Paradigma POLISTAAT JURNAL ILMU SOSIAL DAN ILMU POLITIK

Vol. 4. No. 2 (2021)

DETEKSI DINI ANCAMAN *SOCIAL ENGINEERING HACKER* TERHADAP MATA PELAJARAN RAHASIA DI SEKOLAH STAF DAN KOMANDO ANGKATAN UDARA

Tri Hastuti,[1] Yusa Djuyandi,[2] Wawan Budi Darmawan[3]

[1]Program Magister Ilmu Politik, Universitas Padjadjaran
trihastuti235@gmail.com
[2]Program Studi Ilmu Politik, Universitas Padjadjaran
yusa.djuyandi@unpad.ac.id
[3]Program Studi Ilmu Politik, Universitas Padjadjaran
wawanbd@gmail.com

Doi: 10.23969/paradigmapolistaat.v4i1.4503

Abstract

The basis for conducting research is because of the phenomenon related to social engineering in the Seskoau environment. The concern that arises is the leakage of documents and important information related to strategies, defense facts and others contained in secret subjects, which if widespread are feared to threaten the defense of Indonesia.The research method uses qualitative, through a descriptive approach. The data sources used are primary and secondary data. The technique of collecting data is through interviewing resource persons. The data analysis technique uses the Miles and Huberman model. While the data validation technique uses credibility, transferability, dependability, and confirmability tests. The results of the study found the threat of Social Engineering Hackers in Seskoau. Anticipatory steps taken include: checking the source of the leak, closing access to information in the event of a leak, summoning suspicious Pasis/making an information leak, conducting operations/intelligence activities, diverting material discussions, when suspicious things are indicated, limiting the use of social media in lessons, does not provide material or information related to the Doctrine, does not discuss or share secret subjects in friendly countries, discipline in using passwords, gives warnings / reprimands, does not leak confidential information, is selective in speaking with Pasis of friendly countries, selective in uploading lessons to various media, creating special folders for storing files on computers/laptops, reducing excessive contact with Pasis of friendly countries, committed to always following applicable fixed procedures, always checking n the source of the suspicious action, which was followed up with isolation measures and conducting an investigation, making reports in stages through KORSIS, PAM and POM, as well as reporting as soon as possible to the agency's intelligence agency.

Keywords: Early Detection of Threats, Social Engineering, Secret Subjects

Abstrak

Dasar dilakukan penelitian, karena adanya fenomena terkait *social engineering* di lingkungan Seskoau. Kekhawatiran yang muncul adalah kebocoran dokumen dan informasi-informasi penting terkait strategi, fakta pertahanan dan yang lainnya yang ada dalam mata pelajaran rahasia, yang apabila tersebar luas dikhawatirkan dapat mengancam pertahanan negara Indonesia. Metode penelitian menggunakan kualitatif,

melalui pendekatan deskriptif. Sumber data yang digunakan data primer dan sekunder. Teknik pengumpulan data melalui wawancara Narasumber. Teknik analisis data menggunakan model Miles and Huberman. Sedangkan teknik validasi data menggunakan uji *credibility*, *transferability*, *dependability*, *confirmability*. Hasil penelitian ditemukan adanya ancaman *Social Engineering Hacker* di Seskoau. Langkah antisipasi yang dilakukan meliputi: melakukan pengecekan sumber kebocoran, melakukan penutupan akses informasi jika terjadi kebocoran, melakukan pemanggilan terhadap Pasis yang mencurigakan/membuat suatu kebocoran informasi, melakukan kegiatan operasi/ intelijen, pengalihan bahasan materi, ketika terindikasi adanya hal yang mencurigakan, membatasi penggunaan medsos dalam pelajaran, tidak memberikan materi atau informasi-informasi yang terkait dengan Doktrin, tidak mendiskusikan atau men-share mata pelajaran rahasia pada Pasis negara sahabat, disiplin dalam menggunakan password, memberikan peringatan/teguran, tidak membocorkan informasi yang sifatnya rahasia, selektif dalam berbicara dengan Pasis negara sahabat, selektif dalam mengupload pelajaran ke berbagai media, membuat folder khusus dalam penyimpana file di komputer/laptop, mengurangi kontak berlebihan dengan Pasis negara sahabat, berkomitmen untuk selalu mengikuti prosedur tetap yang berlaku, senantiasa melakukan pengecekan sumber tindakan yang mencurigakan, yang ditindaklanjuti dengan tindakan isolasi dan melakukan penyelidikan, membuat laporan secara berjenjang melalui KORSIS, PAM dan POM, serta melaporkan secepatnya kepada pihak intel lembaga.

Kata Kunci: Deteksi Dini Ancaman, Social Engineering, Mata Pelajaran Rahasia

PENDAHULUAN

Kerjasama internasional dilakukan untuk meningkatkan hubungan persahabatan yang terjalin antar negara. Kerjasama internasional sendiri merupakan suatu bentuk hubungan yang dilakukan oleh negara satu dengan yang lainnya. Pada umumnya, kerjasama internasional ini dilakukan dalam bidang sosial, politik, kebudayaan, pertahanaan keamanan serta ekonomi. Kerjasama antar negara biasa berpedoman kepada politik luar negeri dalam negara itu sendiri. Politik keamanan bukan sekedar keamanan nasional suatu negara dalam wilayah yuridiksi negara dengan kekuatan militer untuk mengamankan dari ancaman dan serangan militer negara lain. Namun, keamanan itu harus dipahami sebagai suatu tindakan pada suatu kondisi dimana tidak adanya ancaman sebagai lawan dari rasa aman.

Pada era internet saat ini, informasi itu sangat mudah diperoleh dan dapat disebarluaskan pula. Oleh karena itu, bagi seseorang, organisasi, pemerintah maupun swasta informasi itu menjadi aset yang sangat berharga. Informasi memiliki nilai dan harus dilindungi, sehingga menjadi penting bagi individu untuk melakukan perlindungan terhadap informasi. Oleh karena itu dibutuhkan keamanan informasi yaitu melindungi informasi dari berbagai ancaman untuk menjamin kelangsungan operasi organisasi, meminimalisasi kerusakan akibat terjadinya ancaman, serta mempercepat kembalinya proses kerja organisasi. Pengamanan informasi sangat dibutuhkan agar kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi dapat terjaga sehingga tidak mengganggu kinerja dan operasional organisasi. Serangan terhadap keamanan informasi dapat berasal dari dalam (insider attacks) dan dari luar (*outsider attacks*). Seperti yang dinyatakan oleh

Mitnick dan Simon (2002) manusia merupakan faktor utama dan penting dalam pengamanan informasi selain teknologi, karena manusia merupakan rantai terlemah dalam rantai keamanan. Oleh sebab itu, dimensi manusia perlu selalu dibina dengan baik agar segala bentuk ancaman dapat dihindari. Salah satu cara yang dapat dilakukan adalah dengan menumbuhkan kesadaran akan pentingnya keamanan informasi.

Penggunaan teknologi informasi dalam sistem informasi modern saat ini, telah memaksa dunia militer untuk meninjau kembali organisasi dan doktrinnya, karena perkembangan teknologi informasi membawa perubahan mendasar pada pola penataan strategis dalam perangkat perang modern tanpa menghilangkan jiwa keprajuritan. Panglima TNI Jenderal Gatot Nurmantyo pada peresmian Satuan Siber TNI, pada tanggal 13 Oktober 2017 di Cilangkap mengatakan bahwa, perkembangan teknologi informasi merupakan tantangan yang harus mampu diantisipasi, sehingga sumber daya informasi di lingkungan TNI dapat terlindungi dari gangguan dan penyalahgunaan maupun pemanfaatan pihak-pihak lain. Penekanan Panglima TNI di atas dapat diartikan bahwa perubahan akibat perkembangan teknologi informasi merupakan hal yang tidak dapat dihindari lagi, sehingga TNI harus dapat menyiapkan perangkat maupun SDM yang memadai. Dalam teknologi informasi dikenal istilah data *breach*. Data *breach* atau pelanggaran data merupakan suatu insiden keamanan di mana informasi diakses tanpa otorisasi. *Department of Justice* Amerika yang disadur oleh Yudi Prayudi (2020) dalam tulisannya yaitu "*data breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, access for an unauthorized purpose, or other unauthorized access, to data, whether physical or electronic.*". Sedangkan *social engineering* atau disingkat (Soceng) merupakan manipulasi psikologis dari seseorang dalam melakukan aksi atau menguak suatu informasi rahasia dengan cara meminta informasi itu langsung kepada korban atau pihak lain yang mempunyai informasi itu. Data *breach* dan *social engineering* memiliki keterkaitan satu sama lainnya, *social engineering* bukanlah sebuah teknik serangan yang anyar/baru. Namun, yang pasti, serangan ini akan terus ada dan dapat dilakukan kapan pun, di mana pun. CERT-UK (2015) dalam penelitian mereka yang berjudul "*An introduction to social engineering*," dikatakan bahwa *social engineering* merupakan salah satu jenis serangan yang paling efektif dan paling produktif untuk mendapatkan informasi dengan cara masuk ke dalam suatu sistem yang memiliki mekanisme keamanan rumit. Celakanya lagi, serangan ini dapat dilakukan tanpa membutuhkan ilmu teknis yang baik. Terdapat empat siklus penting yang sering digunakan dalam mendapatkan informasi melalui *social engineering*. Siklus tersebut adalah: Pertama, *Social engineering* mencari informasi terkait apa yang akan ia cari dan siapa yang bisa ia jadikan target eksploitasi. Kedua, *Social engineering* akan membangun hubungan dengan target yang dimaksud. Membangun hubungan tersebut dapat dilakukan dengan berbagai cara seperti bekerja pada organisasi yang ia jadikan target, membangun hubungan pertemanan ataupun persaudaraan bahkan membangun hubungan emosional. Ketiga, *Social engineering* akan memanfaatkan psikis target untuk mendapatkan informasi dengan bermacam macam cara seperti rayuan, ancaman, suapan, dll. Keempat, ketika informasi berhasil didapatkan, maka *social engineer* akan melengkapi siklus

dengan eksekusi terhadap informasi tersebut.

