Tugas Keamanan Jaringan Informasi

T U GA S

Disusun untuk Memenuhi Tugas Kelompok

pada Mata Keamanan dan Jaminan Informasi yang Diampu oleh Bapak Priyo Sidik Sasongko,S.SI,M.Kom

Disusun oleh :

Sulthan Aulia Fadli	**(24060118140059)**
Sherly Michaelia	**(24060118140137)**
Auliya Daffa Isy	**(24060118140140)**
Syifa Azzahra	**(24060118130149)**

PROGRAM STUDI INFORMATIKA

FAKULTAS SAINS DAN MATEMATIKA

UNIVERSITAS DIPONEGORO

SEMARANG

2021

- Studi Kasus 1 : Kasus Bocornya Data 279 Juta WNI di BPJS Kesehatan
    1. Analisis Kelemahan dan ancaman

        Setelah mengkonfirmasi, BPJS Kesehatan mengakui kebocoran data 279 juta warga Indonesia. Menurut dirut, kebocoran data terjadi akibat adanya tindakan peretasan sistem keamanan digital. Menurut Dirut BPJS Kesehatan, dinamisnya dunia digital membuat kelompok tertentu yang tidak bertanggung jawab bisa membobol data pribadi yang terhimpun melalui platform digital, seperti BPJS Kesehatan. Menurut Kominfo, sampel data pribadi yang beredar telah diinvestigasi sejak 20 Mei 2021. Lalu berdasarkan hasil investigasi, Kominfo menemukan bahwa akun bernama Kotz menjual data pribadi di Raid Forums. Akun Kotz sendiri merupakan pembeli dan penjual data pribadi (reseller).

    2. Pengukuran Kendali atas ancaman

        BPJS Kesehatan mengimplementasikan control objectives for information technologies atau COBIT, serta menjalankan security operation center atau SOC yang bekerja selama 24 jam dalam tujuh hari untuk melakukan pengamatan jika ada yang mencurigakan. Pihak BPJS mengklaim bahwa sistem keamanan teknologi informasi di BPJS kesehatan sangat dijaga keamanannya, walaupun BPJS Kesehatan sudah melakukan sistem keamanan sesuai standar yang berlaku namun masih dimungkinkan terjadinya peretasan mengingat sangat beresikonya dunia peretasan.

    3. Penilaian Efektivitas pengendalian ancaman

        Ada beberapa faktor kebocoran data BPJS, mencakup masalah dana, peralatan dan sumber daya manusia. BPJS harus segera melakukan tindakan terhadap hal - hal tersebut.

        Indonesian Digital Empowering Community (IDIEC) menilai sistem keamanan data yang diterapkan oleh Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan bermutu rendah, seandainya kabar mengenai kebocoran data di lembaga tersebut benar adanya. Ketua Umum Indonesian Digital Empowering Community (IDIEC) M. Tesar Sandikapura mengatakan

ISO27001 yang diterapkan BPJS Kesehatan tidak dapat menjamin sebuah perusahaan aman dari serangan siber. Standar ISO hanya menegaskan bahwa perusahaan atau lembaga pemerintah yang telah mendapatkan sertifikasi, seharusnya telah menerapkan standar operasional keamanan yang ketat. Hal ini membuktikan pihak BPJS tidak efektif dalam upaya pengamanan data.

4. Langkah-langkah investigasi kejadian/kecelakaan

Badan Penyelenggara Jaminan Sosial atau BPJS Kesehatan mulai melakukan tindakan sejak Kamis (20/5/21). Pada Jumat (21/5/2021), direksi melakukan koordinasi dengan Dewan Pengawas BPJS Kesehatan, Badan Sandi dan Siber Negara (BSSN), Kementerian Komunikasi dan Informatika (Kemkominfo), Kementerian Pertahanan (Kemenhan), dan PT Sigma Cipta Caraka (Telkom Sigma). Selain melakukan investigasi dan penelusuran jejak digital, saat ini BPJS juga melakukan mitigasi terhadap hal-hal yang mengganggu keamanan data dalam proses pelayanan dan administrasi.

5. Langkah-langkah pemulihan kecelakaan/kejadian

Untuk membuktikan kebenaran data dari 279 juta, si pengunggah data bahkan memberikan sampel berisi 1 juta data penduduk Indonesia. Sampel tersebut diunggah ke laman berbagi file bayfiles, anonfiles, dan mega. Juga melakukan konfirmasi, siapa yang mengoperasikan data lanjut digital forensik dan melakukan penguatan sistem keamanan teknologi informasi terhadap potensi gangguan keamanan data, antara lain meningkatkan proteksi dan ketahanan sistem.

Juga menindaklanjuti secara hukum dengan melalui UU ITE, namun harus melibatkan delik pelaporan dari pemilik data pribadi (WNI) yang merasa dirugikan. Sanksi paling berat adalah pencabutan ijin Penyelenggaraan Sistem Elektronik (PSE) BPJS Kesehatan oleh Kemenkominfo. RUU PDP segera disahkan, data kesehatan WNI sangat penting dan rahasia. Harus dijaga dengan ekstra ketat tidak boleh bocor sekecil apa pun.

