Mengungkap Kejahatan Siber:
Implikasi Serangan terhadap Citilink dan Tiket.com

Raihanfitri Adi Kalipaksi (2309106096) - Informatika C23

PENDAHULUAN

Dalam dunia yang semakin terhubung melalui teknologi digital, kejahatan siber menjadi salah satu tantangan terbesar bagi perusahaan dan individu di seluruh dunia. Kasus kejahatan siber yang melibatkan Tiket.com dan Citilink pada tahun 2017 merupakan contoh nyata dari bagaimana ancaman ini dapat merugikan tidak hanya aspek finansial perusahaan tetapi juga kepercayaan publik terhadap sistem digital. Serangan ini dilakukan oleh sekelompok hacker yang dipimpin oleh seorang remaja berusia 19 tahun asal Tangerang, SH, yang berhasil melakukan akses ilegal ke sistem aplikasi Tiket.com yang terhubung dengan sistem penjualan tiket Citilink.

Pada awalnya, aksi ilegal ini tampak sederhana, namun dampaknya sangat luas. Para pelaku mencuri kode booking tiket penerbangan dan menjualnya dengan potongan harga 30 hingga 40% melalui platform media sosial seperti Facebook. Tindakan ini menarik perhatian banyak pembeli yang tergiur dengan harga murah, dan pada akhirnya, membuat Tiket.com mengalami kerugian sekitar 4 miliar rupiah, sementara Citilink merugi sekitar 2 miliar rupiah. Kerugian ini diperparah dengan lamanya waktu yang dibutuhkan Tiket.com untuk menyadari adanya penyusupan ke dalam sistem mereka, yang mencapai hampir sebulan. Hal ini menunjukkan betapa rentannya sistem keamanan yang ada pada saat itu.

Dari sudut pandang teknis, kasus ini menarik untuk dianalisis. Meski para hacker tidak menggunakan teknik yang sangat canggih, mereka berhasil mengeksploitasi kelemahan dalam sistem keamanan yang ada. Ruby Alamsyah, seorang ahli digital forensic, bahkan menyebutkan bahwa aksi SH dan rekan-rekannya masih terbilang "ecek-ecek," mengindikasikan bahwa dengan pengetahuan yang terbatas, mereka mampu menyebabkan kerugian yang sangat besar bagi perusahaan-perusahaan tersebut. Penangkapan keempat pelaku oleh Direktorat Siber Bareskrim Polri, yang dilakukan di Balikpapan, membuka jalan bagi pengungkapan lebih lanjut mengenai bagaimana mereka melancarkan aksinya.

Sebagai tambahan, klarifikasi dari Citilink yang menyatakan bahwa mereka tidak menjadi target serangan secara langsung, melainkan merupakan mitra dari Tiket.com, menambah kompleksitas kasus ini. Meski tidak ada pembobolan di situs Citilink, dampak yang ditimbulkan tetap dirasakan oleh kedua pihak. Dalam konteks ini, penting untuk memahami bagaimana kejahatan siber tidak hanya merugikan perusahaan dari segi finansial, tetapi juga dapat merusak reputasi dan kepercayaan pelanggan.

- Kronologi Kasus Kejahatan Siber Tiket.com dan Citilink
    1. Awal Kejadian (11-27 Oktober 2016): Pada periode ini, sekelompok hacker yang dipimpin oleh SH berhasil melakukan akses ilegal ke sistem aplikasi Tiket.com yang terhubung dengan sistem penjualan tiket Citilink. Para pelaku menggunakan teknik hacking untuk mendapatkan akses ke server Tiket.com, kemudian berhasil mencuri kode booking tiket penerbangan.
    2. Metode Penjualan (Oktober 2016): Setelah mendapatkan kode booking, SH dan rekan-rekannya, termasuk MKU (19), AI (19), dan NTM (27), menjual tiket-tiket tersebut dengan diskon 30 hingga 40% melalui akun Facebook pribadi mereka. MKU bertanggung jawab untuk menjual tiket yang dicuri, memberikan potongan harga yang sangat menggiurkan bagi calon pembeli.
    3. Waktu Penemuan (November 2016): Pada 11 November 2016, PT Global Network (Tiket.com) melaporkan adanya pembobolan di situs jual beli tiket online mereka kepada Bareskrim Polri. Pihak Tiket.com baru menyadari adanya penyusupan ini setelah lebih dari sebulan, mengakibatkan kerugian besar bagi perusahaan.
    4. Kerugian yang Dialami: Tiket.com mengalami kerugian sebesar Rp 4.124.000.982 akibat tindakan para hacker. Sebagian besar kerugian ini disebabkan oleh pembatalan tiket dan refund yang harus dilakukan setelah kasus ini terungkap. Citilink, meskipun tidak menjadi target langsung, tetap mengalami kerugian sekitar Rp 1.973.784.434.
    5. Penangkapan Pelaku (28 Maret 2017): Direktorat Siber Bareskrim Polri menangkap keempat pelaku di sebuah rumah di Balikpapan. SH mengakui bahwa ia dan rekan-rekannya membobol server Tiket.com untuk mendapatkan akses ke akun pengguna dan kode booking. Selama interogasi, SH mengungkapkan bahwa ide untuk membobol situs tersebut berasal dari MKU, dan ia belajar hacking secara otodidak melalui internet.

