Tugas Individu 1

Nama : Clement Samuel Marly

NPM : 2206082114

Mata Kuliah : Prinsip – Prinsip Sistem Informasi

Kelas : C

Serangan Siber pada Perusahaan Konsultan Keamanan

Deloitte merupakan salah satu perusahaan layanan profesional terbesar di dunia dengan pendapatan sekitar $38,8 miliar pada tahun 2017 dan jumlah profesional lebih dari 263.000 orang. Deloitte menyediakan jasa audit, pajak, konsultasi, penasihat keuangan, dan panduan keamanan siber untuk lebih dari 85 persen dari 500 perusahaan Fortune dan lebih dari 6.000 perusahaan swasta dan perusahaan menengah di seluruh dunia. Kantor pusat global Deloitte berada di New York.

Pada April 2017, Deloitte menemukan bahwa server email globalnya telah diretas sejak enam bulan yang lalu. Peretas memperoleh akses ke sistem melalui akun administratif yang memberi mereka akses istimewa dan tidak terbatas ke semua area. Akun tersebut hanya memerlukan satu kata sandi dan tidak memiliki verifikasi dua langkah.

Deloitte menawarkan saran kepada kliennya tentang cara mengelola risiko yang ditimbulkan oleh serangan siber yang canggih. Deloitte juga mengoperasikan Pusat Intelijen Cyber untuk memberikan klien mereka keamanan operasional yang berfokus pada bisnis sepanjang waktu. Pada tahun 2012, Deloitte mendapat peringkat sebagai konsultan keamanan siber terbaik di dunia. Perusahaan memperoleh sebesar $12 miliar per tahun untuk biaya konsultasi yang diberikan. Oleh karena itu, kebocoran akses yang terjadi merupakan hal yang sangat memalukan bagi perusahaan.

Penggunaan email di Deloitte digunakan untuk mengkomunikasikan semua jenis informasi sensitif seperti rencana produk baru, strategi pemasaran, taktik merger dan akuisisi, desain produk, data paten, materi hak cipta, dan rahasia dagang. Server yang diterobos berisi email dari 350 klien termasuk Departemen Luar Negeri, Departemen Keamanan Dalam Negeri, Departemen Pertahanan, Departemen Energi, dan Layanan Pos. Selain itu, terdapat juga email dari Perserikatan Bangsa-Bangsa, Institut Kesehatan Nasional, bisnis perumahan Fannie Mae dan Freddie Mac, serta beberapa perusahaan multinasional terbesar di dunia.

Selain email, para peretas memiliki potensi untuk mengakses informasi seperti nama pengguna, kata sandi, dan alamat IP.

Pada awalnya, Deloitte merahasiakan pelanggaran tersebut dan hanya memberi tahu segelintir mitra senior, enam klien yang diketahui terkena dampak langsung oleh serangan tersebut, dan pengacara di firma hukum internasional Hogan Lovells. Firma hukum tersebut tetap memberikan nasihat hukum dan bantuan tentang potensi dampak dari peretasan yang terjadi.

Deloitte membentuk tim yang terdiri dari analis dan pakar keamanan dari dalam dan luar perusahaan untuk melakukan penyelidikan resmi atas peretasan yang terjadi. Tujuannya yaitu untuk memahami bagaimana peretasan terjadi, menilai cakupan insiden, mengidentifikasi apa yang menjadi target peretas, mengevaluasi dampak potensial terhadap klien, dan menentukan respon keamanan siber yang sesuai. Setelah waktu enam bulan berlalu, tim memastikan bahwa peretas tidak lagi berada dalam sistem email, memastikan bahwa tidak ada gangguan bisnis yang mempengaruhi klien, dan merekomendasikan langkah-langkah tambahan untuk meningkatkan keamanan Deloitte secara keseluruhan. Namun, tim tidak dapat menentukan apakah peretas merupakan individu, kompetitor, atau peretas yang disponsori negara.

Serangan tersebut menggambarkan bahwa organisasi mana pun dapat menjadi korban serangan siber, termasuk organisasi yang memiliki spesialisasi di bidang tersebut.

Pertanyaan:

1. Identifikasi konsekuensi apa yang paling buruk bagi Deloitte. Apakah direct impact, business disruption, recovery cost, legal, atau reputation damage? Berikan alasan untuk jawaban Anda.
2. Menurut Anda, respon apa saja yang telah dilakukan dengan baik oleh Deloitte terhadap serangan siber? Apa yang dapat ditingkatkan oleh Deloitte untuk menangani serangan siber tersebut?
3. Identifikasi tiga perubahan atau penyesuaian yang diperlukan pada kebijakan keamanan Deloitte untuk meningkatkan keamanan informasi dan mencegah kemungkinan serangan siber di masa mendatang.

Jawaban:

1. Konsekuensi terburuk bagi Deloitte adalah *reputation* damage atau reputasi yang rusak. Deloitte adalah perusahaan yang bekerja dalam bidang keamanan siber dan memiliki penghargaan pada tahun 2012 sebagai konsultan keamanan siber terbaik di dunia (kasus, paragraf 3 kalimat 3). Kebocoran data dan pelanggaran keamanan siber pada perusahaan akan merusak reputasi Deloitte. Rusaknya reputasi Deloitte dapat menyebabkan hilangnya kepercayaan klien dan hilangnya klien yang sudah ada sehingga pendapatan Deloitte akan menurun. Kehilangan klien yang sudah ada juga bisa berdampak pada kesulitan dalam merekrut klien baru dan mempertahankan karyawan ("Impact of cyber attack on your business", n.d.).

