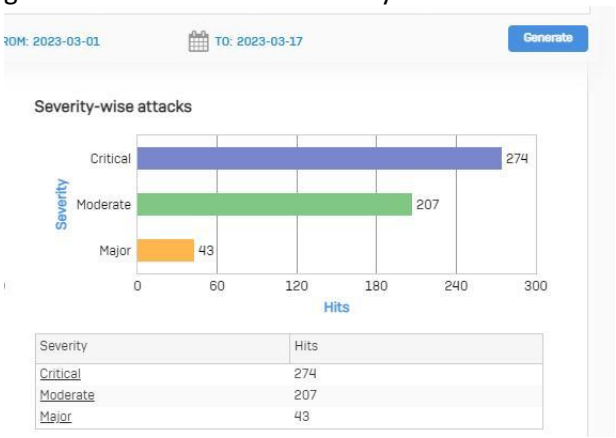
Metode-metode ini dapat berupa serangan brute force, dictionary attack, dll. Dampak yang ditimbulkan dengan adanya serangan terhadap server-webapp yaitu terjadinya serangan Denial Of Service attack, dan web defacement. Kategori serangan pemindaian (scan) merupakan upaya untuk memeriksa jaringan atau sistem komputer dengan menggunakan alat atau skrip otomatis untuk menemukan kerentanan atau mencari celah keamanan yang dapat dieksploitasi.

Dampak serangan pemindaian dapat bervariasi tergantung pada tujuan penyerang dan metode yang digunakan. Apabila target pemindaian adalah port maka dampaknya dapat mengetahui port yang terbuka pada sebuah sistem.

Sedangkan untuk kategori serangan malware-CNC (Command and Control) dapat memiliki dampak negatif yang signifikan yaitu dapat merusak sistem yang terinfeksi dengan cara menghapus atau mengubah file sistem, mengganggu operasi perangkat lunak, atau menghancurkan data penting.

Malware- CNC bahkan dapat membuat sistem tidak berfungsi sama sekali. Selain mengidentifikasi attack categories, perlu dilakukan identifikasi pula

terhadap severity wise attacks atau tingkat keparahan serangan. Berikut ini merupakan gambar hasil identifikasi severity wise attacks:

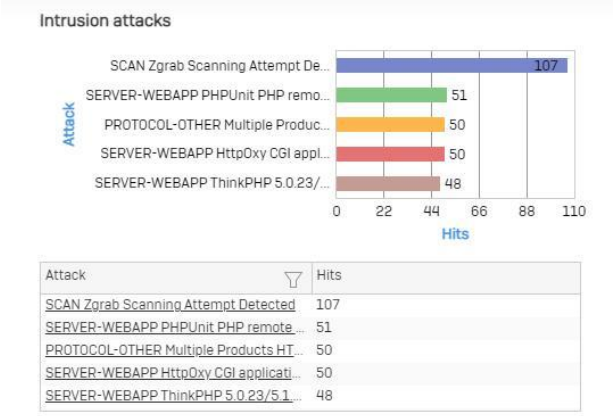


Gambar 5. Identifikasi severity-wise attacks

Pada gambar 4. menunjukkan bahwa target serangan ditujukan pada server dengan tingkat keparahan paling banyak pada tingkat critical. Serangan siber pada tingkat critical memiliki dampak yang serius dan meluas dalam berbagai aspek. Berikut adalah beberapa dampak yang dapat terjadi akibat serangan siber tingkat critical:

