

PENYALAHGUNAAN DATA PRIBADI DALAM ERA CYBERCRIME

Steven Johny Runtuwene¹, Oldi Malfri Lambonan², Sonny R. Kasenda³, Esther Jelly Torar⁴,
Vania V.T Tumewan⁵, Timothy A.A.T Tumewan⁶
steven@polimdo.ac.id¹, oldilambonan@elektro.polimdo.ac.id², sonnykasenda@gmail.com³,
esthertorar@gmail.com⁴, vaniatumewan@gmail.com⁵, vitotumewan134@gmail.com⁶
Politeknik Negeri Manado¹²³⁴⁵⁶

Abstrak

Kejahatan siber merupakan ancaman yang semakin meningkat di era digital saat ini. Studi ini bertujuan untuk menganalisis karakteristik umum yang sering terkait dengan pelaku kejahatan siber. Kami melakukan analisis terhadap berbagai kasus kejahatan siber yang telah tercatat dan mengeksplorasi tren umum yang dapat diidentifikasi. Temuan kami mengungkapkan bahwa pelaku kejahatan siber seringkali memiliki latar belakang teknis yang kuat, menggunakan teknik sosial engineering, serta memanfaatkan kerentan serangan. Mereka juga cenderung beroperasi secara anonim melalui jaringan yang terenkripsi. Pemahaman karakteristik ini dapat membantu dalam pengembangan strategi perlindungan dan penegakan hukum yang lebih efektif dalam menghadapi ancaman kejahatan siber yang telah menjadi ancaman serius dalam dunia digital. Penelitian ini bertujuan untuk mengidentifikasi karakteristik yang biasa ditemukan pada pelaku kejahatan siber.

Kata Kunci: kejahatan siber, data pribadi, analisis kasus.

1. PENDAHULUAN

Kejahatan siber telah menjadi salah satu ancaman terbesar di era digital saat ini. Dalam dunia yang semakin terhubung melalui internet, perbuatan kriminal telah bermetamorfosis menjadi bentuk-bentuk baru yang memanfaatkan kerentan sistem teknologi informasi. Untuk menghadapi ancaman ini, adalah penting untuk memahami karakteristik umum yang sering terkait dengan para pelaku kejahatan siber. Oleh karena itu, studi ini bertujuan untuk menganalisis dan mendokumentasikan karakteristik yang biasa ditemukan pada pelaku kejahatan siber. Tren dalam kejahatan siber selalu berubah seiring dengan perkembangan teknologi dan cara baru para pelaku mengambil keuntungan dari kerentan sistem. Melalui analisis kasus yang tercatat, penelitian ini bertujuan untuk memberikan wawasan lebih mendalam tentang profil para pelaku kejahatan siber. Data yang diperoleh dari analisis kasus ini diharapkan dapat memberikan panduan berharga dalam mengembangkan strategi perlindungan yang lebih efektif dan dalam menegakkan hukum yang lebih tajam dalam menghadapi ancaman kejahatan siber.

Dalam perjalanan studi ini, kami akan mengidentifikasi karakteristik yang umumnya terkait dengan pelaku kejahatan siber, seperti latar belakang

teknis yang kuat, penggunaan teknik sosial engineering, beroperasi secara anonim, dan kemampuan mereka untuk memanfaatkan kerentan sistem dengan kecanggihan tertentu. Hasil analisis yang kami peroleh diharapkan dapat memberikan pemahaman lebih baik tentang bagaimana para pelaku kejahatan siber beroperasi dan bagaimana kita dapat lebih efektif melindungi sistem dan data kita dari ancaman tersebut. Dengan demikian, pendahuluan ini memberikan gambaran umum tentang latar belakang penelitian, tujuan, metode yang digunakan, dan hasil yang diharapkan dicapai melalui analisis karakteristik pelaku kejahatan siber. Dalam bab-bab berikutnya, kami akan merinci hasil analisis tersebut dan menyajikan diskusi mendalam tentang implikasinya dalam melawan ancaman kejahatan siber yang terus berkembang.

2. METODE PENELITIAN

Penelitian ini menggunakan metode analisis kasus, menganalisis berbagai insiden kejahatan siber yang tercatat untuk mengidentifikasi karakteristik umum.

