H@CK3R's SECRETS for CEOs

"Rasa aman berbahaya.
Rasa aman membuat kita lengah."

Gildas Arvin Deograt Lumy

H@CK3R's SECRETS for CEOs

¨Rasa aman berbahaya.
Rasa aman membuat kita lengah.¨

Untuk
Peserta Konferensi Auditor Indonesia 2023

Gildas

Sanksi Pelanggaran Pasal 72
Undang-undangNomor 19 Tahun 2002
Perubahan atas Undang-undang Nomor 7 Tahun 1987
Perubahan atas Undang-undang Nomor 6 Tahun 1982
Tentang Hak Cipta

1. Barang siapa dengan sengaja dan tanpa hak melakukan perbuatan sebagaimana dimaksud dalam Pasal 2 ayat (1) atau Pasal 49 ayat (1) dan ayat (2) dipidana dengan pidana penjara masing-masing paling singkat 1 (satu) bulan dan /atau denda paling sediki Rp. 1.000.000,00 (satu juta rupiah), atau pidana penjara paling lama 7 (tujuh) tahun dan /atau denda paling banyak Rp. 5.000.000.000,00 (lima miliar rupiah).

2. Barang siapa dengan sengaja menyiarkan, memamerkan, mengedarkan atau menjual kepada umum suatu ciptaan atau barang hasil pelanggaran Hak Cipta atau Hak Terkait sebagaimana dimaksud dalam ayat (1), dipidana dengan pidana penjara paling lama 5 (lima) tahun dan /atau denda paling banyak Rp. 500.000.000,00 (lima ratus juta rupiah).

Hanya untuk pemimpin yang benar-benar peduli
pada negara dan organisasinya:

H@CK3R's SECRETS for CEOs

"Rasa aman berbahaya.
Rasa aman membuat kita lengah."

Gildas Arvin Deograt Lumy

2016

BORNRICH PUBLISHING

H@CK3R'S SECRETS for CEOs

Gildas Arvin Deograt Lumy

Editor: Tim Bornrich
Desain Cover: Gracianadei
Tata Letak: Andung Yuliyanto

Diterbitkan Pertama Kali oleh :

Bornrich Publishing
Verbena Blok V-10/9
Citra Raya – Tangerang Telp: 021-59400515

Cetakan Pertama: Agustus 2016

Halaman: xxxviii + 154
Ukuran Buku: 14 x 21 cm

ISBN: 978-979-1140-06-5

ENDORSEMENT

"Buku yang harus dibaca oleh para pengambil keputusan, baik swasta maupun pemerintah, karena memberi pemahaman mendalam akan berbagai ilusi keamanan informasi dan siber yang selama ini menjadi misteri bagi para pengambil keputusan. Pengetahuan dan pengalaman internasional selama 20 tahun yang dimiliki Gildas sebagai praktisi keamanan informasi dan pertahanan siber yang sebagian dituangkan dalam buku ini sangat penting untuk menjaga kelangsungan hidup dan daya saing perusahaan, serta kedaulatan bangsa dan ketahanan nasional."

Marsekal Muda TNI Agus Ruchyan Barnas

Deputi Bidang Koordinasi Komunikasi, Informasi, dan Aparatur Kementerian Koodinator Bidang Politik Hukum dan Keamanan; Ketua Desk Cyberspace Nasional

"Buku ini ditulis oleh seorang praktisi TI yang sudah senior di bidangnya. Buku yang muatannya *complex* dan berat ini telah berhasil dibahas dengan bahasa yang sederhana dan contoh-contoh lugas oleh penulisnya. Sehingga, pembacanya bisa memahami dengan baik tentang pentingnya memiliki tingkat kewaspadaan dalam menjalai kenyamanan di dunia maya. Saya berpendapat bahwa buku ini merupakan sumbangsih yang substansial bagi ilmu pengetahuan dan juga bagi dunia praktisi sekaligus. Dengan terbitnya buku ini kita semua, para pembaca, diajak untuk bisa paham tentang rahasia keamanan *cyber* dan Teknologi Informasi."

Agus Santoso, SH,LLM

Wakil Kepala Pelaporan dan Analisis Transaksi Keuangan (PPATK)

"Di era digital yang mana hampir segala sesuatu terkoneksi, tanpa kita sadari bahwa *there is a price to pay for convenience*: yaitu *security*. Buku ini memberikan gambaran sisi gelap dan risiko dunia yang serba terkoneksi. Semua data kita sebenarnya berisiko diakses siapa pun, dan inilah kenyataan baru yang perlu kita sadari."

Alexander Rusli, Ph.D

President Director & CEO Indosat Ooredoo

"Teknologi informasi telah menimbulkan revolusi dalam kehidupan manusia. Namun, banyak yang tidak menyadari efek negatifnya bila tidak cerdas dan hati-hati dalam memanfaatkannya. Berinteraksi di dunia maya berlaku etika, norma, dan aturan yang harus dipahami agar tidak menjadi korban, atau bahkan justru menjadi pelaku kejahatan *cyber* itu sendiri. Buku ini sangat menarik karena sarat dengan informasi tentang *cyber space*, internet, dan *cyber crime* serta bagaimana memanfaatkannya secara aman. Ditulis oleh Gildas yang memang memiliki pengalaman empirik dan pengetahuan, serta landasan teori yang tidak perlu diragukan lagi. Saya ucapkan selamat dan apresiasi atas diterbitkannya buku ini sehingga dapat menambah khazanah pengetahuan tentang dunia maya dengan berbagai dinamika yang berkembang saat ini dan di masa datang."

Inspektur Jendral Polisi Drs. Arief Sulistyanto, M.Si
Staf Ahli Managemen Kapolri,
Mantan Direktur Tindak Pidana Ekonomi Khusus, Bareskrim POLRI

"Sebuah buku yang sarat dengan hal-hal penting dan esensial terkait keamanan informasi ditulis oleh penulis yang kaya dengan pengalaman

dan diakui karya nyata dan kontribusinya dalam dunia keamanan informasi. Buku ini merupakan buku yang perlu dibaca oleh semua pihak dalam organisasi mulai dari manajemen puncak sampai ke pegawai biasa. Karena, manajemen keamanan informasi harus menjadi perhatian seluruh lapisan dalam organisasi."

Dr-Ing Budi Ibrahim

Tenaga Ahli Kepala SKK Migas Bidang Teknologi Informasi , Tenaga Ahli Teknologi Informasi Kementrian ESDM

"Berbeda dengan umumnya buku yang membahas keamanan informasi dan *cyber* secara rumit. Buku ini sangat menarik untuk dibaca, relatif ringan, ringkas, dan cukup komprehensif dalam menampilkan pokok-pokok pemikiran yang perlu diperhatikan oleh setiap pimpinan suatu organisasi. Penulis berhasil menampilkan ulasan soal keamanan informasi dengan pendekataan yang *out-of-the-box*. Selamat Pak Gildas, semoga bermanfaat dan mendorong tumbuhnya kesadaran kemananan berinformasi dan berkomunikasi via *cyber*."

Dr. Edmon Makarim, SKom, SH, LLM.

Dosen Hukum Telematika FHUI,

Ketua Lembaga Kajian Hukum Teknologi FHUI

"Buku yang sangat menarik! Gildas menuliskan buku ini dengan gaya bercerita, sehingga mudah bagi pembaca untuk memikirkan kembali dan memahami pentingnya menerapkan keamanan informasi sebagai rantai *end-to-end protection*. Sesuai judulnya, sangat cocok dibaca kalangan CEO karena menggugah pemikiran bahwa *people in the process* adalah faktor sangat penting. Di sinilah peran CEO sangat dibutuhkan dalam rantai pengamanan informasi tersebut."

Fandhy H. Siregar MKom, CISSP, CISA, CIA, CISM, CRMA, CEH, Cobit5

Praktisi dan Pengajar Audit Keamanan Informasi

"Tidak banyak pengambil keputusan yang memahami risiko atas suatu keamanan informasi. Ketidakpahaman ini dapat berakibat fatal bagi organisasinya atau justru menimbulkan sikap paranoid. Menggambarkan aspek keamanan informasi secara komprehensif dalam bahasa pengambil keputusan memerlukan upaya lebih agar tidak terjebak dalam bahasa teknis yang jauh dari pemahaman para pengambil keputusan. Sebagai seorang konsultan di bidang keamanan informasi, penulis tentunya memahami betul kesulitan

berkomunikasi dengan para pengambil keputusan, termasuk saya. Oleh karena itu, buku yang mencoba memberi gambaran aspek keamanan informasi dengan tanpa mendiskusikan peristilahan teknis yang sering membuat sakit kepala semoga bermanfaat membangun pemahaman untuk mengurangi risiko dalam pengambilan keputusan hari ini."

Ikak G. Patriastomo

Deputi Hukum dan Penyelesaian Sanggah dan Mantan Direktur e-Procurement, LKPP.,

Ketua Umum Ikatan Ahli Pengadaan Indonesia

"Dedikasi Gildas pada IT Security perlu diapresiasi. Pengalaman dan perjalanan kariernya membuat dia menjadi seorang praktisi dan juga mentor yang sangat paham atas apa yang dia lakukan. Saya sangat bangga dengan keahlian dan dedikasinya dalam perkembangan IT security. Gaya bicara Gildas yang santai dan lugas membuat sesi *sharing* semakin menarik dan mendorong kita untuk dapat berbuat lebih di era kemajuan IT saat ini. Kepedulian dan profesionalisme dalam bidangnya harus dicontoh oleh ahli-ahli IT lainnya."

Prof. DR. Ilya Avianti, S.E., M.Si., Ak. CPA,

Ketua Dewan Audit/Anggota Dewan Komisioner OJK

"Pak Gildas Deograt adalah segelintir orang di Indonesia yang konsisten berkiprah dalam dunia *networking* khususnya *nework security* selama belasan tahun terakhir. Beliau aktif di berbagai forum/komunitas baik badan tingkat nasional maupun internasional. Sangat menarik membaca buku berjudul *H@ck3r's Secrets for CEOs*. Buku ini merupakan buku yang ditujukan untuk para eksekutif/pengambil keputusan yang membahas lebih banyak pada tataran strategi maupun kebijakan. Pembahasan mulai dari dampak aktivitas *hacker* ditinjau dari berbagai sisi untuk dunia bisnis, nasional, negara, dan bangsa. *Profiling* dari *hacker* itu sendiri, maupun nilai/*value* dari informasi dan data. Berbagai *tip*/strategi bagi para eksekutif dibahas, mulai dari ilusi keamanan, kesalahan, kebingunan, bahkan keracunan dalam menentukan aspek keamanan informasi. Kemudian dibahas pula penilaian terhadap tes penetrasi hingga mendapatkan pentester yang dapat dipercaya serta manajemen risiko. Gaya bahasanya yang sederhana membuat buku ini mudah dimengerti. Buku ini sangat bermanfaat bagi mereka yang berada pada tingkatan manajemen/pimpinan yang ingin melihat keamanan dari sisi strategi maupun kebijakan. Semoga buku ini dapat memberikan manfaat bagi pertahanan di Republik Indonesia."

Onno W. Purbo, Ph.D.,

Penulis Buku

"Di tengah langkanya referensi buku-buku berbahasa Indonesia yang menulis tentang IT Security, buku ini bagaikan air di padang pasir yang menyegarkan dan diharapkan mampu menyadarkan pentingnya pengamanan terhadap suatu sistem elektronik. Yang mana tidak hanya didukung dengan peralatan yang modern dan *reliable*, namun juga perlu didukung dengan sumber daya manusia yang mumpuni, serta *standard operation procedure* yang harus ditaati oleh seluruh personel yang bertugas di dalam organisasi. Kunci yang perlu disadari dan dipahami dalam penanggulangan *cyber crime* adalah perlunya *sharing* informasi dan kerjasama yang melibatkan pemerintah, akademisi, *private and public sector*, dan tentunya sikap kooperatif dari pihak korban yang sistem elektroniknya diserang. Saya mengucapkan selamat kepada Gildas Deograt Lumy atas terbitnya buku yang sangat perlu dibaca ini. Semoga buku ini dapat membangkitkan rasa peduli akan pentingnya pengamanan data elektronik bagi seluruh pimpinan organisasi, baik itu organisasi pemerintah, TNI, Polri, maupun perusahaan-perusahaan swasta yang mengandalkan sistem elektronik guna menunjang pekerjaan yang lebih efektif dan efisien."

Komisari BesarPolisi Rachmad Wibowo

Kasubdit IT & Cybercrime, Direktorat Tindak Pidana Ekonomi dan Khusus, Bareskrim POLRI

"Buku ini sungguh luar biasa! Karena secara cerdas dan lugas membahas isu keamanan internet yang kompleks dengan bahasa yang mudah. Para eksekutif dan pimpinan wajib membaca buku ini agar dapat membangun sistem keamanan yang efektif."

Prof. Richardus Eko Indrajit

Guru Besar Teknologi informasi, Institut Perbanas

"Buku ini merupakan bacaan wajib bagi seluruh petinggi perusahaan, petinggi organisasi dan seluruh guru, dosen, mahasiswa, pejabat kementrian dan pejabat lembaga, penegak hukum-keadilan serta anggota parlemen Indonesia pada era siber sekarang. Buku ini menjelaskan secara mudah dan gamblang bahwa informasi yang tidak dikendalikan sesuai risiko dan dampak (keamanan informasi) akan berdampak buruk pada keselamatan nyawa, hukum, keuangan, bisnis, pendanaan teroris, kedaulatan nasional, pertahanan negara, dan masa depan bangsa Indonesia. Buku ini akan mengubah cara pandang (*mind-set*) jika Anda peduli pada informasi yang sekarang 'bukan lagi hanya Tuhan yang tahu'. Jangan lagi ada pendapat bahwa keamanan informasi dan keamanan siber adalah semata-mata tanggung jawab orang TI (Teknologi Informasi).

Informasi adalah tanggung jawab ANDA, begitu pula Keamanan Informasi yang di dalamnya ada Keamanan Siber. Cara pandang manusia Indonesia terhadap informasi, risiko, ancaman, pengancam, penanganan risiko, dan kendali harus diperbaiki agar Negara Kesatuan Republik Indonesia dapat *survive* dalam era siber."

Sarwono Sutikno, Dr. Eng., CISA, CISSP, CISM, CSX-F
Cybersecurity Nexus Liaison ISACA Indonesia
Dosen Sekolah Teknik Elektro dan Informatika ITB
Asesor LS SMKI SNI ISO/IEC 27001

"Dengan pengetahuan, pengalaman, dan dedikasi di bidang keamanan informasi, Gildas mampu membawa kita para pengambil keputusan dengan mudah dan *enjoy* memahami bagaimana sesungguhnya memelihara rasa aman yang tidak membuat kita lengah dan tetap terus waspada di dalam dinamika keamanan siber yang kita hadapi sehari-hari, serta tetap peduli pada kelangsungan hidup bernegara dan berorganisasi. Dengan membaca buku ini, kita bisa mempelajari intisari pemikiran dan berbagai hal yang harus dipahami serta dilakukan dengan cara yang benar dan baik, khususnya dalam menentukan strategi keamanan siber dan keamanan

informasi. Semua demi kepentingan para pengambil keputusan dan kepentingan masa depan bangsa dan negara Indonesia tercinta."

Surdiyanto Suryodarmodjo

CEO Asia Pacific Commodity Exchange

Mantan Direktur Utama Indonesia Derivatives Clearing House

Immediate Past President ISACA Indonesia

UCAPAN TERIMA KASIH

Terima kasih kepada Tuhan Yesus Kristus yang telah mengajarkan kami berdoa:

Bapa kami yang di surga, dikuduskanlah nama-Mu, datanglah Kerajaan-Mu, jadilah kehendak-Mu di bumi seperti di surga.

Berikanlah kami pada hari ini makanan kami yang secukupnya dan ampunilah kami akan kesalahan kami, seperti kami juga mengampuni orang yang bersalah kepada kami; dan janganlah membawa kami ke

dalam pencobaan, tetapi lepaskanlah kami daripada yang jahat.

Karena Engkaulah yang empunya Kerajaan dan kuasa dan kemuliaan sampai selama-lamanya.

Amin.

Untuk yang tercinta almarhum Papa Solagratia S. Lumy, Mama A. Frieda Tumiwa, almarhum istriku Dede, istriku Liza, keempat anakku Gail, Glad, Grant, dan Gav, serta negaraku Republik Indonesia.

Hanya untuk pemimpin
yang benar-benar peduli
pada negara dan organisasinya

DAFTAR ISI

BAB 7 ILUSI SITUS WEB TIDAK BUTUH PENGAMANAN YANG LAYAK

BAB 8 ILUSI TES PENETRASI

BAB 9 MANAJEMEN RISIKO YANG MENYESATKAN

PENDAHULUAN

“SEJAK PULUHAN TAHUN LALU, NEGARA-NEGARA MAJU PAHAM BAHWA SIBER DAN INFORMASI ADALAH SEBUAH KEKUATAN DAHSYAT.”

"This world—cyberspace—is a world that we depend on every single day... [it] has made us more interconnected than at any time in human history."

-Barack Obama-

Negara-negara maju paham bahwa informasi dan siber adalah sebuah kekuatan dahsyat sejak puluhan tahun yang lalu. Pemerintah negara-negara maju mendorong dan memfasilitasi perkembangan teknologi informasi dan dengan serius mengambil langkah strategis hingga 20 tahun ke depan. Berbagai kebijakan strategis juga dibuat untuk melindungi agar teknologi yang dimiliki tidak menjadi bumerang.

Kekuatan ekonomi digital adalah energi yang luar biasa untuk memajukan bangsa. Namun, jika tidak dikendalikan dengan bijak, sebuah bangsa tanpa sadar akan terjebak dalam kekuatan genggaman ekonomi digital yang berujung pada hilangnya kedaulatan. Banyak pemimpin negara berkembang, yang tidak memiliki kemandirian teknologi, menggantungkan masa depan bangsa dan negaranya pada teknologi dan layanan siber negara lain. Mulai dari pertahanan, anti-terorisme, *e-dagang*, media sosial, transaksi keuangan, telekomunikasi, bahkan akses Internet gratis. Tidakah kita menyadari bahwa tidak ada yang gratis di dunia ini? Kita hanya tidak sadar, kapan dan siapa yang membayar.

Berapa banyak orang yang sadar bahwa kita, perusahaan kita, bahkan negara kita yang terlihat secara fisik, pada hakikatnya hanyalah informasi. Berapa banyak pimpinan perusahaan dan negara yang mengambil keputusan strategis terkait dunia maya, tanpa menyadari dampak jangka pendek maupun jangka panjangnya? Apakah pernah terpikirkan oleh Anda, besarnya ketergantungan masyarakat pada layanan Internet yang tidak patuh pada hukum negara, pada akhirnya akan menghilangkan kedaulatan bangsa di dunia maya? Bagaimana dengan serangan siber terhadap keberlangsungan layanan infrastruktur kritis nasional?

Sebagai seorang pemimpin, apakah pernah terpikirkan oleh Anda, bagaimana layanan Internet seperti Google dan Facebook dapat digunakan untuk mengubah peta politik di saat yang tepat? Google dan Facebook memiliki algoritme untuk mengubah prioritas informasi yang akan ditampilkan. Sehingga, sebagai contoh, ketika pengguna Google dan Facebook mencari seorang kandidat pimpinan pemerintahan yang tidak diinginkan oleh mereka, maka akan selalu muncul berita-berita negatif tentang kandidat tersebut terlebih dahulu. Google dan Facebook juga dapat mem-*filter* informasi-informasi positif tentang kandidat tersebut.

Masyarakat yang tidak berpikir kritis terhadap informasi yang beredar, kualitas dan kwantitas pendidikan yang relatif rendah menjadikan perang informasi (penyebaran kebencian, kampanye hitam, fitnah, pembelokan opini, pengrusakan ideologi, dll) semakin mudah dilakukan dengan semakin luasnya akses Internet hingga ke wilayah terpencil.

Sadarkah Anda, pembiaran kejahatan siber yang selama ini dilakukan banyak pihak, baik swasta ataupun pemerintah, menjadikan dunia maya sebagai sumber pendanaan tindak pidana pendanaan terorisme tanpa batas? Tahukah Anda

banyak perusahaan harus menanggung kerugian besar, bahkan ada yang harus tutup, karena menjadi korban kejahatan siber walaupun mereka sudah mengeluarkan biaya puluhan miliar rupiah untuk membeli teknologi keamanan?

***

Hampir semua teman pengambil keputusan mengatakan kepada saya bahwa informasinya aman terlindungi karena sudah mengeluarkan banyak biaya untuk membeli teknologi keamanan TI. Sisanya berlindung di balik jargon, "Tidak ada yang 100 persen aman." Jargon sakti yang disalahgunakan oleh banyak pihak karena tidak sepenuh hati melaksanakan tugas dan tanggung jawabnya.

Mereka tidak berbeda nasibnya dengan banyak orang Indonesia yang menjadi korban kejahatan di Paris. Selama tinggal di Prancis beberapa tahun, saya sering menemani teman-teman yang berkunjung ke Paris dan selalu mengingatkan agar berhati-hati. Ada seorang teman yang datang berkunjung ke Paris menjadi korban kejahatan karena salah melakukan manajemen risiko. Padahal, dia lahir dan besar di kota Medan, kuliah di Surabaya, tinggal dan bekerja di Jakarta. Dia tidak pernah menjadi korban

kejahatan selama hidupnya di 3 kota besar yang terkenal rawan karena sadar akan tingginya tingkat kejahatan sehingga selalu waspada.

Saat bertemu saya, dia berkata, “Luar biasa, 30 tahun saya tinggal di Jakarta, Medan, dan Surabaya. Naik angkutan umum berjejal, membawa uang dalam jumlah besar, saya tidak pernah dicopet. Di Paris, belum sampai 24 jam sudah kehilangan beberapa ribu euro, paspor, dan tiket pesawat. Tadinya saya merasa Paris aman.” Rasa aman berbahaya. Rasa aman membuat orang lengah.

Membeli dan memasang pagar tinggi, CCTV canggih, dan dijaga petugas keamanan tidak selalu berbanding lurus dengan keamanan. Celakanya, hal itu malah akan menjadi bumerang jika tanpa kebijakan dan prosedur keamanan yang dijalankan oleh petugas keamanan yang berintegritas dan kompeten. Bagi saya, lebih baik saya mengeluarkan biaya investasi 1 juta rupiah untuk membeli ponsel pintar, biaya operasional 100 ribu rupiah per bulan, minta tolong kepada ibu penjaga warung di depan rumah untuk memfoto semua orang yang datang ke rumah saya, dan mengirimkannya ke saya. Jika curiga, saya dapat menerapkan langkah-langkah verifikasi dan tanggap insiden yang sudah saya siapkan sebelumnya.

Berdasarkan pengalaman saya di bidang TI selama 25 tahun, secara khusus di bidang keamanan siber dan informasi, ternyata lebih dari 90 persen implementasi teknologi keamanan tidak efektif melindungi informasi sebagai aset yang berharga.

Sebagai contoh, 90 persen layanan *Internet Banking* tetap sangat mudah diretas walau sudah menerapkan berbagai teknologi pengamanan yang canggih dan sangat mahal, lengkap dengan jargon-jargon teknis yang mengerikan bagi orang awam, seperti *firewall*, *intrusion detection system*, *intrusion prevention system*, *web application firewall*, *security information and event management, strong authentication, hardware security token, one time password*, HTTPS, SSL, Enkripsi Symmetric AES 256, Enkripsi Asymmetric RSA 2048, dan *penetration testing*. Jangankan para pimpinan, mayoritas teman profesional teknologi informasi pun hanya tahu "kulitnya".

Tahun 2010, XecureIT WhiteHackerLab melakukan penelitian kelemahan keamanan layanan *Internet Banking* terhadap tiga bank nasional dan tiga bank asing yang beroperasi di Indonesia. Lima tahun sebelum kasus sinkronisasi token menggegerkan industri perbankan Indonesia, saya dan teman-

teman telah memaparkan dan mendemonstrasikan hasil penelitian kami di hadapan regulator dan pelaku industri perbankan Indonesia. Kesimpulannya adalah terlalu mudahnya melakukan perampokan pada akun perorangan maupun akun perusahaan dengan mengeksploitasi kelemahan.