Pada banyak referensi, faktor manusia dinilai sebagai rantai paling lemah dalam sebuah sistem keamanan. Sebuah sistem keamanan yang baik, akan menjadi tidak berguna jika ditangani oleh administrator atau user yang kurang kompeten. Serangan *social engineering* pada dasarnya adalah untuk mendapatkan kepercayaan korban untuk mencuri data, informasi, dan uang. Secara umum, *social engineering* melibatkan komunikasi yang memunculkan urgensi, ketakutan, atau emosi serupa dalam diri korban. Hal ini guna mengarahkan korban untuk segera mengungkapkan informasi sensitif. Resiko yang mungkin terjadi akibat *social engineering* sangat tinggi. Orang-orang dalam cenderung memberi informasi kepada para *social engineer* yang menyamar sebagai pihak yang berhak mendapatkan informasi. Oleh karena itu, keamanan tidak bisa hanya dikaitkan dengan teknologi saja, tetapi juga aspek psikologis. Apabila seorang pegawai yang memiliki informasi vital membocorkannya tanpa sadar, seluruh jaringan keamanan dapat runtuh. Ada beberapa titik lemah manusia yang bisa dimanfaatkan terkait kegiatan *social engineering* ini, diantaranya: Kesatu. Rasa Takut, jika seorang pegawai atau karyawan dimintai data atau informasi dari atasannya, polisi, atau penegak hukum yang lain, biasanya yang bersangkutan akan langsung memberikan tanpa merasa sungkan. Kedua. Rasa Percaya, jika seorang individu dimintai data atau informasi dari teman baik, rekan sejawat, sanak saudara, atau sekretaris, biasanya yang bersangkutan akan langsung memberikannya tanpa harus merasa curiga. Ketiga. Rasa Ingin Menolong, jika seseorang dimintai data atau informasi dari orang yang sedang tertimpa musibah, dalam kesedihan yang mendalam, menjadi korban bencana, atau berada dalam duka, biasanya yang bersangkutan akan langsung memberikan data atau informasi yang diinginkan tanpa bertanya lebih dahulu. Pada tahun 2018 jagat maya diramaikan oleh berita seorang remaja autis asal Inggris bernama Kane Gamble yang telah membobol jaringan internet pejabat Amerika Serikat dan mencuri dokumen-dokumen rahasia negara. Sedikit berbeda dengan tipikal *hacker* yang kita ketahui yang menggunakan kelemahan keamanan teknologi, Gamble justru menggunakan taktik yang memanfaatkan suatu kelemahan yang pasti ada di setiap organisasi, yaitu psikologi manusia.

Sekolah Staf dan Komando Angkatan Udara disingkat Seskoau merupakan lembaga pendidikan pengembangan umum tertinggi tingkat TNI Angkatan Udara, yang mempunyai tugas menyelenggarakan pendidikan pengembangan umum tertinggi di Angkatan Udara, pendalaman materi kejuangan, pengkajian dan pengembangan, doktrin masalah-masalah Pertahanan Negara, Dirgantara serta pengkajian masalah-masalah pendidikan dan latihan di Angkatan Udara. Dalam rangka meningkatkan pemahaman dan pengetahuan mengenai kebijakan, strategi dan desain dibidang peningkatan sumber daya manusia, dan alih teknologi pertahanan. Sekolah Staf dan Komando Angkatan Udara (Seskoau) telah melakukan kerjasama militer dengan beberapa Negara di dunia. Dalam satu dasawarsa pemerintah Indonesia telah menjalin kerjasama internasional (*International Relations*) dengan berbagai negara. Kerjasama militer lintas negara sangat banyak ragamnya, mulai dari alutsista sampai dengan pertukaran personel militernya. Diantara kerja sama tersebut, salah satunya adalah dalam bidang pelatihan

dan pendidikan militer. Bentuk kerja sama pendidikan militer ini antara lain pertukaran Perwira Siswa (Pasis) dan Perwira Penuntun (Patun) yang telah lulus dalam seleksi untuk dapat dikirimkan dari Indonesia ke Mancanegara atau tiap negara yang telah menjalin kerja sama militer, atau sebaliknya dari Mancanegara ke Indonesia. Kerja sama bidang pendidikan militer ini terjalin sudah cukup lama, dari kerja sama ini Perwira Siswa (Pasis) dan Perwira Penuntun (Patun) di tempatkan di lembaga pendidikan (lemdik) militer seperti Sesko TNI, Seskoad, Seskoal dan Seskoau. Seskoau adalah lembaga pendidikan tertinggi Angkatan Udara yang mendapatkan Perwira Penuntun (Patun) dan Perwira Siswa (Pasis) mancanegara lebih dari tiga negara seperti, Malaysia, Singapura, Korea, Australia, Amerika, India, Pakistan dan Saudia Arabia untuk mengikuti pendidikan militer.

Perwira Siswa (Pasis) dan Perwira Penuntun (Patun) harus memiliki kemampuan untuk mengantisipasi dan memprediksi suatu peristiwa yang diperkirakan akan terjadi sehingga menimbulkan sikap waspada terhadap situasi dan kondisi yang berkembang terutama yang akan mengganggu aspek-aspek pertahanan negara kita, yang dituangkan dalam suatu konsep Rencana Tindakan Kontijensi (Rentikon), harus senantiasa dimiliki oleh setiap perwira TNI. Hal ini sesuai dengan Kurikulum Pendidikannya, telah memprogramkan bagi Para Perwira Siswa melaksanakan Kuliah Kerja II Rencana Tindakan Kontijensi yang merupakan salah satu bagian dari proses pembelajaran yang diterapkan di Seskoau, yang mana melalui Kuliah Kerja II ini, diharapkan Pasis Seskoau dapat mengenal dan mengetahui mekanisme pembuatan naskah Rencana Tindakan Kontijensi (Rentikon) Kohanudnas dalam menghadapi kemungkinan timbulnya kontinjensi di wilayah udara. Meskipun mereka mengikuti pendidikan militer di Seskoau dan mendapatkan pelajaran sesuai dengan kurikulum tetapi ada beberapa materi pelajaran yang terdapat didalam kurikulum lembaga tersebut tidak diperkenankan di berikan kepada Perwira Siswa (Pasis) mancanegara, atau dengan kata lain ada beberapa kegiatan pembelajaran dan materi yang tidak boleh diikuti oleh para Perwira Siswa (Pasis) dan Perwira Penuntun (Patun) dari mancanegara dengan alasan untuk menjaga informasi kerahasiaan pertahanan dan keamanan negara. Salah satu contoh materi pelajaran yang tidak diberikan diantaranya adalah salah satu mata pelajaran di Bidang Studi Operasi Udara. Dalam proses pelaksanaan pelatihan dan pendidikan di lembaga pendidikan Seskoau saat ini menggunakan dukungan teknologi informasi berupa aplikasi Learning Management System (LMS) Seskoau yang dapat di akses oleh seluruh Personel Seskoau yang terlibat dalam kegiatan pendidikan, termasuk Perwira Siswa (Pasis) dan Perwira Penuntun (Patun) mancanegara yang mengikuti proses pendidikan ini, melalui jaringan komputer dan internet.

