PENILAIAN RISIKO SERANGAN SIBER PADA SISTEM MANAJEMEN KEAMANAN INFORMASI PT. UAV

RISK ASSESSMENT OF CYBER ATTACKS ON INFORMATION SECURITY MANAGEMENT SYSTEM OF PT. UAV

Tri Adianto[1], Yusuf Ali[2], Edy Saptono[3]

UNIVERSITAS PERTAHANAN
(tri.adianto3595@gmail.com, yusufali8788@gmail.com, edysptn@yahoo.com)

Abstrak – Serangan siber merupakan salah satu ancaman nyata yang muncul akibat perkembangan lingkungan strategis dunia yang semakin dinamis dan kompleks. Di Indonesia, serangan siber tidak hanya menyerang infrastruktur pemerintahan saja, namun juga menyerang infrastruktur kritis nasional lainnya, termasuk: PT. UAV yang merupakan salah satu industri pertahanan yang telah bekerjasama dengan Kementerian Pertahanan dan Tentara Nasional Indonesia dalam memproduksi Alat Peralatan Pertahanan dan Keamanan berupa Pesawat Terbang Tanpa Awak. Artikel ini ditulis dengan tujuan untuk mengidentifikasi, menganalisis dan mengevaluasi risiko serangan siber pada Sistem Manajemen Keamanan Informasi PT. UAV. Artikel ini ditulis berdasarkan hasil penelitian kualitatif dengan menggunakan desain penelitian studi kasus. Pada penelitian ini, proses pengumpulan data dilaksanakan dengan menggunakan metode wawancara, observasi dan studi dokumentasi. Data yang diperoleh kemudian dianalisis melalui tiga tahap, yaitu: kondensasi data, penyajian data dan penarikan kesimpulan/verifikasi. Hasil identifikasi risiko mengungkapkan bahwa terdapat 10 jenis risiko serangan siber yang dapat mengeksploitasi SMKI PT. UAV, yaitu: 1) risiko serangan siber terhadap perangkat keras berupa kegiatan *jamming* dan *network intrusion*, dan 2) risiko serangan siber terhadap perangkat lunak berupa serangan *Distributed Denial of Service*, *SQL injection*, *malware/virus*, *defacement*, *spam*, *worm Stuxnet, ransomware WannaCry* dan penyusupan siber. Setelah dianalisis lebih lanjut, dari kesepuluh risiko serangan siber tersebut ternyata terdapat dua jenis risiko serangan siber yang diperkirakan 'Mungkin Sekali' terjadi dan akan memberikan dampak 'Tinggi' pada aktifitas bisnis yang sedang digeluti oleh PT. UAV. Selain itu, juga ditemukan tiga jenis risiko serangan siber yang telah memiliki skala risiko '5'. Setelah dievaluasi, ketiga jenis risiko tersebut ditentukan sebagai prioritas utama dalam proses pengendalian risiko yang harus dilaksanakan oleh PT. UAV. Berdasarkan hasil temuan tersebut, maka peneliti merekomendasikan kepada manajerial PT. UAV untuk segera menyusun standard operasional prosedur dalam rangka untuk menangani risiko serangan siber yang telah dinilai pada penelitian ini.

Kata Kunci: Industri Pertahanan, Penilaian Risiko, Manajemen Pertahanan, Pertahanan Siber, Serangan Siber, Sistem Manajemen Keamanan Informasi.

[1] Program Studi Manajemen Pertahanan, Fakultas Manajemen Pertahanan, Universitas Pertahanan.
[2] Program Studi Doktoral, Fakultas Keamanan Nasional, Universitas Pertahanan.
[3] Program Studi Doktoral, Fakultas Teknologi Pertahanan, Universitas Pertahanan.

Abstract *– Cyber attack is one of the real threats posesed by dynamic and complex development of world strategic environment. In Indonesia, cyber attack does not only attack the government infrastructure, but also attack the other critical infrastructures, including: PT. UAV, as one of the defense industries that has collaborated with the Ministry of Defence and the Indonesian National Armed Forces in producing Unmanned Aerial Vehicle. This article is written to identify, to analyse and to evaluate the cyber attack risks on the Information Security Management System of PT. UAV. This article is written based on the results of qualitative research using case study research design. In the research, the data collection process was conducted using interviews, observation and documentation studies. Obtained data were analyzed through: data condensation, data display and drawing conclusions/verification. Risk identification results reveal that there are 10 types of cyber attack risk which can exploit the ISMS of PT. UAV, namely: 1) cyber attack risks on hardware, i.e.: jamming and network intrusion, and 2) cyber attack risks on software, i.e.: Distributed Denial of Service, SQL injection, malware/viruses, defacement, spam, worm Stuxnet, ransomware WannaCry and cyber espionage. After further analysis, it revealed that there are two types of cyber attack risk which are estimated to be 'Very Likely' occur and will have a 'High' impact on the business activities carried out by PT. UAV. In addition, it also revealed that there are three types of cyber attack risk which has a risk scale of '5'. After being evaluated, those three types of cyber attack risk are determined as the main risk priority in the risk control process which must be carried out by PT. UAV. Based on these findings, the researchers recommend managerial PT. The UAV to immediately develop a standard operating procedure in order to deal with the cyber attack risks which has assessed in this study.*

Keywords: *Cyber Attack, Cyber Defense, Defense Industry, Defense Management, Information Security System Management, Risk Assessment.*

Pendahuluan

Dinamika perkembangan lingkungan strategis dunia senantiasa menimbulkan spektrum ancaman yang semakin kompleks dan berimplikasi terhadap sistem pertahanan suatu negara, termasuk bagi Indonesia. Salah satu bentuk ancaman yang muncul sebagai akibat perkembangan lingkungan strategis tersebut adalah ancaman serangan siber. Ancaman ini telah terjadi di seluruh dunia dan terus mengalami peningkatan yang signifikan setiap tahunnya. Menurut Agung Nugraha, Plt Deputi Bidang Proteksi Badan Siber dan Sandi Nasional (BSSN), serangan siber ini tidak hanya berpusat pada serangan terhadap infrastruktur pemerintahan saja, namun juga dapat menyerang infrastruktur kritis lainnya, seperti: infrastruktur sektor energi dan sumber daya mineral, sumber daya air, hukum, keuangan dan perbankan, kesehatan, layanan darurat, pertanian, teknologi informasi dan komunikasi, transportasi, pertahanan dan industri strategis lainnya, termasuk sektor industri pertahanan[4].

[4] Sindonews, "BSSN Sebut Ada 10 Sektor yang Rentan Serangan Siber" dalam https://jatim.sindonews.com/read/8917/1/bssn-sebut-ada-10-sektor-yang-rentan-serangan-siber-1553644999.html, 27 Maret 2019, diakses pada 29 Juli 2019.

