PENINGKATAN KEAMANAN APLIKASI KONTROL DENGAN MENGGUNAKAN METODE FIREWALLDAN KASPERSKY ENDPOINT SECURITY 8

ABSTRAK

Aplikasi kontrol merupakan prosedur program transaksi yang dapat mengancam aplikasi khusus seperti aplikasi sistem pembayaran, penggajian, dan pembelian. Pada aplikasi kontrol terdapat beberapa gangguan keamanan seperti resiko atau tingkat bahaya, ancaman, dan kerapuhan sistem. Untuk mengatasi gangguan tersebut terdapat metode keamanan yang dapat digunakan untuk meningkatkan keamanan aplikasi kontrol. Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) adalah sistem yang digunakan untuk mendeteksi dan melindungi sebuah sistem keamanan dari serangan pihak luar atau dalam. Firewall adalah sebuah pembatas antara suatu jaringan lokal dengan jaringan lainnya yang sifatnya publik. Penerapan firewall disebut juga sebagai upaya untuk meningkatkan keamanan pada aplikasi control.

Kata kunci: Firewall, IDS, IPS, Aplikasi Kontrol

M.S. Herawati
Nani Mintarsih

Jurusan Sistem Informasi, Fakultas Ilmu Komputer Universitas Gunadarma
msherawati@staff.gunadarma.ac.id
nanim@staff.gunadarma.ac.id

PENDAHULUAN

Dewasa ini keamanan pada aplikasi kontrol komputer seringkali mengalami gangguan atau ancaman dari para pelaku kejahatan komputer. Oleh sebab itu dibutuhkan keamanan komputer pada aplikasi kontrol yaitu firewall dan antivirus Kaspersky di mana terdapat fitur IDS *(Instrucsion Detection System)* dan IPS *(Intrusion Prevention System)*.

Tujuan pengontrolan adalah untuk memastikan bahwa CBIS telah diimplementasikan seperti yang direncanakan, sistem beroperasi seperti yang dikehendaki dan operasi tetap dalam keadaan aman dari penyalahgunaan atau gangguan.

1. Aplikasi Kontrol

Kontrol aplikasi adalah model prosedur program transaksi dengan kekuatan pembukaan yang mengancam aplikasi khusus, seperti gaji, pembelian dan sistem pembayaran tunai. Kontrol aplikasi terbagi ke dalam 3 kategori yaitu kontrol pemakaian, kontrol proses dan kontrol keluar.

Kontrol pemakaian adalah komponen koleksi data dari informasi sistem bertanggung jawab untuk membawa data ke dalam sistem untuk diproses. Kontrol masuk pada tahap ini didesign untuk menjamin agar transaksi menjadi sah, akurat dan lengkap. Data masukan prosedur bisa juga jadi sumber data-cepat bertindak (sekumpulan) atau input langsung (penuh waktu). Sumber dokumen pemakaian membutuhkan keterlibatan manusia dan mudah mendapatkan untuk kesalahan penulisan. Beberapa tipe dari kesalahan yang dimasukkan ke dalam sumber dokumen tidak dapat ditemukan dan selama perbaikan tahap data pemakaian.

Kontrol yang hati-hati harus mengadakan sumber dokumen fisik di sistem yang digunakan untuk memulai transaksi. Kecurangan sumber dokumen dapat digunakan untuk memindahkan aset dari organisasi. Seorang dengan akses untuk mengorder pembelian dan menerima laporan dapat memalsukan transaksi pembelian ke penjual yang tidak nyata. Jika dokumen ini masuk ke dalam aliran proses data, dengan memalsukan faktur penjualan, sistem dapat memproses dokumen ini sebagai transaksi yang sah. Kekurangan dari kontrol kompensasi lain untuk mendeteksi tipe ini dari kecurangan, sistem dapat membuat laporan pembayaran dan kemudian menulis cek pembayaran.

Batch control adalah metode yang efisien untuk mengatur data transaksi dalam jumlah besar lewat sebuah sistem. Tujuan *batch control* adalah mengendalikan keluaran yang dihasilkan oleh sistem dengan data asli yang dimasukkan ke dalam sistem. Hal ini akan memastikan bahwa semua rekaman dalam kumpulan telah di proses, tidak ada rekaman yang diproses lebih dari sekali, dan pemeriksa transaksi diciptakan dari hasil pemrosesan ke media keluaran dari sistem *Batch control* tidak terbatas sebagai teknik pengendalian masukan.

