CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 2, No. 2, November 2019, hlm. 77-81

PENGARUH ETHICAL HACKING BAGI KEAMANAN DATA PERUSAHAAN

Ahmad Ridha Kelrey[1], Aan Muzaki[2]

[1,2]Magister Teknik Informatika Universitas Islam Indonesia Yogyakarta
Email: [1]18917103@students.uii.ac.id, [2]18917101@students.uii.ac.id

Abstrak

Melindungi aset digital merupakan perhatian yang penting bagi perusahaan, karena serangan siber memengaruhi kinerja bisnis dan reputasi sebuah perusahaan. Tiga konsep dasar keamanan yang penting untuk informasi di internet adalah kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Konsep yang berkaitan dengan orang-orang yang menggunakan informasi itu adalah *authentication*, *authorization*, dan *nonrepudiation*. Keamanan informasi menjadi suatu hal yang mahal pada saat ini, sehingga ethical hacking diperlukan untuk menjamin sebuah sistem informasi perusahaan tersebut cukup handal. Dengan begitu dapat menjaga reputasi perusahaan tersebuat di mata pelangannya.

Kata kunci: *Ethical Hacking, Keamanan Informasi, Confidentiality, Integrity, Availability*

ETHICAL HACKING EFFECT FOR COMPANY DATA SECURITY

Abstract

Protecting digital assets is an important concern for companies, because cyber attacks affect the business performance and reputation of a company. Three basic security concepts that are important for information on the internet are confidentiality, integrity, and availability. Concepts relating to people who use that information are authentication, authorization, and nonrepudiation. Information security is becoming expensive at this time, so ethical hacking is needed to guarantee that a company's information system is quite reliable. That way can maintain the company's reputation in the eyes of its customers.

Keywords: *Ethical Hacking, Information Security, Confidentiality, Integrity, Availability*

1. PENDAHULUAN

Melindungi aset digital merupakan perhatian yang penting bagi perusahaan, karena serangan siber memengaruhi kinerja bisnis dan reputasi sebuah perusahaan. Keamanan teknologi informasi secara umum dan keamanan dunia siber secara khusus adalah area yang berkembang sangat cepat dan membutuhkan evaluasi dan inovasi berkelanjutan. Tujuan serangan cyber tidak berubah dari waktu ke waktu, namun ada perubahan dalam metode serangan melalui peningkatan penggunaan rekayasa sosial (*social engineering*) yang berkonsentrasi pada elemen manusia sebagai titik terlemah dalam struktur keamanan sebuah sistem (Torten, Reaiche, & Boyle, 2018).

Tanpa data, organisasi kehilangan catatan transaksi dan kemampuannya untuk memberikan nilai lebih kepada pelanggan. Setiap bisnis, lembaga pendidikan, atau lembaga pemerintah yang beroperasi dalam konteks modern dengan layanan yang terhubung dan responsif bergantung pada sistem informasi. Bahkan ketika transaksi tidak online, sistem informasi dan data yang mereka proses memungkinkan penciptaan dan pergerakan barang dan jasa. Oleh karena itu, keamanan data, melindungi data dalam transmisi, dalam pemrosesan, dan saat istirahat (penyimpanan) adalah aspek penting dari keamanan informasi. Nilai data memotivasi penyerang untuk mencuri, menyabotase, atau merusaknya. Program keamanan informasi yang efektif yang diterapkan oleh manajemen melindungi integritas dan nilai data organisasi (Whitman, 2016).

Tiga konsep dasar keamanan yang penting untuk informasi di internet adalah kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Konsep yang berkaitan dengan orang-orang yang menggunakan informasi itu adalah *authentication*, *authorization*, dan *nonrepudiation* (Pesante, 2008). Kerahasiaan mengacu pada privasi data di mana data milik perusahaan tidak diungkapkan kepada pihak yang tidak berwenang pada setiap kesempatan. Integritas

data mengacu pada keyakinan bahwa data yang disimpan di cloud tidak dipermainkan oleh pihak yang tidak berwenang. Itu juga berlaku ketika data dalam perjalanan. Ketersediaan data mengacu pada janji bahwa setiap kali perusahaan membutuhkan data, data tersebut harus tersedia bagi mereka tanpa penundaan atau penolakan. Ketiga sifat keamanan data dasar ini banyak diuji dalam model penyebaran cloud publik. Otentikasi adalah bukti bagi seseorang untuk mengakses datanya sendiri. Otorisasi adalah tindakan menentukan apakah seseorang memiliki hak untuk melakukan aktivitas pada data seperti membaca atau menulis. Pengguna harus diautentikasi sebelum melakukan aktivitas yang diizinkan untuk mereka lakukan. Nonrepudiation adalah jaminan bahwa pengguna yang diautentikasi tidak dapat menyangkal setelah melakukan pekerjaan (Kumar, Raj, & Jelciana, 2018).