Pernyataan di atas dibuktikan oleh beberapa fakta terkait serangan siber yang pernah terjadi di Indonesia, seperti: serangan *ransomware WannaCry* yang terjadi pada sektor kesehatan, tepatnya pada Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais, pada tahun 2017 silam. Serangan ini terjadi pada seluruh komputer yang ada di kedua rumah sakit tersebut dan menyebabkan layanan medis terganggu karena komputer yang terinfeksi tidak dapat diakses dan digunakan untuk melayani keperluan pasien[5]. Selain itu, Badan Siber dan Sandi Negara dalam "Laporan Tahunan Honeynet Project BSSN – IHP tahun 2018" melaporkan bahwa Indonesia telah mengalami serangan siber sebanyak 12.895.554 kali selama tahun 2018[6]. Berdasarkan laporan tersebut, maka tidak menutup kemungkinan bahwa Indonesia akan mengalami serangan siber berskala besar dimasa depan. Serangan siber tersebut diperkirakan akan menyerang seluruh infrastruktur kritis nasional yang ada di Indonesia, termasuk industri pertahanan.

Industri pertahanan merupakan salah satu industri strategis yang berperan penting dalam memproduksi dan mengembangkan Alat Peralatan Pertahanan dan Keamanan (Alpalhankam) yang akan digunakan oleh Tentara Nasional Indonesia (TNI) untuk memperkuat sistem pertahanan negara Indonesia. Salah satu industri pertahanan yang dimaksud adalah PT. UAV yang telah bekerjasama dengan Kementerian Pertahanan (Kemhan) dan TNI dalam memproduksi Pesawat Terbang Tanpa Awak (PTTA) yang akan digunakan oleh TNI dalam operasi penginderaan jauh di wilayah perbatasan Indonesia–Malaysia.

Pada sektor industri PTTA, serangan siber pernah telah terjadi pada perusahaan *SZ DJI Technology Co., Ltd* yang merupakan salah satu perusahaan teknologi terbesar asal China yang mengembangkan dan memproduksi *drone* dengan spesifikasi umum dan militer. Serangan siber pada perusahaan DJI terjadi pada tahun 2017 silam. Serangan tersebut berupa kegiatan *cracking* yang memanfaatkan kode *debug* pengembangan *drone* yang

[5] Indriyatno Banyumurti, dkk, "*Kebijakan Cybersecurity dalam Perspektif Multistakeholder – Seri Literasi Digital*", (Jakarta: ICT Watch, 2018), hlm. 52-53.

[6] Badan Siber dan Sandi Nasional, "*Laporan Tahunan 2018 Honeynet Project BSSN – IHP*". (Jakarta, 2018), hlm. 10.

terdapat pada aplikasi *DJI Assistant* 2. Akibatnya, *drone* hasil produksi DJI dapat dikendalikan oleh *cracker* melalui *backdoor* aplikasi pengembangnya[7].

Berdasarkan berita yang disampaikan oleh Kilbride dan Xiao, proses *hacking drone* DJI ini juga dilakukan oleh *cracker* melalui pencurian *cookie* pengguna yang diposting di forum *drone*. *Cookie* tersebut kemudian diganti dengan token identifikasi milik *cracker* sehingga mereka dapat mengakses semua fitur aplikasi pengembang *drone* DJI, seperti: *DJI Mobile App*, *DJI Web Account*, dan *DJI FlightHub*. Melalui akses ini, *cracker* dapat mengakses *log* penerbangan, foto, dan video yang telah diambil oleh *drone* yang bersangkutan. Selain itu, *cracker* tersebut juga dapat mengakses semua informasi pribadi dan profil pengguna yang terhubung dengan aplikasi *drone* DJI[8]. Kondisi ini terjadi sebagai akibat lemahnya kesadaran perusahaan DJI terhadap kemungkinan terjadinya risiko serangan siber pada aplikasi pengembang *drone* yang telah mereka produksi. Kondisi ini tentunya sangat berbahaya dan merugikan, baik bagi perusahaan DJI, masyarakat maupun instansi-instansi lain yang telah menggunakan *drone* produksi DJI.

Untuk mengatasi risiko serangan siber seperti di atas, salah satu cara yang dapat dilakukan oleh industri pertahanan Indonesia adalah melalui penerapan manajemen risiko, khususnya konsep penilaian risiko serangan siber yang bertujuan untuk mengidentifikasi, menganalisis dan mengevaluasi risiko serangan siber yang dapat dihadapi oleh industri pertahanan terkait. Namun, penelitian tentang penilaian risiko serangan siber pada industri pertahanan di Indonesia masih sangat terbatas. Sebagian besar penelitian yang telah ada hanya membahas tentang penilaian risiko pada sistem manajemen keuangan atau keselamatan kerja karyawan. Sehingga hasil penelitian atau literatur yang dapat menjadi pedoman bagi industri pertahanan Indonesia dalam melaksanakan penilaian risiko serangan siber pada SMKI perusahaannya juga masih sangat terbatas.

---

[7] R. K. Nistanto, "Awas! Drone Kini Juga Jadi Sasaran Hacker", dalam https://tekno.kompas.com/read/2017/08/01/19130027/awas-drone-kini-juga-jadi-sasaran-hacker.html, 01 Agustus 2017, diakses pada 29 Juli 2019.

[8] J. Kilbride dan B. Xiao. "Chinese Drone Maker DJI Left Users at High Risk of Spying and Hacking Under Security Flaw", dalam https://www.abc.net.au/news/2018-11-14/dji-drones-were-exposed-to-security-flaw/10491150.html, 14 November 2018, diakses pada 29 Juli 2019.

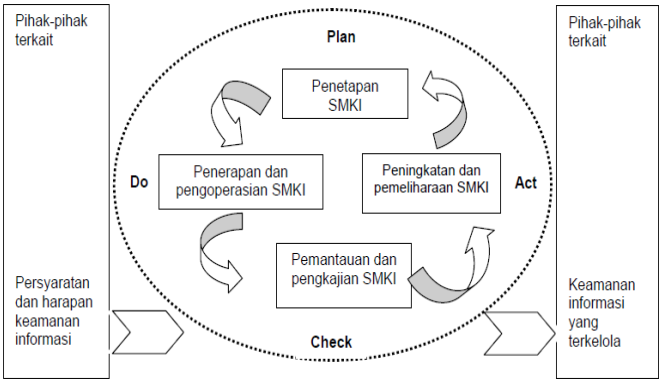
Apabila kondisi terus dibiarkan, maka hal ini tentunya akan berdampak pada berkurangnya kesadaran industri pertahanan, termasuk PT. UAV, tentang pentingnya proses penilaian risiko serangan siber sebagai salah satu upaya awal dalam menanggulangi risiko serangan siber yang dapat membahayakan aset informasi dan proses bisnis perusahaan. Berdasarkan uraian tersebut, maka peneliti telah melakukan penelitian tentang penilaian risiko serangan siber pada Sistem Manajemen Keamanan Informasi (SMKI) PT. UAV. Penelitian ini bertujuan untuk mengidentifikasi, menganalisis dan mengevaluasi risiko serangan siber yang dapat terjadi pada SMKI PT. UAV. Penelitian ini diharapkan dapat memberikan manfaat, baik bagi pemerintah, PT. UAV, masyarakat hingga para akademisi maupun peneliti yang tertarik untuk melaksanakan penelitian lebih lanjut tentang proses penilaian risiko serangan siber pada SMKI suatu instansi/perusahaan di Indonesia.