2. Gangguan Keamanan

Pengamanan jaringan merupakan upaya memberikan keterjaminan jaringan dari gangguan yang mungkin muncul. Secara umum, terdapat 3 sumber/faktor penggganggu keamanan jaringan, yaitu risiko atau tingkat bahaya, ancaman, dan kerapuhan sistem *(vulnerability)*.

Risiko berarti berapa besar kemungkinan keberhasilan para penyusup dalam rangka memperoleh akses ke dalam jaringan komputer lokal yang dimiliki melalui konektivitas jaringan lokal ke*wide-area network*. Secara umum, akses-akses yang diinginkan adalah (a) *read access*: mampu mengetahui keseluruhan sistem jaringan informasi; (b) *write access* : mampu melakukan proses menulis ataupun menghancurkan data yang terdapat di sistem tersebut; (c) *denial of service*: menutup penggunaan utilitas-utilitas jaringan normal dengan cara menghabiskan jatah CPU, bandwidth maupun memori.

Ancaman berarti orang yang berusaha memperoleh akses illegal terhadap jaringan komputer seolah-olah dirinya memiliki otoritas terhadap akses ke jaringan komputer. Tidak ada jaringan yang tidak bisa dijebol. Dengan kata lain tidak ada jaringan komputer yang benar-benar aman. Sifat dari jaringan adalah melakukan komunikasi. Setiap komunikasi dapat jatuh ke tangan orang lain dan disalahgunakan.

Sistem keamanan membantu mengamankan jaringan tanpa menghalangi penggunaannya dan menempatkan antisipasi ketika jaringan berhasil ditembus. User dalam jaringan harus memiliki pengetahuan yang cukup mengenai keamanan dan memahami rencana keamanan yang dibuat. Jika mereka tidak memahami hal tersebut, maka mereka akan menciptakan lubang *(hole)* keamanan pada jaringan.

Kerapuhan *(vulnerability)* menyatakan kelemahan pada sistem yang memungkinkan terjadinya gangguan. Terdapat 3 aspek utama dalam keamanan jaringan yakni *condidentiality/privacy*, *integrity*, dan *availability*. *Confidentiality* adalah kerahasiaan atas data pribadi. Data hanya boleh diakses oleh orang-orang yang bersangkutan atau berwenang. Serangan dapat terjadi berupa penyadapan atas data dengan cara teknis seperti *sniffing*, *logger, Man In The Middle Attack*, maupun non teknis dengan cara *social engineering*. Perlindungan yang dapat dilakukan adalah dengan cara enkripsi yakni mengubah suatu format menjadi format lain yang tersandikan.

Integrity berarti bahwa data tidak boleh diubah (*tampered,altered,modified*) oleh pihak yang tidak berhak. Serangan muncul berupa pengubahan data oleh pihak yang tidak berhak *(spoofing)*. Perlindungan yang dapat dilakukan adalah MAC (*Message Authentication Code), Digital Signature /Certificate*, dan *Hash Function.*

Availability berarti bahwa data tersedia atau dapat diakses saat diperlukan. Serangan yang dilakukan dapat berupa peniadaan layanan (*denial of service.*

distributed denial of service) atau menghambat layanan (*respond server* menjadi lambat, malware, worm,dll). Perlindungan dapat berupa *backup, redundancy*, IDS, DRC, BCP, dan Firewall.

Selain itu ada terdapat empat aspek tambahan yakni *non-repudiation, authentication, access control*, dan *accountability*. *Non repudation* berarti menjaga agar transaksi yang terjadi tidak dapat disangkal atau dipungkiri. Umumnya dipakai pada kegiatan *e-commerce*. Perlindungan berupa *digital signature/ certificate*, kriptografi, dan *logging*. *Authentication* berarti meyakinkan keaslian data, sumber daya, orang yang mengakses data, dan server yang digunakan. Serangan dapat berupa situs palsu, identitas palsu, dan terminal palsu.

