Pembuatan Bahan *Cyber Exercise* sebagai Sarana Latihan Penanganan Insiden *Malware* (Studi Kasus: Instansi XYZ)

Ghina Mariyah Fairuz[1)], Muhammad Yusuf Bambang Setiadji[2)]
(1) Rekayasa Keamanan Siber, ghina.mariyah@bssn.ac.id
(2) Rekayasa Keamanan Siber, yusuf.setiadji@poltekssn.ac.id

Abstrak

Serangan malware semakin berkembang di dunia, termasuk di Indonesia. Salah satu sektor yang menjadi target serangan malware adalah sektor pendidikan. Contoh nyata insiden malware pada sektor pendidikan adalah insiden malware di Instansi pendidikan XYZ. Insiden tersebut mengakibatkan terganggunya layanan e-mail Instansi XYZ, data pribadi mahasiswa hilang atau terenkripsi, serta terganggunya kinerja perangkat elektronik yang terinfeksi. Berkaca dari insiden yang pernah terjadi, Instansi XYZ sebaiknya memiliki kemampuan penanganan insiden. Kemampuan penanganan insiden dapat dilatih melalui kegiatan Cyber Exercise. Penelitian ini bertujuan untuk menghasilkan bahan berupa dokumen Participants Handout dan lingkungan simulasi yang dapat digunakan untuk Cyber Exercise insiden malware oleh pengelola TI Instansi XYZ. Pembuatan bahan dilakukan berdasarkan siklus Cyber Exercise dengan skenario insiden malware jenis ransomware. Skenario penanganan insiden yang dilakukan mengacu pada NIST SP 800-83r1. Berdasarkan penelitian yang dilakukan, diperoleh hasil keluaran berupa mesin virtual sebagai lingkungan simulasi insiden, berkas hasil tangkapan jaringan, dan dokumen Participants Handout yang berisi enam studi kasus skenario insiden.

Kata kunci: *Cyber Exercise*, Insiden, Lingkungan Simulasi, *Malware*, Penanganan Insiden, *Participants Handout*

1. PENDAHULUAN

Serangan siber semakin berkembang dan beragam jenisnya seiring dengan kemajuan teknologi informasi dan komunikasi saat ini. Salah satu serangan siber yang umum terjadi adalah serangan *malware*. Serangan *malware* terus meningkat dan menyebar di seluruh dunia, termasuk di Indonesia. Pada awal tahun 2019, tercatat bahwa Indonesia merupakan negara dengan jumlah serangan *malware* terbanyak dalam lingkup regional Asia-Pasifik [2].

Salah satu sektor yang menjadi target serangan *malware* adalah sektor pendidikan. Sektor ini merupakan salah satu sektor utama target serangan *malware* jenis *trojan* dan merupakan urutan kedua sasaran serangan *malware* jenis *ransomware* [3]. Contoh nyata insiden *malware* pada sektor pendidikan di Indonesia adalah insiden *malware* di Instansi XYZ. Instansi XYZ merupakan salah satu perguruan tinggi kedinasan yang ada di Indonesia. Layanan *e-mail* yang dikelola oleh Unit Laboratorium Instansi XYZ pernah terkena insiden *malware* [4]. *Malware* menginfeksi *mail server* melalui perangkat elektronik pribadi mahasiswa. Hal ini menyebabkan akun *e-mail* mahasiswa yang bersangkutan harus dinonaktifkan dan *mail* Instansi XYZ masuk ke dalam daftar hitam beberapa domain *e-mail*. Selain itu, sebanyak 42 perangkat elektronik milik mahasiswa Instansi XYZ juga pernah terkena insiden *malware* [5]. Tiga puluh enam di antaranya merupakan insiden *malware* pada laptop dan sisanya pada *smartphone*. Kebanyakan dampak dari insiden tersebut adalah munculnya iklan terus-menerus pada perangkat elektronik mahasiswa, serta data pribadi mahasiswa yang hilang ataupun terenkripsi.

Berkaca dari insiden yang pernah terjadi, Instansi XYZ sebaiknya memiliki kemampuan penanganan insiden. Penanganan insiden merupakan mitigasi pelanggaran kebijakan keamanan dan tindakan yang direkomendasikan untuk melakukan mitigasi tersebut [6]. Dengan memiliki kemampuan penanganan insiden, setiap insiden yang terjadi dapat direspon secara sistematis sehingga tindakan yang tepat dapat dilakukan. Selain itu, adanya penanganan insiden juga dapat membatasi dampak kerusakan yang terjadi dan mengurangi biaya pemulihan [7], meminimalisir kehilangan informasi dan gangguan layanan, menjadi bahan pembelajaran untuk penanganan insiden di masa mendatang dan rekomendasi untuk perlindungan yang lebih baik terhadap sistem dan informasi organisasi [6].

Salah satu cara untuk melatih kemampuan penanganan insiden adalah melalui *Cyber Exercise* [8]. *Cyber Exercise* merupakan simulasi keadaan darurat yang melibatkan perencanaan, persiapan, dan pelaksanaan yang dilakukan untuk tujuan latihan dan evaluasi [9]. Dalam penyelenggaraan *Cyber Exercise*, terdapat kebutuhan yang perlu dipersiapkan. Salah satunya yaitu bahan *Cyber Exercise* berupa lingkungan simulasi insiden dan dokumen *Participants Handout*.

Pada penelitian ini dilakukan pembuatan bahan *Cyber Exercise* untuk unit yang membidangi teknologi informasi (TI) di Instansi XYZ. Bahan tersebut diharapkan dapat membantu pengelola TI

dalam melatih kemampuan penanganan insiden dan meminimalisir dampak kerugian yang ditimbulkan.

