Restorative: Journal of Indonesian Probation and Parole System
Volume 1, Issue 1, October 2023, Pages 33-45
https://doi.org/10.61682/restorative.v1i1.5 **E ISSN 3025-812X**

Analisis Peran dan Penanggulangan Kejahatan Siber: Studi Kasus *Spearphishing*

Marhaeni Sekar Fajar Purwani
Balai Pemasyarakatan Kelas I Yogyakarta
Correspondence: marhaeni.purwani.21@alumni.ucl.ac.uk

Received: September 5, 2023	*Revised: September 15, 2023*	*Approved: September 20, 2023*

Citation: Purwani, M. S. F. (2023). Analisis peran dan penanggulangan kejahatan siber. *Restorative: Journal of Indonesian Probation and Parole System, 1(1), 33-45,* https://doi.org/10.61682/restorative.v1i1.5

Abstract. The understanding of the mechanism, modus operandi, and actors involved in a cybercrime is a crucial early step to design cybercrime countermeasure strategies. This paper discusses a hypothetical case of spearphishing that involves the perpetrators, victims, as well as the unwitting participants of the committed cybercrime. Four approaches in cybercrime countermeasures are afterwards elaborated for the aforementioned hypothetical case. It is concluded that countermeasures based on education are the type of countermeasure most feasible and most crucial to be implemented; however, all types of countermeasures have their limitations and therefore have to continuously evolve and develop along with the increasingly sophisticated cybercrime.

Keywords: *actors, analysis, case study, cybercrime, roles*

Abstrak. Pemahaman mengenai mekanisme, modus operandi, serta pihak-pihak yang terlibat dalam kejahatan siber merupakan langkah awal yang penting untuk merancang strategi penanggulangan tindak kejahatan siber. Karya tulis ini membahas sebuah kasus hipotetis serangan *spearphishing* yang melibatkan pelaku, korban, beserta pihak-pihak lain yang tanpa disadari juga terlibat dalam kejahatan siber yang dilakukan. Empat jenis pendekatan dalam penanggulangan kejahatan siber dibahas untuk kasus hipotetis tersebut. Disimpulkan bahwa penanggulangan dengan pendekatan edukasi merupakan jenis penanggulangan yang paling memungkinkan dan paling penting untuk dilaksanakan; namun, setiap jenis penanggulangan memiliki keterbatasan dan harus terus dikembangkan seiring dengan juga kejahatan siber yang semakin canggih.