Access Control adalah mekanisme untuk mengatur "siapa yang boleh melakukan apa " dan "dari mana dan boleh ke mana". Penerapannya membutuhkan klasifikasi data (*public, private,confident, secret*) dan berbasiskan role (kelompok atau grup hak akses). Contoh, ACL antar jaringan , ACL Proxy (pembatasan *bandwith*). *Accountability* berarti adanya catatan atas keperluan pengecekan sehingga transaksi dapat dipertanggungjawabkan. Diperlukan adanya kebijakan dan prosedur *(policy and procedure)*. Implemtasi dapat berupa IDS dan IPS *(firewall)* dan *syslog (router*).

PEMBAHASAN

Pengamanan komputer dilakukan berdasarkan level dan sistem. Berdasarkan level, pengamanan disusun seperti piramida, yaitu keamanan level 0, level 1, level 2, level 3, dan level 4. Sedangkan berdasarkan sistem pengamanan komputer dibedakan menjadi *network topology, security information management*, dan IDS/IPS.

Keamanan Level 0 merupakan keamanan fisik *(physical security)* atau keamanan tingkat awal. Apabila keamanan fisik terjaga maka keamanan di dalam komputer juga akan terjaga. Keamanan Level 1 terdiri dari *database security, data security*, dan *device security*. Dari pembuatan database dapat dilihat apakah digunakan aplikasi yang sudah diakui keamanannya. Selanjutnya adalah memperhatikan *data security* yaitu desain database, karena pendesain database harus memikirkan kemungkinan keamanan dari database. Terakhir adalah device security yaitu alat yang dipakai untuk keamanan dari database tersebut.

Keamanan level 2 merupakan keamanan dari segi keamanan jaringan. Keamanan ini merupakan tindak lanjut dari keamanan level 1. Keamanan level 3 merupakan *information security*. Informasi -informasi seperti kata sandi yang dikirimkan kepada teman atau file-file yang penting, karena takut ada orang yang tidak sah mengetahui informasi tersebut. Keamanan Level 4 adalah keseluruhan dari keamanan level 1 sampai level 3. Apabila satu dari keamanan itu tidak terpenuhi maka keamanan level 4 juga tidak terpenuhi.

Pada network topology sebuah jaringan komputer dapat dibagi atas kelompok jaringan eksternal (internet atau pihak luar), kelompok jaringan internal, dan kelompok jaringan eksternal yang disebut Demilitarized Zone (DMZ). Pihak luar hanya dapat berhubungan dengan host-host yang berada pada jaringan, sesuai dengan kebutuhan. Host-host pada jaringan DMZ secara *default* dapat melakukan hubungan dengan host-host pada jaringan internal. Koneksi secara terbatas dapat dilakukan sesuai kebutuhan. Host-host pada jaringan internal tidak dapat melakukan koneksi ke jaringan luar, melainkan melalui perantara host pada jaringan DMZ, sehingga pihak luar tidak mengetahui keberadaan host-host pada jaringan komputer internal.

Security Information Management (SIM) berfungsi untuk menyediakan informasi yang terkait dengan pengamanan jaringan komputer secara terpusat. Pada perkembangannya SIM tidak hanya berfungsi untuk mengumpulkan data dari semua peralatan keamanan jaringan komputer tapi juga memiliki kemampuan untuk analisis data melalui teknik korelasi dan query data terbatas sehingga menghasilkan peringatan dan laporan yang lebih lengkap dari masing-masing serangan. Dengan SIM, pengelola jaringan komputer dapat mengetahui secara efektif jika terjadi serangan dan dapat melakukan penanganan yang lebih terarah, sehingga organisasi keamanan jaringan komputer tersebut lebih terjamin.

Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) digunakan untuk mendeteksi dan melindungi sebuah sistem keamanan dari serangan pihak luar atau dalam. Pada IDS berbasis, akan menerima kopi paket yang ditujukan pada sebuah host untuk selanjutnya memeriksa paket-paket tersebut. Jika ditemukan paket berbahaya, maka IDS memberi peringatan kepada pengelola sistem. Karena paket yang diperiksa adalah salinan dari paket yang asli, maka jika ditemukan paket yang berbahaya maka paket tersebut akan tetap mencapai host yang ditujunya.

Sebuah IPS lebih aktif daripada IDS. Bekerja sama dengan Firewall IPS dapat memberikan keputusan apakah sebuah paket dapat diterima atau tidak oleh sistem. Apabila IPS menemukan bahwa paket yang dikirim itu berbahaya, maka IPS akan memberitahu firewall sistem untuk menolak paket data itu.