6. Resiko
    a. Resiko terhadap keamanan nasional, karena sebagian besar data kependudukan termasuk TNI Polri dan semuanya ada di sana, dan jika memang benar data itu yang dimiliki dan sesuai dengan kenyataan maka resiko keamanan nasional akan semakin terlihat.
    b. Resiko terhadap reputasi pelaksanaan jaminan kesehatan nasional, ini tentunya akan kontraproduktif jika dihadapkan dengan keinginan pemerintah untuk semakin memantapkan peran jaminan kesehatan nasional sebagai bagian dari pembangunan kesehatan secara nasional.
    c. Seluruh data yang ada pada internal BPJS kesehatan juga berisiko diintervensi dari pusat hingga ke kantor cabang.

- Studi Kasus 2: Viral Uang Nasabah Bank Mandiri Raib Rp 128 Juta
    1. Analisis Kelemahan dan ancaman

        Seorang nasabah bank mandiri mengaku bahwa uangnya raib Rp 128 Juta. Hal tersebut dialami oleh nasabah bernama Asrizal Askha. Berdasarkan keterangannya, itu terjadi pada 5 Februari 2021.Setelah dilakukan pengecekan Bank Mandir mengatakan ke OJK bahwa transaksi yang menyebabkan uangnya raib sah. Tidak ada penjelasan mengenai investigasinya. Tapi dia keberatan dengan pernyataan Bank Mandiri.

        Sesuai rekaman pengaduan nasabah ke call center 14000, pihak Bank Mandiri memperkirakan nasabah telah menjadi korban kejahatan dengan modus penukaran kartu debit dan penguasaan PIN. Sebab, kartu debit yang dipegang nasabah berbeda dengan kartu debit yang terdaftar di Bank Mandiri. Sedangkan kartu yang dipakai bertransaksi tidak lagi dalam penguasaan nasabah.

    2. Pengukuran Kendali atas ancaman

        Dengan adanya kasus hilangnya uang, bank mandiri terus berupaya meningkatkan kualitas layanan secara online di tengah kampanye pembatasan aktivitas sosial akibat pandemi corona. Sehingga dengan hanya di rumah pun, masyarakat tidak terkendala saat membutuhkan layanan perbankan. Bank

mandiri juga terus meningkatkan fitur layanan Mandiri Mobile Online. Yang terbaru, proses mengembangkan layanan pembukaan rekening secara daring (online) agar dapat meningkatkan akses masyarakat pada perbankan.

Pihak Bank Mandiri menghimbau untuk menjaga kartu Mandiri Debit dan kerahasiaan nomor PIN serta tidak menginformasikannya ke siapapun, termasuk orang-orang yang mengaku karyawan Bank Mandiri.

3. Penilaian Efektivitas pengendalian ancaman

Pengendalian ancaman tidak efektif karena permasalahan pada penguasaan PIN oleh pihak pelaku tidak diselesaikan.

4. Langkah-langkah investigasi kejadian/kecelakaan

Awal kejadian adalah saat korban hendak menarik uang di ATM yang dimana saldonya seharusnya sejumlah 128 juta rupiah ternyata adalah kosong. Saat nasabah menelfon pihak bank, dikatakan bahwa telah dilaksanakan transaksi oleh kartu ATM yang dimilikinya. Namun nasabah mengatakan bahwa kartu tersebut ia selalu ia pegang. Investigasi berjalan selama 11 hari kerja terhadap korban. berdasarkan investigasi yang dilakukan, transaksi yang dilakukan dianggap sah karena menggunakan kartu debit dengan PIN yang tepat sehingga uang yang telah "diambil" tidak bisa dikembalikan. Namun dikarenakan kartu debit yang digunakan untuk penarikan uang berbeda dengan kartu debit milik nasabah, kasus ini diperkirakan sebagai kasus penukaran kartu dan penguasaan PIN.

5. Langkah-langkah pemulian kecelakaan/kejadian

Dari cerita tersebut, dinyatakan bahwa pihak bank mandiri tidak bisa bertanggung jawab dan tidak dapat memberikan penggantian atas dana yang hilang dikarenakan nasabah telah menjadi korban kejahatan dengan modus penukaran kartu debit dan penguasaan pin. Sebab, kartu debit yang dipegang nasabah berbeda dengan kartu debit yang terdaftar bank mandiri. Maka dari kejadian tersebut, untuk menjaga kerahasiaan nomor pin dengan tidak

menginformasikannya ke siapapun termasuk juga ke orang-orang yang mengaku karyawan bank itu sendiri.

6. Resiko

Uang nasabah hilang, tidak dikembalikan, dan permasalahan terhadap penguasaan PIN oleh pelaku belum diselesaikan.