Jurnal Ilmiah Teknologi Informasi Asia
Vol.14, No.2, Tahun 2020
ISSN: 2580-8397 (O); 0852-730X (P)

Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi

Johan Ericka Wahyu Prakasa
Jurusan Teknik Informatika
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
Email:johan@uin-malang.ac.id

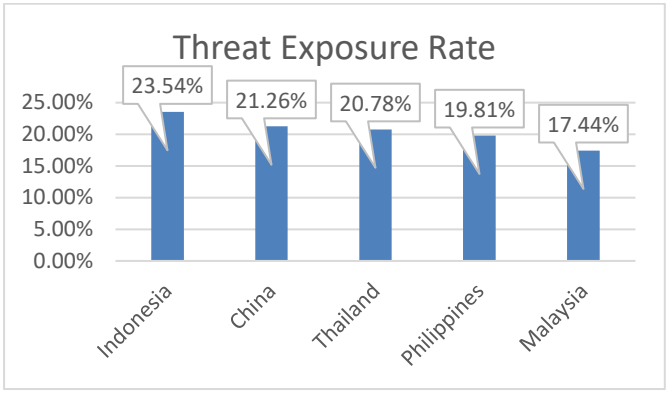
ABSTRAK.Semakin berkembangnya sistem informasi dewasa ini diikuti dengan peningkatan serangan terhadapsistem informasi. Hal ini disebabkan semakin banyak sistem informasi yang menyimpan data – data sensitif penggunanya seperti nomor telepon, Nomor Induk Kependudukan, tanggal lahir bahkan sampai nomor rekening bank. Data – data tersebut sangat rawan untuk di salah gunakan oleh pihak – pihak yang tidak bertanggung jawab. Maka keamanan merupakan salah satu faktor yang harus menjadi pertimbangan utama dalam pengembangan sistem informasi. Penelitian ini mempelajari berbagai teknik serangan kepada sistem informasi.Untuk memudahkan identifikasi, serangan serangan tersebut di klasifikasikan berdasarkan komponen penyusun sistem informasi. Hasil dari penelitian ini menunjukkan bahwa terdapat serangan yang ditujukan pada setiap komponen penyusun sistem informasi. Di akhir penelitian ini memberikan saran untuk meminimalisir dampak dari serangan serta untuk meningkatkan keamanan sistem informasi.
Kata Kunci: *klasifikasi, serangan, sistem informasi, keamanan*

ABSTRACT.Nowadays, many information systems were developed to ease human life. This massive explosion of information systems attracts many attackers to get the valued data inside the information systems. There are many interesting data was held inside the information systems from personal ID Card number to bank accounts. That's why security must be involved in information systems development in the first place. This research study attacks to information systems and classified it into information system components. As a result, there are many attacks on every information system components. This research also gives advises to securing the information system from every information systems components.
Keywords: *information system, attack, classification, mitigation*

1. PENDAHULUAN

Dewasa ini Teknologi Informasi telah memasuki kehidupan manusia secara masif. Berbagai Sistem Informasi dikembangkan untuk memudahkan kehidupan manusia. Tidak jarang Sistem Informasi tersebut menyimpan data – data penggunanya bahkan data yang bersifat pribadi seperti nomor telepon, tanggal lahir, Nomor Induk Kependudukan, nomor rekening bank dan lain sebagainya. Dengan alasan kemudahan dan kenyamanan pengguna akan dengan suka rela menyerahkan data yang dimilikinya untuk disimpan di dalam Sistem Informasi tersebut. Oleh karena itulah serangan terhadap Sistem Informasi semakin meningkat dengan teknik yang semakin beragam.

Menurut laporan (SophosLab, 2013) Indonesia merupakan negara dengan *Threat Exposure Rate* terbesar. *Threat Exposure Rate* diukur dari persentase komputer yang terkena serangan *malware* dalam periode 3 bulan. Laporan tersebut menunjukkan bahwa Indonesia merupakan negara yang paling banyak dijadikan target serangan cyber.



