PANDUAN PENGAMANAN

SISTEM OPERASI MAIL SERVER

GOV-CSIRT (Government Computer Security Insident Response Team)

Pusat Monitoring dan Penanganan Insiden Keamanan Informasi Instansi Pemerintah

Direktorat Kemanan Informasi

Kementerian Komunikasi dan Informatika Republik Indonesia

Pengamanan terhadap Sistem Operasi Mail Server

Lima langkah dasar yang diperlukan untuk menjaga keamanan sistem operasi :

- Perencanaan instalasi dan penerapan sistem operasi host dan komponen lainnya untuk servermail
- Patch dan update sistem operasi host yang diperlukan
- Penguatan dan mengkonfigurasi sistem operasi host untuk menangani keamanan yang memadai
- Instalasi dan konfigurasi kontrol keamanan tambahan, jika diperlukan
- Pengujian sistem operasi host untuk memastikan bahwa keempat langkah sebelumnya secara memadai mengatasi semua masalah keamanan.

Patch dan update sistem operasi

Setelah sistem operasi terinstal, kegiatan berikutnya yang penting adalah instalasi patch atau update sistem yang diperlukan untuk mengoreksi kelemahan yang terdapat pada sistem operasi tersebut. Setiap sistem operasi yang telah diketahui kerentanannya harus diperbaiki sebelum digunakan untuk host mail server. Untuk mendeteksi dan memperbaiki kerentanan ini, administrator server mail harus melakukan berikut ini:

- Membuat dan menerapkan proses patch
- Mengidentifikasi kerentanan dan patch yang berlaku
- Mengurangi kerentanan sementara jika diperlukan dan jika mungkin (sampai patch yang tersedia, diuji, dan diinstal)
- Menginstall secara permanen (patch, hotfix, service pack atau update)

Administrator harus melakukan pengujian terlebih dahulu terhadap patch tersebut sebelum diterapkan ke server mail, karena patch dapat menyebabkan masalah operasional. Walaupun administrator dapat mengkonfigurasi mail serveruntuk men-download patch otomatis, server tidak disarankan dikonfigurasi untuk menginstal patch secara otomatis.

Hapus atau Nonaktifkan Layanan dan aplikasi yang tidak perlu

Idealnya, sebuah mail server harus khusus untuk kebutuhan mail. Ketika mengkonfigurasi sistem operasi, menonaktifkan segala sesuatu kecuali yangsecara tegas diijinkan yaitu, menonaktifkan semua layanan dan aplikasi, aktifkan hanya yang dipersyaratkan oleh server mail, dan kemudian hapus layanan yang tidak diperlukan dan aplikasi. Jika memungkinkan, menginstal sistemo perasi konfigurasi minimal yang diperlukan untuk server aplikasi email.

Pilih pilihan "instalasi minimal" jika tersedia, untuk meminimalkan upaya yang diperlukan dalam menghilangkan layanan yang tidak perlu. Selain itu, skrip uninstall banyak program atau jauh

dari sempurna dalam benar-benar menghapus semua komponen layanan, karena itu, selalu lebih baik untuk tidak menginstal layanan yang tidak perlu. Beberapa jenis umum dari layanan dan aplikasiyang biasanya harus dinonaktifkan jika tidak diperlukan meliputi:

- Layanan File dan printer sharing (misalnya NetBIOS, Network File System [NFS], File Transfer Protocol [FTP])
- Default Web server
- Layanan jaringan Nirkabel
- Remote control dan program akses remote (misalnya, Telnet)
- Layanan Direktori (misalnyaLDAP, Kerberos,)
- Tool pengembangan sistem
- Utility sistem dan manajemen jaringan, termasuk Simple Network Management Protocol (SNMP).

Menghilangkan atau menonaktifkan layanan yang tidak perlu untuk meningkatkan keamanan server mail dilakukan dalam beberapa cara:

- Layanan lain tidak dapat dikompromikan dan digunakan untuk menyerang host atau merusak layanan dari server mail.
- Setiap layanan yang ditambahkan ke host meningkatkan risiko kompromi terhadap host tersebut karena setiap layanan merupakan jalan bagi penyerang.
- Layanan lain mungkin memiliki kekurangan atau mungkin tidak kompatibel dengan server mail itu sendiri.
- Menonaktifkan atau menghapus layanan tersebut mencegah dari aktifitas yang mempengaruhi mail server.
- Host dapat dikonfigurasi agar lebih sesuai dengan persyaratan dari layanan tertentu.
- Layanan yang berbeda mungkin memerlukan hardware yang berbeda dan konfigurasi perangkat lunak, yang dapat menyebabkan kerentanan yang tidak perlu atau mempengaruhi kinerja.
- Dengan mengurangi layanan, jumlah log dan entri log berkurang, sehinggauntuk mendeteksi perilaku yang mencurigakan menjadi lebih mudah.

Organisasi harus menentukan layanan yang akan diaktifkan pada server mail. Jika akses berbasis Webmail akan diberikan, server Web menjalankan aplikasi mail harus berada pada host yang terpisah dari server mail. Memiliki server Web dan mail padahost terpisah membatasi dampak jika salah satu dari mereka terganggu bila dibandingkan dengan memiliki kedua server pada host yang sama. Manfaat dari penggunaan server web dan mail dalam satu host adalah komunikasi yang efisien dan dilindungi, karena server Web dan email berkomunikasi secara langsung dalam sebuah host tidak melalui jaringan.

