IMPLEMENTASI MAIL GATEWAY SECURITY DALAM MENINGKATKAN KEAMANAN EMAIL

Syaeful Anas Aklani [1] , Haeruddin [2], Novita Putri [3]

[1),3)] Sistem Informasi Universitas Internasional Batam
[2)] Teknologi Informasi Universitas Internasional Batam
email : syaeful@uib.ac.id [1)], haeruddin@uib.ac.id [2)], 2031058.novita@uib.edu [3)]

Abstraksi

Penelitian ini bertujuan untuk menerapkan *Mail Gateway Security* pada perusahaan PT. Pundi Mas Berjaya. *Email* merupakan salah satu alat komunikasi utama di perusahaan, baik untuk internal maupun eksternal. Dalam konteks ini, *email gateway security* menjadi penting untuk melindungi informasi sensitif perusahaan. Ancaman seperti *phising*, yang mencuri informasi melalui *email* palsu, *malware* yang merusak sistem, dan *spam* yang mengganggu produktivitas, memerlukan perlindungan yang efektif. Penerapan metode *Mail Gateway Security* merupakan sebuah metode untuk memecahkan masalah dan dilakukan dengan menggunakan pendekatan *Network Development Life Cycle* (NDLC), meliputi tahapan Analisis yang melibatkan identifikasi ancaman dan risiko terhadap email server perusahaan, Desain melibatkan pengembangan topologi sistem *mail gateway* dengan memanfaatkan layanan Aktiva berbasis *cloud*, Implementasi dengan menambahkan reputasi *email server* dan mengkonfigurasikan *mail server Zimbr*a. Hasilnya menunjukan peningkatan keamanan *email* perusahaan, pengurangan spam, dan kemudahan pemantauan aktivitas pengiriman *email*, dengan penerapan *Mail Gateway Security* berbasis *cloud*, perusahaan dapat melindungi data sensitif, menjaga reputasi, dan meningkatkan keberlanjutan bisnis di era digital yang penuh dengan ancaman *cyber*.

Kata Kunci :
Mail Gateway Security, Mail Server, NDLC

Abstract

This research aims to implement Mail Gateway Security at PT. Pundi Mas Berjaya. Email is one of the primary communication tools within the company, used for both internal and external purposes. In this context, email gateway security becomes crucial to protect sensitive company information. Threats such as phishing, which steals information through fake emails, malware that damages systems, and spam that disrupts productivity, require effective protection. The implementation of the Mail Gateway Security method is an approach to solving these problems and is carried out using the Network Development Life Cycle (NDLC) approach, involving the Analysis phase that identifies threats and risks to the company's email server, the Design phase that develops the topology of the mail gateway system using Activa cloud-based services, and the Implementation phase that adds reputation to the email server and configures the Zimbra mail server. The results show an improvement in the company's email security, a reduction in spam, and ease of monitoring email delivery activities. With the implementation of cloud-based Mail Gateway Security, the company can protect sensitive data, maintain its reputation, and enhance business sustainability in this digital era filled with cyber threats.

***Keywords* :**
Mail Gateway Security, Mail Server, NDLC

Pendahuluan

Seiring berkembangnya Teknologi Informasi, khususnya jaringan internet, banyak pengguna menjadi semakin mudah dalam melakukan komunikasi lewat daring dengan internet. Internet merupakan jaringan komunikasi yang menghubungkan jutaan individu yang terpisah oleh jarak, waktu dan di seluruh belahan dunia. Dengan adanya kehadiran internet, orang-orang di seluruh dunia dapat terhubung dengan cepat dan akurat bahkan ketika mereka terpisah oleh jarak yang sangat jauh, karena Internet adalah sarana komunikasi yang paling diminati [1]. Bahkan internet telah menjadi suatu kebutuhan pokok bagi setiap individu [2]. Meningkatnya pengguna internet juga berdampak pada meningkatnya risiko privasi yang dapat mengancam informasi pribadi [3]. Oleh karena itu perlu adanya sistem keamanan informasi. Keamanan informasi dan privasi data merupakan hal yang sangat penting bagi setiap organisasi, baik pemerintah, swasta, maupun non-profit, termasuk PT. Pundi Mas Berjaya. Perusahaan ini bergerak dibidang penyedia jasa solusi untuk perangkat lunak, dan infrastruktur Teknologi Informasi kepada klien di seluruh dunia, melalui tim yang kreatif dan berdedikasi profesional. Perusahaan ini berdiri pada tahun 2014, dimana telah

merancang, mengembangkan, dan menerapkan banyak solusi di bidang seperti *property*, otomotif, transportasi, pengiriman makanan, pengiriman barang dan *ecommerce* [4].

