ANALISIS EVALUASI KEBIJAKAN PADA CYBER SECURITY PERBANKAN

Dewi Chirzah[1*], Evendi Yudhi Al-Fadli[2]

[1*]Program Studi Sains Data, Institut Teknologi Bisnis dan Kesehatan, Indonesia

[2]Program Studi Teknik Informatika, Universitas Perwira Purbalingga, Indonesia

[1*]dewi.chirzah@ibisa.ac.id

[2]yudhi.daily46@gmail.com

ABSTRAK

Bank menurut UU No.10 1998 merupakan lembaga lembaga perantara keuangan yang bertugas menghimpun dan menyalurkan dana masyarakat dalam rangka meningkatkan taraf hidup banyak orang. Dalam rangka penyimpanan informasi dan data yang ada di bank diperlukan adanya cyber security karna perkembangan teknologi yang makin pesat membuat kejahatan siber itu ada. Dalam meningkatkan cyber security di perlukan adanya kebijakan agar tersetruktur dalam pemilihan teknologi yang akan di usung dalam peningkatan cyber security. Setelah kebijakan itu di usung perlu adanya evaluasi kebijakan agar bisa melihat ke efektifnya. Dalam review jurnal ini penulis melakukan review pada kejahatan siber pada sektor perbankan, teknologi yang dipakai dalam kebijakan meningkatkan cyber security pada perbankan, upaya pencegahan yang ada. Dari analisis evaluasi yang ada setiap perbankan memiliki kebijakan sendiri dalam menangani kejahatan siber dan juga setiap teknologi yang dipilih pasti memiliki sebuah celah yang bisa di manfaatkan oleh para pelaku kejahatan siber.

Kata Kunci: Cyber security, Perbankan, Kejahatan siber, Evaluasi, Kebijakan

ABSTRACT

Bank according to Law No. 10 1998 is a financial intermediary institution whose job is to collect and distribute public funds in order to improve the standard of living of many people. In order to store information and data in banks, it is necessary to have cyber security because the rapid development of technology makes cybercrime exist. In improving cyber security, it is necessary to have a policy so that it is structured in the selection of technology that will be carried out in improving cyber security. After the policy has been stretched, it is necessary to evaluate the policy in order to see how effective it is. In this journal review, the authors review cybercrime in the banking sector, the technology used in policies to improve cyber security in banking, existing prevention efforts. From the existing evaluation analysis, each bank has its own policy in dealing with cybercrime and also every technology chosen must have a loophole that can be exploited by cybercriminals.

Keywords: Cyber security, Banking, Cybercrime, Evaluation, Policy

PENDAHULUAN

Era digital berjalan seiring dengan ancaman kejahatan *siber* yang selalu mengintai, selalu berkembang dan memanfaatkan celah. Industri perbankan kemudian menyadari bahwa penilaian berkala diperlukan untuk memahami di mana ada kesenjangan. Oleh karena itu, industri perbankan Indonesia, harus memanfaatkan teknologi terkini untuk mengelola risiko kejahatan *siber*. Dengan meningkatkan *cyber security* dapat meminimalisirkan kejahatan *siber* yang mengintai perbankan yang ada di Indonesia.

Perbankan adalah segala sesuatu yang berkaitan dengan perbankan yang meliputi lembaga, kegiatan usaha, serta cara dan proses penyelenggaraan kegiatan usaha. Pengertian Bank dalam UU No.10 1998 merupakan lembaga lembaga perantara keuangan yang bertugas menghimpun dan menyalurkan dana masyarakat dalam rangka meningkatkan taraf hidup banyak orang (Hadi Ismanto & Harjum Muharam, 2019). Mengenai perlindungan dan tata kelola data, kami menerapkan tata kelola berdasarkan standar internasional. Selain itu, setiap teknologi memiliki serangkaian pemeriksaan keamanan langkah demi langkah yang digunakan untuk meminimalkan pelanggaran keamanan. Lakukan segala upaya untuk memastikan keamanan Data Pelanggan dalam hal orang, proses, dan teknologi.

Tata kelola keamanan informasi mengacu pada aspek teknis itu sendiri, dan telah mengembangkan teknologi keamanan informasi yang tepat. Hal ini pun dilakukan dengan tujuan untuk meminimalisir risiko kebocoran data nasabah dengan mencegah, mendeteksi, dan melakukan monitor terhadap ancaman kejahatan *siber*.

