

Nama Kelompok :

- Adetia Raymond S. (2320506036)
- Oktario Mufti Y. (2320506044)
- Muhammad Ridwan A. (2320506049)

Studi Kasus: Pelanggaran Data Equifax

Pada tahun 2017, Equifax—sebuah biro kredit besar di AS—mengalami pelanggaran data yang sangat besar yang mengungkapkan informasi sensitif dari hampir 148 juta orang Amerika, serta jutaan lainnya di luar negeri.

Pelanggaran ini dianggap sebagai salah satu kegagalan keamanan siber yang menimbulkan pertanyaan serius tentang perlindungan data, pemberitahuan pelanggaran secara tepat waktu, dan akuntabilitas perusahaan. Kasus Equifax menunjukkan bagaimana kurangnya kontrol internal, respon yang terlambat, dan kesalahan etika dalam keamanan TI dapat berdampak luas pada individu dan masyarakat.

1. Masalah Etika

- **Kelalaian dalam Langkah Keamanan Siber**
Equifax sudah tahu tentang celah keamanan—seperti kerentanan Apache Struts—tetapi gagal memperbarui patch keamanan penting tepat waktu. Kelalaian ini memungkinkan peretas mengeksploitasi celah tersebut selama 76 hari, sehingga data pribadi (PII) banyak orang terekspos.
- **Keterlambatan dalam Pemberitahuan Publik**
Meskipun aktivitas jaringan yang mencurigakan sudah terdeteksi, Equifax menunda pemberitahuan kepada konsumen hingga September 2017. Penundaan ini membuat individu yang terdampak kehilangan kesempatan untuk segera mengambil tindakan pencegahan (misalnya, melakukan pembekuan kredit).
- **Masalah Insider Trading**
Ada laporan yang menunjukkan bahwa beberapa eksekutif Equifax menjual saham perusahaan tidak lama setelah pelanggaran data diketahui, namun sebelum informasi tersebut dipublikasikan. Tindakan ini menimbulkan kekhawatiran etis karena mereka menggunakan informasi nonpublik untuk keuntungan pribadi.
- **Komunikasi yang Buruk kepada Konsumen**
Upaya Equifax dalam menyampaikan pemberitahuan pelanggaran—seperti pembuatan situs web khusus yang mirip dengan situs phishing—dapat menyebabkan kebingungan dan risiko tambahan, sehingga mengurangi kepercayaan konsumen.

2. Peran Organisasi Profesional dan Badan Regulasi

- **Pengawasan Regulasi:**
Badan seperti Federal Trade Commission (FTC) dan Consumer Financial Protection Bureau (CFPB) melakukan investigasi yang kemudian menghasilkan penyelesaian dan denda yang cukup besar (hingga \$700 juta) untuk mengatasi kerugian yang ditimbulkan.
- **Kode Etik dan Praktik Terbaik:**
Organisasi seperti ACM dan IEEE memiliki pedoman etika yang menekankan

perlindungan privasi pengguna, pemberitahuan pelanggaran secara cepat, dan akuntabilitas. Pedoman ini menjadi acuan bagi para profesional TI dan menunjukkan kekurangan praktik Equifax.

➤ **Advokasi Industri dan Pelatihan:**

Badan profesional mendorong pelatihan rutin serta penerapan prinsip “privacy by design” dan standar keamanan siber yang kuat. Kasus ini mendorong upaya dalam industri untuk menekankan kembali standar etika dan meningkatkan protokol respon pelanggaran.

3. Solusi dan Rekomendasi

Meningkatkan Transparansi dan Pemberitahuan dengan perusahaan harus memiliki kebijakan untuk segera menginformasikan pelanggaran, sehingga konsumen dapat dengan cepat mengambil tindakan pencegahan seperti pembekuan kredit atau alert penipuan.

Membuat pengawasan Independen dengan organisasi perlu membentuk komite etika dan keamanan siber internal yang independen untuk memantau kepatuhan terhadap protokol keamanan TI dan pedoman etika.

Perkuat Kepatuhan Regulasi dengan diperlukan kerangka kerja regulasi yang lebih ketat dan hukuman yang lebih berat bagi perusahaan yang lalai. Pengawasan yang lebih kuat dari badan seperti FTC dan CFPB dapat mendorong praktik yang lebih baik di seluruh industri.

Adakan Pelatihan Rutin dengan pelatihan etika dan keamanan siber secara berkala bagi para profesional TI dan manajemen sangat penting agar semua staf memahami peran mereka dalam melindungi data konsumen dan menegakkan standar etika.

Kesimpulan

Pelanggaran data Equifax menyoroti tanggung jawab etis besar para profesional TI dan organisasi dalam melindungi informasi sensitif. Dengan gagal mengatasi kerentanan yang diketahui dan menunda pemberitahuan, Equifax tidak hanya melanggar kepercayaan konsumen tetapi juga memicu konsekuensi regulasi dan hukum yang serius. Kepatuhan terhadap kode etik profesional, pengawasan regulasi yang lebih kuat, dan pendekatan proaktif serta transparan terhadap keamanan siber sangat penting untuk mencegah insiden serupa di masa depan. Mengikuti rekomendasi ini penting untuk membangun kembali kepercayaan dan memastikan teknologi berfungsi untuk kebaikan publik sambil menghormati privasi individu.

Sumber:

https://en.wikipedia.org/wiki/2017_Equifax_data_breach