SENI BUDAYA DASAR

HACKING DAN BUDAYA DIGITAL : MEMAHAMI MOTIF, DAMPAK, DAN SOLUSI

Disusun oleh :

Nama : Dany Akmallun Ni’am

Prodi : Teknik Informatika

Nim : 231240001460

Kelas : DC

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NAHDLATUL ULAMA JEPARA

DAFTAR ISI

BAB I
PERMASALAHAN

1.1 Gambaran umum permasalahan

Dalam bidang teknologi, komputer dan internet adalah teknologi yang revolusioner, mahakarya yang sangat luar biasa karena dapat mempertemukan antara individu dengan komponen mesin dalam sebuah jaringan virtual sehingga menghasilkan suatu dunia baru yang disebut dengan dunia maya (Cyberspace).

Komputer dan internet dulunya hanya terbatas pada jenis-jenis tertentu seperti Komputer mini dan Komputer Mainframe. Hal inilah yang dimanfaatkan oleh sebagian orang pada saat itu untuk mengembangkan teknologi agar lebih pesat.. Komunitas hacker mempunyai peran yang sangat vital dalam perkembangan teknologi saat ini. Ada sebuah komunitas, budaya, terdiri dari para programer mahir dan ahli jaringan, yang sejarahnya bermula dari dekade minikomputer pertama yang memiliki time-sharing dan zaman eksperimen awal ARPANET. Dari anggota budaya inilah muncul istilah 'hacker'. Hacker Lah yang membangun internet, sistem operasi komputer, Usenet dan World Wide Web.

Hacker menjadi suatu kultur yang dianggap menyimpang dalam masyarakat. Penilaian ini dapat terjadi berawal dari semangat memberontak dan anti kemapanan. Kemapanan adalah hal yang menjadi tujuan hidup dalam masyarakat industri. Pemberontakan ini mengakibatkan adanya anggapan dari masyarakat modern yang biasanya hidup di kawasan perkotaan dan tidak lepas dari kehidupan industrialisasi bahwa budaya hacking adalah budaya yang menyimpang. Dari sini akan timbul suatu bentuk delinquent subculture yang muncul di masyarakat.

Salah satu pembentukan sebuah kelompok dalam dunia maya yang biasa disebut komunitas virtual. Internet telah mengkonstruksi dunia maya, yang dalam praktiknya menjadi dunia tanpa batas, dunia kebebasan, yang bisa dimasuki dan dimanfaatkan oleh siapapun. Semakin banyak orang yang menggunakan internet, semakin banyak fasilitas yang diciptakan. Fenomena komunitas di internet sangat bervariasi mulai dari kegemaran dan hobi yang sama. Internet telah menghadirkan realitas. Kehidupan barn kepada umat manusia. Internet telah mengubah jarak dan waktu menjadi tidak terbatas.

Adanya internet, manusia dapat melakukan transaksi bisnis, ngobrol, belanja, belajar, dan berbagai aktivitas lain layaknya dalam kehidupan nyata.

Kemajuan teknologi mengakibatkan timbulnya berbagai kelompok - kelompok anak-anak muda di dunia maya, salah satunya adalah hacker. Hacker sering dicap banyak orang sebagai penjahat, beridentitas nakal, suka mencuri, dan membobol jaringan. Setiap ada pemberitaan isu-isu pembobolan dan pengrusakan terhadap situs, selalu dikaitkan dengan hacker. Pada kenyataannya, tidak semua hacker adalah pelaku kejahatan.