Konsep Sistem Manajemen Keamanan Informasi (SMKI) pertama kali dikembangkan oleh *International Organization for Standardization* (ISO) melalui pembuatan sejumlah standard tentang SMKI. Salah satu standard yang sering digunakan dalam mengelola SMKI adalah ISO/IEC 27001: 2013 *Information Technology – Security Techniques – Information Security Management Systems – Requirement*[9]. Di Indonesia, standard ini telah diadopsi oleh Badan Standardisasi Nasional (BSN) menjadi standard SNI ISO/IEC 27001: 2013. Pada standard tersebut, BSN mendefenisikan SMKI sebagai bagian dari sistem manajemen yang secara keseluruhan berdasarkan pendekatan risiko bisnis dilaksanakan untuk menetapkan, menerapkan dan mengoperasikan, memantau dan mengkaji, serta meningkatkan dan memelihara keamanan informasi[10].

Pada dasarnya, standard ini mengadopsi model *Plan-Do-Check-Act* (PDCA) yang diterapkan untuk membentuk seluruh proses SMKI seperti diilustrasikan pada gambar berikut:

[9] International Organization for Standardization, *ISO 27001: 2013 Information Technology – Security Techniques – Information Security Risk Management Systems – Requirements*. (Switzerland, 2013).

[10] Badan Standardisasi Nasional, *Standar SNI ISO/IEC 27001:2013 Teknologi Informasi – Teknik Keamanan – Sistem Manajemen Keamanan Informasi – Persyaratan*, (Jakarta, 2013), hlm. 3.



Gambar 1. Model PDCA pada Penerapan SMKI di Indonesia
Sumber: *International Organization for Standardization*, 2013

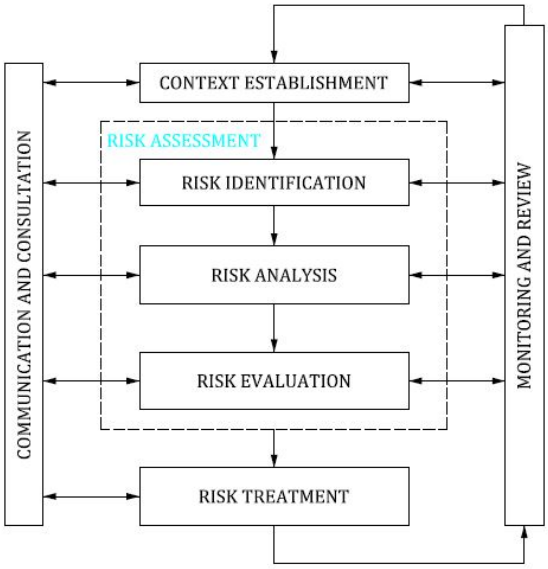
Badan Standardisasi Nasional menjelaskan:

1. Tahap *Plan* (Penetapan SMKI) dilaksanakan melalui kegiatan penetapan kebijakan, sasaran, proses dan prosedur SMKI yang sesuai untuk mengelola risiko dan memperbaiki keamanan informasi agar menghasilkan hasil yang sesuai dengan kebijakan dan sasaran organisasi secara keseluruhan.
2. Tahap *Do* (Penerapan dan Pengoperasian SMKI) dilaksanakan melalui penerapan dan pengoperasian kebijakan, pengendalian, proses dan prosedur SMKI yang telah direncanakan sebelumnya.
3. Tahap *Check* (Pemantauan dan Pengkajian SMKI) dilaksanakan dengan cara mengakses dan mengukur kinerja proses terhadap kebijakan, sasaran dan pengalaman praktis yang terjadi sebelum kemudian dilaporkan hasilnya kepada pihak manajemen atas untuk dikaji lebih lanjut.
4. Tahap *Act* (Peningkatan dan Pemeliharaan SMKI) diselenggarakan dalam bentuk pengambilan tindakan korektif dan pencegahan berdasarkan hasil internal audit SMKI dan hasil tinjauan manajemen dalam rangka untuk mencapai perbaikan yang berkesinambungan dalam SMKI yang telah terbentuk.

Penerapan model PDCA ini dilselenggarakan dalam seluruh proses pengamanan informasi dalam rangka untuk melindungi keamanan aset informasi dan citra organisasi dari berbagai insiden yang merugikan, misalnya gangguan atau kegiatan hacking pada suatu organisasi[11].

[11] Badan Standardisasi Nasional, *Standar SNI ISO/IEC 27001:2013 Teknologi Informasi – Teknik Keamanan – Sistem Manajemen Keamanan Informasi – Persyaratan*, (Jakarta, 2013), hlm. v.

Proses penilaian risiko pada SMKI diuraikan lebih lanjut dalam standard ISO/IEC 27005: 2018 – *Information Technology – Security Techniques – Information Security Risk Management.* Standard ini memuat gambaran seluruh proses manajemen risiko keamanan informasi beserta kegiatan-kegiatan didalamnya. Proses manajemen risiko berdasarkan standard ini dapat diilustrasikan sebagai berikut[12]:



Gambar 2. Proses Manajemen Risiko berdasarkan ISO/IEC 27005:2018
Sumber: *International Organization for Standardization*, 2018

Berdasarkan Gambar 2 di atas dapat diketahui bahwa proses penilaian risiko (*Risk Assessment*) pada standard ISO/IEC 27005: 2018 meliputi tiga tahapan, yaitu:

1. *Risk Identification*

Risk identification (identifikasi risiko) merupakan proses untuk menemukan, menginventarisir dan menggolongkan unsur risiko. Proses ini bertujuan untuk menentukan risiko apa yang dapat menyebabkan kerugian bagi perusahaan sekaligus untuk mendapatkan informasi tentang bagaimana, dimana dan mengapa kerugian tersebut dapat terjadi. Proses identifikasi risiko pda tahap ini dapat dilaksanakan melalui kegiatan: 1) identifikasi aset, 2) identifikasi ancaman, 3) identifikasi kontrol yang ada, 4) identifikasi kelemahan dan 5) identifikasi dampak dari hilangnya kerahasiaan, keutuhan dan ketersediaan suatu informasi yang tersimpan dalam SMKI[13].

2. *Risk Analysis*

Risk Analysis (analisis risiko) merupakan proses penggunaan informasi secara sistematik untuk mengidentifikasi dan memperkirakan risiko. Proses ini dilaksanakan dengan cara menganalisis kemungkinan terjadinya skenario kegagalan

[12] International Organization for Standardization, *ISO 27005: 2018 Information Technology – Security Techniques – Information Security Risk Management*, (Switzerland, 2018), hlm. 3.