Grafik 1 ***Riskiest Countries by SophosLab Report 2013*** **(SophosLab, 2013)**

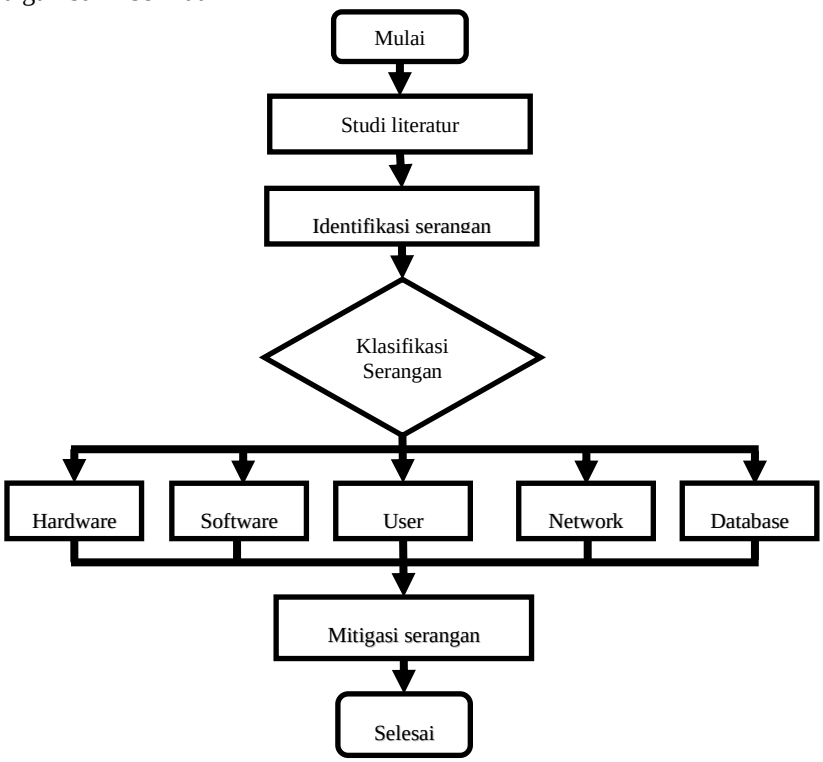
Untuk mengatasi keamanan internet, Indonesia telah memiliki lembaga khusus yang bernama ID-SIRTII / CC (*Security Incident Response Team on Internet Infrastructure/Coordination Center*). Lembaga ini merupakan lembaga atau koordinator resmi untuk insiden pada infratruktur internet di Indonesia. Pada laporan tahunan tahun 2018, ID-SIRTII/CC melaporkan bahwa Indonesia menerima total 232.447.974 serangan yang terdiri dari 122.435.215 aktivitas malware, 16.939 insiden website, 2.885 laporan insiden dari masyarakat dan 1.872 informasi celah keamanan (ID-SIRTII, 2018). Pada laporan tersebut juga didapatkan fakta bahwa selain Indonesia menjadi sasaran dari serangan cyber, Indonesia juga merupakan negara sumber serangan terbanyak.

Gambar 1. Laporan Pemantauan Keamanan Internet Indonesia 2018 (ID-SIRTII, 2018)

Laporan diatas menunjukkan bahwa keamanan pada dunia maya di Indonesia cukup lemah. Hal ini dapat dilihat dari banyaknya jumlah serangan yang ditujukan pada berbagai sistem informasi yang ada di Indonesia, baik serangan yang berasal dari luar Indonesia maupun serangan yang berasal dari dalam Indonesia sendiri. Oleh karena itulah faktor keamanan pada Sistem Informasi saat ini harus menjadi prioritas utama dalam pembangunan sebuah sistem informasi. Maka pada penelitian ini akan mengklasifikasikan berbagai serangan yang diterima oleh sistem informasi berdasarkan komponen penyusun dari sistem informasi tersebut. Hal ini perlu dilakukan untuk memudahkan identifikasi model serangan pada setiap komponen penyusun sistem informasi sehingga akan dapat diketahui langkah pencegahan yang paling efektif untuk setiap model serangan.

2. METODE

Penelitian ini menggunakan metode studi literatur untuk mengetahui penelitian serupa yang telah dilakukan. Setiap penelitian akan di bahas secara singkat untuk mengetahui perbedaan dari masing – masing penelitian yang telah dilakukan.Sehingga dapat diketahui dengan jelas kebaruan metode yang diusulkan melalui penelitian ini dibandingkan dengan penelitian yang telah dilakukan sebelumnya. Alur penelitian ini dapat dilihat pada gambar 2 berikut ini