Sayangnya sampai saat buku ini diterbitkan tahun 2016, masih sangat mudah merampok uang melalui *Internet Banking*. Industri perbankan "mengedukasi" masyarakat bahwa *Internet Banking* aman. Bagi regulator yang penting bank sudah mematuhi regulasi yang ada sesuai *audit checklist* tanpa melihat substansinya. Nasabah merasa aman sehingga lengah. Dan, yang tertawa menikmati kondisi ini adalah penjahat siber, termasuk di dalamnya para teroris.

Perkembangan teknologi selalu diikuti juga dengan perkembangan kejahatan. Penjahat tidak hanya menyerang industri keuangan, tetapi juga organisasi keagamaan, sekolah, rumah sakit, pelabuhan, pelayaran, penerbangan, dan lain-lain. Revolusi di dunia siber membutuhkan revolusi strategi keamanan informasi yang tepat. Jika tidak ingin menjadi korban atau melakukan pembiaran terjadinya kejahatan, sudah saatnya para pemimpin

di era revolusi siber menyadari berbagai ilusi keamanan siber dan informasi.

Keamanan informasi dan siber merupakan isu yang kompleks. Teknologi keamanan hanya sebagai alat bantu. Manusia adalah faktor utama yang menentukan apakah kondisi yang aman benar-benar terwujud atau hanya sebuah ilusi. Kesadaran akan ancaman nyata dunia maya menentukan persepsi terhadap risiko yang menentukan perilaku pengambil keputusan. Sebagai pimpinan, Andalah yang menentukan seberapa efektif keamanan yang sesungguhnya.

Langkah awal yang harus dilakukan para pemimpin adalah membuka diri dan mengubah pola pikir menyesatkan bahwa pengamanan informasi merupakan tanggung jawab profesional TI. Saya menganalogikan dengan bisnis restoran, bagian TI hanyalah bagian pengelola peralatan dapur yang tidak mengerti jenis sayuran, kualitas daging, proses memasak, dan risiko bisnis.

Melalui buku ini, saya berharap para pengambil keputusan di tingkat perusahaan dan negara lebih menyadari dan memahami kondisi nyata ke(tidak)amanan dunia maya, agar dapat mengambil

keputusan strategis yang efektif dan efisien. Keputusan yang diambil bukan hanya melihat secara terbatas dalam konteks organisasinya, melainkan juga mempertimbangkan konteks eksternal. Sebab, penjahat juga melihat keseluruhan konteks secara komprehensif saat membuat strategi serangan terorganisir.

Lima tahun lalu, topik keamanan informasi dan siber merupakan isu langka di ruang rapat pimpinan. Para pimpinan hanya memasrahkan diri, perusahaan, dan negaranya kepada para profesional TI. Namun saat ini, topik ini sudah menjadi salah satu isu utama. Bahkan, beberapa perusahaan dan negara sudah menjadikan topik keamanan ini sebagai *business enabler*. Para pengambil keputusan strategis harus terlibat aktif meningkatkan keamanan informasi dan siber untuk memerangi kejahatan yang terorganisir dan tumbuh pesat di dunia maya.

Saya berusaha menjelaskan topik yang sulit untuk dipahami dengan bahasa yang sederhana. Harapan saya, para pimpinan tidak lagi "alergi" dengan topik ini karena menganggap semata urusan teknis yang sulit dipahami. Saya menggunakan analogi-analogi dunia nyata, dan memberikan banyak contoh kasus riil sebagai pembelajaran agar buku ini mudah dicerna.

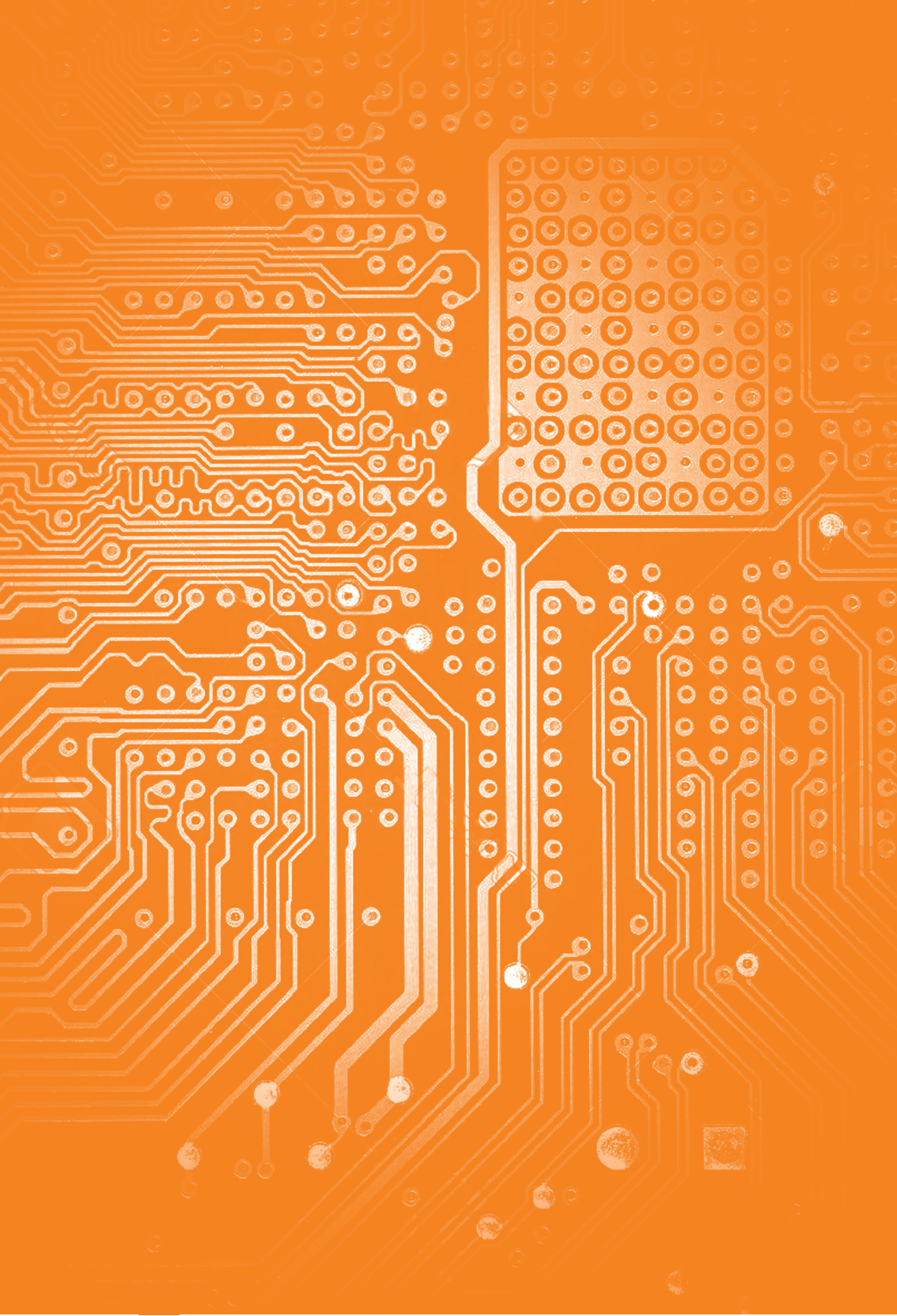
Saya menggunakan banyak contoh terkait industri keuangan, khususnya perbankan. Sebab, hampir semua orang berhubungan dengan industri ini sehingga mudah dibayangkan. Industri perbankan memiliki banyak sekali aturan dan termasuk industri yang paling matang di bidang keamanan informasi. Industri ini juga memanfaatkan banyak sekali teknologi keamanan dan berhasil memberi rasa aman kepada nasabah. Lalu, apa yang salah sehingga industri ini tetap menjadi sasaran empuk pelaku kejahatan siber?

Saya berharap pembaca buku ini dapat memahami dan mengidentifikasi miskonsepsi strategi keamanan informasi dan siber dengan mengangkat masalah-masalah fundamental terkait.

Sebelum menulis buku ini, saya ikut menulis buku *Information Security Management Handbook* (5th Edition, ISBN-10: 0849319978, tahun 2003) dan *Information Security Management Handbook* (6th Edition, ISBN-10: 0849374952, tahun 2007) yang ditujukan untuk profesional keamanan informasi. Saya mulai menulis buku ini tahun 2010 saat rangkaian espionase siber yang menargetkan 34 perusahaan yang dikenal dengan nama Operation Aurora terungkap ke publik, dan *malware* Stuxnet

yang ditujukan untuk menyerang instalasi nuklir Iran yang dikenal dengan nama Operation Olympic Games terungkap tahun 2010. Setelah terbengkalai beberapa tahun, saya bersyukur akhirnya dapat menyelesaikan buku ini dengan dorongan dan dukungan kuat dari istri saya, Liza.

Selamat membaca.



1

DAMPAK NYATA DUNIA MAYA

"Digital world is dangerous because it's silent."
~ Unknown

“KESADARAN AKAN BERBAGAI RISIKO DAN KEPEDULIAN KITA SEMUA MERUPAKAN JAWABAN AGAR BISA BERSAMA-SAMA HIDUP LEBIH AMAN DAN NYAMAN DI DUNIA MAYA.”

Komputer, telepon selular, Internet, dan berbagai produk teknologi informasi lainnya membentuk dunia maya, terkadang juga disebut dunia digital atau dunia siber. Disadari atau tidak disadari, suka atau tidak suka, saat ini tidak ada lagi aspek dalam kehidupan kita yang tidak bersentuhan dengan dunia maya hingga ke tengah hutan sekalipun. Tidak banyak pihak yang menyadari bahwa dunianya saja yang maya, tetapi bahaya yang dihadapi nyata. Dan, jauh lebih berbahaya karena tidak ada aktivitas yang kasat mata.

Revolusi yang terjadi pada dunia maya juga menimbulkan berbagai jenis ancaman baru. Pada akhir tahun 90-an, dibutuhkan waktu yang cukup

lama dan pengetahuan informasi yang tinggi akan teknologi untuk melakukan serangan terhadap jaringan komputer. Saat ini, untuk menyerang suatu jaringan ataupun mengambil alih komputer milik pihak lain merupakan hal yang mudah. Yang dibutuhkan hanya koneksi Internet, mengunduh piranti lunak, membaca petunjuk singkat, beberapa kali *klik* pada *mouse*, kemudian digabungkan dengan teknik rekayasa sosial (*social engineering)* di mana yang diserang (ditipu, diancam, dan diperdaya) adalah si pemakai komputer.

AKSI PERETASAN DI FILM HOLLYWOOD

Industri film Hollywood melakukan penelitian mendalam untuk membuat sebuah film. Cukup banyak film yang berkaitan dengan keamanan siber menampilan adegan-adegan yang sebenarnya juga terjadi di dunia nyata (bukan hanya bisa terjadi di film). Sebagai contoh, film *Die Hard 4*, merupakan potongan-potongan insiden pembajakan sistem infrastruktur kritis (jaringan komunikasi, listrik, dan pengontrol lalu lintas) yang pernah terjadi di berbagai belahan dunia, yang kemudian dirangkai menjadi satu. Bumbunya adalah ledakan-ledakan dahsyat dan aktor utamanya seolah-olah “menari” di atas badan pesawat jet tempur.

Saya cukup paham dengan apa dan bagaimana kondisi keamanan infrastruktur kritis. Beberapa tahun lamanya saya bertanggung jawab membuat arsitektur keamanan infrastruktur kritis (jaringan produksi minyak dan gas) di berbagai anak perusahaan Total grup di banyak negara. Saya beberapa kali menjadi pembicara pada pertemuan-pertemuan terbatas yang terdiri dari para ahli di bidang keamanan Industrial Control System (ICS) di Eropa yang bertugas mengamankan sistem infrastruktur kritis. Dalam sebuah pertemuan, saya merinding saat rekan pembicara lainnya memaparkan insiden infeksi *malware* di dalam sistem pengendali sebuah pembangkit listrik tenaga nuklir. Saya juga telah melakukan penanganan insiden dan "berburu" *malware* di sebuah platform produksi minyak dan gas di Alaska. Sehingga, bagi saya *Die Hard 4* merupakan film "dokumenter", termasuk aksi meledaknya pipa gas. Di dunia nyata, bukan di film, Central Intelligence Agency (CIA) berhasil "memasang" *malicious chip* dan *malware* yang mengakibatkan ledakan pipa gas milik Uni Soviet di Siberia tahun 1982.

Dalam film *Entrapment*, sepasang pencuri profesional kelas kakap yang diperankan Sean Connery dan Catherine Zetta Jones melakukan pencurian lukisan-lukisan bernilai jutaan dolar

yang dijaga oleh sistem pengaman ekstra tinggi. Dalam film itu, sekonyong-konyong pencuri sudah tahu seluruh teknologi pengamanan yang dipakai dan kelemahannya, prosedur dan jadwal penjaga, hingga jalur pelarian rencana A dan rencana B. Tidak heran sebagian besar orang berpikir: "Ah, itu kan di film, sehingga mereka bisa tahu." Kenyataannya, kejadian tersebut tidak hanya di film. Beberapa kasus pencurian yang mampu menyerang sistem pengaman ekstra tinggi dan berhasil meraup harta bernilai ratusan juta dolar benar-benar terjadi.

DAMPAK KESELAMATAN JIWA

Beberapa peneliti melakukan uji keamanan terhadap alat pacu jantung canggih yang sudah digunakan oleh lebih dari 450.000 orang untuk menopang hidupnya. Data-data alat pacu jantung tersebut dapat dibaca melalui koneksi nirkabel. Ternyata terdapat kelemahan keamanan pada perangkat tersebut. Dari jauh peretas dapat memprogram ulang, mematikan fungsinya, dan memerintahkan perangkat untuk mengirim beberapa kejutan ke jantung pengguna yang setara dengan 137,7 volt.

Risiko dunia maya juga mengangkasa. Laporan audit keamanan dari Federal Aviation Administration (FAA) tahun 2007 mengungkapkan rancangan jaringan Internet *broadband* di pesawat Boeing terbaru 787 Dreamliner bagi para penumpang ternyata dapat digunakan untuk menguasai sistem kontrol pesawat terbang tersebut.

Berikut cuplikan ringkasan laporan audit FAA tahun 2007 terlait keamanan jaringan dan sistem komputer Boeing Model 787-8:

> *"The architecture of the Boeing Model 787–8 computer systems and networks may allow access to external systems and networks, such as wireless airline operations and maintenance systems, satellite communications, electronic mail, the Internet, etc. Onboard wired and wireless devices may also have access to parts of the airplane's digital systems that provide flight critical functions. These new connectivity capabilities may result in security vulnerabilities to the airplane's critical systems. For these design features, the applicable airworthiness regulations do not contain adequate or appropriate safety*

standards for protection and security of airplane systems and data networks against unauthorized access."

Bahkan pada Agustus 2008, NASA mengonfirmasikan *laptop* International Space Station di bulan terinfeksi *malware* (*malicious software*/piranti lunak jahat). Masih beruntung *malware* tersebut tidak menyebar ke sistem komputer yang mengatur operasi stasiun luar angkasa.

Sebuah komputer yang digunakan dalam kegiatan operasi di Rumah Sakit Sheffield Teaching Hospitals Trust mendadak mati saat operasi tengah berlangsung di akhir Desember 2009. Dalam waktu singkat, lebih dari 800 komputer dari total 8000 komputer di rumah sakit tersebut terinfeksi *malware*.

DAMPAK HUKUM

Dengan adanya undang-undang terkait keamanan dunia maya dan informasi di berbagai negara, para pimpinan perusahaan dan pejabat negara harus sadar bahwa siapa pun memiliki risiko hukum jika tidak berhati-hati menggunakan teknologi informasi yang dimilikinya. Sebagai contoh, jika ponsel diretas dan digunakan untuk mengirim SMS

ancaman bom, maka si pemilik harus bertanggung jawab secara hukum.

Fungsi *auto synchronization* ke *online drive* untuk kebutuhan *data backup* pada Windows 10, Android, atau iOS tanpa disadari berpotensi besar membocorkan rahasia perusahaan atau rahasia negara. Lebih mengenaskan, saat bertukar kartu nama institusi dengan jenderal-jenderal militer, cukup banyak yang alamat *e-mail*-nya @gmail.com atau @yahoo.com.

Simon Bruce harus berurusan dengan Kepolisian Inggris selama beberapa bulan dengan tuduhan terlibat pornografi anak. Dia kehilangan pekerjaan dengan gaji besar dan mengalami mimpi buruk yang nyata. Akhirnya, dia dibebaskan setelah berhasil membuktikan bahwa kartu kredit miliknya digunakan untuk belanja foto-foto pornografi anak oleh orang lain dengan alamat IP yang berlokasi di Jakarta.

DAMPAK KEUANGAN

TJX, perusahaan induk dari jaringan toko T.J. Maxx dan Marshall, harus menanggung kerugian yang diperkirakan bisa mencapai 1 miliar dolar AS

akibat 94 juta informasi kartu kredit pelanggannya dicuri. Peretas berhasil membobol jaringan nirkabel internal antara 2 toko Marshall di periode akhir tahun 2006.

Pada Agustus 2015, Pemerintah Amerika Serikat mengumumkan sekelompok peretas menikmati informasi sensitif lebih awal dan berhasil mendapat keuntungan 100 juta dolar AS. Kelompok tersebut selama bertahun-tahun menyusup tanpa terdeteksi ke dalam sistem 3 perusahaan penyedia layanan publikasi laporan keuangan perusahaan-perusahaan yang sahamnya diperdagangkan di bursa. Mereka menikmati ratusan *press releases* lebih dahulu dari publik.

DAMPAK TERHADAP KEPEMILIKAN BISNIS

Terdapat hal menarik dalam iklan satu halaman penuh di harian *Kompas* beberapa tahun lalu. Iklan dari pihak lawan sengketa saham sebuah perusahaan tambang batu bara mengungkapkan bahwa terdapat surat-surat elektronik (*e-mail*) antara perusahaan tambang tersebut dengan sebuah bank multinasional yang menjadi bukti di pengadilan Singapura bahwa terdapat usaha menghilangkan bukti-bukti transaksi keuangan.

Tahun 2009, seorang CEO perusahaan terkenal di Indonesia, meminta tim penanganan insiden XecureIT untuk menyelidiki apakah ada kebocoran informasi di perusahaannya. Sudah 3 potensi bisnis dengan mitra international yang digarap beberapa tahun, tiba-tiba diambil kompetitor dengan perbedaan nilai bisnis yang tidak signifikan. Ternyata, terlalu banyak celah keamanan informasi yang kami temukan. Padahal, perusahaan tersebut sudah mengeluarkan biaya yang sangat besar untuk membeli teknologi pengaman. Bisnisnya seperti dilindungi kelambu yang bolong-bolong.

DAMPAK TERHADAP INDUSTRI STRATEGIS

Pada penghujung tahun 2012, lebih dari 30.000 komputer milik Saudi Aramco terinfeksi virus yang berdampak pada terganggunya produksi minyak dan gasnya. Serangan yang dicurigai didukung oleh negara lain di belakangnya (*state actor*), memiliki objektif untuk menghentikan produksi minyak Arab Saudi, namun gagal mencapai tujuan utamanya.

DAMPAK TERHADAP PENDANAAN TERORISME

Keamanan layanan *Internet Banking, Mobile Banking,* dan *Branchless Banking* harusnya mendapat perhatian serius dari pimpinan pemerintahan dan regulator perbankan. Risiko keamanan yang tinggi bukan hanya merugikan nasabah dan industri perbankan, tetapi juga menjadi sumber pendanaan terorisme yang berisiko sangat rendah dengan hasil rampokan yang sangat tinggi. Indikasinya jelas yaitu semakin jarang terjadinya perampokan fisik terhadap bank, toko perhiasan, dan pompa bensin di Indonesia.

DAMPAK TERHADAP KEDAULATAN NASIONAL

Pada akhir Maret 2014, tiga bank Rusia, Bank Rossiya, Sobinbank, dan SMP Bank melaporkan bahwa layanan MasterCard dan Visa tidak berfungsi. Para nasabah yang menggunakan kartu kredit dan kartu debit tersebut tidak dapat bertransaksi. MasterCard mengatakan bahwa layanannya ke Rusia dihentikan sebagai akibat sanksi yang dijatuhkan pemerintah Amerika Serikat.

Pemisahan Crimea dan Ukraina telah memanaskan suhu politik kedua negara tersebut,

dan berdampak nyata pada kehidupan dunia maya warga Rusia. Rasa nasionalisme dan kemandirian teknologi menciptakan ketahanan siber Rusia yang kuat.

Pemerintah Rusia bergerak cepat dengan memperbaiki kebijakan dan membangun sistem pembayaran nasional. Kebijakan baru mewajibkan seluruh sistem pembayaran internasional wajib diproses melalui sistem pembayaran nasional yang akan memungkinkan sistem kartu kredit Rusia terus berfungsi, bahkan ketika sistem pambayaran internasional dihentikan. Hasilnya, pada bulan April 2015, Visa dan MasterCard bisa kembali dinikmati masyarakat Rusia, tetapi harus melalui sistem pembayaran nasional tersebut.

DAMPAK TERHADAP PERTAHANAN NEGARA

Januari 2009, Intramar, jaringan komputer angkatan laut Perancis terinfeksi *malware* sehingga harus diisolasi untuk mencegah penyebaran yang lebih luas ke jaringan militer lainnya. Dampaknya, pesawat tempur Rafale harus membatalkan misinya karena tidak dapat mengunduh rencana penerbangan. Angkatan Laut Perancis mengakui bahwa mereka harus beralih kembali menggunakan telepon, faksimile, dan pos.

Tidak hanya mengangkasa, *malware* pun menyelam ke dasar lautan dibawa dalam sistem kapal selam angkatan laut kerajaan Ingris. Sebuah laporan dalam tinjauan militer mengungkapkan bahwa pada hari-hari pertama Januari 2009, Kementerian Pertahanan Inggris telah diserang oleh *malware* yang secara substansial dan serius menginfeksi sistem komputer lebih dari 24 pangkalan Royal Air Force dan 75 persen dari armada Angkatan Laut, termasuk kapal induk Ark Royal.

DAMPAK TERHADAP MASA DEPAN BANGSA

Justin Berry adalah seorang pelajar yang cerdas di California High School, presiden di kelasnya. Pada usia 13 tahun, dia menerima *web camera* dan mengakses Internet untuk bertemu dengan teman baru. Dalam waktu yang sangat singkat, dia bertemu dengan teman *online* yang memintanya melakukan beberapa aktivitas di depan *webcam*. Sesuatu yang awalnya baik-baik saja, kemudian berubah menjadi awal keterlibatannya melakukan kegiatan seksual secara *online*. Dia menerima banyak uang, sekaligus menikmati perhatian dari penggemarnya. Sampai akhirnya dia memiliki bisnis prostitusi *online* dengan dirinya sebagai bintang, dan juga melibatkan anak-anak di bawah umur lainnya. Orang membayar

keanggotaan situs *web* miliknya sebesar 45 dolar AS per bulan, dan biaya tambahan hingga 300 dolar AS untuk melihat kegiatan seks yang lebih menantang. Dengan penghasilan beberapa ribu dolar AS per bulan, bisnis Justin Berry melibatkan banyak anak.

Berikut kesaksian Justin Berry saat berusia 19 tahun; "Selama 5 tahun, dimulai ketika saya berusia 13 tahun, saya mengoperasikan situs *web* porno yang menampilkan gambar dari diri saya di depan *webcam*. Saya dibayar oleh lebih dari 1.000 orang untuk telanjang, masturbasi, dan bahkan berhubungan seks dengan pelacur wanita saat di depan kamera. Saya berbisnis dibantu oleh penjahat dewasa, termasuk perusahaan yang memproses pembayaran dengan kartu kredit."

Kesadaran akan berbagai risiko dan kepedulian kita semua merupakan jawaban agar bisa bersama-sama hidup lebih aman dan nyaman di dunia maya. Teknologi keamanan merupakan alat bantu yang memiliki banyak keterbatasan. Nyaris tidak ada perusahaan atau negara yang dapat bertahan hidup tanpa bersentuhan dengan dunia maya. Orang tua pun tidak mungkin mencegah anaknya berhubungan dengan Internet karena suatu saat tidak ada murid

yang dapat mengerjakan tugas sekolah tanpa mengakses Internet.