2. LANDASAN TEORI

Pada bab ini akan dijelaskan beberapa teori yang mendukung penelitian berdasarkan hasil tinjauan beberapa literatur terkait *malware*, insiden, penanganan insiden, dan *Cyber Exercise*.

2.1. *Malware*

Malware atau *malicious software* merupakan semua perangkat lunak yang digunakan dengan tujuan untuk melanggar sistem komputer dan kebijakan keamanan yang berhubungan dengan aspek kerahasiaan, keutuhan, dan ketersediaan [1]. *Malware* juga dapat diartikan sebagai kode yang melakukan aksi berbahaya. *Malware* dapat berupa *script*, kode, *executable file*, maupun bentuk lainnya, yang dapat tersebar melalui banyak media, seperti situs internet, *e-mail*, ataupun USB. Penyerang dapat menggunakan *malware* untuk mencuri informasi rahasia, memata-matai sistem yang disusupi, ataupun mengambil alih kontrol terhadap sistem targetnya [10].

2.2. Insiden

Insiden keamanan komputer merupakan suatu pelanggaran atau ancaman pelanggaran yang terjadi terhadap keamanan komputer, peraturan yang disepakati, atau kebijakan standar keamanan [6]. Insiden juga didefinisikan sebagai kejadian yang sebenarnya atau dinilai berpotensi membahayakan kerahasiaan, integritas, atau ketersediaan sistem informasi, atau informasi yang diproses, disimpan, atau ditransmisikan oleh sistem; atau yang merupakan pelanggaran atau ancaman pelanggaran kebijakan keamanan, prosedur keamanan, atau kebijakan penggunaan yang dapat diterima [11].
Contoh-contoh insiden yaitu sebagai berikut:

1. Adanya kebocoran data organisasi ke pihak yang tidak bertanggung jawab sehingga menimbulkan kerugian bagi organisasi.
2. Penyerang menggunakan *botnet* untuk mengirimkan permintaan koneksi dalam jumlah sangat banyak sehingga menyebabkan komputer target menjadi tidak berfungsi dengan baik.
3. Dokumen penting milik organisasi menjadi terenkripsi karena adanya *malware* yang berhasil menyusup ke dalam jaringan internal organisasi.

2.3. Penanganan Insiden

Berdasarkan NIST SP 800-61r2, penanganan insiden dan respon insiden merupakan hal yang sama, yaitu mitigasi pelanggaran kebijakan keamanan dan tindakan yang direkomendasikan untuk melakukan mitigasi tersebut [6]. Pada standar ini, tindakan penanganan insiden berupa sebuah siklus yang terdiri dari beberapa fase seperti yang tercantum pada Gambar 1. Siklus penanganan insiden pada NIST SP 800-61r2 ditujukan untuk insiden siber secara umum. Panduan ini kemudian dijadikan sebagai acuan dalam standar NIST lainnya, yaitu NIST SP 800-83r1 *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*. Tahapan penanganan insiden dalam NIST SP 800-83r1 secara spesifik ditujukan untuk insiden *malware* dan tetap sejalan dengan siklus penanganan insiden pada NIST SP 800-61r2.

Gambar 1 Siklus Penanganan Insiden
Sumber: NIST SP 800-61r2

2.4. *Cyber Exercise*

Cyber Exercise merupakan simulasi keadaan darurat yang melibatkan perencanaan, persiapan, dan pelaksanaan yang dilakukan untuk tujuan latihan dan evaluasi [9]. Kegiatan ini berguna untuk melatih kemampuan personel dalam melakukan penanganan insiden [6]. Salah satu manfaat dari *Cyber Exercise* adalah dapat memastikan personel telah siap dan mampu melakukan penanganan insiden secara efisien dengan mengikuti prosedur yang ada, serta dapat memperlihatkan kekurangan pada prosedur tersebut sehingga nantinya dapat dijadikan bahan evaluasi untuk perbaikan [12].

Dalam pelaksanaan *Cyber Exercise*, diperlukan persiapan yang matang dan sesuai dengan kebutuhan organisasi. Oleh karena itu, agar *Cyber Exercise* berhasil dilakukan, maka dilakukan langkah-langkah yang disebut siklus *Cyber Exercise*. Seperti yang terlihat pada Gambar 2, siklus ini terdiri dari empat fase, yaitu *Identifying*, *Planning*, *Conducting*, dan *Evaluating* [12].

Gambar 2 Siklus *Cyber Exercise*
Sumber: Diolah kembali dari [12]

Pada fase *Identifying* dilakukan pengumpulan informasi untuk menentukan tujuan, hasil, lingkup, jenis, gambaran skenario insiden, dan skenario *Cyber Exercise*. Kemudian pada tahap *Planning*, dilakukan persiapan pelaksanaan dengan pembuatan skenario dan lingkungan simulasi yang akan digunakan peserta *Cyber Exercise*. Selanjutnya pada fase *Conducting*,

dilakukan kegiatan *Cyber Exercise*. Fase terakhir yaitu fase *Evaluating*, meliputi pelaksanaan *hotwash*, pembuatan *After Actions Report* (AAR), dan mendokumentasikan pelajaran yang dapat diambil (*lesson-learned*) dari kegiatan *Cyber Exercise*.