[13] International Organization for Standardization, *ISO 27005: 2018 Information Technology – Security Techniques – Information Security Risk Management*, (Switzerland, 2018), hlm. 13

pengamanan informasi beserta konsekuensi yang akan diterima akibat hilangnya kerahasiaan, keutuhan dan ketersediaan dari aset informasi yang tersimpan[14].

3. *Risk Evaluation*

Risk Evaluation (evaluasi risiko) merupakan proses membandingkan risiko yang diperkirakan terhadap kriteria evaluasi risiko yang telah ditetapkan untuk menentukan level dan prioritas risiko. Proses ini dilaksanakan menggunakan data yang diperoleh dari hasil analisis risiko dengan maksud untuk membuat keputusan yang tepat tentang tindakan pengendalian risiko yang akan dilaksanakan di masa depan[15].

Ketiga tahapan dalam proses penilaian risiko di atas digunakan sebagai landasan dalam melaksanakan penilaian risiko serangan siber pada penelitian ini. Serangan siber atau kejahatan siber sendiri dapat didefenisikan sebagai segala upaya penggunaan jaringan komputer untuk tujuan kriminal melalui penyalahgunaan teknologi digital[16]. Serangan siber ini merupakan kegiatan yang memanfaatkan komputer sebagai media yang didukung oleh sistem telekomunikasi, baik itu *dial up system*, menggunakan jalur telepon, ataukah *wireless system* yang menggunakan antena khusus yang nirkabel[17]. Pada dasarnya, serangan siber ini dilakukan oleh individu, organisasi khusus, institusi resmi, atau suatu negara dengan tujuan untuk mencuri, merusak atau memanipulasi data yang terdapat pada jaringan sistem informasi atau perangkat digital yang dapat menjadi sarana komunikasi di dunia maya[18].

Pendapat di atas didukung oleh pernyataan Kementerian Pertahanan Republik Indonesia dalam Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber yang menjelaskan secara rinci bahwa:

---

[14] International Organization for Standardization, *ISO 27005: 2018 Information Technology – Security Techniques – Information Security Risk Management*, (Switzerland, 2018), hlm. 17.

[15] International Organization for Standardization, *ISO 27005: 2018 Information Technology – Security Techniques – Information Security Risk Management*, (Switzerland, 2018), hlm. 20.

[16] Abdul Wahid dan Mohammad Labib. *Kejahatan Mayantara (Cyber Crime)*. (Jakarta: PT. Refika Aditama, 2005).

[17] Maskun, *Kejahatan Siber (Cyber Crime): Suatu Pengantar*, (Jakarta: Kencana, Prenada Media Grup, 2013).

[18] Scoot W. Beidleman, *Defining and Deterring Cyber War*, (U.A. Army War College, Carlisle Barracks, 2009).

> "*Serangan siber merupakan segala bentuk perbuatan, perkataan, pemikiran baik yang dilakukan dengan sengaja maupun tidak sengaja oleh pihak mana pun, dengan motif dan tujuan apa pun, yang dilakukan di lokasi mana pun, yang disasarkan pada sistem elektronik atau muatannya (informasi) maupun peralatan yang sangat bergantung pada teknologi dan jaringan dalam skala apa pun, terhadap obyek vital maupun nonvital dalam lingkup militer dan nonmiliter, yang mengancam kedaulatan negara, keutuhan wilayah dan keselamatan bangsa*"[19].

Serangan siber ini disinyalir dapat mengakibatkan terjadinya perang siber dan gangguan siber yang akan mengganggu keamanan nasional hingga kedaulatan suatu negara.

Menurut Mcdonnell dan Sayers, sebagaimana dikutip oleh Kementerian Pertahanan Republik Indonesia dalam buku "Pedoman Pertahanan Siber", ancaman serangan siber dapat dikategorikan sebagai berikut[20]:

1. Ancaman Perangkat Keras (*Hardware Threat*), yaitu ancaman yang disebabkan oleh pemasangan peralatan tertentu yang berfungsi untuk melakukan kegiatan tertentu dalam suatu sistem, sehingga peralatan tersebut merupakan gangguan terhadap sistem Jaringan dan Perangkat Keras lainnya. Ancaman ini dapat berupa:
   a. kegiatan *jamming*, dan
   b. *network intrusion*.
2. Ancaman Perangkat Lunak (*Software Threat*), yaitu ancaman yang disebabkan oleh masuknya *software* tertentu yang berfungsi untuk melakukan berbagai kegiatan, seperti: pencurian informasi, perusakan informasi atau sistem, manipulasi informasi dan lain sebagainya. Ancaman ini dapat berupa[21]:

[19] Kementerian Pertahanan Republik Indonesia, *Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber*, (Jakarta, 2014) hlm. 5.

[20] Kementerian Pertahanan Republik Indonesia, *Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber*, (Jakarta, 2014) hlm. 12.

[21] Kementerian Pertahanan Republik Indonesia, *Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber*, (Jakarta, 2014) hlm. 7-11.

a. serangan *advanced persistent threats* (APT),
b. serangan *denial of service* (DoS),
c. serangan *distributed denial of service* (DDoS),
d. serangan *defacement*,
e. serangan *phishing*,
f. serangan *malware/virus*,
g. penyusupan siber,
h. serangan *spam*, dan
i. serangan *spoofing*.

3. Ancaman Data atau Informasi (*Data or Information Threat*), yaitu ancaman yang diakibatkan oleh penyebaran data atau informasi tertentu dengan tujuan untuk kepentingan tertentu. Ancaman ini dapat berupa[22]:
   a. kegiatan *interruption*,
   b. kegiatan *interception*,
   c. kegiatan *modification*, dan
   d. kegiatan *fabrication*.

Seluruh ancaman siber yang diuraikan di atas disinyalir dapat mengancam aset yang dimiliki oleh suatu negara/ instansi/perusahaan yang ada di dunia, khususnya yang tersimpan dalam SMKI.

Metode Penelitian

Artikel ini ditulis berdasarkan hasil penelitian kualitatif dengan menggunakan pendekatan studi kasus yang merupakan sebuah penyelidikan empiris yang dilakukan untuk menginvestigasi fenomena kontemporer dalam konteks kehidupan nyata ketika batas antara fenomena dan konteks tidak begitu jelas[23]. Pada artikel ini, peneliti menggunakan jenis penelitian studi kasus tunggal, dimana kasus yang akan diteliti hanya ada satu, yaitu tentang penilaian risiko serangan siber pada SMKI PT. UAV. Proses pengumpulan data pada penelitian ini dilaksanakan dengan menggunakan metode wawancara, observasi dan studi dokumentasi.