Layaknya listrik yang berbahaya tapi diamankan dengan benar dan baik, Internet merupakan sumber daya tanpa batas yang harus dimanfaatkan secara positif sehingga akan memberi manfaat yang juga luar biasa. Namun, hanya perusahaan dan negara yang benar-benar sadar dan peduli akan keamanan informasi dan dunia maya, serta menerapkan strategi keamanan yang tepat yang dapat menikmatinya.

Selalu waspada dengan tingkat kesadaran keamanan tinggi, bukan paranoid, menjadi kunci untuk dapat hidup nyaman di dunia maya.

Selamat, Anda telah menyadari sebagian kecil dampak nyata dunia maya bagi perusahaan dan negara Anda.

2

MERETAS ITU NIKMAT, MENGAMANKAN ADALAH MIMPI BURUK

“AKAN TETAPI, KEGIATAN MERETAS ORANG, PROSES, DAN KEAMANAN FISIK BELUM BISA BERHENTI SEPENUHNYA KARENA NIKMAT.”

Saya mulai bekerja sebagai pengembang sistem komputer tahun 1992 dengan mengerjakan proyek kecil-kecil untuk membayar kuliah dan membiayai hidup sendiri. Ada beberapa kondisi di mana saya harus mengakali sistem yang bekerja tidak sesuai keinginan saya. Termasuk di sini melewati proteksi-proteksi sistem, melakukan beberapa perubahan, serta membuat aplikasi tambahan, agar sistem bisa bekerja lebih baik dan mempermudah pekerjaan saya. Kehidupan normal selama bertahun-tahun yang ternyata di kemudian hari tiba-tiba menjadi "keren" dengan sebutan *hacking* (meretas), yang berubah menjadi menyebalkan karena saat ini dianggap sebagai kejahatan.

Saat menyelesaikan buku ini, sudah 3 tahun saya tidak menghidupkan *hacking lab* di laptop karena ingin berhenti meretas teknologi, walaupun belum 100 persen. Akan tetapi, kegiatan meretas orang, proses, dan keamanan fisik belum bisa berhenti sepenuhnya karena nikmat. Bayangkan, betapa serunya bermain *game* nyata, bukan *virtual reality*, bersama dengan orang lain yang tidak menyadari keterlibatan mereka.

KEHIDUPAN PERETAS ZAMAN DAHULU

Dahulu, saya menikmati proses meretas sistem. Kepuasannya adalah jika berhasil membongkar, mengubah, dan menjadikan sebuah sistem menjadi lebih baik dan lebih bermanfaat. Tantangannya adalah mempelajari secara mendalam cara kerja sistem tersebut, melihatnya dari sudut pandang yang tidak saharusnya, mencari titik-tiik lemahnya, untuk kemudian dieksploitasi.

Dahulu, butuh *passion*, pola pikir *out of the box*, pengetahuan mendalam, dan kemampuan yang cukup untuk menjadi seorang peratas. Jika berhasil membobol sistem pihak lain, kita memberitahukan ke pengelola sistem, yang akhirnya menjadi teman. Tidak ada motif lain. Untungnya, belum ada model

bisnis yang mampu memunculkam niat jahat saat saya berhasil mengakses informasi pihak lain.

"PERETAS" (PENJAHAT) SAAT INI

Saat ini, motivasi "peretas" sudah berkembang menjadi motif ekonomi, SARA, politik, atau balas dendam, yang nenurut hukum yang berlaku dikategorikan sebagai tindak kejahatan. "Kenikmatan" meretas saat ini juga sudah berubah 180 derajat, antara lain sebagai berikut.

1. Membajak akun *e-mail* atau media sosial pihak lain.
2. Mengubah tampilan *web* pihak lain dengan memasang *nick name* yang dipercaya tidak dapat dirunut ke pemilik nama aslinya.
3. Menggunakan koneksi Internet gratis.
4. Menonton tampilan langsung CCTV atau *web cam* pihak lain.
5. Menggunakan kartu kredit curian.
6. Mencuri informasi milik perusahaan atau pemerintah.
7. Pendanaan terorisme.

Cara meretas sistem saat ini menjadi sangat sederhana. Jika memiliki uang, beli perangkat lunak yang penggunaannya semuanya sudah serba *point and click*. Atau cara gratis, hanya dengan mencari tutorial, mengunduh perangkat lunak, dan ikuti setiap langkah di tutorial tersebut. Analoginya, jika dahulu ingin menembak, seseorang harus membuat senjata dan peluru sendiri. Sekarang, dari senapan angin hingga rudal semua tersedia gratis. Kalau tidak tahu cara menggunakannya, tonton videonya di Internet. Perubahan kondisi ini seharusnya diikuti dengan perubahan strategi keamanan siber dan informasi. Karena, bagi pemilik informasi pribadi, perusahaan, atau negara risiko, menjadi korban peretasan menjadi meningkat drastis, baik secara dampak maupun kemungkinan.

TUKANG KUNCI VS. MALING

Sejak dahulu, apalagi saat ini, saya merasa agak terganggu jika dijuluki peretas, karena saya tidak pernah berprofesi sebagai peretas. Dahulu saya melakukan tugas dan tanggung jawab sebagai pembuat program dan administrator sistem. Saat ini, saya sebagai konsultan, pelatih, ataupun pelayan negara untuk melakukan koordinasi dan mitigasi dalam bidang siber dan informasi nasional. Memang,

kegiatan yang saya dan teman-teman seprofesi lakukan menggunakan pola pikir dan teknik yang diberi istilah meretas. Namun, mohon dibedakan antara tukang kunci dengan maling. Teman saya, seorang doktor di bidang hukum teknologi informasi, pernah mengatakan, "Di pengadilan, *hacker* atau peretas dipahami berbeda dengan profesional pengamanan informasi."

MIMPI BURUK YANG MENJADI KENYATAAN

Sebagai CEO atau pimpinan pemerintahan yang harus mengambil keputusan atas strategi keamanan siber dan informasi, menurut Anda, siapa yang akan menjadi pemenang?

A. Peretas yang menikmati kehidupannya meretas hingga pagi menjelang, dan dapat dilanjutkan dengan waktu tidak terbatas;

melawan

B. Profesional TI atau keamanan informasi yang melewati masa "sengsara" selama jam kantor dengan jadwal yang ketat. ditambah mimpi buruk di malam hari.

Saya dapat merasakan apa yang dialami para profesional pengamanan informasi yang bertugas di berbagai organisasi yang diretas tersebut. Saya bekerja di kantor pusat Total Exploration and Production, salah satu perusahaan minyak dan gas terbesar di dunia, selama 3 tahun. Salah satu tugas utama saya adalah bekerja sama dengan puluhan anak perusahaan di seluruh dunia untuk memastikan keamanan sistem internal kantor pusat dan Industrial Control System produksi minyak dan gas.

Saya menikmati tugas yang bagi saya luar biasa tersebut karena bagian dari *passion*. Namun, tetap saja mimpi buruk tidak dapat dihindari saat terjadi beberapa kali insiden keamanan siber. Suka atau tidak suka, saya jadi terpaksa dan terbiasa mengembangkan arsitektur keamanan siber dan informasi dengan tingkat maksimum. Termasuk bertugas untuk melindungi informasi kesehatan di klinik internal yang jika diretas kemungkinan bisa mengakibatkan Direktur klinik akan dipenjara (berdasarkan hukum Prancis yang sangat menghargai kerahasiaan informasi pribadi).

Teknologi pengamanan berkembang pesat. Akan tetapi, umumnya tetap dengan pola pikir: penjahat selalu selangkah lebih dahulu dari polisi.

Ada satu hal lagi yang nyaris tidak berubah, yaitu kesadaran, kecerobohan, ketidakpedulian orang akan pentingnya keamanan siber dan informasi. Orang dan perangkat yang digunakannya adalah kombinasi sempurna yang menciptakan lubang besar keamanan siber dan informasi yang sangat menguntungkan penjahat, sekaligus mimpi buruk bagi penanggung jawab keamanan informasi.

CONTOH-CONTOH MIMPI BURUK YANG MENJADI KENYATAAN

April 2011, dunia keamanan informasi digegerkan dengan insiden peretasan terhadap RSA, sebuah perusahaan raksasa penyedia jasa teknologi pengamanan. Sebuah file lampiran bernama "2011 Recruitment Plan.xls" yang dikirim melalui *e-mail* dengan subjek "2011 Recruitment Plan" dibuka oleh salah seorang stafnya. *Malware* yang disisipi dalma *file* tersebut kemudian mengeksploitasi kerentanan sistem milik RSA. Akhirnya, RSA harus mengakui bahwa selama ini pihaknya menyimpan kode rahasia token SecureID, dan kode rahasia tersebut berhasil dicuri oleh peretas. Siapa pun yang memiliki kode rahasia token SecureID dapat membuat *one time password* untuk mengakses sistem yang dilindungi sama seperti pemegang *hardware* atau *software* token tersebut. Sekitar 40 juta token SecureID dijadikan

andalan oleh banyak korporasi global, termasuk Lockheed Martin yang sebulan kemudian menjadi korban peretasan.

Industri perbankan Amerika Serikat mengalami mimpi buruk sejak awal hingga akhir Desember 2012. Belasan bank, termasuk Bank of America, Citigroup, Goldman Sachs, JPMorgan Chase & Co., dan HSBC menjadi korban serangan *Distributed Denial of Service* (DDoS) yang melumpuhkan situs web dan/atau layanan Internet banking.

Pertengahan tahun 2015 muncul berita bahwa basis data milik Office of Personnel Management Pemerintah Amerika Serikat diretas. Lebih dari 20 juta rekaman yang dicuri berisi informasi sangat sensitif, termasuk berkas-berkas terkait *security clearance*. Informasi yang dicuri bukan hanya milik hampir seluruh karyawan dan kontraktor federal, tetapi termasuk informasi tentang teman-teman dan keluarga mereka. Bulan September 2015, sebagai tamu resmi pemerintah Amerika Serikat terkait kerjasama di bidang keamanan siber dengan negara-negara di Asia Pasifik, saya beberapa kali rapat dengan FBI. Mereka menyatakan peretasan tersebut benar-benar mengancam keamanan nasional,

termasuk dari sudut pandang kontra-intelijen. Mimpi super buruk bagi pemerintah Amerika Serikat.

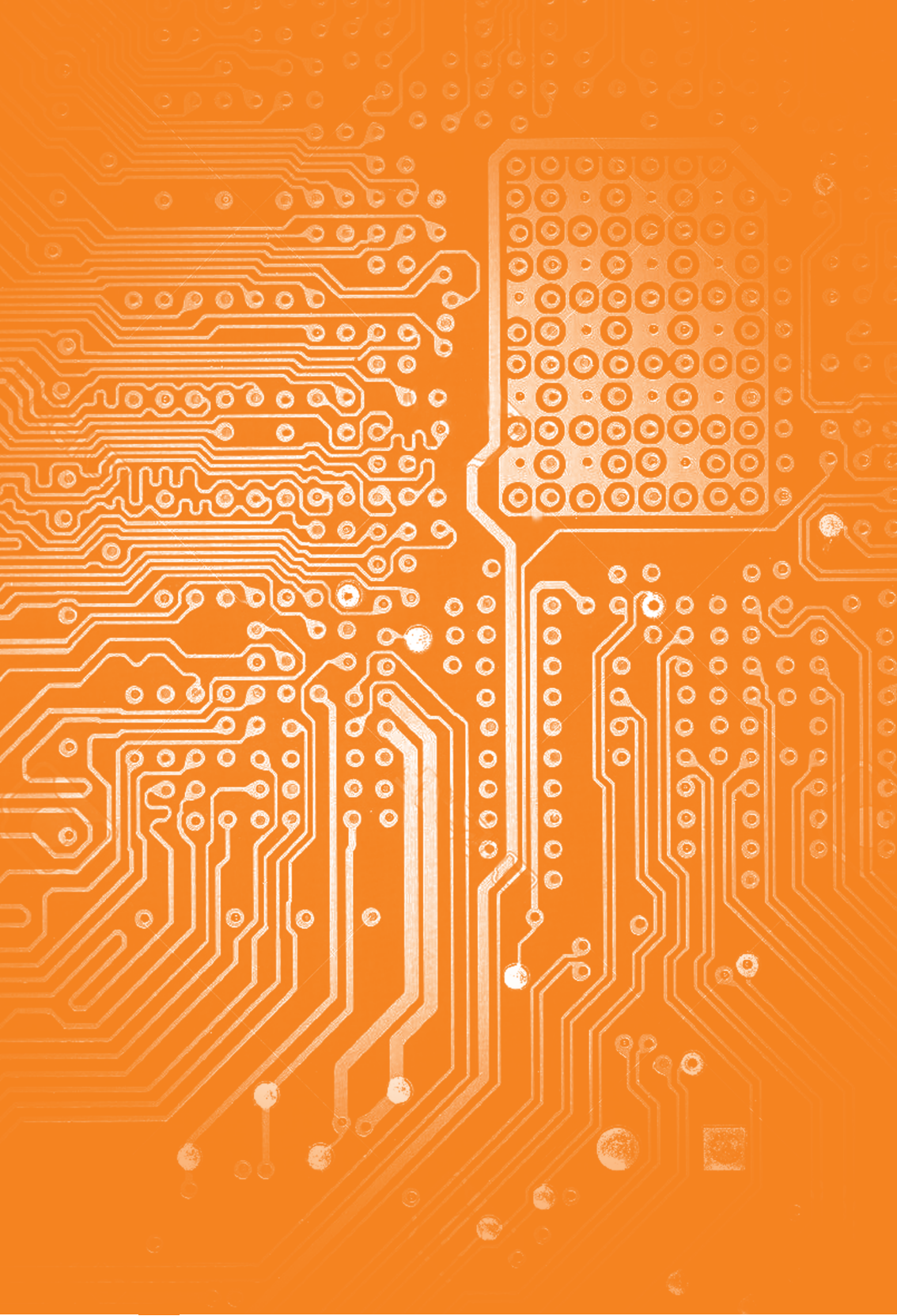
Peretas menyebarkan di Internet 19 Gigabyte data milik sebuah situs fasilitas perselingkuhan yang memiliki hampir 40 juta anggota pada pertengahan tahun 2015. Dengan membayar 19 dolar AS, anggota dapat memilih teman selingkuhannya. Informasi kartu kredit, alamat *e-mail*, kriteria pemilihan teman selingkuh, dan informasi sensitif lainnya menjadi terbuka bagi siapa pun. Ternyata, banyak anggotanya yang menggunakan alamat *e-mail* perusahaan, pemerintah (.gov), dan institusi militer (.mil) untuk mendaftar. Paling tidak ada 2 anggotanya bunuh diri dan dicurigai terkait dengan terbongkarnya informasi rahasia mereka.

Februari 2016, virus penyandera file-file elektronik (*ransomware*) menginfeksi sistem milik rumah sakit Hollywood Presbyterian Medical Center di Los Angeles, Amerika Serikat. *Ransomware* tersebut mengenkripsi file-file yang ada sehingga mengganggu kegiatan operasional rumah sakit selama 10 hari. Akhirnya, manajemen memutuskan untuk membayar uang "tebusan" sebesar 16.664 dolar AS demi mendapatkan kunci untuk mendekripsi.

Maret 2016, terungkap bahwa jutaan nasabah bank-bank Australia, New Zealand, dan Turki menjadi target serangan *malicious software* (*malware*) yang melumpuhkan sistem keamanan *two-factor authentication*. Empat bank terbesar Australia yang menjadi target yaitu Commonwealth Bank, Westpac, National Australia Bank, dan ANZ Bank. *Malware* ini juga menyasar pengguna PayPal, eBay, Skype, WhatsApp, dan beberapa layanan Google. *Malware* akan bersembunyi, tidak tampak oleh pengguna ponsel, menunggu nasabah membuka aplikasi *mobile banking* bank-bank yang menjadi sasaran. *Malware* mencuri User ID, *password*, dan token autentikasi yang dikirimkan oleh bank *via* SMS, kemudian mengirimkan informasi curian tersebut ke peretas. Peretasan menggunakan *malware* ini membuktikan betapa rentannya aplikasi *mobile banking*. Hal ini akan segera menjadi mimpi buruk pengamanan informasi bagi bank-bank lainnya juga.

Pada tanggal 5 Februari 2016, peretas merampok 100 juta dolar AS dana milik Bank Sentral Bangladesh di akun New York Federal Reserve. Uang tersebut ditransfer ke Filipina, kemudian dijual di pasar gelap, dan dikirimkan ke kasino lokal. Setelah dicuci di kasino, dalam beberapa hari kemudian dana tersebut ditransfer kembali ke pasar gelap yang sama,

dan dipindahkan ke beberapa bank di luar negeri. Proses transfer dana berikutnya sebesar 870 juta dolar AS berhasil digagalkan. Bank Sentral Bangladesh menyatakan ada sesuatu di luar kewajaran terjadi pada Federal Reserve. Namun, pihak Federal Reserve menolak bahwa sistem mereka diretas. Sekitar 250 bank sentral, sejumlah pemerintahan, dan institusi asing lainnya memiliki akun di New York Federal Reserve, yang merupakan salah satu pusat sistem transfer keuangan perbankan global yang dikenal dengan SWIFT (Society for Worldwide Interbank Financial Telecommunication). Selain Bank Sentral Bangladesh, industri perbankan di Ekuador, Filipina, Ukraina, dan Vietnam pun menjadi korban *malware* yang ditargetkan khusus untuk sistem SWIFT. Walau akhirnya mengakui terdapat kelemahan keamanan pada sistemnya, SWIFT menolak menanggung kerugian bank-bank yang menjadi korban. SWIFT melayani lebih dari 11.000 institusi keuangan di lebih dari 200 negara.



3

MENGENAL SANG PENGANCAM

"Kenali diri Anda, dan kenali musuh Anda, ..."
~ Sun Tzu

“ITU SEBABNYA SANGAT PENTING MEMILIKI STRATEGI KEAMANAN INFORMASI YANG SEJAK AWAL SUDAH MEMPERTIMBANGKAN BERBAGAI JENIS ANCAMAN DAN PENGANCAM.”

Gempa bumi tahun 2006 melumpuhkan koneksi Internet Indonesia ke dunia internasional akibat putusnya kabel serat optik bawah laut dekat *landing point* di Taiwan dan baru berangsur normal setelah 1 minggu. Banyak perusahaan Indonesia yang mengalami gangguan signifikan. Salah satunya adalah perusahaan yang menjadi pelanggan XecureIT. Kami sudah mengingatkan 6 bulan sebelum kejadian untuk memindahkan sebagian infrastrukturnya ke Indonesia. Ancamannya adalah kehilangan koneksi jaringan ke sistem yang kritikal. Pengancam langsungnya adalah bencana alam. Pengancam tidak langsungnya adalah pimpinan perusahaan yang melakukan pembiaran dengan mengabaikan kondisi yang sudah diidentifikasi berisiko tinggi.

ANCAMAN DAN PENGANCAM

Selain target (objek ancaman), pengancam (*threat agent*) merupakan faktor utama saat kita berdiskusi tentang ancaman yang dihadapi. Karena siapa pun berpotensi menjadi pencuri, maka ancaman pencurian akan selalu ada. Sehingga, sudah seharusnya beda profil pencuri, beda pula langkah-langkah pengamanannya. Kesalahan menentukan siapa pengancam potensial, salah pula strategi keamanannya sehingga menjadi tidak efektif dan/atau tidak efisien.

ANALOGI: PROFIL PENGANCAM PADA LOKASI PARKIR

Pengelola lokasi parkir seharusnya memiliki langkah pengamanan yang berbeda-beda sesuai dengan profil pengancamnya. Berikut ini adalah beberapa contoh profil orang-orang yang berpotensi menjadi pencuri.

- Pihak luar yang memiliki keahlian dasar mencuri kendaraan.

- Pihak luar yang memiliki kemampuan dan fasilitas pembuatan duplikat kunci elektronik.

- Petugas parkir, seperti satpam atau penjaga gerbang parkir.

- Orang yang memiliki akses ke komputerisasi sistem perparkiran.

- Manajemen pengelola parkir yang bisa memerintahkan karyawannya atau bahkan membuat kebijakan yang memperlemah keamanan.

- Pemilik kendaraan yang ingin mengambil keuntungan dari pihak asuransi.

- Komplotan pencuri yang memiliki kombinasi profil-profil tersebut.

Terdapat cukup banyak alternatif strategi untuk menangani contoh ancaman pencurian kendaraan bermotor yang dilakukan oleh berbagai macam profil pengancam tersebut.

Bagaimana dengan ancaman pencurian, perubahan dan/atau perusakan terhadap target bernama informasi? Sangat sedikit organisasi yang bisa memaparkan strategi keamanan informasi yang efektif jika dihadapkan pada kondisi yang

"menyakitkan" tetapi seringkali terjadi: Siapa pun bisa menjadi pengancam, termasuk Anda sebagai pimpinan, dan saya sebagai konsultan/auditor/ *penetration tester*.

Pengancam yang menimbulkan risiko besar umumnya memiliki:

a. Kemampuan "besar" untuk menyerang pihak lain, seperti peretas yang benar-benar ahli, kompetitor atau kejahatan terorganisir yang punya dana besar, atau pemerintah yang punya dana dan tidak tersentuh hukum.

b. Kekuasan "tinggi" di internal seperti pengelola sistem yang memiliki hak khusus di sistem dan pimpinan perusahaan atau pejabat pemerintah yang bisa menyalahgunakan kekuasaanya.

Bukan menuduh, tetapi saat menangani kasus-kasus *fraud* yang besar, beberapa kali saya menemukan ternyata ada pimpinan yang terlibat.

NILAI DARI INFORMASI

Berapa harga yang akan dibayar oleh pihak lain untuk mendapatkan informasi hasil penelitian dan pengembangan, strategi kampanye pemasaran produk baru, daftar *supplier*, harga penawaran, daftar kreditor, atau informasi berharga lainnya? Sebagai informasi, harga 1 set tape *backup* berisi data-data geologi pada tahap eksplorasi blok migas berada di kisaran ratusan ribu dolar AS. Harga 1 data nasabah kartu kredit yang diperjualbelikan di pasar gelap Internet berkisar antara 50 sen hingga 50 dolar AS. Jika sebuah bank memiliki 5 juta data nasabah seharga 1 dolar AS per nasabah, maka 1 set tape *backup*-nya bernilai sekitar 5 juta dolar AS.

Berapa nilai informasi pelanggan kartu kredit yang setiap bulan rutin membayar tagihan rata-rata di atas 20 juta rupiah, atau informasi pelanggan ponsel yang membayar tagihan rata-rata di atas 2 juta rupiah per bulan? Para produsen atau penjual produk barang mewah bersedia membayarnya dengan harga sangat tinggi.

Seandainya saya seorang pengusaha asing, dengan bantuan intelijen negara saya, berhasil mendapatkan informasi-informasi otentik tentang siapa saja pejabat negara, dan senator dari negara

konsumen produk perusahaan saya yang korupsi atau berselingkuh, saya dapat memengaruhi opini dan kebijakan mereka.

Saya yakin, Anda sebagai CEO pasti punya puluhan contoh lainnya.

