TINJAUAN ISU KEAMANAN JARINGAN KOMPUTER DI TEMPAT KERJA

Intan Yuniar Purbasari

Jurusan Teknik Informatika, Fakultas Teknologi Industri, UPN Veteran Jawa Timur
Email: intan.yuniar@gmail.com

Abstrak *- Dalam tulisan ini akan dibahas beberapa isu keamanan jaringan komputer yang terdapat di tempat kerja. Tempat kerja yang dimaksud disini tidak hanya meliputi dunia perkantoran saja, tetapi juga di dunia industri secara umum, yang melibatkan pemakaian komputer dalam segala bentuk – mulai dari desktop hingga telepon VOIP dan sistem kontrol monitoring dan akuisisi data (SCADA – Supervisory Control and Data Acquisition) – serta penggunaan jaringan komputer pada perangkat komputer tersebut. Di bagian akhir tulisan ini juga dibahas langkah-langkah strategis untuk mengatasi permasalahan keamanan jaringan komputer yang telah dibahas.*

Kata Kunci: Keamanan jaringan komputer, tempat kerja, analisis

Teknologi komputer telah menjadi bagian yang melekat di tempat kerja saat ini. Jaringan, khususnya, telah digunakan untuk mendukung fungsi bisnis di industri (pabrik) dan juga di kantor. Di pabrik, teknologi terbaru dalam sistem kontrol monitoring dan akuisisi data (SCADA – *Supervisory Control and Data Acquisition*) telah mengakomodasi penggunaan internet berbasis protokol untuk menyediakan aplikasi klien tipis dan mengambil keuntungan dari beberapa fitur keamanan seperti VPN (*Virtual Private Network*) dan *Secure Socket Layer* [1]. Salah satu perangkat Cisco, *Ethernet-to-the-Factory* (EttF), juga menyediakan konektivitas antara pabrik dan sistem bisnis dan menjanjikan koneksi yang lebih fleksibel serta dapat diandalkan antara keduanya untuk memasukkan informasi lebih banyak dari kedua belah pihak [2]. Sementara itu di perkantoran, Internet, bersama dengan semua aplikasi yang didasarkan di atasnya (e-mail, instant messaging, VoIP, dan banyak lagi), memiliki peran besar untuk mendukung bisnis dan komunikasi antar-perorangan.

THREAT x VULNERABILITY = RISK

Tren penggunaan Internet di perkantoran telah menimbulkan beberapa risiko keamanan dalam bidang teknologi informasi di dalam perusahaan. Untuk diskusi lebih lanjut mengenai risiko-risiko keamanan, pembahasan akan dimulai dengan mengidentifikasi ancaman keamanan serta kerentanan yang berkaitan dengan tempat kerja saat ini.

Beberapa ancaman keamanan teknologi informasi yang umumnya dapat terjadi di tempat kerja adalah:

Spam

Ini jenis ancaman yang biasanya sangat terkait dengan e-mail, meskipun tidak selalu. Menurut [3], diperkirakan bahwa pada akhir tahun 2006, akan ada sekitar 84 miliar pesan setiap hari dikirim dari bisnis e-mail. Sangat memungkinkan bahwa akan terdapat lebih dari pada jumlah tersebut pada tahun 2012. Dari jumlah itu, hampir seperempatnya bersifat e-mail pribadi dan hampir dua pertiga karyawan mengirim e-mail bisnis melalui akun e-mail pribadi yang berbasis Web.

E-mail, apakah mereka berbasiskan Web ataupun server perusahaan, membawa risiko masing-masing untuk perusahaan. Salah satu contoh nyata dari ancaman e-mail adalah spam atau e-mail yang tidak diinginkan oleh penerima. Jika server mail perusahaan tidak memiliki perangkat lunak yang kuat dan memiliki filter spam yang dikonfigurasi dengan benar, atau lebih buruk lagi, tidak ada filter sama sekali, maka sangat mungkin bahwa e-mail spam akan mulai membanjir masuk ke dalam hard-drive dan mengkonsumsi ruang penyimpanan data. Hal ini akan mengakibatkan respon server menjadi lambat. Belum lagi hilangnya waktu yang berharga dari karyawan

untuk membaca atau menghapus spam. Hal yang sama terjadi juga pada server mail yang berbasiskan web. Server mail dari web mungkin memiliki beberapa filter spam yang lebih baik, tetapi mereka mungkin tidak dikonfigurasi sesuai dengan kebijakan keamanan tertentu dari perusahaan.