Kata kunci: *analisis, kejahatan siber, pelaku, peran, studi kasus*

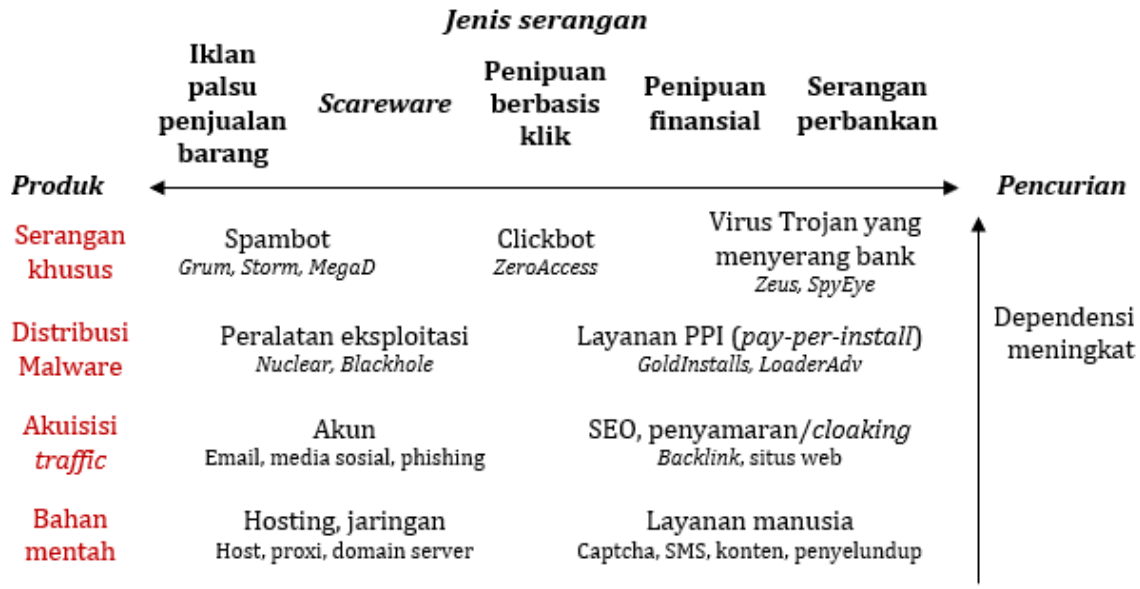
Pendahuluan

Kejahatan yang melibatkan komputer atau jaringan dikategorikan sebagai kejahatan siber (*cybercrime*), dan dilakukan baik dalam skala kecil, di mana pelaku atau korban bersifat perorangan atau kelompok kecil maupun dalam skala besar yang, sebagai contoh, melibatkan jaringan kriminal yang tersebar secara internasional. Seiring dengan berkembangnya teknologi informasi serta *trend* penggunaan platform dan peranti elektronik, *trend* dan jenis kejahatan siber pun berevolusi. Ponsel pintar/*smartphone* kini menjadi piranti utama yang digunakan oleh sebagian besar orang untuk mengakses internet, menggantikan komputer dan laptop, sementara semakin banyak layanan yang berbasis *cloud*. Perkembangan ini memunculkan target-target baru dalam kejahatan

siber; di sisi lain, jenis kejahatan siber baru muncul baik akibat modus operandi pelaku yang berkembang maupun kelemahan akibat miskonfigurasi sistem *cloud* (Anderson et al., 2019).

Kejahatan siber yang semakin canggih perlu difasilitasi oleh berbagai peralatan, pelaku yang menjalankan peran yang berbeda-beda, dan sumber daya lain yang dibutuhkan untuk mengeksekusi setiap tahapan dalam kejahatan ini. Dampaknya, kini muncul pasar underground di mana prinsip-prinsip ekonomi berjalan—terdapat penawaran (*supply*) maupun permintaan (*demand*) atas berbagai komoditas fisik maupun kemampuan atau *skill* yang memang dirancang untuk melakukan tindakan yang meyalahgunakan teknologi melalui misalnya peretasan, pengiriman *malware* atau virus, mengirimkan *traffic* palsu yang menghabiskan sumber daya aplikasi, dan sebagainya (Kirwan & Power, 2013). Pasar gelap infrastruktur ini terdiri dari berbagai peran berdasarkan jenis kejahatan siber yang dilakukan, namun secara umum meliputi penyedia bahan mentah, akuisisi lalu lintas (*traffic*), distribusi *malware*, dan pembawa serangan yang bersifat spesifik. Thomas et al. (2015) memaparkan taksonomi pelaku pasar gelap kejahatan siber sebagai berikut beserta contohnya:

Gambar 1.
Taksonomi kejahatan siber



Terlepas dari struktur ataupun taksonomi yang berperan dalam kejahatan siber tertentu, selalu ada *profit center* (pusat pengumpulan keuntungan) di mana dihasilkan keuntungan yang digunakan dalam tindak kriminal, dan *support center* yang menyediakan berbagai macam sumber daya sumber daya yang diperlukan, baik berupa aplikasi, pengetahuan, atau sumber daya yang bersifat material (Thomas et al., 2015). Pihak-pihak yang terlibat kejahatan siber itu sendiri tidak terbatas pada pelaku dan korban; bisa terdapat pihak-pihak yang tidak menyadari bahwa mereka sedang membantu atau memfasilitasi tindak kejahatan siber, namun tidak secara langsung

dirugikan oleh kejahatan ini. Penelitian ini bertujuan memahami pihak yang terlibat dalam suatu kejahatan siber yang spesifik, serta tindakan penanggulangan yang dapat dilakukan dengan berbagai pendekatan.

Metodologi

Penelitian ini menggunakan satu buah kasus hipotetis yang diadaptasi dari sejumlah serangan siber yang terjadi di dunia nyata. Pendekatan yang digunakan dalam penelitian ini adalah kajian kepustakaan. Pendekatan kajian pustaka dalam penelitian adalah metode yang melibatkan analisis terhadap literatur yang telah ada untuk memahami, mengevaluasi, dan mensintesis pengetahuan yang relevan dengan topik penelitian. Penelitian ini menitikberatkan terkait dengan kejahatan siber dan penanggulangannya, serta literatur lain yang terkait, untuk mengidentifikasi pihak-pihak yang terlibat dalam kasus kejahatan siber dalam kasus hipotetis tersebut. Selanjutnya, dibahas contoh strategi penanggulangan kejahatan siber melalui pendekatan teknis, legal, ekonomis, dan edukasi.

Untuk memahami secara konkrit peran dan interaksi berbagai pihak dalam kejahatan siber, kita dapat mempelajari studi kasus kejahatan siber *phishing* berikut ini: Serangan *DarkHotel* menyasar daerah Asia Timur dan mengincar hotel-hotel tempat diselenggarakannya konferensi di sektor kesehatan yang sedang marak digelar. Serangan ini memperdaya karyawan-karyawan hotel yang kurang waspada atau tidak menyadari tipuan yang dilakukan, dan pada akhirnya membocorkan informasi sensitif tentang tamu-tamu hotel tersebut melalui surat elektronik (email) yang terlihat tidak berbahaya. Serangkaian email yang terlihat resmi dirancang untuk meyakinkan para karyawan hotel tentang keaslian email yang berisi permintaan reservasi. Domain situs web palsu dibuat dengan meniru situs web rumah sakit-rumah sakit ternama untuk meningkatkan legitimasi email *spearphishing* (*phishing* yang mengincar target tertentu) yang dikirim, yang menjelaskan bahwa *file* yang dilampirkan berisi detail kegiatan konferensi yang ingin diselenggarakan dan nama-nama tamu undangannya.