Konfigurasi Otentikasi User pada Sistem Operasi

Untuk servermail, pengguna resmi yang dapat mengkonfigurasi sistem operasi terbatas pada administrator server mail yang ditunjuk. Para pengguna yang dapat mengakses server mail, bisa berkisar dari karyawan sebuah organisasi. Mengaktifkan otentikas ioleh komputer host melibatkan bagian konfigurasi dari sistem operasi, firmware, dan aplikasi, seperti perangkat lunak yang mengimplementasikan layanan jaringan. Dalamkasus khusus, untuk situs high-value/high-risk, organisasi juga dapat menggunakan perangkat keras otentikasi, seperti token. Gunakan mekanisme otentikasi yang yang ditransmisikan secara clear text melalui jaringan sangat tidak dianjurkan, karena informasi dapat dicegat dan digunakan oleh penyerang.

Menghapus atau menonaktifkan account dan group default yang tidak dibutuhkan. Konfigurasi default dari sistem operasi sering kali berisi akun Guest (dengan dan tanpa password), administrator atau account level root dan account yang terkait dengan layanan lokal dan jaringan. Nama dan password untuk account tersebut sudah dikenal.

Untuk memastikan penggunaan otentikasi user dengan tepat, ikuti langkah-langkah berikut :

- Hapus atau menonaktifkan account yang tidak perlu untuk menghilangkan penggunaannya oleh penyerang, termasuk account guest pada komputer yang berisi informasi sensitif. Jikaada keharusan untuk mempertahankan account guest atau group default, batasi hak akses dan ganti password default sesuai dengan kebijakan password organisasi. Untuk account default yang perlu dipertahankan, ubah nama(terutama untuk account administrator atau level root) dan password.
- Buat group pengguna. Memasangkan pengguna ke grup yang diperlukan. Kemudian menetapkan hak akses kelompok terhadap resources yang didokumentasikan.
- Buat account pengguna, identifikasi pengguna yang akan diberi wewenang untuk menggunakan setiap komputer dan layanannya. Account hanya dibuat seperlunya.
- Memeriksa kebijakan password organisasi, pasangkan password yang tepat pada masing-masing account. Tetapkan kebijakan penggunaan password berdasarkan pada :
    - Panjang karakter password, tetapkan panjang karakter minimal 8 karakter.
    - Kompleksitas, menggunakan jenis karakter yang berbeda, kombinasi huruf besar dan kecil, karakter alphanumeric dan non alphanumeric, tidak menggunakan kata yang terdapat di dalam kamus.
    - Usia password, jangka waktu dimana password tidak diubah. Memaksa pengguna untuk mengganti password secara periodik. Password level administrator atau root seharusnya diubah tiap 30 hingga 120 hari.
    - Otoritas, tetapkan administrator yang dapat mengubah atau me-reset password dan pembuktian yang dibutuhkan sebelum perubahan diijinkan.

- Konfigurasi komputer untuk menghindari aktifitas penebakan password
  Pengguna yang tidak sah dapat mencoba untuk mendapatkan akses ke komputer dengan menggunakan perangkat lunak otomatis untuk mencoba-coba semua kata sehingga dapat menebak password yang digunakan. Sebaiknya batasi jumlah usaha login (penggunaan password), ketika dalam sekian kali usaha login gagal maka account terkunci.
- Instal dan konfigurasi mekanisme keamanan lain untuk memperkuat sistem otentikasi. Jika informasi pada servermail memerlukan itu, pertimbangkan untuk menggunakan mekanisme otentikasi lainnya seperti biometrik, smart card, sertifikat client/server,atau sistem satu kali password.

Penyerang dapat menggunakan sniffer jaringan dan dapat dengan mudah mencuri password dilewatkan melalui jaringan dalam bentuk teks. Namun, mekanisme otentikasi berbasis password merupakan cara yang ekonomis dan tepat jikapassword tersebut dilindungi. Penerapan teknologi otentikasi dan enkripsi, seperti Secure Socket Layer(SSL) / Transport Layer Security(TLS), Secure Shell(SSH), atau Virtual Private Networks (VPN) (bagi pengguna jarak jauh), bermanfaat untuk melindungi password selama proses transmisi.

Install dan Konfigurasi Kontrol Keamanan Tambahan

Administrator perlu untuk memilih, menginstal, dan mengkonfigurasi perangkat lunak tambahan untuk memberikan kontrol keamanan tambahan. Kontrol keamanan yang diperlukan meliputi:

- Anti-malware, seperti anti-virus, anti-spyware, dan detektor rootkit, untuk melindungi sistem operasi dari malware dan untuk mendeteksi dan membasmi virus, malware dan sebagainya.
- Perlunak IDS/IPS berbasis host, untuk mendeteksi serangan yang dilakukan terhadap server mail.
- Firewall berbasis host, untuk melindungi server dari akses yang tidak sah Perangkat lunak Patch management, untuk memastikan bahwa kerentanan dapat segera ditangani. Perangkat lunak patch management dapat digunakan hanya untuk menerapkan patch, atau juga untuk mengidentifikasi kerentanan baru dalam sistem operasi server mail, layanan, dan aplikasi.