Menurut [4], pada kuartal pertama tahun 2010, ada sekitar 183 miliar e-mail spam harian dan topik yang paling populer adalah iklan farmasi (sekitar 81% dari spam). Selain itu, juga dilaporkan bahwa telah terjadi eksploitasi pada link server iklan CNN dan pengguna yang tertipu akan diarahkan ke situs web spamming.

Virus dan Worm

Ancaman ini tidak hanya dapat menyebar melalui e-mail, tetapi juga melalui software Instant Messaging dan bahkan perangkat mobile. Menurut Melanie Turek di [5], hanya sekitar sepertiga dari perusahaan yang telah menggunakan software Instant Messaging yang aman dan dikelola oleh perusahaan itu sendiri. Dua pertiga perusahaan masih memperbolehkan karyawannya untuk menggunakan layanan Instant Messaging (IM) publik yang tidak terlindungi. Hal ini membuat proses pemantauan lalu lintas IM menjadi sulit dan jaringan perusahaan menjadi rentan terhadap virus dan worm.

Di lain pihak, perangkat mobile memiliki penyimpanan memori yang relatif lebih kecil dan kecepatan prosesor yang lebih lambat dari pada komputer desktop. Hal ini menjadikan penambahan software keamanan (seperti antivirus dan manajemen password) dalam perangkat mobile pribadi dapat sangat memperlambat kinerja sehingga perangkat mobile tersebut menjadi tidak dapat digunakan lagi [6]. Inilah sebabnya mengapa sebagian besar perangkat mobile tidak memiliki perangkat lunak keamanan pra-instal. Virus dan worm lalu dapat menyebar dengan menggunakan komunikasi Bluetooth dan menginfeksi sistem operasi. Mereka dapat mengakses file pribadi, mencuri password, atau melakukan konfigurasi ulang sistem. Caribe dan Commwarrior adalah contoh worm yang dapat menginfeksi perangkat mobile Symbian OS [7].

Eavesdropping

Teknologi berbasiskan jaringan telah membuat jalan untuk merangkul teknologi telepon (yaitu percakapan suara) di tempat kerja. Dengan Voice over IP (VoIP), perusahaan telah berhasil membuat lalu lintas suara menjadi bagian dari infrastruktur teknologi informasi untuk menghemat biaya dan meningkatkan produktivitas.

Meskipun teknologi ini memberikan banyak keuntungan, perlu dicatat pula bahwa seluruh ancaman keamanan pada infrastruktur teknologi informasi kini juga berlaku untuk teknologi telepon. Dengan menghubungkan ke LAN yang sama dengan garis suara, seorang hacker bisa mengakses paket suara dan merekam percakapan. Ini akan menjadi masalah serius jika percakapan tersebut adalah percakapan yang bersifat rahasia.

Serangan lain datang dalam bentuk *Denial of Service* (DoS), dengan memanipulasi jaringan dan melumpuhkan IP PBX yang mengeksploitasi kurangnya *access control list* pada VLAN sehingga penyerang bisa mendapatkan akses ke VLAN dimana telepon VoIP atau server berada dan mengirim pesan palsu atau membanjiri jaringan dengan paket [9, 10]. Ini adalah serangan yang paling umum pada VoIP dengan dampak potensialnya adalah ketidakmampuan server untuk memulai panggilan, panggilan terputus (*call dropped*), dan adanya sinyal sibuk yang konstan. [10] telah melakukan studi tentang implementasi VoIP dan melakukan penilaian keamanan di beberapa perusahaan dan telah mengidentifikasi beberapa kerentanan yang mungkin ada pada sebuah perusahaan seperti:

a. Kebijakan organisasi → Kebijakan "build first, secure later", yakni kebijakan yang mementingkan sebuah teknologi dibuat dulu, dan segi keamanan akan dipikirkan kemudian. Perusahaan bersikeras untuk segera mengimplementasikan VoIP dan mungkin secara tidak sengaja melewatkan pemeriksaan persyaratan keamanan.
b. Kontrol Jaringan dan Arsitektur → Inkonsistensi dalam protokol jaringan filtering dan routing. Dalam tahap awal implementasi, konfigurasi jaringan mungkin tidak terlalu dibatasi untuk tujuan pengujian dan ini berpotensi akan membuka beberapa titik yang dapat diakses oleh penyerang untuk menyelinap masuk dan menguping percakapan atau mengakses direktori sistem.

