MORALITY OPAQUE IN VULNERABILITY DISCLOSURE

Penulis: Muhammad Zia ul Haq

Latar Belakang

Keamanan dalam dunia teknologi informasi (infosec) menjadi salahsatu perhatian yang tiada hentinya dibahas oleh berbagai kalangan, baik yang berkonsetrasi pada bidang TI, maupun masyarakat umum yang tidak lepas hajat hidupnya dari peran TI. Perhatian yang sangat besar ini pantas terjadi dikarenakan keamanan merupakan keniscayaan yang diharapkan dapat dirasakan bagi setiap pihak yang terkait dengan teknologi informasi. Perhatian ini dijewantahkan dengan usaha dan investasi yang sangat tinggi. Pada tahun 2016, sekitar 81,6 miliar dollar dihabiskan oleh berbagai pihak hanya untuk memastikan keamanan sistem informasi mereka (Gartner, 2016). Diantara persoalan keamanan yang paling mendapat perhatian adalah masalah celah kelemahan sistem yang menimbulkan kerentanan keamanan. Dasar utama *flaw* (celah) dapat dikategorikan sebagai rentan *(vulnerable)* hanya jika berpotensi munculnya penyalahgunaan (Brian Ruder, 1978). Penyalahgunaan ini berawal dari tindakan eksploitasi pada sistem yang didasari pengetahuan yang dimiliki oleh si penyerang akan adanya kerentanan *(vulnerability)* dalam sistem targetnya.

Terbukanya akses ke sumber yang menyediakan informasi tentang celah keamanan suatu sistem yang rentan, pada satu sisi akan menjadikan sistem tersebut semakin beresiko dari tindakan eksploitasi bahkan pada tingkat yang sangat masif. Namun pada sisi lain, keterbukaan ini juga dianggap berdampak positif, baik bagi pengguna maupun pengembang sistem jika dikaitkan dengan aspek-aspek tertentu.

Dilema ini kemudian dapat dihubungkan dan dianalisa berdasarkan tinjauan etika dalam komputer yang dimaksudkan untuk menemukan benang merah dari perbedaan pendapat tentang bagaimana seharusnya suatu *vulnerability* dari sebuah sistem disikapi secara etis dan bermoral. Tujuannya adalah, agar dampak yang ditimbulkan dan berpotensi merugikan dapat diminimalisir sejak dini melalui sikap etis yang dimiliki oleh pihak yang menemukan celah tersebut, pihak pemilik sistem serta pihak-pihak lainnya yang turut mengetahui keberadaannya.

Vulnerability Disclosure

Vulnerability yang juga disebut sebagai *attacker surface* (Edward Skoudis, 2005) didefinisikan sebagai celah dan kelemahan dari desain suatu sistem dan implementasinya (operasional dan manajemen) yang dapat dieksploitasi untuk mengganggu keamanan sistem (Steve Christey, 2002). Termasuk didalamnya hal yang terkait dengan kontrol internal, prosedur dan administrasi (Longley, 1987). Dari berbagai definisi yang ada, dapat disimpulkan bahwa celah keamanan dalam sebuah sistem informasi tidak saja ditemukan dalam aset, namun juga berpotensi ada pada manajemen dan kebijakan. Hal ini berarti bahwa, potensi adanya celah kelemahan dalam sistem komputer memang sangat besar. Sehingga para ahli berkesimpulan; tidak satupun sistem komputer, terlebih lagi yang terhubung dengan komputer lainnya yang memiliki tingkat keamanan 100% (Oliva, 2004). Meski demikian, tidak semua sistem dinyatakan bermasalah terutama jika celah tersebut belum atau tidak diketahui.

Untuk mengetahui ada tidaknya celah pada suatu sistem, selain dilakukan dengan sengaja melalui serangkaian aktivitas internal (audit dan *penetration test* contohnya), atau aktivitas yang dilakukan oleh pihak ketiga melalui *computer offences* (hacking) (Maurushat, 2014), juga dapat diketahui tanpa kesengajaan (Gary Stoneburner, Alice Goguen, Alexis Feringa, 2002). Bahkan dapat diketahui hanya dengan mengakses beberapa sumber yang menyediakan informasi tentang kelemahan-kelemahan yang dapat dieksploitasi. Ketersediaan informasi *vulnerability* yang berasal dari sumber-sumber

tertentu menjadi satu problematika etika (Stephen Northcutt, 2004) yang secara khusus terkait dengan sebuah istilah yakni *vulnerability disclosure.* Techopedia mendifinisikan *vulnerability disclosure* sebagai kebijakan yang dipraktekkan baik bagi individu maupun organisasi dalam penyingkapan dan publikasi informasi yang berkenaan dengan celah keamanan dan eksploitasi sistem komputer, jaringan dan perangkat lunak (Techopedia, 2017).