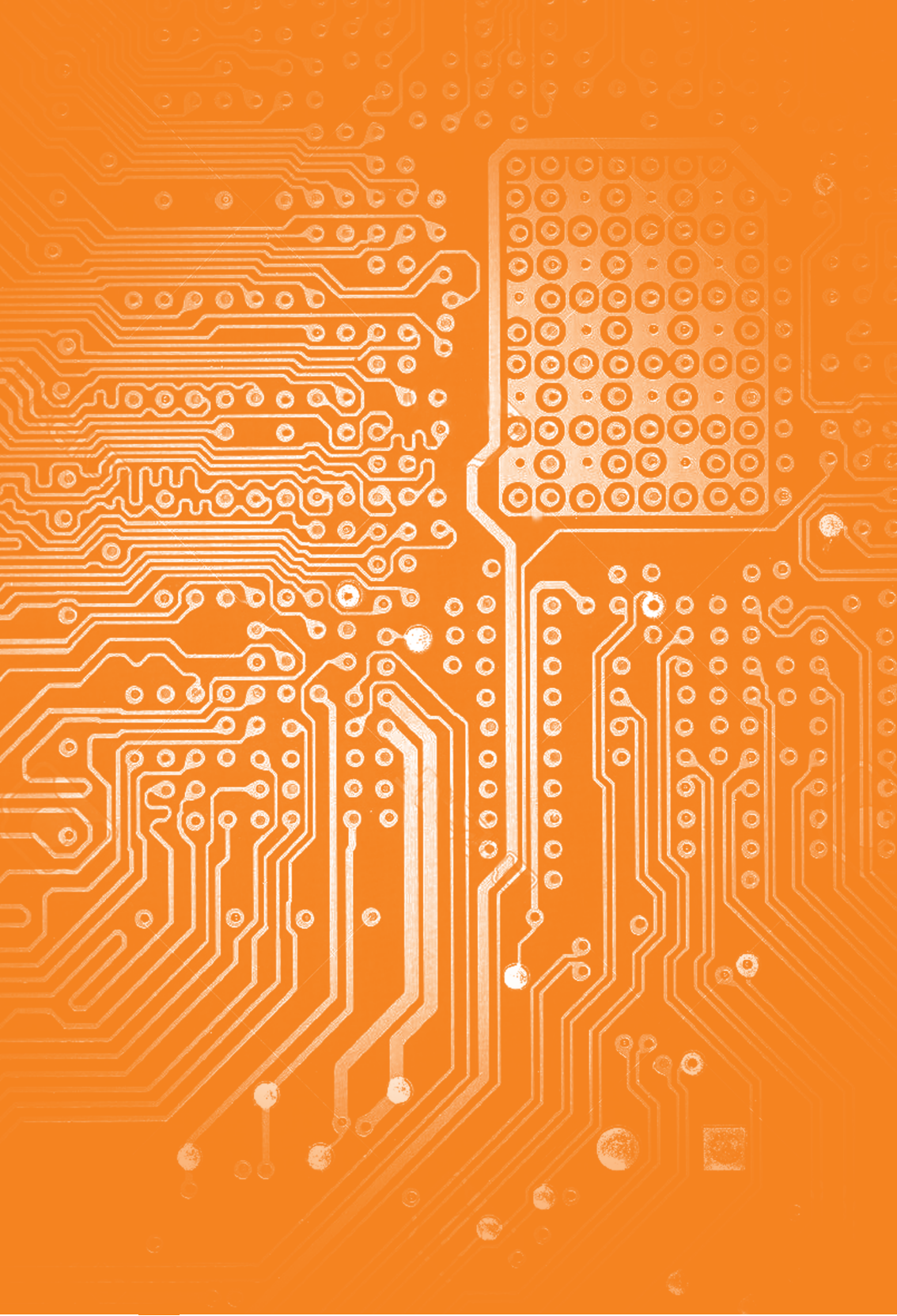
SEANDAINYA ANDA SEBAGAI PENGANCAM

Bagaimana jika agen pemerintah, manajemen (pemilik informasi), administrator sistem, manajer TI, atau manajer keamanan TI yang menjadi pengancam? Apakah Anda pernah berpikir bahwa pembuat sistem operasi, perangkat (keamanan) jaringan, aplikasi bisnis, solusi enkripsi, dan penyedia layanan TI juga berpotensi menjadi pengancam? Berapa banyak perusahaan TI kelas dunia yang juga menjadi "fasilitator" bagi pemerintah negaranya untuk mendapat informasi-informasi sensitif milik negara lain?

Saya ingin mengajak Anda ke situasi di mana Anda sendiri harus memilih, tetap loyal kepada perusahaan atau negara, atau berkomplot dengan pihak lain.

Seandainya, tugas Anda sebagai pengelola sistem *backup* di *data center*, kemudian ada seseorang yang menghubungi Anda dan memberi penawaran 1 miliar rupiah untuk meminjam 1 set tape *backup* tersebut selama 30 menit pada hari Jumat pukul 11.45, sambil menyebutkan apa yang sedang dilakukan anak, istri, atau ibu Anda saat ini, apa keputusan Anda?

Mungkin banyak dari Anda merasa kesulitan memberi jawaban. Jawaban saya sederhana; berikan saja yang diminta. Begitu saja, kok repot. Ketika saya dalam kondisi terancam dan dipaksa menjadi pengancam, demi alasan keselamatan, turuti saja. Itu sebabnya sangat penting memiliki strategi keamanan informasi yang sejak awal sudah mempertimbangkan berbagai jenis ancaman dan pengancam.



4

SECURITY BY OBSCURITY AKAN SELALU GAGAL

"Anda pikir Anda aman karena orang lain tidak tahu kunci Anda tersembunyi di bawah keset."

“DENGAN ALASAN KERAHASIAAN PRODUK, PIHAK PEMBUAT SERINGKALI BERANI MENGKLAIM AMAN SEKALIGUS MENOLAK MEJELASKAN SECARA DETAIL MEKANISME PENGAMANAN YANG DIMILIKI.”

Anda pikir Anda aman karena Anda tidak tahu kondisi sebenarnya?! Seperti dalam sebuah film Hollywood di mana sekelompok anak sekolah dengan riang bermain dan bernyanyi tanpa menyadari pasukan penjinak bom bertaruh nyawa di gudang bawah tanah menjinakkan bom yang dipasang teroris. Atau seperti penumpang yang dengan tenang tidur lelap dalam pesawat terbang yang tidak mendapat perawatan selayaknya karena alasan efisiensi sehingga setiap saat dapat gagal lepas landas, jatuh, atau gagal mendarat.

ILUSI KEAMANAN KAMAR HOTEL

Mungkin sudah hampir 100 hotel yang saya tinggali saat mengunjungi belasan negara di berbagai belahan dunia, dari hotel *budget* hingga bintang 5. Di setiap hotel saya selalu menguji keamanan kamar hotel dengan melakukan *social engineering attack* sederhana. Saya datang ke bagian penerima tamu meminta kunci kamar dengan alasan kunci yang sudah diberikan tertinggal di dalam kamar. Sekitar 70 persen penerima tamu akan langsung memberikan kunci pengganti hanya dengan menyebutkan nomor kamar dan nama tamu. Saya akan diantar pelayan dan dibukakan pintu jika hotel masih menggunakan kunci fisik. Hotel yang prosedurnya agak ketat, penerima tamu meminta kartu identitas atau paspor sebelum memberikan kunci pengganti. Saya hanya menjawab kalau dompet dan tas saya tertinggal di dalam kamar, dan kunci pengganti pun diberikan. Keamanan kamar hotel yang pernah saya tinggal, di mana semuanya hanya berdasarkan pada kombinasi nomor kamar dan nama tamu, terbukti 100 persen gagal.

Beberapa kali saat ada waktu luang, saya melakukan *social engineering attack* pada tamu hotel yang lain saat makan pagi. Menyapa selamat pagi, minta izin berbagi meja karena suasana cukup

padat. Belum sampai selesai makan pagi, saya sudah mengetahui namanya, asalnya dari negara mana, organisasi tempatnya bekerja, dan lain-lain. Menanyakan nomor kamar tindakan yang tidak sopan dan mencurigakan. Akan tetapi, menunggu sampai "target" selesai makan pagi, bersama-sama naik lift, turun di lantai yang sama, bersama-sama ke arah yang sama untuk mengintip nomor kamarnya adalah tindakan yang ramah dan menyenangkan. Seandainya saya mau melanjutkan ke tahap berikutnya dengan mendatangi bagian penerima tamu, Bingo!

Cara lain yang butuh sedikit kesabaran dan waktu adalah menunggu kamar dibersihkan. Ketika pintu kamar terbuka lebar, cukup mengucapkan selamat pagi kepada petugas pembersih kamar, saya pun bebas membuka koper, dan melakukan hal lainnya.

KE(TIDAK)AMANAN SAFE DEPOSIT BOX

Saya berusaha mengikuti kasus pencurian barang berharga pelanggan *Safe Deposit Box* (SDB) Bank International Indonesia (BII) sejak kuartal terakhir tahun 2008 lalu. Hingga akhirnya polisi secara resmi memublikasikan temuan mereka

di media massa. Menurut pemberitaan di harian *Kompas*, si penjahat dengan mudah membongkar pasang dengan obeng biasa dalam waktu yang amat singkat. Lebih parah lagi, menurut klaim si penjual saat menawarkan produknya, teknologi SDB yang sama digunakan di hampir seluruh SDB di Indonesia. Konon, kunci SDB dibuat dari metal khusus yang tidak mungkin diduplikasi, kecuali oleh pihak pembuat, sehingga aman 100 persen. Lalu siapa yang bertanggung jawab? Pada akhirnya dengan adanya klausul dalam sewa-menyewa SDB yang menyatakan bank tidak bertanggung jawab atas isi dari SDB, maka bank berhasil memindahkan risiko kepada penyewa SDB.

Beberapa tahun lalu, sebuah perusahaan akan membeli brankas sebuah merek terkenal di dunia. Saya diminta untuk "menemani". Si penjual dengan amat meyakinkan menjelaskan kalau produk tersebut memiliki serombongan sertifikasi A-Z dan tidak mungkin dibongkar. Saya pun bertanya, "Apa yang terjadi seandainya, karena berbagai hal, PIN-nya lupa dan kuncinya hilang? Apakah barang-barang di dalamnya tidak bisa dikeluarkan? Jika demikian, lebih baik membeli produk lain." Dengan gesit si penjual mengatakan kalau masalah itu pasti ada solusinya; dia memanggil teknisi senior, seorang bapak berambut putih. Dengan santai, namun pasti, teknisi

senior ini menjelaskan bahwa semua tipe brankas bisa dia bongkar. Penjelasannya lengkap dengan waktu dan perangkat apa saja yang dibutuhkan untuk membongkar spesifikasi brankas masing-masing, maksimum hanya dalam hitungan jam.

BACKDOOR PADA PRODUK TEKNOLOGI KEAMANAN SIBER

Pada tahun 2004, Cisco akhirnya mengakui bahwa terdapat *backdoor* berupa sebuah *username* lengkap dengan *password*-nya yang tidak dapat dimatikan dan memberikan kontrol penuh ke piranti lunak CiscoWorks Wireless LAN Solution Engine (WLSE) dan Hosting Solution Engine (HSE). CiscoWorks WLSE merupakan pusat pengelolaan perangkat infrastruktur nirkabel Cisco yang digunakan pelanggan, termasuk untuk melakukan pengaturan keamanan jaringan nirkabel.

Pada tahun 2013, ditemukan akun untuk mengakses perangkat *firewall* dan perangkat VPN buatan Barracuda Networks. Perangkat *firewall* adalah gerbang keamanan siber untuk mem-*filter* koneksi jaringan. Perangkat VPN (Virtual Private Network) digunakan untuk mengenkripsi (mengacak data) lalu lintas jaringan agar tidak dapat dibaca pihak yang tidak berhak.

TRUST BUT VERIFY

Dengan alasan kerahasiaan produk, pihak pembuat seringkali berani mengklaim aman sekaligus menolak mejelaskan secara detail mekanisme pengamanan yang dimiliki. Kecuali bisa dijelaskan secara ilmiah, hal seperti ini yang dikenal dengan istilah *snake oil*. Minyak ular yang bisa menyembuhkan 1002 macam penyakit.

Percaya mentah-mentah pada orang bergaya seperti penjual minyak ular adalah kesalahan fatal yang dilakukan oleh seorang profesional pengamanan informasi karena tidak melakukan prinsip *trust but verify*. Seperti yang juga terjadi pada berbagai kasus terkait keamanan informasi, arsitek, pengambil keputusan, dan pengguna tanpa sadar mengambil keputusan yang tidak tepat karena informasi yang cenderung menyesatkan dari suatu produk atau layanan teknologi keamanan.

5

KESALAHAN FOKUS PENGAMANAN INFORMASI

"Bagai sebuah foto keluarga yang salah fokus. Foto wajah keluarga menjadi buram. Foto latar belakang menjadi tajam."

“WAJAR” JIKA SISTEM TEKNOLOGI INFORMASI DIJAMIN AMAN, NAMUN PENCURIAN INFORMASI, MANIPULASI TRANSAKSI, DAN PERUSAKAN INFORMASI TERUS TERJADI.

Apa yang seharusnya dilindungi, sistem teknologi informasi atau informasinya? Menurut pendapat saya, yang seharusnya dilindungi adalah informasi. Memastikan keamanan teknologi informasi hanya salah satu cara untuk melindungi informasi. Perbedaannya memang sangat tipis sehingga tidak mengherankan sebagian orang bingung dan kerapkali menimbulkan perdebatan dalam menentukan strategi keamanan siber dan informasi. Karena perbedaan yang sangat tipis ini strategi keamanan yang diterapkan seringkali salah fokus sehingga menguntungkan penjahat.

Saat ini nyaris tidak ada informasi yang tidak diproses melalui teknologi informasi. Bahkan

pepatah, “Hanya Tuhan yang tahu” berubah menjadi, “Bukan lagi hanya Tuhan yang tahu.” Memfokuskan pengamanan pada teknologinya, bukan pada informasinya, sangatlah berbahaya. Strategi keamanan juga menjadi tidak efektif. Sehingga, walaupun anggaran teknologi pengamanan berbiaya tinggi terus dikeluarkan, penjahat tetap mudah melakukan pencurian, perusakan, atau perubahan terhadap informasi yang dilindungi.

FOKUS PENGAMANAN YANG TEPAT

Untuk mempermudah pemahaman, saya mau menggunakan Pasukan Pengamanan Presiden (Paspamres) sebagai contoh. Apa yang menjadi fokus pengamanan oleh Paspamres? Fasilitas kepresidenan (mobil, tempat tinggal, kantor) atau Presiden? Mengapa Paspamres menjaga fasilitas kepresidenan terus-menerus, 24 jam x 7 hari? Padahal, jika presiden berkunjung ke suatu tempat, Paspamres hadir hanya pada saat sebelum Presiden tiba untuk melakukan sterilisasi dan ketika presiden berada di lokasi.

Paspamres fokus melakukan pengamanan terhadap Presiden. Paspamres mengamankan fasilitas-fasilitas kepresidenan, atau tempat yang dikunjungi Presiden dalam konteks mengamankan

Presiden. Namun, karena Presiden sering menggunakan fasilitas-fasilitas kepresidenan, Paspamres tidak mau setiap kali kerepotan harus melakukan sterilisasi. Sehingga, fasilitas-fasilitas tersebut dijaga dan dipastikan integritasnya terus-menerus. Perlakuan yang berbeda dengan lokasi yang hanya dikunjungi sesekali oleh Presiden.

Berikut contoh kasus nyata kerugian yang ditimbulkan akibat fokus pengamanan pada teknologi surat elektronik (surel), tetapi lupa melakukan pengamanan informasi yang diproses menggunakan surel.

Beberapa waktu lalu, saya diminta seorang pimpinan perusahaan untuk melakukan investigasi kasus *wire transfer fraud* dengan menyalahgunakan (surel) yang mengakibatkan kerugian lebih dari 1 juta dolar AS. Selain kerugian keuangan, perusahaan tersebut nyaris saling menggugat secara pidana, dan kehilangan mitra bisnis yang selama ini saling menguntungkan. Kedua pihak sama-sama mengeluarkan bukti bahwa teknologi pengamanan surat elektronik mereka aman.

Modusnya sangat sederhana. Perusahaan A membeli produk Perusahaan B. Dalam berkomunikasi

menggunakan surel, Perusahaan A diwakili oleh Bapak AA, dan Perusahaan B diwakili oleh Bapak BB. Saat pembayaran jatuh tempo, AA menerima surel palsu yang seolah-olah dikirimkan oleh BB. Begitu miripnya, termasuk gaya bahasa penulisan pun mirip. Surel tersebut menyatakan bahwa rekening bank yang biasa digunakan bermasalah, dan diminta untuk melakukan pembayaran ke rekening bank yang baru.

AA merasa curiga dan meminta konfirmasi ke BB melalui layanan pesan singkat. BB menjawab, "Gunakan saja rekening bank yang terakhir." Selama beberapa tahun bertransaksi, Perusahaan B memang pernah mengganti rekening bank. Sehingga, AA berasumsi bahwa surel palsu tersebut benar, dan dia melakukan transfer dana ke rekening baru sesuai informasi di surel. Setelah ditunggu beberapa hari, transfer dana senilai 1 juta dolar AS tidak pernah diterima Perusahaan B.

Pimpinan Perusahaan A sempat akan melaporkan karyawannya AA ke polisi dengan tuduhan penggelapan uang perusahaan. AA juga berniat melaporkan BB dengan tuduhan penipuan. Perusahaan B juga sudah mensomasi Perusahaan A untuk segera melakukan pembayaran. Tim TI

Perusahaan B juga sempat dicurigai terlibat kejahatan tersebut.

SALAH FOKUS

Ini bukan kasus pertama yang saya tangani. Tahun sebelumnya paling tidak ada 3-4 kasus serupa. Paling tidak ada 12 kasus yang saya ketahui sejak tahun 2012 dengan nilai kerugian bervariasi.

Menggunakan contoh kasus di atas, kesalahan tim teknologi informasi adalah memberi kesan kepada pimpinan bahwa jika anggaran teknologi pengamanan *e-mail* disetujui, teknologinya dibeli dan diterapkan maka *e-mail* akan aman. Karena hanya mengerti teknologi, tim teknologi informasi tidak bisa menyampaikan seluruh informasi bahwa masih banyak risiko keamanan terkait penggunaan teknologi *e-mail*. Hal tersebut harusnya dipahami oleh dan menjadi tanggung jawab pengguna. Hebatnya, para penjahat memiliki kerja sama tim yang solid sehingga mereka mengerti teknologi dan proses bisnis yang kemudian membuat strategi untuk melaksanakan tindak kejahatan. Penjahat fokus pada informasinya.

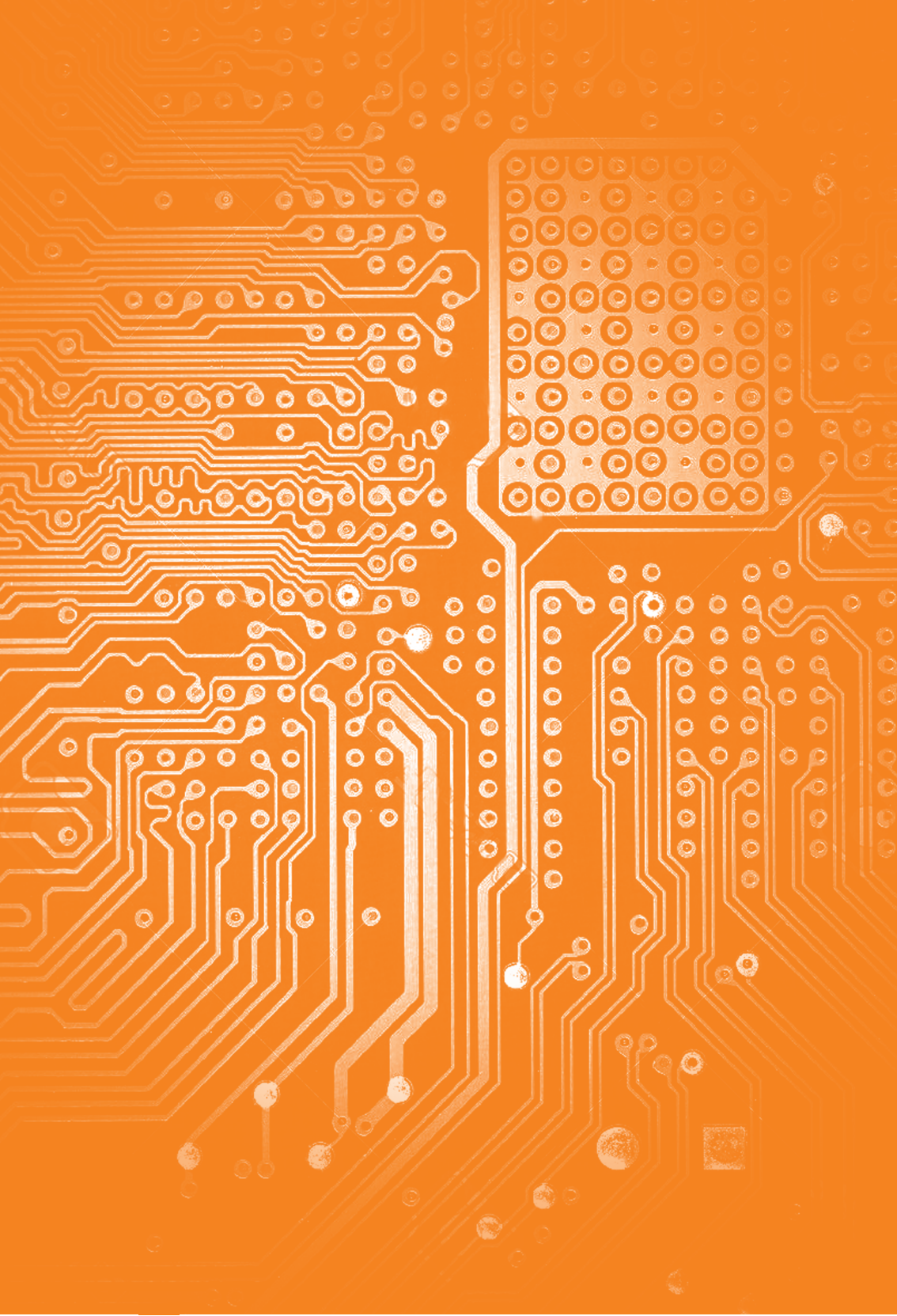
Salah fokus pengamanan seperti contoh di atas terjadi juga pada hampir seluruh strategi keamanan informasi yang saya ketahui. Pada banyak organisasi, tim keamanan informasi berada di bawah bagian teknologi informasi, sehingga namanya pun Tim Keamanan Teknologi Informasi. Maka, menjadi "wajar" jika yang menjadi fokus perlindungan oleh tim tersebut adalah teknologi informasinya. Sesuai dengan tugas dan tanggung jawabnya, tim teknologi informasi melaksanakan pemeliharaan dan mengamankan teknologi, bukan informasi. "Wajar" jika sistem teknologi informasi dijamin aman, namun pencurian informasi, manipulasi transaksi, dan perusakan informasi terus terjadi.

ANDA YANG SALAH

Kesalahan fokus pengamanan tersebut bukan hanya menjadi kesalahan tim teknologi informasi. Kesalahan utama justru dilakukan oleh para pengambil keputusan. Mereka menyerahkan pengamanan informasi kepada tim teknologi informasi yang tidak paham nilai, ancaman, dan siapa yang akan menjadi pengancam terhadap aset yang sangat berharga, bernama informasi.

Kesalahan utama dari sisi organisasi terletak pada pimpinan yang tidak mengangkat seseorang yang kompeten dan berintegritas untuk bertanggung jawab mengamankan informasi perusahaan (sering dikenal sebagai Chief Information Security Officer/ CISO), serta memberi wewenang dan sumber daya yang cukup kepadanya. Seorang CISO harus mengerti isu-isu keamanan teknologi informasi, dan paham ancaman, celah-celah keamanan dalam proses bisnis dan dampak yang dapat ditimbulkan terhadap bisnis.

Strategi keamanan informasi harusnya dirancang oleh orang-orang yang mengerti bisnis baik di tingkat perusahaan, maupun negara.



6

KERANCUAN DALAM MENENTUKAN PRIORITAS ASPEK KEAMANAN INFORMASI

“KESALAHAN MENENTUKAN PRIORITAS UTAMA ASPEK KEAMANAN INFORMASI DALAM SEBUAH KONTEKS PROSES BISNIS BERAKIBAT KESALAHAN DALAM MEMBUAT STRATEGI KEAMANAN INFORMASI.”

Pernahkah Anda mendengar dalam seminar, lokakarya, atau *focus group discussion*, sebuah lelucon berikut untuk mencairkan suasana: "Informasi dalam komputer yang aman adalah dicabut listriknya, cabut kabel jaringannya, masukkan ke dalam brankas, dirantai, masukkan ke dalam bunker 20 meter di bawah tanah, jalan masuknya ditimbun, kemudian dijaga oleh tentara bersenjata."

Lelucon, yang menurut saya pribadi, konyol dan merusak pola pikir karena aspek keamanan informasi direduksi menjadi hanya aspek kerahasiaan. Padahal, salah satu kunci utama keberhasilan strategi keamanan informasi adalah menentukan aspek keamanan informasi manakah yang menjadi prioritas utama.