Pelaku akan meluncurkan virus Trojan yang memberikan akses jarak jauh, sebut saja virus PoisonIvy. Virus ini dibuat agak berbeda dengan virus yang sebelumnya pernah dipakai dan sudah terdeteksi oleh aplikasi antivirus. Setelah instalasi, sejumlah modul akan diinstal untuk merekam data kartu kredit tamu dan *travel agency* mitra hotel yang tersimpan di komputer tersebut. Selain itu, modul serangan ini juga menyalin data pribadi semua tamu yang tercatat, termasuk tanggal lahir, alamat email, nomor telepon, dan nomor paspor.

Serangan ini didanai dengan menjual voucher *e-commerce* (misalnya Amazon, AliBaba) dan menjual ulang dengan harga mahal di platform lain seperti e-Bay. Voucher ini dijual ke pembeli di negara berkembang untuk mengurangi risiko penangkapan oleh aparat penegak hukum. Selain itu, para pelaku juga membeli kartu EMV (Europay, Mastercard dan Visa) dengan chip yang dapat diprogram, yang digunakan untuk menarik dana dalam jumlah besar dari rekening korban tanpa harus mengetahui PIN pemilik rekening.

Hasil dan Pembahasan

Dalam kasus di atas, terlihat bahwa tindak kejahatan siber tidak hanya melibatkan pihak pelaku dan korban (yaitu para tamu dan instansi yang datanya dicuri), namun terjadi dengan andil dari karyawan hotel yang bertindak dengan anggapan bahwa email yang merespon adalah email asli, dan secara tidak sengaja membuka *file* lampiran email yang berisi virus dan berujung pada terpasangnya *malware*. Secara rinci, pihak-pihak yang berperan dalam tindak kejahatan siber ini dipaparkan dalam Tabel 2.

Tabel 2. Analisa Peran dalam kejahatan siber *spearphishing*

	Pelaku	Peran	Kemampuan
Para Pelaku Kriminal (satu atau lebih peran dapat dijalankan oleh pihak yang sama)			
Support Center	Dalang	Merencanakan operasi kejahatan siber; membeli domain, *malware*, kartu chip EMV, dan sumber daya lain yang dibutuhkan	Merencanakan keseluruhan operasi kejahatan; menjalin jejaringkriminal dengan pelaku kriminal lain; memperoleh sumber daya yang dibutuhkan
	Pengembang situs website palsu	Membuat kesan legitimasi dan keaslian dalam tindak penipuan	Desain web, terutama untuk berpura-pura menjadi situs website yang resmi
	Pembuat virus Trojan yang berisi *malware* PoisonIvy	Menciptakan *malware* yang menjalankan fungsi yang diinginkan: menembus sistem pertahanankomputer hotel, merekam data kartu kredit, dan menyalin data korban yang tersimpan	
	Administrator server komando dan pengendalian (*command-and-control*/ C&C)	Mengelola data yang diperoleh, menjalankan komando selanjutnya	Manajemen data; menghindari deteksi misalnya dengan terus menerus berpindah domain server
Pihak-pihak yang terlibat tanpa sadar			
Profit Centre	Pegawai hotel yang terperdaya (dapat juga dianggap sebagai korban email palsu)	Membocorkan informasi pribadi para tamu dan instansi mitra dengan mengeklik tautan/*file* lampiran yang berisi muatan Trojan	Mengoperasikan komputer di mana data para korban disimpan, dan/atau mengendalikan data para tamu dan instansi mitra
	Pihak-pihak yang terlibat dalam pendanaan kejahatan siber: penyedia voucher, platform *e-commerce*	Tanpa sepengetahuan mereka memfasilitasi pendanaan kejahatan siber yang mengakibatkan kerugian pada para korban	Mendeteksi pembelian atau penjualan berskala besar yang mencurigakan dalam platform mereka
	Pembeli *voucher* di negara berkembang	Memberikan penghasilan pada para pelaku kejahatan siber tanpa disadari	Memutuskan membeli atau tidak membeli barang yang tersedia dalam platform e-commerce

	Bank	Pihak yang data serta aset nasabahnya dicuri dalam kejahatan siber	Mengimplementasikan verifikasi dua langkah *(two-factor authentication*) untuk otorisasi penarikan dana dalam jumlah yang melebihi jumlah tertentu, atau melebihi sekian persen dari dana yang tersimpan
	Korban		
	Tamu hotel dan instansi mitra yang datanya dicuri	Menjadi insentif bagi para pelaku kriminal untuk melakukan kejahatan siber	Memonitor instansi atau lembaga mana saja yang menyimpan data pribadi mereka