Morality Opaque dalam VD

Vulnerability Disclosure oleh banyak pihak berwenang dan pada kebanyakan negara, tidak digolongkan sebagai suatu tindakan kriminal (Biancuzzi, 2008). Meskipun demikian para ahli memandang bahwa keberadaannya perlu diatur secara etis, dikarenakan kemungkinan dampaknya yang berpotensi sangat serius terhadap keamanan sistem. Pengaturan etika ini dituangkan dalam dokumen kebijakan dengan bentuk yang berbeda-beda oleh berbagai pihak sesuai dengan perspektif yang dimilikinya. Contohnya dalam kebijakan Vulnerability Disclosure yang diatur oleh Cisco (Cisco, 2017), Cloudflare (Cloudflare, 2017) dan Microsoft (Microsoft, 2017). Meski dengan redaksi yang berbeda, pada dasarnya ketiga perusahaan ini setidaknya telah menetapkan rambu-rambu dan etika yang relatif jelas terkait dengan VD. Walaupun telah tercantum dalam *policy*, pada prakteknya, tidak seluruh kemungkinan fakta yang ada, dapat diatur dan dituangkan dalam susunan redaksional. Adanya ketidak jelasan pada persoalan ini kemudian dapat dikategorikan menjadi tanggung jawab moral yang kabur (morally opaque).

Morally Opaque merupakan istilah yang dialamatkan pada suatu praktek tertentu yang belum cukup diakui oleh para ahli (Brey, 2000). Tertuang dan terdefinisi secara tekstual namun prakteknya belum menunjukkan netralitas dalam aspek moral. *Morally Opaque* dalam konteks VD secara umum tergambar dalam perdebatan dan perbedaan perspektif berbagai pihak yang dapat dirangkum kedalam 3 (tiga) pandangan, yakni:

- ***Secrecy*** **atau** ***non-disclosure*** (Knapp, 2009), penemu celah keamanan menyembunyikan temuannya, tidak mengordinasikannya pada pemilik sistem dan tidak pula memublikasikan temuannya. Perspektif ini berdasar pada sebuah alasan bahwa dengan membuka celah keamanan ke publik dapat menyebabkan eksploitasi yang akan merugikan semua pihak. Menyembunyikannya menjadikan sistem relatif aman dari gangguan yang masif. Secara sepintas konsep ini sangat moralis, namun faktanya, beberapa pihak menggunakan *secrecy vulnerability* untuk mendapatkan keuntungan sepihak dan kelompoknya sebanyak-banyaknya. Ketidakterbukaan penemu kelemahan sistem komputer ke publik, menjadikan stakeholder sistem tersebut tidak sadar akan adanya ancaman bahkan eksploitasi oleh pihak tertentu.

- ***Responsible*** **atau** ***coordinated disclosure*** (Andrew Cencini, 2005), mengordinasikan dan memberikan waktu kepada vendor sistem untuk melakukan perbaikan, sebelum melakukan publikasi *vulnerability* kepada publik. Konsep ini banyak dianjurkan oleh beberapa perusahaan seperti yang telah disebutkan diatas. Secara teori, pendekatan ini menjadi konsep ideal; terjalinnya hubungan dan kordinasi antara pengembang dan penemu *vulnerability* berpeluang besar memberi solusi yang tepat bagi keamanan sistem tersebut. Biasanya pihak pengembang mengeluarkan *patch* untuk sistemnya sekaligus memublikasikan bersamaan dengan *vulnerability* yang ditemukan.

  Namun dalam prakteknya, pihak pengembang kadang tidak begitu proaktif terhadap laporan yang ada, sebaliknya tidak jarang ditemukan, pihak penemu meminta imbalan atas temuannya. Fakta ini menjadikan kesepakatan antar kedua pihak menjadi buntu. Kebanyakan *policy* yang diberlakukan oleh perusahaan yang menerapkan c*oordinated disclosure*, tidak mendeskripsikan adanya imbalan dari penemuan *vulnerability* pada sistem mereka. Salahsatu alasannya adalah adanya kekhawatiran, ketika imbalan diberlakukan, maka sistem mereka akan mendapatkan percobaan penetrasi yang masif oleh pihak-pihak yang

menginginkan imbalan tersebut, disamping perusahaan harus menyiapkan dana yang tidak sedikit untuk "membayar" setiap temuan yang ada.