Analisis ini bertujuan untuk menganalisis kebijakan *cyber security* pada perbankan berdasarkan analisis awal peneliti di temukan bahwa seringkali kebijakan *cyber security* menjadi multitafsir. Selanjutnya penelitian ini berupaya untuk memberikan suatu strategi tentang upaya yang dilakukan mempersempit ruang gerak kejahatan *siber* yang merupakan implikasi dari *cyber security*.

TINJAUAN PUSTAKA

A. Kebijakan

Kebijakan adalah variabel paling krusial yang pengaruhnya sangat besar dalam penyelesaian setiap masalah publik. Implementasi juga menjadi pembuktian apakah pemerintah memiliki respon dan cara yang tepat dalam merangkul kepentingan masyarakat. Sedangkan evaluasi kebijakan merupakan akhir dari tahapan kebijakan. Pada tahap ini dapat dilihat bagaimana implementasi kebijakan, kerugian, manfaat dan hasil dari kebijakan yang diterapkan tersebut positif atau negatif. Evaluasi juga menjadi tolak ukur terhadap kebijakan-kebijakan selanjutnya yang akan diambil pemerintah atau pelaksana (Permatasari, 2020).

B. Cyber Security

Cybersecurity adalah kegiatan untuk melindungi sistem komputer seperti program aplikasi dan data serta informasi yang ada dari berbagai serangan dan akses yang tidak sah. Tindakan keamanan *siber* ini mencakup alat, kebijakan, konsep keamanan, dll, yang dapat digunakan untuk melindungi organisasi, dan asset pengguna. Untuk menerapkan *Cyber security* di lingkungan Organisasi/Yayasan anda dibutuhkan biaya/anggran yang tidak sedikit dengan kata lain bahwa, untuk menerapkan *cyber security* perusahaan/organisasi harus

memiliki budget atau anggaran yang besar dan mencatatnya di dalam laporan keuangan secara tepat (Marcelina, Suryati, & Yulianti, 2022)

C. Evaluasi

Evaluasi merupakan bagian penting dari sistem pendidikan dan pengajaran dalam berbagai bentuk dan waktu pengajarannya. Istilah evaluasi pemakaiannya sering di pertukarkan karena konsep yang mendasarinya kurang di pahami oleh penggunannya. Istilah yang dimaksud adalah penilaian, pengukuran dan tes. Dengan demikian, konsep-konsep dasar yang terkait langsung perlu diketahui oleh setiap pembelajar. Evaluasi/ penilaian pada dasarnya bertujuan menentukan evektivitas dan evisiensi kegiatan pembelajaran dengan indikator utama pada keberhasilan atau kegiatan pembelajar dalam mencapai tujuantujuan pembelajaran yang di tetapkan (Suardipa & Primayana, 2020).

D. Kejahatan Siber

Kejahatan siber adalah jenis kejahatan yang terkait dengan penggunaan teknologi informasi yang tidak terkendali dan ditandai dengan metode teknologi yang mengandalkan tingkat keamanan dan keandalan yang tinggi dari informasi yang dikirimkan dan diakses oleh konsumen *internet*. (Suharto & Apriyani, 2021).

METODE PENELITIAN

Penelitian kualitatif merupakan suatu pendekatan dalam melakukan penelitian yang berorientasi pada fenomena atau gejala alam. Penelitian kualitatif bersifat *fundamental* dan naturalistik, dan tidak dapat dilakukan di laboratorium, melainkan di lapangan. Oleh karena itu, penelitian semacam ini sering disebut penyelidikan naturalistik, atau studi lapangan (Dr. H. Zuchri Abdussamad, 2021). Jadi penulis menggunakan cara mengumpulkan dan *mereview* jurnal yang sudah ada, agar bisa melakukan penganalisisan evaluasi yang di lakukan oleh perbankan.

HASIL DAN PEMBAHASAN

Dari beberapa jurnal yang telah penulis dapatkan, penulis membuat *review* mengenai 3 jurnal yang memiliki topik mengenai evaluasi kebijakan *cyber security* pada sektor perbankan. Jurnal pertama berjudul "Evaluasi Kebijakan Cyber Security Sektor Perbankan Bank BTN Cabang Surabaya". Jurnal ini memaparkan evaluasi kebijakan keamanan *siber* Bank BTN cabang Surabaya. Dalam evaluasinya dilakukan dalam 2 minggu sekali dan hasilnya bisa dikatakan sangata baik karna mengambil Langkah *prefentiv* dalam menyikapi dan pencegahan terhadap kejahatan *siber* yang mungkin bisa menyerang sektor perbankan.