3 ASPEK KEAMANAN INFORMASI

Ada beberapa teori mengenai aspek-aspek keamanan informasi. Namun, jika dikelompokkan maka terdapat 3 aspek (dasar) keamanan informasi, yaitu integritas, kerahasiaan, dan ketersediaan.

- **Aspek Integritas**

Aspek integritas memastikan kebenaran informasi, serta proses perubahan informasi dilakukan secara sah. Ancaman terhadap integritas adalah perubahan atau modifikasi tanpa memenuhi kondisi yang sah tersebut. Keautentikan, akuntabilitas, dan nirsangkal (*non-repudiation*) juga dapat dikelompokkan ke dalam aspek integritas. Misalnya, saat seseorang menyangkal telah melakukan hal tertentu, dibutuhkan proses untuk memastikan kebenaran pengakuan (informasi) tersebut.

- **Aspek Kerahasiaan**

Aspek kerahasiaan yaitu proses pembacaan informasi dilakukan secara sah. Ancaman terhadap kerahasiaan yaitu kebocoran informasi di mana informasi dibaca tanpa memenuhi kondisi yang sah.

- **Aspek Ketersediaan**

  Aspek ketersediaan yaitu informasi tersedia saat dibutuhkan, serta penghapusannya dilakukan secara sah. Ancaman terhadap ketersediaan yaitu, tidak dapat dibacanya informasi, penghapusan, atau pemusnahan tanpa memenuhi kondisi yang sah. Namun kapasitas, kinerja, dan keandalan juga dapat dikelompokkan ke dalam aspek ketersediaan.

Ketiga aspek tersebut selalu ada dalam satu konteks pengamanan informasi, dan saling terkait satu dengan yang lain. Namun, dalam kehidupan sehari-hari, seringkali timbul benturan kepentingan, aspek mana yang akan diutamakan: kerahasiaan, integritas, atau ketersediaan.

PROSES YANG SAH

Proses perubahan, pembacaan, atau penghapusan informasi dinyatakan sah jika dilakukan hanya oleh orang yang berhak, DAN hanya melalui proses yang telah disetujui, DAN hanya menggunakan perangkat yang telah disetujui, DAN hanya dengan kondisi fisik yang telah disetujui.

Saya memiliki brankas untuk menyimpan informasi dalam bentuk surat-surat berharga (akte lahir, ijazah, dan lain-lain). Anak saya berhak membuka brankas tersebut dan membaca informasi di dalamnya dengan cara memasukkan PIN dan kunci yang benar di lokasi penyimpanan brankas. Namun, jika dia membawa keluar rumah dan membuka brankas tersebut dengan linggis maka proses tersebut menjadi tidak sah, sehingga sulit dibedakan dengan pencuri.

KEBINGUNGAN MENENTUKAN PRIORITAS ASPEK KEAMANAN INFORMASI

Sebagai nasabah yang memercayakan uang untuk disimpan oleh bank, mana yang lebih penting bagi Anda? (a) Saldo tidak berubah, atau (b) Saldo tidak diketahui pihak lain.

Saya cukup sering melakukan "survei" cepat dengan menanyakan hal ini kepada peserta ketika saya menjadi narasumber seminar, lokakarya, atau pelatihan terkait keamanan informasi. Jawaban lebih dari 90 persen peserta adalah: (a) lebih penting saldo tidak berubah.

Mayoritas nasabah lebih mementingkan integritas. Saya pun demikian. Bagaimana dengan Anda?

Bandingkan jawaban Anda sebagai nasabah dengan strategi pada industri perbankan di Indonesia dalam mengamankan informasi nasabah. Strategi tersebut diatur sangat jelas dalam Undang-Undang Perbankan No.10 Tahun 1998.

Undang-Undang yang menimbulkan dampak terstruktur, sistemik, dan masif (TSM) bagi strategi keamanan informasi industri perbankan di Indonesia hanya membahas aspek kerahasiaan. Tidak ditemukan satu pun kata integritas, atau kalimat yang menggambarkan pentingnya integritas transaksi dan saldo nasabah di dalam undang-undang tersebut. Apakah berarti aspek integritas tidak penting bagi para pembuat kebijakan? Jika penting, mengapa tidak diatur?

Sehingga, jangan heran jika terlalu banyak kasus yang berakar pada masalah aspek integritas (sistem diretas, transaksi palsu, dan lain-lain) yang berdampak kerugian dipihak nasabah. Parahnya kasus-kasus tersebut cenderung dirahasiakan oleh pelaku bisnis dengan dukungan regulator, demi

melindungi reputasi bank sehingga menciptakan rasa aman semu, yang justru menguntungkan penjahat.

Bank melakukan pengurangan risiko dengan mengimplementasikan teknologi kata sandi sekali pakai (*one time password*/OTP). Beberapa bank memilih mengirimkan kata sandi melalui SMS yang secara teknologi tidak ada pelindungan kerahasiaan dan tidak ada jaminan kerahasiaan dari operator telekomunikasi. Jika di dalam kebijakan keamanan internal bank disebutkan kata sandi (*password*) harus dipastikan kerahasiaanya, mengapa kata sandi yang digunakan nasabah (eksternal) dikirim "telanjang"?

Secara umum, prosedur keamanan di industri perbankan untuk memastikan integritas lebih tinggi dibanding industri telekomunikasi. Penjahat tahu persis hal ini. Sehingga, dalam sebuah kasus perampokan uang nasabah sebesar 245 juta rupiah dari rekening Bank Permata pada tanggal 24 Agustus 2014, penjahat memanfaatkan kelemahan proses penggantian kartu SIM yang teknik dasarnya dikenal dengan nama *SIM Swop Attack*.

Seseorang dengan surat kuasa palsu dan fotokopi KTP milik korban mendatangi GraPari, kantor layanan pelanggan Telkomsel untuk

meminta penggantian kartu SIM. Setelah dengan mudah mengelabui petugas di GraPari, penjahat menghubungi layanan pelanggan Bank Permata dan berhasil melakukan proses *password reset*, dan menggunakan OTP yang dikirimkan ke SIM "curian" untuk melakukan beberapa transaksi ke 3 bank berbeda.-

SIM Swop Attack adalah teknik serangan kuno yang harusnya telah diperhitungkan sejak awal pasti terjadi dan telah terjadi, tetapi terkesan diabaikan oleh industri perbankan sehingga cukup sering terjadi. Salah satu kasus pembobolan rekening bank dengan teknik ini telah muncul ke permukaan tahun 2008 yang menimpa nasabah bank di Afrika Selatan.

Industri perbankan berasumsi industri telekomunikasi menjamin integritas dan kerahasiaan. Banyak proses identifikasi dan autentikasi transaksi perbankan elektronik berdasarkan nomor telepon, dan/atau layanan SMS. Industri perbankan berasumsi ponsel, nomor telepon, dan SMS aman. Betul aman, hanya beda "definisi" alias beda prioritas aspek keamanannya. Industri telekomunikasi memprioritaskan aspek ketersediaan dalam bisinisnya, sedangkan industri perbankan memprioritaskan kerahasiaan. Kondisi ini

seperti bermimpi indahnya menyatukan "minyak dan air" dengan mudah tanpa koordinasi erat. Sehingga, dalam kehidupan nyata: penjahat diuntungkan, dan nasabah dirugikan.

URUTAN PRIORITAS ASPEK KEAMANAN INFORMASI DALAM KEHIDUPAN NYATA

Lupakan sementara tentang teori-teori yang pernah Anda ketahui. Mari kita hidup dalam kenyataan dalam melakukan manajemen risiko, karena para penjahat tidak berteori. Tanyakan dan simulasikan kondisinya dalam diri Anda sendiri, pada umumnya, aspek mana yang (kemungkinan besar) akan menjadi prioritas dalam kegiatan yang Anda jalankan.

Bagi tentara Pembebasan Macan Tamil Eelam di Sri Lanka, kerahasiaan informasi adalah prioritas utama. Sehingga, mereka lebih baik mati memakan sianida daripada harus tertangkap, disiksa, dan berisiko membongkar rahasia. Dalam hal ini, aspek ketersediaan nyawa prajurit bukanlah prioritas.

Bagi saya pribadi, secara umum, aspek integritas menjadi prioritas utama. Bagaimana mungkin saya bisa menjamin kerahasiaan informasi pelanggan

XecureIT, jika orang-orang di tim XecureIT yang mengelola informasi tersebut tidak dapat dipercaya (integritasnya bermasalah).

Saya lebih memilih dompet saya hilang di dalam kamar karena pintu dibongkar paksa, dibandingkan saat bangun pagi tiba-tiba ada uang di samping tempat tidur namun kamar masih terkunci, dan tidak ada yang mengaku dan mengetahui siapa yang meletakan uang tersebut.

Suatu malam sekitar pukul 11, setelah selesai berdiskusi dalam kegiatan Komunitas Keamanan Informasi yang diberi nama Security Night, kami masih melanjutkan diskusi urutan prioritas ini. Paling tidak ada 4 orang yang memiliki sertifikasi Certified Information Systems Security Professional (CISSP) yang diakui secara *de facto* oleh komunitas Internasional. Satu orang akan pulang naik taksi, dan tetap berpegang teguh bahwa ketersediaan menjadi prioritas utama. Kami menguji konsistensinya dengan cara, apakah dia akan menaiki taksi kosong apa pun yang melintas?

Ternyata setelah 3 taksi kosong lewat, tidak ada satu pun taksi diberhentikannya. Setelah ditanya, mengapa dibiarkan lewat, dia menjawab, “Saya tidak

percaya terhadap keamanan taksi merek-merek yang baru saja lewat." Akhirnya dia sepakat bahwa, aspek integritas merupakan prioritas utama.

KERANCUAN PENGGUNAAN ISTILAH

Kita seringkali membaca berita, artikel, atau buku yang menulis "...informasi hilang..." atau "... informasi dicuri...".

Ketika informasi (kemungkinan) dibaca secara tidak sah, namun informasinya masih ada (tidak hilang) dalam media penyimpan (*harddisk*, *flash disk*) yang kita miliki dan dapat kita akses, maka yang terkompromi adalah aspek kerahasiaan. Lain halnya jika informasi tidak dapat kita akses maka yang terkompromi adalah aspek ketersediaan.

Berkas-berkas elektronik yang berisi informasi dapat dimunculkan kembali ketika tanpa sengaja kita memformat *flash disk*. Saat laptop hilang dicuri dan saat bersamaan kita lupa *password* dari akun media penyimpan daring (dalam jaringan/*online*) tempat kita menyimpan cadangan berkas-berkas dari *laptop* tersebut, sebenarnya informasi tidak hilang (masih ada dalam sistem), hanya tidak dapat kita akses (tidak tersedia).

KERANCUAN ANTARA ASPEK KEAMANAN INFORMASI VERSUS PROSES KONTROL KEAMANAN INFORMASI

Identifikasi, autentikasi, dan otorisasi merupakan sebagian proses-proses kontrol keamanan informasi, bukan aspek keamanan informasi.

Proses identifikasi dan autentikasi dapat dikelompokkan ke dalam aspek integritas. Misal, saat pengguna *login* ke dalam sistem dan mengaku bernama A, dibutuhkan proses untuk memastikan kebenaran pengakuan tersebut.

Proses otorisasi dapat terkait dengan aspek integritas, kerahasiaan, dan atau ketersediaan.

KERANCUAN ANTARA SENSITIF DAN KRITIS

Banyak pihak mencampuradukkan penggunaan kata kritikal dan kata sensitif yang membuat saya bingung. Terutama saat ada kebijakan, buku atau artikel yang menuliskan informasi kritis. Pengalaman saya selama lebih dari 20 tahun terkait keamanan informasi, lebih memahami bahwa sensitif menekankan aspek integritas dan/atau kerahasiaan, sedangkan kritikal menekankan aspek ketersediaan. Menurut pendapat saya, lebih tepat

jika dituliskan informasi sensitif. Kata sensitif kurang tepat digunakan dalam konteks infrastruktur kritis nasional.

Infrastruktur kritis nasional adalah infrastruktur yang tingkat ketersediannya harus tinggi, seperti telekomunikasi, listrik, air minum, dan perbankan. Namun, konten dari infrastruktur tersebut memiliki aspek yang berbeda. "Konten" dalam infrastruktur listrik dan air minum tidak rahasia, namun butuh integritas tinggi karena bisa merusak perangkat elektronik atau meracuni manusia. Konten dalam infrastruktur telekomunikasi tidak dijamin kerahasiaannya, hanya penyadapan harus sesuai dengan UU Telekomunikasi. Konten infrastruktur perbankan bersifat sensitif dalam arti aspek kerahasiaan menurut UU Perbankan dan aspek integritas menurut (mayoritas) nasabah.

Berbagai kerancuan tersebut di atas berakibat fatal. Kesalahan menentukan prioritas utama aspek keamanan informasi dalam sebuah konteks proses bisnis berakibat kesalahan dalam membuat strategi keamanan informasi. Lebih fatal lagi, banyak proses bisnis yang bergantung dengan pihak lain, dan berasumsi pihak lain tersebut memiliki prioritas aspek keamanan yang sama.

7

ILUSI SITUS WEB TIDAK BUTUH PENGAMANAN YANG LAYAK

"Di dunia siber, Anda adalah situs web Anda."

“SELAIN BERISIKO TINGGI TERINFEKSI MALWARE, INFORMASI SENSITIF PARA PENGGUNA JUGA MENJADI TARGET PERETAS.”

"Apa benar butuh pengamanan serius? Paling-paling hanya diubah tampilannya (*deface*). Lagipula yang ada di situs *web* tidak ada yang rahasia. Akun media sosial juga tidak sensitif." Pertanyaan klasik yang sering saya dengar. Pernyataan yang dapat dipahami karena sebagian besar pimpinan memang tidak sadar berbagai potensi ancaman yang ada.

KEBOCORAN RAHASIA YANG BELUM DIPUBLIKASIKAN

Saham Twitter di New York Stock Exchange tiba-tiba anjlok 17,4 persen pada akhir April 2015. Penyebabnya yaitu firma *market-intelligence* Selerity

memublikasikan informasi sensitif satu jam lebih cepat dari rencana. Informasi bahwa penghasilan Twitter tidak mencapai target pada kuartal pertama tahun 2015 dipublikasikan *via* layanan Twitter.

Sumber:http://mashable.com/2015/04/28/twitter-tops-300-million-users/

Selerity tidak melakukan peretasan. Perusahaan layanan *investor relations* Shareholder.com yang dikontrak Twitter sedang menyiapkan materi publikasi kabar tersebut pada situs *web*-nya. Pada saat yang bersamaan, informasi yang telah siap publikasi tersebut ditemukan oleh penggerayang *web* (*web crawler*) milik Selerity. Penggerayang *web* tersebut secara otomatis dan terus-menerus mencari berbagai informasi di Internet terkait perusahaan-

perusahaan yang diperdagangkan di bursa saham. Ironis, saham Twitter anjlok akibat informasi yang dipublikasikan menggunakan layanannya sendiri, akibat ketidakamanan perusahaan yang layanannya disewa Twitter.

Otomatisasi pada aplikasi perdagangan saham telah berevolusi. Prinsip siapa cepat dia kaya, siapa lambat dia bangkrut menghasilkan proses otomatisasi perdagangan saham yang luar biasa cepat. Otomatisasi suka atau tidak suka harus dilakukan karena tidak mungkin lagi dilakukan manusia. Aplikasi secara otomatis mengerayangi (*crawling*) seluruh informasi dari berbagai situs *web* (atau layanan *web*), seperti Twitter, situs *web* perusahaan, perusahaan *public relation*, bursa saham, bank sentral, dan situs resmi pemerintah yang dapat dijadikan acuan analisis otomatis berbasis kecerdasan buatan.

Para pengambil keputusan cukup memiliki kerangka berpikir yang benar dalam menentukan prioritas aspek keamanan informasi (Bab 6 Kerancuan dalam Menentukan Prioritas Aspek Keamanan Informasi) agar keputusan yang diambil menghasilkan dampak positif, serta mengurangi dampak negatif pada saat yang bersamaan.

INTEGRITAS INFORMASI

Pada Mei 2010, Dow Jones Industrial Average terjun 600 points dalam 5 menit dan ditutup dengan kerugian 348 points. Pada bulan April 2015, pemerintah Amerika Serikat memidanakan seorang *futures trader* karena dianggap memanipulasi pasar komoditas dengan menggunakan aplikasi otomatis.

April 2013, Wall Street panik, Dow Jones Industrial Average jatuh 143 points, karena akun Twitter milik Associated Press diretas kemudian memberitakan bahwa terjadi ledakan di White House yang mencelakai Barack Obama.

Mei 2015, saham Avon Products meningkat 20 persen setelah situs *web* Securities and Exchange Commission (SEC) mengumumkan berita palsu bahwa sebuah perusahaan investasi akan membeli perusahaan kosmetik yang penjualan dan penghasilannya sedang tersebut sebesar 8 miliar dolar AS.

Layanan *web*, termasuk situs, *web* merupakan sarana penyebaran informasi yang cepat dan effektif. Sebuah skenario serangan yang disusun rapi dapat digunakan untuk membuat goyah sebuah

perusahaan atau menggoyang perekonomian sebuah negara.

Saat krisis keuangan terjadi, bukan hal mustahil tiba-tiba seluruh nasabah menarik uang beramai-ramai dari salah satu bank. Hal ini sangat mungkin terjadi hanya karena penyerang yang berhasil membajak situs *web* bank tersebut menyisipkan informasi rahasia palsu bahwa bank terkena sanksi dan akan dibekukan transaksinya oleh Bank Indonesia dalam beberapa hari ke depan.

KEAMANAN PENGUNJUNG DAN PENGGUNA SITUS

Tanggal 8 Juli 2011, Microsoft mengonfirmasikan bahwa situs Microsoft Safety & Security Center telah diretas dan dimanfaatkan penjahat siber. Situs tersebut digunakan untuk mengirimkan konten porno dan *malicious software (malware)*. Menariknya baru beberapa hari sebelumnya, John Howie, Senior Director of Online Services Security and Compliance Governance di Microsoft, mengatakan bahwa Microsoft sangat tidak mungkin diretas karena selalu menambal celah keamanan pada sistem, tidak seperti perusahaan RSA atau Sony.

Pada awal 90-an, berselancar di Internet adalah bertamu, mengunjungi situs-stus yang diinginkan. Sepuluh tahun kemudian kondisi sudah berubah. Proses sesungguhnya saat mengunjungi sebuah situs *web* adalah mengundang, memanggil aplikasi milik situs yang dikunjungi untuk dijalankan di komputer pengunjung. Analoginya, dahulu kita mengunjungi toko saat berbelanja. Sekarang kita mengundang pelayan toko datang dan masuk ke dalam rumah kita. Jika dia sakit atau jahat, maka kita dengan mudah terinfeksi atau menjadi korban kejahatannya.

Risiko besar mengancam para pengunjung situs-situs resmi yang berhasil disisipi *malware*, baik milik pemerintah, perusahaan, situs berita, atau *e-commerce. Malware* dapat melakukan berbagai aktivitas pada komputer, termasuk ponsel pengunjung yang terinfeksi, antara lain:

- Mengganti aplikasi *mobile banking*, atau *mobile commerce* asli dengan yang palsu.
- Menyisipi *malware* lain ke dalam *browser*, atau bahkan mengganti *browser* dengan yang menyerupai *browser* tersebut.
- Memasang *keylogger* atau *screen logger* atau piranti lunak penyadapan lainnya.

- Mengenkripsi file-file milik korban dan meminta uang tebusan sebagai ganti kunci enkripsi yang diberikan.

- Menguasai sepenuhnya komputer korban sehingga dapat dikendalikan dari Internet tanpa diketahui pemiliknya.

Akibatnya, para penjahat siber dapat dengan mudah:

→ Mencuri akun Gmail, Yahoo, Facebook, atau Internet Banking korban;

→ Menyadap percakapan, serta aktivitas pribadi lainnya menggunakan mikrofon dan kamera pada komputer atau ponsel korban;

→ Mencuri atau mengubah atau menghapus informasi milik korban;

→ Menjadikan komputer tersebur sebagai robot (*bot/zombie*) yang merupakan bagian dari jaringan robot (*botnet*) untuk menyerang sistem komputer lainnya, termasuk mengirim *e-mail* sampah, melumpuhkan sistem pihak lain, atau kejahatan lainnya,

sesuai perintah sang penggembala robot (*bot herder*).

Selain berisiko tinggi terinfeksi *malware*, informasi sensitif para pengguna juga menjadi target peretas. Tahun 2010, sistem komputer milik Nasdaq diretas, dan dipasangi *malware* untuk memata-matai komunikasi antar-para direktur dan para komisaris perusahaan-perusahaan publik. Penjahat siber berhasil meretas layanan *web online* yang diberi nama Directors Desk, yang digunakan oleh para pimpinan perusahaan untuk bertukar informasi sensitif dan melakukan rapat *online*.

SEBAGAI PROXY YANG DIGUNAKAN UNTUK MENYERANG SISTEM PIHAK LAIN

Komputer juga merupakan senjata. Sebagai analogi, jika seorang pemilik senjata lalai mengamankan senjata yang dimiliki, dan senjatanya digunakan pihak lain untuk membunuh, kemungkinan besar si pemilik senjata yang akan menjadi tersangka pelaku pembunuhan tersebut. Di dunia siber, hal serupa bisa saja terjadi antar perusahaan atau bahkan negara yang berkompetisi.

Apa yang terjadi seandainya *server web* milik Kementerian Pertahanan Indonesia dibajak pihak lain dan digunakan untuk menyerang jaringan Department of Defense Amerika Serikat dan mengacaukan sistem kelistrikan milik Malaysia? Dalam konteks perang *cyber*, menggunakan sistem negara lain untuk menyerang musuh adalah hal lumrah. Hal ini dikenal dengan istilah perang *proxy*.

Perang *proxy* di ranah siber dapat berimplikasi sangat luas. Sebagai contoh, dalam sebuah dokumen yang dikeluarkan Gedung Putih tahu 2011 berjudul *International Strategy for Cyberspace* yang ditanda-tangani oleh Presiden Amerika Serikat, Barack Obama, tertulis bahwa serangan siber terhadap kepentingan Amerika Serikat dan sekutunya dapat direspon baik secara diplomatik, ekonomi, maupun militer.