Fandy merupakan salah satu contoh hacker muda yang berprestasi di Indonesia. Berawal dari game, kemudian jatuh hati pada kegiatan hacking. Begitulah awal mula Fandy panggilan akrab Fandy Winata, menyukai dunia maya dan berhasil menjadi juara termuda Cyber Defence Competition, sebuah kompetensi bergengsi antar programmer Indonesia pada usia 15 tahun 4. Fandy tidak pemah membayangkan akan menjadi seorang peretas (hacker) ketertarikannya pada dunia cyber terfokus pada game online yang dikenalkan abangnya saat masih duduk di kelas III SD. Pelajar kelas IX di SMP Sutomo II Medan ini memenangkan lomba tersebut bersama timnya O'r Republic. Bermula belajar dari komunitas hacker newbie, dan bersama para hacker pemula membuat komunitas baru, Indonesia Security Down (ISD) yang sempat booming juga, masuk berita di Rusia pas ada cyber war antara Indonesia dan Israel. Lalu kenai dengan hacker asal Irlandia, Syria, Eropa chatting ~ chatting tukar ilmu tentang perang cyber. Kini Fandy Winata jadi juara Hacker termuda Indonesia.

Di Indonesia sendiri, hacker sudah ada sejak abad 20 saat tanah air menjadi ladang subur perkembangan internet. 5 Beberapa kelompok hacker di Indonesia saat itu cukup banyak, diantaranya Sidoarjo hacker Link, anti- hackerLink, kecoa elektronic, Surabaya Hacker Link, X-Code, dan echo. Hacker di Indonesia mencapai masa keemasan pada kisaran tahun 2000, yaitu Anti Hacker Link. Pihaknya mampu membobol puluhan situs internet kala itu baik dari dalam dan luar negeri. Uniknya, pendiri dari Anti Hacker Link ini adalah seorang anak yang belum genap berumur 17 tahun bemama Wenas Agustiawan yang biasa dikenal dengan nama hC (hantu Crew).

Namun akhirnya dia tertangkap basah saat melakukan aksi pembobolan pada sebuah situs di Singapura di dalam apartemennya. Dengan penangkapan itu, he membuat rekor sebagai hacker Indonesia pertama yang diproses secara hukum.

Sebenarnya, hC tidak bisa lolos dari jerat hukum yang ada eli Singapura. Akan tetapi karena dia masih di bawah umur, sehingga dia hanya didenda sebesar Rp 150.000,- saja. Apabila pengadilan Singapura menunggu proses pengadilan selama 1 minggu saja, hC bisa dipenjarakan, sebab setelah seminggu hC yang berasal dari Malang, Jawa Timur tersebut sudah genap berumur 17 tahun. Namun pihak pengadilan tidak ingin menunda proses pengadilan terhadap hC.

Hacker memiliki tujuan yang beragam ada yang baik dan buruk. Berdasarkan tujuannya itu ada 4 Kategori hacker yaitu **White Hat Hacker, Blue Hat Hacker, Gray Hat Hacker,** dan **Black Hat Hacker**. Hanya Black Hat Hacker yang dapat diklaim mempunyai tujuan buruk, sedangkan Gray Hat Hacker bekerja antara baik dan buruk. White Hat Hacker lebih sering disebut dengan Ethical Hacker merupakan julukan bagi peretas yang secara etis tidak mengambil keuntungan dari kelemahan dalam suatu sistem komputer, White Hat Hacker secara umum memprioritaskan dirinya untuk melindungi sistem tersebut. Bisa menyerang maupun mencegah, inilah target. Blue Hat Hacker merupakan peretas yang bekerja untuk perusahaan atau instansi. Mereka bekerja untuk melakukan uji coba sistem keamanan komputer sebelum dipasarkan. Perusahaan Microsoft mempunyai hacker yang mereka juluki sebagai Blue Hat Microsoft Hacker.

Motivasi seorang hacker sangat beragam dan seringkali kompleks. Beberapa hacker terdorong oleh hasrat intelektual dan rasa ingin tahu, ingin memahami bagaimana sistem komputer dan jaringan berfungsi, serta mencari tantangan teknis yang memacu kemampuan mereka. Di sisi lain, ada hacker yang memotivasi diri mereka sendiri oleh keinginan untuk mendapatkan keuntungan finansial, dengan mencuri data pribadi, informasi keuangan, atau mengakses akun bank. Selain itu, ada pula motivasi ideologis, di mana hacker bertindak sebagai bentuk protes terhadap pemerintah atau perusahaan besar. Terakhir, ada juga motivasi yang muncul dari budaya hacker itu sendiri, dimana reputasi dan prestise dalam komunitas menjadi pendorong untuk terus mencari prestasi teknis dalam dunia hacking.