Salah satu media komunikasi yang paling banyak digunakan di perusahaan adalah *email*. Tentunya pegawai-pegawai yang bekerja diperusahaan tersebut menggunakan *email* sebagai sarana komunikasi karena perusahaan menggunakan *email* untuk berkomunikasi di internal dan eksternal. Komunikasi internal meliputi komunikasi antara karyawan, dan komunikasi eksternal digunakan dengan pihak luar perusahaan, seperti pelanggan, pemasok, atau mitra bisnis. Secara umum hal ini yang membuat *email* menjadi sarana komunikasi yang penting dalam perusahaan dan mudah digunakan serta dimengerti oleh semua orang. Dengan menggunakan *email* secara efektif, pegawai perusahaan dapat meningkatkan efektivitas dan efisiensi komunikasi dalam perusahaan. Jika informasi penting Perusahaan disebarluaskan, dapat menimbulkan risiko kerugian bagi bisnis Perusahaan. Oleh karena itu, penting untuk memiliki sistem keamanan saat menggunakan *email* di perusahaan. Mengamankan *email* perusahaan merupakan hal yang sangat penting karena *email* sering kali menjadi sarana utama komunikasi bisnis dan menyimpan banyak informasi sensitif dan penting, dikarenakan *email* sangat mudah terjadi serangan seperti serangan *Phising*, *Malware*, *Spam*, dan *Virus*. Bentuk kejahatan siber yang dilakukan oleh penipu (*scammers)* adalah tindakan *phising* [5]. *Phising* merupakan ancaman umum terhadap aspek privasi keamanan informasi yang penting sehingga penting bagi pegawai perusahaan untuk menyadari adanya konsep dan bahayanya. *Phising* adalah tindakan kriminal yang mencuri informasi pribadi orang lain dengan menggunakan entitas elektronik, yang salah satunya adalah *email* [6]. *Malware* adalah *software* yang dapat digunakan untuk mengganggu perangkat komputer, mengumpulkan informasi sensitif, atau mengakses sistem komputer [7]. *Spam* merupakan surat sampah atau *email* yang tidak diminta, sering kali dikirim dalam jumlah besar ke penerima yang tak terhitung jumlahnya di seluruh dunia dan sering kali berhubungan dengan narkoba atau pornografi [8]. *Virus* adalah program yang dapat menggandakan dirinya sendiri dan menyebar ke komputer lain, virus pada *email* biasanya menyebar melalui lampiran *email* yang terinfeksi. *Virus* biasanya menyebar melalui *email*. Seringkali orang yang sistem *email*-nya terinfeksi *virus* tidak menyadarinya, *virus* tersebut kemudian dikirimkan ke tempat lain melalui *email*-nya [9]. Dampak lain dari serangan diatas dapat menyebabkan *mail server* tidak dapat mengirim *email* ke eksternal karena masuk kategori *blacklist*.

Oleh karena itu perlu adanya sistem keamanan yang dapat melindungi *email server* agar dapat beroperasi dengan baik. Salah satu sistem yang dapat mengurangi risiko serangan tersebut yaitu dengan menggunakan *Mail Gateway Security*. *Mail Gateway Security* ini merupakan sebuah perangkat atau layanan yang digunakan untuk melindungi *email* dari berbagai ancaman, seperti *spam*, *phising*, *malware*, dan *virus*. Sistem ini di tempatkan di antara jaringan internal dan internet, sehingga dapat memindai semua *email* yang masuk dan keluar dari jaringan. Dengan adanya sistem keamanan *email* yang sangat tinggi dapat membantu individu dan organisasi untuk menghindari serangan *phising*, *malware*, *spam*, *virus*, dan meminimalisir *blacklist* [10]. Mengamankan *email* merupakan investasi yang sangat penting dalam menjaga keberlanjutan dan keberhasilan bisnis serta melindungi data dan reputasi perusahaan tersebut. Pegawai perlu membiasakan diri untuk konsisten dalam meningkatkan perilaku keamanan siber mereka [11]. Oleh sebab itu Sistem Keamanan Perusahaan harus ditingkatkan, salah satunya dengan menggunakan Sistem *Mail Gateway Security*. Sistem ini dapat membantu melindungi Perusahaan dari berbagai serangan *email* dengan cara, Memblokir spam, mendeteksi dan menghapus *malware*, memindai *email* untuk *phising*.

