Automatisasi Penanganan Insiden dan Deteksi Phishing

Makalah Tugas Kuliah EL6115

Operasi Keamanan dan Incident Handling

Oleh

YOGI KRISTIAWAN

NIM : 23215097

Dosen :

Ir. BUDI RAHARDJO, MSc., PhD.

SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA

INSTITUT TEKNOLOGI BANDUNG

2016

ABSTRAK

Phishing merupakan salah satu serangan terhadap jaringan dimana penyerang menciptakan replika dari suatu halaman web untuk menipu pengguna. Untuk model penanganan dan deteksi phishing yang akan diusulkan berdasarkan pada pemrosesan insiden phishing otomatis menggunakan alat PhiGARo. Meskipun PhiGARo mampu memproses insiden *phishing* secara otomatis, namun penangannya terbatas pada adanya laporan insiden *phishing* dari *user*. Oleh sebab itu untuk meminimalkan ketergantungan dari input user salah satu cara yang dapat digunakan adalah dengan menggunakan *honeypot*. *Honeypots* digunakan untuk menangkap *e-mail* dari *phishers*, secara otomatis mendeteksi pesan yang berisi *phishing* dan segera mentransfernya ke PhiGARo.

Kata kunci: *phishing*; phiGARo; *honeypot*; *e-mail*

DAFTAR ISI

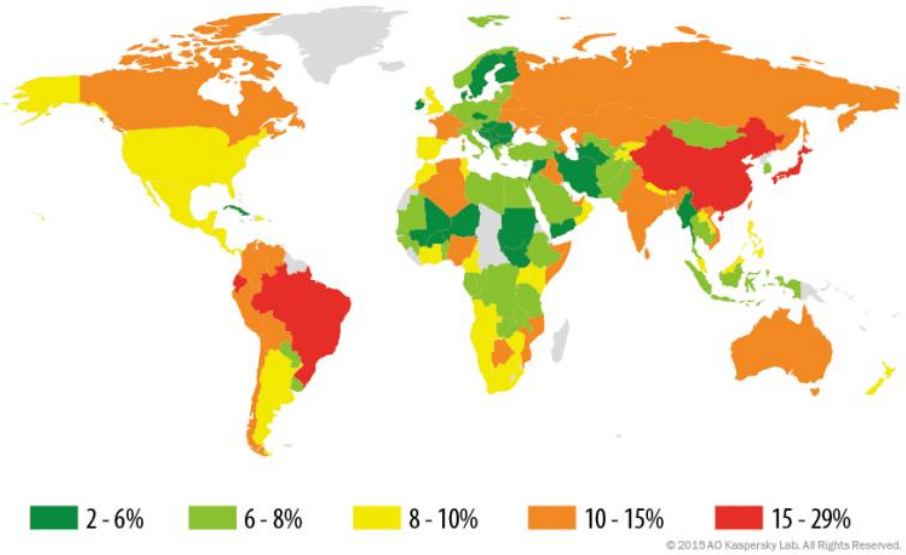
DAFTAR GAMBAR

Bab I Pendahuluan

Seiring dengan kemajuan berbagai kegiatan dalam lingkup teknologi informasi, semakin meningkat pula resiko serangan terhadapnya. Salah satu jenis serangan yang umum terjadi ialah *social enginering*. *Social enginering* adalah tindakan memanipulasi seseorang untuk mengambil tindakan yang bukan atau belum menjadi prioritas utama dari target. Hal tersebut dapat berupa untuk memperoleh informasi, mendapatkan akses, atau membuat target melakukan suatu aksi tertentu [1].

Terdapat berbagai macam jenis serangan *social engineering* salah satu yang terkenal ialah *phishing*. *Phishing* merupakan suatu kegiatan pencurian informasi dengan menggunakan surat elektronik sebagai media penyampai informasi seolah-olah surat tersebut telah dikirim oleh pihak-pihak terpercaya lalu meminta user mengisi formulir yang disediakan dengan informasi tertentu [2].