Ethical hacking adalah disiplin dalam meningkatkan dan menggabungkan kerentanan sistem yang diketahui dan mungkin melibatkan unsur rekayasa sosial (*social engineering*) yang dilakukan dengan cara yang bertanggung jawab. Ethical hacking identik juga disebut sebagai ”*Network penetration* (*pen*) *test*” dan biasanya akan melibatkan elemen fisik juga. Seorang hacker yang baik, ibaratkan akan menyerang sebuah pintu, membukanya, dan mendapatkan akses tanpa merusak pintu tersebut, baik dengan cara mengambil kunci, mengurangi atau merusak sistem yang terkomputerisasi (Ellis, 2017).

2. KONSEP KEAMANAN INFORMASI

Perlindungan informasi di era informasi elektronik dan digital ini lebih penting, dan lebih kompleks, daripada sebelumnya. Kerugian atau pencurian informasi yang penting bagi produk, metode, atau proses perusahaan mungkin sangat menghancurkan. Di era persaingan global ini, yang terpenting menerapkan program komprehensif untuk perlindungan informasi sangat penting dan tidak dapat dilebih-lebihkan.

Keamanan adalah perlindungan. Perlindungan dari musuh yang akan melakukan kejahatan, dengan sengaja atau tidak sengaja adalah tujuan utama keamanan. Keamanan nasional, misalnya, adalah sistem berlapis-lapis yang melindungi kedaulatan negara, asetnya, sumber dayanya, dan rakyatnya. Untuk mencapai tingkat keamanan yang sesuai untuk suatu organisasi juga membutuhkan sistem yang beragam. Organisasi yang sukses harus memiliki banyak lapisan keamanan untuk melindungi operasinya, infrastruktur fisik, orang, fungsi, komunikasi, dan informasi.

Gambar 1. CIA Triangle (ibm.com)

Prinsip keamanan informasi merupakan perlindungan terhadap aspek-aspek berikut:

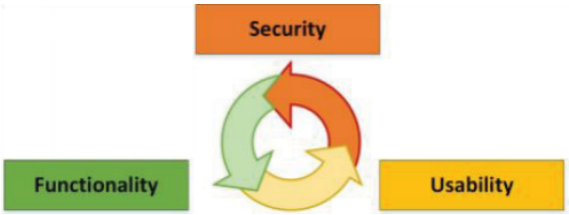
a. Confidentiality (kerahasiaan) yaitu aspek yang menjamin kerahasiaan data atau informasi, dan memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima, dan disimpan.
b. Integrity (integritas) yaitu aspek yang menjamin bahwa data tidak dilakukan perbuahan tanpa izin dari pihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini tetap terpenuhi.
c. Availability (ketersediaan) yakni aspek yang menjamin bahwa data tersedia ketika dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait.

Aspek ancaman terhadap keamanan informasi diantaranya adalah:

a. Interruption yaitu data dan informasi dalam sistem komputer dirusak dan dihapus data atau informasi tersebut tidak dapat diakses saat dibutuhkan.
b. Interception yaitu Informasi disadap oleh orang yang tidak berhak.
c. Modification yaitu aktivitas menyadap lalu lintas informasi yang sedang dikirim dan mengubah data atau informasi yang melintas tersebut tanpa ijin.
d. Fabrication yaitu orang yang meniru pemberi informasi, sehingga pihak yang menerima menyangka informasi tersebut berasal dari orang yang benar/ dikehendaki oleh si penerima informasi.

Dalam suatu sistem, tingkat keamanan adalah ukuran dari kekuatan keamanan dalam sistem, fungsionalitas, dan kegunaan. ketiga komponen ini dikenal sebagai segitiga keamanan, fungsionalitas, dan kegunaan. Pertimbangkan bola dalam segitiga ini, jika bola lebih dekat dengan keamanan, itu berarti sistem mengkonsumsi lebih banyak sumber daya untuk keamanan dan fitur serta fungsi sistem dan kegunaan memerlukan perhatian. Sistem yang aman harus memberikan perlindungan yang kuat

bersama dengan menawarkan semua layanan dan fitur serta kegunaan bagi pengguna.