Berdasarkan latar belakang di atas, bagaimana menerapkan *Sistem Mail Gateway Security*. Dimana menggunakan metode *Network Development Life Cycle* (NDLC). Metode ini digunakan agar penerapan *Sistem Mail Gateway Security* secara sistematis, sehingga apa yang akan dicapai sesuai dengan tujuan.

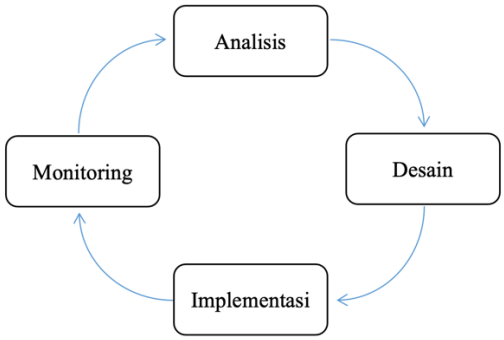
Tinjauan Pustaka

Email adalah bentuk komunikasi resmi dalam dunia bisnis yang memiliki peranan krusial, tetapi sekaligus membawa risiko terhadap ancaman-ancaman kriminal yang berbasis email. Beberapa contoh dari ancaman tersebut melibatkan praktik seperti spam, phising, malware, dan spoofing. Umumnya, pesan spam berisi konten promosi terkait berbagai produk dan jasa. Jenis spam yang paling dikenal adalah inbound spam, yaitu spam yang masuk langsung ke dalam kontak surat elektronik (mailbox) pengguna [12]. Spam biasa dikenal sebagai email komersial tanpa izin atau email berlebihan tanpa izin, yang dapat menimbulkan berbagai masalah dalam komunikasi sehari-hari. Dampak negatif yang diakibatkan oleh spam seperti iklan perjudian dan konten pornografi. Spam atau email sampah merupakan bentuk penyalahgunaan pengiriman pesan elektronik yang digunakan untuk menampilkan berita, iklan, dan lainya, yang dapat mengakibatkan ketidaknyamanan bagi para pengguna [13]. Kemudian phising juga merupakan salah satu tindakan kejahatan yang dimana phising dilakukan untuk menarik korban ke dalam jebakan phisher, phisher biasa menggunakan email, spanduk, atau pop-up untuk menipu pengguna agar mengakses halaman web tiruan, dimana pengguna kemudian diminta untuk memberikan informasi pribadi [14]. Mail server berperan sebagai server yang bertugas mengirim dan menerima pesan email, mirip dengan fungsi kantor pos. Fungsinya melibatkan berbagai tugas penting, termasuk penyimpanan dan keamanan

data instansi atau perusahaan yang terdapat dalam pesan email. Mail server ini bekerja dalam jaringan pribadi karena hanya digunakan oleh perusahaan atau instansi yang memiliki mail server tersebut [15]. Mail gateway yang bekerja dengan menganalisis konten email yang menyaring pesan yang mencurigakan atau berbahaya, dan memastikan bahwa email yang masuk atau keluar mematuhi kebijakan keamanan dan aturan tertentu. Selain itu, mail gateway juga dapat menyediakan enkripsi untuk melindungi keamanan informasi yang dikirim melalui email [16].