Selanjutnya, data yang diperoleh di uji keabsahannya dengan menggunakan metode triangulasi sumber. Metode ini dilakukan dengan cara membandingkan dan mengecek kembali derajat kepercayaan dari suatu data atau informasi yang diperoleh dengan cara membandingkan data hasil wawancara dengan data hasil observasi dan studi dokumentasi terkait dengan isu yang

[22] D. Ariyus, *Pengantar Ilmu Kriptografi: Teori, Analisis dan Implementasi*, (Yogyakarta: Penerbit Andi, 2008).

[23] Robert K. Yin, *Studi Kasus: Desain & Metode*, (Jakarta: Rajagrafindo Persada, 2011).

relevan dengan topik penelitian[24]. Selanjutnya, data hasil penelitian tersebut dianalisis dengan menggunakan teknik analisis data kualitatif, yaitu: kondensasi data, penyajian data dan penarikan kesimpulan atau verifikasi[25].

Hasil dan Pembahasan

Pada artikel ini, penilaian risiko serangan siber pada SMKI PT. UAV dilaksanakan melalui tiga tahapan, yaitu: 1) identifikasi risiko, 2) analisis risiko dan 3) evaluasi risiko. Secara lebih rinci ketiga tahap penilaian risiko serangan siber tersebut dapat diuraikan sebagai berikut:

1. Identifikasi Risiko

Kegiatan identifikasi risiko serangan siber pada artikel ini dilakukan untuk menemukan, menginventarisir dan menggolongkan unsur risiko yang dapat menyebabkan kerugian bagi perusahaan, sekaligus untuk mendapatkan informasi tentang bagaimana, dimana dan mengapa kerugian tersebut dapat terjadi. Proses identifikasi risiko pada penelitian ini dilaksanakan melalui beberapa kegiatan sebagai berikut:

a. Identifikasi Aset

Proses identifikasi aset pada penelitian ini dilaksanakan dengan cara mendaftar seluruh aset yang dimiliki oleh PT. UAV dalam ruang lingkup SMKI yang diterapkannya. Aset-aset tersebut kemudian diidentifikasi dan digolongkan ke dalam dua kategori aset, yaitu: aset utama yang tersimpan dalam SMKI dan aset pendukung kinerja SMKI. Kegiatan ini menghasilkan sebuah daftar yang menunjukkan seluruh aset yang dimiliki oleh perusahaan seperti berikut:

Tabel 1. Daftar Aset Utama dan Aset Pendukung SMKI PT. UAV terkait Risiko Serangan Siber

No	Jenis Aset	Kode Aset	Keterangan Aset
Aset Utama			
1	Data dan Informasi	A–01	Data Rancangan/ Desain Produk Perusahaan
		A–02	Data Hasil Penginderaan
Aset Pendukung			
2	Perangkat keras	A–03	Komputer Server
		A–04	Komputer Klien
		A–05	Perangkat Keras Jaringan Komputer

[24] Lexy J. Moleong, *Metodologi Penelitian Kualitatif (Edisi Revisi*), (Bandung: PT. Remaja Rosdakarya, 2017).

[25] Matthew B. Miles, A. Michael Huberman; dan J. Saldaña, *Qualitative Data Analysis: A Methods Sourcebook, 3rd Edition*, (United States of America: SAGE Publications Inc, 2014).

3	Perangkat Lunak	A–06	Sistem Operasi
		A–07	*Microsoft Office*
		A–08	Aplikasi Desain Produk
		A–09	*Website* Perusahaan
		A–10	Aplikasi *E-mail*

Sumber: Diolah oleh Peneliti, 2019

b. Identifikasi Ancaman

Proses identifikasi ancaman pada penelitian ini dilaksanakan dengan cara mendaftar seluruh jenis ancaman serangan siber yang dapat terjadi pada SMKI PT. UAV, baik ancaman yang berasal dari internal maupun eksternal perusahaan. Kegiatan ini menghasilkan sebuah daftar ancaman serangan siber yang diperkirakan dapat mengeksploitasi SMKI PT. UAV seperti berikut:

Tabel 2. Daftar Risiko Serangan Siber yang Dapat Mengeksploitasi SMKI PT. UAV

No	Jenis Risiko	Kode Ancaman	Keterangan Risiko
1	Ancaman Perangkat Keras	T–01	Kegiatan *Jamming*
		T–02	*Network Intrusion*
2	Ancaman Perangkat Lunak	T–03	Serangan *Distributed Denial of Service* (DDoS)
		T–04	Serangan *SQL Injection*
		T–05	Serangan *Malware/Virus*
		T–06	Serangan *Defacement*
		T–07	Serangan *Spam*
		T–08	Penyusupan Siber
		T–09	Serangan *Worm Stuxnet*
		T–10	Serangan *Ransomware WannaCry*

Sumber: Diolah oleh Peneliti, 2019

c. Identifikasi Kontrol yang Telah Ada

Proses identifikasi kontrol yang telah ada pada penelitian ini dilaksanakan dengan cara mewawancarai pihak yang berwenang dalam menerapkan manajemen risiko di perusahaan. Berdasarkan hasil wawancara dengan narasumber terkait, diketahui bahwa manajemen risiko yang telah diterapkan oleh PT. UAV merupakan kebijakan pimpinan perusahaan yang secara umum baru membahas tentang manajemen risiko keselamatan kerja, anggaran dan keamanan sistem informasi. Hingga penelitian ini selesai dilaksanakan, belum ada penjabaran lebih lanjut terkait manajemen risiko serangan siber pada perusahaan tersebut. Kondisi ini dapat dimaklumi dikarenakan hingga saat ini masih belum ada aturan maupun pedoman khusus, baik yang diterbitkan oleh Kementerian Pertahanan maupun Badan Standardisasi Nasional terkait pedoman manajemen risiko serangan siber yang dapat diterapkan oleh seluruh perusahaan yang ada di Indonesia.

d. Identifikasi Kerentanan

Proses identifikasi kerentanan pada penelitian ini dilaksanakan dalam rangka untuk mengetahui seluruh kerentanan yang dimiliki oleh SMKI perusahaan.

Kegiatan identifikasi kerentanan ini dilaksanakan dengan cara mendaftar seluruh kerentanan sistem yang mungkin dieksploitasi oleh ancaman yang telah teridentifikasi pada kegiatan sebelumnya. Kerentanan yang dimaksud dapat ditinjau dari segi organisasi, personel, lokasi, perangkat keras, hingga perangkat lunak. Proses identifikasi ini menghasilkan sebuah daftar kerentanan yang dimiliki oleh SMKI perusahaan.

e. Identifikasi Dampak

Proses identifikasi dampak pada penelitian ini dilakukan dengan cara mengidentifikasi konsekuensi atau kerugian yang akan dialami oleh perusahaan akibat hilangnya kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) dari suatu data atau informasi. Hasil identifikasi dampak ini selanjutnya akan diuraikan pada tahap analisis risiko sebagai bahan pertimbangan dalam membuat kebijakan terkait proses pengamanan informasi oleh pihak perusahaan.