Jumlah serangan *phishing* tidaklah sedikit. Pada kuartal 3 2015 sendiri Kaspersky [3] mencatat ada 36.300.537 kali percobaan serangan pishing atau meningkat 6 juta percobaan lebih dibanding kuartal sebelumnya. Sementara dari sumber yang sama untuk distribusinya dapat dilihat pada gambar 1.



Gambar 1.1 Persentasi Penyebaran Phishing

Pada makalah ini akan dibahas model automatisasi pencegahan dam penanganan insiden response terhadap serangan pishing. Penerapan automatisasi nantinya akan memanfaatkan tool bernama PhiGARo (Phishing: Gather, Analyze, React, and Distribute) yang berfungsi untuk memproses kejadian phishing dan mencegah kerugian lebih lanjut terkait dengan insiden tersebut. Makalah ini terdiri atas empat bab. Bab I berisi tentang pendahuluan, Bab II berisi tinjauan pustaka mengenai penelitian yang berkaitan dengan topik makalah, Bab III berisi rincian tahapan dari model proses penangan insiden terhadap phishing, dan Bab IV berisi kesimpulan dari makalah ini.

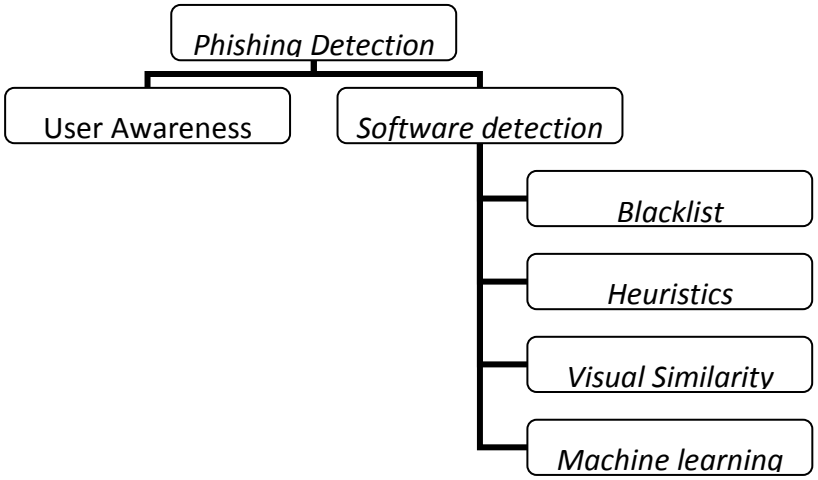
Bab II Tinjauan Pustaka

Pada bab ini berisi tinjauan pustaka mengenai penelitian yang berhubungan dengan topik makalah antara lain:

II.1 Mendeteksi *Phishing*

Tujuan umum dari mendeteksi adanya serangan phishing adalah untuk menemukan teknik otomatis mendeteksi atau filter terhadap phishing e-mail. Teknik ini dapat diterapkan oleh *mailservers* atau e-mail klien. Phishing dibedakan sesuai dengan tanda-tanda yang umum, e-mail phishing biasanya berisi link website phishing atau kata kunci seperti password, login, dll.

Pendekatan untuk melakukan deteksi phishing dapat dibedakan menjadi 2 yakni melalui kesadaran pengguna untuk membedakan antara e-mail phishing atau bukan dan melalui piranti lunak yang di buat berdasarkan kriteria tertentu untuk mendeteksi adanya serangan phishing. Berikut merupakan pendekatan deteksi phishing oleh Khonji et al [4].



Gambar 2.1 Pendekatan deteksi *phishing*

II.2 PhiGARo

PhiGARo (Phishing: Gather, Analyze, React, and Distribute) [5] merupakan sebuah piranti lunak untuk penanganan insiden response terhadap phishing secara otomatis. Piranti lunak ini menggabungkan fungsi alat untuk identifikasi serangan dari data yang tersedia (NetFlow, surat log), alat untuk respon anti-phishing dan alat untuk manajemen insiden keamanan (seperti *Request Tracker*) phishing.