Metode Penelitian

Network Development Life Cycle (NDLC) terdapat beberapa tahapan meliputi analisis, desain, implementasi dan pemantauan. Tahapan-tahapan ini yang digunakan untuk mengembangkan dan mengimplementasikan sistem *Mail Gateway Security* [17], [18]. Metode NDLC ini dapat membantu untuk mengimplementasikan sistem *Mail Gateway Security* secara teratur, efisien, dan sesuai dengan kebutuhan penelitian ini. Berikut adalah penjelasan tahapan-tahapan *Network Development Life Cycle* (NDLC) yang akan diterapkan pada penelitian ini:



Gambar 1. *Network Development Life Cycle* (NDLC)

1. Analisis

Pada tahapan ini akan mengidentifikasikan ancaman dan risiko yang dihadapi *email server* perusahaan. Ancaman dan risiko tersebut dapat berasal dari berbagai sumber, seperti *malware*, *phising*, dan *spam*.

2. Desain

Pada tahap ini akan mengembangkan desain meliputi topologi perancangan Sistem *Mail Gateway Security* menggunakan draw.io. Rencana tersebut mencakup spesifikasi teknis untuk *Mail Gateway Security* yang akan digunakan.

3. Implementasi

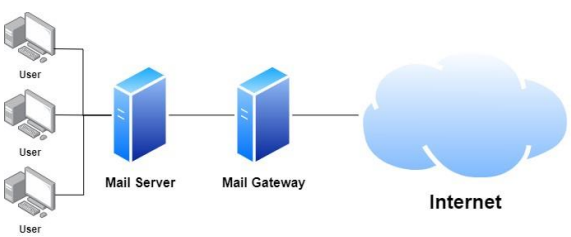
Pada tahapan ini melakukan penerapan, instalasi, konfigurasi *Mail Gateway Security* sesuai dengan rencana yang telah didesain pada tahapan sebelumnya. Kemudian, melakukan uji coba untuk memastikan bahwa *Mail Gateway Security* berfungsi. Implementasi merupakan langkah sebenarnya yang menentukan sukses/gagalnya suatu proyek yang akan dibangun [19].

4. Monitoring

Pada tahap monitoring ini penulis akan melakukan pemantauan dan pengujian terhadap kinerja *Mail Gateway Security* untuk memastikan bahwa sistem ini dapat melindungi *email server* perusahaan dari ancaman dan risiko.

Hasil dan Pembahasan

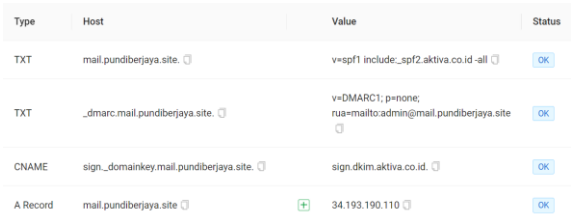
Email spam, *email malware*, dan *phising* adalah jenis *email* berbahaya yang dapat menyebabkan dampak negatif bagi individu dan organisasi. *Email spam* dapat mengganggu produktivitas dengan memenuhi kotak masuk pengguna dengan pesan yang tidak diinginkan dan tidak relevan. Hal ini dapat membuat sulit untuk menemukan email penting dan menghabiskan waktu untuk menyortir *email spam*. *Email spam* terkadang berisi tautan atau lampiran berbahaya yang dapat menginstal *malware* di komputer Anda atau mencuri informasi pribadi pengguna. *Email spam* dapat merusak reputasi pengguna dengan membuat terlihat seperti seseorang yang tidak profesional atau tidak memperhatikan keamanan *email*. Selain itu terdapat ancaman lain seperti *email malware* yang dapat mencuri informasi pribadi Anda, seperti nama, alamat, nomor telepon, dan informasi keuangan. Informasi ini kemudian dapat digunakan untuk melakukan penipuan identitas atau kejahatan lainnya. *Malware* juga dapat menyandera file Anda dan menuntut tebusan untuk melepaskannya. Hal ini dapat menyebabkan pengguna kehilangan data penting atau bahkan merusak komputer. Ancaman lain yang berbahaya adalah *phishing* yang sering digunakan untuk menipu orang agar mengungkapkan informasi keuangan mereka, seperti nomor kartu kredit atau kata sandi *bank*. Informasi ini kemudian dapat digunakan untuk melakukan penipuan atau pencurian identitas. *Phishing* juga dapat merusak reputasi pengguna atau reputasi organisasi. Jika seseorang tertipu oleh *email phishing* yang dikirim dari alamat *email* pengguna atau alamat *email* organisasi, dapat menimbulkan hilangnya reputasi pengguna. Oleh karena itu penting untuk meningkatkan sistem keamanan *mail server*.
Adapun tahapan penggunaan *Mail Gateway Security* sebagai berikut : [20]