Kurikulum pendidikan Seskoau terkait mata pelajaran yang tidak dapat diikuti oleh Perwira Siswa (Pasis) dan Perwira Penuntun (Patun) mancanegara, hal ini tertuang dalam Keputusan Kasau Nomor Kep/863/VI/2018 tanggal 8 November 2018 tentang Kurikulum Pendidikan Seskoau, yang ditindaklanjuti melalui Prosedur Tetap (Protap) Nomor Kep/32/V/2020 tentang Mata Pelajaran Seskoau yang tidak diikuti oleh Pasis Negara sahabat. Maksud pembuatan prosedur tetap tentang mata pelajaran Seskoau yang tidak diikuti oleh Pasis negara sahabat

adalah sebagai pedoman bagi para pelaksana pendidikan di lingkungan Seskoau supaya tidak ada kesimpangsiuran keberadaan Pasis Negara sahabat dalam penyelenggaraan pendidikan di lingkungan Seskoau. Ada beberapa mata pelajaran dari tiap departemen yang tidak diikuti oleh Pasis Negara sahabat atau dapat dikatakan sifatnya rahasia bahkan sangat rahasia, yaitu diantaranya; Kesatu. Departemen kepemimpinan dan kejuangan, meliputi: MP. Doktrin Hanneg. Kedua. Departemen operasi, meliputi: Jaklat operasi udara, Jaklat operasi TNI, Renkon, Rentinkon (Teori dan Aplikasi). Ketiga. Departemen masalah strategis, meliputi: Strategi militer, Strategi perang udara, kekuatan nasional, kepentingan nasional. Keempat. Departemen ilmu pengetahuan dan teknologi, meliputi: Intelijen udara, Intelijen strategis.

Fenomena yang terjadi yaitu terkait Pasis negara sahabat atau Pasis mancanegara yang sedikit mulai mengetahui informasi tentang adanya mata pelajaran rahasia dilingkungan Seskoau. Hal tersebut diketahui dari adanya komunikasi antar Pasis Indonesia dengan Pasis mancanegara maupun antara Pasis mancanegara dengan Dosen Pengajar. Kondisi ini dapat mendorong adanya indikasi *social engineering* yang dilakukan oleh Pasis mancanegara. Sebagaimana diketahui bahwa *social engineering* ini merupakan suatu ancaman, yang mana kegiatannya memanipulasi psikologis dari seseorang dalam melakukan aksi atau menguak suatu informasi rahasia. Interaksinya bisa dilakukan melalui berbagai jalur komunikasi seperti, *voice call* (telepon), *Short Message Service* (sms), *email*, *direct message* (DM), *WhatsApp*, atau bahkan bertemu langsung dengan orang nya/target/korban. Sehingga perlu dilakukannya deteksi dini terkait ancaman *social enginering* ini, agar kerahasiaan tersebut tetap terjaga. Mengacu pada fenomena yang terjadi, maka diyakini perlu dilakukan penelitian lebih spesifik dan mendalam terkait ancaman *social engineering* ini dengan menuangkannya kedalam sebuah tesis dengan judul “Deteksi Dini Ancaman *Social Engineering Hacker* Terhadap Prosedur Tetap Mata Pelajaran Rahasia dan Sangat Rahasia di Lembaga Pendidikan Militer Seskoau Lembang”. Kekhawatiran yang muncul adalah kebocoran dokumen dan informasi-informasi penting terkait strategi, fakta pertahanan dan yang lainnya yang ada dalam mata pelajaran rahasisa tersebut, yang apabila tersebar luas dikhawatirkan dapat mengancam pada pertahanan negara Indonesia.

Penelitian yang sama telah dilakukan juga oleh Rafizan (2011) dalam judul penelitiannya “Analisis Penyerangan *Social Engineering*”. Hasil penelitiannya menyatakan bahwa Seorang *hacker* dalam mendapatkan sasarannya tidak terbatas hanya dengan menggunakan komputer untuk mengeksploitasi kelemahan-kelemahan sasarannya. Mereka juga dapat menjadikan manusia sebagai sasarannya untuk mendapatkan informasi-informasi penting yang dapat digunakan untuk menerobos suatu sistem keamanan. Cara yang dipakai seperti itu ialah *social engineering*, yang bertujuan untuk membuat agar staff/manusia yang menjadi sasarannya memberikan informasi-informasi yang dia inginkan. Jika *hacker* tersebut telah memiliki informasi-informasi penting yang dibutuhkan olehnya untuk menerobos sistem keamanan, maka sistem keamanan yang telah dipasang akan menjadi tidak berguna. Untuk menanggulangi masalah seperti ini adalah dengan cara meningkatkan kesadaran dari staff/pengguna mengenai *social engineering* dan ancamannya.

Selain itu perusahaan juga harus memiliki dokumen resmi yang jelas berupa standar, prosedur, atau kebijakan mengenai keamanan informasi, sehingga staff/pengguna dapat mengikuti, mematuhi, dan selalu menjadikan dokumen resmi tersebut sebagai acuan atas segala tindakan yang dilakukan di perusahaan tersebut. Kemudian oleh Imas Rahmadhtul Hidayah (2020) dengan judul penelitian "Representasi *Social Engineering* Dalam Tindak Kejahatan Dunia Maya (Analisis Semiotik Pada Film Firewall)". Hasil penelitiannya menyatakan bahwa representasi *social engineering* yang tercermin yaitu *reverse social engineering* berbasis interaksi sosial. *Hacker* tidak hanya melakukan penyerangan luar seperti melakukan penyebaran virus dan sejenisnya melainkan menggunakan teknik lain yang lebih 'elegan' dengan menyerang melalui jalur dalam (internal). Penyerang internal terkesan massif dan terstruktur, sehingga tidak terdeteksi oleh sistem keamanan (berbasis interaksi sosial). Selanjutnya hasil penelitian dari Shivam Lohani (2018) dalam judul penelitiannya "*Social Engineering: Hacking into Humans*". Hasil penelitiannya menyatakan bawah "*Social engineering proves to be one of the most dangerous phases of hacking and information gathering. Also due to lack of knowledge and awareness, the Social Engineering is growing day by day. The conclusion is that it is impossible to stop social engineering attacks as there is no patch for the human vulnerability. Educating people about the Social Engineering and its adverse effects can certainly decrease this type of attacks but cannot be fully prevented*". Hal ini menunjukan bahwa *social engineering* terbukti menjadi salah satu fase peretasan dan pengumpulan informasi yang paling berbahaya. Kemudian penelitian dari Jain, Tailang, Goswami, Dutta, Singh Sankhla, & Rajeev Kumar (2016) dalam judul penelitiannya "*Social Engineering: Hacking a Human Being through Technology*". Hasil penelitiannya menyatakan bahwa "*how much strong a company's security is, there is always a loophole of manipulation since human trust is a liable factor. Social engineers manipulate their victims into giving their personal information and bank details as humans can be manipulated easily due to their tendency to trust, which can be taken a great advantage of by these attackers*." Hal ini dimaksudkan seberapa kuat keamanan perusahaan, selalu ada celah manipulasi karena kepercayaan manusia adalah faktor yang bertanggung jawab. Serta penelitian dari Kumar, Chaudhary and Nagresh (2015) dengan judul penelitiannya "*Social Engineering Threats and Awareness: A Survey*". Hasil penelitiannya menyatakan bahwa "*even after using the best and even the most expensive security technologies, an organization or a company or an individual is completely vulnerable. It means it is very easy for a good attacker to gather information about that organization just by gaining trust and being friendly with the user*." Hal ini menunjukan begitu sangat mudah bagi *social engineers* untuk mengumpulkan informasi tentang organisasi tersebut hanya dengan mendapatkan kepercayaan dan bersikap ramah dengan pengguna.

Berdasarkan hasil penelitian terdahulu tersebut diatas, terdapat satu hal yang memiliki kesamaan bahwa, ancaman keamanan informasi menggunakan suatu cara yang dinamakan *social engineering* yang menimbulkan efek besar terhadap gangguan keamanan informasi pada suatu organisasi dari ancaman serangan tersebut. Sedangkan perbedaan penelitian ini adalah fokus pada deteksi

dini terhadap ancaman serangan *social engineering* yang diharapkan munculnya kesadaran dan kepedulian dari para stakeholder atau seluruh komponen organisasi akan pentingnya keamanan informasi serta dapat memberikan rekomendasi pembentukan perangkat keamanan informasi.

METODE PENELITIAN

A. Desain Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode kualitatif. Penelitian kualitatif merupakan penelitian yang berupaya membangun pandangan orang yang diteliti secara rinci serta dibentuk dengan kata-kata, gambaran yang menyeluruh, mendalam dan rumit (Tohirin, 2013:2). Metodelogi penelitian kualitatif bertujuan untuk menganalisis dan mendeskripsikan fenomena atau obyek penelitian melalui aktivitas sosial, sikap dan persepsi orang secara individu atau kelompok.

Adapun jenis pendekatan penelitian ini adalah deskriptif. Jenis penelitian deskriptif kualitatif yang digunakan pada penelitian ini dimaksudkan untuk memperoleh informasi mengenai deteksi dini ancaman *Social Enginering Hacker* terhadap mata pelajaran rahasia secara mendalam dan komprehensif. Selain itu, dengan metode kualitatif diharapkan dapat diungkapkan langkah-langkah antisipatif yang dilakukan Seskoau terhadap ancaman *Social Engineering Hacker* pada mata pelajaran rahasia di Seskoau.