Dalam membuat keputusan apakah sebuah paket data berbahaya atau tidak, IDS dan IPS dapat menggunakan metode *Signature-based Intrusion Detection System* atau Anomaly-based Intrusion Detection System. Pada SID telah tersedia daftar yang dapat digunakan untuk menilai apakah paket yang dikirim berbahaya atau tidak. Pada *Anomaly based Intrusion Detection System* harus dilakukan konfigurasi terhadap dan agar dapat mengetahui pola paket seperti apa saja yang akan ada pada sebuah sistem jaringan komputer. Paket anomali tidak sesuai dengan kebiasaan jaringan komputer tersebut.

Sistem deteksi intrusi (IDS) adalah sebuah perangkat atau aplikasi perangkat lunak yang memantau jaringan atau sistem kegiatan untuk kegiatan berbahaya atau pelanggaran kebijakan dan menghasilkan laporan ke stasiun manajemen. Beberapa sistem mungkin mencoba untuk menghentikan upaya intrusi tapi ini tidak diperlukan atau diharapkan dari sistem pemantauan .

Deteksi intrusi dan sistem pencegahan (IDPS) terutama difokuskan pada identifikasi insiden yang mungkin terjadi , penebangan informasi tentang mereka , dan pelaporan usaha . Selain itu, organisasi menggunakan IDPS untuk keperluan lain , seperti mengidentifikasi masalah dengan kebijakan keamanan, mendokumentasikan ancaman yang ada dan menghalangi orang dari melanggar kebijakan keamanan . IDPS telah menjadi tambahan yang diperlukan untuk infrastruktur keamanan hampir setiap organisasi.

IDPS informasi biasanya catatan yang berkaitan dengan kejadian yang diamati , memberitahu administrator keamanan peristiwa penting yang diamati dan menghasilkan laporan . Banyak IDPS juga dapat menanggapi ancaman yang terdeteksi dengan mencoba untuk mencegah berhasil . Mereka menggunakan beberapa teknik respon, yang melibatkan IDPS menghentikan serangan itu sendiri, mengubah lingkungan keamanan (misalnya konfigurasi ulang firewall) atau mengubah isi serangan itu.

Dalam sistem pasif, sistem deteksi intrusi (IDS) sensor mendeteksi pelanggaran keamanan potensial, menyimpan informasi tersebut dan sinyal peringatan pada konsol dan / atau pemilik. Dalam sistem reaktif, juga dikenal sebagai sistem pencegahan intrusi (IPS), IPS auto-respon terhadap aktivitas yang mencurigakan dengan mengatur ulang sambungan atau dengan memprogram ulang firewall untuk memblokir lalu lintas jaringan dari sumber berbahaya yang dicurigai. The IDPS Istilah ini umumnya digunakan di mana ini bisa terjadi secara otomatis atau atas perintah operator, sistem yang baik "mendeteksi *(alert)"* dan "mencegah".

Meskipun keduanya berhubungan dengan keamanan jaringan, sistem deteksi intrusi (IDS) berbeda dari firewall. Firewall membatasi akses antara jaringan untuk mencegah intrusi dan sinyal serangan dari dalam jaringan. Sebuah IDS mengevaluasi intrusi yang diduga telah terjadi dan sinyal alarm. Sebuah IDS juga jam tangan untuk serangan yang berasal dari dalam sistem. Hal ini secara tradisional dicapai dengan memeriksa jaringan komunikasi, mengidentifikasi heuristik dan pola (sering dikenal sebagai tanda tangan) serangan komputer umum, dan mengambil tindakan untuk mengingatkan operator. Sebuah sistem yang mengakhiri koneksi disebut sistem pencegahan intrusi, dan merupakan bentuk lain dari sebuah firewall lapisan aplikasi.

Firewall adalah pembatas antara jaringan lokal dengan jaringan lainnya yang sifatnya publik (dapat diakses oleh siapapun) sehingga setiap data yang masuk dapat diidentifikasi untuk dilakukan penyaringan sehingga aliran data dapat dikendalikan untuk mencegah bahaya/ancaman yang datang dari jaringan publik.