1) Pencurian Data Pribadi: Serangan siber tingkat critical sering kali bertujuan untuk mencuri data sensitif, termasuk informasi pribadi, seperti nomor kartu kredit, data medis, atau informasi identitas. Dampaknya dapat melibatkan pencurian identitas, penipuan keuangan, atau penyalahgunaan data pribadi lainnya.
2) Gangguan Layanan Publik: Serangan siber tingkat critical dapat mengganggu layanan publik yang penting bagi masyarakat, seperti sistem panggilan darurat, sistem keamanan publik, atau layanan kesehatan. Dampaknya bisa sangat serius dan bahkan mengancam nyawa manusia.
3) Kerugian Finansial: Serangan siber tingkat critical dapat menyebabkan kerugian finansial yang signifikan bagi perusahaan dan individu. Biaya yang terkait dengan memulihkan sistem, memperbaiki kerusakan, menginvestigasi serangan, dan menjaga keamanan ke depannya dapat menjadi sangat tinggi.
4) Penurunan Kepercayaan: Serangan siber tingkat critical dapat merusak kepercayaan masyarakat terhadap organisasi yang menjadi target serangan, termasuk pemerintah, perusahaan, atau lembaga publik. Kejadian ini dapat mengganggu hubungan bisnis, mempengaruhi reputasi, dan berdampak negatif pada citra suatu entitas. Oleh karena itu, serangan siber tingkat critical membutuhkan perhatian serius dan tindakan yang cepat untuk mencegahnya, melindungi infrastruktur penting, dan memperkuat pertahanan siber secara keseluruhan.

Dalam identifikasi cyber threats perlu diperhatikan pula terkait Intrusion attacks. Intrusion attacks atau biasa disebut serangan intrusi merupakan upaya yang dilakukan oleh pihak yang tidak sah untuk memasuki atau mengakses sistem komputer, jaringan, atau sumber daya lainnya secara tidak sah. Tujuan dari serangan intrusi adalah untuk mendapatkan akses yang tidak sah, mengambil alih kendali sistem, mencuri data sensitif, menyebabkan kerusakan, atau melakukan tindakan merusak lainnya. Berikut ini merupakan gambar hasil identifikasi intrusion attacks yang telah terdeteksi oleh perangkat Next Generation Firewall (NGFW).



Gambar 6. Identifikasi *instrusion attacks*

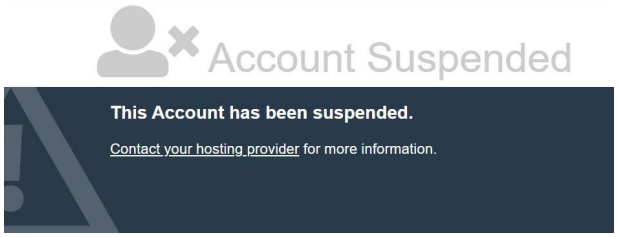
Pada gambar 4.7 menunjukkan bahwa intrusi serangan yang paling sering terjadi yaitu SCAN Zgrab Scanning Attempt Detected yang menunjukkan adanya upaya pemindaian untuk mengakses berbagai file di server oleh ZGrab Vulnerability Scanner. Karena akses ke file tersebut biasanya dibatasi, upaya untuk mengakses file tersebut mungkin menunjukkan upaya pengintaian oleh penyerang. Dampak dari adanya SCAN Zgrab Scanning adalah Information Disclosure atau biasa disebut penyerang dapat memperoleh informasi sensitif dari sistem yang rentan.

c) **Tindakan Respon Insiden**

Langkah yang diambil untuk mengatasi, menangani, dan memulihkan sistem dari serangan

atau insiden keamanan siber merupakan tindakan perbaikan dalam respon terhadap insiden siber. Tujuannya adalah untuk membatasi kerusakan, serta memulihkan sistem yang terkena, dan mencegah serangan serupa di masa depan. Tindakan respon insiden dilakukan dengan melakukan penahanan (containment), penghapusan (eradication) serta pemulihan (recovery).