c. Konfigurasi Node → Layanan yang tidak dikonfigurasi dengan baik dan direktori yang di-*share* melalui jaringan yang tidak terlindungi. Seorang penyerang dapat menelusuri direktori *shared* di dalam jaringan yang berisi file-file konfigurasi sistem atau catatan pelanggan, serta memperoleh akses ke file yang menyimpan password dan data pelanggan yang bersifat penting dan rahasia, lalu melancarkan serangan *buffer overflow* atau melakukan konfigurasi ulang pada sistem.
d. Streaming media → Ketika pengguna melakukan streaming media pada sistem yang tidak terenkripsi, hal ini akan memudahkan penyerang untuk menguping pembicaraan dan mengambil informasi rahasia perusahaan.

Spoofing

Teknologi Supervisor Kontrol dan Data Akuisisi (SCADA) telah bergerak ke arah sistem yang berbasis Internet Protocol (IP) selama beberapa tahun belakangan ini. Walaupun masih ada keraguan apakah ancaman dunia maya memang ada untuk SCADA [11], tetapi sesungguhnya memang nyata. Mulai dari serangan replay, spoofing, serta man-in-the-middle attack, semua ancaman tersebut siap untuk mengeksploitasi setiap kerentanan yang ada di dalam sistem SCADA.

Salah satu bentuk kerentanan pada SCADA adalah kurangnya otentikasi antara master dan perangkat remote sebelum membangun koneksi dalam sebagian besar sistem kontrol utilitas listrik [12]. Tanpa adanya otentikasi apapun, sebuah pesan palsu dapat dikirim oleh penyerang yang berpura-pura datang dari perangkat yang valid. Ini disebut spoofing. Pesan palsu tersebut dapat berupa data status palsu dan mengganggu kerja dari keseluruhan sistem.

Bentuk kerentanan lain adalah meningkatnya penggunaan dari sistem perangkat lunak SCADA komersial [11]. Hal ini berpeluang untuk membuka kerentanan kesalahan dari software (*software bug*).

Tidak ada data pasti tentang jumlah sebenarnya dari serangan cyber ke sistem SCADA karena perusahaan cenderung menyembunyikannya dari masyarakat, namun ada beberapa laporan tentang serangan yang sukses dilakukan pada sistem SCADA di berbagai negara, seperti perusahaan perpipaan gas di Rusia pada tahun 2000 dan pengolahan limbah Australia pada tahun 2001 [13].

Phising

Teknologi jaringan sosial juga ikut memainkan peranan yang penting dalam menyebarkan malware dengan menggunakan teknik phishing. Seperti dilaporkan pada tahun 2010 oleh survei perusahaan TrendMicro di [14], penggunaan teknologi jejaring sosial di tempat kerja telah meningkat dari 19 persen pada 2008 menjadi 24 persen pada tahun 2010. Meningkatnya jumlah pengguna di jejaring sosial merupakan alasan yang tepat untuk menyebarkan malware melalui jejaring sosial. Koobface, yang merupakan anagram dari FACEBOOK, menggunakan pesan palsu antara "teman" di Facebook dan mengelabui pengguna untuk menginstal perangkat lunak berbahaya di dalam komputer mereka. Malware kemudian dapat mencuri informasi pribadi dari pengguna. Serangan lain berupa eksploitasi kelemahan keamanan Facebook di mana informasi dasar tentang pengguna dapat dilihat oleh siapa saja, terlepas dari pengaturan keamanan yang diterapkan [15]. Penyerang dapat saja mencuri informasi yang seharusnya bersifat rahasia dan lalu menyalahgunakannya.

TINDAKAN PENCEGAHAN

Berikut ini beberapa strategi tindakan pencegahan yang dapat dilakukan untuk menghindari terjadinya serangan pada sistem jaringan komputer di tempat kerja:

Pencegahan untuk E-mail spam

Cara termudah untuk mencegah e-mail spam adalah menginstal perangkat lunak "anti-segalanya" yang selalu diperbarui, dan itu juga mencakup anti-spam, dalam komputer server mail dan komputer klien [16]. Hal ini setidaknya akan mengurangi jumlah spam, meskipun tidak sepenuhnya mencegah spam untuk dapat masuk ke dalam jaringan internal kantor. Dimungkinkan juga terdapat "False Positive" dan False Negative", yakni kesalahan dalam pengklasifikasian e-mail spam atau bukan, yang dibuat oleh filter spam. Beberapa penelitian telah dilakukan untuk meningkatkan kemampuan filter spam dalam mengenali spam yang lebih canggih. Salah satu contohnya

adalah penelitian di [17] yang menggunakan gabungan antara teori himpunan kasar, algoritma genetika, dan *reinforcement learning* untuk lebih baik dalam mengenali struktur spam.