Gambar 2. Diagram Alur penelitian

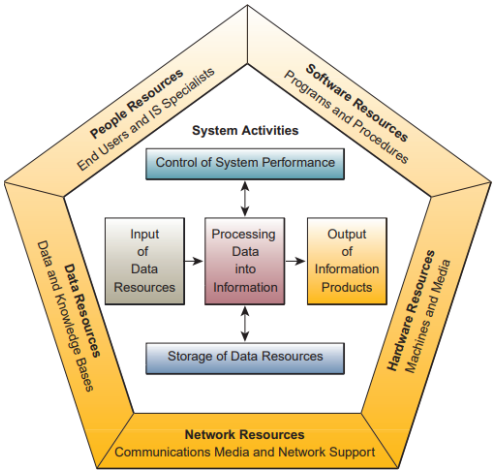
Penelitian – penelitian yang telah dilakukan sebelumnya kebanyakan berfokus kepada bagian tertentu dari sistem informasi (basis data, jaringan komunikasi dan sebagainya).Salah satu pendekatan yang digunakan adalah dengan menggunakan kerangka kerja (*framework*). Penelitian yang telah dilakukan (Mohammed & Mohammed, 2017)mengungkapkan bahwa usaha untuk membentuk *Security Risk Management framework* telah dilakukan dalam membentuk *National Infrastructure Protection Plan*. Framework ini dibangun berdasarkan proses asesmen terhadap resiko sistem, implementasi dari *security framework*, pemantauan aktivitas dan peninjauan kembali. Untuk mendapatkan hasil yang paling optimal dibutuhkan pendekatansecara terintegrasi mulai dari penggunaan alat asesmen, identifikasi terhadap ancaman internal maupun eksternal serta pembentukan *framework* yang fleksibel sehingga dapat digunakan pada berbagai macam sistem informasi. Pada penelitian lain (Ali, Husain, & Sharma, 2017) juga telah membahas serangan – serangan terhadap teknologi terkini seperti pada *cloud computing*, *internet of things*, *drone* dan *big data*. Dari penelitian tersebut diketahui bahwa perkembangan teknologi terkini juga diikuti oleh perkembangan teknik serangan.Telah ditemukan serangan – serangan terhadap teknologi yang relatif baru seperti serangan pada *cloud computing*, *botnet* yang menjadikan perangkat IoT menjadi zombie (*Mirai botnet*), serangan *ransomware* yang semakin masif, serangan pada *drone* (drone-jacking) serta serangan pada *big data*. Penelitian terhadap Faktor pengguna / manusia terhadap keamanan data juga telah dilakukan(Safianu, Twum, & Hayfron-Acquah, 2016). Hasil dari penelitian ini menunjukkan bahwa teknologi saja tidak cukup untuk mencegah kebocoran data. Faktor manusia merupakan titik terlemah dari sistem informasi. Semakin banyak model serangan yang ditujukan kepada pengguna sistem informasi, karena lebih mudah dan tingkat keberhasilan yang lebih tinggi dibandingkan menyerang sistem informasi itu sendiri. Maka pelatihan tentang keamanan data kepada pengguna sistem informasi sangat diperlukan untuk meminimalisir kemungkinan terjadinya kebocoran data. Penelitian terhadap serangan *cyber* kepada instansi pemerintah juga telah dilakukan (Babate, Musa, Kida, & Saidu, 2015). Pada penelitian ini menyebutkan beberapa teknik serangan yang digunakan oleh pada *cyber criminals* antara lain *phising* dan *email spamming*, *botnet*, *malware* dan *spyware*, *key loggers*, *social engineering*, *distributed denial of services*, *virus* dan *worms*.

Indonesia telah memiliki aturan terkait *cyber crime* yang disusun dalam Undang – Undang

Informasi dan Transaksi Elektronik atau dikenal dengan UU-ITE (Indonesia, 2008). Undang – undang ini selain mengatur tentang transaksi elektronik, juga terdapat beberapa pasal tentang *cyber crime*. Untuk kasus serangan terhadap sistem Informasi, UU-ITE telah membahas khususnya pada pasal – pasal berikut ini :

- Pasal 30
  - Ayat 1 tentang mengakses komputer / sistem elektronik tanpa hak
  - Ayat 2 bertujuan untuk memperoleh Informasi / dokumen elektronik
  - Ayat 3 dengan cara melanggar / menjebol sistem pengamanan
- Pasal 31
  - Ayat 1 melakukan penyadapan
  - Ayat 2 melakukan perubahan terhadap data yang disadap
- Pasal 32
  - Ayat 1 melakukan perubahan / perusakan / menghilangkan Informasi elektronik
  - Ayat 2 memindahkan Informasi / dokumen elektronik tanpa hak
  - Ayat 3 mengakibatkan terbukanya Informasi / dokumen elektronik rahasia
- Pasal 33
  - melakukan tindakan yang mengakibatkan terganggunya sistem elektronik
- Pasal 35
  - melakukan manipulasi Informasi / dokumen elektronik sehingga dianggap otentik (hoax)

Penelitian ini bertujuan untuk meningkatkan keamanan sistem informasi melalui klasifikasi serangan terhadap sistem informasi. Klasifikasi dilakukan berdasarkan komponen penyusun sistem informasi sehingga memudahkan langkah pencegahan serangan yang efektif. Sistem informasi terdiri dari beberapa komponen penyusun antara lain perangkat keras, perangkat lunak, jaringan komunikasi, basis data dan manusia (O'Brien & Marakas, 2017). Setiap komponen ini memiliki celah keamanan (*vulnerabilities*) yang dapat di manfaatkan (*eksploit*) atau di serang (*attack*) sehingga dapat menimbulkan kerusakan pada sistem Informasi atau bahkan kebocoran data.