3. METODE PENELITIAN

Metode penelitian yang digunakan pada penelitian ini menggunakan siklus *Cyber Exercise* yang dikeluarkan oleh ENISA (*European Network and Information Security Agency*). Berdasarkan Gambar 3, tahapan penelitian diawali dengan melakukan identifikasi masalah. Kemudian dilanjutkan dengan pengumpulan data. Setelah mendapatkan data yang dibutuhkan, dilakukan fase *Identifying* dan fase *Planning* dari siklus *Cyber Exercise* sehingga mendapatkan hasil penelitian berupa lingkungan simulasi dan dokumen *Participant Handout* sebagai bahan *Cyber Exercise*. Bahan tersebut selanjutnya dapat digunakan pada saat penyelenggaraan *Cyber Exercise*. Namun, pada penelitian ini fase *Conducting* dan fase *Evaluating* tidak dilakukan karena keterbatasan waktu penelitian, sehingga kegiatan *Cyber Exercise* beserta pelaksanaan evaluasinya tidak dapat diselenggarakan.

Gambar 3 Tahapan Penelitian
Sumber: Olahan sendiri

4. HASIL DAN PEMBAHASAN

Pada bagian ini akan dibahas pembuatan bahan *Cyber Exercise* berdasarkan fase *Identifying* dan *Planning* dalam siklus *Cyber Exercise*.

4.1. Fase *Identifying*

Fase *Identifying* dilakukan melalui diskusi bersama *stakeholder* terkait. Pada penelitian ini, diskusi dilakukan antara peneliti dengan Unit Laboratorium selaku pengelola TI Instansi XYZ, yang diwakili oleh Pranata Komputer selaku pihak yang selama ini menangani insiden siber di Instansi XYZ. Hasil dari kegiatan diskusi tercantum pada Tabel 1.

Tabel 1 Hasil fase *Identifying*

Pembahasan	Hasil	Latar Belakang
Identifying Clear Objectives	Melatih kemampuan penanganan insiden di Instansi XYZ	Adanya insiden siber yang terjadi di Instansi XYZ dan semakin meningkatnya serangan siber di dunia.
Choosing High Level Scenario	Insiden *malware*	Terjadinya insiden *malware* di Instansi XYZ yang menimpa *mail server* Instansi XYZ maupun perangkat elektronik milik mahasiswa.
Choosing Type of Exercise	*Operation-based*	Pada *Cyber Exercise* tipe ini, peserta melakukan praktik secara langsung pada lingkungan simulasi yang disediakan sehingga dapat melatih kemampuan penanganan insiden secara teknis.
Identifying Key Participants	- *Organizer*: Peneliti	Organisasi yang memimpin penyelenggaraan *Cyber Exercise* adalah Unit Laboratorium selaku pihak yang mengelola TI di Instansi XYZ. Namun, pada penelitian ini peran *Organizer* dilakukan oleh peneliti.
	- *Planner*: Peneliti	Organisasi atau individu yang terlibat dalam perencanaan *Cyber Exercise* adalah Unit Laboratorium selaku pihak yang mengelola TI di Instansi XYZ. Namun, pada penelitian ini peran *Planner* dilakukan oleh peneliti.
	- *Participant*: Pranata Komputer	Pranata Komputer merupakan pihak yang selama ini menangani insiden siber di Instansi XYZ.
	- *Exercise director*, *moderator* atau *leadership team*: Tidak ditentukan	Pada penelitian ini, peran *Moderator* tidak digunakan karena fase *Conducting* tidak dilakukan.
	- *Monitor* atau *Facilitator:* Tidak ditentukan	Pada penelitian ini, peran *Monitor* tidak digunakan karena fase *Conducting* tidak dilakukan.
	- *Observer:* Tidak ditentukan	Pada penelitian ini, peran *Observer* tidak digunakan karena fase *Conducting* tidak dilakukan.
	- *Evaluator:* Tidak ditentukan	Pada penelitian ini, peran *Evaluator* tidak digunakan karena fase *Evaluating* tidak dilakukan.
Setting Size and Scope	Skala kecil yang dibatasi hanya dalam lingkup Instansi XYZ, yang pada pelaksanaannya diwakili oleh jajaran Unit Laboratorium selaku pengelola TI di Instansi XYZ.	Studi kasus penelitian yang dibatasi hanya di lingkup Instansi XYZ.

4.2. Fase *Planning*

Pada fase ini dilakukan pengembangan skenario dan pembuatan lingkungan simulasi yang sesuai dengan keluaran dari fase sebelumnya. Skenario insiden *malware* yang sudah ditentukan pada fase *Identifying* selanjutnya dikembangkan menjadi skenario yang lebih detail.

4.2.1. Identifikasi Serangan

Identifikasi serangan diawali dengan menentukan spesimen *malware* yang akan digunakan. *Malware* tersebut sebaiknya memberikan gambaran insiden yang realistis. Spesimen *malware* yang digunakan berjumlah 5 sampel berjenis *Trojan Downloader* dan *Ransomware*, yang termasuk jenis *malware* terbanyak yang menyerang Indonesia. Dilakukan analisis statis dan dinamis terhadap lima sampel tersebut. Analisis statis dilakukan dengan mempelajari dan memahami *source code* dari sampel *malware*, sedangkan analisis dinamis dilakukan dengan mempelajari perilaku dari sampel *malware* yang dijalankan. Informasi terkait spesimen *malware* didapatkan dari analisis statis menggunakan Virus Total. Analisis dinamis dilakukan selama sekitar satu jam di dalam lingkungan virtual. Adapun sampel *malware* yang menunjukkan dampak berbahaya tercantum pada Tabel 2.