6. Klarifikasi dari Citilink: Setelah kejadian ini, Citilink memberikan klarifikasi bahwa serangan tidak terjadi pada situs resmi mereka, melainkan pada sistem partner mereka, yaitu Tiket.com. Citilink menegaskan bahwa semua transaksi yang dilakukan di situs mereka tetap aman dan tidak ada pembobolan yang terjadi di server Citilink.
7. Dampak Jangka Panjang: Kasus ini menyoroti pentingnya keamanan siber dalam bisnis digital, terutama dalam industri perjalanan dan tiket online. Meskipun pelaku hanya menggunakan teknik yang dianggap tidak canggih, dampak dari tindakan mereka dapat merugikan perusahaan miliaran rupiah. Kasus ini juga meningkatkan kesadaran akan risiko yang dihadapi oleh platform online dalam mengelola data sensitif dan transaksi keuangan.

ISI

Kasus kejahatan siber yang melibatkan Tiket.com dan Citilink pada tahun 2016 memberikan dampak yang signifikan, baik dari segi finansial maupun reputasi. Tiket.com mengalami kerugian sekitar Rp 4,1 miliar akibat pembatalan tiket dan pengembalian dana yang harus mereka lakukan setelah terjadinya pembobolan data. Hal ini berimbas pada arus kas perusahaan, yang terpaksa menghadapi tantangan dalam mengelola kerugian yang terjadi. Sementara itu, Citilink merugi sekitar Rp 1,9 miliar karena sejumlah pembeli membatalkan tiket yang mereka beli secara ilegal. Dampak finansial ini tidak hanya menghantam kedua perusahaan secara langsung, tetapi juga menciptakan efek domino yang memengaruhi mitra bisnis dan pemasok lainnya dalam industri perjalanan.

Lebih dari sekadar kerugian finansial, insiden ini menimbulkan keraguan di kalangan pelanggan terhadap keamanan transaksi online. Kepercayaan publik terhadap sistem pemesanan tiket digital mengalami penurunan, dan banyak pengguna menjadi lebih skeptis dalam melakukan transaksi melalui platform online. Hal ini menunjukkan bahwa keamanan siber bukan hanya masalah teknis, tetapi juga berkaitan erat dengan reputasi perusahaan dan loyalitas pelanggan. Dalam dunia bisnis yang semakin bergantung pada teknologi, kepercayaan konsumen menjadi aset yang sangat berharga, dan kehilangan kepercayaan dapat berakibat fatal bagi kelangsungan bisnis.

Menanggapi insiden ini, Tiket.com dan Citilink mengambil langkah cepat untuk memperbaiki situasi dan mencegah terulangnya kejadian serupa di masa depan. Tiket.com melakukan audit menyeluruh terhadap sistem keamanan mereka, melibatkan ahli keamanan siber untuk mengidentifikasi dan menutup celah yang dimanfaatkan oleh para pelaku. Selain itu, mereka berinvestasi dalam teknologi keamanan yang lebih canggih, termasuk enkripsi data dan sistem pemantauan real-time untuk mendeteksi aktivitas mencurigakan lebih awal. Citilink, meskipun tidak menjadi target langsung, juga memperkuat kerjasama dengan mitra untuk meningkatkan perlindungan data, serta memastikan bahwa semua transaksi di platform mereka tetap aman dan terlindungi.