1.2 Permasalah yang timbul

Aktivitas hacking merupakan tantangan serius dalam era digital yang semakin terkoneksi. Aktivitas hacking, baik yang dilakukan oleh individu-individu dengan motif finansial, politis, atau bahkan hasrat intelektual, telah memunculkan dampak yang luas dan merugikan pada berbagai tingkatan, mulai dari individu hingga perusahaan besar dan bahkan negara-negara. Masalah-masalah seperti pencurian data pribadi, Penyalahgunaan Informasi serta Dampak sosial dan Budaya telah menjadi perhatian utama dalam upaya menjaga keamanan siber dan melindungi privasi online. Beberapa dampak dari aktivitas hacking :

1.2.1 Pencurian Data Pribadi

Pencurian data pribadi yang muncul dari aktivitas hacking adalah ancaman serius terhadap privasi dan keamanan individu. Dalam dunia digital yang semakin terhubung, hacker seringkali berhasil mengakses informasi sensitif seperti nomor identitas, informasi keuangan, alamat, atau bahkan riwayat medis pengguna. Akibat dari pencurian data ini bisa sangat merugikan, termasuk potensi penyalahgunaan identitas, penipuan keuangan, dan ancaman serius terhadap privasi individu. Selain itu, data yang dicuri juga dapat diperdagangkan atau dijual di pasar gelap digital, menciptakan risiko yang lebih besar bagi korban. Oleh karena itu, upaya perlindungan data pribadi dan kesadaran tentang keamanan siber menjadi semakin penting guna melindungi informasi sensitif dan menjaga privasi online.

1.2.2 Penyalahgunaan Informasi

Penyalahgunaan informasi yang muncul akibat aktivitas hacking adalah masalah yang dapat mengakibatkan konsekuensi serius. Informasi yang dicuri oleh peretas, seperti data pribadi, keuangan, atau bisnis, dapat digunakan untuk berbagai tujuan jahat. Penyalahgunaan informasi ini dapat mencakup penipuan finansial, pencurian identitas, atau bahkan pemerasan. Selain itu, informasi yang diperoleh oleh peretas juga dapat digunakan untuk merusak reputasi individu atau organisasi, melakukan serangan siber yang lebih lanjut, atau bahkan mendukung kegiatan kriminal. Semakin berkembangnya teknologi, semakin penting untuk memahami risiko penyalahgunaan informasi dan mengambil

langkah-langkah yang efektif untuk melindungi data sensitif dan mencegah kerugian yang disebabkan oleh aktivitas hacking.

1.2.3 Dampak Sosial dan Budaya

Dampak sosial dan budaya dari aktivitas hacking telah menjadi semakin signifikan dalam era digital saat ini. hacking telah meresap ke dalam berbagai aspek kehidupan sosial dan budaya, memunculkan permasalahan yang kompleks. Secara sosial, tindakan hacking dapat merusak kepercayaan dalam hubungan online, menimbulkan ketidaknyamanan emosional, dan menciptakan ketidakpastian terkait privasi individu. Selain itu, budaya hacker yang mengagungkan prestasi teknis dan kebebasan online juga mempengaruhi pandangan masyarakat terhadap hacking. Di sisi lain, hacking dalam konteks politik atau aktivisme dapat menciptakan dinamika budaya yang menimbulkan pertanyaan tentang etika dan moralitas dalam dunia siber. Selain itu, pihak berwenang dan lembaga keamanan siber terus berusaha untuk memahami dan menangani dampak budaya hacking dalam upaya untuk menjaga keamanan siber dan integritas data. Dengan perubahan cepat dalam teknologi dan perkembangan budaya digital, penting untuk terus memantau dan mengatasi dampak sosial dan budaya dari aktivitas hacking dengan bijak dan berkelanjutan.

