VULNERABILITY ASSESSMENT SISTEM MANAJEMEN KEAMANAN INFORMASI STUDI KASUS SISTEM SIDARLING DAN JAGABAYA KOTA DENPASAR

I Gede Putu Krisna Juliharta[1)] I Ketut Suwidiana[2)] I Putu Cikal Taruna[3)]
Program Studi Sistem Informasi [1)3)] Program Studi Informatika[2)]
Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Primakara, Denpasar, Bali[1) 2)]
krisna@primakara.ac.id[1)] suwidiana@gmail.com[2)] cikaltaruna@gmail.com[3)]

ABSTRACT

Vulnerability Assessment (VA) is one way of measuring system and network security. VA is one part of a preventive control in a series of information technology (IT) controls. In the Denpasar City Government, there are many service applications for the community that are integrated within the scope of e-government. A vulnerability assessment was carried out on the SIDARLING service system (Environmental Awareness and Care Information System) and the JAGABAYA service system. The results obtained 8 vulnerabilities for the SIDARLING system and 8 vulnerabilities for the JAGABAYA system.
***Keywords**: Vulnerability assessment, server, information technology.*

ABSTRAK

Vulnerability Assessment (VA) adalah salah satu cara pengukuran terhadap keamanan sistem dan jaringan. VA merupakan salah satu bagian pengendalian *preventif* dalam rangkaian pengendalian teknologi informasi (TI), di Pemerintah Kota Denpasar ada banyak aplikasi layanan kepada masyarakat yang terintegrasi dalam lingkup *e-government*. Dalam penelitian ini dilakukan pengukuran *vulnerability assessment* terhadap sistem layanan SIDARLING (Sistem Informasi Sadar dan Peduli Lingkungan) dan sistem layanan JAGABAYA, hasil didapatkan 8 *vulnerability* untuk sistem SIDARLING dan 9 *vulnerability* untuk sistem JAGABAYA.
Kata Kunci : *Vulnerability assessment*, server, teknologi informasi.

PENDAHULUAN

Vulnerability Assessment (VA) adalah salah satu cara pengukuran terhadap keamanan sistem. VA merupakan salah satu bagian pengendalian *preventif* dalam keseluruhan rangkaian pengendalian teknologi informasi (TI), di samping berbagai metode pengendalian terhadap keamanan yang lain seperti detektif dengan IDS (*Intrusion Detection System*), atau pencegahan dengan *firewall* dan antivirus. VA diharapkan dapat menjadi tolak ukur dalam proses pengawasan dan pengendalian akan keamanan informasi dalam organisasi.

Pada praktiknya di industri, permintaan akan VA umumnya datang setelah terjadi proses pemeriksaan TI yang kemudian berlanjut pada pemeriksaan keamanan data. VA sering kali merupakan tindak lanjut dari proses perencanaan strategi keamanan informasi, kelengkapan standar industri hingga faktor regulasi. Di Indonesia sebagian besar permintaan VA datang dari industri yang memiliki ketergantungan tinggi pada TI seperti industri perbankan atau telekomunikasi atau pun dari industri yang sudah matang dalam pengelolaan TI-nya mereka sangat memahami bahwasanya keamanan adalah hal yang penting dalam menjaga kepercayaan pengguna.

METODE PENELITIAN

Keamanan Sistem Informasi

Keamanan sistem informasi merupakan hal yang perlu mendapat perhatian saat membangun sebuah sistem informasi. Bayangkan kita membuat sebuah rumah yang lengkap dengan jendela dan pintu, tetapi kita tidak membuat kunci untuk pintu dan jendela. Hal ini dapat menyebabkan seseorang bisa dengan mudah memasuki

rumah kita, bahkan mungkin melakukan pencurian. Sama halnya dengan membangun sistem informasi, keamanan sistem informasi digunakan untuk menghindari seseorang yang tidak memiliki akses untuk dapat masuk ke dalam sistem.

Menurut G. J. Simons, keamanan sistem informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik[3]. Menurut John D. Howard dalam bukunya "*An Analysis of Security Incidents on The Internet*" menyatakan bahwa keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengaksesan jaringan yang tidak bertanggung jawab [3].