Tabel 2 Informasi sampel *malware* beserta dampaknya

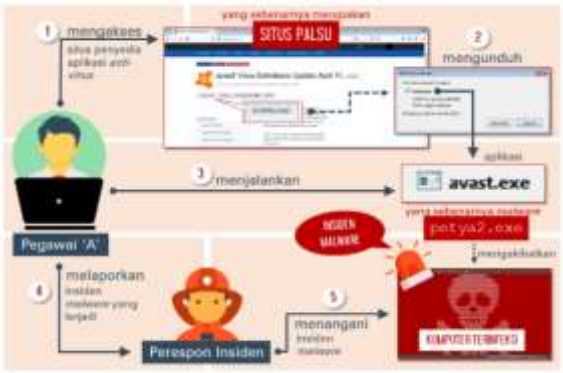
Jenis	No.	Nama *file*	Dampak yang terlihat
Ransomware	3	wannacry.exe	Sistem terinfeksi dan terlihat dampak terenkripsinya *file-file* pada sistem kemudian muncul aplikasi untuk meminta bayaran jika target ingin mendapatkan datanya kembali.
	5	petya2.exe	Sistem terinfeksi dan terlihat dampaknya pada sistem muncul tampilan meminta bayaran jika target ingin mendapatkan kunci dekripsi.

Aktivitas berbahaya terlihat pada sampel 3 dan 5 spesimen *malware* jenis *ransomware* dengan nama *file* wannacry.exe dan petya2.exe. Berkaitan dengan jenis *malware* tersebut, diketahui bahwa sistem yang terinfeksi oleh *ransomware* yang melakukan enkripsi dapat dipulihkan dengan aplikasi dekripsi. Hal ini perlu dipertimbangkan karena keberhasilan aplikasi dekripsi akan memberikan gambaran penanganan insiden yang lebih jelas ketika pelaksanaan *Cyber Exercise*.

Saat ini telah ada aplikasi dekripsi untuk kedua tipe *ransomware* tersebut, namun yang berhasil mendekripsi saat uji coba adalah aplikasi dekripsi untuk *ransomware* tipe Petya dengan nama petya_key.exe. Oleh karena itu, *malware* sampel 5 digunakan sebagai serangan di dalam lingkungan simulasi insiden.

4.2.2. Rancangan Skenario Insiden

Setelah menentukan spesimen *malware* yang akan digunakan, selanjutnya ditentukan rancangan skenario awal serangan *malware* tersebut. Pada penelitian ini, rancangan skenario inisiasi serangan yaitu penyerang menyediakan suatu situs palsu yang berisikan *malware*, lalu diakses oleh korban. Setelah itu korban mengunduh aplikasi yang merupakan *malware* tersebut. Pada skenario insiden, ditetapkan bahwa korban merupakan pegawai Instansi XYZ bernama 'A'. Situs palsu yang diakses oleh korban menyerupai situs penyedia aplikasi *anti-virus* terpercaya, sehingga korban mengunduh dan menjalankan aplikasi dari situs palsu tersebut. Setelah menyadari komputernya terkena insiden, korban melaporkan peristiwa tersebut kepada pengelola TI selaku perespon insiden siber di Instansi XYZ. Gambaran dari rancangan skenario insiden yang telah dibuat dapat dilihat pada Gambar 4.



Gambar 4 Rancangan skenario insiden
Sumber: Olahan sendiri

4.2.3. Pembuatan Lingkungan Simulasi Insiden

Untuk mewujudkan rancangan skenario, dilakukan pembuatan situs palsu seperti pada Gambar 5 sebagai media untuk menyisipkan *malware*. *File malware* akan terunduh ketika korban memilih tombol dengan fitur *download* pada situs tersebut. *File malware* dibuat menyerupai aplikasi *anti-virus* yang ditawarkan pada situs palsu, sehingga nama *file malware* yang disisipkan diubah terlebih dahulu menjadi avast.exe.

Gambar 5 Tampilan situs palsu
Sumber: Olahan sendiri

Setelah membuat skenario inisiasi serangan, dilakukan persiapan perangkat maupun aplikasi yang digunakan dalam merancang lingkungan simulasi sesuai dengan spesifikasi seperti pada Tabel 3.

Tabel 3 Spesifikasi lingkungan simulasi

Nama Mesin	Spesifikasi	Alamat IP / Mode Jaringan	Aplikasi yang digunakan
VM_Victim	Windows 7 Ultimate, RAM 1024 MB	10.0.2.6 / NAT *Network*	Mozilla Firefox
VM_Attacker	Ubuntu 18.04, RAM 1435 MB	10.0.2.10 / NAT *Network*	Apache *web server*
VM_Monitor	Ubuntu 18.04, RAM 1435MB	10.0.2.7 / NAT *Network* dengan mode *Promiscuous*: *Allow VMs*	Wireshark, INetSim

Skenario insiden direalisasikan dalam lingkungan simulasi dengan langkah-langkah berikut:

1. Menjalankan *web server* di mesin VM_Attacker agar situs palsu dapat diakses oleh korban.
2. Menjalankan aplikasi INetSim dan Wireshark di mesin VM_Monitor. Aplikasi INetSim digunakan sebagai penyedia layanan simulasi internet sehingga koneksi menuju internet yang melalui alamat IP VM_Monitor tidak disambungkan ke jaringan internet yang asli. Aplikasi Wireshark digunakan untuk menangkap data pada lalu lintas jaringan selama serangan.
3. Menjalankan skenario yang telah dibuat, yaitu korban mengakses situs palsu melalui mesin VM_Victim dan mengunduh aplikasi avast.exe.
4. Korban menjalankan aplikasi yang telah diunduh. Sistem operasi memunculkan peringatan bahwa aplikasi yang akan dijalankan tidak berasal dari sumber terpercaya, namun tidak dihiraukan oleh korban dan dijalankan. Setelah itu, komputer korban mati secara tiba-tiba. Hal ini ditunjukkan dari *log* Virtualbox yang mencatat bahwa status mesin VM_Victim menjadi 'PoweredOff' seperti pada Gambar 6.
5. Mesin VM_Victim telah terinfeksi *malware*, hal ini menunjukkan bahwa insiden berhasil disimulasikan. Selanjutnya yaitu melakukan ekstraksi mesin VM_Victim ke dalam format OVA. *File* OVA inilah yang akan menjadi lingkungan simulasi penanganan insiden.