B. Informan

Informan penelitian merupakan sumber data yang dimintai informasinya sesuai dengan masalah penelitian. Subjek yang memenuhi parameter yang dapat mengungkap hal di atas sehingga memungkinkan data dapat diperoleh. Parameternya adalah sebagai berikut:

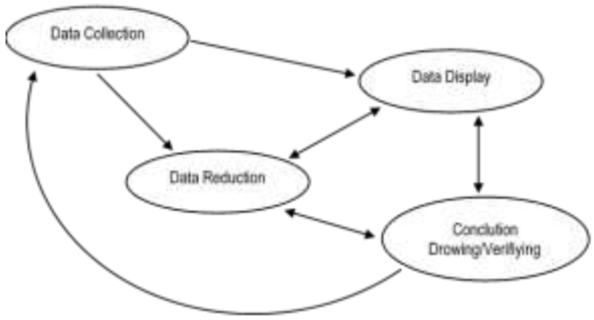
1) Mengetahui kurikulum pembelajaran Seskoau berdasarkan Kep. Kasau No. Kep/863/XI/2018
2) Mengetahui Prosedur Tetap (PROTAP) berdasarkan No. Kep/32/V/2020
3) Terlibat langsung dalam hal implementasi Kep. Kasau No. Kep/863/XI/2018 dan Protap No. Kep/32/V/2020

Berdasarkan kriteria di atas, subjek penelitian yang dianggap memenuhi karakteristik yaitu koordinator pendidik (dosen dan patun), koordinator tenaga kependidikan (staf penyelenggara), dan ketua pasis lokal. Untuk lebih jelasnya dapat dilihat pada tabel dataset dibawah ini:

C. Teknik Analisis Data

Pada penelitian ini, teknik analisis data yang digunakan peneliti menggunakan model Miles and Huberman. Analisis data dalam penelitian kualitatif, dilakukan pada saat pengumpulan data berlangsung, dan setelah selesai pengumpulan data dalam periode tertentu. Pada saat wawancara, peneliti sudah melakukan analisis terhadap jawaban yang diwawancarai.

Dalam analisis data, peneliti menggunakan model *interactive model*, yang unsur-unsurnya meliputi reduksi data (*data reduction*), penyajian data (*data display*), dan *conclutions drowing/verifiying*. Alur teknik analisis data dapat dilihat seperti gambar di bawah ini.



Gambar 1 Komponen dalam analisis data

Untuk teknik analisis data pada penelitian ini, penulis menggunakan tiga prosedur perolehan data, yaitu meliputi:

1) Reduksi Data (*Data Reduction*)
Reduksi data adalah proses penyempurnaan data, baik pengurangan terhadap data yang dianggap kurang perlu dan tidak relevan, maupun penambahan data yang dirasa masih kurang. Data yang diperoleh di lapangan mungkin jumlahnya sangat banyak. Reduksi data berarti merangkum, memilih hal-hal yang pokok, memfokuskan pada hal-hal yang penting, dicari tema dan polanya (Sugiyono, 2007:247). Dengan demikian data yang akan direduksi memberikan gambaran yang lebih jelas, dan mempermudah peneliti untuk melakukan pengumpulan data selanjutnya, dan mencarinya bila diperlukan.
2) Penyajian Data/Display
Dengan mendisplay atau menyajikan data akan memudahkan untuk memahami apa yang terjadi selama penelitian berlangsung. Setelah itu perlu adanya perencanaan kerja berdasarkan apa yang telah dipahami. Dalam penyajian data selain menggunakan teks secara naratif, juga dapat berupa bahasa nonverbal seperti bagan, grafik, denah, matriks, dan tabel. Penyajian data merupakan proses pengumpulan informasi yang disusun berdasarkan kategori atau pengelompokan-pengelompokan yang diperlukan.
3) Verifikasi Data (*Conclusions drowing/ verifiying*)
Langkah terakhir dalam teknik analisis data adalah verifikasi data. Verifikasi data dilakukan apabila kesimpulan awal yang dikemukan masih bersifat sementara, dan akan ada perubahan-perubahan bila tidak dibarengi dengan bukti-bukti pendukung yang kuat untuk mendukung pada tahap pengumpulan data berikutnya (Sugiyono, 2007:252). Bila kesimpulan yag dikemukan pada tahap awal, didukung dengan bukti-bukti yang valid dan konsisten saat penelitian kembali ke lapangan mengumpulkan data, maka kesimpulan yang dikemukakan merupakan kesimpulan yang kredibel atau dapat dipercaya.

D. Instrumen Penelitian

Berdasarkan teknik pengumpulan data yang digunakan, maka instrumen penelitian ini menggunakan panduan wawancara dan panduan dokumentasi.

Berikut adalah tabel kisi-kisi panduan wawancara dan dokumentasi.

Table 1 Kisi-kisi panduan wawancara

No	Dimensi	Indikator
1	Ancaman *social engineering Hacker*	1. *Reciprocation* (Timbal Balik) 2. *Consistency* (Konsistensi) 3. *Social Validation* (Validasi Sosial) 4. *Liking* (Kesukaan) 5. *Authority* (Otoritas) 6. *Scarcity* (kelangkaan)
2	Pemahaman Protap mata pelajaran rahasia	1. Pemahaman konsep protap 2. Pemahaman hakikat protap 3. Pemahaman implementasi protap
3	Langkah antisipatif Ancaman *social engineering Hacker*	1. Pencegahan kebocoran informasi 2. Keamanan akses informasi 3. Verifikasi kontak 4. Mengikuti prosedur 5. Pelaporan tindakan mencurigakan 6. Menjaga emosi 7. Pelatihan berkelanjutan 8. Pemberian edukasi kepada perwira siswa negara sahabat (mancanegara)

E. Teknik Validasi Data

Uji keabsahan/kevalidan data dalam penelitian kualitatif meliputi: uji *credibility*, *transferability*, *dependability*, dan *confirmability*.

Agar data dalam penelitian kualitatif dapat dipertanggungjawabkan sebagai penelitian ilmiah, maka selanjutnya perlu dilakukan suatu uji yaitu uji keabsahan atau uji validasi data. Adapun uji validasi data yang dapat dilaksanakan dalam penelitian ini yaitu, meliputi:

1) *Credibility*
Uji *credibility* (kredibilitas) atau uji kepercayaan terhadap data hasil penelitian yang disajikan oleh peneliti agar hasil penelitian yang dilakukan tidak meragukan sebagai sebuah karya ilmiah dilakukan.

2) *Transferability*
Transferability merupakan validitas eksternal dalam penelitian kualitatif (Sugiyono, 2007:276). Validitas eksternal menunjukkan derajat ketepatan atau dapat diterapkannya hasil penelitian ke populasi di mana sampel tersebut diambil. Pertanyaan yang berkaitan dengan nilai transfer sampai saat ini masih dapat diterapkan/dipakai dalam situasi lain. Bagi peneliti nilai transfer sangat bergantung pada si pemakai, sehingga ketika penelitian dapat digunakan dalam konteks yang berbeda di situasi sosial yang berbeda validitas nilai transfer masih dapat dipertanggungjawabkan.

3) *Dependability*
Penelitian yang *dependability* atau *reliabilitas* adalah penelitian apabila penelitian yang dilakukan oleh orang lain dengan proses penelitian yang sama akan memperoleh hasil yang sama pula. Pengujian *dependability* dilakukan dengan cara melakukan audit terhadap keseluruhan proses penelitian. Dengan cara auditor yang independen atau pembimbing yang independen mengaudit keseluruhan aktivitas yang dilakukan oleh peneliti dalam melakukan penelitian. Misalnya bisa dimulai ketika bagaimana

Vol. 4. No. 2 (2021)

peneliti mulai menentukan masalah, terjun ke lapangan, memilih sumber data, melaksanakan analisis data, melakukan uji keabsahan data, sampai pada pembuatan laporan hasil pengamatan.

4) *Confirmability*
Objektivitas pengujian kualitatif disebut juga dengan uji *confirmability* penelitian. Penelitian bisa dikatakan objektif apabila hasil penelitian telah disepakati oleh lebih banyak orang. Penelitian kualitatif uji *confirmability* berarti menguji hasil penelitian yang dikaitkan dengan proses yang telah dilakukan. Apabila hasil penelitian merupakan fungsi dari proses penelitian yang dilakukan, maka penelitian tersebut telah memenuhi standar *confirmability*.

HASIL DAN PEMBAHASAN

A. Hasil Peneilitian

Tahap wawancara telah peneliti lakukan di Sekolah Staf dan Komando Angkatan Udara (Seskoau) Lembang, Kab. Bandung Barat terhadap tiga (3) orang Narasumber. Selanjutnya Narasumber berhasil diwawancarai secara intensif yang meliputi Narasumber 1 yaitu koordinator pendidik, kemudian Narasumber 2 yaitu koordinator staf penyelenggara, dan Narasumber 3 yaitu koordinator pasis lokal.