PhiGARo merupakan instrumen yang memungkinkan penanganan langsung terhadap insiden phishing. Alat ini memberikan instrumen dan metrik untuk identifikasi calon korban phishing lainnya. Selanjutnya, tidak hanya fungsi identifikasi tapi juga menawarkan fungsionalitas seperti secara otomatis memberitahukan korban terhadap bahaya suatu *e-mail phishing*, IP *blocking* dan alamat *e-mail* filtering.

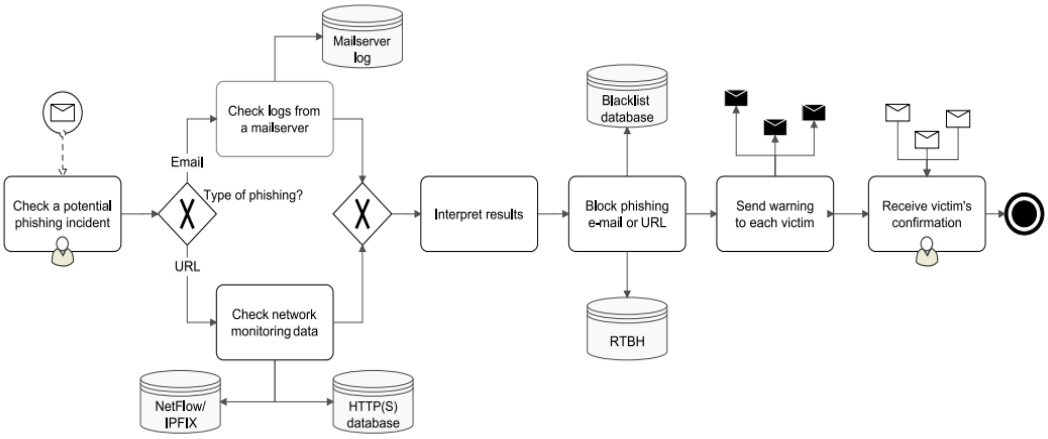
II.3 ***Honeypot***

Honeypot merupakan suatu sistem yang dibuat menyerupai aslinya dan digunakan untuk mengundang penyerang dengan ruang lingkup untuk mendeteksi, dan memantau tindakan yang mereka lakukan [6]. *Honeypot* dibuat bertujuan agar penyerang menjadikannya sebagai sasaran aksinya, dalam hal penanganan insiden phishing kita berupaya agar penyerang mengirim *e-mail phishing* ke alamat *honeypot* sebelum atau disaat yang bersamaan penyerang mengirimnya juga ke e-mail pengguna biasa. Dengan mengetahuinya *e-mail phishing* lebih dahulu atau bersamaan dibanding pengguna biasa, kita akan mampu melakukan upaya pencegahan serangan *phishing*.

BAB III Pembahasan

III.1 Penanganan Insiden Response Phishing

Sebuah kejadian yang mengakibatkan terganggunya kinerja dari suatu sistem tidak akan pernah bisa dihilangkan. Oleh sebab itu penanganan respon terhadap hal yang berpotensi merugikan tersebut perlu disiapkan. Penanganan terhadap phishing pada makalah ini memiliki tujuan utama untuk melindungi pengguna pada suatu jaringan tertentu dari responnya terhadap e-mail phishing dan mengakses web phishing. Menggunakan PhiGARo sebagai bagian utama penanganan insiden response terhadap phishing berikut merupakan diagram alur penanganannya.