Gambar 2. Skema Jaringan *Mail Gateway Security*

Pada gambar 2 merupakan desain skema jaringan yang menerapkan keamanan *mail server* menggunakan *mail gateway security*. Pada gambar

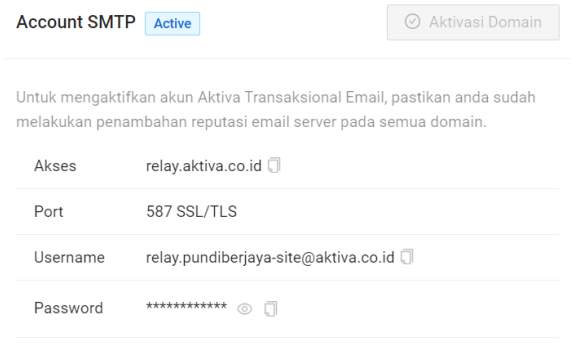
tersebut dapat dilihat bahwa pada saat *mail server* ingin mengirim *email* ke luar atau menerima *email* dari luar akan melalui *email gateway security*. *Email gateway security* menggunakan aktiva berbasis *cloud*. *Mail server* secara normal akan melakukan pengiriman *email* ke *server* dengan domain yang berbeda secara langsung, dengan menggunakan *mail gateway security*, makan *mail server* akan mengirim *email* ke *server gateway security* terlebih dahulu. Selanjutnya *mail gateway* yang akan meneruskan ke e*mail* tujuan. Sehingga *mail server* pada dasarnya hanya membutuhkan koneksi ke *mail gateway security*, sedangkan *mail gateway security* harus terhubung ke *internet*. Sehingga *mail server* tidak memerlukan proteksi yang tinggi, melainkan *mail gateway* yang sudah memiliki fitur untuk mencegah jika terjadi ancaman pada *email*.



Gambar 3. Penambahan reputasi *email*

Tahapan berikutnya adalah melakukan implementasi *mail gateway security*. Pada penelitian ini menggunakan *email server* Zimbra 8.8.15 Colaboration yang berjalan pada sistem operasi Ubuntu *server* 20.04 LTS, dan *mail gateway* menggunakan Aktiva berbasis *cloud*. Pada tahapan pertama penambahan Reputasi *Email Server*. Penambahan reputasi untuk meningkatkan akurasi penerimaan *email* di *inbox* penerima dengan menambahkan record SPF, DMARC dan DKIM di DNS Public.

Tahapan kedua, melakukan konfigurasi pada *mail server Zimbra* untuk mengarahkan pengiriman *email* melalui *gateway*.

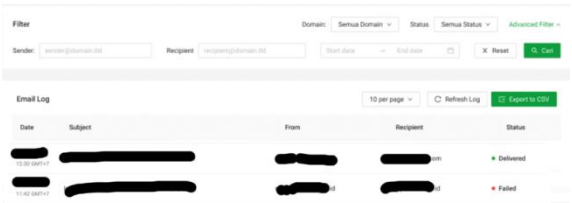


Gambar 4. Akun SMTP

1. Remote server Zimbra menggunakan SSH dan akses ke console
2. Login sebagai user root dari sistem operasi Linux
3. Jalankan perintah berikut untuk login sebagai user Zimbra

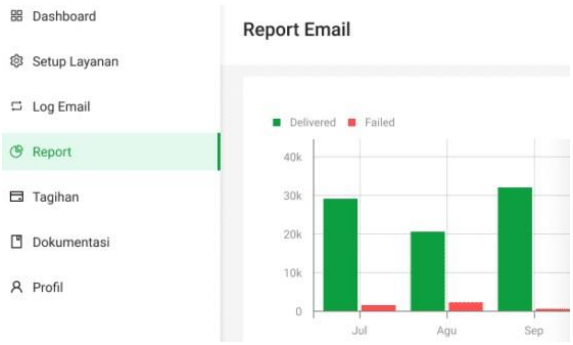
   su - zimbra
4. Ketikkan perintah berikut pada console email server Zimbra