Gambar 2. Security, Functionality, Usability Triangle

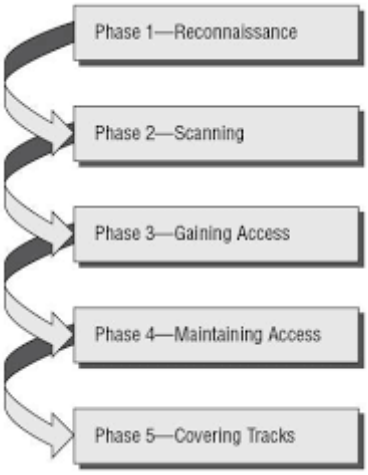
3. KONSEP HACKING

Hacking adalah teknik yang dilakukan oleh seseorang (hacker, cracker, penyusup, atau penyerang) untuk menyerang suatu sistem, jaringan, dan aplikasi dengan cara mengkesploitasi kelemahan dengan maksud untuk mendapatkan hak akses atas data dan sistem.

Istilah "Hacking" dalam keamanan informasi mengacu pada mengeksploitasi kerentanan dalam suatu sistem, membahayakan keamanan untuk mendapatkan perintah dan kontrol yang tidak sah atas sumber daya sistem. Tujuan peretasan dapat mencakup modifikasi sumber daya sistem, gangguan fitur dan layanan untuk mencapai tujuan. Ini juga dapat digunakan untuk mencuri informasi untuk penggunaan apa pun seperti mengirimkannya ke pesaing, badan pengawas atau mempublikasikan informasi sensitif.

Hacker dapat diklasifikasikan dalam kategori yang berbeda, secara umum terdapat tiga kategori yakni :

a. Black Hat Hacker adalah tipikal hacker yang berbahaya dan jahat, biasanya dimotivas oleh uang, balas dendam, kriminal, dll. Mereka mendapatkan akses tidak sah kedalam sistem, merusaknya dan atau mencuri informasi yang sensitif.
b. White Hat Hacker dikenal sebagai Ethical Hacker. Mereka tidak pernah bermaksud untuk merusak suatu sistem, namun mereka mencoba untuk mengetahui kelemahan dalam komputer atau sistem jaringan sebagai bagian dari penetration testing dan/atau vulnerability assessments.
c. Grey Hat Hacker adalah hacker diantara black hat dan white hat hacker. Terkadang melakukan peretasan dengan memanfaatkan kelemahan sistem layaknya black hat hacker. Di satu sisi menjadi konsultan keamanan layaknya white hat hacker.



Gambar 3. Metode Hacking

Reconnaissance

Reconnaissance adalah tahap mengumpulkan data, dimana hacker akan mengumpulkan data tentang target dari berbagai sumber yang mendukung. Baik nama anggota keluarga, tanggal lahir, tempat kerja beserta informasi didalamnya. Dan itu hanya sebagian kecil kegunaan dari tahapan Reconnaissance.

Reconnaissance terbagi menjadi dua yaitu Active Reconnaissance dan Passive Reconnaissance.

a. Active Reconnaissance

Hacker melakukan proses pengumpulan informasi dengan cara yang sangat beresiko karena beraktifitas langsung dengan korban atau rekan korban.

b. Passive Reconnaissance

Hacker melakukan pencarian informasi tanpa sepengetahuan korban, sebagai contoh hacker akan melakukan *profiling* data korban di internet.

Scanning

Scanning adalah tahap secara aktif menyelidiki kerentanan yang bisa dimanfaatkan dari target.

Gaining access

Gaining access adalah tahapan proses penetrasi sudah dilakukan. Hacker akan berusaha menguasai sistem target dari kelemahan target sistem yang telah diperoleh dari hasil scanning.

Maintaining access

Maintaining access adalah tahap proses dimana hacker telah mendapatkan akses ke sistem. Kemudian hacker menanamkan *backdoor* ke dalam sistem agar dia tetap mendapatkan akses tersebut.