Gambar 3.1 Diagram Alur Penanganan Insiden Respon Pishing

Lebih detail terkait cara kerja PhiGARo adalah sebagai berikut ;

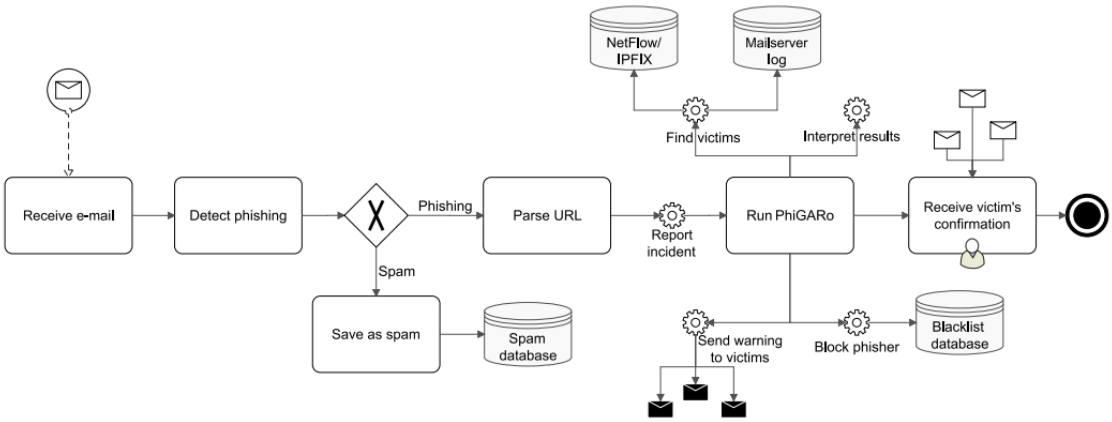
1. User yang mengidentifikasi adanya phishing dalam e-mail mereka melapor melalui e-mail atau *web form* dan diterima oleh Request Tracker .
2. PhiGARo lalu mengevaluasi jenis phishing untuk menentukan metode yang digunakan untuk mengidentifikasi korban lainnya. Jika phishing berisi alamat URL, monitoring jaringan dan sistem log dari server e-mail akan digunakan untuk identifikasi korban lainnya. Lalu URL yang dilaporkan diperiksa untuk mengetahui URL yang sebenarnya tersembunyi di balik Penyingkat URL dan pengalihan URL.

Untuk menemukan lokasi korban phishing lainnya yang telah mengakses alamat URL tersebut digunakan NetFlow. NetFlow memproses *network traffic* pada lapisan ketiga dari model OSI. Setelah mengetahui alamat *IP address* dari *phishing website* PhiGARo lalu mencari adanya network traffic antara *IP address* dan network yang di monitoring. Selanjutnya Alamat *IP address*, dimana situs phishing diakses, ditandai sebagai calon korban phishing.

3. Jika tidak ada URL dalam pesan phishing, sistem log dari server e-mail diurai. PhiGARo mencari e-mail yang dikirim untuk menanggapi pesan phishing. E-mail tanggapan terhadap pesan phishing dikenal oleh *timestamps* dan alamat e-mail dari pengirim dan penerima. Selanjutnya korban dapat langsung diidentifikasi berdasarkan alamat e-mail mereka.
4. Ketika korban lainnya sudah diidentifikasi melalui e-mail atau IP address. PhiGARo berlanjut dengan interpretasi hasil dan *false positive detection* disaring. *False positive detection* terjadi saat korban mengakses situs phishing, tapi tidak ada data yang dikirimkan.
5. Selanjutnya dilakukan tindakan pencegahan yakni dengan memblokir dan pelaporan modul. PhiGARo terhubung pada mekanisme memblok yang digunakan dalam. RTBH (Remotely- Triggered Black Hole) digunakan untuk memblokir setiap *traffic* antara jaringan terlindung dan *IP address* dimana situs phishing tersimpan. Sementara E-mail *address* phishing diteruskan ke mailservers yang kemudian melakukan filter pesan yang mengandung alamat tersebut
6. Langkah terakhir dari pemrosesan insiden phishing oleh PhiGARo adalah memberitahukan korban. PhiGARo mengirimkan peringatan e-mail ke semua korban yang teridentifikasi. Peringatan itu berisi penjelasan kejadian, sampel pesan phishing, bukti kegiatan korban, dan *screenshot website phishin*. Insiden ini kemudian ditandai sudah diselesaikan di request tracker.