Pada tahap penahanan (containment) dilakukan dengan menonaktifkan sistem yang terkena serangan untuk menjaga dampak dari sebuah insiden agar tidak tersebar secara luas. Berikut ini merupakan gambar sistem yang sudah dinonaktifkan:



Gambar 7. Menonaktifkan sistem aplikasi

Setelah tahap penahanan (containment) kemudian melakukan tahap penghapusan (eradication) yang bertujuan untuk melakukan restorasi sistem yang terkena serangan. Kegiatan yang dilakukan pada tahap penghapusan (eradication) yaitu menghilangkan komponen-komponen insiden seperti menghapus malicious file yang diupload oleh penyerang. Kemudian pada tahap terakhir merupakan tahap pemulihan (recovery). Fase Pemulihan ini merupakan fase dimana sistem yang terkena insiden berjalan normal sama seperti sebelum terdampak insiden. Berikut ini merupakan gambar sistem yang sudah dipulihkan:

Gambar 8. Memulihkan sistem aplikasi

Melakukan pemulihan sistem dengan menggunakan file backups yang terakhir dimiliki dan memastikan celah atau pemicu insiden tertutup sehingga tidak terulang kembali pada sistem yang sudah dipulihkan tersebut. Melakukan validasi sistem untuk memastikan sudah tidak ada aplikasi atau file yang rusak atau terinfeksi. Begitu pula kesalahan atau kekurangan konfigurasi sistem untuk kemudian disesuaikan kembali.

5. KESIMPULAN

Perangkat Next Generation Firewall (NGFW) berhasil mendeteksi jenis intrusi dan kategori serangan pada kasus web defacement yang terjadi. Dengan intrusi dan kategori serangan tersebut memungkinkan penyerang mendapatkan celah kerentanan pada server web yang berakibat terjadinya information disclosure atau penyerang mendapatkan informasi sensitif dari sistem yang rentan. Tindakan yang disarankan yaitu memantau lalu lintas dari jaringan untuk mengetahui adanya aktivitas yang mencurigakan. Selain itu untuk membatasi adanya malicious file yang diupload oleh pengguna, dapat dilakukan penambahan kode pada fungsi upload file yaitu dengan membatasi hanya file-file tertentu yang dapat di-upload serta melakukan backup dan update akun secara periodik untuk mencegah adanya insiden yang terjadi.

DAFTAR PUSTAKA

BSSN, Badan Siber dan Sandi Negara. (2021). Laporan Tahunan Monitoring Keamanan Siber. Jakarta Selatan: Badan Siber dan Sandi Negara.

Fitria, A. (2020). Implementasi Double Deep Packet Intrusion Detection Dan Prevention System (IDPS) Inspection dengan Perangkat Firewall NGFW dan Application Security Manager Pada Cloud Datacenter PT.XYZ. UG JURNAL, 14 (6), 1-17. Diambil darihttps://ejournal. gunadarma. ac.id/index.p hp/ugjournal/article/view/4950

Fitrianti. (2014). Membangun Model Kebijakan Nasional Keamanan Siber Dalam Sistem Pertahanan Negara. Jakarta: Universitas Pertahanan Indonesia.

Indriantoro, N. dan Supono, B. (2013). Metodologi Penelitian Bisnis Untuk Akuntansi dan Manajemen. Yogyakarta: FEB Universitas Gajah Mada.

Putra, R. D., Supartono, dan Deni D.A.R. (2018). Ancaman Siber Dalam Persfektif Pertahanan Negara, siber Threats In State Defense Persfectives, Jurnal Prodi Perang Asimetris | Agustus 2018, 4(2). Diambil dari : https://jurnalprodi.idu.ac.id/index.php/PA/article/download

Sugiyono. (2015). Metodelogi Penelitian Kuantitatif, Kualitatif Dan R&D. Bandung: Alfabeta.

Van Busten, M. (2009). Optimalisasi Firewall Pada Jaringan Skala Luas. Jar. Komput. Malang: Universitas Brawijaya.

Whitman, M. E., & Mattord, H. J. (2010). Management of information security, Third Edition. Boston: Course Technology

Yusuf, M. L., Karsono,K, dan Budhisantosa, N. (2020). Analisis Performance Next Generation Firewall dan Mikrotik RB1100 Sebagai Firewall Untuk Keamanan Jaringan. JIK: Jurnal Ilmu Komputer, 5(1), 15-30. Diambil dari https://ejurnal.esaunggul.ac.id/index.php/JIK /article/view/4613.