Gambar 6 Status mesin VM_Victim
Sumber: Olahan sendiri

6. Memastikan *file* OVA dapat digunakan untuk simulasi penanganan insiden dengan cara melakukan impor OVA tersebut. Pada Gambar 7 terlihat bahwa *file* OVA dapat dijalankan dan memunculkan tampilan yang tidak biasa. Selanjutnya tampilan komputer tersebut di-*capture* dan disimpan sebagai bukti terjadinya insiden.

Gambar 7 Tampilan mesin yang telah terinfeksi
Sumber: Olahan sendiri

7. Menghentikan proses *capture* jaringan pada Wireshark di mesin VM_Monitor dan menyimpan hasilnya dalam *file* PCAP.

4.2.4. Rancangan Skenario Penanganan Insiden

Skenario penanganan insiden dirancang berdasarkan standar NIST SP 800-83r1 *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* [13]. Standar ini dipilih karena berisi panduan penanganan insiden yang secara spesifik ditujukan untuk insiden *malware* sehingga sesuai dengan skenario insiden yang telah dibuat. Hasil dari tahap ini digunakan untuk membuat studi kasus di dalam dokumen *Participants Handout*. Hasil rancangan skenario penanganan insiden sesuai dengan urutan tindakan penanganan insiden pada NIST SP 800-83r1 dijabarkan pada Tabel 4.

4.2.5. Pembuatan Dokumen *Participants Handout*

Pada penelitian ini, dokumen *Participants Handout* untuk Instansi XYZ dibuat dengan mengacu pada dokumen *Participants Handout* kegiatan *The 2019 Critical Information Infrastructure Cyber Exercise: Malware Attack and Mitigation Strategy* yang diselenggarakan oleh Badan Siber dan Sandi Negara (BSSN). Secara umum, dokumen tersebut terdiri dari Pendahuluan, Deskripsi Kegiatan, Pelaksanaan dan Skenario Kegiatan, serta Studi Kasus [17].

Dokumen *Participants Handout* untuk Instansi XYZ berisi gambaran umum kegiatan beserta studi kasus insiden yang dibahas. Gambaran umum kegiatan *Cyber Exercise* terdiri dari latar belakang, tujuan, peserta, dan deskripsi kegiatan. Studi kasus terdiri dari deskripsi kasus, pertanyaan, keterangan material pendukung/alat bantu, dan petunjuk guna menjawab pertanyaan pada studi kasus tersebut.

Pembuatan dokumen *Participants Handout* dilakukan secara bertahap dengan langkah-langkah berikut:

1. Membuat rancangan dokumen

Rancangan dokumen *Participants Handout* dilakukan oleh peneliti sebagai pihak yang mewakili Unit Laboratorium dalam menjalankan peran *Planner*. Hasil rancangan dokumen *Participants Handout* tercantum pada Tabel 5.