Pengujian Keamanan Terhadap Sistem Operasi

Pengujian Keamanan secara berkala dari sistem operasi merupakan hal yang penting untuk mengidentifikasi kerentanan dan untuk memastikan efektifitas tindakan pengamanan yang sudah dilakukan. Metode pengujian yang dilakukan terhadap sistem operasi dapat dilakukan

dengan metoda vulnerability scanning dan penetrasi testing. Vulnerability scanning dilakukan dengan menggunakan scanner otomatis untuk memindai kerentanan yang terdapat pada host atau kelompok host. Penetrasi testing merupakan proses pengujian yang dirancang untuk menggangu jaringan menggunakan tool dan metodologi dari penyerang. Vulnerability scanning harus dilakukan secara berkala, seperti mingguan atau bulanan, dan penetrasi testing harus dilakukan setidaknya setiap tahun.

Pengamanan Terhadap Isi dan Server Mail

Penguatan aplikasi server mail merupakan langkah penting dalam melindungi server mail dari gangguan. Bagian penting dari keamanan mail ini melindungi isi email yang melintasi server, yang meliputi penyaringan konten, pemindaian malware, dan pencegahan spam. Keamanan konten email juga dapat melibatkan enkripsi email untuk menjaga kerahasiaan dan tanda tangan digital untuk mendukung integritas.

Memperkuat aplikasi server mail

Untuk memperkuat server mail ini kita bisa lakukan dengan dua tindakan berikut :

Melakukan instalasi secara aman server mail

Selama instalasi server email, langkah-langkah berikut seharusnya dilakukan :

- Install perangkat lunak server mail pada sebuah host dedicated
- Gunakan patch atau upgrade kelemahan yang telah diketahui
- Buat sebuah dedicated disk fisik atau logik untuk mailbox
- Hapus atau non aktifkan semua layanan yang tidak dibutuhkan
- Hapus atau nonaktifkan semua account login default yang dibuat oleh proses instalasi server mail
- Hapus semua dokumentasi manufaktur dari server
- hapus file-file contoh dari server
- Gunakan template keamanan atau script untuk memperkuat server
- Konfigurasi ulang banner dari layanan SMTP, POP dan IMAP agar tidak menginformasikan versi dan jenis sistem operasi dan server mail
- Nonaktifkan perintah-perintah email yang tidak perlu (contoh: VRFY dan EXPN)

Konfigurasi kontrol akses pada sistem operasi dan server mail

Pada umumnya sistem operasi host dari server mail menyediakan kemampuan untuk menetapkan hak akses terhadap file, device dan sumber daya lain pada sebuah host. Administrator server mail harus mempertimbangkan bagaimana cara terbaik untuk mengkonfigurasi kontrol akses untuk melindungi informasi yang tersimpan di server mail dari dua perspektif:

- Batasi akses dari aplikasi mail server untuk subset dari sumber daya komputasi
- Membatasi akses dari pengguna melalui kontrol akses tambahan ditegakkan oleh mail server, di mana tingkat yang lebih rinci tentang kontrol akses yang diperlukan.

Pengaturan yang tepat dari kontrol akses dapat membantu mencegah pengungkapan informasi sensitif. Selain itu, kontrol akses dapat digunakan untuk membatasi penggunaan sumber dayapada saat terjadi serangan DoS terhadap server mail.

File-file yang umum harus dikontrol adalah sebagai berikut:

- File konfigurasi dan perangkat lunak aplikasi
- File konfigurasi dan perangkat lunak sistem
- File-file log dan sistem audit
- File-file yang secara langsung berkaitan dengan mekanisme keamanan :
    - File-file password Hash dan file lain yang digunakan dalam otentikasi
    - File yang berisi informasi otorisasi yang digunakan dalam kontrol akses
    - Bahan kunci kriptografi yang digunakan untuk menyediakan layanan yang mampu menjaga kerahasiaan, integritas, dan non-repudiation

Untuk mengurangi dampak dari beberapa jenis serangan DoS, konfigurasi server mail untuk membatasi jumlah sumber daya sistem operasi. Beberapa contoh termasuk:

- Instalasi mailbox pengguna pada server, hard drive, atau partisi logis yang berbeda dari sistem operasi dan aplikasi server mail
- Konfigurasi aplikasi mail server sehingga tidak dapat mengkonsumsi semua ruang yang tersedia pada hard drive atau partisi
- Batasi ukuran file lampiran yang diizinkan
- Memastikan file-file log disimpan di lokasi dengan ukuran yang tepat.

Melindungi email dari malware

Banyak pesan email dikirim dengan lampiran berupa program executable, gambar, musik, dan suara. Banyak bentuk malware, termasuk virus, worm, trojan horse, dan spyware-malware ditransmisikan dalam lampiran dimaksudkan untuk melanggar privasi pengguna.