Penanggulangan Kejahatan Siber

Mengingat pelaku kejahatan siber terus berkembang dan memperbaharui virus, *malware*, atau piranti yang digunakan untuk menghindari deteksi, penanggulangan kejahatan siber merupakan persaingan persenjataan (*armrace*) yang tak berkesudahan antara pelaku kriminal dan pihak-pihak yang berupaya melindungi korban potensial serangan kejahatan siber. Pendekatan yang digunakan untuk melawan kejahatan siber bermacam-macam berdasarkan tipe serangan yang dilakukan. Untuk kasus hipotetis di atas, akan dipaparkan satu contoh upaya penanggulangan yang menggunakan pendekatan teknis, legal, ekonomis, dan edukasi.

1. *Penanggulangan dengan pendekatan teknis:* mengimplementasikan *whitelist* (daftar putih) yang terdiri dari situs website resmi para pemaku kebijakan dan instansi-instansi terkait, serta membuat protokol peringatan/pemberitahuan apabila ada orang yang mengakses situs di luar daftar ini

   Whitelist adalah sebuah daftar yang memuat alamat situs, entitas individual, ataupun bentuk akun lain yang dapat dipercaya. Daftar ini berkebalikan dengan *blacklist* atau daftar hitam, yang dalam konteks kejahatan siber merupakan daftar entitas yang diketahui berbahaya dan karenanya diblokir atau tidak boleh diakses. Protokol *whitelist* dalam strategi penanggulangan kasus hipotetis di atas diimplementasikan pada komputer hotel. Sebagaimana diterapkan sebelumnya oleh Li et al. (2014) dalam penelitiannya, setelah *whitelist* dibuat, dapat dipasang *prompt* untuk mengkonfirmasi keaslian situs apabila pegawai hotel akan mengakses situs dengan URL yang mirip (namun tidak sama persis) dengan situs yang ada dalam *whitelist*. Selain itu, dapat juga diterapkan protokol yang melarang pegawai untuk meng-input kata sandi ataupun data lainnya yang spesifik ke dalam website yang ada di luar *whitelist*, sebagaimana diimplementasikan dalam IEPlug dalam peramban Internet Explorer.

   Untuk mengimplentasikan *whitelist* yang efektif, perlu dilakukan pembaharuan terus menerus pada *whitelist* untuk memasukkan *entry* baru bagi pemangku

kepentingan yang baru atau yang mengubah situs resminya. Untuk mengoptimalkan efektivitas penggunaan *whitelist*, pegawai juga perlu dilatih untuk mendeteksi URL yang mencurigakan, menghiraukan tampilan peringatan yang muncul, serta menjalankan protokol yang tepat apabila ancaman terdeteksi oleh sistem. Oleh karena itu, perusahaan perlu memikirkan bagaimana menyusun dan menegakkan protokol seperti ini, misalnya dengan menetapkan rantai komando (*chain of command*) yang jelas atau konsultasi keamanan antar-jabatan sebelum pegawai diberi otoritas untuk mengakses URL tertentu atau meng-input data.

Protokol *whitelist* semata tidak dapat melindungi sistem dari serangan Trojan berisi *malware* atau jenis serangan lain apabila situs web resmi yang masuk *whitelist* telah diserang terlebih dahulu oleh pelaku kejahatan siber, misalnya dengan mengubah tautan ke alamat yang berisi *malware*. Karenanya, sistem pengamanan dari dalam komputer sendiri juga harus kokoh, misalnya dengan memasang aplikasi antivirus yang mutakhir, dan menerapkan filter yang kuat (misalnya dalam aplikasi persuratan elektronik) untuk mendeteksi konten berbahaya atau pesan yang mengindikasikan *phishing*.

2. *Penanggulangan dengan pendekatan legal*: memberkuat kerjasama internasional untuk menegakkan hukum dan regulasi yang berlaku

Perlunya kerjasama internasional yang mengikat secara hukum untuk melawan kejahatan siber timbul dari betapa mudahnya pelaku kejahatan siber untuk melakukan tindak kejahatan melintasi batas-batas negara. Meskipun banyak negara-negara yang telah menyusun undang-undang terkait dengan penipuan dan tindak pidana lain yang dilakukan secara daring, Brenner (2011) menemukan bahwa terdapat perbedaan yang besar antar negara mengenai definisi kejahatan siber, sehingga penyidikan, penangkapan ataupun tindakan hukum lain sulit dilakukan melampaui yurisdiksi suatu negara.