3. HASIL DAN PEMBAHASAN

Pencurian data pribadi menjadi hal biasa ketika Covid-19 muncul. Bahkan, sertifikat vaksinasi Presiden Joko Widodo belakangan ini banyak dibagikan di media sosial. Sertifikat ini akan berasal dari aplikasi PeduliLindungi dengan memperoleh Nomor Induk Kependudukan (NIK) dari Komisi Pemilihan Umum (KPU). Selain data presiden, kasus kebocoran juga terjadi beberapa bulan lalu. Sekitar 279 juta data peserta BPJS Kesehatan dipertukarkan di RaidForums. Hal ini menunjukkan bahwa pemerintah harus selalu memperhatikan perlindungan data pribadi. Melindungi data pribadi menjadi semakin penting, terutama di masa pandemi, seiring dengan mulai beralihnya transaksi secara online akibat adanya pembatasan mobilitas masyarakat. Meningkatnya pencurian data pribadi berarti bahwa setiap individu harus mengambil sejumlah tindakan pencegahan saat mengakses Internet. Menjaga keamanan data pribadi menjadi kebutuhan yang semakin penting di tengah meningkatnya serangan siber. Berdasarkan data Cyber Police, selama lima tahun terakhir, pencurian data meningkat setiap tahunnya. Pada tahun 2016, terdapat 20 kasus yang dilaporkan, pada tahun 2020 jumlahnya meningkat menjadi 182 kasus. Kehilangan data, serangan kejahatan dunia maya seperti malware dan phishing dapat mengakibatkan hilangnya data bisnis penting seperti data penjualan dan transaksi keuangan. Hilangnya data dapat menyebabkan kerugian finansial yang signifikan, kerusakan reputasi, dan bahkan tindakan hukum. Lemahnya perlindungan data di Indonesia mengakibatkan maraknya kebocoran data. Terbukti dengan sering terjadinya kasus kejahatan siber, seperti hacking (peretasan) maupun cracking (pembajakan) media sosial yang berujung pada pembobolan data pribadi, pemerasan hingga penipuan daring. Di Indonesia, perlindungan hukum terhadap data pribadi masih dinilai belum optimal, terbukti dengan masih banyaknya kasus penyalahgunaan data pribadi seseorang tanpa sepengetahuan pemiliknya karena kurangnya keamanan dan pengawasan yang ketat dari pengguna data. Jika kita membuat akun di jejaring sosial, mengunduh aplikasi dari Play Store, dll, secara tidak langsung atau seolah-olah kita telah menyetujui bahwa pengguna layanan dapat mengakses data pribadi kita. Namun, ketika konsumen mengetahui data ini, ia tidak memiliki hak atau jaminan untuk melindungi keamanan data pribadinya. Hal ini dimungkinkan karena pemilik data hanya berkewajiban memberikan data pribadinya kepada penyedia layanan. Penyedia layanan tidak boleh melihat sebaliknya, karena hal ini tidak berarti bahwa pemberian data pribadi dari pemilik data kepada penyedia layanan juga memberikan hak kepada penyedia layanan untuk memberikan atau menyebarkan data tersebut kepada pihak ketiga dan jika hal ini benar-benar terjadi, maka

pihak layanan tindakan penyedia dapat dianggap sebagai pelanggaran hukum.

- Pertama, mengenai password. Gunakan kata sandi yang berbeda untuk akun dan jejaring sosial yang berbeda. Gunakan juga kombinasi angka dan huruf kapital agar tidak mudah ditebak.
- Kedua, jangan membuka tautan mencurigakan yang disebarluaskan melalui email, SMS, atau saluran lainnya. Hal ini dapat menyebabkan phishing atau malware.
- Ketiga, gunakan perangkat lunak yang sah dan lakukan pembaruan rutin untuk memperbaiki lubang keamanan. Perangkat lunak ilegal, yakni bajakan, cenderung tidak menerima pembaruan, sehingga dapat membuka celah keamanan yang memungkinkan peretas melakukan aksinya.
- Keempat, hindari penggunaan koneksi Internet nirkabel (Wi-Fi) di manapun. Tidak jarang jaringan Wi-Fi di tempat umum tidak aman.
- Kelima, pastikan pengguna tidak mengungkapkan data pribadi, seperti email, kata sandi, dll. orang lain untuk menjaga kerahasiaan informasi penting.

5. KESIMPULAN

Akses ilegal adalah kejahatan dunia maya Cyber Crime yang menggunakan komputer sebagai sasaran atau objek utama dalam melakukan pencurian data jaringan dan pembobolan situs. Kejahatan yang menjadikan sistem dan fasilitas teknologi informasi sebagai sasaran atau objek, misalnya pencurian data pribadi, pembuatan dan penyebaran virus, pembobolan situs atau website dan sebagainya. Melalui pencurian data jaringan rahasia milik orang lain maka secara langsung seseorang sebagai subjek hukum telah melakukan aktivitas yang disebut dengan Cyber Crime. Kejahatan dunia maya sering disebut Cyber Crime.

6. DAFTAR PUSTAKA

- <https://fhukum.unpatti.ac.id/jurnal/sasi/article/view/394/285>
- file:///C:/Users/HP/Downloads/1059-5536-2-PB%20(1).
- <https://databoks.katadata.co.id/datapublish/2021/09/07/pencurian-data-pribadi-makin-marak-kala-pandemi-dwi-hadya-jayani,07-09-2021,15.30>
- <https://katadata.co.id/anchar/infografik/617631d62337a/lima-cara-menjaga-data-pribadi-alfons-yoshio,25-10-2021,11.26>
- <https://nasional.kompas.com/read/2022/09/16/02400071/kejahatan-siber--pengertian-karakteristik-dan-faktor-penyebabnya-issaha-harruma,16-09-2022,02.40>
- <https://www.semanticscholar.org/search?q=cibercrime&sort=relevance&page=4>