Ada beberapa tujuan penggunaan

firewall, antara lain (1) mencegah atau mengendalikan aliran data tertentu. Artinya, setiap paket yang masuk atau keluar akan diperiksa, apakah cocok atau tidak dengan kriteria yang ada pada standar keamanan yang didefinisikan dalam firewall; (2) melindungi dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/ kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau local area network (LAN); (3) mencegah upaya berbagai *trojan horses*, virus, phishin, *spyware* untuk memasuki sistem yang dituju dengan cara mencegah hubungan dari luar, kecuali yang diperuntukan bagi komputer dan port tertentu; (4) mem-filter serta meng-audit traffic yang melintasi perbatasan antara jaringan luar maupun dalam.

Pengamanan dengan Firewall

Banyak jaringan dirserang karena kurangnya pengawasan. Ada dua tipe sistem pengamanan sebagai implementasi dari firewall, yakni *Packet Filtering* dan *Proxy Services*. Paket filtering merupakan sistem untuk mengontrol keluar-masuknya paket dari antara host dalam dan host luar secara selektif. Sistem ini dapat memberikan jalan atau menghalangi paket yang dikirim, sangat mengkitalkan arsitektur *Screened Router* yang menjadi filter dengan menganalisis bagian kepala dari setiap paket yang dikirim.

Bagian kepala dari paket ini berisikan informasi penting yaitu IP source address, IP destination address, protocol (dengan melihat apakah paket tersebut berbentuk TCP, UDP atau ICMP), port sumber dari TCP atau UDP, port tujuan dari TCP atau UDP, tipe pesan dari ICMP, dan ukuran paket.

Packet Filtering mengawasi secara individual dengan melihat melalui router, sebuah perangkat keras yang dapat berfungsi sebagai sebuah server karena harus membuat keputusan untuk me-rout seluruh paket yang diterima. Alat ini juga harus menentukan seperti apakah pengiriman paket yang telah didapat itu kepada tujuan yang sebenarnya. *Router* tersebut saling berkomunikasi dengan protokol-protokol untuk me-*rout*.

Protokol yang dimaksud adalah Routing Information Protocol (RIP) atau Open Shortest Path First (OSPF) yang menghasilkan sebuah *table routing* yang menunjuk tujuan dari paket yang diterima. Router yang menjadi filter pada *packet filtering* dapat menyediakan sebuah *choke point* (sebuah *channel* sempit yang sering dipakai oleh penyerang sistem dan dapat dipantau dan dikontrol) untuk semua pengguna yang memasuki dan meninggalkan network. Sistem ini beroperasi di tingkat network layer dan transport layer dari tingkatan protokol pada tingkatan Transmission Control Protocol (TCP/IP).

Proxy memberikan akses internet untuk satu buah host atau sejumlah kecil host dengan menyediakan akses untuk seluruh host. Sebuah proxy server untuk protokol tertentu atau sebuah set dari protokol dapat dijalankan pada sebuah *dual-homed host* atau pada *bastion host*. Proxy ini sangat mendukung arsitektur dari client/server. Clinet/server membentuk sebuah sistem di mana komponen-komponen dari software saling berinteraksi.

Para klien dapat meminta seluruh kebutuhan dan pelayanan yang dinginkan dan server menyediakannya. Sistem proxy harus mendukung seluruh pelayanan yang diminta dan diperlukan oleh klien. Sebab itu server harus mempunyai file server yang sangat besar dan selalu aktif. File-file itu digunakan oleh setiap komputer yang terhubung baik dalam Lokal Area Network (LAN) ataupun Wide Area Network (WAN).

Pada file server selain dari list yang cukup panjang sebagai database yang dapat digunakan oleh setiap klien yang menggunakan alamat IP legal, terdapat juga file-file untuk aplikasi yang bekerja pada server utama. Proxy merupakan sistem pengamanan yang memerlukan alamat IP yang jelas dan valid, karena server utama terdapat di internet.

Firewall peka terhadap kesalahan konfigurasi dan kegagalan untuk menerapkan kebijakan, sehingga diperlukan tambahan atau peningkatan keamanan lain. Oleh karena itu, konfigurasi dan administrasi firewall harus dilakukan secara hati-hati, sehingga organisasi seharusnya dapat bertahan dengan mengurangi kelemahan *(vurnerabilities)* dan gangguan baru.