Tindakan preventif lainnya adalah dengan membatasi penggunaan e-mail perusahaan untuk komunikasi bisnis saja. Karyawan tidak boleh diizinkan menggunakan akun e-mail perusahaan untuk mengakses situs e-commerce jika untuk kepentingan pribadi, atau situs-situs lain di luar yang disetujui oleh pihak perusahaan.

Pencegahan untuk virus dan worm pada e-mail, Instant Messaging, dan perangkat mobile

Serupa dengan penanggulangan untuk e-mail spam, penanggulangan yang pertama adalah dengan menginstal perangkat lunak antivirus dan memperbaruinya secara teratur. Karyawan juga harus dididik untuk tidak sembarangan mengklik link yang tidak dikenal atau mencurigakan yang mereka terima di kotak surat mereka untuk menghentikan penyebaran virus lebih jauh lagi.

Karena menginstal perangkat lunak antivirus di perangkat mobile terlalu mahal (dalam hal ruang dan kinerja) untuk sebagian besar jenis perangkat, produsen perangkat mobile harus memvalidasi input saat mengembangkan fitur yang terkait dengan teknologi Bluetooth yang mencegah *buffer overflow* dan penelusuran ilegal pada direktori file [7]. Mereka juga harus menonaktifkan protokol-layanan multiplexer (*Protocol-Service Multiplexer*/PSM) yang tidak perlu dan kanal RDComm untuk mencegah penyerang mendapatkan akses ke layanan standar pada perangkat dan juga pintu belakang (*backdoor*) dari sistem.

Dari sisi pengguna, pertahanan terbaik terhadap serangan malware adalah dengan menonaktifkan layanan Bluetooth saat tidak digunakan untuk memblokir setiap upaya untuk terhubung ke perangkat mobile.

Pencegahan untuk *eavesdropping* (dan serangan lainnya) pada VoIP

Protokol signaling dan media stream yang tidak terenkripsi adalah kerentanan yang "mengundang" penyerang untuk menguping percakapan di jalur VoIP [10]. Oleh karena itu, sangatlah penting untuk selalu mengenkripsi setiap paket yang dikirim melalui jalur VoIP untuk mencegah penyerang mendengarkan percakapan yang bersifat rahasia.

Untuk mengatasi serangan *Denial of Service* yang mengeksploitasi kerentanan dalam kontrol arsitektur dan jaringan, sangat disarankan untuk menerapkan *Access Control Lists* (ACL) antara VLAN-VLAN yang ada dalam jaringan perkantoran, sehingga lalu lintas suara hanya akan mengalir antara subnet dan mencegah akses yang tidak sah untuk menjelajah antara VLAN-VLAN dan mencari lokasi Server untuk memulai serangan.

Pencegahan untuk *spoofing* (dan serangan lainnya) pada SCADA

Untuk mencegah serangan spoofing yang mengeksploitasi kurangnya otentikasi antara master dan perangkat remote sebelum membuat sambungan, perusahaan harus menegakkan otentikasi untuk setiap akses ke sistem SCADA, baik dari pengguna di luar atau di dalam, dan pastikan bahwa setiap sambungan terenkripsi dengan aman dan sepenuhnya diawasi [12]. Bagian otentikasi dan enkripsi menjamin bahwa setiap akses ke sistem ini berasal dari sumber yang sah, sedangkan bagian pengawasan diperlukan untuk memantau siapa saja yang membuat perubahan ke jaringan.

Tindakan pencegahan lainnya yang harus dilakukan jika sebuah perusahaan menggunakan software SCADA komersial, pastikan bahwa mereka memiliki patch terbaru dan update untuk menutup pintu belakang yang dapat dieksploitasi oleh penyerang.

Pencegahan untuk *phising* pada media jejaring sosial

Satu penanggulangan sederhana yang dapat dilakukan di tempat kerja adalah hanya dengan melarang akses ke situs jejaring sosial, seperti yang telah diterapkan oleh banyak bank, menurut sebuah survei oleh [18] pada bulan April 2010.