Data yang tidak terungkap melalui wawancara, selanjutnya dilengkapi dengan data hasil observasi langsung secara partisipatif yang dilakukan oleh peneliti selama penelitian berlangsung. Untuk memperkuat substansi data hasil wawancara dan observasi, maka dilakukanlah penelusuran terhadap dokumen-dokumen dan arsip yang ada. Selanjutnya semua data hasil penelitian ini diuraikan berdasarkan fokus dari rumusan masalah penelitian yang meliputi ancaman Social Engineering Hacker, pemahaman prosedur tetap, dan langkah antisipatif terhadap Social Engineering Hacker pada mata pelajaran rahasia di Seskoau, untuk lebih jelasnya adalah sebagai berikut:

1) *Ancaman Social Engineering Hacker Pada Mata Pelajaran Rahasia Di Seskoau*
Untuk mengetahui seperti apa ancaman *Social Engineering Hacker* yang terjadi di Seskoau, peneliti menggali informasi dengan fokus pada enam (6) aspek yaitu meliputi *reciprocation*, *consistency*, *social validation*, *liking*, *authority*, dan aspek *scarcity*.

a) *Reciprocation*
Berdasarkan hasil wawancara dengan Narasumber koordinator pendidik terkait aspek *Reciprocation* (timbal balik), peneliti menggali informasi dengan menanyakan apakah seluruh pendidik sering berinteraksi dengan Pasis negara sahabat (mancanegara).

Dari ketiga Narasumber dapat dianalisis kembali bahwa, ada sedikit perbedaan jawaban yang diberikan oleh Narasumber 2, yang menyatakan tidak sering berinterkasi, kalaupun terjadi interaksi hal tersebut berkaitan dengan permasalaan administrasi bukan dalam hal mata kuliah. secara umum sering terjadi interaksi antara pendidik di Seskoau dengan Pasis negara sahabat, maupun antara Pasis Indonesia dengan Pasis negara sahabat. Interaksi terjadi baik ketika dalam proses pembelajaran dikelas maupun ketika pembelajaran di luar kelas. Sebagian dari mereka berinteraksi melalui jejaring media sosial.

b) *Consistency*
Konsisten merupakan perilaku yang tetap dan tidak berubah. Konsisten adalah sebuah sikap yang positif dan mencerminkan seseorang tersebut kompeten. Untuk menerapkan kebiasaan konsisten, maka dipastikan juga kemampuan untuk bisa menjalaninya. Cara konsisten adalah melakukan yang sudah seharusnya dilakukan, seperti taat dan patuh terhadap suatu peraturan ataupun prosedur. Untuk mengetahui tingkat konsistensi dari pendidik, staff penyelenggara, dan Pasis Indonesia, peneliti melanjutkan wawancara dengan menanyakan apakah Pasis negara sahabat (mancanegara) pernah menanyakan terkait mata pelajaran rahasia kepada saudara/i.

Berdasarkan informasi dari ketiga Narasumber dapat dianalisis kembali bahwa, secara umum terdapat indikasi adanya kegiatan social engineering yang dilakukan oleh sebagian dari Pasis negara sahabat. Hal tersebut dirasakan oleh mayoritas pendidik dan mayoritas Pasis Indonesia. Sebagian dari Pasis negara sahabat menggali informasi tersebut ketika diluar kelas atau diluar jam pembelajaran. Hal ini dirasa memungkinkan, karena dalam waktu tersebut interaksi diantara sesama Pasis biasanya berlangsung lama.

c) *Social Validation*
Validasi bertujuan untuk menunjukkan bahwa sistem dari suatu prosedur tetap sesuai dengan spesifikasinya dan bahwa sistem tersebut memenuhi yang diharapkan. Kemudian dalam waktu yang berbeda peneliti menggali informasi lebih lanjut dengan cara menanyakan, apakah saudara/i pernah mengikuti kehendak/keinginan dari pasis negara sahabat (mancanegara) terkait materi pembelajaran.

Berdasarkan hasil wawancara dengan para Narasumber. Dari ketiga Narasumber yang telah peneliti analisis bahwa, secara umum baik itu pihak dari pendidik, staff penyelenggara, maupun dari Pasis Indonesia, semuanya memegang komitmen terhadap prosedur tetap yang berlaku di Seskoau. Mereka berkomitmen untuk tidak pernah mengikuti kehendak atau keingin dari Pasis negara sahabat dalam hal materi pembelajaran. Apalagi terkait mata pelajaran rahasia.

d) *Liking*
Kesukaan secara umum dapat digambarkan dalam berbagai bentuk diantaranya yaitu: rasa suka, hormat, persahabatan, dan kepercayaan. Kesukaan tidak bisa dijelaskan sepenuhnya melalui persepsi dan kepercayaan mereka mengenai atribut-atribut yang disukainya. Pada dasarnya, terdapat rasa suka atau minat besar yang berbeda dari atribut-atribut spesifik yang mendasarinya. Dalam kaitannya dengan Social Engineering Hacker, peneliti bertanya kepada Narasumber terkait aspek *Liking* (kesukaan) yaitu ketika pelaksanaan belajar dikelas, apakah saudara/i menyukai terhadap pola belajar Pasis negara sahabat (mancanegara).

Dari ketiga Narasumber dapat dianalisis kembali bahwa, secara umum baik itu pendidik, staff penyelenggara dan Pasis Indonesia, semuanya menyukai terhadap pola belajar yang dilakukan oleh Pasis negara sahabat. Terlebih lagi pola

disiplin belajar yang mereka lakukan, terkait rasa keingintahuan mereka terhadap sesuatu/ materi dalam pembelajaran.

e) *Authority*

Otoritas adalah suatu kewenangan yang didapatkan oleh seseorang atau kelompok guna menjalankan kewenangan tersebut sesuai dengan kewenangan yang diberikan, kewenangan tidak boleh dijalankan melebihi kewenangan yang diperoleh. Otoritas merupakan kemampuan yang dimiliki seseorang dalam suatu hal. Untuk mengetahui apakah terdapat ancaman pada tingkat otoritas sumber daya manusia yang ada di Seskoau, maka dalam wawancara penelitian ini, lebih lanjut peneliti bertanya kepada Narasumber mengenai apakah saudara/i pernah mempercayai terhadap kemampuan dalam sesuatu hal yang dimiliki oleh Pasis negara sahabat (mancanegara).

Dari ketiga Narasumber dapat dianalisis kembali bahwa, secar umum sering terjadi interaksi antara pendidik di Seskoau dengan Pasis negara sahabat, maupun antara Pasis Indonesia dengan Pasis negara sahabat. Interaksi terjadi baik ketika dalam proses pembelajaran dikelas maupun ketika pembelajaran di luar kelas. Sebagian dari mereka berinteraksi melalui jejaring media sosial.

f) *Scarcity*

Aspek yang dinilai selanjutnya adalah aspek dari *Scarcity*. Untuk menggali informasi tersebut peneliti bertanya kepada Narasumber ketika situasi pembelajaran dikelas, apakah saudara/i memiliki rasa takut/khawatir ada dari Pasis negara sahabat (mancanegara) yang menanyakan terkait mata pelajaran rahasia.

Dari ketiga Narasumber yang telah peneliti analisis bahwa, secara umum ada rasa takut/khawatir dan cemas apabila ada dari Pasis negara sahabat (mancanegara) yang menanyakan terkait mata pelajaran rahasia. Hal tersebut dirasakan oleh mayoritas dari staff penyelenggara maupun oleh mayoritas Pasis Indonesia, namun hal tersebut tidak terjadi dengan pendidik di Seskoau, mereka tidak memiliki rasa takut/khawatir dan cemas jika ada dari Pasis negara sahabat (mancanegara) yang menanyakan terkait mata pelajaran rahasia. Hal ini didasarkan pada komitmen yang harus dilaksanakan oleh setiap pendidik di Seskoau, apabila ada dari Pasis negara sahabat yang terindikasi mencurigakan, maka pendidik langsung mengalihkan pokok bahasan tersebut.

2) *Pemahaman Prosedur Tetap (Protap) Mata Pelajaran Rahasia Oleh Seluruh Pasis Indonesia, Staf dan Pejabat Seskoau.*

Secara umum prosedur memiliki tujuan untuk mempermudah dan memperlancar setiap pekerjaan yang dilaksanakan dalam rangka memberikan kemudahan. Adanya prosedur yang baik, diharapkan urutan kegiatan atau langkah-langkah tersebut dilakukan dengan baik guna mencapai tujuan yang baik pula. Dengan prosedur tetap setidaknya setiap sumber daya manusia mengetahui tentang apa tugasnya, apa yang tidak boleh dilakukannya, dan apa yang harus dilakukannya.

a) Pemahaman Konsep Protap

Dalam mengimplementasikan suatu prosedur, harus dibarengi

dengan tingkat pemahaman yang baik. Selanjutnya dalam kaitannya dengan pemahaman Prosedur Tetap (Protap) mata pelajaran rahasia oleh seluruh Pasis Indonesia, Staf penyelenggara, dan Pendidik di Seskoau. Peneliti melanjutkan wawancara dengan menanyakan kepada Narasumber apakah seluruh pendidik di Sekolah Staf dan Komando Angkatan Udara (Seskoau) memahami konsep dari Prosedur Tetap (Protap) berdasarkan No. Kep/32/V/2020.