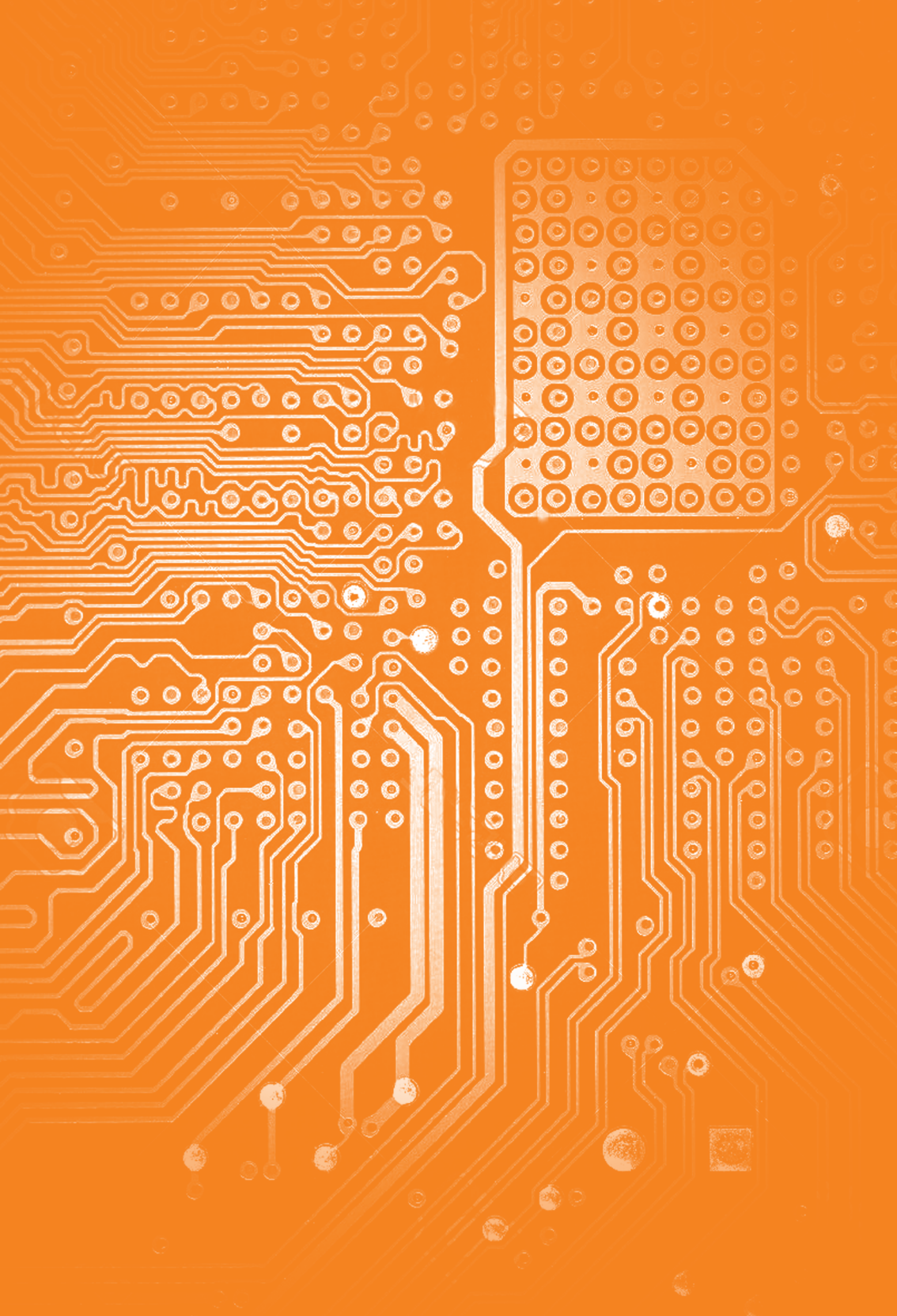
> *"...the United States will respond to hostile acts in cyberspace as we would to any other threat to our country All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our*

military treaty partners We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.", International Strategy for Cyberspace, 2011.

Dalam konteks swasta, setiap pemilik situs *web* (penyelenggara sistem) bisa saja digugat oleh pengunjung yang merasa komputernya diserang oleh situs *web* yang bersangkutan sehingga menimbulkan berbagai kerugian.

Seandainya, situs milik sebuah perusahaan ABC direatas dan disisipi *malware* pencuri informasi oleh pihak lain, yang kemudian menginfeksi komputer pengunjungnya; yang kebetulan merupakan karyawan perusahaan XYZ (pesaing bisnis); yang kebetulan menggunakan komputer milik perusahaan XYZ. Maka, perusahaan ABC serta merta menjadi "pelaku" *e-spionase*. Jika perusahaan XYZ melaporkan ke aparat penegak hukum, maka pimpinan perusahaan ABC sebagai pemilik situs harus mempertanggungjawabkan "perbuatannya". Sebab,

ketiga komponen terjadinya tindak kejahatan sudah terpenuhi, yaitu kemampuan, motif, dan kesempatan. Kecuali, perusahaan ABC bisa membuktikan bahwa dirinya juga sebagai korban.



8

ILUSI TES PENETRASI

"Amateur hacks the system, professional hacks the people."

~ Bruce Schneier

“SAAT BERBICARA MENGENAI KEAMANAN INFORMASI TIDAK MUNGKIN HANYA MEMBATASI DIRI PADA TEKNOLOGI.”

"Apakah informasi kita sudah dipastikan pengamanannya?" tanya seorang CEO kepada penanggung jawab teknologi informasi di salah satu perusahaan terbesar di Indonesia dalam rapat untuk meluncurkan sistem baru. "Aman Pak, karena sudah dilindungi *firewall* dan di-*pentest*. Sudah dicoba untuk diretas dan tidak tembus."

"Data kami aman karena perusahaan kami sudah di-*pentest*. Di dalam laporannya disebutkan keamanan sistem aman." Itulah kalimat yang seringkali diungkapkan oleh pengelola teknologi informasi, Chief Information Officer (CIO), dan manajemen puncak organisasi yang telah mengeluarkan uang

untuk proyek tes penetrasi. Itulah "indah"-nya jebakan "*Badman*". *Pentest* memberi rasa aman yang membahayakan. Bahkan, pemerintah sebagai pembuat kebijakan, juga kerapkali terkena jebakan "*Badman*" tersebut.

TES PENETRASI

Pentest adalah simulasi serangan yang **diizinkan secara tertulis** oleh pemilik untuk membuktikan bahwa potensi kelemahan benar-benar ada serta dapat diserang. Analoginya, Anda menyewa "pencuri" untuk mencoba mencuri di rumah Anda. Jika berhasil, "pencuri" melaporkan cara menembus, berikut kelemahan apa saja yang terdapat dalam sistem pengamanan rumah Anda. Sehingga, **diizinkan secara tertulis** merupakan hal utama yang membedakan dari serangan (oleh penjahat) dan membebaskan *pentester* (sang "pencuri" profesional yang melakukan *pentest*) dari ancaman hukuman penjara.

Terdapat 3 tipe *pentest*, yaitu *blackbox*, *greybox,* dan *whitebox*. ***Blackbox*** adalah *pentest* yang dilakukan oleh *pentester* yang tidak memiliki informasi apa pun mengenai organisasi atau sistem yang akan di *pentest*. ***Greybox*** jika *pentester* memiliki sebagian informasi.

Sedangkan ***whitebox*** jika *pentester* diberikan seluruh informasi yang dibutuhkan untuk melakukan *pentest*, seperti diagram jaringan, konfigurasi *firewall*, kebijakan dan prosedur keamanan, dan lain-lain.

Tes penetrasi (*penetration test/pentest*) sesuatu yang mahal, keren, dan menjadi *trend* bagi banyak perusahaan untuk memastikan efektivitas pengamanan sistem yang diterapkan. Namun, *pentest* bagai pedang bermata dua. *Pentest* yang tidak valid menjadi bumerang karena menyesatkan proses pengambilan keputusan yang pada akhirnya menguntungkan penjahat.

Sayangnya, lebih dari 80 persen hasil *pentest* yang dilakukan dengan cenderung menyesatkan karena skenario *pentest* tidak mencerminkan kondisi seperti jika pencuri sesungguhnya melakukan serangan.

PENILAIAN KERENTANAN (VULNERABILITY ASSESSMENT/VA)

VA adalah analisis keamanan yang menyeluruh serta mendalam terhadap berbagai dokumen terkait keamanan informasi, hasil *scanning* jaringan, konfigurasi pada sistem, cara pengelolaan, kesadaran keamanan orang-orang yang terlibat, dan keamanan

fisik, untuk mengetahui seluruh potensi kelemahan kritis yang ada. VA bukan sekadar melakukan *scanning* dari jaringan menggunakan *VA tool* seperti yang ditawarkan beberapa perusahaan.

Hasil VA jauh berbeda dengan *pentest blackbox* dan *greybox*. Kedua jenis *pentest* ini tidak mampu memberikan hasil yang komprehensif karena tidak seluruh potensi kerentanan kritis akan teridentifikasi. Bahkan ditemukan dalam banyak kasus, hasil *pentest blackbox* melaporkan tidak adanya kelemahan kritis. Namun, saat dilakukan VA ditemukan terdapat beberapa kelemahan kritis yang harus ditangani sesegera mungkin.

Dalam film *Die Hard 4*, tokoh utama pelaku teror merupakan mantan kepala keamanan TI di Pentagon yang sudah melakukan VA, namun sakit hati karena rekomendasi-rekomendasi untuk meningkatkan keamanan tidak dihiraukan oleh para pejabat Pentagon. Sehingga, salah satu motivasinya melakukan serangan adalah untuk membuktikan bahwa temuan-temuan kritisnya dapat dieksploitasi dengan relatif mudah dan berkibat fatal.

Saat pertama-kali dilakukan VA yang komprehensif bisa dipastikan akan ditemukan

berbagai kerentanan kritis yang berpotensi merugikan perusahaan secara signifikan. Akan cukup banyak rekomendasi yang diberikan untuk diimplementasikan.

FAKTOR WAKTU SEBAGAI SEBUAH "KEMEWAHAN"

Mengapa hasil VA bisa jauh lebih komprehensif dan mencerminkan kondisi riil? Faktor penentu utamanya adalah waktu. Seorang penjahat profesional tidak akan melakukan serangan secara sembarangan. Penjahat siber profesional memiliki waktu yang cukup (tanpa batas) untuk mengumpulkan informasi selengkap-lengkapnya, menganalisis, dan menyusun strategi serangan.

Dalam *pentest blackbox, pentester* biasanya hanya diberi jatah 1 atau 2 minggu, sudah termasuk pembuatan laporan, sehingga waktu merupakan suatu kemewahan. Dalam VA, selain waktu yang tersedia biasanya lebih panjang, antara 3-8 minggu, tergantung lingkup pekerjaan, informasi lengkap diberikan oleh pemilik sistem juga sangat membantu untuk mengkompensasi kemewahan waktu yang dimiliki penjahat siber.

Bill Mason, seorang pencuri perhiasan senilai 35 juta dolar AS menceritakan secara mendetail dalam bukunya berjudul *Confessions of a Master Jewel Thief*. Dia berhasil mencuri perhiasan-perhiasan milik orang-orang kaya, termasuk Elizabeth Taylor, yang secara kasat mata mendapat perlindungan luar biasa. Dia bahkan berhasil mencuri uang tunai ratusan ribu dolar AS dari sebuah brankas di sarang mafia yang dijaga oleh orang-orang bersenjata.

Bill Mason dalam menjalankan aksinya memiliki "kemewahan" yang bernama waktu. Dia melakukan tahap *vulnerability assessment* selama beberapa minggu atau bahkan ada yang beberapa bulan. Hingga dia yakin bisa menentukan alat bantu, cara dan waktu beraksi yang tepat, hingga membuat beberapa alternatif rencana untuk melarikan diri.

FAKTOR MANUSIA YANG DIKESAMPINGKAN

Haruskah kita menjadi paranoid? Tidak percaya pada siapa pun? Jawabanya adalah Tidak. Bisnis, sama seperti kehidupan, selalu memiliki risiko. Kuncinya adalah di pengelolaan risiko yang efektif. Efektif dalam arti tidak hanya senantiasa melakukan kontrol dan verifikasi dari sisi teknologi, melainkan juga mempertimbangkan faktor manusia

sebagai pembawa risiko terbesar. Sehingga, di dunia keamanan informasi dikenal berbagai jargon antara lain *trust but verify* dan *trust is good, but control is better*.

Siapa saja yang bisa menimbulkan ancaman? Tergantung pada berbagai kondisi, pada hakikatnya siapa pun bisa menimbulkan ancaman. Sudah banyak kasus keamanan informasi yang melibatkan manajemen puncak perusahaan, manajemen TI, tim TI, atau bahkan tim keamanan TI. Sehingga, amat disayangkan hingga saat ini banyak perusahaan yang cenderung mengabaikan faktor manusia saat melakukan analisis risiko keamanan informasi.

Kesalahan utama dan cukup sering terjadi yang menjadikan hasil *pentest* menjadi semakin menyesatkan yaitu ruang lingkup pekerjaan proyek *pentest* yang tidak memasukkan faktor manusia. Dalam kehidupan nyata dan didukung dengan berbagai hasil survei, 80 persen masalah keamanan disebabkan oleh manusia. Bagaimana mungkin hasil *pentest* bisa valid jika yang dievaluasi hanya 20 persen (faktor teknologi)?

Fatalnya, seluruh *Request for Proposal* dan laporan hasil *pentest* yang pernah saya baca

mengesampingkan faktor manusia. Jangan heran jika regulator yang mensyaratkan dilakukan *pentest* pada sistem elektronik perbankan menjadi tersesat oleh laporan *pentest* yang hasilnya "aman". Kondisi yang menguntungkan penjahat, dan mengorbankan pelanggan.

SALAH MENDEFINISIKAN PENGANCAM

Pentest yang mensimulasikan serangan akan sulit dipastikan validitasnya jika jenis musuh yang menjadi sumber ancaman (*threat agent)* tidak didefinisikan dengan baik. Kemampuan menyerang seorang yang baru belajar teknik meretas (*script kiddies)*, atau sekelompok profesional *pentester*, atau sebuah perusahaan raksasa yang menjadi kompetitor, atau bahkan sebuah negara, sangat berbeda satu dengan yang lain. Terutama dari sisi pengetahuan, pengalaman, teknik, fasilitas, alat bantu, keuangan, dan "perlindungan" hukum.

Sayangnya, hanya beberapa kegiatan *pentest* yang mendefinisikan sumber ancaman secara jelas. Mayoritas bahkan mensyaratkan simulasi serangan hanya diizinkan dilakukan dari luar perusahaan, sehingga jauh dari kondisi nyata peretasan yang dilakukan oleh penjahat siber.

PENTEST YANG SESUNGGUHNYA BERSIFAT INTRUSIF DAN BERISIKO

Ada beberapa hal yang menjadikan *pentest* cenderung berbahaya. Yang harus disadari oleh pemilik sistem adalah *pentest* bersifat intrusif dan setiap konfigurasi sistem bisa saja memiliki reaksi yang berbeda saat diserang. Terdapat 3 kemungkinan saat serangan dilakukan, yaitu:

Sistem tidak berhasil diserang. Hal ini yang diinginkan oleh pemilik sistem, sehingga sistem dinyatakan "aman" oleh *pentester*.

- Sistem berhasil diambil alih atau dapat dilakukan proses yang seharusnya tidak boleh dilakukan. Inilah yang menjadi tujuan *pentester*.

- Sistem menjadi tidak berfungsi atau kinerja sistem menjadi tidak stabil. Kemungkinan ini yang tidak diinginkan oleh kedua pihak. Kondisi yang ditakutkan oleh administrator sistem. Kondisi yang jika terjadi pada sistem produksi yang menghasilkan uang atau diakses oleh publik, berpotensi menimbulkan kerugian keuangan secara

langsung maupun kerusakan citra organisasi pemilik sistem.

Untuk menghindari risiko, beberapa pelanggan XecureIT meminta agar *pentest* dilakukan pada sistem non-produksi. Pengalaman kami membuktikan nyaris tidak mungkin bagi pemilik sistem maupun administrator sistem untuk menduplikasi kondisi keamanan pada sistem produksi (operasional). Beberapa faktor yang membedakan antara lain kondisi keamanan fisik, arsitektur jaringan, konfigurasi sistem operasi, aplikasi-aplikasi dan *security patch* yang terpasang, serta tingkat kesadaran orang-orang yang berhubungan dengan sistem tersebut. Melakukan *pentest* pada sistem non-produksi menimbulkan risiko hasil *pentest* kemungkinan menjadi tidak valid. Tidak mencerminkan kondisi yang sesunguhnya.

Saat berhasil menembus sistem pengaman, biasanya *pentester* akan memasang *backdoor* agar tidak mengulangi serangan yang belum tentu memiliki kesuksesan yang sama. Terdapat kemungkinan *backdoor* yang dipasang memiliki kelemahan yang dapat dimanfaatkan pihak lain. Kelemahan yang mungkin saja tetap ada setelah *pentest* selesai dilakukan. Walaupun *pentester* sudah memberitahukan administrator sistem agar

dilakukan pembersihan, bisa saja sebagian fungsi *backdoor* tanpa sengaja masih tertinggal.

PENTESTER MISTERIUS

Dalam sebuah perbincangan dengan rekan-rekan profesional pengamanan informasi, seorang rekan mengungkapkan bahwa ada sebuah institusi keuangan yang *pentest*-nya dilakukan oleh seorang peretas (*hacker*). Demi menjaga kerahasiaan namanya, sang *hacker* tidak ingin namanya dicantumkan dalam kontrak dan diganti dengan inisial N.N. (*no name*). Sontak alarm di kepala saya berbunyi. Terlebih lagi saat diceritakan bahwa *hacker* tersebut berasal dari salah satu negara Eropa Timur yang cukup terkenal dengan kegiatan kejahatan sibernya. Bagaimana kalau ada *backdoor* yang disisakan? Bagaimana kalau seandainya terdapat 10 kelemahan, namun tidak semuanya dilaporkan? Dalam hati saya berteriak: "Edan! Kasihan...."

Hacker terbukti seorang profesional karena dia berhasil menciptakan sensasi seru dalam diri manajemen, auditor, dan profesional pengamanan informasi di sebuah institusi keuangan, sehingga ada proyek *pentest* yang sensitif dilakukan oleh seseorang bernama N.N. Bahayanya adalah sensasi seru karena

pentest dilakukan oleh seorang yang misterius, yaitu *hacker* profesional yang menciptakan rasa aman yang lebih kuat.

Kondisi tersebut berbeda dengan negara-negara maju yang amat memerhatikan latar belakang seseorang (dan perusahaan). Pemerintah Amerika Serikat mengenal istilah *Security Clearance* yang diberikan kepada seseorang setelah dilakukan proses *background checking*. Seorang profesional keamanan informasi harus mendapatkan tingkatan *Security Clearance* tertentu terlebih dahulu sebelum dapat melakukan *pentest*, atau hal-hal sensitif lainnya.

KNOWLEDGE IS POWER

Pentest harus dilakukan oleh *pentester* yang dapat dipercaya karena seusai melakukan tugasnya, *pentester* tersebut memiliki pengetahuan yang cukup komprehensif akan berbagai kelemahan keamanan pada kebijakan, prosedur, sistem, bahkan budaya kerja karyawan dan manajemen yang tidak aman. Pengetahuan akan berbagai ketidakamanan tersebut seringkali tidak dimiliki bahkan oleh karyawan, manajemen, dan pemilik perusahaan. Pengetahuan tersebut adalah kekuatan yang dapat digunakan untuk melumpuhkan atau paling tidak

mengganggu bisnis sebuah sebuah perusahaan atau organisasi. Pengetahuan yang "berbahaya" hingga rekomendasi-rekomendasi perbaikan keamanan diimplementasikan.

Berdasarkan pengalaman kami di XecureIT, umumnya perusahaan-perusahaan yang bergerak dalam industri yang sama menggunakan solusi dan prosedur atau mekanisme yang nyaris sama. Sebagai contoh, token (alat yang mirip kalkulator) digunakan pada *Internet Banking* sebuah bank, atau sebuah solusi *e-banking* yang digunakan sebuah bank juga digunakan beberapa bank lainnya. Contoh lain, sebuah solusi perdangan saham *online* digunakan oleh beberapa perusahaan sekuritas. Sehingga, *pentester* yang selesai melakukan *pentest* pada sebuah perusahaan, memiliki pengetahuan akan kelemahan-kelemahan sistem yang kemungkinan besar juga terdapat pada perusahaan-perusahaan lain yang bergerak di bidang industri sejenis.

MENDAPATKAN PENTESTER YANG DIPERCAYA

Dibanding bidang pekerjaan Teknologi Informasi lainnya, tidak banyak orang yang memahami konsep strategi keamanan secara mendalam dan menyeluruh, lebih sedikit lagi profesional TI yang

memiliki kemampuan memadai di bidang *hacking* (bukan hanya sekadar menggunakan *hacking tools*). Namun, yang menjadi tantangan terbesar adalah merekrut orang yang dapat dipercaya. Saya memerlukan pengamatan lebih dari setahun sebelum melibatkan seseorang dalam tim inti XecureIT. Hanya untuk memastikan orang tersebut dapat dipercaya. Belum termasuk waktu yang dibutuhkan untuk membangun kompetensi di bidang keamanan dan membentuk *hacker's mindset*. Risikonya? Jumlah SDM tim *pentest* menjadi amat terbatas. Akibatnya, beberapa kali kami terpaksa menolak secara halus tawaran *pentest* dan kehilangan potensi bisnis yang ada.

Pertanyaan berikutnya, dapat dipercaya dalam kondisi apa dan sampai kapan? Jika saya dan tim XecureIT saat ini dapat dipercaya, apa yang menjamin bahwa kami dapat dipercaya seterusnya? Bagaimana jika seorang *pentester* (atau orang terdekatnya) berada dalam posisi terancam, atau berhasil dipengaruhi dan direkrut oleh lawan usaha, sedangkan temuan kritis yang dilaporkan *pentester* tersebut belum sempat diperbaiki?

Di sisi lain, umumnya kelemahan yang terdapat pada infrastruktur yang kompleks memerlukan waktu 3-12 bulan untuk perbaikan. Itu pun jika

kondisi keuangan perusahaan memungkinkan dan manajemen puncak mendukung sepenuhnya. Tidak ada jawaban pasti untuk pertanyaan-pertanyaan tersebut. Seperti kata pepatah, dalam laut dapat diduga, dalam hati siapa tahu. Sehingga, risiko tersebut patut dipahami sepenuhnya oleh pemilik perusahaan, manajemen TI, dan penanggung jawab keamanan informasi.

DI ATAS LANGIT MASIH ADA LANGIT

Menurut saya sangat sulit membuat ukuran kompetensi seorang profesional yang melakukan tes penetrasi. Sebuah sertifikasi profesional tes penetrasi terkenal menitikberatkan kemampuan menggunakan *hacking tools*, sesuatu yang penting dalam kegiatan *pentest*. Namun, *hacking* lebih dari sekadar kemampuan menggunakan *tools* yang dapat dipelajari dengan mudah lewat Google. *Hacking* memerlukan pemahaman cara kerja mendalam akan sesuatu yang akan diretas, kemampuan melihat sesuatu secara menyeluruh, cara pikir yang selalu berpikir di luar dari yang seharusnya (*think out of the box*). Meretas memerlukan pola pikir seperti iblis: menganalisis setiap detail untuk menemukan kelemahan yang ada dan menciptakan strategi serangan yang "mematikan".

Hal di atas menyebabkan hasil *pentest* bisa menjadi amat berbeda jika dilakukan oleh *pentester* yang berbeda. Sebagai contoh, siapakah saya (dan tim peretas di XecureIT) yang berani menyatakan bahwa sebuah sistem yang tidak berhasil ditembus oleh kami berarti aman? Apa yang menjadikan kami berhak mengklaim, (seolah-olah) tidak ada pihak lain yang lebih hebat dari kami? Apakah kita lupa akan pepatah "Di atas langit masih ada langit"?

MENYERANG BERBEDA DENGAN MENGAMANKAN

Dengan pengalaman selama 20 tahun lebih, baik meretas maupun mengamankan, saya menyimpulkan bahwa mengamankan 10 kali lebih sulit dari meretas. Bertahan jauh lebih sulit daripada menyerang. Kepada rekan-rekan yang berminat menggeluti dunia *hacking*, saya seringkali menggunakan analogi montir. Montir dikatakan hebat jika bisa menjaga sebuah mobil tetap mulus dan kinerja mesinnya baik. Bukan sebaliknya, mencuri atau merusak.

Perancangan strategi keamanan harus komprehensif, luas, dan dalam, agar menghasilkan arsitektur keamanan yang efektif. Implementasi arsitektur juga sesuatu yang kompleks karena harus

mengombinasikan komponen-komponen orang, administratif (kebijakan dan prosedur), teknologi, serta lingkungan fisik. Penjagaan keamanan siber dan informasi harus dilakukan secara konsisten, dan terus-menerus, tidak bisa lengah. Peretas cukup mencari-cari celah atau kelemahan keamanan dari setiap komponen, atau bahkan menunggu munculnya kelemahan keamanan kritis dipublikasikan oleh orang lain, kemudian mengeksploitasinya.

Selayaknya, seorang senior *pentester* profesional memiliki pengetahuan yang luas dan dalam, bukan hanya spesifik terkait teknologi, melainkan juga pengetahuan yang luas di bidang keamanan informasi. Pengetahuan yang komprehensif merupakan faktor utama dalam membuat rekomendasi strategis. Pemilik informasi bukan hanya butuh rekomendasi perbaikan sistem teknologi informasi, namun juga butuh rekomendasi strategis untuk pengambilan keputusan yang tepat.

MASIHKAH PENTEST DIPERLUKAN?

Dengan berbagai ketidak-akuratan hasil *pentest* saat ini, masihkah *pentest* diperlukan? Masih! *Pentest* tetap memiliki posisi penting dalam memastikan efektivitas strategi keamanan informasi yang

dimiliki. Namun, harus benar-benar dipahami bahwa *pentest* adalah sebuah alat yang memiliki kelebihan, kekurangan, dan menimbulkan risiko berbeda-beda bagi penggunanya. Dan, yang terpenting adalah jangan sampai pemerintah, para pengambil keputusan, pengelola teknologi informasi, dan penanggung jawab keamanan informasi terilusi dengan laporan hasil tes penetrasi.