Selanjutnya, berdasarkan data hasil identifikasi risiko yang telah diuraikan di atas, maka peneliti membuat sebuah skenario risiko serangan siber yang dapat terjadi pada SMKI PT. UAV sebagai berikut:

Tabel 3. Skrenario Risiko Serangan Siber yang Dapat Terjadi pada SMKI PT. UAV

Kode Aset	Kode Ancaman	Keterangan Risiko
A–01	T–05	Serangan *Malware/Virus*
	T–09	Serangan *Worm Stuxnet*
	T–10	Serangan *Ransomware WannaCry*
A–02	T–05	Serangan *Malware/Virus*
	T–09	Serangan *Worm Stuxnet*
	T–10	Serangan *Ransomware WannaCry*
A–03	T–01	Kegiatan *Jamming*
	T–02	*Network Intrusion*
A–04	T–01	Kegiatan *Jamming*
	T–02	*Network Intrusion*
A–05	T–01	Kegiatan *Jamming*
	T–02	*Network Intrusion*
	T–03	Serangan *Distributed Denial of Service* (DDoS)
	T–08	Penyusupan Siber
A–06	T–05	Serangan *Malware/Virus*
	T–09	Serangan *Worm Stuxnet*
	T–10	Serangan *Ransomware WannaCry*
A–07	T–05	Serangan *Malware/Virus*
	T–09	Serangan *Worm Stuxnet*
	T–10	Serangan *Ransomware WannaCry*
A–08	T–05	Serangan *Malware/Virus*
A–09	T–04	Serangan *SQL Injection*
	T–06	Serangan *Defacement*
	T–08	Penyusupan Siber
A–10	T–07	Serangan *Spam*
	T–08	Penyusupan Siber

Sumber: Diolah oleh Peneliti, 2019

2. Analisis Risiko

Kegiatan analisis risiko pada artikel ini, dilaksanakan dilaksanakan dengan cara:

1) **Menganalisis tingkat kemungkinan terjadinya risiko** akibat kegagalan pengamanan informasi yang

dilakukan oleh perusahaan. Proses analisis ini dilaksanakan dengan cara mengestimasi peluang terjadinya risiko serangan siber pada SMKI perusahaan dalam kurun waktu satu tahun. Proses estimasi tersebut didasarkan pada pedoman berikut:

Tabel 4. Pedoman Penilaian Kemungkinan Terjadinya Risiko

Kemungkinan Risiko	Nilai Risiko	Keterangan
Sangat Tidak Mungkin	1	Ancaman hampir tidak pernah terjadi
Tidak Mungkin	2	Frekuensi terjadinya risiko jarang (sekitar 1–5 kali/semester)
Mungkin	3	Frekuensi terjadinya risiko cukup sering (sekitar 6–10 kali/semester)
Mungkin Sekali	4	Frekuensi terjadinya risiko sering (sekitar 10–20 kali/semester)
Sering	5	Frekuensi terjadinya risiko sangat sering (sekitar >20 kali/semester)

Sumber: Diolah oleh Peneliti, 2019

2) **Menganalisis dampak yang akan diterima** oleh perusahaan akibat kegagalan pengamanan informasi yang dilakukan oleh perusahaan. Proses analisis ini dilaksanakan dengan cara mengestimasi tingkat dampak yang akan diterima perusahaan akibat terjadinya serangan siber dalam kurun waktu satu tahun. Proses estimasi ini didasarkan pada pedoman berikut:

Tabel 5. Pedoman Penilaian Dampak Terjadinya Risiko

Dampak Risiko	Nilai Risiko	Keterangan
Sangat Rendah	1	Dampak yang ditimbulkan tidak signifikan dan tidak mengganggu SMKI perusahaan.
Rendah	2	Dampak yang ditimbulkan memberikan gangguan kecil terhadap layanan SMKI perusahaan.
Sedang	3	Dampak yang ditimbulkan memberikan gangguan sedang terhadap layanan SMKI perusahaan.
Tinggi	4	Dampak yang ditimbulkan memberikan gangguan besar pada SMKI perusahaan.
Sangat Tinggi	5	Dampak yang ditimbulkan sangat krusial dan mengganggu layanan utama pada SMKI perusahaan.

Sumber: Diolah oleh Peneliti, 2019

3) **Menentukan skala dari setiap risiko** yang dapat terjadi dan berdampak terhadap bisnis perusahaan. Proses penentuan skala risiko ini dilakukan dengan cara mengkombinasikan tingkat kemungkinan dan dampak terjadinya risiko berdasarkan matriks analisis risiko berikut:

Tabel 6. Matriks Analisis Risiko

Matriks Analisis Risiko			Kemungkinan Terjadinya Insiden				
			1	2	3	4	5
			Sangat Tidak Mungkin	Tidak Mungkin	Mungkin	Mungkin Sekali	Sering
Dampak Bisnis	1	Sangat Rendah	0	1	2	3	4
	2	Rendah	1	2	3	4	5
	3	Sedang	2	3	4	5	6
	4	Tinggi	3	4	5	6	7
	5	Sangat Tinggi	4	5	6	7	8

Sumber: *International Organization for Standardization*, 2018

Berdasarkan tiga ketentuan yang telah ditetapkan di atas, maka hasil analisis risiko serangan siber pada penelitian ini dapat disajikan pada tabel berikut:

Tabel 7. Hasil Analisis Risiko Serangan Siber pada SMKI PT. UAV

No	Jenis Risiko	Kemungkinan Risiko	Dampak Risiko	Skala Risiko
1	Kegiatan *Jamming*	2	1	1
2	*Network Intrusion*	3	2	3
3	Serangan *Distributed Denial of Service* (DDoS)	3	2	3
4	Serangan *SQL Injection*	3	3	4
5	Serangan *Malware/Virus*	4	3	5
6	Serangan *Defacement*	3	1	2
7	Serangan *Spam*	4	2	4
8	Penyusupan Siber	3	1	2
9	Serangan *Worm Stuxnet*	3	4	5
10	Serangan *Ransomware WannaCry*	3	4	5

Sumber: Diolah oleh Peneliti, 2019

3. Evaluasi Risiko

Proses evaluasi risiko pada artikel ini dilaksanakan dengan cara menentukan level risiko dan prioritas risiko. Proses penentuan level risiko dilaksanakan sesuai estimasi risiko berdasarkan probabilitas terjadinya suatu insiden akibat risiko serangan siber yang telah teridentifikasi sebelumnya. Proses penentuan level risiko ini mengacu pada matriks evaluasi risiko berikut:

Tabel 8. Matriks Evaluasi Risiko

Level Risiko	Skala Risiko
Rendah	0 – 2
Sedang	3 – 5
Tinggi	6 – 8

Sumber: *International Organization for Standardization*, 2018

Berdasarkan ketentuan di atas, maka hasil evaluasi risiko pada penelitian ini dapat disajikan pada tabel berikut:

Tabel 9. Hasil Evaluasi Risiko Serangan Siber yang Dapat Terjadi pada SMKI PT. UAV