Gambar 3. Komponen penyusun Sistem Informasi (O'Brien & Marakas, 2017)

3. HASIL DAN PEMBAHASAN

Dari hasil studi literatur, ditemukan beberapa jenis serangan terhadap sistem informasi. Serangan – serangan tersebut kemudian di klasifikasikan berdasarkan komponen penyusun sistem informasi sebagai berikut

3.1 Serangan Terhadap Perangkat Keras

Serangan terharap perangkat keras komponen sistem informasi (*sever / workstation*) masih menjadi salah satu serangan yang berakibat cukup fatal. Pada penelitian yang telah dilakukan (Alves & Morris, 2018) terdapat beberapa *malware* yang menyerang *hardware* antara lain *chipset level backdoor*, *stealth hard-drive backdoor*, *Intel Processor's SMM exploit*, *I/O MMU vulnerability*, *L3 cache side channel attack* dan *malicious USB Device*. Meskipun secara praktis serangan ini lebih sulit untuk dilakukan karena membutuhkan akses langsung ke perangkat keras, namun apabila terjadi akan berakibat sangat fatal. Penelitian lain di bidang ini telah dilakukan dengan fokus utama pada *trojan circuit*(Bloom, Leontie, Narahari, & Simha, 2012). Penelitian ini membahas bahwa dimungkinkan untuk memasukkan sebuah

trojan (malicious code) kedalam IC yang digunakan oleh komputer. Apabila hal ini terjadi maka produsen komponen komputer akan mengalami *distrust* yang dapat mengakibatkan kerugian yang sangat besar. Karena selama ini tidak terdapat kontrol pada produsen IC sehingga injeksi *trojan* kedalam IC oleh pihak – pihak yang berkepentingan sangat dimungkinkan.

3.2 Serangan Terhadap Perangkat Lunak

3.2a Serangan terhadap sistem operasi

Serangan terhadap sistem operasi sebagian besar mentargetkan memory atau dikenal dengan *memory-corruption vulnerability*. Pada penelitian yang dilakukan pada disertasinya (Gens, 2018) menyebutkan bahwa serangan seperti *rowhammer* menyerang DRAM sehingga dapat mengakibatkan ketidak-stabilan sistem operasi (*crash*) atau bahkan dapat mengakibatkan *privileges escalation*. Pada penelitian tersebut membuktikan bahwa akses ke alamat memori yang terlarang dapat mengakibatkan pengguna biasa mampu menjalankan aplikasi setara administrator (*root*). Serangan lain pada sistem operasi disebut dengan CLKscrew (Tang, Sethumadhavan, & Stolfo, 2017) dapat dilakukan melalui *software* dan dapat mengacaukan sistem kelistrikan (*power*) komputer. Pada penelitian ini membuktikan bahwa kode program yang dibuat (*malicious code*) dapat mengakibatkan ketidak stabilan supply arus listrik pada sistem komputer. Serangan lain yang cukup terkenal karena berimbas pada sistem prosesor Intel x86 dan *ARM-based microprocessors*yang saat ini banyak digunakan di pasaran (Kee, et al., 2018). Serangan ini memiliki beberapa varian yaitu *Bounds Check Bypass, Branch Target Injection, Rogue Data Cache Load, Rogue System Register Cache, Speculative Store Bypass*. Serangan ini memungkinkan untuk pembacaan data langsung melalui memory(Kocher, 2019). Dengan memanfaatkan celah keamanan yang ada pada prosesor Intel x86 dan ARM, penyerang dapat mengakses alamat memori yang terlarang sehingga dimungkinkan terjadi kebocoran data langsung dari RAM. Apabila data – data ini di rangkai (pembacaan terhadap alamat memory dilakukan sesuai dengan pola peletakan data) maka akan didapatkan informasi yang seharusnya hanya dapat diakses oleh sistem operasi.

3.2b Serangan terhadap layanan sistem operasi (*services*)

Sistem operasi memiliki *services* / layanan yang berfungsi untuk melakukan proses – proses yang dibutuhkannya. Salah satu serangan yang paling terkenal yang ditujukan pada layanan adalah *Distributed Denial of Service*(Jaafar, Abdullah, & Ismail, 2019). Pada penelitian ini menjabarkan beberapa teknik DDoS antara lain *Session Flooding Attack, Request Flooding Attack, Asymmetric Attack, Slow Request/Response Attack*. Tujuan dari serangan ini adalah untuk menyibukkan *service* (misal HTTP) sehingga tidak dapat melayani *request* dari pengguna lainnya dan website tidak dapat diakses. Serangan lain yang banyak dilakukan pada layanan sistem operasi adalah serangan pada *secure shell* (ssh). *Secure shell* merupakan layanan untuk melakukan manajemen terhadap server secara *remote*. Satu – satunya teknik yang dapat digunakan untuk menyerang *Secure Shell* adalah dengan *brute-force attack*. Meskipun teknik ini sudah cukup lama digunakan dan dinilai kurang efektif, namun dengan adanya *botnet* teknik ini menjadi jauh lebih efektif dari sebelumnya (Salamatian, Huleihel, Beirami, Cohen, & Medard, 2019). Botnet merupakan perangkat yang terhubung ke jaringan internet yang dapat digunakan untuk melakukan serangan (salah satunya *Denial of Services*) secara terdistribusi.