Clearing Tracks

Clearing Tracks adalah tahap hacker akan menutup jejaknya dengan menghapus log file dan jejak-jejak yang mungkin ditinggalkan.

4. PENTINGNYA ETHICAL HACKING

Meningkatnya aktivasi berbahaya, kejahatan dunia maya dan munculnya berbagai bentuk serangan lanjutan memerlukan perlunya penetrasi tester yang menembus keamanan sistem dan jaringan untuk ditentukan, mempersiapkan dan mengambil tindakan pencegahan dan perbaikan terhadap serangan agresif ini.

Pada awal konflik internasional, organisasi teroris mendanai penjahat cyber untuk melanggar sistem keamanan, baik untuk mengkompromikan fitur keamanan nasional atau untuk memeras jumlah besar dengan menyuntikkan malware dan menolak akses. Menghasilkan maraknya kejahatan dunia maya. Organisasi menghadapi tantangan memperbarui taktik pencegahan peretasan, memasang beberapa teknologi untuk melindungi sistem sebelum menjadi korban peretas. Malware, virus, dan ransomware berkembang biak setiap hari dan menciptakan kebutuhan akan layanan *ethical hacking* untuk melindungi jaringan bisnis, agen pemerintah, atau pertahanan.

World Economic Forum (WEF) sekarang menganggap kejahatan dunia maya sebagai salah satu ancaman terbesar bagi bisnis dan ekonomi, sebagaimana dicatat dalam Laporan Risiko Global 2019. Dan itu bukan lagi hanya perusahaan besar yang berisiko. Hiscox memperkirakan bahwa usaha kecil saja adalah target dari 65.000 serangan cyber setiap hari, yang mengarah pada peretasan yang berhasil setiap 19 detik dan biaya pembersihan rata-rata £ 25.700 per tahun. Identifikasi dari mana serangan ini dapat berasal harus menjadi bagian dari proses manajemen risiko dan setiap organisasi yang terhubung ke Internet harus berasumsi bahwa itu akan menjadi korban, cepat atau lambat. Memahami ini adalah langkah pertama untuk menilai kerentanan suatu organisasi - tetapi memprediksi bagaimana hal itu dapat dikompromikan tidaklah mudah.

Lanskap ancaman terus berubah dan bisnis perlu melakukan semua yang mereka bisa untuk tetap up to date. Misalnya, laporan terbaru Symantec mengamati penurunan aktivitas ransomware untuk pertama kalinya sejak 2013.3 Pergeseran ini mungkin disebabkan oleh penurunan aktivitas kit eksploitasi dan perpindahan ke kampanye email sebagai metode distribusi alat tebusan utama. Namun, ini memperlihatkan organisasi-organisasi yang sangat bergantung pada lalu lintas email - yang mengarah ke infeksi perusahaan meningkat sebesar 12%. Symantec juga mencatat peningkatan serangan formjacking, dengan rata-rata 4.800 situs web dikompromikan dengan kode formjacking setiap bulan. Seringkali pengecer kecil dan menengah yang menyuntikkan kode ke situs mereka yang kemudian dapat menyebar secara global ke bisnis apa pun yang menerima pembayaran online. Organisasi juga harus beradaptasi strategi pertahanan mereka sebagai pelanggaran dapat terjadi melalui cloud, dari kerentanan dalam chip perangkat keras, melalui open source DevOps dan dengan menginfeksi perangkat Internet of Things (IoT). Dan adaptasi ini bukanlah proses yang mudah bagi organisasi untuk mencapai, terutama pada saat semakin sulit untuk merekrut dan mempertahankan para profesional keamanan cyber yang mahir secara teknis.4 Akibatnya, semua organisasi perlu mengadopsi budaya sadar-keamanan cyber yang didukung di semua tingkatan, dari anggota dewan hingga junior kantor, dan tertanam dalam semua pengambilan keputusan. Memiliki kebijakan dan prosedur yang tepat di tempat sangat penting dan ini juga harus mencakup perangkat yang dimiliki karyawan. Keamanan dunia maya tentunya harus menjadi bagian dari nilai-nilai kunci organisasi mana pun. Pengujian penetrasi adalah salah satu cara untuk memastikan ini terjadi.