Jurnal kedua berjudul "Penyusunan Kebijakan Kebijakan Teknologi Informasi Pada Transaksi Elektronik *Banking* Perbankan Umum Berdasarkan Peraturan Bank Indonesia 9/15/*PBI*/2007 Dengan Menggunakan *Matriks Cobit* 4.1 Dan *ISO*/*IEC* 27000". Jurnal kedua ini membahas tentang evaluasi kebijakan teknologi informasi di sektor perbankan mengenai transaksi elektronik bankingnya. Dalam evaluasianya menggunakan *Matriks Cobit* 4.1 dan *ISO/IEC* 27000. Hasil penelitian menemukan bahwa dalam penerapanya terdapat resiko kejahatan *siber* yang masih bisa mengintai walaupun teknologi tersebut telah di terapkan.

Jurnal ketiga berjudul "*Re-Assessment* Konsistensi Dokumen Kontrol Sertifikasi *ISO* 27001:2013 (*ISMS*) di Bagian Komunikasi Satelit *Monitoring* PT. Bank BRI, TBK". Jurnal

ketiga ini membahas mengenai evaluasi dan konsultasi mengenai cyber security yang telah diterapkan untuk *memonitoring* komunikasi satelit dengan menggunakan teknologi *ISO* 27001:2013. Hasil evaluasinya dalam kebijakan tersebut harus di kaji ulang dalam rangka peningkatan *cyber security* yang ada di PT. Bank BRI.

Dari beberapa jurnal diatas, penulis mengambil poin poin yang terkait mengenai analisis evaluasi kebijakan *cyber security* pada sektor perbankan. Berikut adalah poin poin dari ketiga jurnal diatas :

1. Data kejahatan siber yang sedang trend pada sektor perbankan

Tabel 1. Jumlah Kejahatan *Siber* Trend Pada Perbankan

Jumlah Penipuan *Daring*	Aksi *Ilegal*	Tahun
1430	153	2017
1781	263	2018
1617	248	2019
1319	303	2020
508	167	2021

Sumber: (Rudiatno & Cheryta, 2022)

Dari data yang didapatkan, total kejahatan siber yang sedang trend pada sektor perbankan, dari tahun ketahun naik turun tidak setabil itu menandakan bahwa *cyber security* di Indonesia masih perlu di tingkatkan agar kejahatan di sektor perbankan semakin menurun.

2. Perbedan *ISO/IEC* 27001: 2013 dengan *ISO* 27000

Dari jurnal di atas dalam melakukan peningkatan *cyber security* dalam bidang monitoring komunikasi satelit perbankan agar meningkatnya keamanan informasi nasabah maupun dari pihak bank.

Tabel 2. ISO/IEC 27001: 2013 dan ISO 27000

No.	ISO/IEC 27001: 2013	ISO 27000
K1	Ruang Lingkup Standar	*Security Policy*
K2	Referensi Normatif	*Organization of information security*
K3	Ketentuan dan Definisi	*asset Management*
K4	Konteks Organisasi	*Human Resources Security*
K5	Kepemimpinan	*Physical & Environmental security*
K6	Perencanan	*Communication & Operation Management*
K7	Pendukung	*Access Control*
K8	Operasi	*Information Systems Acquisition, Development & Maintenance*
K9	Evaluasi Kinerja	*Information Security Incident Management*
K10	Peringkat	*Business Continuity Management*
K11		*Compline*

Sumber: (Hariman, 2018), (Sigit Tri Yuwono, 2022)

Dalam perbedan penggunan *ISO* terdapat perbedan yaitu Memiliki kelebihan satu dalam kausal dan perencanan karna dalam perencanan *ISO/IEC* 27001: 2013 hanya ada 4

sedangakan *ISO* 27000 ada 5 perencanan. Jadi dalam tahap pengevaluasianya akan ada beberapa Langkah yang berbeda.