Aspek Keamanan Informasi

Informasi merupakan salah satu aset penting dari perusahaan. Perusahaan melakukan pengolahan terhadap informasi, kemudian hasilnya disimpan dan dibagikan[6]. Keamanan sistem informasi terdiri dari perlindungan terhadap aspek-aspek berikut ini:

1. *Confidentiality* (Kerahasiaan)

Aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan [3].

2. *Integrity* (Integritas)

Aspek yang menjamin bahwa data tidak diubah tanpa ada ijin pihak yang berwenang (*authorized*), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek *integrity* ini [3].

3. *Availability* (Ketersediaan)

Aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memasti- kan *user* yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bila- mana diperlukan) [3].

Sumber lain menyebutkan bahwa aspek keamanan sistem informasi melingkupi 4 aspek. Grafinkel mengemukakan bahwa keamanan komputer melingkupi 4 aspek, yaitu privasi, *integrity*, *authentication* dan *availability*[7]. Selain keempat hal di atas, masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic commerce*, yaitu *access control* dan *non-repudiation* [7].

Keamanan Jaringan

Keamanan jaringan merupakan aktivitas yang dilakukan untuk melindungi jaringan yang ada. Menggunakan penerapan teknologi dan proses pengamanan untuk melindungi jaringan dari ancaman yang berasal dari luar maupun dalam jaringan. Keamanan jaringan melibatkan seluruh pihak dalam organisasi ataupun institusi untuk ikut bersama melindungi isi dan informasi dari institusi tersebut. Keamanan jaringan yang efektif adalah membagi faktor-faktor jaringan dan jenis ancamannya, untuk bisa melakukan penanggulangan atau bahkan menghilangkannya dari jaringan yang ada.

Ada beberapa faktor keamanan jaringan yaitu :

1. *Vulnerability*

Vulnerabilities merupakan kelemahan atau kerentanan yang dapat menyebabkan para penyerang mendapatkan akses ilegal untuk masuk ke dalam suatu sistem. *Vulnerability* merupakan persimpangan dari tiga elemen yaitu: aliran sistem (*gap/weakness*), penyerang mengakses sistem yang cacat, dan penyerang mempunyai kemampuan untuk menyerang akses yang cacat tersebut. Ada empat faktor utama penyebab ancaman terhadap keamanan jaringan yaitu, *technology weakness*, *configuration weakness*, *security policy weakness*, dan *human error*.

2. *Threat*

Thereat merupakan ancaman yang datang dari seseorang yang tertarik dan memiliki kemampuan untuk mengambil keuntungan dari kelemahan keamanan. Ada banyak peralatan, *script*, dan program yang dapat digunakan untuk menyerang jaringan dan perangkatnya. Secara umum, peralatan komputer yang sering menjadi target adalah *endpoints*, seperti server dan komputer desktop. Ancaman ada berbagai macam jenis di antaranya ancaman terhadap infrastruktur fisik yang meliputi ; ancaman terhadap perangkat keras, ancaman terhadap lingkungan, ancaman kelistrikan, dan ancaman pada saat perawatan. Ancaman yang berasal dari jaringan, yang bisa berasal dari dalam maupun dari luar jaringan.

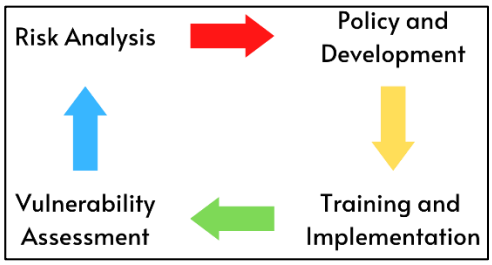
3. *Attacks*

Attacks atau serangan merupakan seseorang yang dengan sengaja melakukan aktivitas yang menyebabkan sesuatu yang buruk terjadi terhadap suatu sistem. Ada beberapa metode dalam melakukan serangan di ataranya; *network enumeration* (mencari informasi tentang jaringan), *vulnerabilities analysis* (menganalisa kelemahan), dan *exploitation*.