1.3 Akibat dari permasalahan

hacking atau hacking dapat menimbulkan berbagai akibat serius yang bervariasi tergantung pada motif peretas, sifat serangan, dan sasaran yang dipilih. Beberapa akibat umum mencakup kerugian keuangan, kehilangan data pribadi, kerusakan reputasi bagi individu dan perusahaan, kerugian bisnis, serta gangguan layanan online. Selain itu, hacking juga dapat menciptakan ketidaknyamanan emosional, mengakibatkan potensi penyalahgunaan informasi, dan memicu penyelidikan hukum serta sanksi hukum yang serius, seperti penjara bagi peretas yang tertangkap. Dampak sosial dan budaya juga signifikan, mempengaruhi pandangan masyarakat terhadap keamanan online, memicu debat tentang etika hacking, dan mendorong perubahan dalam kebijakan privasi. Oleh karena itu, pemahaman akan potensi risiko dan konsekuensi hacking menjadi penting dalam menjaga keamanan siber dan melindungi data serta privasi dalam dunia digital yang terus berkembang.

BAB II
PEMBAHASAN

2.1 Tinjauan Pustaka

Dalam konteks masalah manusia dan budaya dalam hacking, berbagai teori dan pandangan ahli telah muncul untuk memahami motivasi, dampak, dan implikasi sosial dari aktivitas hacking. Di bawah ini adalah beberapa teori dan pendapat ahli :

2.1.1 Teori Subkultur Hacker

Teori ini, yang dikembangkan oleh peneliti seperti Richard Stallman, Kevin Mitnick, dan Bruce Sterling, menggambarkan hacking sebagai subkultur dengan nilai-nilai unik. Subkultur ini mencakup budaya kerja yang kreatif, etika berbagi informasi, dan hasrat terhadap pengetahuan teknis. Ini menjelaskan bagaimana budaya peretas mempengaruhi tindakan dan motivasi mereka.

2.1.2 Teori Sosiologi Konflik

Beberapa ahli menginterpretasikan hacking sebagai bentuk perlawanan terhadap struktur sosial dan ekonomi yang ada. Mereka berpendapat bahwa hacking adalah reaksi terhadap ketidakpuasan terhadap ketidakadilan sosial, dan serangan siber dapat digunakan untuk mengganggu kekuatan yang dominan.

2.1.3 Teori Psikologi

Beberapa psikolog telah memeriksa aspek psikologis dari hacking, termasuk motif dan perilaku peretas. Mereka mempertimbangkan faktor-faktor seperti rasa ingin tahu, kebutuhan akan pengakuan, dan tingkat kecerdasan dalam menjelaskan perilaku hacker.

2.1.4 Teori Politik dan Aktivisme

Bagi beberapa ahli, hacking dianggap sebagai bentuk aktivisme digital. Mereka berpendapat bahwa hacking dapat digunakan untuk mengungkapkan ketidakpuasan terhadap pemerintah, korporasi, atau isu-isu sosial tertentu. Teori ini menghubungkan hacking dengan gerakan politik dan budaya yang lebih besar.

2.1.5 Pendekatan Interdisipliner

Beberapa ahli menggabungkan berbagai disiplin ilmu seperti sosiologi, psikologi, dan etika untuk menghadapi masalah hacking dari sudut pandang yang komprehensif. Mereka berusaha untuk memahami hacking sebagai fenomena yang kompleks yang dipengaruhi oleh faktor budaya, sosial, dan individu.

Pendekatan ini mencerminkan kompleksitas hacking dalam masyarakat modern, di mana faktor budaya, psikologis, politis, dan teknis semuanya saling terkait. Memahami berbagai teori dan pandangan akan membantu dalam mengembangkan pemahaman yang lebih mendalam tentang fenomena hacking dan membantu merumuskan kebijakan dan tindakan yang tepat dalam menghadapinya.