Perundang-undangan dan regulasi perlu diimplementasikan bekerja sama dengan sektor privat yang berpotensi atau rawan untuk mengalami serangan siber (Holt, 2018). Termasuk di dalam kerja sama ini di antaranya adalah pengaturan standar keamanan untuk produsen ponsel dan komputer, serta penerapan sanksi hukum untuk pelanggaran standar keamanan ini. Organisasi yang menyimpan data pribadi konsumen atau kliennya juga harus mematuhi regulasi terkait penyimpanan dan perlindungan data, seperti *Data Protection Act* yang diterapkan di Inggris. Dalam contoh di atas, meskipun hotel di mana terjadi serangan siber dapat dipandang sebagai korban kejahatan siber, kegagalan pihak hotel untuk melindungi data para korban dapat juga dikenai sanksi hukum.

Dengan terus berevolusinya modus operandi pelaku kejahatan siber, bentuk kesepakatan internasional yang diperlukan di bidang keamanan siber juga terus berubah seiring dengan berjalannya waktu. Perkembangan di bidang teknologi informasi dan keamanan siber seharusnya menjadi pertimbangan dalam penetapan standar-standar internasional, yang kemudian disepakati oleh negara-negara (Ilchenko et al., 2019). Pada akhirnya, kesediaan negara-negara untuk menjalin kerja

sama dan untuk patuh pada standar internasional dalam memerangi kejahatan siber bergantung pada kepentingan nasionalnya dalam panggung perpolitikan global, dan penandatanganan persetujuan semacam ini akan ditentukan oleh itikad baik setiap negara untuk berdiskusi dan berkompromi tentang aspirasi mereka.

3. *Penanggulangan dengan pendekatan ekonomis*: menerapkan sanksi pada platform *e-commerce* dan bank yang gagal mendeteksi adanya transaksi tipuan atau yang mencurigakan

Seperti halnya dengan penanggulangan kejahatan siber melalui penyusunan *whitelist*, tindakan penerapan sanksi merupakan upaya preventif, dan bukan dilakukan ketika kejahatan siber sudah terjadi. Hasan et al. (2021) menemukan bahwa instansi perbankan perlu terus mengembangkan penerapan protokol keamanan siber terlepas dari ada-tidaknya serangan siber. Protokol keamanan siber ini perlu dikembangkan untuk memastikan adanya sistem pertahanan yang berfungsi sebelum, pada saat, dan sesudah kejahatan siber dilakukan (Raghavan & Parthiban, 2014).

Dalam perspektif pencegahan kejahatan secara situasional (Clarke, 1995), tindakan penanggulangan ini bekerja dengan mengurangi imbalan/*reward* dan meningkatkan usaha/*effort* yang harus dilakukan pelaku kriminal untuk memonetisasi data pribadi yang mereka peroleh. Dengan adanya ancaman sanksi finansial apabila bank/platform *e-commerce* gagal mendeteksi transaksi mencurigakan, ketika suatu instansi ini mendeteksi ketidakwajaran dalam transaksi yang dilakukan oleh suatu akun, mereka dapat memblokir akses ke aset yang dimiliki oleh akun tersebut, dan mensyaratkan protokol otentifikasi tertentu untuk dilakukan terlebih dahulu sebelum pengguna layanandapat mengakses akun tersebut. Apabila proses otentifikasi perlu menggunakan data yang tidak dimiliki oleh pelaku kriminal (misalnya nama ibu, yang kecil kemungkinannya untuk disimpan datanya di *database* hotel), pelaku kriminal tidak akan dapat secara optimal meraup keuntungan dari rekening bank yang telah dibobol. Selain itu, pelaku kriminal mungkin akan harus beralih ke bank-bank yang lebih kecil yang menerapkan protokol keamanan yang lebih longgar.

Strategi penanggulangan ini, meskipun demikian, dapat diakali oleh para pelaku dengan melakukan monetisasi dengan cara yang tidak terdeteksi oleh protokol keamanan yang diterapkan untuk transaksi mencurigakan, misalnya dengan melakukan beberapa transaksi terpisah dengan jarak waktu tertentu, atau dengan menjual barang-barang untuk pendanaan menggunakan lebih dari satu akun *e-commerce*. Kekurangan lain metode penanggulangan ini adalah bahwa, meskipun strategi ini dapat mengurangi profitabilitas kejahatan siber, kebijakan ini juga akan berdampak pada nasabah yang memang perlu memindahkan dana dalam jumlah besar atau melakukan tindakan yang dapat dianggap mencurigakan oleh pihak bank. Protokol otentifikasi yang menyulitkan dalam proses transaksi mungkin akan mendapatkan sambutan negatif dari nasabah. Namun, manfaat di bidang keamanan dari strategi ini bisa dibilang jauh lebih besar daripada kerugiannya. Bank dan

platform *e-commerce* juga dapat menerapkan kebijakan ini dengan disertai informasi yang dapat membantu nasabah memahami mengapa protokol keamanan perlu diterapkan.