4. *Vulnerability Assessment*

Vulnerability Assessment (VA) merupakan bagian dari proses *risk assessment* seperti digambarkan dalam sebuah lingkaran siklus antara (Anjar, 2006):

- Analisa Risiko (*Risk analysis*)
- *Policy development*
- *Training & implementation*
- *Vulnerability assessment & penetration testing*



Gambar 1 Siklus Vulnerability Assessmenet

Sebagai sebuah proses yang terus menerus dan membentuk suatu kerangka siklus maka hasil dari VA akan digunakan untuk mengimplementasikan strategi keamanan informasi di perusahaan tersebut. Begitu pun strategi keamanan yang telah dibuat harus tetap dievaluasi Sebagai suatu proses VA sebaiknya dilakukan secara kontinu dan terus menerus, umumnya VA ini dilakukan:

Saat implementasi program baru, pada implementasi program baru biasanya departemen TI akan membuka akses ke mesin *production* oleh pihak ketiga seperti *programmer*, vendor ataupun *consultant*. Implementasi ini dimungkinkan menyebabkan terbukanya lubang kerawanan baru yang belum ada.

Secara periodik dalam waktu-waktu tertentu, digunakan untuk memantau apabila ada perubahan yang dilakukan oleh pengguna akhir. VA secara periodik inilah yang dinilai sebagai cara yang paling baik. Proses VA sendiri memiliki berbagai tingkatan, sehingga perusahaan dapat memilih tingkatan mana yang akan digunakan dalam pengukurannya. Tingkatan ini dapat di sesuaikan dengan kondisi di masing-masing tempat.

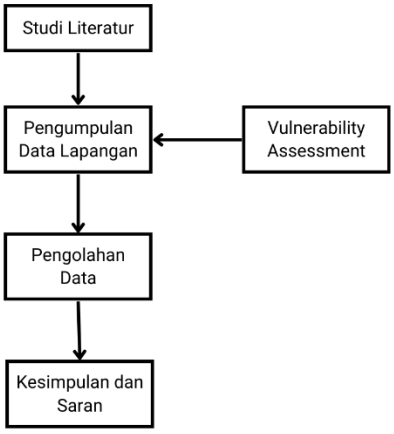
Tingkat I: Pengukuran peraturan dan kebijakan (*Policy assessment*) Pengukuran ini meliputi peraturan, kebijaksanaan, standar operasi di *client* dalam cakupan keamanan informasi.

Tingkat II: Evaluasi Jaringan Pengukuran ini meliputi kinerja jaringan, keamanan jaringan hingga ancaman-ancaman terhadap jaringan kerja. Pengukuran jenis ini memerlukan alat bantu seperti *scanning* atau data *capture*. Evaluasi jaringan ini bertujuan untuk mendapatkan informasi mengenai kondisi sebenarnya yang terjadi di lapangan, bagaimana tingkat kesadaran akan keamanan informasi yang sudah diterapkan selama ini.

Tingkat III: *Test* penetrasi (*Penetration Test*) *Penetration test* sebenarnya menggunakan prinsip yang sama dengan *network evaluation* dimana pembedanya bahwa *penetration test* dilakukan dalam kondisi gelap, tanpa mengetahui konfigurasi dan kondisi sebenarnya seperti apa.

METODE PENELITIAN

Vulnerability assessment dilakukan selama 30 hari. Langkah *assessment* (Gambar 2.) adalah dengan cara melakukan analisa ke mesin sistem SIDARLING dan JAGABAYA.



Gambar 2 Perancangan Penelitian

Gambar 2. Menjelaskan mengenai perancangan penelitian yang meliputi :

1. Studi literatur yang memiliki tujuan memahami dan mencari referensi dalam pelaksanaan penelitian *vulnerability assessment.*
2. Pengumpulan data lapangan merupakan tahapan untuk melakukan proses VA dengan melakukan penilaian keamanan secara obyektif menggunakan *tools* yang diperuntukkan untuk mengecek *vulnerability* pada sistem.
3. Hasil dari pengumpulan data adalah proses pengolahan data dan membuatnya menjadi laporan dan tulisan ilmiah serta memberikan kesimpulan dan saran.

HASIL DAN PEMBAHASAN

Berdasarkan hasil *vulnerability assessment* yang dilaksanakan pada sistem SIDARLING dan JAYABAYA, didapatkan hasil sebagai berikut:

SEVERITY	NUMBER OF INSTANCE	NAME
MEDIUM	2	Vulnerable JS Library
MEDIUM	8	X-Frame-Options Header Not Set
LOW	8	Absence of Anti-CSRF Tokens
LOW	3	Cookie No HttpOnly Flag
LOW	3	Cookie without SameSite Attribute
LOW	2	Cookie Without Secure Flag
LOW	9	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
LOW	71	X-Content-Type-Options Header Missing

Gambar 3 Hasil Assessment Sistem Aplikasi SIDARLING

Gambar 3 untuk sistem aplikasi SIDARLING, dari 8 *vulnerability*, terdapat 2 *vulnerability* level *medium* dan 6 *vulnerability* level *low* dengan total 106 celah kebocoran. Jika melihat detail dari *vulnerability* yang didapatkan, kebocoran yang terjadi adalah dikarenakan *website* dan *cookies* yang belum diatur ke *Https* yang membuat akses informasi mudah diakses oleh penyerang.