3. Upaya Pencegahan kejahatan siber pada sektor perbankan

   Kejahatan *siber* merupakan hal yang tidak bisa dihindari dan terus berkembang mengikuti teknologi yang ada, strategi kebijakan terkait *cyber security* (Rudiatno & Cheryta, 2022) sebagai berikut:

   1. Membuka akses informasi dan ketersediaan jaringan yang baik;
   2. Bekerjasama dengan kemanan *cyber* luar negeri;
   3. Mengakomodasi *programmer local*;
   4. Meningkatkan alokasi anggaran dan focus pada peningkatan *cyber security*;
   5. Memperkuat seluruh institusi pemerintah dan menyiapkan ahli keamanan *cyber* di setiap posisi Lembaga pemerintah.

   Beberapa strategi tersebut setidaknya ditujukan untuk membendung kejahatan siber berskala besar yang terjadi di Indonesia kususnya pada sektor perbankan.Tentunya celah bagi para pelaku kejahatan siber untuk melakukan aksi dapat dikendalikan dan dipersempit oleh pemerintah.

KESIMPULAN

Dari analisis yang telah dilakukan, bahwa cara yang di lakukan setiap perbankan memiliki kebijakan tersendiri dalam melakukan penanganan kejahatan *siber,* oleh karna itu teknologi yang di usung dalam upayanya pun berbeda. Terbukti dari data yang didapatkan, kasus kejahatan *siber* terus ada dengan adanya naik turun dalam kasus kejahatan *siber* pada sektor perbankan dengan berbagai macam bentuk serangan. Hal inilah yang membuat perlu adanya kesadaran mengenai *cyber security* dan upaya pencegahan dari kejahatan *siber* dari masa ke masa, karna teknologi semakin canggih otomatis cara untuk melakukan kejahatan *siber* semakin canggih.

DAFTAR PUSTAKA

Dr. H. Zuchri Abdussamad, S. M. (2021). *Metode Penelitian Kualitatif.* Indonesia: CV. Syakir Media Press.

Hadi Ismanto, A. W. (2009). *Perbankan Dan Literasi Keuangan.* Yogyakarta, Sleman: Grup Penerbitan CV BUDI UTAMA.

Hadi Ismanto, A. W., & Harjum Muharam, I. R. (2019). *Perbankan Dan Literasi Keuangan.* Yogyakarta: Grup Penerbitan CV BUDI UTAMA.

Hariman, R. I. (2018). Penyusunan Kebijakan Keamanan Teknologi Informasi Pada Transaksi Electronic Banking Perbankan Umum Berdasarkan Peraturan Bank Indonesia Nomor 9/15/PBI/2007 Dengan Menggunakan Matriks Cobit 4.1 Dan ISO/IEC 27000. *Syntax Literate : JurnalIlmiah Indonesia –ISSN : 2541-0849 e-ISSN : 2548-1398*, 99-111.

Marcelina, D., Suryati, & Yulianti, E. (2022). Workshop Teknologi Informasi "Dasar Cyber Security" Pada SMK PGRI Tanjung Raja Ogan Ilir (OI). *JURNAL ABDIMAS MANDIRI VOLUME 6 No. 2* , 67-72.

Permatasari, I. A. (2020). Kebijakan Publik (Teori, Analisis, Implementasi dan Evaluasi Kebijakan). In A. M. Dr. Drs. Chazali H. Situmorang, *Kebijakan Publik (Teori,*

Analisis, Implementasi dan Evaluasi Kebijakan) (pp. 34-38). Yogyakarat: CV. The Journal Publishing.

Rudiatno, & Cheryta, A. M. (2022). Evaluasi Kebijakan Cyber Security Sektor Perbankan Bank BTN Cabang Surabaya. *e-Jurnal Apresiasi Ekonomi Volume 10, Nomor 3*, 321-331.

Sigit Tri Yuwono, N. P. (2022). Re-Assessment Konsistensi Dokumen Kontrol Sertifikasi ISO 27001:2013 (ISMS) di Bagian Komunikasi Satelit Monitoring PT. Bank BRI, TBK. *Jurnal IKRAITH-INFORMATIKA Vol 6 No 2*, 21-28.

Suardipa, I. P., & Primayana, K. H. (2020). Peran Desain Evaluasi Pembelajaran Untuk Meningkatkan Kualitas Pembelajaran. *Jurnal Widya Carya*, 88-100.

Suharto, M. A., & Apriyani, M. N. (2021). Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional. *Jurnal RisalahHukum, Volume 17, Nomor 2*, 98-107.