3.2c Serangan terhadap aplikasi

Aplikasi adalah target yang paling utama pada serangan. Karena pada aplikasi-lah yang menyimpan informasi / data pengguna. Serangan yang paling umum dilakukan terhadap aplikasi adalah *Cross Site Scripting (XSS).* Berdasarkan laporan dari Akamai pada tahun 2018, XSS merupakan salah satu dari 3 serangan yang paling banyak dilakukan terhadap website (Akamai, 2018). Teknik ini disebut juga dengan *client-side code injection attack* karena client akan memasukkan kode program yang akan di eksekusi (secara tidak sengaja) oleh sistem informasi. Misalnya memasukkan kode program pada inputan *email* sehingga ketika sistem informasi diminta untuk menampilkan *email* secara otomatis kode program tersebut akan di jalankan. Lebih lanjut XSS dapat dimanfaatkan sebagai pembuka bagi serangan lainnya seperti CSRF (*Cross Site Request Forgery*) (Niakanlahiji & Jafarian, 2019). CSRF merupakan teknik serangan yang memaksa pengguna sistem informasi yang telah ter-autentikasi untuk menjalankan aksi yang tidak diinginkannya seperti perubahan data (password / email) (Moustafa & Lalia, 2019). Yang membahayakan adalah aksi tersebut dilakukan oleh pengguna yang ter-autentikasi sehingga sistem tidak mendeteksi adanya aksi yang ilegal.

3.3 Serangan Terhadap Jaringan Komunikasi

Jaringan komunikasi data merupakan salah satu titik yang banyak mendapatkan serangan. Serangan pada jaringan komputer lebih ke arah penyadapan data (*data interception*). Meskipun sejak kemunculan perangkat *network switch* yang tidak lagi memungkinkan untuk melakukan penyadapan data pada

jaringan komputer, namun dengan semakin masif nya penggunaan jaringan nirkabel (*wireless network*) menjadikan teknik penyadapan data dapat dilakukan bahkan dengan lebih mudah. Penelitian yang telah dilakukan (Zou, Zhu, Wang, & Hanzo, 2016) menunjukkan bahwa pada dasarnya terdapat 2 model serangan pada jaringan komputer. Model pertama yaitu serangan aktif menggunakan *signaljammer* yang bertujuan untuk mengganggu transmisi data. Sedangkan model kedua yaitu model pasif lebih ke penyadapan data. Pada penelitian tersebut di jabarkan tentang berbagai teknik serangan yang mungkin dilakukan pada *physical layer (signal jamming)*, *data-link layer (ARP Spoofing)*, *network layer (Smurf attack)* sampai pada *application layer* (*SMTP Attack, cross site scripting*).

3.4 Serangan Terhadap Basis Data

Basis data merupakan tempat dimana semua data berada. Sistem informasi akan sangat bergantung kepada basis data. Oleh karena itulah serangan terhadap basis data masih merupakan serangan terbanyak yang dilakukan sampai tahun 2018 yang lalu(Akamai, 2018).Serangan yang paling terkenal pada basis data adalah SQL Injection. Namun serangan pada basis data juga dapat disebabkan karena miskonfigurasi sistem basis data misalnya tidak dilakukannya pembatasan terhadap host user yang dapat mengakibatkan user tersebut dapat mengakses basis data dari manapun, penggunaan *port default* serta penggunaan *common username & password*(Sharma, 2016). Pada penelitian lain, klasifikasi ancaman terhadap sistem manajemen basis data (DBMS) juga telah dilakukan pada table 1 berikut ini.

Table 1. Details of VDBMS,TDBMS and SMDBMS(Kothari, Suwalka, & Kumar, 2019)

Vulnerabilities (VDBMS)		Threats (TDBMS)	Security Method (SMDBMS)
Vendor Bug	Buffer overflow Programming errors	May damage or voiolate the database	Unathorized access control policy
Poor Architecture	Weak form of encryption	May damage database environment components (network, applications, operating systems, DBMS and data)	Sorion Security Model Jaodia-Dogan Security Model
Misconfiguration	Not properly locking database	Loss of integrity of the database	Physical database integrity protection Logical data integrity protection Data element integrity protection
Incorrect Usage	SQL Injection	Misuse of availability of database	Intrusion Detection Sytems
Irresponsible DBA	Deactivation of necessary security mechanism	Easy access of data	The access control models for databases should be expressed in terms of the logical data model
Hidden flaws in DB	Undetected defects	Allow hackers to connect to the database server by exploring those defects	Intrusion Detection System
Unathorized users	Unathorized user steal the credentials of authorized user	Easy access of database servers	Intrusion Detection System
Misused privileges	Authorized users take advantaged of their privileges	Maliciously access or destroy data	DBA should provide security in the basis of above mentioned principles.