Berdasakan hasil penggalian informasi dari ketiga Narasumber bahwa, mayoritas dari pendidik, staf penyelenggara, dan Pasis Indonesia memahami terkait konsep dari Prosedur Tetap (PROTAP) berdasarkan No. Kep/32/V/2020. Mayoritas dari mereka mendapatkan pemahaman tersebut melalui sosialisasi yang dilakukan oleh pihak penyelenggara, seperti ketika pelaksanaan apel.

b) Pemahaman Hakikat Protap

Standar Operasional Prosedur (SOP) atau Prosedur Tetap (Protap) merupakan serangkaian instruksi tertulis yang dibakukan dan didokumentasikan dari aktivitas rutin dan berulang yang dilakukan di Seskoau. Prosedur Tetap (Protap) adalah penetapan tertulis mengenai apa yang harus dilakukan, bagaimana, kapan, dimana dan oleh siapa. Prosedur Tetap (Protap) dibuat untuk menghindari terjadinya variasi dalam proses pelaksanaan kegiatan yang akan menghambat kinerja organisasi secara keseluruhan.

Berdasakan hasil analisis informasi terhadap ketiga Narasumber bahwa, secara umum mayoritas dari pendidik, staf penyelenggara, dan Pasis Indonesia memahami terkait hakikat dari Prosedur Tetap (PROTAP) berdasarkan No. Kep/32/V/2020. Namun ada sebagian dari Pasis Indonesia yang secara hakikat belum memahami Prosedur tersebut. Meskipun demikian sebagian dari mereka tetap diberikan edukasi bertahap yang dilaksanakan pada kegiatan-kegiatan penunjang lainnya, yang tentunya tetap berkomitmen untuk melaksanakan Protap tersebut.

c) Pemahaman Implementasi Protap

Sebelum mengimplementasikan suatu prosedur tetap, pemahaman terhadap prosedur tetap harus terrealisasi terlebih dulu. Hal ini bertujuan agar pelaksana prosedur tetap dapat dengan mudah melaksanakan atau mengimplementasikan prosedur tetap tersebut. Berkaitan dengan hal tersebut, selanjutnya peneliti menanyakan apakah seluruh pendidik di Sekolah Staf dan Komando Angkatan Udara (Seskoau) memahami implementasi dari Prosedur Tetap (PROTAP) berdasarkan No. Kep/32/V/2020.

Berdasarkan hasil analisis informasi yang telah peneliti lakukan terhadap ketiga Narasumber, bahwa secara umum mayoritas dari pendidik, staf penyelenggara, dan Pasis Indonesia, semuanya telah mengimplematasikan terkait Prosedur Tetap (PROTAP) berdasarkan No. Kep/32/V/2020 tentang mata pelajara Seskoau yang tidak diikuti oleh Pasis negara sahabat. Komitmen tersebut teguh dilaksanakan demi menjaga kebocoran dokumen dan informasi-

Vol. 4. No. 2 (2021)

informasi penting terkait strategi, fakta pertahanan dan yang lainnya yang ada dalam mata pelajaran rahasia, yang apabila tersebar luas dikhawatirkan dapat mengancam pertahanan negara Indonesia.

3) Langkah Antisipatif Yang Dilakukan Seskoau Terhadap Ancaman Social Engineering Hacker P ada Mata Pelajaran Rahasia Di Seskoau.

Langkah antisipatif merupakan suatu langkah pencegahan dini sebelum sesuatu hal terjadi menimpa. Langkah antisipatif dinilai penting keberadaannya demi menghindari suatu resiko yang bisa berdampak pada suatu kerugian. Begitu juga dengan ancaman *Social Engineering Hacker* terhadap mata pelajaran rahasia di Seskoau, kalau hal tersebut terjadi kekhawatiran yang muncul adalah kebocoran dokumen dan informasi-informasi penting terkait strategi, fakta pertahanan dan yang lainnya, bahkan apabila tersebar luas dikhawatirkan dapat mengancam pada cakupan yang lebih luas lagi yaitu pertahanan negara Indonesia.

Berkenaan dengan hal tersebut, peneliti menggali informasi mengenai langkah antisipatif yang telah dilakukan Seskoau dengan fokus pada aspek pencegahan kebocoran informasi, keamanan akses informasi, verifikasi kontak, mengikuti prosedur, pelaporan tindakan mencurigakan, menjaga emosi, pelatihan berkelanjutan, dan pemberian edukasi kepada perwira siswa negara sahabat (mancanegara).

a) Pencegahan Kebocoran Informasi

Berdasarkan hasil wawancara dengan Narasumber, diketahui bahwa pihak penyelengara pendidikan telah melakukan antisipasi dalam mencegah *Social Engineering Hacker* di Sekolah Staf dan Komando Angkatan Udara (Seskoau). Salah satu langkah yang telah ditempuh adalah dalam upaya pencegahan kebocoran informasi. Untuk mendapatkan informasi tersebut selanjutnya peneliti menanyakan kepada Narasumber terkait apakah seluruh pendidik di Sekolah Staf dan Komando Angkatan Udara (Seskoau) melakukan pencegahan kebocoran informasi terkait mata pelajaran rahasia sesuai Protap yang berlaku.

Berdasarkan hasil analisis yang telah peneliti lakukan terhadap ketiga Narasumber dalam kaitannya mencegah terjadinya kebocoran informasi, bahwa langkah awal yang dilakukan yaitu mengecek sumber kebocoran tersebut dan menutup akses tersebut. Hal tersebut sudah benar dilakukan oleh Narasumber ke 1, dengan tujuan agar tidak terjadi kebocoran yang lebih besar. Tindakan selanjutnya yaitu melakukan pemanggilan terhadap Pasis yang bersangkutan, yang selanjutnya diberikan edukasi dan pemahaman terkait pentingnya informasi tersebut. Apabila informasi tersebut sudah tersebar maka pihak dari Seskoau dapat melakukan operasi, hal ini bertujuan untuk memutus rantai informasi.

b) Keamanan Akses Informasi

Dalam hal penggalian informasi tentang langkah keamanan akses. Peneliti kemudian bertanya kepada Narasumber apakah seluruh pendidik di Sekolah Staf dan Komando Angkatan Udara

(Seskoau) menjaga keamanan akses informasi.

Bardasarkan hasil analisis informasi terkait keamanan akses informasi yang telah peneliti lakukan terhadap ketiga narasumber, bahwa tindakan menggunakan password, operasi intelijen, dan pemberian teguran-teguran merupakan salah satu langkah antisipasi agar social engineering ini tidak terjadi. Tindakan-tindakan tersebut harus selalu disosialisasikan terlebih lagi pada Pasis Indonesia yang memiliki keseringan dalam berinterkasi dengan Pasis negara sahabat. Terlebih lagi bagi mereka yang aktif dalam menggunakan jejaring media social.

c) *Verifikasi Kontak*

Verifikasi merupakan satu bentuk pengawasan terhadap suatu dokumen dengan berpedoman dan kriteria yang berlaku. Langkah selanjutnya yang dapat dikategorikan sebagai antisipasi terhadap ancaman *Social Engineering Hacker* adalah kegiatan verifikasi.

Hasil analisis informasi terhadap ketiga Narasumber dalam kaitannya dengan kegiatan verifikasi kontak, bahwa tindakan koordinasi merupakan langkah tepat yang dilakukan, dimana dalam proses tersebut update data akan dilakukan guna menghindari adanya kontak-kontak berlebihan yang tidak dikenal. Hal lainnya yang dapat dilakukan yaitu melalui verifikasi kontak terhadap Pasis negara sahabat.

d) *Mengikuti Prosedur*

Sebagaimana diketahui bahwa prosedur merupakan serangkaian aksi yang spesifik, tindakan atau operasi yang harus dijalankan atau dieksekusi dengan cara yang baku agar selalu memperoleh hasil yang sama dari keadaan yang sama. Mengikuti prosedur berarti mengikuti serangkaian kegiatan yang dijalankan dengan cara yang sama. Langkah mengikuti terhadap suatu prosedur dapat dilakukan, hal ini guna mengetahui apakah terdapat ancaman atau tidak pada suatu prosedur tetap.

Berdasarkan hasil analisis informasi terhadap ketiga Narasumber dalam kaitannya dengan prosedur, bahwa apa-apa yang sudah dilakukan baik oleh pihak pendidik, pihak staff penyelenggara, maupun oleh Pasis Indonesia sudah sesuai. Mayoritas dari mereka semua sudah mengikuti prosedur tetap tersebut. Prosedur tetap dapat dilaksanakan berdasarkan sosialisai yang mereka telah dapatkan sebelumnya. Meskipun demikian memang tidak seluruhnya perlu pengamanan dan sosialisasi terus menerus, yang terpenting adalah dalam hal penekanan yang dilakukan terhadap perlunya melaksankana prosedur tetap tersebut.

e) *Pelaporan Tindakan Mencurigakan*

Pelaporan terhadap suatu tindakan yang mencurigakan termasuk kedalam suatu langkah antisipatif dalam mencegah suatu ancaman yang datang. Seperti halnya ancaman *Social Engineering Hacker*, ancaman tersebut dapat diketahui apabila terdapat suatu laporan yang mencurigakan.