Menentukan apakah akan mengizinkan beberapa jenis lampiran bisa menjadi keputusan sulit bagi suatu organisasi. Organisasi harus menentukan jenis lampiran yang memungkinkan. Pendekatan paling sederhana adalah untuk memungkinkan semua jenis lampiran. Jika ini terjadi, maka beberapa jenis malware scanner (misalnya perangkat lunak anti-virus, anti-spyware) harus dipasang untuk menyaring malware. Pendekatan yang lebih baik adalah untuk menyaring jenis lampiran yang memiliki potensi berbahaya (misalnya, file ekstensi Vbs,Ws, WSC) di server mail atau mail gateway. Meskipun penyaringan pada ekstensi tersebut adalah langkah yang baik, efektivitasnya terbatas karena penyerang dapat mengubah ekstensi. Bukan hanya memeriksa ekstensi, penyaringan harus memeriksa file header, footer, atau aspek-aspek identitas lainnya dari file jika memungkinkan, untuk mengidentifikasi lampiran.

Penyerang kadang-kadang mengirim email yang memiliki hyperlink ke sebuah file berbahaya di situs Web, jika pengguna mengklik hyperlink dan menggunakan HTTPS, file berbahaya akan didownload dan dilindungi oleh HTTPS, sehingga terlindungi dari deteksi kontrol keamanan jaringan. Organisasi bisa menyaring hyperlink aktif dalam pesan email untuk mencegah hal ini, tetapi ini akan mengurangi kegunaan dari pesan email bagi pengguna, menempatkan hyperlink

ke file dalam pesan email akan mengurangi beban pada server mail dibandingkan dengan melampirkan file ke dalam sebuah pesan.

Organisasi juga harus mempertimbangkan untuk membatasi ukuran maksimum dari file lampiran yang dapat diterima pada sebuah email.Hal ini juga bermanfaat bagi server mail untuk mengurangi latency antrian mail, kebutuhan storage, dan kebutuhan prosesor pada server.

Enkripsi email cenderung membuat penyaringan lebih rumit atau tidak efektif .Setiap pesan yang dienkripsi, filtering pada server mail dan atau perangkat perimeter tidak efektif kecuali mereka dapat mendekripsi, scan, dan kembali mengenkripsi pesan tersebut.

Selain lampiran email, malware dapat dikirim melalui email dengan cara lain. Misalnya, banyak mail client yang mendukung pesan berbasis HTML. Pesan-pesan ini sering mengandung konten aktif dalam bentuk bahasa scripting client-side atau kontrol objek yang dapat mempengaruhi klien. Jenis konten aktif yang paling populer adalah ActiveX, Java, JavaScript, dan Visual Basic Script (VBScript). Organisasi harus menentukan apakah mengizinkan atau memblokir konten aktif dalam pesan email.

Pesan berbasis HTML juga sering berisi konten yang tidak diinginkan lainnya, seperti pesan spam dan phishing. Phishing merupakan cara untuk mengelabui orang agar mengungkapkan informasi pribadi sensitif. Sebagai contoh, penyerang bisa mengirim pesan email kepada korban yang terlihat seolah-olah dikirim dari organisasi yang terkenal. Email tersebut dimaksudkan untuk menipu pengguna agar menanggapi email dan mengungkapkan data pribadi. Jika sebuah mail server tidak memiliki pendeteksi malware (misalnya anti-virus, anti-spyware), potensi ancaman keamanan yang ditimbulkan oleh malware akan meningkat bagi pengguna akhir.

Scanning Malware

Untuk melindungi ancaman dari virus, worm, dan bentuk lain dari malware, perlu untuk menerapkan sistem pemindaian pada satu atau beberapa titik di proses pengiriman email. Scanning malware dapat diterapkan pada firewall, relay mail, atau tool-mail gateway, server mail dan di host pengguna akhir.

Scanning pada Firewall, mail relay atau mail gateway

Scanning malware pada firewall, mail relay atau mail gateway dapat mencegat pesan sebelum pesan sampai ke server mail. Perangkat menyediakan koneksi pada port 25, memindai setiap pesan, kemudian melewatkan pesan yang tidak berisi malware ke mail server. Kelemahan pendekatan ini adalah bahwa pemindaian yang berkesinambungan terhadap trafik SMTP dapat mengurangi kinerja firewall/ mailrelay /emailgateway.

Manfaat scanning email pada firewall, mail relay, atau mail gateway adalah sebagai berikut:

- Dapat memindai email di kedua arah (inbound dan outbound dari jaringan organisasi)
- Dapat menghentikan sebagian besar pesan yang berisi malware pada perimeter sebelum mereka memasuki jaringan dan dilewatkan ke mail server
- Dapat menerapkan scanning untuk email masuk dengan sedikit perubahan konfigurasi server email yang ada
- Dapat mengurangi jumlah email mencapai server mail, yang memungkinkan mereka untuk beroperasi secara lebih efisien dengan biaya operasional yang lebih rendah
- Dapat mengurangi jumlah scanning yang akan dilakukan oleh server mail, sehingga mengurangi beban mereka
- Secara terpusat dapat mengelola pemindaian untuk memastikan kepatuhan terhadap kebijakan keamanan organisasi.

Scanning malware melalui firewall, mail relay, atau mail gateway memiliki sejumlah kelemahan:

- Tidak dapat memindai email-email yang terenkripsi

Scanning pada Mail Server

Banyak aplikasi yang tersedia untuk memindai isi dari tempat penyimpanan pesan di mail server. Aplikasi ini memeriksa email yang dikirim antara pengguna internal, yang biasanya tidak melewati firewall organisasi/ mailrelay /mail gateway. Melakukan scanning pada mail server juga memberikan lapisan tambahan perlindungan terhadap malware, dan juga membantu untuk menghentikan penyebaran malware internal. Beberapa server mail menawarkan application programming interface(API) yang mendukung integrasi dari pemindaian malware, konten filtering, blocking lampiran, dan layanan keamanan lainnya di dalam MTA.