   echo 'relay.aktiva.co.id relay.pundiberjaya-site@aktiva.co.id:(nBChLWzxVL3XXXXXXX> /opt/zimbra/conf/relay_password
   postmap /opt/zimbra/conf/relay_password
   postmap -q relay.aktiva.co.id /opt/zimbra/conf/relay_password
   zmprov ms `zmhostname` zimbraMtaSmtpSaslPasswordMaps lmdb:/opt/zimbra/conf/relay_password
   zmprov ms `zmhostname` zimbraMtaSmtpSaslAuthEnable yes
   zmprov ms `zmhostname` zimbraMtaSmtpCnameOverridesServername no
   zmprov ms `zmhostname` zimbraMtaSmtpTlsSecurityLevel may
   zmprov ms `zmhostname` zimbraMtaSmtpSaslSecurityOptions noanonymous
   postconf -e sender_dependent_default_transport_maps=lmdb:/opt/zimbra/conf/aktiva-bysender
   echo '#List Domain Relay' > /opt/zimbra/conf/aktiva-bysender
   postmap /opt/zimbra/conf/aktiva-bysender
   postfix reload



Gambar 5. Log pengiriman *email*

Pada gambar 5 merupakan log pengiriman *email* yang di kirim dari *mail server* dengan menggunakan email *gateway*. Tampilan ini dilihat pada dashboard pada laman aktiva *mail gateway*.



Gambar 6. Report pengiriman *email*

Pada gambar 6 merupakan report pengiriman *email* setiap bulan, dimana terdapat *email* yang terkirim dan *email* yang gagal.

Oleh karena itu, jika tanpa menggunakan Mail Gateway Security, email server Perusahaan menjadi lebih rentan terhadap berbagai ancaman siber seperti spam, phishing, malware, dan virus. Ancaman-ancaman ini dapat mengakibatkan dampak negatif pada Keamanan informasi, produktivitas, dan reputasi Perusahaan. Pegawai perlu menghadapi risiko penerimaan email spam yang mengganggu, potensi serangan phising yang dapat menyebabkan kehilangan data sensitif, serta risiko terkena malware atau virus yang dapat merusak sistem dan menyebabkan kerugian finansial.
Dengan menerapkan Mail Gateway Security, Perusahaan dapat mengurangi risiko dan dapat meningkatkan Keamanan email secara signifikan. Efek positifnya meliputi:

a. Pengurangan Spam
Mail gateway security dapat menyaring dan memblokir email spam secara efektif, mengurangi gangguan pada kotak masuk pengguna dan meningkatkan focus pada email yang benar-benar penting.

b. Deteksi dan Pencegahan Phising
Sistem ini dapat mendeteksi pola dan karakteristik phising dalam email, membantu mencegah pegawai jatuh korban dari upaya penipuan phising.

c. Proteksi dari Malware dan Virus
Mail gateway security dapat memindai lampirkan email dan tautan yang mencurigakan, mencegah malware dan virus masuk ke dalam sistem Perusahaan. Ini dapat melindungi data sensitive dan mencegah kerusakan pada perangkat.

d. Tindakan Pencegahan
Mail gateway security memberikan kemampuan pemantauan aktivitas email secara real-time, memungkinkan Perusahaan untuk mengidentifikasi dan menanggapi potensi ancaman dengan cepat.

Mail Gateway Security bekerja sebagai lapisan pertahanan tambahan antara email server Perusahaan dan internet. Berikut adalah langkah-langkah umum cara kerja Mail gateway security :

a. Pemindaian Email
Setiap email yang masuk dan keluar dari email server Perusahaan diperiksa oleh mail gateway security. pemindaian mencakup Pengecekan terhadap spam, phising, malware, dan virus.

b. Filtrasi Konten
Mail gateway security melakukan filtrasi konten untuk memastikan bahwa email yang masuk sesuai dengan kebijakan Keamanan Perusahaan. Ini melibatkan identifikasi dan penolakan email dengan konten yang mencurigakan atau berbahaya.

c. Deteksi Pola dan Tanda Tangan
Jika ancaman terdeteksi, mail gateway security akan mengambil Tindakan pencegahan sesuai dengan kebijakan yang telah ditetapkan. Ini bisa mencakup memindahkan email ke folder spam, menolak pengiriman, atau memberikan peringatan kepada pengguna.

d. Enkripsi dan Dekripsi
Beberapa mail gateway security juga menyediakan layanan enkripsi untuk melindungi Keamanan informasi yang dikirim melalui email.

e. Pemantauan dan Pelaporan
Mail gateway security menyediakan fungsi pemantauan dan pelaporan yang memungkinkan Perusahaan untuk melacak aktivitas email, menganalisis potensi ancaman, dan menghasilkan laporan Keamanan.