2.2 Langkah-Langkah pemecahan masalah

Langkah-langkah masalah dalam konteks permasalahan manusia dan budaya terkait dengan hacking atau Peretasan memerlukan pendekatan yang holistik dan komprehensif. Pendidikan dan Kesadaran Edukasi adalah kunci dalam pemecahan masalah ini. Meningkatkan kesadaran tentang risiko hacking, etika digital, dan keamanan siber adalah langkah pertama yang penting. Program pendidikan dan kesadaran dapat membantu individu dan organisasi menjadi lebih waspada terhadap ancaman hacking. Mengembangkan dan mengimplementasikan praktik keamanan siber yang kuat adalah penting. Ini termasuk penggunaan perangkat lunak keamanan yang mutakhir, pengelolaan kata sandi yang kuat, enkripsi data, serta pemantauan dan deteksi serangan yang aktif. Kerjasama antara individu, perusahaan, dan lembaga keamanan siber sangat penting. Berbagi informasi tentang ancaman dan taktik hacking dapat membantu memitigasi risiko yang lebih baik.

Mengadopsi hukum yang ketat terkait dengan hacking, serta mengambil tindakan hukum terhadap peretas yang tertangkap, adalah langkah penting dalam menegakkan hukum dan menjadikan hacking sebagai tindakan yang berisiko. Memahami dan mempromosikan etika digital yang baik dapat membentuk budaya yang lebih positif dalam penggunaan teknologi. Hal ini dapat mencakup mengajarkan nilai-nilai seperti privasi, kebebasan berbicara, dan tanggung jawab online. Mengubah budaya organisasi dan masyarakat yang mendukung keamanan siber adalah langkah

yang penting. Ini termasuk mempromosikan sikap positif terhadap pelaporan keamanan, menghargai privasi, dan membangun komunitas yang saling mendukung dalam melawan hacking. Investasi dalam penelitian keamanan siber dan inovasi teknologi adalah langkah yang penting dalam mengatasi permasalahan hacking. Teknologi yang lebih aman dan solusi keamanan yang canggih dapat membantu mengurangi risiko.

Jika terjadi hacking, penting untuk melakukan penyelidikan insiden yang menyeluruh untuk memahami bagaimana serangan terjadi dan mengidentifikasi pelaku. Ini akan membantu dalam memperbaiki keamanan dan mengambil langkah-langkah preventif lebih lanjut. Masalah hacking sering melibatkan pelaku di berbagai negara. Oleh karena itu, kerja sama internasional dalam menangani hacking dan mengadili pelaku menjadi semakin penting. Pemecahan masalah hacking memerlukan upaya lintas sektoral dan lintas batas. Ini adalah tantangan yang berkelanjutan dalam era digital yang terus berkembang, dan pendekatan yang efektif harus bersifat proaktif, adaptif, dan kolaboratif.

2.3 Pemecahan masalah

Dalam mengatasi permasalahan hacking dalam perspektif manusia dan budaya, ada sepuluh langkah kunci yang dapat ditempuh. Pertama, meningkatkan kesadaran tentang keamanan siber dan etika digital adalah tahap awal yang sangat penting. Ini melibatkan pendidikan dan kampanye kesadaran untuk memberikan pemahaman tentang risiko hacking kepada individu dan organisasi. Selanjutnya, langkah-langkah seperti menerapkan praktik keamanan siber yang kuat, berbagi informasi dan kerjasama antar pemangku kepentingan, penegakan hukum yang ketat, serta pengembangan sistem pemantauan keamanan yang efektif dan respons cepat terhadap serangan adalah bagian dari langkah-langkah komprehensif dalam melindungi diri dari ancaman hacking.