Dengan WEF mengkonfirmasikan bahwa kejahatan dunia maya adalah salah satu ancaman terbesar bagi bisnis, tampaknya mengejutkan bahwa dalam laporan baru-baru ini, hanya 38% dari para pemimpin bisnis mengatakan bahwa meningkatkan keamanan dunia maya adalah prioritas untuk investasi TI mereka. Ancaman ini tidak akan hilang, jadi pertanyaan utama bagi banyak bisnis adalah: apakah kita benar-benar membutuhkan pengujian penetrasi? Di lingkungan hari ini, jawabannya akan selalu ya. Tentu saja, pengujian penetrasi dipandang sebagai latihan yang mahal. Namun, seperti kebanyakan hal, organisasi perlu menyeimbangkan biaya dengan risiko serangan. Bagi sebagian orang, biaya serangan lebih nyata - misalnya, apakah bisnis sangat bergantung pada aplikasi online untuk memproses data pribadi yang dapat dicuri? Atau apakah jaringan dan infrastrukturnya penting untuk bisnis? Hal ini membuat pengujian penetrasi lebih mudah dijual kepada eksekutif tingkat C atau direktur keuangan. Bagi orang lain yang tidak memroses data sensitif, dampak serangan atau pelanggaran dapat mencakup kerusakan reputasi atau pelanggan yang marah karena down-time di situs web.

Pengujian penetrasi adalah bentuk *ethical hacking* tetapi, untuk kejelasan, agar peretasan dapat diklasifikasikan sebagai etis perlu ada perjanjian antara peretas etis dan organisasi dengan persetujuan tertulis dari organisasi. Kalau tidak, menurut surat hukum tersebut, Undang-Undang Penyalahgunaan Komputer Inggris 1990, misalnya hanya peretasan. Lebih dari itu, perusahaan keamanan mana pun yang dipilih harus memiliki kredensial dan kualifikasi yang tepat.

5. KESIMPULAN

Keamanan informasi menjadi suatu hal yang mahal pada saat ini, sehingga ethical hacking diperlukan untuk menjamin sebuah sistem informasi perusahaan tersebut cukup handal. Dengan begitu dapat menjaga reputasi perusahaan tersebuat di mata pelangannya.

Pencurian data perusahaan mungkin bukan hanya satu aspek dari segala upaya peretasan. Perusahaan mungkin mempunyai anggaran yang tidak terbatas untuk dibelanjakan pada aspek keamanan siber, tetapi penetration testing terhadap sistem informasi perusahaan dapat membantu memprioritaskan pengeluaran yang tidak diinginkan dan mencegah terjadinya pengeluaran yang tidak diinginkan.

DAFTAR PUSTAKA

ELLIS, S. R. (2017). *Ethical Hacking*. *Computer and Information Security Handbook*. Elsevier Inc. https://doi.org/10.1016/B978-0-12-803843-7.00030-2

ECCOUNCIL. 2008. *Module I: Introduction to Ethical Hacking*, *Ethical Hacking and Countermeasures Version 6*

KUMAR, P. R., RAJ, P. H., & JELCIANA, P. (2018). ScienceDirect Procedia Computer Science Exploring Data Security Issues and Solutions in Cloud Computing. *Procedia Computer Science*, *125*(2009), 691–697. https://doi.org/10.1016/j.procs.2017.12.089

PESANTE, L. (2008). Introduction to Information Security, (January), 1–3. Retrieved from https://www.us-cert.gov/sites/default/files/publications/infosecuritybasics.pdf

TORTEN, R., REAICHE, C., & BOYLE, S. (2018). US CR. *Computers & Security*. https://doi.org/10.1016/j.cose.2018.08.007

WHITMAN, M. E. (2016). *Principles of Information Security Fifth Edition*.

'The Global Risks Report 2019'. World Economic Forum. www.wefo- rum.org/reports/the-global-risks- report-2019. [Accessed 04-Aug 2019]

'UK small businesses targeted with 65,000 attempted cyber attacks per day'. Hiscox. www.hiscoxgroup.com/news/press-releases/2018/18-10-18. [Accessed 04-Aug 2019]

'2019 Internet Security Threat Report'. Symantec. www.symantec.com/security- centre/threat-report. [Accessed 04-Aug 2019]

TOUHILL, GREGORY. 'Challenges on Cyber security Landscape Demand Strong Leadership'. ISACA, 20 Mar 2019. www. isaca.org/Knowledge-Centre/Blog/ Lists/Posts/Post.aspx?ID=1154. [Accessed 04-Aug 2019]