Berdasarkan informasi dari ketiga Narasumber, dapat dianalis kembali bahwa dalam kaitannya dengan pelaporan tindakan mencurigakan bahwa, langkah antisipasi yang dapat dilakukan

adalah sudah sesuai yaitu dengan melakukan pengecekkan terhadap sumber tindakan yang mencurigakan tersebut. Kemudian dilakukan tindakan isolasi disertai penyelidiakan lebih lanjut yang apabila ditemukan fakta kebocoran maka, secepatnya melakukan pelaporan secara bertahap atau berjenjang. Untuk tindakan pelaporan sudah sesuai prosedur yaitu melalui KORSIS yang kemudian dilanjutkan ke PAM dan POM Seskoau. Bahkan kalo diperlukan dapat dilaporkan ke kedutaan besar negara sahabat tersebut.

f) *Menjaga Emosi*

Ketidakmampuan mengontrol emosi dapat menjadikan suatu ancaman tertentu bagi suatu pihak. Atas dasar tersebut peneliti menggali informasi lebih lanjut terkait langkah antisipasi dalam mencegah *Social Engineering Hacker* dengan bertanya mengenai apakah seluruh pendidik di Sekolah Staf dan Komando Angkatan Udara (Seskoau) mampu menjaga emosi ketika ada Pasis negara sahabat (mancanegara) yang menanyakan detail terhadap mata pelajaran rahasia.

Berdasarkan hasil analisis informasi terhadap ketiga Narasumber penelitian bahwa, diketahui mayoritas dari para pendidik, staff pengajar dan pihak Pasis Indonesia mampu menjaga emosi masing-masing apabila ada Pasis negara sahabat (mancanegara) yang menanyakan detail terhadap mata pelajaran rahasia tersebut. Sebagian dari mereka lebih memilih bersabar dengan berusaha mengalihkan ke pembahasan yang lain dan ada juga sebagian yang menganggap hal tersebut sebagai sebuah wacana baru. Tindakan tersebut dirasa telah sesuai mengingat betapa besarnya tanggungjawab yang harus diterima apabila informasi tersebut bocor hingga sedetil-detilnya.

g) *Pelatihan Berkelanjutan*

Langkah antisipasi selanjutnya adalah fokus pada pelatihan yang berkelanjutan. Untuk mengetahui nya, peneliti langsung menanyakan kembali kepada Narasumber tentang apakah seluruh pendidik di Sekolah Staf dan Komando Angkatan Udara (Seskoau) memberikan pelatihan berkelanjutan kepada seluruh Pasis berdasarkan kurikulum pembelajaran Seskoau berdasarkan Kep. Kasau No. Kep/863/XI/2018.

Berdasarkan hasil analisis informasi yang telah peneliti lakukan terhadap ketiga peneliti dalam kaitannya dengan pelatihan berkelanjutan. Mayoritas Narasumber menganggap bahwa pelatihan berkelanjutan memang sangat sangat dibutuhkan, hal ini dapat membantu dalam pengerjaan tugas-tugas yang diberikan. Mayoritas dari Pasis Indonesia membutuhkan pelatihan-pelatihan yang terprogram bersama. Meskipun dalam pelaksanaannya harus selalu berinterkasi dengan Pasis negara sahabat, mereka tetap berkomitmen untuk melaksanakan Prosedur Tetap yang berlaku.

h) *Pemberian Edukasi Kepada Perwira Siswa Negara Sahabat (Mancanegara)*

Keberadaan edukasi sangat penting, karena dapat memberikan pengetahuan dan memberikan pencerahan. Lebih lanjut peneliti menggali informasi tentang bagaimana langkah edukasi yang

dilakukan di Seskoau terhadap ancaman dari adanya *Social Engineering Hacker*.

Berdasarkan hasil analisis informasi yang telah peneliti lakukan terhadap ketiga Narasumber dalam penelitian ini. Pemberian edukasi kepada Pasis negara sahabat selalu dilakukan. Edukasi diberikan berupa sosialisai dan pendampingan. Sosialisasi dilakukan pada saat dilakukannay apel pagi. Dalam sosialisi tersebut penting untuk disampaikan terkait hal-hal yang diperbolehkan dilakukan dan hal-hal yang tidak diperbolehkan dilakukan di lembaga. Hal ini dilakukan agar Pasis negara sahabat paham terhadap segala peraturan yang berlaku selama mengikuti pendidikan di Seskoau.

B. Pembahasan

Berdasarkan hasil wawancara yang telah dilakukan terhadap 3 Narasumber, maka dapat dijelaskan kembali bahwa secara umum terdapat ancaman *Social Engineering Hacker* pada mata pelajaran rahasia di Seskoau.

Ancaman *social engineering Hacker* dapat terjadi ketika didapatinya suatu kesalahan, yang mana kesalahan tersebut biasanya di eksploitasi oleh *hacker* dengan menggunakan *social engineering*. Ada beberapa cara/teknik dalam mengeksploitasi suatu kesalahan/kelemahan, diantaranya: *Hacker* memanfaatkan rasa takut calon korban, kejadian ini terjadi jika seseorang dimintai data atau informasi dari atasannya, biasanya yang bersangkutan akan langsung memberikan tanpa merasa sungkan. Kemudian *Hacker* memanfaatkan rasa percaya calon korban, kejadian ini terjadi jika seorang individu dimintai data atau informasi dari teman baik, atau rekan sejawat, biasanya yang bersangkutan akan langsung memberikannya tanpa harus merasa curiga, dan biasanya *Hacker* memanfaatkan ketika muncul rasa ingin menolong, kejadian ini terjadi jika seseorang dimintai data atau informasi dari orang yang sedang tertimpa musibah, dalam kesedihan yang mendalam, menjadi korban bencana, atau berada dalam duka, biasanya yang bersangkutan akan langsung memberikan data atau informasi yang diinginkan tanpa bertanya lebih dahulu. Seorang *Hacker* akan mengeksploarasi tentang tipe penyerangan ini dengan cara menganalisa, mengumpulkan literatur, dan mencari permasalahan yang pernah terjadi, agar dapat memberi informasi. Setelah mengetahui faktor-faktor ancaman dari kegiatan *social engineering*. Selanjutnya dibutuhkan pemahaman yang kuat agar dapat terhindar dari *Social Engineering* tersebut, diantaranya: jika dulu *hacker* berusaha menyerang targetnya hanya dibalik komputer melalui jaringan internet, sekarang ini mereka memiliki cara lain yang memungkinkan bagi mereka untuk dapat mengakses sistem yang menjadi sasaran mereka tanpa mengandalkan seluruh kemampuan technical yang dimiliki. Kemudian bahwa sebagian besar korban belum mengenal tentang *social engineering* karena faktor sulitnya untuk mengidentifikasi sebuah insiden yang terjadi dalam keamanan sebagai akibat dari social engineering. Kesulitan untuk mengidentifikasi insiden yang disebabkan oleh *social engineering* juga sering diakibatkan karena user yang menjadi korban jarang yang mau melaporkan insiden tersebut, karena sebab utama dari terjadinya insiden tersebut dikarenakan karena kesalahan user itu sendiri. Selanjutnya adalah meningkatkan kewaspadaan dengan

memberi pemahaman yang jelas mengenai *social engineering* dan ancaman yang dapat ditimbulkannya. Dengan adanya pemahaman mengenai *social engineering* diharapkan masyarakat dapat lebih waspada akan adanya ancaman yang nyata ini.

Setelah mengetahui ancaman dan memahami bagaimana *social engineering* dapat terjadi, langkah-langkah antisipatif harus dilakukan guna menghindari dan meminimalisir dampak yang dapat ditimbulkan dari kejahatan *social engineering* tersebut. Untuk mengurangi resiko tersebut, maka perlu dilakukan sosialisasi dan pelatihan berkelanjutan terhadap sumber daya-sumber daya terkait mengenai ancaman keamanan dan bagaimana caranya mengenali dan mengantisipasi serangan *Social Engineering* tersebut. Menurut peneliti ada beberapa hal yang dapat dilakukan untuk mencegah dampak *social engineering*, diantaranya melakukan langkah antisipatif melalui mencegah kebocoran *password*, selalu meningkatkan keamanan akses informasi, melakukan langkah-langkah dalam memverifikasi kontak yang dimiliki, selalu taat dan patuh dalam mengikuti prosedur, cepat tanggap dalam melakukan pelaporan apabila ditemukan tindakan-tindakan yang mencurigakan, selalu menjaga emosi apabila menghadapi suatu masalah yang membutuhkan kesabaran yang tinggi, tetap memberikan pelatihan-pelatihan yang sifatnya berkelanjutan, dan selalu memberikan edukasi bagi pihak-pihak terkait, agar langkah antisipatisi ini dapat terlaksana dengan baik.