3.5 SERANGAN TERHADAP PENGGUNA / MANUSIA

Social engineering merupakan serangan yang paling banyak digunakan untuk mendapatkan informasi rahasia yang diketahui oleh pengguna terkait sistem informasi yang diaksesnya (misal : *username & password* pengguna untuk masuk kedalam sistem informasi). Teknik yang banyak digunakan adalah adalah *Evil Twin*. *Evil Twin* akan membelokkan koneksi internet target dengan berpura – pura menjadi *Access Point* yang telah dikenal target sebelumnya. Karena paket data yang dikirimkan melalui perangkat *Evil Twin* maka penyadapan data dapat di lakukan (Agarwal, Biswas, & Nandi, 2018). Serangan lain pada pengguna komputer yang memiliki tingkat keberhasilan cukup tinggi yaitu *phising*. *Phising* merupakan upaya untuk mendapatkan informasi rahasia pengguna komputer (username / password / pin / no. rekening bank dll) dengan cara menipu pengguna agar memasukkan informasi tersebut pada website yang telah dibuat menyerupai website aslinya. Bahkan pada laporan terbarunya, Anti-Phising Working Group menyebutkan bahwa pada kuartal ke 4 tahun 2019 terdapat sebanyak 162.155 website phising yang terdeteksi(Group, 2020) meskipun jumlah ini menurun dari kuartal sebelumnya.

Tabel 2. Identifikasi model serangan pada komponen penyusun sistem informasi

Komponen Sistem Informasi	Jenis Serangan
Hardware (Perangkat keras)	- chipset level backdoor
	- stealth hard-drive backdoor
	- Intel processor's SMM exploit
	- I/O MMU vulnerability
	- L3 cache side channel attack
	- Trojan circuit
Software (Perangkat Lunak)	
Sistem Operasi	- RowHammer
	- CLKscrew
	- Bounds Check Bypass
	- Branch Target Injection
	- Rogue Data Cache Load
	- Rogue System Register Cache
	- Speculative Store Bypass
Layanan Sistem Operasi	- Session Flooding Attack
	- Request Flooding Attack
	-Asymmetric Attack
	- Slow Request/Response Attack
	- SSH Bruteforce Attack
Aplikasi	- Cross Site Scripting (XSS)
	- Cross Site Request Forgery
Network (jaringan komunikasi)	- Signal Jammer
	- ARP Spoofing
	- Smurf Attack
	- SMTP Attack
Database (basis data)	- SQL Injection
	- Buffer overflow
	- Weak form of encryption
User (Pengguna)	- Social Engineering
	- Evil Twin Attack
	- Phising attack

Dari tabel 2 diketahui bahwa terdapat berbagai model serangan pada setiap komponen penyusun sistem informasi. Dari hasil penelitian ini disusun beberapa saran untuk melakukan mitigasi / pencegahan dari serangan – serangan tersebut.

3.6 Mitigasi Serangan Pada Perangkat Keras

Dari penelitian yang telah dilakukan, serangan pada perangkat keras merupakan serangan yang cukup sulit dilakukan karena penyerang harus memiliki akses fisik ke komputer yang akan di serang. Maka langkah yang dapat dilakukan untuk memitigasi serangan ini adalah dengan memberikan pengamanan fisik di ruang server / *data center*(AL-FEDAGHI & Alsumait, 2019). Pengamanan fisik mulai dari akses kontrol terhadap ruang *data center*, akses kontrol terhadap *server rack* dan akses kontrol terhadap fisik *server*.

Dengan diterapkannya pengendalian terhadap pengguna yang mengakses ruang server, maka serangan ini akan dapat di minimalisir.

3.7 Mitigasi Serangan Pada Perangkat Lunak

3.7a Mitigasi serangan pada sistem operasi

Mitigasi serangan terhadap sistem operasi dapat dilakukan dengan melakukan *update* terhadap sistem informasi yang digunakan. Update akan memberikan perbaikan terhadap sistem operasi teruma dari sisi keamanan (selain perbaikan aspek lain seperti tampilan, penambahan fitur). Dengan selalu mengikuti update yang disediakan oleh produsen sistem operasi, maka celah keamanan yang ada dapat tertutup. Selain itu penggunaan *software* bajakan akan dapat membahayakan sistem operasi.Sebagian besar aplikasi *crack* untuk membajak *software* akan membuka *backdoor* yang memungkinkan malware untuk masuk kedalam sistem.