Selain itu, perubahan budaya yang mendukung keamanan siber, investasi dalam penelitian keamanan siber, penyelidikan insiden yang teliti, dan kerja sama internasional menjadi elemen-elemen penting dalam pemecahan masalah ini. Dengan langkah-langkah ini, kita dapat bergerak menuju pemecahan masalah yang lebih efektif dalam menjaga keamanan dalam era digital yang terus berkembang.

BAB III
KESIMPULAN DAN SARAN

3.1 Kesimpulan dan saran

3.1.1 Kesimpulan

hacking atau peretasan adalah masalah kompleks dalam perspektif manusia dan budaya dalam era digital. Dalam pemahaman ini, kita melihat bagaimana hacking tidak hanya melibatkan tindakan teknis, tetapi juga mencakup faktor budaya, sosial, dan individu yang mempengaruhinya. hacking dapat memiliki dampak serius, termasuk pencurian data pribadi, penyalahgunaan informasi, dan dampak sosial serta budaya yang luas. Untuk mengatasi permasalahan ini, pendekatan holistik diperlukan, yang mencakup pendidikan dan kesadaran, praktik keamanan siber yang kuat, kerjasama antar pemangku kepentingan, penegakan hukum, dan inovasi teknologi.

3.1.2 Saran

Saran untuk mengatasi hacking dan menjaga keamanan siber, diperlukan langkah-langkah yang komprehensif.

1. Pendidikan dan Kesadaran : Tingkatkan kesadaran tentang risiko hacking dan etika digital melalui program pendidikan dan kampanye kesadaran.
2. Kerjasama Antar Pemangku Kepentingan: Berbagi informasi tentang ancaman hacking dan kerja sama antar individu, perusahaan, dan lembaga keamanan siber.
3. Penegakan Hukum: Tindak hacking secara hukum dan adili pelaku yang tertangkap.
4. Inovasi Teknologi: Investasikan dalam penelitian keamanan siber dan teknologi yang lebih aman.
5. Perubahan Budaya: Promosikan budaya yang mendukung keamanan siber, termasuk menghargai privasi dan membangun komunitas yang mendukung.
6. Kerja Sama Internasional: Tingkatkan kerja sama lintas negara dalam menangani hacking.

DAFTAR PUSTAKA

Buku

Jasman. 2015. *Panduan Praktis WEB hacking dari subkultural programmer*. Cetakan kesatu, C.V ANDI OFFSET (Penerbit ANDI). Yogyakarta.

E-journal

Indah Sari. indah.alrif@gmail.com (Mengenal hacking Sebagai Salah Satu Kejahatan Di Dunia Maya), Universitas Dirgantara Marsekal Suryadarma.

Hasbi Ash Shaddiqi, SKRIPSI. (Subkultur Anak Muda Hacker Di Dunia Maya), IR - Perpustakaan Universitas Airlangga.

Bambang Hartono. bambanghartono@rocketmail.com (Hacker Dalam Perspektif Hukum Indonesia), Fakultas Hukum UBL, Jl. Za Pagar Alam No 26 Labuhan Ratu, Bandar Lampung 35142. E-jurnal UNDIP : https://ejournal.undip.ac.id/index.php/mmh/article/view/9021/7326

MOHD. Yusuf DM, Suryadi, Robi Hamid. boyke457@gmail.com (Analisis Kejahatan hacking Sebagai Bentuk Cyber Crime Dalam Sistem Hukum yang berlaku di Indonesia). Ilmu Hukum, Fakultas Hukum, Universitas Lancang Kuning.

Gani, A.G. 2018, Cybercrime (Kejahatan Berbasis Komputer), Jurnal Sistem Informasi Universitas Suryadarma, Vol 5, No 1, DOI: https://doi.org/10.35968/jsi.v5i1.18

Sumber Rujukan dari Website

https://chat.openai.com/c/cf9d6f50-3d57-4dfb-a437-b0d640c9fa53. Diakses tanggal 29 September 2023.