Level Risiko	Skala Risiko	Risiko
Rendah	1	Kegiatan *Jamming*
	2	Serangan *Defacement*
	2	Penyusupan Siber
Sedang	3	*Network Intrusion*
	3	Serangan *Distributed Denial of Service* (DDoS)
	4	Serangan *SQL Injection*
	4	Serangan *Spam*
	5	Serangan *Malware/Virus*
	5	Serangan *Worm Stuxnet*
	5	Serangan *Ransomware WannaCry*

Sumber: Diolah oleh Peneliti, 2019

Selanjutnya, proses penentuan prioritas risiko pada penelitian ini dilaksanakan berdasarkan beberapa ketentuan berikut:

1) Skala risiko tertinggi mendapat prioritas paling tinggi.
2) Apabila terdapat lebih dari satu risiko yang memiliki skala risiko yang sama, maka prioritas risiko ditentukan berdasarkan urutan kemungkinan terjadinya risiko dari tertinggi hingga terendah.
3) Apabila masih terdapat lebih dari satu risiko yang memiliki skala dan kemungkinan yang sama, maka prioritas risiko ditentukan berdasarkan urutan dampak terjadinya risiko dari yang tertinggi hingga terendah.
4) Apabila masih terdapat lebih dari satu risiko yang memiliki skala, kemungkinan dan dampak yang sama, maka prioritas risiko ditentukan berdasarkan *judgement* dari pemilik perusahaan atau pihak yang berkepentingan dalam mengelola risiko tersebut.

Berdasarkan ketentuan yang telah diuraikan di atas, maka hasil penentuan prioritas risiko pada penelitian ini dapat disajikan pada tabel berikut:

Tabel 10. Hasil Penentuan Prioritas Risiko Serangan Siber pada SMKI PT. UAV

Prioritas Risiko	Skala Risiko	Kemungkinan Risiko	Dampak Risiko	Risiko
1	5	4	3	Serangan *Malware/Virus*
2	5	3	4	Serangan *Worm Stuxnet*
	5	3	4	Serangan *Ransomware WannaCry*
3	4	3	3	Serangan *SQL Injection*
4	4	4	2	Serangan *Spam*
5	3	3	2	*Network Intrusion*
	3	3	2	Serangan *Distributed Denial of Service* (DDoS)
6	2	3	1	Serangan *Defacement*
	2	3	1	Penyusupan Siber
7	1	2	1	Kegiatan *Jamming*

Sumber: Diolah oleh Peneliti, 2019

Berdasarkan hasil penentuan prioritas risiko serangan siber yang disajikan pada Tabel 9 di atas, diketahui bahwa risiko serangan *malware/virus* merupakan prioritas pertama yang harus segera ditangani oleh pihak manajerial PT. UAV. Hal ini dikarenakan risiko serangan *malware/virus* pada penelitian ini telah memiliki skala risiko '5' dan disinyalir 'mungkin sekali' terjadi, serta akan memberikan dampak yang 'sedang' terhadap kinerja SMKI PT. UAV. Selain itu, penentuan risiko serangan *malware/virus* sebagai prioritas pertama juga didasarkan pada pertimbangan hasil temuan tim BSSN yang menunjukkan bahwa serangan *malware* merupakan

salah satu serangan siber terbesar dan sering terjadi di Indonesia pada tahun 2018 dengan total serangan berjumlah 513.863 serangan[26]. Sehingga perlu segera dilakukan beberapa tindakan pengelolaan risiko yang diharapkan dapat meminimalisir atau bahkan mengurangi nilai skala risiko tersebut.

Selanjutnya, prioritas pengendalian risiko yang kedua adalah serangan *worm Stuxnet* dan *ransomware WannaCry*. Kedua risiko ini harus dipertimbangkan karena selain memiliki skala risiko '5', kedua serangan siber tersebut disinyalir akan memberikan dampak yang 'tinggi' terhadap proses bisnis yang sedang digeluti oleh PT. UAV. Selain itu, penentuan prioritas ini juga didasarkan pada hasil temuan Farwell dan Rohozinski yang menunjukkan bahwa serangan *worm Stuxnet* merupakan serangan yang sangat berbahaya dan telah mengeksploitasi lebih dari 60.000 komputer yang ada di dunia, diantaranya komputer yang ada di Amerika Serikat, Australia, Azerbaijan, China, Finlandia, India, Inggris, Iran, Jeman, Korea Selatan, Malaysia, dan Indonesia[27]. Sedangkan untuk *ransomware WannaCry*, hasil temuan Akbanov, dkk, mengungkapkan bahwa serangan *ransomware WannaCry* telah berhasil mengekploitasi lebih dari 300.000 komputer yang digunakan di 150 negara, baik pada sektor kesehatan, pemerintahan, telekomunikasi, hingga sektor produksi minyak dan gas[28].

Berdasarkan uraian tersebut, peneliti menganggap bahwa ketiga risiko serangan siber di atas harus menjadi prioritas utama dalam proses pengendalian risiko yang akan dilaksanakan oleh PT. UAV. Hal ini dikarenakan ketiga risiko serangan siber tersebut telah memiliki skala risiko '5' yang berarti tidak menutup kemungkinan bahwa tahun depan skala risiko dari ketiga serangan siber tersebut dapat berubah menjadi skala '6' atau menjadi risiko berlevel tinggi apabila tidak segera dikelola dengan baik. Selanjutnya pengendalian risiko dapat dilaksanakan sesuai prioritas risiko yang telah dijabarkan pada Tabel 9 di atas.

---

[26] Badan Siber dan Sandi Nasional, "*Laporan Tahunan 2018 Honeynet Project BSSN – IHP*". (Jakarta, 2018), hlm. 10.

[27] James P. Farwell dan Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival*, Vol. 53, No. 1, 2011, hlm. 23-40.

[28] Maxat Akbanov, Vassilios G. Vassilakis dan Michael D. Logothetis, "WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms". *Journal of Telecommunications and Information Technology*, Vol. 1, No. 1, 2019, hlm. 113-124.