Dengan cara ini, maka Mail Gateway Security tidak hanya memberikan perlindungan terhadap ancaman siber, tetapi juga membantu Perusahaan dalam mengelola risiko Keamanan email dengan cara yang efisien.

Kesimpulan dan Saran

Implementasi Mail Gateway Security dengan melibatkan metode *Network Development Life Cycle* (NDLC) menggunakan layanan Aktiva berbasis cloud terbukti efektif. Langkah-langkah yang mencakup penambahan reputasi *email server*, mengkonfigurasi *mail server Zimbra*, dan memantau aktivitas pengiriman *email* yang memberikan hasil positif. Layanan ini tidak hanya mempercepat pengiriman *email*, tetapi juga memberikan perlindungan terhadap *spam*, *malware*, *virus*, dan *phising*. Hasil dari penelitian ini menunjukan bahwa layanan Aktiva *Mail Gateway* berbasis *cloud* efektif dalam melindungi *email server*, mengurangi *spam*, dan memudahkan pemantauan aktivitas pengiriman *email*. Dengan ini, penerapan *mail gateway security* dengan pendekatan *Network Development Life Cycle* (NDLC), khususnya dengan menggunakan layanan Aktiva *mail gateway*, dapat meningkatkan keamanan *email* perusahaan, melindungi data sensitif, dan menjaga reputasi perusahaan dari ancaman dunia maya.

Daftar Pustaka

[1] P. Tampubolon, Syaeful, E. Lau, F. Favian, and R. Winata, “Penggunaan Internet Sehat Dan Aman Pada Siswa-Siswi Sekolah Menengah Atas Swasta Maha Bodhi Karimun,” *Prosiding National Conference for Community Service Project (NaCosPro)*, vol. 4, no. 1, pp. 140–144, 2022, [Online].

Available: http://journal.uib.ac.id/index.php/nacospro

[2] Y. A. B. Suprio and M. Najib, "Analisa Dampak Kesadaran Keamanan Informasi Pengguna Aplikasi Whatsapp Terhadap Penyebaran Link Web Phising," *Institut Teknologi dan Bisnis Stikom Bali*, pp. 318–322, 2022.

[3] L. N. Elsa, A. C. Nur, N. M. Putu Jeanny, and A. I. S. Ramadhana, "Kesadaran Ancaman Privasi Serta Perilaku Perlindungan Privasi dalam Menggunakan Sosial Media," *Seminar Nasional Teknologi dan Sistem Informasi*, pp. 101–109, 2021.

[4] " PT. PUNDI MAS BERJAYA." Accessed: Jan. 05, 2023. [Online]. Available: https://www.pmberjaya.com/

[5] A. Muftiadi, T. P. M. Agustina, and M. Evi, "Studi Kasus Keamanan Jaringan Komputer: Analisis Ancaman Phising Terhadap Layanan Online Banking," *Hexatech : Jurnal Ilmiah Teknik*, vol. 1, no. 2, pp. 60–65, 2022.

[6] Rumini, Norhikmah, A. Mustofa, and S. Pradana, "Perbandingan Pengujian Deteksi Phising menggunakan Metode SVM dengan Kernel RBF dan Linear," *SISTEMASI:Jurnal Sistem Informasi* , vol. 12, no. 3, pp. 754–759, 2023, [Online]. Available: http://sistemasi.ftik.unisi.ac.id

[7] A. R. Q. Syahwidi, S. Cahyono, and R. N. Yasa, "Analisis Aplikasi Cryptowallet Tiruan Terhadap Indikasi Android Malware," *INFO KRIPTO Jurnal Ilmiah Kriptologi*, vol. 17, no. 1, pp. 23–31, 2023.