Tabel 4 Hasil rancangan skenario penanganan insiden

Preparation
1. Instansi XYZ memiliki pegawai yang bertugas sebagai perespon insiden, yaitu Pranata Komputer yang termasuk ke dalam jajaran Unit Laboratorium Instansi XYZ. 2. Pranata Komputer terdiri dari dua orang dan belum memiliki ketetapan mekanisme komunikasi dan koordinasi dalam hal penanganan insiden. 3. Instansi XYZ belum memiliki Standar Operasional Prosedur (SOP) penanganan insiden, khususnya insiden *malware*. 4. Instansi XYZ memiliki sumber daya yang dapat digunakan untuk melakukan penanganan insiden secara umum, seperti komputer dan perangkat jaringan.
Detection and Analysis
1. Deteksi oleh perespon insiden dilakukan dengan menerima laporan atau informasi tentang terjadinya insiden dari seorang pegawai Instansi XYZ bahwa komputernya menampilkan informasi yang tidak biasa setelah dinyalakan ulang. 2. Perespon insiden mengumpulkan informasi yang dapat mendukung hipotesis awal, yaitu informasi terkait kronologi peristiwa yang terjadi dan kondisi komputer korban saat itu. 3. Berdasarkan pernyataan korban, diketahui bahwa sebelum komputer korban mati secara tiba-tiba, korban mengunduh aplikasi *anti-virus* dan melakukan instalasi pada komputer tersebut. Kondisi komputer korban saat itu masih terhubung dengan internet dan fitur *file sharing* masih aktif. 4. Perespon insiden menyusun tindakan penanganan insiden sesuai dengan urutan prioritas berdasarkan panduan penanganan insiden seperti NIST SP 800-83r1. 5. Perespon insiden memastikan penyebab insiden dengan cara menganalisis lalu lintas jaringan menggunakan Wireshark dan mendapatkan aplikasi yang diunduh oleh korban. 6. Perespon insiden melakukan analisis statis terhadap aplikasi tersebut menggunakan situs Virus Total, sehingga dapat diketahui nama lain aplikasi tersebut, nilai *hash*, waktu pembuatan, dan aktivitas yang dilakukan oleh aplikasi tersebut saat menginfeksi komputer korban.
Containment
Perespon insiden mencegah penyebaran *malware* dan dampak lanjutan pada komputer terinfeksi. Hal ini dilakukan dengan metode penghentian layanan dan konektivitas, yaitu: 1. Perespon insiden memutus koneksi internet pada komputer terinfeksi. 2. Perespon insiden menonaktifkan fitur *file sharing* komputer lain yang terhubung dengan komputer terinfeksi.
Eradication
Pada skenario insiden, *ransomware* tipe Petya yang menginfeksi komputer korban melakukan *reboot* dan enkripsi terhadap sistem komputer tersebut. Hal ini menyebabkan sistem tidak dapat diakses sehingga tindakan penghapusan *malware* pada sistem tidak dapat dilakukan secara manual sebagaimana menghapus suatu *file* pada umumnya. Oleh karena itu, dibutuhkan *tools* tambahan dalam melakukan tahap ini. Salah satu *tools* yang dapat digunakan adalah aplikasi dekripsi. Langkah-langkah yang dilakukan ialah: 1. Mencari informasi terkait aplikasi dekripsi untuk *ransomware* tipe Petya yang sesuai dengan hasil analisis statis. Diketahui bahwa terdapat aplikasi dekripsi bernama petya_key yang dikeluarkan pada tahun 2017. Aplikasi tersebut diklaim dapat mendekripsi sistem yang terinfeksi *ransomware* tipe Petya versi lama [14] [15]. Berdasarkan hasil analisis statis, diketahui bahwa *malware* penyebab insiden dikompilasi pada tanggal 30 Januari 2016, sehingga termasuk tipe Petya versi lama dan sesuai dengan aplikasi dekripsi petya_key. 2. Mengunduh aplikasi dekripsi petya_key. 3. Menghapus penyebab insiden *malware* dengan aplikasi petya_key pada komputer terinfeksi. 4. Perespon memperbaiki kondisi/perangkat yang menjadi sumber kerawanan sehingga menyebabkan terjadinya insiden, guna mencegah insiden serupa terulang kembali. Langkah-langkah yang dapat dilakukan untuk mencegah insiden *ransomware* Petya pada komputer korban antara lain: memasang *patch* MS17-010, menonaktifkan fungsi SMBv1, dan memperbarui *signature* pada *anti-virus* atau *anti-malware* [16].
Recovery
Perespon insiden pemulihan fungsi dan data milik sistem terinfeksi seperti kondisi semula dengan menghubungkan kembali koneksi internet dan mengaktifkan fitur *file sharing*.
Post-Incident Activity
1. Memperoleh pelajaran dari insiden yang terjadi dan menyusun rencana kedepannya. Tindakan yang dapat dilakukan oleh perespon insiden antara lain: a. Memberikan himbauan kepada seluruh pegawai dan mahasiswa Instansi XYZ agar meningkatkan kesadaran keamanan siber; b. Memberikan himbauan kepada seluruh pegawai dan mahasiswa Instansi XYZ agar tidak mengunduh aplikasi dari sumber yang tidak terpercaya dan memeriksa terlebih dahulu keamanan berkas yang diunduh dari internet sebelum menjalankannya; c. Memberikan himbauan kepada seluruh pegawai dan mahasiswa Instansi XYZ agar senantiasa melakukan *back-up* secara berkala; d. Memasang *patch* MS17-010 pada komputer yang ada di Instansi XYZ; e. Menonaktifkan fungsi SMBv1 pada komputer yang ada di Instansi XYZ; f. Memperbarui *signature* pada *anti-virus* atau *anti-malware* pada komputer yang ada di Instansi XYZ; dan g. Merancang Standar Operasional Prosedur (SOP) penanganan insiden Instansi XYZ agar terdapat acuan tetap dalam melakukan penanganan insiden. 1. Membuat laporan penanganan insiden.

Tabel 5 Rancangan dokumen *Participants Handout*

Hal.	Isi	Rincian Isi
1	*Cover*	Judul dokumen, yaitu *Cyber Exercise Instansi XYZ Participants Handout*.
2	Pendahuluan	• Latar Belakang • Tujuan • Peserta Kegiatan
3	Deskripsi Kegiatan	Penjelasan terkait kegiatan *Cyber Exercise* akan dibagi ke dalam tiga sesi, yakni sesi pembuka, utama, dan penutup.
4 – 7	Studi Kasus	Deskripsi kasus, pertanyaan, keterangan material pendukung/alat bantu, dan petunjuk

Rangkaian studi kasus dibuat berdasarkan rancangan skenario penanganan insiden yang diubah ke dalam bentuk pertanyaan dan dielaborasi sesuai dengan urutan tahapan penanganan insiden sehingga menghasilkan enam studi kasus pada rancangan dokumen *Participants Handout*.

2. Melakukan simulasi dokumen

Untuk menghasilkan dokumen *Participants Handout* yang dapat dipahami oleh peserta *Cyber Exercise*, dilakukan simulasi terhadap rancangan dokumen tersebut. Simulasi ini juga bertujuan untuk mendapatkan saran guna perbaikan rancangan dokumen. Simulasi dilakukan oleh *Planner* selaku pihak yang terlibat dalam perencanaan kegiatan *Cyber Exercise*. Pada proses simulasi, peneliti sebagai pihak yang menjalankan peran *Planner*, diwakili oleh pihak lain, yaitu mahasiswa Instansi XYZ yang pernah terkena insiden *malware*. Pelaksanaan simulasi dilakukan melalui penyebaran kuesioner kepada 41 mahasiswa sebagai responden.

Berdasarkan hasil pelaksanaan simulasi, dinyatakan bahwa seluruh responden memahami isi rancangan dokumen *Participants Handout*, serta terdapat sepuluh saran yang diterima, yaitu tiga saran tidak diterima, enam saran diterima, dan satu saran diterima dengan penyesuaian. Saran-saran yang diterima selanjutnya diterapkan pada rancangan dokumen *Participants Handout* guna perbaikan dokumen tersebut.