Kesimpulan dan Rekomendasi

Pada penelitian ini telah dilaksanakan proses penilaian risiko serangan siber pada SMKI PT. UAV. Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan di atas, maka dapat disimpulkan bahwa:

1. Identifikasi risiko serangan siber telah dilaksanakan melalui kegiatan: identifikasi aset, identifikasi ancaman, identifikasi kontrol yang telah ada, identifikasi kelemahan dan identifikasi dampak dari suatu risiko terhadap SMKI PT. UAV. Hasil identifikasi risiko menunjukkan bahwa terdapat 10 jenis risiko serangan siber yang dapat menyerang SMKI PT. UAV. Berdasarkan jenisnya, risiko serangan siber tersebut dapat digolongkan menjadi dua, yaitu: 1) risiko serangan siber terhadap perangkat keras, yaitu: kegiatan *jamming* dan *network intrusion*, dan 2) risiko serangan siber terhadap perangkat lunak, yaitu: serangan *Distributed Denial of Service* (DDoS), SQL *injection*, *malware/virus*, *defacement*, *spam*, *worm Stuxnet*, *ransomware WannaCry*. dan penyusupan siber.
2. Analisis risiko serangan siber telah dilaksanakan melalui kegiatan: analisis kemungkinan terjadinya risiko, analisis dampak yang akan diterima dan analisis skala risiko. Hasil analisis risiko menunjukkan bahwa terdapat dua jenis risiko serangan siber yang 'Mungkin Sekali' terjadi, yaitu: risiko serangan *malware/virus* dan *spam*. Selanjutnya, terdapat dua jenis risiko serangan siber yang diperkirakan akan memberikan dampak 'Tinggi' pada aktifitas bisnis yang sedang dilaksanakan oleh PT. UAV, yaitu: serangan *worm Stuxnet* dan *ransomware WannaCry*. Selain itu juga terdapat tiga jenis risiko serangan siber yang telah memiliki skala risiko '5', yaitu: serangan *malware/virus*, *worm Stuxnet* dan *ransomware WannaCry*.
3. Evaluasi risiko serangan siber telah dilaksanakan melalui kegiatan: penentuan level risiko dan penentuan prioritas risiko. Hasil penentuan level risiko menunjukkan bahwa terdapat 3 jenis risiko serangan siber yang berlevel 'Rendah' dan 7 jenis risiko serangan siber yang berlevel 'Sedang'. Selanjutnya, hasil penentuan

prioritas pengendalian risiko menunjukkan bahwa risiko serangan *malware/virus*, *worm Stuxnet* dan *ransomware WannaCry* merupakan risiko yang harus menjadi prioritas utama dalam proses pengendalian risiko oleh PT. UAV. Selanjutnya proses pengendalian risiko dapat dilaksanakan sesuai urutan prioritas pengendalian risiko yang telah ditentukan, yaitu pada serangan SQL *injection*, *spam*, *network intrusion*, *distributed Denial of Service* (DDoS), *defacement*, penyusupan siber, dan kegiatan *jamming*.

Berdasarkan hasil penelitian dan pembahasan, serta kesimpulan yang telah di uraikan di atas, maka peneliti merekomendasikan:

1. PT. UAV disarankan untuk segera melaksanakan penilaian risiko secara lebih mendalam terhadap seluruh risiko serangan siber yang disinyalir akan sangat berbahaya bagi PT. UAV di masa depan, yaitu: risiko serangan *malware/virus*, *spam*, *worm Stuxnet* dan *ransomware WannaCry*. Penilaian risiko ini diharapkan dapat membantu manajerial PT. UAV dalam memahami lebih lanjut tentang kemungkinan dan dampak yang dapat disebabkan oleh seluruh risiko serangan siber tersebut terhadap kinerja SMKI maupun bisnis yang sedang digeluti oleh PT. UAV di masa depan. Namun, proses penilaian risiko yang akan dilaksanakan juga tidak boleh mengabaikan risiko serangan siber lainnya yang sewaktu-waktu juga dapat berkembang hingga memiliki tingkat kemungkinan, dampak dan skala risiko yang tinggi terhadap kinerja SMKI maupun bisnis yang digeluti oleh PT. UAV di masa depan.
2. PT. UAV disarankan untuk segera membuat rencana pengendalian risiko atau standard operasional prosedur (SOP) terkait risiko serangan siber yang telah memiliki level risiko "Sedang" dan menjadi prioritas utama pada penelitian ini. Pembuatan SOP tersebut diharapkan dapat membantu dan mempermudah manajerial PT. UAV untuk meminimalisir atau bahkan menghilangkan risiko serangan siber yang dimaksud.
3. Akademisi atau Peneliti selanjutnya disarankan untuk melakukan penelitian lebih lanjut terkait proses penilaian risiko serangan siber pada instansi pemerintahan, organisasi, industri, atau perusahaan lainnya.

Sehingga hasil penelitian yang diperoleh dapat digunakan sebagai landasan untuk mengembangkan konsep penilaian risiko serangan siber yang dapat membantu Kementerian Pertahanan dalam membangun sistem pertahanan siber yang tangguh dan berdaya tangkal tinggi terhadap ancaman serangan siber.

Daftar Pustaka

Buku:

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi: Teori, Analisis dan Implementasi*. Penerbit Andi.

Badan Siber dan Sandi Nasional. (2018). *Laporan Tahunan 2018 Honeynet Project BSSN – IHP*.

Badan Standardisasi Nasional. (2013). Standar SNI ISO/IEC 27001:2013: Teknologi Informasi – Teknik Keamanan – Sistem Manajemen Keamanan Informasi – Persyaratan.

Banyumurti, Indriyatno, dkk. (2018). *Kebijakan Cybersecurity dalam Perspektif Multistakeholder – Seri Literasi Digital*. ICT Watch.

Beidleman, Scoot W. (2009). *Defining and Deterring Cyber War*. U.A. Army War College, Carlisle Barracks.

International Organization for Standardization. (2013). ISO 27001: 2013: Information Technology – Security Techniques – Information Security Risk Management Systems – Requirements.

International Organization for Standardization. (2018). *ISO 27005: 2018 Information Technology – Security Techniques – Information Security Risk Management*.

Maskun. (2013). *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Kencana, Prenada Media Grup.

Miles, M.B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook*. SAGE Publications Inc.

Moleong, L. J. (2017). *Metodologi Penelitian Kualitatif*. PT. Remaja Rosdakarya.

Wahid, A. & Labib, M. (2005). *Kejahatan Mayantara (Cyber Crime)*. PT. Refika Aditama.

Yin, R. K. (2011). *Studi Kasus: Desain & Metode*. Rajagrafindo Persada.

Jurnal:

Akbanov, M., Vassilakis, V. G., & Logothetis, M. D. (2019). WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms. *Journal of Telecommunications and Information Technology*. 1(1), 113-124.

Farwell, J. P. & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, 53(1), 23-40.

Peraturan/Perundang-Undangan:

Kementerian Pertahanan Republik Indonesia. (2014). Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber.

Website:

Kilbride, J. & Xiao, B. (2018). "Chinese Drone Maker DJI Left Users at High Risk of Spying and Hacking Under Security Flaw". dalam https://www.abc.net.au/news/2018-11-14/dji-drones-were-exposed-to-security-flaw/10491150.html, diakses pada 29 Juli 2019.

Nistanto, R. K. (2017). "Awas! Drone Kini Juga Jadi Sasaran Hacker". dalam https://tekno.kompas.com/read/2017/08/01/19130027/awas-drone-kini-juga-jadi-sasaran-hacker.html, diakses pada 29 Juli 2019.

Sindonews. (2018). *BSSN Sebut Ada 10 Sektor yang Rentan Serangan Siber*. dalam https://jatim.sindonews.com/read/8917/1/bssn-sebut-ada-10-sektor-yang-rentan-serangan-siber-1553644999.html, diakses pada 29 Juli 2019.