[8] N. Adila, S. Khasanah, and T. Sutabri, "Strategi Perancangan Sistem Amavis dan Spamassassin pada Spam Mail," *Jurnal Sain dan Teknik*, vol. 5, no. 2, pp. 154–166, 2023.

[9] A. Suhaemin and Muslih, "Karakteristik Cybercrime di Indonesia," *EduLaw : Journal of Islamic Law and Yurisprudance*, vol. 5, no. 2, pp. 15–26, 2023.

[10] N. Vadila and A. R. Pratama, "Analisis Kesadaran Keamanan Terhadap Ancaman Phishing," *Automata*, vol. 2, no. 2, 2021.

[11] A. Kusumaningrum, H. Wijayanto, and B. D. Raharja, "Pengukuran Tingkat Kesadaran Keamanan Siber di Kalangan Mahasiswa saat Study From Home dengan Multiple Criteria Decision Analysis (MCDA)," *Jurnal Ilmiah SINUS*, vol. 20, no. 1, pp. 69–78, Jan. 2022, doi: 10.30646/sinus.v20i1.586.

[12] A. Harbani and A. Sidiyantoro, "Implementasi Simple Mail Transfer Protocol Relay Pada Mail Gateway Untuk Menentukan Konten Email Spam," *Jurnal Ilmiah Teknologi - Informasi & Sains*, vol. 12, no. 1, pp. 57–66, 2022, doi: 10.36350/jbs.v12i1.

[13] H. Hassanah, "Tindakan Hukum Terhadap Pelaku Penyebaran Virus Komputer Melalui E-Mail (Cyber Spamming) Berdasarkan Ketentuan Tentang Informasi dan Transaksi Elektronik," *Res Nullius Law Journal*, vol. 5, no. 1, pp. 1–8, 2023, doi: 10.34010/rnlj.v%vi%i.8317.

[14] E. Ginting, M. P. Sinaga, M. R. Nurdin, and M. D. Putra, "Analisis Ancaman Phising Terhadap Layanan Online Perbankan (Studi Kasus Pada Bank BRI)," *UNES Journal of Scientech Research*, vol. 8, no. 1, pp. 41–47, 2023, [Online]. Available: https://ojs.ekasakti.org/i

[15] A. A. Lubis, J. Pinem, M. A. S. Lubis, and D. Kiswanto, "Implementasi Roundcube pada Mail Server untuk Lingkungan Program Studi Ilmu Komputer UNIMED," *BLEND SAINS JURNAL TEKNIK*, vol. 1, no. 3, pp. 194–201, 2023, doi: 10.12345/10.56211/blendsains.v1i3.163.

[16] I. G. M. N. Desnanjaya, A. A. G. B. Ariana, I. M. A. Nugraha, and I. G. Adnyana, "Sistem Informasi Persuratan Berbasis Web dan SMS Gateway," *Informatics Journal*, vol. 7, no. 1, pp. 1–15, 2022.

[17] H. Haeruddin and K. Kelvin, "Analisa Penggunaan VPN L2TP dan SSTP di Masa Pandemi Covid-19," *Jurnal Ilmu Komputer dan Bisnis*, vol. 13, no. 1, pp. 105–114, May 2022, doi: 10.47927/jikb.v13i1.279.

[18] A. Averian, A. Budiono, and U. Y. Kurnia, "Analisis dan Pengoptimalisasi Jaringan Wireless Local Area Network (WLAN) Pada PT.XYZ Dengan Menggunakan Metode Network Development Life Cycle (NDLC)," *e-Proceeding of Engineering*, vol. 10, no. 2, pp. 1325–1330, 2023.

[19] Suhendri, D. Susanti, and D. Dicky, "Penerapan Keamanan Email dengan Sistem Pretty Good Privacy Menggunakan Metode NDLC (Studi Kasus : Polres Majalengka)," *INFOTECHjournal*, vol. 6, no. 2, pp. 1–9, 2020.

[20] R. Sahtyawan, "Penerapan Zero Entry Hacking didalam Security Misconfiguration pada VAPT (Vulnerability Assessment and Penetration Testing)," *JURNAL OF INFORMATION SYSTEM MANAGEMENT*, vol. 1, no. 1, pp. 18–22, 2019.