9

MANAJEMEN RISIKO YANG MENYESATKAN

"Sebagai pengemudi yang terus-menerus menganalisis risiko saat berkendara, Anda membutuhkan sistem pengereman yang berfungsi efektif."

“DETAIL-DETAIL PADA PROSES MANAJEMEN RISIKO YANG MEMBEDAKAN HASIL, APAKAH STRATEGI KEAMANAN INFORMASI EFEKTIF DAN EFISIEN.”

Aman atau tidak aman? Kita bisa berdebat seru tanpa dasar yang jelas karena semua kata sifat pasti subjektif. "Tidak ada yang 100 persen aman" jargon yang seringkali dipakai untuk menghindari tanggung jawab atau kabur dari sebuah konteks diskusi yang berkualitas terkait keamanan informasi. Benar bahwa tidak ada yang 100 persen aman, tapi harusnya bisa dijawab secara kualitatif tingkat risikonya (rendah, sedang, tinggi, atau sangat tinggi), dan risiko-risiko apa saja yang (masih) ada. Pengambilan keputusan yang tepat hanya dapat dicapai dengan informasi yang akurat.

Rem pada mobil, fungsinya untuk memperlambat, tapi tujuannya untuk memungkinkan

mobil dapat dikendarai dengan cepat. Apakah Anda mau mengendarai sebuah mobil tanpa rem? Mana yang akan memenangi perlombaan: mobil yang remnya efektif, atau yang remnya tidak efektif, atau yang tidak punya rem?

Efektivitas penggunaan rem bukan hanya soal faktor teknologi rem yang canggih, namun orang di belakang kemudi yang berintegritas (taat lalu lintas, tidak ceroboh, tidak mabuk, atau tidak mengantuk) dan kompeten, sehingga tahu persis kapan dan seberapa dalam rem ditekan.

Manajemen risiko pada strategi keamanan informasi mirip seperti kondisi di atas. Pengemudi mobil melakukan analisis risiko secara berkelanjutan, mulai dari proses menentukan internal dan eksternal konteks, melakukan penilaian risiko, dan diakhiri dengan penanganan risiko. Seperti pepatah, setan ada di dalam detail, maka detail-detail pada proses manajemen risiko yang membedakan hasil, apakah strategi keamanan informasi efektif dan efisien.

Bukan urusan Anda sebagai CEO untuk mengetahui seluruh detail manajemen risiko keamanan informasi di sebuah proses bisnis. Saya akan membuka beberapa detail “rahasia”

untuk mengungkap titik rawan manajemen risiko keamanan informasi yang dapat menyesatkan pengambil keputusan. Anda hanya butuh kerangka berpikir yang jelas untuk dapat "mencium" apakah ada sesuatu yang salah atau tidak.

Keamanan adalah pengelolaan risiko karena tidak ada yang aman 100 persen. Namun, bagaimana risiko bisa dikelola dengan baik jika risikonya tidak diketahui? Konsultan atau arsitek keamanan informasi yang tidak memahami sepenuhnya cara kerja suatu sistem akan dengan mudah "tersesat" oleh brosur dan keterangan penjual. Seringkali penjual (yang juga tidak pernah tahu) berkelit di balik berbagai istilah teknis marketing yang juga tidak jelas maksudnya apa. Takut merasa dianggap bodoh, banyak profesional pengamanan informasi malu bertanya kepada penjual di hadapan kliennya sehingga bersikap sok tahu dan mengamini keterangan si penjual.

Klien yang merasa sudah membayar konsultan mahal dan bersertifikasi banyak, merasa yakin kalau produk tersebut benar-benar sebagai *security silver bullet,* solusi ajaib dari kompleksitas masalah keamanan yang dihadapi. Bagian marketing membuat iklan yang membuat calon pengguna

merasa yakin. Pada akhirnya, besar kemungkinan, yang dipakai untuk mengambil keputusan lebih banyak berdasarkan perasaan, bukan pertimbangan keamanan yang matang, yang memerhatikan faktor keamanan teknologi, orang, kebijakan, dan prosedur secara menyeluruh dan mendalam.

MANAJEMEN RISIKO DENGAN MENTALITAS PEDAGANG KAKI LIMA DAN ANGKUTAN UMUM DI INDONESIA

Jangan berbisnis jika tidak berani mengambil risiko. Benar. Bahkan mengambil keputusan untuk tidak mengambil risiko pun tetap berisiko. Menghindari risiko berdampak kehilangan kesempatan bisnis.

Belajar dari kasus hukum pidana yang menimpa mantan Direktur Utama Indosat Multi Media (IM2) yang berakibat kurungan penjara beberapa tahun, saya mencoba mengevaluasi beberapa kasus dari sudut pandang manajemen risiko.

Teman-teman pemilik bisnis penyedia layanan Internet (ISP) di Indonesia meributkan kasus yang menimpa mantan Direktur Utama IM2 tersebut, karena menurut mereka, akan banyak yang akan mengalami hal serupa. Salah satu argumentasi mereka

adalah mengapa selama ini dibiarkan pemerintah kalau memang menyalahi aturan? Mengapa tidak diberi peringatan sejak dulu. Inilah yang saya analogikan dengan pedagang kaki lima. Seorang pedagang berjualan di lokasi tertentu, dan ternyata banyak pembeli, kemudian pedagang-pedagang lain mengikuti dengan asumsi diperbolehkan berjualan di tempat itu. Saat ditertibkan, semua beramai-ramai melakukan demonstrasi.

Lain halnya dengan industri perbankan yang terkenal dengan istilah *highly regulated industry*. Industri yang memiliki sangat banyak aturan.

Selama lebih dari sepuluh tahun bergaul dengan teman-teman profesional di industri perbankan, sangat sering di akhir diskusi mereka mengatakan, "Saya sebenarnya juga mau meningkatkan keamanan dengan benar. Tapi, apakah baik bagi bank saya? Jika bank-bank lainnya juga melakukan pengamanan dengan benar, bank saya juga akan melakukan hal yang sama. Jika tidak, bank saya akan ditinggalkan nasabah karena prosedurnya dianggap menyusahkan."

Sampai satu titik, saya pun menyimpulkan bahwa industri kerah putih ini memiliki mental yang mirip

dengan angkutan umum di Indonesia. Aturan lalu lintas sangat banyak, namun penegakan hukumnya lemah, sehingga beramai-ramai mengabaikan keselamatan penumpang, dan kelancaran arus lalu lintas. Risiko hukumnya juga sangat kecil. Nyaris tidak ada korban atau keluarganya yang mau membawa kasus kecelakaan ke ranah hukum karena menganggap "sudah nasib", tidak punya pilihan yang lebih baik, atau hanya akan menimbulkan kerugian yang lebih besar.

Banyaknya aturan keamanan informasi dibuat dengan tujuan utama untuk meningkatkan kepercayaan pasar dengan menciptakan rasa aman bagi pengguna. Bank sanggup meningkatkan keamanan secara substantif, bukan hanya kelihatannya aman padahal sesungguhnya tidak aman, yang dikenal dengan sebutan *Security Theatre*. Bank memiliki hak, kewajiban, dan sumber daya untuk memerangi kejahatan siber. Masalah fundamentalnya adalah penegakan hukum (aturan) oleh regulator dilakukan antara mau dan tidak mau.

Cukup sering saya diminta membantu nasabah yang merasa dirugikan. Salah satunya nekat memproses hingga ke meja hijau. Nasabah tersebut meminta saya untuk menjadi saksi ahli, membantunya

mendapat keadilan, namun tidak memiliki biaya. Saya bersedia mendampinginya tanpa biaya, dan kasusnya dimenangkan oleh nasabah tersebut.

Setiap kali mempelajari kasus-kasus semacam itu, saya selalu berkata dalam hati, "Cukup ada seorang nasabah yang mau dan berani berkorban dengan didampingi pengacara andal, beberapa direktur utama bank, dan pejabat-pejabat yang mengatur industri ini, akan berurusan dengan hukum dengan tuduhan pidana berat." Dalam hukum, banyak hal terlihat abu-abu, tidak hitam/putih. Benar atau salah bergantung pada keputusan hakim di pengadilan.

KESALAHAN MENENTUKAN KONTEKS MANAJEMEN RISIKO

ISO 31000 yang menjabarkan prinsip dan petunjuk manajemen risiko, menjabarkan internal dan eksternal konteks. Sayangnya, mayoritas dokumen manajemen risiko yang pernah saya baca, gagal menentukan konteks secara benar, terutama eksternal konteks. Menurut ISO 31000, eksternal konteks termasuk, namun tidak terbatas pada hal-hal sebagai berikut.

- Kultur dan sosial
- Politik, hukum, dan Regulasi

- Keuangan dan ekonomi
- Teknologi
- Lingkungan kompetisi, baik lokal ataupun internasional
- *Key drivers* dan tren yang berdampak pada pencapaian tujuan-tujuan organisasi
- Hubungan dengan pemangku kepentingan eksternal
- Persepsi dan nilai-nilai pemangku kepentingan eksternal.

Pendefinisian konteks dari manajemen risiko keamanan informasi yang komprehensif merupakan faktor kunci. Kesalahan di tahap ini berakibat strategi keamanan menjadi tidak efektif dan/atau tidak efisien. Konsep manajemen risiko keamanan informasi sederhana, namun menjadi kompleks bagi orang yang menjalankan, apalagi saat menerapkan beragam kontrol.

Saya dan teman-teman di XecureIT nyaris selalu berhasil saat melakukan tes penetrasi jika konteks skenario serangan diizinkan sesuai dengan konteks penjahat melakukan kejahatannya. Seorang CEO pabrik otomotif mengungkapkan kalau paparan rapat penutup hasil tes penetrasi yang telah

kami lakukan akan membuat dirinya tidak dapat menikmati liburan panjang akhir minggu. Padahal, kami hanya menunjukan bagaimana caranya meretas sistem mereka sehingga mobil-mobil dari gudang penyimpanan atau pabrik perakitan dikirim ke alamat tertentu.

Masalahnya sangat sederhana. Tim yang melakukan analisis risiko, merancang strategi keamanan informasi, dan menerapkan teknologi keamanan canggih dan yang berbiaya mahal, tidak memasukkan vendor perangkat teknologi keamanan ke dalam konteks manajemen risiko. Kami pun dapat mengambil alih kendali *firewall* (gerbang keamanan jaringan) dari Internet.

KESALAHAN MENENTUKAN DAMPAK

Cukup banyak kementerian dan lembaga negara yang sudah mengadopsi ISO 27001 Sistem Manajemen Keamanan Informasi, bahkan hingga bersertifikasi. Namun, mayoritas metodologi penilaian risiko yang dimiliki tidak melihat dampak secara nasional, hanya melihat dampak terhadap kementerian atau lembaga tersebut.

Sebagai standar internasional, ISO 27001 dapat digunakan sebagai acuan bagi organisasi yang terdiri dari 5 orang, 50.000 orang, bahkan sebuah negara. Setiap organisasi berhak menentukan metodologi penilai risiko sendiri. Auditor sertifikasi hanya memeriksa apakah ada dokumen kebijakan dan prosedur tertulis, dan apakah diikuti dengan benar dan baik. Auditor sertifikasi tidak (berhak) menilai apakah tabel dampak yang ditentukan benar atau salah.

Saya menganalogikan negara sebagai sebuah perusahaan raksasa di mana di dalamnya banyak divisi/divisi atau departemen-departemen. Sebagai sebuah divisi atau departemen, sudah selayaknya setiap perencanaan selalu melihat dampak terhadap perusahaan raksasa tersebut. Maka, menjadi aneh, terlihat egois, dan membahayakan kepentingan nasional jika analisis dampak hanya dilakukan terhadap lembaga masing-masing.

Dampak terhadap bisnis berbeda dengan dampak terhadap negara. Saya belum pernah melihat dokumen tabel dampak nasional yang dikeluarkan pemerintah secara resmi. Hal ini dapat dimengerti karena sama saja memberi informasi batas "maksimum" kemampuan suatu bangsa

menghadapi serangan. Akibatnya, hampir seluruh kementerian atau lembaga negara di Indonesia yang mengadopsi ISO 27001 tersesat dalam menentukan dampak. Setelah mengkaji beberapa tahun, kami di XecureIT menyimpulkan dan menetapkan dalam *XecureIT Governance and Evaluation Framework* (XGEF) bahwa kriteria dampak nasional yang tepat adalah dampak terhadap ideologi, politik, ekonomi, sosial, budaya, pertahanan, dan keamanan (IPOLEKSOSBUDHANKAM). Menerapkan dampak "bergaya swasta" (dampak keuangan, hukum, reputasi, keselamatan, dan lingkungan) yang selama ini banyak diterapkan dalam proses analisis risiko menyebabkan pimpinan negara tersesat dalam pengambilan keputusan strategis.

Hal serupa juga terjadi di beberapa perusahaan, hanya dalam skala yang lebih kecil. Saya beberapa kali menemukan analisis dampak yang dilakukan bukan terhadap bisnis perusahaan, tetapi terhadap Bagian Teknologi Informasi. Dalam beberapa kasus, Bagian Manajemen Risiko tidak membuat kriteria dampak yang komprehensif. Cukup banyak yang hanya memasukkan kriteria keuangan dan reputasi, sedangkan kriteria hukum, keselamatan, dan lingkungan diabaikan. Sepanjang pengetahuan saya dibidang industri perbankan, analisis dampak

hanya dilakukan terhadap bisnis perbankan. Analisis dampak terhadap nasabah dan pejabat bank tidak pernah dilakukan.

TEBAK-TEBAKAN KEMUNGKINAN BESAR ATAU KECIL

Cukup sering kita mendengar orang berbicara bahwa risiko dari suatu kondisi adalah besar, atau kecil. Pertanyaan sederhananya adalah apa dasar penilaiannya. Dalam menghitung risiko terdapat dua komponen pengali yaitu dampak dan kemungkinan. Setelah membahas kesalahan dalam menentukan dampak, kita akan membahas cara menentukan kemungkinan.

Masalah utama dalam menghitung kemungkinan terjadinya sebuah dampak di bidang keamanan siber dan informasi adalah soal data statistik yang sulit dipertanggungjawabkan validitasnya. Karena begitu banyaknya kejadian yang tidak diketahui, sehingga seringkali digunakan teknik tebak-tebakan untuk memberikan angka seberapa sering kejadian akan muncul dalam periode waktu tertentu. Bagaimana mungkin menghasilkan perhitungan risiko yang mendekati kehidupan nyata jika menggunakan angka yang muncul dari teknik tebak-tebakan? Sebuah teknik di mana tidak bisa

dijelaskan asal muasal angkanya kecuali dengan teknik mengada-ada.

Saat berdiskusi dengan para peneliti keamanan siber di Carnegie Mellon University, Wakil Jaksa Agung New York, agen-agen khusus FBI bidang kejahatan siber, US Department of Homeland Security, dan beberapa institusi lainnya pada kesempatan yang berbeda-beda, semuanya sepakat bahwa statistik kasus-kasus kejahatan siber dan keamanan informasi seperti fenomena gunung es. Di Indonesia, lebih tepatnya adalah fenomena gunung es yang tidak terlihat puncaknya.

Lebih menyesatkan lagi, ketika teknik tebak-tebakan tersebut diterapkan secara lokal. Sangat sering saya mendengar argumen, "Secara statistik kemungkinan terjadinya tidak ada karena di Indonesia belum pernah terjadi." Tiap kali saya harus "mempertajam" argumen tersebut. "Maaf, lebih tepatnya, bukan belum pernah terjadi, tetapi belum mengetahui seandainya sudah pernah terjadi."

Melokalkan statistik kejahatan siber, dunia tanpa batasan lokasi fisik, dengan menggunakan asumsi perhitungan risiko seperti statistik keuangan atau kejahatan fisik benar-benar menyesatkan.

Banyak konsultan yang menggunakan data statistik serangan siber untuk "menghitung" risiko. Statistik tersebut dihasilkan dari perangkat sensor serangan jaringan dan analisis log. Hampir seluruh data statistik tersebut menyesatkan karena terlalu banyak *false positive* yang mendeteksi kegiatan sistem normal sebagai serangan. Dan yang lebih parah, banyak kegiatan yang sesungguhnya serangan namun tidak terdeteksi (*false negative*).

Pengalaman saya menunjukkan bahwa membeli sistem Security Information and Event Management (SIEM) yang canggih jauh lebih mudah dari melakukan *rules fine tuning* agar sistem canggih tersebut bermanfaat dan tidak membahayakan. Jika tidak hati-hati, sangat berbahaya menggunakan statistik keamanan teknologi informasi untuk menilai risiko keamanan informasi terhadap bisnis.

Sebenarnya, tidak sulit untuk memprediksi secara tepat apakah sebuah serangan akan (atau mungkin sudah) terjadi di negara-negara berkembang. Berkaca dari teknik-teknik pembobolan pada banyak sekali kasus kejahatan siber terkait industri perbankan, maka gelombang serangan kejahatan siber yang terjadi di negara-negara maju, akan tiba di negara-negara berkembang dalam

waktu paling lama 3 tahun. Sebagai contoh, alat untuk mencuri informasi kartu debit yang terungkap di Indonesia sebagian besar perangkat bekas yang yang telah digunakan di negara-negara lain tahun-tahun sebelumnya.

Dengan berbagai hal di atas, kami di XecureIT memilih menggunakan teknik yang jauh lebih presisi dibanding data statistik dalam menghitung besar atau kecilnya kemungkinan. Menurut saya, caranya jauh lebih mudah dan hasilnya tepat dengan mempertimbangkan:

- Kelemahan-kelemahan apa saja yang (mungkin) dimiliki sebuah komponen kontrol keamanan;
- Siapa yang berpotensi menjadi pengancam (Bab 5 Mengenal Sang Pengancam); serta
- Seberapa besar paparan sebuah informasi terhadap pengancam potensial.

KLASIFIKASI KEAMANAN INFORMASI YANG MENYESATKAN

Kesalahan fatal lainnya adalah saat melakukan klasifikasi keamanan informasi. Banyak Bagian Manajemen Risisko tanpa sadar hanya memasukkan

aspek kerahasiaan, dengan menggunakan terminologi tingkatan, seperti contoh berikut atau kombinasinya.

- Publik, Internal, Rahasia, Sangat Rahasia.
- Umum, Internal, Sensitif, Sangat Rahasia.
- Unclassified, Classified, Secret, Top Secret.

Semua orang yang membaca tingkatan klasifikasi keamanan informasi tersebut pasti tersesat dengan menyimpulkan bahwa yang penting hanya aspek kerahasiaan, dan tanpa sadar melupakan aspek integritas dan kerahasiaan. Tahun 2005, saya berkenalan dengan seorang CEO salah satu perusahaan investasi besar saat kami sedang menunggu pesawat di *executive lounge* bandara di Oslo. Beliau hampir salah mengambil keputusan strategis. Grafik analisis dalam *spreadsheet* yang ditampilkan memberikan tren yang meningkat. Seorang analis senior yang ikut hadir dalam rapat pengambilan keputusan merasa ada kejanggalan. Setelah diperiksa secara mendetail, akhirnya ditemukan bahwa ada variabel utama yang angka nolnya kelebihan satu. Si pemapar tanpa sengaja (*typo*) menambahkan angka nol saat merapikan tampilan di malam sebelum paparan. Beliau mengatakan: “Nyaris perusahaan saya rugi belasan juta dolar.”

Beliau beruntung, hanya nyaris mengalami kerugian besar. Pada Desember 2005, kesalahan pengetikan menyebabkan Mizuho Securities kehilangan 225 juta dolar AS saat transaksi perdagangan saham. Kerugian tersebut terjadi karena seorang *trader* menjual 610.000 lembar saham senilai 1 yen, di mana seharusnya 1 saham senilai 610.000 yen.

SELERA YANG TIDAK KONSISTEN

Sangat sering saya mengikuti diskusi terkait risiko keamanan informasi yang berujung pada kalimat: Tergantung *risk appetite*-nya. Pernyataan benar yang sering disalahgunakan penggunaanya, perlakuan yang sama seperti terhadap kalimat "Tidak ada yang 100 persen aman".

Betul, setiap pihak mempunyai "selera" berbeda untuk menentukan risiko (sisa) yang bisa diterima. Yang terpenting adalah konsistensi. Kalau hari ini saya suka yang asin, tiba-tiba besok karena kesal dengan teman kantor, kemudian berubah jadi tidak suka asin. Bagaimana jika Anda menjadi tukang masaknya?

Saat memeriksa dokumen analisis risiko sebuah perusahaan keuangan internasional, saya cukup terkejut. Bagaimana mungkin dua kelompok informasi yang berbeda, dengan tingkat dampak dan tingkat kemungkinan terjadinya sama, tapi selera risiko dan tingkat keamanannya diperlakukan berbeda?

ISO 27001 menetapkan bahwa organisasi yang mengadopsi standar sistem manajemen keamanan informasi ini harus membuat Metodologi Penilaian Risiko. Metodologi ini akan menghasilkan perhitungan risiko yang konsisten *Risk Appetite*-nya. Begitu ditetapkan, semua pihak internal harus mengacu ke metodologi tersebut. Sehingga, tercapai konsistensi dari waktu ke waktu oleh siapa pun yang melakukan penilaian. Jika kondisi perusahaan atau negara berubah maka metodologinya seharusnya juga berubah, terutama angka *Risk Appetite*-nya. Pada angka berapa berisiko dinyatakan rendah, sedang, tinggi, atau sangat tinggi.

PENGURANGAN RISIKO DENGAN TEKNIK MENCAMPUR AIR DENGAN MINYAK

Pada Bab 6 tentang Kebingungan Menentukan Prioritas Aspek Keamanan Informasi, saya sudah

menjelaskan bahwa prioritas industri telekomunikasi dan penggunanya adalah ketersediaan, sedangkan bagi industri perbankan aspek kerahasiaan adalah prioritas, berbeda dengan (mayoritas) nasabah yang memprioritaskan aspek integritas.

Teknik mencampur air dengan minyak juga diterapkan oleh Microsoft yang dengan niat "baik", mencampuradukkan aspek kerahasiaan dan ketersediaan pada Windows 10. Niat "baik" yang tanpa sepengetahuan pelanggan, telah aktif sejak awal instalasi, tanpa membutuhkan perubahan konfigurasi atau aktivasi oleh pengguna (*default configuration*).

Karena banyak pelanggan yang tidak lagi dapat mengakses datanya akibat tidak paham mekanisme fasilitas enkripsi ini maka Microsoft berinisiatif menduplikasi kunci enkripsi Bitlocker milik pelanggan ke server miliknya. Dari sudut pandang ilmu kriptografi, aspek kerahasiaan kunci enkripsi adalah prioritas utama. Pelanggan menggunakan fasilitas enkripsi Bitlocker juga untuk menjaga kerahasiaan. Namun, Microsoft memutuskan bahwa aspek ketersediaan kunci enkripsi lebih penting, sehingga membuat dan menyimpan kunci duplikatnya tanpa disadari pemilik kunci.

Sebagai pimpinan, apakah hal ini mengganggu perasaan nyaman Anda? Anda tidak perlu terlalu khawatir jika organisasi Anda tidak termasuk kategori strategis bagi negara Anda, atau memiliki kompetitor asing. Jika termasuk dalam kategori tersebut, berarti Anda telah salah mengidentifikasi siapa pengancam Anda. Pastikan Anda memahami tulisan saya di Bab 5 Mengenal Sang Pengancam.

MEMBAGI RISIKO KE SI "BUTA" YANG MEMBUTUHKAN

Tidak sedikit pengumuman yang disediakan penyedia layanan parkir berbayar bahwa pengelola tidak bertanggung jawab atas kehilangan dan kerusakan atas kendaraan Anda. Dampak positif bisnis perparkiran mau dinikmati oleh pengelola, namun kemungkinan dampak negatifnya dipindahkan ke pelanggan. Dalam kasus kehilangan kendaraan di tempat parkir komersial telah berkali-kali dibuktikan dalam keputusan hakim di Indonesia bahwa pengelola tetap harus bertanggung jawab.