Solusi lain yang lebih "lembut" diusulkan oleh para sebagian besar ahli keamanan seperti yang dilaporkan dalam [19], bahwa harus ada kebijakan keamanan mengenai penggunaan situs jejaring sosial dan penggunaannya perlu dipantau untuk melindungi karyawan dan juga

data perusahaan yang bersifat sensitif. Sebuah nasihat yang bijak adalah jangan pernah mengklik link apapun tanpa terlebih dahulu memeriksa kemana link tersebut menuju.

Keputusan untuk menampilkan profil pengguna secara publik tanpa pengaturan keamanan yang diterapkan di Facebook mungkin masih dianggap kontroversial [20], namun pengguna masih memiliki pilihan untuk membatasi apa yang orang lain dapat lihat dengan cara memanfaatkan *Account*, Privasi, dan Aplikasi Pengaturan link di Facebook. Dengan cara seperti ini, pengguna dapat memilih siapa saja yang dapat melihat informasi atau foto tertentu dan menyimpan informasi pribadi mereka hanya untuk mereka yang dikategorikan sebagai teman dekat.

DAFTAR RUJUKAN

[1] Anonymous. (2010). SCADA. [Online]. Available: http://en.wikipedia.org/wiki/SCADA.

[2] Anonymous. (2009). Cisco Ethernet-to-the-Factory: At a Glance. [Online]. Available: http://www.cisco.com/web/strategy/docs/manufacturing/c45-567755_ettf_aag.pdf.

[3] K. Kalinich, "*Personal E-Mail Creates Workplace Risks*," *National Underwriter. P & C*, vol. 110, p. 27, 2006.

[4] Anonymous, "*Internet Threats Report Q1 2010*," CommTouch, Netanya, Israel 2010.

[5] M. Turek, "*Instant Messaging: Security, Control And Compliance*," *Business Communications Review*, vol. 36, p. 32, 2006.

[6] B. Michael and J. Viega, "*Mobile Device Security Introduction*," *IEEE SECURITY & PRIVACY*, vol. 8, pp. 11-12, 2010.

[7] J. P. Dunning, "*Taming the Blue Beast A Survey of Bluetooth-Based Threats*," *IEEE SECURITY & PRIVACY*, vol. 8, pp. 20-28, 2010.

[8] A. Kondolojy. (2010). *Security Issues in Instant Messenger*. [Online]. Available: http://www.ehow.com/list_6701370_security-issues-instant-messenger.html.

[9] C. Stredicke, "*Why VoIP security matters*," *Communications News*, vol. 44, p. 30, 2007.

[10] P. Thermos, "*Evaluating the Security of Enterprise VoIP Networks*," *IT Professional Magazine*, vol. 11, p. 30, 2009.

[11] B. Clint, W. Jeff, and P. Chris, "*SCADA Security, Compliance, and Liability - A Survival Guide*," *Pipeline & Gas Journal*, vol. 235, p. 82, 2008.

[12] A. Bartels, "*Assessing and addressing cyber threats to control systems*," *POWER*, vol. 152, pp. 40-44, 2008.

[13] C. P. Sandip and S. Pritimoy, "*Securing SCADA systems*," *Information Management & Computer Security*, vol. 16, p. 398, 2008.

[14] Anonymous, "*Trend Micro Reports Global Rise in Workplace Social Networking*," New York: PR Newswire, 2010.

[15] D. Sancho, "*Security Guide to Social Networks*," Trend Micro, Inc., Cupertino, California, USA 2009.

[16] G. Hinson, T. Bass, M. Iacovacci, D. Parker, S. l. Grange, C. Norman, R. O. Regalado, P. Hillier, G. Choo, M. Smith, L. Bell, and A. Aylward. (2007). *Top Information Security Risks for 2008*. [Online]. Available: http://www.iso27001security.com/Top_information_security_risks_for_2008.pdf.

[17] C.-M. Chen, C.-S. Laih, G.-H. Lai, and T. Chen, "*A collaborative anti-spam system*," *Expert Systems with Applications*, vol. 36, pp. 6645-6649, 2009.

[18] R. Horn, "*The new risks of social networking*," *Texas Banking*, vol. 99, pp. 8-3, 2010.

[19] Anonymous. (2010). *Social Networking Weakens Enterprise Security*. *Information Week* [Online]. Available: http://www.informationweek.in/Security/10-07-14/Social_Networking_weakens_enterprise_security.aspx.

[20] M. E. Kabay. (2010). *Privacy issues in social-networking sites. Network World* [Online]. *(Journal Article)*. Available: http://www.networkworld.com/newsletters/sec/2010/092710sec1.html.