Pemindaian malware yang dilakukan pada server mail menyediakan beberapa keuntungan:

- Dapat memindai email di kedua arah (inbound dan outbound)
- Dapat dikelola secara terpusat untuk memastikan kepatuhan terhadap kebijakan keamanan organisasi dan update signature malware diterapkan secara teratur
- Menawarkan perlindungan kepada pengguna internal dari malware yang berasal dari jaringan internal.

Memindai malware pada mail server memiliki sejumlah kelemahan:

- Mungkin memerlukan modifikasi signifikan dari konfigurasi mail server yang ada
- Tidak dapat memindai email terenkripsi
- Memerlukan spesifikasi perangkat keras yang lebih tinggi untuk menangani beban dari sebuah organisasi besar.
- Hanya dapat mendeteksi ancaman yang telah dikenal, menawarkan sedikit perlindungan terhadap zero-day exploit.

Scanning pada host client

Scanner malware juga dapat di installpada host klien. Email masuk di-scan dan email outbound diperiksa. Keuntungan utama dari jenis ini adalah bahwa pemindaian didistribusikan di banyak host dan karena itu memiliki efek minimal terhadap kinerja setiap host individu. Jika mesin klien terinfeksi malware, host diharapkandapat menghentikan penyebaran malware ke mail server dan klien email lainnya.

Manfaat darisistem scanning malware yang dilakukan di sisi klien adalah sebagai berikut:

- Tidak memerlukan modifikasi di mail server
- Dapat memindai email terenkripsi ketika mereka didekripsi oleh pengguna
- Menawarkan perlindungan kepada pengguna internal, bahkan ketika malware diterima dari pengguna internal.

Kelemahan dari pemindaian malware berbasis client-side adalah sebagai berikut:

- Serangan dapat mengambil waktu sebelum user mengupdate scanner malware, sehingga organisasi menjadi lebih rentan terhadap penyebaran malware.
- Dapat sengaja atau tanpa sengaja dinonaktifkan atau dilemahkan oleh pengguna.
- Hanya dapat mendeteksi ancaman yang telah dikenal, menawarkan sedikit perlindungan terhadap zero-day exploit.

Content Filtering

Content filtering bekerja dengan cara yang mirip seperti scanning malware pada server firewall atau email kecuali bahwa mencari email yang berisi konten yang tidak diinginkan selain malware, seperti spam atau email mengandung bahasa yang tidak pantas.

Kepedulian pengguna

Selain menggunakan software anti-virus dan scanning malware lainnya, serta perangkat lunak penyaring konten, organisasi harus mendidik pengguna tentang bahaya yang ditimbulkan oleh malware dan cara yang efektif untukmenghindari ancaman, termasuk tindakan berikut:

- Jangan pernah membuka attachment dari pengirim yang tidak dikenal.
- Jangan membuka attachment dengan nama yang mencurigakan atau berpotensi berbahaya atau file berekstensi (misalnya attachment .txt, .vbs, .exe) dari pengirim yang dikenal.
- Scan semua lampiran menggunakan perangkat lunak pemindai malware sebelum file tersebut dibuka.
- Update database signature perangkat lunak pemindai malware setiap hari
- Memperingatkan pengguna tentang penyebaran malware dan bagaimana mengidentifikasi email yang mungkin berisi malware.

Memblokir server pengirim spam

Selalu ada entitas yang berusaha mengeksploitasi suatu sarana komunikasi untuk mempublikasikan ide-ide atau produk mereka. Emailtidak terkecuali, istilahyang paling umum untuk pesan ini email komersial yang tidak diinginkan lebih dikenal sebagai spam. Sebagian besar pengguna menerima spam email setiap hari. Administrator sistem harus mengawasi lalu lintas email yang melintasi server mereka untuk mengurangi jumlah spam mencapai pengguna. Manfaat tambahan dari pelaksanaan server berbasis kontrol spam adalah akan mengurangi ukuran mailbox, yang pada gilirannya mengurangi kebutuhan tempat penyimpanan di server.

Untuk mengontrol pesan spam, administrator harus mengatasi tiga masalah berikut:

- Pastikan spam tidak dapat dikirim melalui mail server yang kita kelola.
- Melaksanakan penyaringan spam untuk pesan masuk.
- Blok pesan-pesan dari server-server yang dikenal sebagai pengirim spam.

Daftar mail server yang di kenal sebagai pengirim spam sering disebut ORB (open relay blacklist) atau DNS Blacklist (DNSBL).

Otentikasi relay mail

Mengkonfigurasi otentikasi relay mail mengurangi kemungkinan seseorang menggunakan sebuah server mail untuk mengirim spam. Dua metode yang tersedia untuk mengendalikan relay mail. Yang pertama adalah untuk mengontrol subnet atau domain dari mana pesan dikirim.Metode kedua adalah membutuhkan pengguna untuk mengotentikasi dirinya sebelum mengirim pesan. Ini sering disebut sebagai otentikasi relay atau SMTPAUTH, yang merupakan pengembangan SMTP yang mendukung otentikasi pengguna.