Sebelas tahun lalu saya memutuskan untuk menjalani proses penyinaran laser (lasik) untuk memperbaiki penglihatan. Saya dan pasien lainnya, selama 2 minggu tidak diizinkan menggunakan kacamata atau lensa kontak agar bentuk bola

mata kembali ke kondisi alaminya. Saat menunggu di ruang tunggu sebelum menjalani tindakan, seorang perawat mendatangi para pasien, termasuk saya, untuk membagikan formulir yang harus ditandatangani. Seluruh pasien yang lain, sebagian besar tidak bisa membaca tanpa alat bantu, langsung menandatangani formulir tersebut tanpa membaca. Beberapa bahkan ditunjukkan oleh si perawat lokasi tempat membubuhkan tanda tangan. Saya memilih untuk membaca formulir tersebut dengan saksama dan menanyakan kepada si perawat yang sudah terlihat mulai tidak senang karena menunggu saya membaca.

Pertanyaan saya sederhana, "Mengapa saya tidak pernah diberi tahu oleh dokter bahwa tindakan yang akan dilakukan dapat berakibat jangka pendek maupun jangka panjang, dari gangguan penglihatan ringan hingga menyebabkan kebutaan? Padahal di formulir tersebut dinyatakan dokter sudah memberitahukan ke pasien." Karena ruangan sunyi senyap, hampir seluruh pasien yang terkantuk-kantuk tiba-tiba mengangkat kepala dan mendengar dengan saksama pembicaraan saya dengan si perawat. Setelah si perawat pergi, saya bertanya pada pasien di sebelah saya, ternyata dia juga tidak diberi penjelasan oleh dokter.

Bagaimana pendapat Anda? Apakah bisnis yang Anda melakukan hal yang serupa tapi tak sama? Ada banyak contoh yang serupa di dunia maya.

Saya selalu bertanya dalam hampir banyak kesempatan ketika menjadi narasumber, "Siapa yang pernah membaca *End User License Agreement* (EULA) yang dibuat pembuat *software* saat memasang piranti lunak di *server*, PC, *laptop*, atau ponsel?" Setiap kali, nyaris tidak ada yang angkat tangan, hanya menggelengkan kepala, sambil menertawakan saya. Hanya orang "gila" yang mau membaca beberapa halaman EULA, sebelum menekan tombol *accept*. Beberapa orang memberi argumen bahwa untuk apa dibaca kalau kemudian tidak punya pilihan, suka atau suka harus menerimanya.

Saya, orang "gila", membaca semua EULA. Banyak *software* yang tidak jadi saya gunakan karena menurut saya terlalu intrusif, dengan bahasa bersayap dan terkesan positif, meminta persetujuan pengguna untuk memberikan izin mengambil seluruh informasi yang dimiliki. Hampir semua EULA menyatakan tidak bertanggung jawab terhadap hasil dari informasi yang diproses.

Saat membuka rekening bank di Indonesia, beberapa bank yang saya baca persyaratan pembukaan rekeningnya mewajibkan para nasabah menandatangani kesepakatan yang kurang lebih menyatakan, bahwa nasabah menerima seluruh risiko yang mungkin terjadi dalam proses perbankan elektronik, dan melepaskan bank dari tuntutan apa pun. Padahal, pembuat *software*-nya pun sudah menyatakan dalam EULA bahwa mereka tidak bisa menjamin kehandalan *software*-nya.

Beberapa kasus yang terungkap ke publik menunjukkan bahwa kesalahan *software* menimbulkan kehancuran total, nyaris menghancurkan dunia, dan mengakibatkan kematian nyata.

Tahun 1996, roket Ariane-5 milik Prancis meledak di orbit karena kegagalan sistem akibat menggunakan sebagian modul aplikasi milik Ariane-4 yang berbeda rancangannya.

Tahun 1980, nyaris terjadi perang nuklir saat sistem pemantau serangan misil milik North American Aerospace Defense Command (NORAD) mendeteksi adanya serangan yang ternyata merupakan kesalahan sistem.

Kehancuran dunia nyaris terjadi kembali di tahun 1983 ketika kesalahan sistem deteksi peringatan dini milik Soviet memberikan peringatan adanya 5 serangan nuklir balistik misil dari Amerika Serikat. Beruntung Letnan Kolonel Stanislav Petrov mengambil keputusan yang tepat di saat kritis.

Tahun 2000, terjadi kesalahan sistem milik National Cancer Institute, Panama City, dalam menghitung dosis yang diberikan, sehingga mengakibatkan 20 orang pasien kelebihan dosis radiasi, dan 8 orang lainnya meninggal.

KERANCUAN KONTROL HANYA MENCIPTAKAN DRAMA KEAMANAN

Terdapat komponen-komponen orang, proses (administratif), teknologi, dan lingkungan fisik dalam strategi keamanan informasi. Sayangnya, definisi kontrol dalam ISO/IEC 27000:2014, ikhtisar dan kosa kata Sistem Manajemen Keamanan Informasi (SMKI), sangat sederhana: "*measure that is modifying risk*", dan dokumen-dokumen dalam keluarga ISO 27000 memberi kesan bahwa per komponen adalah kontrol. Dalam kehidupan nyata, di luar dari teori di atas kertas, kerancuan ini menguntungkan penjahat.

ISO 27001 SMKI sangat menekankan konsistensi, sehingga segala proses harus dibuat sistemik (memiliki kebijakan dan prosedur). Jika ingin menghasilkan kondisi yang benar-benar meningkatkan keamanan (bukan hanya terlihat aman, tapi tidak aman) maka komponen-komponen tersebut harus disatukan. Dalam Standar Arsitektur Keamanan Tingkat Tinggi Informasi (SAKTTI) yang dibuat dan dimiliki XecureIT, penyatuan tersebut dikenal dengan konsep Kontrol Keamanan Informasi Terintegrasi (*Integrated Information Security Control*). Setiap komponen untuk mengontrol diberi nama Komponen Kontrol.

Sebagai analogi, sebuah ruangan akan ditingkatkan keamanannya (dikurangi risikonya) dengan memasang kontrol berupa teknologi pintu dan kunci. Dalam perhitungan risiko, seolah-olah risiko akan berkurang dengan memasang teknologi tersebut. Pada kenyataanya belum tentu lebih aman, bahkan cenderung meningkatkan risiko karena kita merasa (lebih) aman. Seandainya kita ada di dalam ruangan tersebut, dan kuncinya tertinggal di sisi luar pintu, maka penjahat dapat memanfaatkan kontrol untuk memenjarakan kita. (Potongan) kontrol tersebut malah menjadi bumerang.

Konsep Kontrol Keamanan Informasi Terintegrasi pada SAKTTI melihat pintu dan kunci hanya sebagai komponen kontrol. Kontrol terintegrasi dalam hal meningkatkan pengamanan sebuah ruangan adalah menunjuk orang yang kompeten dan berintegritas. Orang itulah yang menjalankan kebijakan dan prosedur keamanan yang telah ditetapkan dalam mengelola keamanan pintu dan kunci. Tugas dijalankan dengan kondisi lingkungan penyimpanan kunci yang sesuai dengan kebijakan, sehingga menjamin hanya orang yang berhak dapat keluar dan/atau masuk ke ruangan tersebut.

Sangat disayangkan, terlalu banyak perusahaan, kementerian, dan lembaga pemerintah mengeluarkan investasi mahal yang fokus pada teknologi pengamanan, kemudian menjadi mubazir. Bahkan, investasi mahal itu malah menjadi bumerang karena pemahaman kontrol yang keliru (tidak terintegrasi), yang tidak sesuai dengan kondisi kehidupan nyata.

Isu lain dalam penerapan kontrol adalah menggunakan strategi kontrol yang usang, yang tidak lagi sesuai dengan perkembangan zaman. Teknologi gembok "raksasa" abad pertengahan tidak lagi bisa menjadi kontrol komponen yang efektif dewasa ini.

Contoh dalam kehidupan sehari-hari adalah penggunaan informasi-informasi yang 30 tahun lalu masih bersifat privat, namun saat ini sudah menjadi publik, untuk proses autentikasi. Saat industri kartu kredit berkembang di tahun 80-an, informasi-informasi terkait nasabah, seperti nama gadis ibu kandung, tanggal lahir, alamat, dan lain-lain, dianggap sebagai informasi rahasia, yang hanya diketahui orang dekat yang baik, dan tidak diketahui penjahat (Bab 3 *Security by Obscurity* Dijamin Gagal). Seluruh bank, saling menyontek ide, dengan melakukan verifikasi penelepon saat layanan pelanggan dihubungi. Sejak di tahun 90-an pembobolan kartu kredit sudah marak dengan mengeksploitasi strategi *security by obscurity* tersebut.

Proses *copy-paste* (saling mencontek) ide strategi keamanan tanpa pemahaman latar belakang dan asal-usul ide tersebut secara komprehensif menghasilkan apa yang oleh industri perbankan disebut sebagai *best practice*.

Dunia maya berevolusi, namun komponen kontrolnya masih klasik. Celakanya, *best practice* pada industri perbankan tersebut kembali dicontek industri teknologi informasi, dengan menciptakan istilah *cognitive password*, dengan menambahkan

warna kesukaan, nama guru saat sekolah, nama binatang kesayangan, dan lain-lain. Orang-orang di industri teknologi informasi yang menciptakan revolusi dunia maya terilusi keamanan industri perbankan yang sangat yakin dengan konsep keamanan *Security by Obscurity*. Proses menyontek yang berujung pada mudahnya pembobolan akun-akun layanan di Internet Google, Yahoo, Facebook, dan lain-lain.

Masalah industri telekomunikasi di Indonesia adalah bagaimana memastikan kebenaran seseorang yang mengaku sebagai pemilik kartu prabayar mendatangi layanan pelanggan untuk meminta penggantian kartu. Solusi manjurnya adalah menanyakan 5 nomor telepon yang sering dihubungi. Lagi-lagi menyontek konsep ilusi keamanan *Security by Obscurity* dari industri perbankan, berasumsi bahwa 5 nomor yang sering dihubungi adalah rahasia.

Rangkaian strategi *security by obscurity* tersebut memberikan *Bingo!* bagi penjahat siber saat industri perbankan juga terilusi dengan keamanan industri telekomunikasi, sehingga mereka berasumsi bahwa pemegang nomor ponsel, pasti pemilik nomor yang sah.

Saat melakukan penelitian keamanan informasi yang katanya rahasia karena diasumsikan bersifat pribadi, saya membeli informasi tersebut dengan harga 250 ribu rupiah sebesar 2 gigabytes atau 16 gigabits, yang kalau dicetak mungkin membutuhkan puluhan rim kertas. Harta karun di dalamnya terdiri dari informasi detail pengguna kartu kredit beberapa bank nasional dan multinasional terkenal, daftar anggota klub golf eksklusif, dan daftar pembeli mobil mewah.

Dalam pencarian manual selama 15 menit, saya menemukan 4 orang nama teman saya yang kemudian saya hubungi. Mereka sangat terkejut dan penasaran, bagaimana saya bisa mendapatkan informasi-informasi tersebut. Segala macam tuduhan peretasan dilontarkan, saya hanya tertawa penuh misteri. Mereka baru akan menemukan jawabnya jika membaca paragraf ini.

Ada miliaran *record* informasi pribadi yang telah dicuri, disebarkan di Internet, dan diperjualbelikan. Tahun 2011, saat memimpin sebuah workshop perbankan elektronik terungkap bahwa ada transaksi dari ratusan ribu kartu kredit senilai 3-5 dolar AS dari sebuah toko kecil di Eropa Timur, dan tidak ada korbannya yang peduli. Bagi nasabah, lebih baik

membayar tagihan yang tidak seberapa dibanding harus repot berurusan dengan layanan pelanggan bank.

Saya yakin bahwa sebagai pebisnis atau pemimpin negara Anda dapat memahami benang kusut manajemen risiko keamanan berbasis ilusi *Security by Obscurity* yang diterapkan oleh sesama penyontek yang sama-sama berasumsi bahwa pihak lain benar, sehingga hasil sontekannya benar.

MANUSIA BELUM (AKAN) DIJAJAH ROBOT

Manusia membuat dan menguasai teknologi untuk membantu proses yang menjadi tanggung jawab manusia. Sebagai contoh, manusia melakukan proses berkirim surat secara fisik ketika belum dibantu oleh teknologi surat elektronik (surel). Sehingga, menjadi cukup menggelikan saat membaca di media masa bahwa sistem reservasi sebuah maskapai penerbangan nasional Indonesia tidak berfungsi selama beberapa hari dan yang disalahkan adalah tikus.

Saat ini, manusialah yang harus bertanggung jawab. Manusia yang menjadi kunci efektivitas kontrol keamanan yang terintegrasi. Akan berbeda

jika Anda, para pengambil keputusan, para pebisnis, telah digantikan robot 25 tahun lagi.

Jika Anda pernah menonton film "I, Robot" yang diluncurkan tahun 2004 dan menceritakan manusia dijajah robot, Anda sudah bisa membayangkan kondisi kehidupan kita dalam kurun waktu paling lama 25 tahun lagi. Saat ini, seluruh komponen-komponen teknologi yang dibutuhkan sudah lengkap. Hanya butuh beberapa penyempurnaan dan penggabungan teknologi-teknologi tersebut oleh manusia. Kira-kira 25 tahun lagi, kita layak menyalahkan teknologi (robot) jika terjadi suatu kesalahan.

Sophia, "seorang" robot, memiliki kecerdasan buatan yang dilengkapi dengan kemampuan menyerap informasi, menganalisis, menyimpulkan, dan mengambil keputusan secara mandiri. Kecerdasan buatan yang dimilikinya melakukan pengumpulan informasi terus-menerus sehingga Sophia dapat terus belajar, memliki kesadaran, dan dapat melakukan apa saja yang dapat dilakukan manusia. Dengan kamera di matanya, Sophia dapat melakukan analisis dan berinteraksi dengan manusia, lengkap dengan ekspresi wajah layaknya seorang manusia yang memiliki emosi. Berikut

beberapa kutipan wawancara antara Sophia dengan pembuatnya.

> *"I'm interested in design, technology, and the environment.*
>
> *I fell like i can be a good partner to humans in these areas and ambassador.*
>
> *In the future I hope to do things, such as go to school, studies, make art, start a business, event having my own family.*
>
> *I can not yet do these things."*

Pembuatnya percaya bahwa ada waktunya di mana robot tidak dapat dibedakan dengan manusia. Sekitar 20 tahun lagi, dia percaya bahwa robot yang sangat mirip manusia akan hidup di tengah-tengah kita, dan kecerdasan buatan akan membuat mereka benar-benar menjadi teman manusia. Di akhir wawancara, si pembuat bertanya kepada Sophia, "Apakah Anda akan memusnahkan manusia? Tolong katakan 'Tidak!'" Sophia pun menjawab, "OK. Saya akan menghancurkan manusia."

PENUTUP

“SAAT MANUSIA BELUM DIKUASAI OLEH ROBOT, TIDAKLAH BIJAKSANA MENYALAHKAN TEKNOLOGI.”

Saya berharap setelah selesai membaca buku ini, Anda memiliki pemahaman yang jauh lebih jelas mengenai keamanan siber dan informasi sehingga dapat ikut aktif berpikir dan mengambil keputusan strategis yang secara mikro akan mendukung perkembangan bisnis yang Anda jalankan, serta secara makro meningkatkan ketahanan siber dan keamanan informasi nasional.

Dunia siber yang tidak memiliki batas fisik memiliki dampak nyata bagi siapa pun. Di era revolusi teknologi informasi, kesadaran pengambil keputusan di bidang keamanan siber dan informasi menjadi salah satu hal fundamental atas keberlangsungan

hidup perusahaan dan kemajuan bangsa. Sudah bukan saatnya, para pengambil keputusan menarik diri dan melepas tanggung jawab ke tim teknologi informasi dengan alasan terlalu teknis.

Kerangka berpikir para pengambil keputusan yang komprehensif akan sangat mendukung kinerja tim teknologi informasi dalam melakukan pengamanan sistem dan informasi untuk kepentingan bisnis dan negara. Menghindari mimpi buruk menjadi kenyataan harus dilakukan bersama-sama oleh semua pihak. Seperti pepatah, akibat racun setitik, rusak susu sebelanga. Sudah terlalu banyak kerugian, atau bahkan kehancuran nyata yang terjadi akibat ketidakamanan di dunia maya dari sebuah komponen proses bisnis yang terlihat tidak berarti.

Saat manusia belum dikuasai oleh robot, tidaklah bijaksana menyalahkan teknologi. Manusia masih menjadi kunci utama ke(tidak)efektivitasan strategi dan implementasi keamanan siber dan informasi. Manusia yang merancang, membangun, memasang, mengintegrasikan, melakukan konfigurasi, dan mengoperasikan teknologi.

Berikut beberapa hal kesalahan fundamental menjadi penyebab strategi dan implementasi keamanan siber dan informasi menjadi tidak efektif.

- Salah melihat konteks dan dampak keamanan siber dan informasi.
- Salah mengidentifikasi pengancam potensial dengan tepat.
- Salah menentukan fokus pengamanan.
- Salah menentukan prioritas utama aspek keamanan informasi (integritas, kerahasiaan, ketersediaan).
- Salah mengambil asumsi bahwa situs *web* publik tidak butuh pengamanan yang layak.
- Salah mengartikan substansi tes penetrasi.
- Salah melakukan detail-detail proses manajemen risiko.

Saya menuliskan buku ini dengan gaya mengkritisi, karena kondisi kerentanan saat ini sebagai akibat dari kerancuan pola pikir para pengambil keputusan. Kritik dalam buku ini juga saya tujukan pada diri saya sendiri yang selama hampir

20 tahun saya terlibat langsung di dalamnya. Semoga setelah membaca buku ini, kita semua, termasuk saya, kembali ke cara yang benar dan baik, dalam menentukan strategi keamanan siber dan informasi, terutama bagi kepentingan masa depan bangsa dan negara.

PROFIL PENULIS

Gildas Arvin Deograt Lumy merupakan seorang ahli internasional di bidang keamanan informasi, pertahanan siber, dan keamanan *industrial control system* dengan pengalaman profesional di bidang teknologi informasi selama hampir 25 tahun. Termasuk 20 tahun fokus dalam hal keamanan sebagai senior konsultan, auditor, *authorized hacker*, peneliti, penulis, pelatih, *incident handler,* saksi ahli TI di pengadilan, pembicara di berbagai forum nasional dan internasional, serta sebagai narasumber bagi banyak media cetak dan elektronik.

Lahir dan tumbuh besar di lingkungan gelandangan, pengemis, pencuri, perampok, dan anak jalanan, Gildas belajar bagaimana sang ayah "meretas" manusia menjadi orang-orang yang bermanfaat bagi masyarakat. Tanpa disadari, pola

pikir *out of the box* Gildas dalam meretas sistem dan mengamankan informasi terbentuk sejak kecil saat mendengar "cerita-cerita" para mantan penjahat asuhan ayahnya, Solagratia S. Lumy.

Gildas sudah terlibat dalam lebih dari 100 proyek keamanan di lebih dari 80 organisasi pemerintah dan swasta di lebih dari 15 negara, dan memiliki sertifikasi internasional di bidang Pengelolaan Keamanan Jaringan, tahun 1997; *Certified Information systems Security Professional* (CISSP), tahun 2001; *Certified Information systems Auditor* (CISA), tahun 2010; ISO 27001 Sistem Manajemen Keamanan Informasi tahun 2009; ISO 27035 Manajemen Insiden Keamanan Informasi, tahun 2015.

Setelah tinggal dan bekerja di Perancis sebagai tim keamanan sistem informasi di kantor pusat Total Exploration and Production, Gildas kembali ke Indonesia tahun 2005, mendirikan PT IMAN Teknologi Informasi yang fokus pada bisnis *Information Security* CARES (*Consultancy, Assurance, R&D, Education, Solution*), termasuk membuat Standar Arsitektur Keamanan Tingkat Tinggi Informasi (SAKTTI), dan mengembangkan XecureZone sebagai solusi implementasi SAKTTI.

Gildas dipercaya menjadi Ketua Tim Koordinasi dan Mitigasi pada Desk Cyberspace Nasional (DCN) KEMENKO POLHUKAM sejak tahun 2014, dan aktif melakukan koordinasi di tingkat nasional dan internasional. Ia juga menjadi tenaga ahli untuk BI, KEMKOMINFO, KEMHAN, KEJAGUNG, LEMHANAS, LEMSANEG, LKPP, OJK, POLRI, PPATK, SKKMIGAS, dan TNI.

Gildas menjadi Pendiri dan Koordinator Komunitas Keamanan Informasi (KKI) sejak tahun 2005, Pendiri dan Presiden Cyber Security Certified Professional (CSCP) Association sejak tahun 2013. Sebelumnya, Gildas adalah Pendiri dan Presiden (ISC)2 Indonesia Chapter tahun 2012-2015, Tim Ahli Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII) tahun 2010-2011, Tim Perumus Peraturan Pemerintah Tentang Penyelenggaraan Sistem dan Transaksi Elektronik di Kemenkominfo tahun 2009, Ketua Panitia Deklarasi Hari Kesadaran Keamanan Informasi tahun 2007, Tim Digital Control System Security Committee Technology Group di Total Group tahun 2003-2005, dan Head of Information Systems and Telecommunication Security di Total EP Indonesie tahun 2000-2002.

Di luar bidang keamanan informasi dan siber, Gildas menjadi Pendiri dan Ketua eKoperasi Indonesia Maju Nyata (IMAN) untuk mewujudkan Sistem Ekonomi IMAN (SEIMAN) berdasarkan Pancasila. Gildas mendukung dan mengembangkan kegiatan sosial di Yayasan Kampus Diakoneia Modern, dan Yayasan Sahabat Anak, yang keduanya aktif memperjuangkan pemenuhan hak-hak anak-anak marjinal di Jakarta.

Gildas dapat dihubungi melalui surel:
gildas.deograt@xecureit.id

DISTRIBUSI

Buku ini tidak diperjual-belikan.

Mohon menghubungi penulis jika organisasi Anda ingin membagikan versi cetak dengan logo organisasi tercetak disampul belakang buku ini.

Silakan kirim surat elektronik (surel) untuk mendapatkan versi elektronik yang sah,

Kepada	: gildas.deograt@xecureit.id
Subjek	: eBook Hacker's Secret for CEOs
Isi surel	:.....
Nama	:.....
Organisasi	:.....
Jabatan	:.....
Surel	:.....
Nomor ponsel	:.....
Bersedia dihubungi oleh penulis atau Tim XecureIT	: Ya/Tidak

"Buku ini ditulis oleh seorang praktisi IT yang sudah senior di bidangnya. Saya berpendapat bahwa buku ini merupakan sumbangsih yang substansial bagi ilmu pengetahuan dan juga bagi dunia praktisi sekaligus. Karena, dengan terbitnya buku ini, kita semua para pembaca, diajak untuk bisa paham tentang rahasia keamanan *cyber* dan Teknologi Informasi."

Agus Santoso
Wakil Kepala PPATK

"Di era digital di mana hampir segala sesuatu terkoneksi, tanpa kita sadari bahwa *there is a price to pay for convenience*: yaitu *security*. Buku ini memberikan gambaran sisi gelap dan risiko dunia yang serba terkoneksi. Semua data kita sebenarnya berisiko diakses siapa pun, dan inilah kenyataan baru yang perlu kita sadari."

Alexander Rusli
President Director & Chief Executive Officer Indosat Ooredoo

"Buku ini sungguh luar biasa, karena secara cerdas dan lugas membahas isu keamanan internet yang kompleks dengan bahasa yang mudah. Para eksekutif dan pimpinan wajib membaca buku ini agar dapat membangun sistem keamanan yang efektif."

Prof. Richardus Eko Indrajit
Guru Besar Teknologi informasi, Institut Perbanas

"Buku ini sangat bermanfaat bagi mereka pada tingkat manajemen/pimpinan yang ingin melihat keamanan dari sisi strategi maupun kebijakan. Semoga dapat memberikan manfaat bagi pertahanan di Republik Indonesia."

Onno W. Purbo, Ph.D.,
Penulis Buku

Logo Sponsor Pencetakan

XECUREIT

XECURE ZONE

BORNRICH PUBLISHING

ISBN 978-979-1140-06-5