4. *Penanggulangan dengan pendekatan edukasi:* Meningkatkan kesadaran dan wawasan dalam mendeteksi email tipuan dan indikasi *phishing* melalui pelatihan yang bersifat periodik atau rutin

Pendekatan ini merupakan elemen yang krusial dalam upaya pencegahan kejahatan siber (Marshall, 2008). Pelaku kejahatan siber malakukan *social engineering* atau rekayasa sosial untuk memanipulasi manusia agar melakukan kesalahan yang berujung pada serangan siber (misalnya mengeklik tautan palsu atau membuka *file* berbahaya). Teknik rekayasa ini sangat diperlukan oleh para kriminal agar *malware* mereka sukses menginfiltrasi sistem tertentu, karena biasanya tetap diperlukan proses penginputan dalam bentuk tertentu oleh pengguna komputer untuk dapat menyebarluaskan infeksi yang menyerang (Furnall, 2010). Serangan *spearphishing* dirancang khusus untuk mengincar korban dengan cara yang terkait langsung dengan minatatau kepentingan mereka. Berdasarkan temuan Caputo et al. (2014), hal ini menjelaskan mengapa pegawai hotel dalam kasus hipotetis di atas menjadi korban tipu daya serangan ini: email palsu yang digunakan oleh para pelaku berisi informasi yang relevan dan wajar bagi pegawai (permintaan *booking* untuk acara konferensi), dan karenanya membuat para pegawai merasa bahwa mereka perlu segera merespon email tersebut.

Nield (2017) menekankan pentingnya mengenali situs web yang sekiranya dirancang untuk menyerupai situs resmi, baik dari segi tampilan ataupun alamat situs. Kebiasaan lain yang dapat dibentuk melalui edukasi adalah tidak mengeklik langsung tautan yang dimuat di dalam email, melainkan mengetik secara manual alamat situs (Ghazi-Tehrani & Pontell, 2021). Namun, pelatihan keamanan siber yang hanya dilakukan satu kali tidak akan cukup untuk mengurangi risiko serangan *phishing* dalam jangka panjang. Pelatihan yang berkelanjutan diperlukan seiring dengan modus operandi serangan siber yang makin canggih. Dampaknya, strategi penanggulangan ini memerlukan divisi pengembangan SDM yang mampu memahami perkembangan serangan siber, merancang protokol edukasi yang diperlukan, serta memiliki sumber daya yang cukup untuk melatih segenap pegawai yang kinerjanya berhubungan dengan internet. Di samping itu, sejauh apa seorang pegawai perlu dididik akan bergantung pada seberapa familiar mereka selama ini dengan internet dan pengoperasian komputer. Contoh konkrit ketergantungan ini adalah temuan Lin et al. (2019) bahwa individu yang berusia lanjut lebih rentan menjadi korban *spearphishing* daripada orang muda.

Tidak hanya pada operator komputer atau piranti yang digunakan dalam serangan kejahatan siber, edukasi juga perlu diberikan kepada masyarakat umum yang berpotensi untuk menjadi korban kejahatan siber. Pengguna internet, menurut Kirlappos & Sasse (2012), perlu mewaspadai tawaran diskon barang-barang bermerk yang dirasa mencurigakan, atau kiriman pesan yang berisi ‘pemberitahuan

darurat' yang menyuruh pengguna untuk melakukan tindakan segera. Di sisi lain, mengingat peramban/*browser* maupun aplikasi persuratan elektronik masa kini pada umumnya sudah menerapkan berbagai protokol keamanan, perlu juga diberikan edukasi mengenai bagaimana seseorang harus merespon ketika muncul tanda-tanda peringatan seperti pemberitahuan sertifikat laman situs web yang invalid, atau dugaan email berisi *Spam*.

Di antara empat contoh strategi penanggulangan yang telah dibahas di atas, edukasi dalam rangka peningkatan kewaspadaan dan kesadaran tentang keamanan merupakan strategi yang dapat secara langsung diterapkan pada orang-orang yang berwenang mengelola sistem komunikasi daring dan *database* suatu organisasi. Peran krusial pendekatan edukasi dapat disimpulkan dari besarnya peran perilaku *user* baik untuk memfasilitasi maupun mencegah berbagai jenis serangan siber, dan berbagai cara pelaku kejahatan siber mengeksploitasi kelemahan dan kelalaian manusia dalam operasinya. Secara khusus, pelatihan yang bertujuan meningkatkan kewaspadaan sangat penting dalam mencegah *spearphishing* seperti kasus hipotetis di atas, karena pelaku *spearphishing* kemungkinan besar sudah menggunakan sumber daya yang dimilikinya untuk mengenali sasaran serangan terlebih dahulu, dan merancang email dan situs yang relatif meyakinkan.