Tidak cukup kalau hanya digunakan software firewall. Kerjasama yang baik dan kompak antara firewall dengan file keamanan atau antivirus adalah hal yang sangat esensial untuk membuat pertahanan PC yang ideal dalam mencegah *malware* dan *hacker*. Antivirus akan me-*manage* keamanan sistem internal dan firewall berfungsi sebagai tembok atau pembatas access antara sistem internal dan dengan akses keluar masuk sistem internal dan external baik itu data dan jaringan. Dengan adanya antivirus dan firewall yang terpasang pada komputer online serangan hacker atau program-program berbahaya seperti Trojan, Worm, Malware dan jenis virus lainnya yang mencoba mengakses masuk ke komputer melalui jaringan komputer atau internet dapat dicegah.

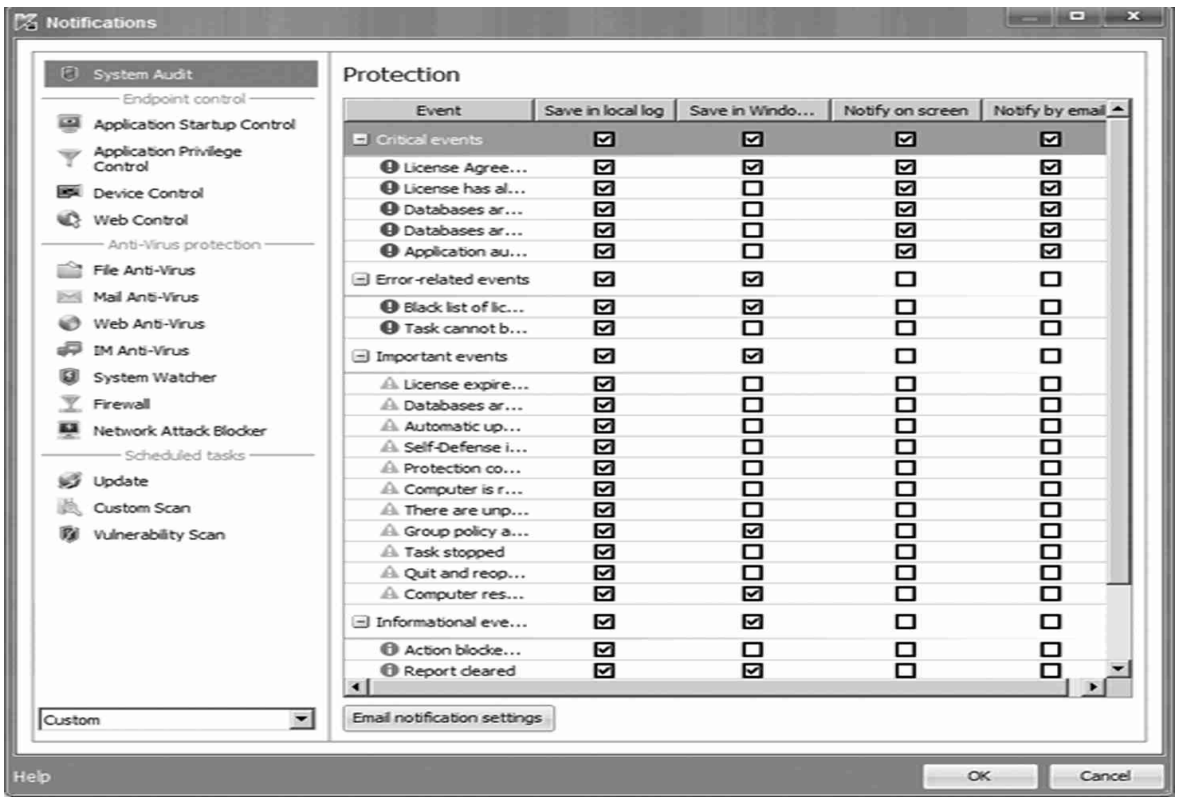
Kaspersky Endpoint Security 8

Pada Kaspersky, IDS bekerja secara otomatis sebagai bagian dari paket jaringan filtering. IDS bertugas mendeteksi port scanning, serangan DoS, dll dan memblokir alamat komputer yang mencoba untuk menyerang.

Pada Kaspersky, IPS mendeteksi tipe serangan yang berbeda dengan scanning network traffic menggunakan signature dari network attack. Pada saat default, saat serangan terdeteksi, komponen memblokir paket jaringan antara penyerangan komputer dan komputer user selama 1 jam. Langkah ini mencegah penyusup atau virus dan memberi perlindungan terhadap serangan DoS.