Sebuah mail server yang dikonfigurasi secara tidak benar dapat dimanfaatkan dan digunakan untuk mengirim atau merelay spam. Jika mail server ditemukan menjadi open relay, akan dimasukkan dalam daftar hitam. Setiap organisasi berlangganan dan menggunakan blacklist tidak akan dapat menerima email dari server blacklist.

Akses email berbasis Web

Bagi organisasi yang menyediakan akses sistem email berbasis Web. Beberapa hal berikut perlu diperhatikan :

- Mekanisme otentikasi dari Web front-end harus menggunakan enkripsi.
- Web server harus menggunakan SSL / TLS untuk mengenkripsi semua komunikasi dengan klien.
- Server Web harus diperkuat sistem keamanannya sebelum menghubungkannya ke jaringan.

Penerapan infrastruktur jaringan yang aman

Infrastruktur jaringan yang mendukung server mail memainkan peran penting dalam keamanan server mail. Pada kebanyakan konfigurasi, infrastruktur jaringan adalah garis pertahanan pertama antara internet dan mail server. Bagian ini membahas komponen jaringan yang dapat mendukung dan melindungi mail server untuk lebih meningkatkan keamanan mereka secara keseluruhan. Sementara masalah keamanan adalah hal yang terpenting, pertimbangan infrastruktur jaringan dipengaruhi oleh banyak faktor selain keamanan, termasuk biaya, kinerja dan kehandalan.

Komposisi danStrukturJaringan

Firewall dan router merupakan perangkat atau sistem yang mengontrol aliran lalu lintas antara jaringan. Mereka dapat melindungi server mail dari kerentanan yang melekat dalam Transmission Control Protocol/Internet Protocol (TCP/ IP) dan membantu mengurangi masalah keamanan yang terkait dengan aplikasi dan sistem operasi yang tidak aman. Komposisi dan struktur jaringan merupakan hal paling penting yang mempengaruhi keamanan server mail, karena mereka menentukan elemen infrastruktur jaringan yang melindungi server mail. Misalnya, jika mail server terletak sebelum firewall, maka firewall tidak dapat digunakan untuk mengontrol lalu lintas ke dan dari server mail. Komposisi dan struktur jaringan juga menentukan bagian lain dari jaringan yang rentan jika server mail ini diganggu.

Demilitarized Zone (DMZ)

Sebuah DMZ mencegah pengguna-pengguna di luar dari mail server mendapatkan akses secara langsung ke jaringan internal organisasi (intranet).

Penerapan DMZ meliputi penempatan firewall antara router perbatasan organisasi dan jaringan internal dan menyediakan segmen jaringan baru yang hanya dapat dicapai melalui perangkat DMZ. Mail server atau gateway mail ini ditempatkan pada segmen baru, bersama dengan komponen jaringan infrastruktur lainnya dan server yang harus diakses secara eksternal. Misalnya, jika akses berbasis Web mail ini ditawarkan, server terkait biasanya ditempatkan pada DMZ. Pada beberapa konfigurasi, router perbatasan itu sendiri dapat bertindak sebagai firewall sederhana.

Keuntungan DMZ dari sudut pandang keamanan adalah sebagai berikut:

- Mail server mungkin lebih baik dilindungi, dan jaringan lalu lintas ke dan dari server mail dapat dimonitor.
- Gangguan terhadap server mail tidak secara langsung mengancam jaringan produksi internal.
- Kontrol yang lebih besar dapat diberikan terhadap pengamanan server mail karena lalu lintas dari dan ke server mail dapat dikontrol.

- Konfigurasi jaringan DMZ dapat dioptimalkan untuk mendukung dan melindungi mail server.

Kelemahan dari DMZ dari sudut pandang keamanan adalah sebagai berikut:

- Serangan DoS ditujukan pada mail server mungkin memiliki efek pada jaringan internal.
- Perlindungan yang ditawarkan olehDMZ tergantung sebagian besar pada konfigurasi firewall.

MailGateway

Penggunaan mail gateway di DMZ menambahkan perlindungan lebih lanjut untuk server mail. Lapisan tambahan membuat mail server lebih sulit untuk diserang. Sebuah mail gateway bertindak seperti proxy antara mail server dan Internet. Semua pesan dan komunikasi harus melalui proxy sebelum diteruskan ke mail server. Karena mail gateway umumnya hanya menyediakan fungsi terbatas, jauh lebih mudah memperkuat dan mengamankannya dibanding mail server yang berfungsi penuh.

Konfigurasi Elemen Jaringan

Setelah mail server telah diposisikan di jaringan, elemen infrastruktur jaringan harus dikonfigurasi untuk mendukung dan melindunginya. Elemen-elemen dari infrastruktur jaringan yang mempengaruhi keamanan mail server adalah firewall, router, IDS/IPS, dan switch. Masing-masing memiliki peran penting bagi keseluruhan strategi melindungi mail server melalui perlindungan berlapis.