Batasan dan Serangan Balik

Meskipun menciptakan *whitelist* dapat membantu mengurangi risiko bocornya data ke pihak-pihak yang tidak diizinkan, strategi penanggulangan ini tidak akan efektif apabila para user yangmengoperasikan komputer tidak dilatih dengan baik untuk merespon dengan tepat notifikasi peringatan keamanan serta untuk mematuhi protokol keamanan yang telah ditetapkan. Bahkan apabila suatu organisasi telah menjalankan pelatihan yang optimal untuk mencegah berhasilnya serangan *phishing*, dan hasil pelatihan ini telah diimplementasikan secara sempurna di seluruh lini perusahaan, pelaku kejahatan siber tetap dapat menerobos tindakan penanggulangan. Mengacu padakasus hipotetis yang dibahas sebelumnya, pelaku kejahatan siber dapat menyerang balik misalnya dengan dua metode berikut:

1. *Meretas situs website resmi yang pemangku kepentingan (stakeholder)*

   Apabila situs web atau email resmi suatu organisasi sudah diretas, hotel tetap akan mengalami serangan *malware* meskipun yang diakses adalah situs resmi. Dari sisi pemilik situs web yang diretas, akan butuh waktu dan tenaga bagi organisasi tersebut untuk memberi tahu semua mitra dan pemangku kepentingan tentang pelanggaran keamanan ini. Dalam waktu yang dibutuhkan ini, pelaku kejahatan bisa saja mengirim email yang tampak asli dari alamat email yang sudah ada dalam *whitelist*, namun sesungguhnya memuat konten atau tautan yang berbahaya.
2. *Mengembangkan zero-day malware*

   Zero-day malware adalah *malware* dengan struktur dan karakteristik yang sama sekali baru dan belum pernah digunakan atau dideteksi sebelumnya. Kiriman atau lampiran yang memuat *zero-day malware* tidak akan terdeteksi oleh aplikasi

antivirus yang beroperasi berdasarkan data *signature* virus (Gandotra et al., 2016). Karenanya, serangan *zero-day malware* tidak akan men-*trigger* peringatan keamanan yang sudah diajarkan pada para pegawai bagaimana cara meresponnya. Untuk mendeteksi *zero-day malware*, metode deteksi yang lebih canggih seperti *transferred deep-convolutional generative adversarial network* (Kim et al., 2018) perlu diimplementasikan, sehingga memerlukan sumber daya yang lebih mahal dan strategi implementasi yang lebih rumit.

Sementara itu, dua strategi penanggulangan kejahatan siber, yaitu yang menggunakan pendekatan ekonomis dan legal, diimplementasikan pada tingkat nasional/internasional, dan secara umum kurang dapat diandalkan oleh individu atau organisasi yang membutuhkan perlindungan dari serangan siber yang bersifat segera atau *real-time*. Sanksi ekonomi dan kerjasama internasional dalam bidang hukum juga berfokus pada konsekuensi kejahatan siber, bukan pada mitigasi dan pencegahan dilakukannya tindak kejahatan siber itu sendiri. Selain itu, modus operandi serangan siber terus berubah dan berkembang, sehingga bisa saja mengeksploitasi kelemahan dalam sistem keamanan siber yang sebelumnya belum diatur dalam perundang-undangan yang ada. Jika pelaku kejahatan siber melakukan hal ini, regulasi dan peraturan hukum yang ada dapat menjadi kurang berguna untuk menghadapi serangan yang lebih mutakhir.

Kesimpulan

Serangan siber melibatkan berbagai pihak, baik pelaku yang secara sadar melakukan tindak kejahatan siber, maupun pihak-pihak yang tanpa sadar ikut memfasilitasi keberhasilan serangan siber melalui tipu daya para pelaku. Kejahatan siber yang semakin berkembang memunculkan pasar gelap yang memperjualbelilkan sumber daya yang dibutuhkan untuk menjalankan kejahatan siber, baik yang berupa perangkat keras/perangkat lunak, maupun *skill* tertentu yang berguna.

Peran perilaku user dalam keberhasilan serangan siber adalah krusial, sehingga penanggulangan yang menggunakan pendekatan edukasi menjadi sangat penting untuk diberikan pada mereka yang menggunakan internet dalam setting perusahaan maupun privat. Pendekatan teknis juga perlu diterapkan, misalnya dengan membatasi akses ke situs-situs yang tidak masuk dalam *whitelist* dan menerapkan protokol keamanan berupa peringatan keamanan dan verifikasi dua langkah/*two-factor authentification*. Selain itu, penanggulangan kejahatan siber di tingkat nasional, regional, atau internasional juga dapat diterapkan dengan membuat kebijakan serta menjalin kerja sama yang menyasar atau mengurangi insentif dilakukannya kejahatan siber. Pada akhirnya, mitigasi serta penanggulangan kejahatan siber memiliki keterbatasan dan harus terus berkembang, mengingat pelaku kriminal kejahatan siber terus berlomba-lomba dengan pengembangan perlindungan siber untuk unggul dalam dalam ‘perang’ kejahatan siber.