III.2 Deteksi Phishing dengan *Honeypot*

Pada penjelasan sebelumnya telah dijelaskan cara penangan insiden respon pada serangan fishing menggunakan alat PhiGARo. Kelemahan dari alat tersebut adalah sebuah insiden baru dapat di proses jika sudah ada pengguna yang melapor adanya e-mail phishing didalam e-mailnya. Untuk mengatasinya Martin Husak dan Jakub Cegan mengusulkan model baru dengan menggunakan honeypot [7]. Honeypots digunakan untuk menangkap, mendeteksi, and melaporkan phishing.



Gambar 3.2 Diagram Alur penanganan insiden respon phishing menggunakan *honeypot*

Lebih detail terkait cara kerja model penanganan insiden respon menggunakan *honeypot* adalah sebagai berikut ;

1. Honeypot yang di buat untuk menarik e-mail phishing ke honeypot e-mail address.
2. E-mail yang masuk akan di cek oleh honeypot apakan e-mail tersebut merupakan phishing atau spam.
3. Honeypot selanjutnya melakukan pengecekan dengan cara pencarian alamat URL pada e-mail tersebut. Setelah didapat URL tersebut akan diperiksa untuk mengetahui URL yang sebenarnya tersembunyi di balik Penyingkat URL dan pengalihan URL. Jika hasilnya diduga phishing maka honeypot akan membuat laporan insidennya lalu melanjutkannya ke PhiGARo. Namun jika di dalam e-mail tersebut tidak ditemukan

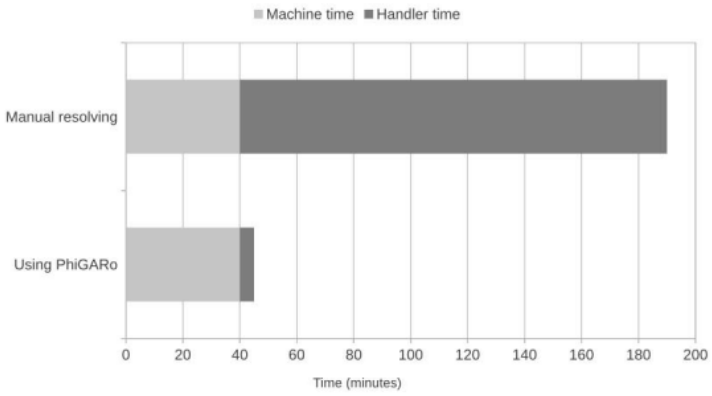
URL atau ditemukan namun setelah dilakukan pengecekan URL tersebut aman. Maka e-mail tersebut akan disimpan ke dalam database spam.

4. Proses penanganan selanjutnya akan dilakukan oleh PhiGARo (hal 11-12).

Permasalahan utama dalam penerapan honeypot ini adalah bagaimana cara agar phisher mengetahui e-mail address dari honeypot. Untuk mengatasi masalah tersebut adalah dengan cara melakukan penyebaran e-mail address dari honeypot. Terdapat 2 cara untuk melakukannya. Pertama cara pasif yakni dengan mempublishnya pada halaman utama dari website yang sering dikunjungi sehingga dapat dengan mudah diakses oleh *web crawler*. Kedua cara aktif yakni dengan mempublish alamat e-mail tersebut langsung ke websites yang didedikasikan memang untuk phishing atau dapat juga dengan menawarkannya langsung di *black market.*