Hal lainnya yang dapat dilakukan untuk menanggulangi masalah seperti ini adalah dengan cara meningkatkan kesadaran dari berbagai pihak terkait (staff/pengguna) mengenai social engineering dan ancamannya. Selain itu instansi juga harus memiliki dokumen resmi yang jelas berupa standar, prosedur, atau kebijakan mengenai keamanan informasi, sehingga pihak terkait (staff/pengguna) dapat mengikuti, mematuhi, dan selalu menjadikan dokumen resmi tersebut sebagai acuan atas segala tindakan yang dilakukan di perusahaan tersebut.

KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan terkait ancaman, implementasi dan langkah antisipasi terhadap *Social Engineering Hacker* di Sekolah Staf dan Komando Angkatan Udara (Seskoau). Selanjutnya peneliti berkesimpulan terdapat ancaman *Social Engineering Hacker* di Sekolah Staf dan Komando Angkatan Udara (Seskoau) yang terindikasi dari seringnya interaksi melalui jejaring media sosial, adanya sebagian dari Pasis negara sahabat yang menanyakan mata pelajaran rahasia, timbulnya rasa percaya terhadap kemampuan yang dimiliki Pasis negara sahabat, dan munculnya rasa khawatir yang dirasakan oleh apabila ada Pasis negara sahabat yang menanyakan mata pelajaran rahasia. Kemudian dalam hal pemahaman terhadap Prosedur Tetap (Protap) No. Kep/32/V/2020, mayoritas pendidik, staff penyelenggara dan Pasis Indonesia telah memahami. Namun demikian tidak semua Pasis Indonesia memahami konsep dan hakekat dari Prosedur Tetap (Protap) tersebut.

Selanjutnya mengenai langkah antisipasi yang telah dilakukan dalam hal pencegahan ancaman *Social Engineering Hacker* meliputi: melakukan pengecekan sumber kebocoran dan melakukan penutupan akses informasi jika terjadi kebocoran, melakukan pemanggilan terhadap Pasis yang mencurigakan/ membuat suatu kebocoran informasi, melakukan kegiatan operasi/ intelijen, pengalihan bahasan materi, ketika terindikasi adanya hal yang

mencurigakan, membatasi penggunaan medsos dalam pelajaran, tidak memberikan materi atau informasi-informasi yang terkait dengan Doktrin, tidak mendiskusikan, men-share mata pelajaran rahasia pada siswa asing, disiplin dalam menggunakan password, memberikan peringatan/ teguran, tidak membocorkan informasi-informasi apapun, terlebih lagi informasi tersebut merupakan informasi yang sifatnya rahasia, selektif dalam berbicara dengan Pasis negara sahabat, selektif dalam mengupload pelajaran ke berbagai media, membuat folder khusus dalam penyimpanan file di komputer atau di laptop, mengurangi kontak berlebihan dengan Pasis negara sahabat, berkomitmen untuk selalu mengikuti prosedur tetap yang berlaku, senantiasa melakukan pengecekan sumber tindakan yang mencurigakan, yang ditindaklanjuti dengan tindakan isolasi dan melakukan penyelidikan, membuat laporan secara berjenjang melalui korsis, PAM dan POM, dan melaporkan secepatnya kepada pihak intel lembaga.

DAFTAR PUSTAKA

A’raf, A. (2015). Dinamika Keamanan Nasional. *Jurnal Keamanan Nasional. Vol. I No. 1*.

Abass, I. A. (2018). Social Engineering Threat and Defense: A Literature Survey. *Journal of Information Security. Department of Computer Science, Al Jouf University, Al-Jawf, KSA, 9*(: 2153-1242), 257-264.

Akbar, S., Rabi', A., Minggu, D., & Mujahidin, I. (2019). Frequency Hopping Video Real Time Untuk Pengamanan Data Pengintaian Operasi Inteligence TNI. *JASIEK, Vol.1, No.1*, pp. 19~27.

aliyhafiz.com. (2020, 02 15). *Social Engineering, Pengertian, Langkah-Langkah, Dan Cara Menghindarinya*. Retrieved 12 30, 2020, from https://aliyhafiz.com/social-engineering/#Pengertian_Social_Engineering

Allen, M. (2001). *Social Engineering: A Means To Violate A Computer System.* https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529.

Buzan, B. G. (1991). *People, States and Fear: an Agenda for International Security Studies in the Post-Cold War.* Boulder: Lynne Rienner Publisher.

Buzan, B. G. (March 1997). Rethinking Security after the Cold War. *JSTOR - Cooperation and Conflict, 32, No.1*(Sage Publications, Ltd.), pp. 5-28.

CERT-UK. (2015). *An Introduction to social engineering.* A CERT-UK PUBLICATION.

Chalk, P. (2000). Non-Military Security And Global Order. The Impact of Extremism, Violence and Chaos on National and International Security. https://www.palgrave.com/gp/book/9780333773734.

Cooper, P. K. (2017). Organizational Security Threats Related Toportable Data Storage Devices: Qualitative Exploratory Inquiry. *Dissertation Presented in Partial Fulfillment. University of Phoenix. ProQuest 10265419.* ProQuest LLC.

Februariyanti, H. (2006). Standar dan Manajemen Keamanan Komputer. *Jurnal Teknologi Informasi DINAMIK Volume XI, No. 2,* 134-142. ISSN: 0854-9524.

Gollmann, D. (2011). *Computer Security THIRD EDITION.* Hamburg

University of Technology: A John Wiley and Sons, Ltd., Publication.

Gondohanindijo, J. (2010, 03 24). Pengamanan Sistem Berkas. *Majalah Ilmiah Informatika. Fakultas Ilmu Komputer Universitas AKI, 1 No.2*, 24. Retrieved 11 30, 2020, from Keamanan Informasi - BPPTIK: https://bpptik.kominfo.go.id/2014/03/24/404/keamanan-informasi/

Haftendorn, H. (1991). The Security Puzzle: Theory-Building and Discipline-Building in International Security. *International Studies Quarterly, 35, No.1*(https://doi.org/10.2307/2600386), 3-17.

Herjanto, E., & Kristiningrum, E. (2006). KAJIAN STANDAR BIDANG KEAMANAN. *Jurnal Standardisasi Vol. 8 No. 1*, 18-26.

Hough, P., Moran, A., Pilbeam, B., & Stokes, W. (2020). *International Security Studies. Theory and Practice. 2nd Edition.* London: eBook Published 5 August 2020.

Lubis, N. L., & Hasnida. (2011). *Memahami Dasar- Dasar Konseling dalam Terori dan Praktik.* Jakarta: Kencana, Hal. 243.

Perwita, A. A. (2006). *Hakikat Prinsip dan Tujuan Pertahanan-Keamanan Negara, dalam Tim Propatria Institute, Mencari Format Komprehensif Sistem Pertahanan dan Keamanan Negara.* Jakarta: Propatria.

Perwita, A. A. (2008). *Dinamika Keamanan Dalam Hubungan Internasional Dan Implikasinya Bagi Indonesia.* Bandung: Universitas Katolik Parahyangan.

Prayitno, H., & Amti, E. (2004). *Dasar-Dasar Bimbingan dan Konseling.* Jakarta: Rineka Cipta.

Rafizan, O. (2011). *ANALISIS PENYERANGAN SOCIAL ENGINEERING.* https://mti.kominfo.go.id/index.php/mti/article/view/26/23: Jurnal Penelitian Teknologi Informasi dan Komunikasi Vol 2 No.2. Retrieved from https://media.neliti.com/media/publications/233773-analisis-penyerangan-social-engineering-26c4bb1f.pdf

Seskoau. (2020). Prosedur Tetap Tentang Mata Pelajaran Seskoau Yang Tidak Diikuti Oleh Pasis Negara Sahabat. Lembang, Kab.Bandung Barat: Markas Besar Angkatan Udara Sekolah Staf dan Komando.

Sitepu, A. P. (2011). *Studi Hubungan Internasional.* Yogyakarta: GRAHA ILMU.

Spears, P. D. (2013). Education And The Degree Of Data Security. *A Dissertation Presented in Partial Fulfillment. Capella University. UMI 3610702.* ProQuest LL.

Suherman, Widodo, P., & Gunawan, D. (2017). Efektivitas Keamanan Informasi Dalam Menghadapi Bahaya Social Engineering. *Jurnal Prodi Peperangan Asimetris, 3, No.1*, 73-90.

Susetyo, H. (2008). Menuju Paradigma Keamanan Komprehensif Berperspektif Keamanan Manusia dalam Kebijakan Keamanan Nasional. *Lex Jurnalica, 6 No.1*, 2.

Ullman, R. H. (1983). Redefining Security. *International Security The MIT Press, 8, Number 1, Summer*(pp. 129-153), 129.

Velicia, V., Wisanjaya, I., & Widiatedja, I. (2015). Perlindungan Hukum Terhadap Indonesia Dalam Kasus Penyadapan Oleh Australia. *Program Kekhususan Hukum Internasional dan Hukum Bisnis*

Internasional Fakultas Hukum Universitas Udayana. *ojs.unud.ac.id*.