Implikasi

Studi lebih lanjut mengenai kejahatan siber dapat dilakukan berangkat dari analisa peran yang telah dilakukan, dengan fokus misalnya pada pelaku yang spesifik serta bagaimana peran pelaku tersebut dalam kejahatan siber dapat dihalangi. Penyusunan rencana penanggulangan kejahatan siber juga dapat dikembangkan dengan dasar teoretis yang beragam, seperti yang sebelumnya dilakukan oleh Djanggih & Qamar (2018) menggunakan teori-teori kriminologi. Pengembangan studi kejahatan siber juga perlu terus dilakukan seiring dengan munculnya jenis-jenis kejahatan siber baru.

Referensi

Anderson, R., Barton, C., Böhme, R., Clayton, R., Gañán, C., Grasso, T., Levi, M., Moore, T., & Vasek, M. (2019). Measuring the Changing Cost of Cybercrime. *The 2019 Workshop on the Economics of Information Security*

Brenner, S. W. (2011). Defining cybercrime: A review of federal and state law. *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-Related Crime*, 15–104.

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going Spear Phishing: Exploring Embedded Training and Awareness. *IEEE Security & Privacy*, *12*(1), 28–38. https://doi.org/10.1109/MSP.2013.106

Clarke, R. V. (1995). Situational Crime Prevention. *Crime and Justice*, *19*, 91–150. https://doi.org/10.1086/449230

Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta: Research Law Journal*, *13*(1), 10–23. https://doi.org/10.15294/pandecta.v13i1.14020

Furnall, S. (2010). Hackers, viruses, and malicious software. In *Handbook of Internet Crime* (pp. 173–193). Willan Publishing.

Gandotra, E., Bansal, D., & Sofat, S. (2016). Zero-day malware detection. *2016 Sixth International Symposium on Embedded Computing and System Design (ISED)*, 171–175. https://doi.org/10.1109/ISED.2016.7977076

Ghazi-Tehrani, A. K., & Pontell, H. N. (2021). Phishing Evolves: Analyzing the Enduring Cybercrime. *Victims & Offenders*, *16*(3), 316–342. https://doi.org/10.1080/15564886.2020.1829224

Hasan, M. F., Al-Ramadan, N. S., & Professor, A. (2021). Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case. In *Social Science and Humanities Journal* (Vol. 05).

Holt, T. J. (2018). Regulating Cybercrime through Law Enforcement and Industry Mechanisms. *The ANNALS of the American Academy of Political and Social Science*, *679*(1), 140–157. https://doi.org/10.1177/0002716218783679

Ilchenko, O., Chumak, V., Kuzmenko, S., Shelukhin, O., & Dobrovinskyi, A. (2019). Fishing as a cybercrime in the Internet banking system: economic and legal aspects. *Journal of Legal, Ethical and Regulatory Issues*, *22*, 1.

Kim, J.-Y., Bu, S.-J., & Cho, S.-B. (2018). Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders. *Information Sciences*, *460–461*, 83–102. https://doi.org/10.1016/j.ins.2018.04.092

Kirlappos, I., & Sasse, M. A. (2012). Security Education against Phishing: A Modest Proposal for a Major Rethink. *IEEE Security & Privacy Magazine*, *10*(2), 24–32. https://doi.org/10.1109/MSP.2011.179

Kirwan, G., & Power, A. (2013). *Cybercrime: The Psychology of Online Offenders*. Cambridge University Press. https://books.google.co.id/books?id=U35HVJyADlEC

Li, L., Berki, E., Helenius, M., & Ovaska, S. (2014). Towards a contingency approach with whitelist- and blacklist-based anti-phishing applications: what do usability tests indicate? *Behaviour & Information Technology*, *33*(11), 1136–1147. https://doi.org/10.1080/0144929X.2013.875221

Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). Susceptibility to Spear-Phishing Emails. *ACM Transactions on Computer-Human Interaction*, *26*(5), 1–28. https://doi.org/10.1145/3336141

Marshall, A. S. P. (2008). Identity and identity theft. In R. Bryant (Ed.), *Investigating Digital Crime* (pp. 179–193). Wiley.

Nield, D. (2017, January). *4 Computer Security Threats You Might Not Be Protecting Against*. Https://Gizmodo.Com/4-Computer-Security-Threats-You-Might-Not-Be-Protecting-1791226612.

Raghavan, A. R., & Parthiban, L. (2014). The effect of cybercrime on a Bank's finances. *International Journal of Current Research & Academic Review*, *2*(2), 173–178.

Thomas, K., Huang, D., Wang, D., Bursztein, E., Grier, C., Holt, T. J., Kruegel, C., McCoy, D., Savage, S., & Vigna, G. (2015). Framing dependencies introduced by underground commoditization. *Workshop on the Economics of Information Security.*