3. Melakukan perbaikan dokumen.

Saran yang diterima diterapkan pada penulisan rangkaian Studi Kasus di dokumen *Participants Handout* sebagaimana yang tercantum pada Tabel 6.

Tabel 6 Studi Kasus pada Dokumen *Participants Handout*

Hal.	Keterangan	Isi
4	Kasus ke-	1
	Judul kasus	Laporan Terjadinya Insiden
	Deskripsi Kasus	Pada pukul 15.55 WIB, seorang pegawai 'A' Instansi XYZ menyampaikan kepada jajaran Unit Laboratorium terkait komputernya yang menampilkan informasi tidak biasa setelah dinyalakan ulang.
	Pertanyaan	Sebagai perespon insiden, apa informasi yang diperlukan dari pegawai tersebut untuk mengetahui detail peristiwa yang terjadi?
	Alat Bantu	Tangkapan layar komputer terinfeksi setelah dinyalakan ulang (Screenshot1.png)
	Petunjuk	Jabarkan hal-hal yang perlu ditanyakan kepada pegawai 'A' selaku pelapor insiden untuk mendukung hipotesis awal dari insiden yang terjadi.
4	Kasus ke-	2
	Judul kasus	Rencana tindakan yang akan dilakukan
	Deskripsi Kasus	Berdasarkan pernyataan pegawai 'A', sebelumnya ia mengunduh aplikasi yang diyakini merupakan *anti-virus*. Akan tetapi tiba-tiba komputernya mati ketika menjalankan aplikasi tersebut. Saat dinyalakan ulang, komputer menampilkan informasi yang tidak biasa. Komputer pegawai 'A' diketahui dalam kondisi terhubung dengan internet dan jaringan lokal, serta fitur *file sharing* yang masih aktif.
	Pertanyaan	Apa tindakan yang akan anda lakukan? Tuliskan berdasarkan urutan prioritas.
	Alat Bantu	Dokumen NIST SP.800-83r1 *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
	Petunjuk	1. Pelajari dokumen NIST SP.800-83r1. Dokumen tersebut merupakan panduan penanganan insiden yang secara spesifik ditujukan untuk insiden *malware.* 2. Buat rencana tindakan yang akan anda ambil selaku perespon insiden berdasarkan tahapan penanganan insiden yang telah anda pelajari.
5	Kasus ke-	3
	Judul kasus	Analisis *Malware*
	Deskripsi Kasus	Agar dapat mengidentifikasi apa yang terjadi pada komputer pegawai 'A', anda mencari tahu tentang aplikasi yang diunduh sebelum insiden terjadi.
	Pertanyaan	1. Apa aplikasi yang diunduh oleh pegawai 'A'? Dapatkan sampel aplikasi tersebut. 2. Kapan aplikasi tersebut diunduh? 3. Apa jenis aplikasi berbahaya (*malware*) yang menginfeksi komputer pegawai 'A'? 4. Berapa nilai *hash* aplikasi tersebut? 5. Apa saja nama lain aplikasi tersebut? 6. Kapan aplikasi tersebut dikompilasi? 7. Apa aktivitas yang dilakukan oleh aplikasi tersebut pada komputer yang terinfeksi?
	Alat Bantu	1. *File* PCAP 2. Wireshark 3. Virus Total
	Petunjuk	1. Lakukan analisis *file* PCAP menggunakan Wireshark. 2. Dapatkan *file malware* dari *file* PCAP tersebut. Harap berhati-hati, jangan sampai tereksekusi. 3. Lakukan analisis statis pada *malware* menggunakan situs Virus Total.
6	Kasus ke-	4
	Judul kasus	Menghilangkan Penyebab Insiden
	Deskripsi Kasus	Anda telah mengetahui *file* yang menginfeksi komputer pegawai 'A'. Selanjutnya dilakukan pencegahan penyebaran *malware* dan memutus dampak lanjutan, dengan cara menghentikan koneksi internet dan fitur *file sharing.* Tindakan selanjutnya menghilangkan penyebab insiden dari komputer terinfeksi.
	Pertanyaan	Bagaimana cara menghilangkan *malware* penyebab insiden dari komputer terinfeksi? Dokumentasikan langkah-langkah yang anda lakukan.
	Alat Bantu	1. VM_Victim.ova 2. Aplikasi Virtualbox 3. Aplikasi dekripsi 4. Mesin virtual tambahan dengan sistem operasi Windows
	Petunjuk	1. Impor *file* VM_Victim.ova menggunakan aplikasi Virtualbox 2. Ikuti petunjuk penggunaan aplikasi dekripsi 3. Gunakan mesin virtual tambahan untuk menjalankan aplikasi dekripsi
6	Kasus ke-	5
	Judul kasus	Upaya Pencegahan
	Deskripsi Kasus	*Malware* berhasil dihilangkan, selanjutnya anda perlu memperbaiki kondisi/perangkat yang menjadi sumber kerawanan sehingga menyebabkan terinfeksinya komputer. Hal ini