Konfigurasi Router/Firewall

Router merupakan perangkat yang dapat menyediakan kontrol akses pada paket IP.Router yang difungsikan sebagai firewall dapat menyediakan informasi-informasi berikut :

- Alamat IP sumber
- Alamat IP tujuan
- Jenis trafik
- Status dan port TCP/UDP

Keuntungan menggunakan router sebagai firewall, antara lain :

- Biaya relative lebih murah

Kekurangan dari penggunaan router sebagai firewall, antara lain :

- Kerentanan terhadap serangan layer aplikasi(misalnya, tidak dapat memeriksa isi email)
- Kerentanan terhadapserangan melalui port-port yang diperbolehkan (router umumnya lebih lemah dari firewall karena router tidak melakukan analisis pada layer aplikasi)
- Kesulitan konfigurasi dan administrasi
- Keterbatasan kemampuan logging

- Kemampuan pemrosesan mungkin lebih terbatas
- Kurangnya serangkaian rule dan kemampuan filtering.

Untuk melindungi mail server menggunakan firewall, pastikan bahwa firewall sudah di-patch dengan patch terbaru dan dikonfigurasi untuk mendukung item berikut:

- Mengendalikan semua lalu lintas antara internet dan mail server
- Memblokir semua lalu lintas inbound ke mail server kecuali lalu lintas yang dibutuhkan, seperti TCP port 25 (SMTP).
- Blok alamat IP atau subnet yang dilaporkan IDSatau IPS menyerang jaringan organisasi
- Blokir alamat network "daftar hitam" yang diidentifikasi oleh pusat keamanan terpercaya
- Informasikan pada administrator jaringan atau server mail tentang adanya aktivitas mencurigakan melalui sarana yang tepat
- Menyediakan konten penyaringan
- Menyediakan pemindaian malware
- Melindungi terhadap serangan DoS
- Mencatat informasi-informasi, berikut:
  - Waktu / tanggal
  - Antarmuka alamat IP
  - Produsen nama spesifik-acara
  - Serangan Standar acara identifier (jika ada)
  - Sumber dan tujuan alamat IP
  - Sumber dan tujuan nomor port
  - Protokol jaringan

Intrusion Detection / Prevention System (IDS/IPS)

Intrusion Detection System(IDS) merupakan sebuah aplikasi yang memantau peristiwa yang terjadi dalam sistem atau jaringan dan menganalisa mereka untuk mendeteksi adanya tanda-tanda yang berpotensi menjadi insiden, pelanggaran atau ancaman terhadap keamanan komputer. Sedangkan Intrusion Prevention System (IPS) memiliki semua kemampuan dari IDS dan juga dapat mencoba untuk menghentikan potensi ancaman, insiden yang muncul.

Agar IDS/IPS berhasil melindungi mail server pastikan IDPS mampu dan dikonfigurasi untuk:

- Memonitor lalu lintas jaringan ke dan dari server mail
- Memantau perubahan pada file-file penting yang terdapat di server mail
- Memonitor sumber daya sistem yang tersedia pada host mail server(host-based)
- Blok alamat IP atau subnet yang menyerang jaringan organisasi
- Informasikan pada administrator jaringan atau server mail tentang adanya aktivitas mencurigakan melalui sarana yang tepat
- Mendeteksi kegiatan scanning dan serangan

- Mencatat informasi-informasi, berikut:
  - Waktu / tanggal
  - alamat IP Sensor
  - Nama serangan manufaktur tertentu
  - Nama serangan standard
  - Alamat IP sumber dan tujuan
  - Nomor Port sumber dan tujuan
  - Protokol jaringan
  - Informasi packet header sebaiknya di-capture untuk membantu proses analisis dan forensik
  - Update signature serangan baru secara periodik.

Jaringan Switch

Switch merupakan perangkat yang menyediakan konektivitas antara dua atau lebih host yang terletak pada segmen jaringan yang sama. Pengaturan sistem keamanan terhadap jaringan switch dilakukan untuk menghindari bentuk serangan seperti ARP Spoofing

Switch dapat memiliki dampak negatif pada jaringan berbasis IDPS.Pada umumnya jaringan switch mengijinkan administrator untuk mengkonfigurasi port tertentu pada switch, sehingga port tersebut mereplikasi semua trafik yang melewati switch tersebut untuk digunakan oleh IDS. Hal ini mengijinkan IDPS berbasis network melihat semua trafik pada jaringan tertentu. Ketika beban tinggi, switch mungkin perlu menghentikan proses span tersebut dan akibatnya IDPS tidak dapat memonitor aktifitas jaringan.

Pengamanan Terhadap Client-Client Mail

Pengamanan terhadap client-client pengguna email juga tidak kalah penting, dalam banyak kasus bagian client memiliki resiko lebih besar dibanding dengan server mail.Berikut ini rekomendasi penggunaan aplikasi mail client.

Instalasi dan Konfigurasi aplikasi-aplikasi Client

Langkah yang paling penting dalam mengamankan mail client adalah untuk memastikan bahwa semua pengguna menggunakan patch yang terbaru.S ebagian besar mail client memiliki kerentanan signifikan. Untuk mengakses server mail dapat dilakukan menggunakan aplikasi mail client dan juga melalui browser. Sehingga update patch dilakukan terhadap aplikasi mail klien dan juga browser yang digunakan juga perlu update patch.