- *Full Disclosure* , membuka *vulnerability* secara detail ke publik melalui media publik (Maurushat, 2014), baik yang terkait maupun tidak ada hubungannya dengan pemilik sistem. *Full Disclosure* dapat diakses melalui beberapa forum, mailing list dan website yang memberi kesempatan bagi siapa saja berkontribusi untuk mempublikasi temuannya dan informasi tambahan yang terkait dengan temuan kelemahan sistem komputer yang ditemukan. Beberapa diantaranya mencantumkan cara mengeksploitasi kelemahan tersebut, contohnya pada website exploit-db.com. Alasan yang mendasari konsep ini adalah bahwa kelemahan sistem komputer utamanya yang luas digunakan, harus diketahui oleh masyarakat secara umum, utamanya bagi penggguna. Hal ini bertujuan memberi *warning* kepada mereka untuk berhati-hati sekaligus mengandung tuntutan bagi pengembang agar segera melakukan perbaikan sistem. Pengembang, secara psikologis dipaksa untuk secepatnya memberikan respon dan melakukan *patching* sebagai bentuk tanggung jawab sekaligus untuk menjaga reputasinya.

  Namun pendekatan diatas, juga memiliki sisi yang buram dalam aspek moral. Realitas yang terjadi menunjukkan penyalahgunaan informasi *vulnerable system* yang dipublikasikan secara umum kerap ditemukan pada aktivitas *hacking* (Steven DeFino, Larry Greenblatt, 2012) utamanya yang dilakukan oleh pemula. Kemudahan dalam menemukan target, menjadikan aktivitas eksplotasi dan penetrasi ke sistem komputer menjadi marak dan sangat merugikan banyak pihak.

Ketiga pendekatan yang diuraikan diatas; secara konsep, memiliki dasar yang terdeskripsi dengan baik. Meski demikian, implementasinya masih menyisakan masalah "terselubung" yang berdampak pada tindakan-tindakan yang terkait dengan moralitas. Bahkan beberapa diantaranya dapat menimbulkan reaksi yang berlawanan dengan hukum

seperti manipulasi dan pengrusakan sistem, pencurian data permintaan tebusan. Dari ketiga pilihan yang ada, model *coordinated disclosure* dipandang oleh beberapa pihak sebagai pilihan yang memiliki kemaslahatan paling banyak. Selain diatur dalam draf kebijakan yang disosialisasikan dan diterapkan oleh beberapa lembaga negara seperti yang dilakukan di Amerika, Inggris dan Australia (Lohrmann, 2016). Beberapa perusahaan terkenal telah menerapkan kebijakan terkait pemberian imbalan yang menjadi persoalan dalam penerapan *coordinated disclosure* melalui program yang disebut sebagai *bug bounty program* (Techtarget, 2017).

Kesimpulan dan Saran

Dari pembahasan yang diuraikan diatas, terdapat beberapa hal yang dapat disimpulkan, sebagai berikut:

- *Vulnerability* menjadi sesuatu yang sangat serius bagi keamanan sistem komputer, olehnya dipandang perlu adanya satu kesimpulan dalam menyikapi keterbukaannya. Khususnya dalam hal bagaimana kemudian *vulnerability* tersebut dipublikasikan dan disikapi.
- Teorinya, ketiga pendekatan ini telah didasari oleh argumentasi etis, namun pada prakteknya menimbulkan keburaman dalam aspek moral.
- Meskipun VD dipandang bukan merupakan tindakan kriminal, namun adanya *morally opaque* pada VD, berpotensi memunculkan pelanggaran hukum.
- Beberapa lembaga negara dan perusahaan telah mengatur VD dalam sebuah kebijakan (*policy)* dan dikaitkan dengan aspek etika dan moral dalam teknologi informasi dalam bentuk pendekatan yang disebut sebagai *coordinated disclosure.*

Sebagai penutup, penulis juga menyertakan beberapa saran sebagai berikut:

- Persoalan etika dan moral dalam *vulnerability disclosure* menjadi tanggung jawab seluruh pihak; baik pemilik sistem, pembuat sistem, pihak yang menemukan

kelemahan sistem, pihak yang mempublikasi dan pihak yang mengakses informasi kelemahan tersebut.