Hal.	Keterangan	Isi
		dilakukan untuk mencegah insiden yang sama terulang kembali.
	Pertanyaan	Apa yang harus anda lakukan sebagai upaya pencegahan insiden *malware* tersebut?
	Alat Bantu	*Web browser*
	Petunjuk	1. Pelajari insiden yang telah terjadi dan tentukan tindakan yang perlu anda lakukan selaku perespon insiden di Instansi XYZ. 2. Cari informasi tentang upaya pencegahan insiden *malware* tersebut menggunakan *web browser*.
7	Kasus ke-	6
	Judul kasus	Pembuatan Laporan
	Deskripsi Kasus	Setelah memastikan komputer telah terbebas dari *malware*, maka komputer perlu dikembalikan ke kondisi normal agar dapat digunakan sebagaimana harusnya. Koneksi internet dan fitur *file sharing* kembali diaktifkan. Selanjutnya anda memperoleh pelajaran dari insiden yang terjadi lalu membuat laporan insiden sebagai dokumentasi penanganan insiden yang telah dilakukan.
	Pertanyaan	Buat laporan yang menjabarkan penanganan insiden yang telah anda lakukan beserta hal-hal yang anda dapatkan selama kegiatan tersebut.
	Alat Bantu	*Template* laporan insiden
	Petunjuk	Buat laporan penanganan insiden menggunakan *template* yang telah disediakan. Cantumkan informasi yang telah anda peroleh dari pengerjaan kasus-kasus sebelumnya.

Studi Kasus telah diperbaiki berdasarkan saran-saran dari responden. Selanjutnya dokumen *Participants Handout* telah berhasil dibuat dan dapat digunakan sebagai bahan *Cyber Exercise*.

5. KESIMPULAN

Berdasarkan penelitian yang dilakukan, dapat diperoleh kesimpulan untuk menjawab rumusan masalah dalam penelitian ini, yaitu:

1. Hasil pembuatan lingkungan simulasi insiden berupa *file* OVA yang telah terinfeksi *malware* jenis *ransomware*. Lingkungan simulasi insiden dibuat berdasarkan hasil diskusi pada fase *Identifying* sehingga sesuai dengan kebutuhan pengelola TI Instansi XYZ. *File* OVA ini selanjutnya dapat digunakan pada kegiatan *Cyber Exercise* sebagai material pendukung/alat bantu dalam penanganan insiden *malware*.
2. Dokumen *Participants Handout* berisi gambaran umum *Cyber Exercise* dan studi kasus insiden yang disusun sesuai dengan tahapan penanganan insiden pada standar NIST SP 800-83r1. Setiap studi kasus terdiri dari deskripsi kasus, pertanyaan, keterangan material pendukung/alat bantu, dan petunjuk guna menjawab pertanyaan pada studi kasus tersebut. Dokumen *Participants Handout* ini selanjutnya dapat digunakan oleh pengelola TI Instansi XYZ sebagai panduan dalam kegiatan *Cyber Exercise*.
3. Untuk menambah wawasan dan kemampuan objek penelitian, dapat dilakukan penelitian lebih lanjut dengan menggunakan skenario insiden lain, membuat lingkungan simulasi insiden yang lebih nyata, serta melaksanakan fase *Conducting* dan *Evaluating.*

REFERENSI

[1] R. Sharp, "An Introduction to Malware," DTU, 2007.

[2] "Cybercrime tactics and techniques Q1 2019," Malwarebytes Labs, 2019.

[3] "2019 State of Malware," Malwarebytes Labs, 2019.

[4] B. Sangkaya, Interviewee, *Data Dukung Latar Belakang Penelitian Terkait Insiden Malware di Instansi XYZ.* [Wawancara]. 06 Juli 2020.

[5] G. M. Fairuz, *Kuesioner tentang Insiden Malware pada Mahasiswa Instansi XYZ,* 2019.

[6] P. Cichonski dan K. Scarfone, "NIST Special Publication 800-61r2 Computer Security Incident Handling Guide Recommendations," National Institute of Standards and Technology, Gaithersburg, 2012.

[7] "Creating a Computer Security Incident Response Team (CSIRT)," Carnegie Mellon University, Pitssburgh.

[8] BSSN, "BSSN Selenggarakan Cybersecurity Drill Test Sektor Pemerintah," Badan Siber dan Sandi Negara, 2019. [Online]. Available: https://bssn.go.id/bssn-selenggarakan-cybersecurity-drill-test-sektor-pemerintah/. [Diakses 2019 November 24].

[9] J. Kick, "Cyber Exercise Playbook," MITRE Corporation, Wlesbaden, 2014.

[10] M. K. A., Learning Malware Analysis, Birmingham: Packt Publishing, 2018.

[11] L. Johnson, Computer Incident Response and Forensics Team Management, Waltham: Elsevier, 2015.

[12] ENISA, "Good Practice Guide on National Exercises," 2009.

[13] M. Souppaya dan K. Scarfone, "NIST Special Publication 800-83 Guide to Malware Incident Prevention and Handling for Desktops and Laptops," National Institute of Standards and Technology, Gaithersburg, 2013.

[14] Hasherezade, "Github Petya Key," 26 Juli 2017. [Online]. Available:

https://github.com/hasherezade/petya_key. [Diakses Juli 2020].

[15] Hasherezade, "Malwarebytes LABS Bye-bye Petya!," Malwarebytes, 24 Juli 2017. [Online]. Available: https://blog.malwarebytes.com/malwarebytes-news/2017/07/bye-bye-petya-decryptor-old-versions-released/. [Diakses Juli 2020].

[16] BSSN, "Waspada Bahaya Serangan Ransomware "Petya" dan Tindakan Pencegahannya," BSSN, 28 Juni 2017. [Online]. Available: https://bssn.go.id/waspada-bahaya-serangan-ransomware-petya-dan-tindakan-pencegahannya/. [Diakses Juli 2020].

[17] BSSN, *The 2019 Critical Information Infrastructure Cyber Exercise: Malware Attack and Mitigation Strategy*, Jakarta, 2019.