SEVERITY	NUMBER OF INSTANCE	NAME
MEDIUM	5	Vulnerable JS Library
MEDIUM	22	X-Frame-Options Header Not Set
LOW	24	Absence of Anti-CSRF Tokens
LOW	6	Cookie No HttpOnly Flag
LOW	6	Cookie without SameSite Attribute
LOW	4	Cookie Without Secure Flag
LOW	2	Cross-Domain JavaScript Source File Inclusion
LOW	24	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
LOW	164	X-Content-Type-Options Header Missing

Gambar 4 Hasil Assessment Sistem Aplikasi JAGABAYA

Gambar 4 untuk sistem aplikasi JAYABAYA, dari 9 *vulnerability*, terdapat 2 *vulnerability* level *medium* dan 7 *vulnerability* level *low* dengan total 257 celah kebocoran. Jika melihat detail dari *vulnerability* yang didapatkan, kebocoran yang terjadi adalah dikarenakan *website* yang belum diatur ke *Https* yang membuat akses informasi mudah diakses oleh penyerang serta terdapat satu atau beberapa *file script* dari domain pihak ketiga.

SIMPULAN

Dalam penelitian yang telah dilakukan dapat ditarik kesimpulan bahwa untuk proses manajemen *software* atau aplikasi belum dilakukan dengan baik hal tersebut dapat dilihat dari:

1. Aplikasi yang digunakan pada mesin server sudah kadaluwarsa dan hingga saat ini belum dilakukan proses *update*.
2. Celah yang terjadi antara lain penggunaan *framework* atau *library* pengembangan yang lawas atau tidak diperbaharui, belum adanya *optimisasi Cookies* pada setiap halaman *website*, hingga adanya File *Cross-Domain JavaScript Source* yang memungkinkan peretas untuk mengakses *database* hingga mencuri data-data yang ada di dalamnya.
3. *Vulnerability assessment* baru dilakukan pada dua mesin yang digunakan oleh *public*, ke depannya perlu lebih banyak lagi aplikasi di *e-government* Kota Denpasar yang diukur dengan *vulnerability assessment*.
4. Dalam proses *vulnerability assessment* belum dilakukan perhitungan untuk dampak dari kerentanan yang ada. Untuk penelitian selanjutnya dapat dilakukan pengukuran *business impact analysis*.

DAFTAR PUSTAKA

[1] Agung Nugroho (2009), "*Studi Kasus Celah Keamanan pada Jaringan Nirkael yang menerapkan WEP (Wired Equivalent Privacy)*", Yogyakarta, STMIK AMIKOM

[2] Andreas Hadiyono, Sutresna Wati, I. Wayan Simri Wicaksana. (2008) "*Analisa Log Router Untuk Meningkatkan Keamanan Jaringan*", Jakarta, Seminar Ilmiah Nasional Komputer dan Sistem Intelijen.

[3] Anjar Priandoyo, 2006, "Vulnerability Assessment untuk Meningkatkan Kesadaran Pentingnya Keamanan Informasi". Jurnal Sistem Informasi Vol. 1 No. 2September. Jakarta Universitas Maranatha.

[4] Chris McNab.2007. "*Network Security Assessment : know Your Network"*. USA.O'Reilly

[5] Faturachman Husein, "Implementasi Indeks KAMI di Universitas Sam Ratulangi", E-Journal Teknik Informatika Vol. 12 No. 1 (2017) ISSN: 2301-8364

[6] I Gede Putu Krisna Juliharta, "Investigasi Keamanan Aplikasi Teknologi Informasi dengan Teknik Packet Sniffing", Seminar Nasional Informatika Vol.1 No.2, Universitas Pembangunan Nasional "Veteran" Yogyakarta, 2016.

[7] Insecure.org. 2009. “Free Security Scanner For Network Exploration & Security Audits” diakses pada tanggal 20 oktober 2018.