Konfigurasi Fitur-Fitur Keamanan pada klien Mail

Aplikasi mail client tidak dapat dikonfigurasi dengan aman dalam konfigurasi default. Mail client harus dikonfigurasi untuk:

- Nonaktifkan download dan pengolahan konten aktif, seperti kontrol ActiveX, applet Java, dan JavaScript. Ini dapat menyebabkan masalah untuk aplikasi mail yang digabung dengan Web browser, karena menonaktifkan fungsi ini dapat mempengaruhi browser Web, di mana fungsi tersebut mungkin diperlukan.
- Aktifkan fitur anti-spam dan anti-phishing, jika tersedia. Fitur-fitur ini sering memiliki pengaturan lebihpermisif secara default, sehingga mungkin bermanfaat dari perspektif keamanan untuk mengatur mereka ke tingkat yang lebih tinggi.

Konfigurasi Akses dan Otentikasi

Sebaiknya mekanisme otentikasi dipasangkan pada aplikasi mail client ketika hendak mengakses mail server. Otentikasi ini dilakukan dengan menggunakan username dan password, agar lebih memudahkan proses otentikasi biasanya user memanfaatkan fitur “remember password”, meskipun memberi kemudahan bagi pengguna, hal ini juga dapat menimbulkan resiko, sejauh penyerang dapat memiliki akses logis atau fisik ke host dari mail client.

Menonaktifkan fungsi mengingat password merupakan cara yang efektif untuk meningkatkan keamanan mail client.

Semua jaringan komunikasi yang menggunakan konfigurasi default SMTP, POP,dan IMAP terjadi tidak terenkripsi. Hal ini membuat username, password,dan pesan dapat dicegat dan dimodifikasi. Untuk meningkatkan keamanan antara komunikasi klien dan server, komunikasi ini dapat di-enkripsi menggunakan SSL/TLS.

Pengamanan Sistem Operasi pada Host Client

Banyak sistem operasi menyediakan sejumlah pengaturan konfigurasi dan langkah-langkah lain untuk meningkatkan keamanan dari mail client baik secara langsung maupun tidak langsung. Sistem operasi hosta dalah komponen kunci dari keamanan secara keseluruhan dari sebuah host klien. Berikut ini yang harus dilakukan untuk mengamankan sistem operasi host:

- Perbarui versi patch gunakan yang paling aman.
- Hanya mengizinkan pengguna yang sesuai untuk mengakses pesan yang disimpan secara lokal dan file konfigurasi mail client.
- Konfigurasi Windows Script Host (WSH) (hanya host yang menggunakan windows) :
- Hapus WSH atau hanya mengizinkan administrator untuk mengakses
- Ubah tindakan default dari file-file ekstensi berikut:
    - JS(JavaScript)
    - JSE(JavaScriptEncoded File)
    - VBE(VBScript Encoded File)
    - VBS(Visual Basic Script)
    - WS(Windows File Script)
    - WSF (Windows Script File)
    - WSC (Windows Script Component)
    - WSH (Windows Script Host Settings File)
- Pada host Windows, mengkonfigurasi mereka untuk menampilkan ekstensi file penuh (ini memastikan bahwa lampiran email seperti iloveyou.txt.vbs ditampilkan bukan iloveyou.txt).
- Menginstal aplikasi anti-virus dan mengkonfigurasinya untuk secara otomatis memindai semua pesan masuk dan dokumen lampirannya. Instalasi dan gunakan aplikasi anti-spyware jika perangkat lunak anti-virus tidak menawarkan kemampuan anti-spyware.
- Instalasi firewall personal untuk melindungikomputer dari komunikasiyang tidak sah.
- Pastikan bahwa komponen-komponen penting dari sistem operasi terlindungi dari code berbahaya
- Gunakan aplikasi file enkripsi untuk melindungi email yang disimpan secara lokal di hard drive pengguna.

No		Checklist
Patch dan upgrade sistem operasi		
1	Buat dan menerapkan proses patch	
2	Mengidentifikasi, menguji dan menginstall semua patch dan upgrade sistem operasi yang diperlukan	
Hapus atau Nonaktifkan layanan dan aplikasi yang tidak diperlukan		
3	Hapus atau Nonaktifkan layanan dan aplikasi yang tidak diperlukan	
4	Gunakan host-host terpisah untuk server web, direktori dan layanan-layanan lain	
Konfigurasi mekanisme otentikasi user pada sistem operasi		
5	Hapus atu non aktifkan account dan group-group yang tidak diperlukan	
6	Buat account dan group pengguna untuk komputer komputer tertentu	
7	Periksa kebijakan password organisasi dan mengatur password account dengan tepat	
8	Konfigurasi komputer untuk terhindar dari penebakan password	
9	Menginstall dan mengkonfigurasi mekanisme keamanan lain untuk memperkuat otentikasi	
Konfigurasi kontrol resource dengan tepat		
10	Mengatur kontrol akses untuk file, direktori, perangat dan sumber daya lainnya	
11	Batasi hak akses terhadap sistem yang terkait tool kepada administrator yang diberi wewenang	
Install dan konfigurasi kontrol keamanan tambahan		
12	Pilih, install dan konfigurasi perangkat lunak tambahan untuk menyediakan kontrol-kontrol yang diperlukan	
13	Uji keamanan dari sistem operasi	
14	Uji sistem operasi secara periodik untuk mencari kelemahan	