- Memperjelas keburaman aspek moral kedalam bentuk hukum yakni dengan melakukan klasifikasi dampak negatif dari setiap pendekatan yang berpotensi pada pelanggaran hukum positif dan memuatnya kedalam peraturan/ perundang-undangan yang diberlakukan beserta ancaman sanksi pelanggarannya.

Referensi

Andrew Cencini, K. Y. (2005, 12 07). *Software Vulnerabilities: Full-, Responsible-, and Non-Disclosure.* Retrieved from Washington University: https://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/software_vulnerabilities_by_cencini_yu_chan.pdf

Biancuzzi, F. (2008, 02 26). *The Laws of Full Disclosure.* Retrieved from SecurityFocus: http://www.securityfocus.com/columnists/466

Brey, P. (2000). Disclosive Computer Ethics: The Exposure and Evaluation of Embedded Normativity in Computer Technology. *Computers and Society*, 10-16.

Brian Ruder, J. D. (1978). *An Analysis of Computer Security Safeguards for Detecting and Preventing Intentional Computer Misuse.* Washington: US. Department of Commerce.

Cisco. (2017, 04 01). *Vendor Vulnerability Reporting and Disclosure Policy*. Retrieved from Cisco: http://www.cisco.com/c/en/us/about/security-center/vendor-vulnerability-policy.html

Cloudflare. (2017, 04 01). *Cloudflare Vulnerability Disclosure Policy*. Retrieved from CloudFlare: https://www.cloudflare.com/disclosure/

Edward Skoudis, T. L. (2005). *Counter Hack Reloaded, Step-by-Step Guide to Computer Attacks and Effective Defenses.* New Jersey: Prentice Hall.

Floridi, L. (2010). *The Cambridge Handbook of Information and Computer Ethics.* Cambridge: Cambridge University Press 2010.

Friedman B., K. P. (2006). Value sensitive design and information systems . *Human-computer Interaction in Management Information Systems*, 348-372.

Gartner. (2016, 08 09). *Press Release* . Retrieved from Gartner: http://www.gartner.com/newsroom/id/3404817

Gary Stoneburner, Alice Goguen, Alexis Feringa. (2002). *Risk Management Guide for Information Technology Systems.* Gaithersburg: National Institute of Standards and Technology.

Knapp, K. J. (2009). *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions: Threat Analysis and Response Solutions.* Hersey: IGI Global.

Lohrmann, D. (2016, 12 04). *Why Governments Need Coordinated VUlnerability Discolosure Programs.* Retrieved from Government Technology: http://www.govtech.com/blogs/lohrmann-on-cybersecurity/governments-need-coordinated-vulnerability-disclosure-programs.html

Longley, D. (1987). *Data & computer security dictionary of standards, concepts, and terms.* New York, N.Y : Stockton Press .

Maurushat, A. (2014). *Disclosure of Security Vulnerabilities: Legal and Ethical Issues.* London: Springer Science & Business Media.

Microsoft. (2017, 04 01). *Coordinated Vulnerability Disclosure*. Retrieved from Microsoft Security TechCenter: https://technet.microsoft.com/en-us/security/dn467923.aspx

Oliva, L. M. (2004). *Information Technology Security: Advice from the Experts.* Hersey: Idea Group Inc.

Stephen Northcutt, C. M. (2004). *IT Ethics Handbook: Right and Wrong for IT Professionals.* Rockland: Synggress Publishing.

Steve Christey. (2002, 02). *Responsible Vulnerability Disclosure Process.* Retrieved from Internet Engineering Task Force: https://tools.ietf.org/pdf/draft-christey-wysopal-vuln-disclosure-00.pdf

Steven DeFino, Larry Greenblatt. (2012). *Official Certified Ethical Hacker Review Guide: For Version 7.1.* Boston: Cengage Learning.

Techopedia. (2017, 04 01). *Definition - What does Vulnerability Disclosure mean?* . Retrieved from Techopedia: https://www.techopedia.com/definition/16171/vulnerability-disclosure

Techtarget. (2017, 04 07). *Definition, Bug Bountry Program.* Retrieved from Techtarget Whatis.com : http://whatis.techtarget.com/definition/bug-bounty-program