3.7b Mitigasi serangan pada layanan (*service*) sistem operasi

Serangan pada layanan sistem operasi dapat disebabkan oleh celah keamanan (*vulnerability*) yang terdapat pada layanan tersebut maupun dari serangan (secara disengaja). Tujuan dari serangan terhadap layanan (*service*) sistem operasi adalah untuk mendapatkan akses terhadap layanan tersebut (pada layanan SSH, FTP) atau agar layanan tersebut tidak dapat di akses (DDoS). Mitigasi yang dapat dilakukan yaitu memasang dan mengkonfigurasi *firewall* pada server untuk mengurangi serangan – serangan tersebut.

3.7c Mitigasi serangan pada aplikasi

Serangan pada aplikasi seringkali dilakukan dengan memanfaatkan celah keamanan yang tidak sengaja ter-ekspos oleh pembuat aplikasi. Hal ini seringkali disebabkan oleh kesalahan logika pemrograman. Untuk memitigasi serangan pada aplikasi adalah dengan menerapkan teknik *secure coding*. Secude coding merupakan teknik pemrograman yang mempertimbangkan sisi keamanan dari kode program yang digunakan.

3.8 Mitigasi serangan pada jarigan komputer

Mitigasi serangan pada jaringan komputer dapat dilakukan mulai dari desain jaringan komputer yang benar serta pemasangan aplikasi monitoring jaringan yang memiliki fitur *Intrusion Detection Ssytem* / *Intrusion Prevention System*. Desain jaringan yang direkomendasikan adalah desain jaringan komputer yang dapat berkembang mengikut perkembangan organisasi nya, serta dalam proses perkembangannya berdampak minimal terhadap jaringan *existing*. Terutama pada jaringan komputer nirkabel, harus memperhatikan faktor keamanan akses nya. Autentikasi pengguna jaringan komputer juga perlu di lakukan untuk mengidentifikasi setiap pengguna jaringan komputer misalnya menggunakan 802.1x (Kovačić, Đulić, & Šehidić, 2017) atau menggunakan sistem *captive portal*.

3.9 Mitigasi serangan pada basis data

SQL Injection dengan berbagai variannya merupakan serangan utama pada basis data. Penyebab dari serangan ini bukanlah merupakan kesalahan *Data Base Management System* namun lebih ke kesalahan logika pemrograman yang digunakan. Maka penggunaan kode SQL sebagai input pada sistem informasi harus di batasi. Teknik pembatasan tersebut telah di lakukan pada penelitian sebelumnya (O.P, O.S, & L.M., 2016). Pada penelitian tersebut para peneliti mengubah karakter spesial kedalam format HTML kemudian pengecekan dilakukan menggunakan regular *expression* dan *exceptions*.

3.10 Mitigasi serangan pada pengguna sistem informasi.

Edukasi merupakan cara yang paling efektif dalam memitigasi serangan terhadap pengguna sistem informasi. Dengan edukasi pengguna akan dapat mengetahui hal – hal yang boleh dilakukan serta hal – hal yang berpotensi bahaya. Untuk memperkuat edukasi, pada orgasisasi tertentu seperti pada perusahaan dapat menerapkan *policy* / aturan dalam penggunaan sistem informasi. Di tunjang dengan *Standard Operational Procedure* baku akan sangat efektif dalam memitigasi serangan terhadap pengguna sistem informasi karena setiap hal harus dilakukan sesuai dengan prosedur.

4. KESIMPULAN dan SARAN

Dari penelitian yang telah dilakukan, diketahui adanya model serangan pada masing – masing komponen penyusun sistem informasi. Dengan dilakukannya klasifiksai serangan akan memudahkan dalam mengidentifikasi setiap serangan yang mungkin ditujukan pada sistem informasi. Hasil dari penelitian ini menunjukkan bahwa terdapat model serangan pada setiap komponen penyusun sistem informasi yang dapat membahayakan sistem informasi tersebut. Mitigasi merupakan tindakan yang dilakukan untuk meminimalisir dampak yang ditimbulkan oleh setiap serangan. Mitigasi terhadap serangan pada masing – masing komponen juga telah di sampaikan pada penelitian ini. Dengan mengetahui berbagai serangan pada sistem informasi beserta mitigasinya, maka akan dapat dikembangkan sistem informasi yang lebih aman dalam segala aspek.

Penelitian ini dapat dikembankan lebih lanjut dengan mengklasifikasikan sistem informasi yang ada saat ini berdasarkan *platform* yang digunakannya. Dengan demikian dapat diketahui serangan – serangan yang dapat diaplikasikan pada masing – masing platform secara lebih detail sehingga saran pencegahan yang dapat diberikan juga akan semakin detail.