Kaspersky Endpoint Security 8 for Windows memungkinkan mode pemberitahuan yang berbeda, seperti pop-up pesan dalam system tray dan email pemberitahuan. User dapat meng-konfigurasi modus pemberitahuan secara

Gambar 1 : KSN Reputation Service



Gambar 2 : Dialog Notification Protection

individual untuk setiap jenis acara. Untuk mengkonfigurasi modus pemberitahuan, yang dilakukan adalah:

1. Buka jendela utama *Kaspersky Endpoint Security 8 for Windows.*
2. Buka tab *Settings.*
3. Pilih *Pengaturan lanjutan* > *antar muka* di frame kiri. Frame kanan akan menampilkan pengaturan antarmuka.
4. Klik tombol *Settings* pada bagian *Pemberitahuan.*
5. *Notifikasi* akan terbuka. Notifikasi berisi daftar komponen aplikasi dan tugas di frame kiri, dan event log untuk komponen yang dipilih atau tugas di frame kanan.
6. Pilih komponen atau tugas di frame kiri. Komponen ditandai di *Beritahu pada layar* kolom akan pemberitahuan output dalam bentuk pop-up. Komponen ditandai dalam *Beritahu oleh* kolom *email* akan mengirimkan email notifikasi.
7. Klik tombol *pengaturan pemberitahuan Email.*

Disarankan untuk meng-konfigurasi opsi ini secara terpusat melalui *Kaspersky Security Center 9* Administration Console. Caranya:

1. Aktifkan *acara pemberitahuan Send by* opsi *email*.
2. Masukkan *alamat pengirim*, dan alamat *server SMTP* dan *Pelabuhan* di bidang yang sesuai.
3. Masukkan *nama pengguna* dan *Sandi* account pengguna yang ditentukan dalam bidang *alamat pengirim*.
4. Masukkan *alamat penerima di* bagian *penerima Pemberitahuan*.
5. Klik *Test* untuk menguji pengiriman notifikasi.
6. Pilih modus Kirim: *Jika peristiwa terjadi*, atau *Menurut jadwal*

Gambar 3 : Dialog Notification Setting

7. Klik *OK* dua kali.
8. Klik *Simpan* di jendela utama dari Kaspersky Endpoint Security 8 for Windows untuk menyimpan perubahan.

KESIMPULAN

Pengamanan jaringan merupakan upaya memberikan keterjaminan jaringan atas gangguan yang mungkin muncul. Secara umum, terdapat 3 sumber atau faktor pengganggu keamanan pada jaringan, yakni risiko atau tingkat bahaya, *integrity*, dan *availability*.

Metode pengamanan komputer terbagi atas 5 level, mulai dari level 0 sampai dengan level 4. Tingkat keamanannya dimulai dari keamanan fisik, database security, data security, dan device security, keamanan dalam informasi security sampai dengan keseluruhan dari keamanan level 1 sampai level 3. Apabila ada satu dari keamanan itu tidak terpenuhi maka keamanan level 4 juga tidak terpenuhi.

Antivirus dan firewall merupakan solusi terbaik untuk mengatasi keamanan aplikasi kontrol karena Antivirus akan mengendalikan keamanan sistem internal dan firewall berfungsi sebagai tembok atau pembatas access antara sistem internal dengan akses keluar masuk sistem internal dan external, baik data dan jaringan. Antivirus dan firewall yang terpasang pada komputer online bisa mencegah serangan hacker atau program-program berbahaya seperti Trojan, Worm, Malware dan jenis virus lainnya yang mencoba mengakses masuk ke komputer melalui jaringan komputer atau internet.

DAFTAR PUSTAKA

Alamsyah. 2011. *Implementas I Keama-\-nan Instrusion Detection System (IDS).*

Ardiyanto, Yudhi, 2010. *System Instrusion Detection System*.Sourcefire Inc.: USA.

Basten, Marco van. 2009. *Optimalisasi Firewall pada Jaringan Skala Luas.* Universitas Sriwijaya: Palembang.

Deris, Setiawan. 2005. *Sistem KeamananKomputer*. Elex Media Komputindo: Jakarta

Mikdar, Muhammad., Zhafar, N. Eko., Zulfariana. Zara. 2011. *Analisa Algoritma Sistem Keamanan Komputer Menggunakan Sidik Jari dengan Metode Minutiae pada HP Compaq 2210B Notebook PC,* Jakarta : Universitas Gunadarma