   Dibandingkan dengan konsekuensi yang lain seperti *direct impact, business disruption, recovery cost,* dan *legal*, reputasi adalah konsekuensi yang paling sulit untuk diperbaiki. Sesuai dengan perkataan Warren Buffet, orang terkaya ketiga tahun 2015, untuk membuat reputasi diperlukan 20 tahun dan hanya lima menit untuk menghancurkan reputasi tersebut. Reputasi yang sudah rusak memerlukan banyak hal untuk diperbaiki, mulai dari pembuktian kembali kemampuan Deloitte dalam bidang keamanan siber sampai mendapatkan kembali kepercayaan klien. Tidak hanya itu, Deloitte juga harus mengeluarkan biaya tambahan untuk memulihkan reputasinya melalui program pemasaran dan kampanye publisitas (Crimmins, 2022).

   Konsekuensi lain yang dialami oleh Deloitte relatif berhubungan dengan keuangan dalam jangka pendek, namun reputasi yang rusak akan merugikan Deloitte dalam jangka panjang. Hilanganya kredibiltas Deloitte dan kepercayaan klien akan membuat Deloitte kehilangan klien dan sulit mendapatkan klien baru. Hal tersebut akan menurunkan pendapatan Deloitte dan merusak prediksi keuangan Deloitte. Dalam jangka panjang, uang yang masuk ke dalam Deloitte bisa kurang dari uang yang keluar sehingga Deloitte perlu melakukan banyak reformasi dalam perusahaan dan melepaskan banyak pekerja (Nickels et al., 2016).

2. Beberapa respons yang telah dilakukan dengan baik oleh Deloitte antara lain:
   - Membentuk tim yang terdiri dari analis dan pakar keamanan dari dalam dan luar perusahaan untuk melakukan penyelidikan resmi atas peretasan yang terjadi dan

merekomendasikan langkah-langkah tambahan untuk meningkatkan keamanan Deloitte secara keseluruhan (kasus, paragraf 6 kalimat 1).

- Memberi tahu beberapa klien yang terkena dampak langsung dari serangan siber dan meminta bantuan dari firma hukum internasional untuk memberikan nasihat hukum (kasus, paragraf 5 kalimat 1).
- Memastikan bahwa tidak ada gangguan yang mempengaruhi klien (kasus, paragraf 6 kalimat 3).

Namun, Deloitte dapat meningkatkan responsnya melalui:

- Memberitahukan klien mengenai serangan siber dan cara mereka dapat melindungi informasi mereka sendiri.
- Meningkatkan keamanan sistem melalui pengadaan *two factor authentication* (2FA) atau verifikasi dua langkah dan meminta semua akun yang berhubungan dengan Deloitte untuk diubah sandinya untuk mencegah serangan siber lanjut.

Hal – hal tersebut dapat membantu Deloitte dalam menjaga integritas atau reputasi Deloitte dan mencegah kerusakan lebih lanjut dari serangan siber (Knell, 2021).

3. Perubahan atau penyesuaian yang dapat dilakukan pada kebijakan keamanan Deloitte:
   - Meningkatkan keamanan perusahaan melalui pembuatan sistem keamanan baru dan mengimplementasikan verifikasi dua langkah (2FA) untuk akun administratif. Akun yang penting juga bisa diminta untuk mengubah sandi setiap beberapa periode waktu untuk meningkatkan keamanan. Deloitte juga bisa mempekerjakan tim IT yang memiliki spesialisasi dalam bidang *network and security* saat membuat sistem keamanan baru.
   - Meninjau ulang kebijakan atau peraturan Deloitte dan memperbaiki masalah yang ditemukan selama investigasi tim.
   - Melakukan penyuluhan atau pelatihan keamanan siber kepada seluruh karyawan Deloitte dengan cara menjelaskan jenis – jenis serangan siber seperti *phishing, ransomware, data breaches, cyberespionage,* dan lainnya.
   - Melakukan audit atau pengecekan secara rutin terhadap sistem informasi Deloitte untuk mengetahui terjadinya serangan siber dan memastikan terjaganya data.

Audit mencakup pengujian keamanan dan pengecekan kebocoran data. Adanya audit secara rutin akan membantu Deloitte dalam mengidentifikasi kelemahan keamanan dan mengetahui adanya kebocoran data.

Perubahan atau penyesuaian tersebut akan membantu Deloitte untuk meningkatkan keamanan informasi dan mencegah kemungkinan serangan siber di masa mendatang (“Cyber Security Risk Management”, n.d.).

Referensi

Crimmins, A. (2022). *How to you rebuild your reputation if you fall from Grace*. The Corporate Governance Institute. Diakses pada 27 Februari, 2023, melalui https://www.thecorporategovernanceinstitute.com/insights/guides/how-can-i-get-my-good-reputation-back/

Cyber Security Risk Management. *Cyber Security for Business*. (n.d.). Diakses pada 27 Februari, 2023, melalui https://www.nibusinessinfo.co.uk/content/cyber-security-risk-management

Impact of cyber attack on your business. *Cyber Security for Business*. (n.d.). Diakses pada 27 Februari, 2023, melalui https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business

Knell, N. (2021). *5 ways to prepare for a cyberattack*. GovTech. Diakses pada 27 Februari, 2023, melalui https://www.govtech.com/security/5-ways-to-prepare-for-a-cyberattack.html

Nickels, W. G., McHugh, J. M., & McHugh, S. M. (2016). *Understanding business*. McGraw-Hill Education.