DAFTAR RUJUKAN

Ali, M., Husain, D., & Sharma, M. (2017). A study on Emerging Cyber Technologies, Threats and Prevention in Information Security. *IOSR Journal of Computer Engineering*, 49-54.

Babate, A., Musa, M., Kida, A., & Saidu, M. (2015). State of Cyber Security: Emerging Threats Landscape. *International Journal of Advanced Research in Computer Science & Technology*, 113-119.

Agarwal, M., Biswas, S., & Nandi, S. (2018). An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack. *International Journal of Wireless Information Networks*.

Akamai. (2018). *State of Te Internet: Security - Web Attack Report Infographic, 2018.* Akamai.

AL-FEDAGHI, S., & Alsumait, O. (2019). Towards a conceptual foundation for physical security: Case study of an it department. *International Journal of Safety and Security Engineering*, 137-156.

Alves, T., & Morris, T. (2018). Hardware-based Cyber Threats. *ICISSP 2018 - 4th International Conference on Information Systems Security and Privacy*, 259-266.

Bloom, G., Leontie, E., Narahari, B., & Simha, R. (2012). Hardware and Security: Vulnerabilities and Solutions. In S. K. Das, K. Kant, & N. Zhang, *Handbook on Securing Cyber-Physical Critical Infrastructure* (pp. 305-331). Elsevier.

Gens, D. (2018). *OS-Level Attacks and Defenses : From Software to Hardware-Based Exploits.* Technische Universität Darmstadt.

Group, A. P. (2020). *Phishing Activity Trends Report, 4th Quarter 2019.* APWG.

ID-SIRTII. (2018). *Laporan Tahunan ID-SIRTII.* ID-SIRTII.

Indonesia, P. (2008). *Undang - Undang No. 11*. Jakarta: Sekretariat Negara.

Jaafar, G. A., Abdullah, S. M., & Ismail, S. (2019). Review of recent detection methods for HTTP DDoS attack. *Journal of Computer Networks and Communications*, 1-10.

Kee, W. J., Kadir, M. A., Wahab, F. A., Mohamad, A. H., Mohamad, A. M., & Abidin, A. F. (2018). A Review on Spectre Attacks and Meltdown with its Mitigation Techniques. *International Journal of Engineering & Technology 7*, 209-213.

Kocher, P. H. (2019). Spectre attacks: Exploiting speculative execution. *2019 IEEE Symposium on Security and Privacy (SP)*, 1-19.

Kothari, H., Suwalka, A. K., & Kumar, D. (2019). Various Database Attacks, Approaches and Countermeasures To Database Security. *International Journal of Advance Research in Computer Science and Management*, 357-362.

Kovačić, S., Đulić, E., & Šehidić, A. (2017). Improving the Security of Access to Network Resources Using the 802.1x Standard in Wired and Wireless Environments. *22nd Internacionalna Naučno-Stručna Konferencija Informacione Tehnologije 2017*.

Mohammed, D., & Mohammed, S. (2017). Survey of Information Security Risk Management Models. *International Journal of Business, Humanities and Technology*, 23-26.

Moustafa, K., & Lalia, S. (2019). Implementation of Web Browser Extension for Mitigating CSRF Attack. *WorldCIST'19 2019. Advances in Intelligent Systems and Computing* (pp. 867-880). Springer.

Niakanlahiji, A., & Jafarian, J. H. (2019). WebMTD: Defeating Cross-Site Scripting Attacks Using Moving Target Defense. *Security and Communication Networks Volume 2019*, 1-13.

O.P, V., O.S, Y., & L.M., K. (2016). SQL Injection Prevention System. *2016 International Conference Radio Electronics & InfoCommunications*.

O'Brien, J. A., & Marakas, G. M. (2017). *Introduction to Information System.* McGraw Hill.

Safianu, O., Twum, F., & Hayfron-Acquah, J. (2016). Information System Security Threats and Vulnerabilities: Evaluating the Human Factor in Data Protection. *International Journal of Computer Applications*, 8-14.

Salamatian, S., Huleihel, W., Beirami, A., Cohen, A., & Medard, M. (2019). Why Botnets Work: Distributed Brute-Force Attacks Need No Synchronization. *IEEE Transactions on Information Forensics and Security, vol. 14, no. 9*, 2288-2299.

Sharma, P. (2016). Database Security: Attacks and Techniques. *International Journal of Scientific & Engineering Research, Volume 7, Issue 12*, 313-318.

SophosLab. (2013). *Security Threat Report.* SophosLab.

Tang, A., Sethumadhavan, S., & Stolfo, S. (2017). CLKSCREW: Exposing the Perils of Security Oblivious Energy Management. *26th USENIX Security Symposium* (pp. 1057-1074). Vancouver, BC, Canada: USENIX Association.

Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proceedings of the IEEE* (pp. 1727-1765). IEEE.