Kasus ini juga mendorong kesadaran akan pentingnya keamanan siber di kalangan perusahaan digital dan regulator. Banyak perusahaan mulai menyadari bahwa investasi dalam keamanan siber adalah kebutuhan, bukan sekadar biaya tambahan. Regulasi terkait perlindungan data dan keamanan siber menjadi semakin ketat, mendorong perusahaan untuk mengimplementasikan langkah-langkah proaktif dalam melindungi informasi pelanggan. Dengan meningkatnya serangan siber di seluruh dunia, pelajaran yang didapat dari kasus ini menjadi pengingat penting bagi semua pelaku bisnis untuk terus meningkatkan sistem keamanan mereka agar tidak menjadi korban kejahatan siber di masa depan.

PENUTUP

Kasus kejahatan siber yang melibatkan Tiket.com dan Citilink mencerminkan betapa rentannya sistem digital yang ada dan bagaimana dampak dari serangan semacam itu dapat merembet ke berbagai aspek, mulai dari kerugian finansial hingga reputasi perusahaan. Tanggapan terhadap insiden ini harus bersifat menyeluruh, tidak hanya mengandalkan langkah-langkah reaktif, tetapi juga proaktif. Salah satu tindakan penting adalah melakukan evaluasi menyeluruh terhadap kebijakan keamanan siber yang ada, termasuk peningkatan teknologi firewall, pengembangan algoritma deteksi intrusi, serta penerapan sistem otentikasi yang lebih kuat untuk melindungi data sensitif.

Selanjutnya, perusahaan perlu berinvestasi dalam pelatihan keamanan siber bagi seluruh karyawan untuk meningkatkan kesadaran akan potensi ancaman dan cara menghindarinya.

Pendidikan ini harus mencakup pemahaman tentang phishing, malware, dan praktik terbaik dalam penggunaan sistem informasi. Selain itu, penting bagi Tiket.com dan Citilink untuk bekerja sama dengan pihak berwenang dalam membangun jaringan intelijen siber yang lebih efektif, sehingga ancaman dapat dideteksi dan ditangani sebelum merugikan perusahaan dan pengguna.

Regulasi pemerintah yang lebih ketat juga dibutuhkan untuk memberikan perlindungan yang lebih baik terhadap data pribadi dan transaksi keuangan di platform online. Dengan adanya kerjasama antara sektor swasta dan pemerintah, diharapkan akan terbentuk ekosistem digital yang lebih aman dan terpercaya. Pada akhirnya, penting bagi perusahaan untuk memahami bahwa keamanan siber adalah investasi jangka panjang yang tidak hanya melindungi aset perusahaan, tetapi juga menjaga kepercayaan konsumen dan reputasi di pasar yang semakin kompetitif.

REFERENSI

Asril, S. (2017, April 5). *Cerita remaja 19 tahun peretas situs tiket.com Dan Raup Hampir RP 1 miliar*. KOMPAS.com. https://nasional.kompas.com/read/2017/04/05/08135311/cerita.remaja.19.tahun.peretas.situs.tiket.com.dan.raup.hampir.rp.1.miliar

K, N. W. (2017, March 30). *Kasus Pembobolan situs tiket online, Ini Penjelasan Citilink*. detiknews. https://news.detik.com/berita/d-3460864/kasus-pembobolan-situs-tiket-online-ini-penjelasan-citilink

Kallo, E. (2021, December 25). *Cyber crime: Studi Kasus tiket.com Dan Citilink Rugi milyaran rupiah Akibat Penyusup*. Koridor.Online. https://www.koridor.online/cyber-crime-studi-kasus-tiket-com-dan-citilink-rugi-milyaran-rupiah-akibat-penyusup/

Prihadi, S. D. (2017, March 31). *Begini Cara Hacker bobol situs tiket.com*. teknologi. https://www.cnnindonesia.com/teknologi/20170331145137-185-204065/begini-cara-hacker-bobol-situs-tiketcom

Qodir, A. (2017, March 30). *Hacker remaja Ini Sukses Bobol situs tiket.com di server citilink, kerugian ditaksir rp 4,1 miliar*. Tribunnews.com. https://www.tribunnews.com/nasional/2017/03/30/hacker-remaja-ini-sukses-bobol-situs-tiketcom-di-server-citilink-kerugian-ditaksir-rp-41-miliar