III.3 Hasil Implementasi Penelitian

Penerapan penanganan insiden respon terhadap phishing menggunakan PhiGARo telah dilakukan oleh Martin Husak dan Jakub Cegan [7]. Hasilnya selama tahun 2012 sebanyak 79 kasus insiden phishing berhasil diselesaikan sementara tahun 2013 meningkat menjadi 133 kasus insiden phishing. Sementara perbandingan waktu yang dibutuhkan untuk menyelesaikan kasus insiden phishing dapat dilihat pada gambar 3.3. Pada gambar tersebut nampak penggunaan PhiGARo sebagai alat penanganan insiden phishing secara otomatis dapat mempercepat waktu penyelesaian insiden sebesar lebih dari 100 jam.



Gambar 3.3 Rata-rata Waktu yang Dibutuhkan untuk Menyelesaikan Kasus Insiden Phishing pada Tahun 2013

BAB IV Kesimpulan dan Saran

Untuk penangangan insiden respon terhadap serangan *phishing* secara otomatis dengan penerapan alat PhiGARo mampu secara otomatis menemukan korban phishing menggunakan *network monitoring* dan sistem log dari mailservers. Serangann serupa lebih lanjut dapat dicegah dengan menghalangi pesan *phishing* dan akses ke *phishing website*. Lalu insiden phishing yang telah terjadi didokumentasikan dan disimpan untuk dapat penyelidikan di masa mendatang. Penerapan PhiGARo juga dapat menghemat ratusan jam waktu yang dihabiskan untuk penanganan insiden.

Honeypot digunakan sebagai solusi ketergantungan terhadap laporan user ke PhiGARo. Dengan penerapannya phishers ditarik agar mengirim serangan *phishing* ke alamat *e-mail honeypot* yang tersedia. E-mail yang masuk kemudian dilakukan deteksi kemungkinan adanya *URL phishing* untuk selanjutnya jika dideteksi adanya hal tersebut akan diteruskan ke PhiGARo. Selanjutnya penyebaran alamat *e-mail honeypot* juga diperlukan untuk memperbesar kemungkinan *phishers* mengirim *e-mail phishing.* Cara yang digunakan dapat dengan meletakkan pada alamat website yang sering dikunjungi orang, alamat website yang memang didedikasikan untuk *phishing*, sampai dengan menawarkannya langsung di *black market.*

Saran

1. Mengatasi *phising* dengan software detection seperti PhiGARo saja tidaklah cukup. Pelatihan terkait dengan *user awareness* juga perlu dilakukan
2. Penelitian lebih lanjut terkait *phishing detection* lebih lanjut perlu terus dilakukan mengingat teknik *phishing* saat ini yang terus berkembang.

DAFTAR PUSTAKA

[1] C. Hadnagy, *Social Engineering : The Art of Human Hacking*, United State of Amerika: Wiley Publishing. Inc , 2011.

[2] *Technical Trends in Phishing Attacks*, US-CERT, J. Milletary, 2012

[3] J. Milletary, *Social Engineering : The Art of Human Hacking*, United State of Amerika: Wiley Publishing . Inc , 2011.

[4] M. Khonji, Y. Iraqi, and A. Jones, "Phishing Detection: A Literature Survey," Communications Surveys Tutorials, IEEE, vol. 15, no. 4, pp. 2091–2121, Apr 2013.

[5] J. Cegan, J. Soukal, M. Dra sar, and J. Vykopal, "PhiGARo – tool for phishing incident processing," Masaryk University, 2012. [Online]. Available: http://www.muni.cz/ics/services/csirt/tools/phigaro

[6] A. Pauna, "Improved Self Adaptive Honeypots Sapable of Detecting Rootkit Malware," 2012 9th International Conference on Communications (COMM), pp. 281-284, 2012.

[7] M. Husak and J. Cegan, "PhiGARo: Automatic Phishing Detection and Incident Response Framework," *Availability, Reliability and Security (ARES), 2014 Ninth International Conference on*, Fribourg, 2014