Denise Felicia Tiowanni (K1 - 13522013)
Erdianti Wiga Putri Andini (K1 - 13522053

Social Media Used for Hacking

Berdasarkan artikel ‘Dampak Sosial Media’ yang terdapat pada halaman tugas edunex.com, didapatkan informasi bahwa *hacking* adalah kegiatan ilegal yang menjadi kerugian terbesar dari media sosial bagi orang-orang. *Hacking* adalah aktivitas mendapatkan akses ke informasi pribadi dan terbatas milik orang lain tanpa izin. Dalam penelitian penulis artikel tersebut mengenai kelebihan dan kekurangan media sosial, para peneliti menemukan bahwa remaja dan anak-anak adalah kelompok yang paling rentan menjadi korban hacker. Fenomena ini semakin memprihatinkan dengan adanya laporan pada bulan Januari 2019, di mana sejumlah akun pribadi di Facebook, WhatsApp, dan Twitter telah diretas. Sebagian besar *hacker* melakukan aksi mereka dengan cara meretas akun-akun ini, kemudian memeras para korban dengan memposting informasi pribadi mereka di media sosial atau mengancam untuk mengungkapkan data sensitif mereka. Tindakan ini tidak hanya menempatkan kehidupan pribadi individu dalam bahaya, tetapi juga dapat mengakibatkan stres psikologis dan dampak sosial yang serius bagi korban. Selain itu, *hacker* sering kali mengirimkan pesan spam yang dapat menciptakan gangguan atau bahkan melakukan penipuan yang merugikan. Masalah ini menjadi semakin kompleks karena *hacking* bukan hanya berdampak pada individu, tetapi juga dapat mencakup pencurian data bisnis yang vital. Data yang dicuri dari bisnis dapat menyebabkan kerugian finansial yang signifikan, baik untuk perusahaan itu sendiri maupun untuk pelanggan mereka. Dalam banyak kasus, kerugian finansial ini bisa berlanjut dengan dampak jangka panjang terhadap reputasi dan stabilitas bisnis.

Pada tahun 2020, terdapat beberapa kasus *hacking* atau peretasan yang menimpa tokoh masyarakat dan organisasi di Indonesia. Bivitri Susanti, seorang pakar hukum dan pengajar di Sekolah Tinggi Hukum Indonesia Jentera, menjadi korban peretasan akun media sosialnya pada 20 April 2020, menjelang aksi demonstrasi[1]. Akun Instagramnya mengunggah konten yang menuduh partai politik tertentu sebagai dalang aksi, dan WhatsApp pribadinya juga diretas. Bivitri menyebut peretasan ini sebagai pelanggaran hak asasi manusia dan meminta tindakan tegas dari pemerintah. Selain itu, sejumlah anggota Aliansi Mahasiswa Indonesia (AMI) juga mengalami peretasan akun WhatsApp mereka menjelang aksi demonstrasi pada 21 April[1]. Sebanyak 11 orang dari AMI, termasuk Ketua BEM Universitas Indonesia, menjadi korban peretasan, yang sudah pernah terjadi sebelumnya pada aksi demonstrasi 1 April. Kasus lain menimpa akun Instagram Lampung Memanggil, yang dikelola oleh organisasi gerakan sipil[1]. Akun ini diretas setelah mereka memberikan ultimatum kepada pemerintah untuk menstabilkan harga pangan dan bahan bakar minyak. Akses ke akun tersebut hilang menjelang konsolidasi yang diadakan pada 15 April. Peretasan juga dialami oleh Ketua Umum Pengurus Besar Pergerakan Mahasiswa Islam Indonesia (PB PMII), Muhammad Abdullah Syukri[1]. Akun WhatsApp-nya diduga diretas pada 9 April, kemungkinan terkait dengan aksi kritik mahasiswa terhadap berbagai isu nasional. Akun WhatsApp Abdullah kemudian dikloning dan digunakan untuk menghubungi orang lain atas namanya. Kasus serupa terjadi pada Koordinator Pusat BEM Seluruh Indonesia, Kaharuddin HSN DM, yang mengalami peretasan akun Instagram dan WhatsApp pada 7 April[1]. Peretasan ini menyulitkannya berkomunikasi dengan mahasiswa dan wartawan. Ketua Umum Aliansi Jurnalis Independen (AJI), Sasmito Madrim, juga menjadi korban peretasan pada 23 Februari[1]. Akun media sosialnya mengunggah konten tidak senonoh dan pesan dukungan terhadap proyek pembangunan Bendungan Bener di Wadas, Purworejo. AJI mengecam peretasan ini sebagai serangan terhadap kebebasan pers. Terakhir, sejumlah akun WhatsApp dan media sosial pengurus Badan Eksekutif Mahasiswa Universitas Indonesia (BEM UI) diretas pada 27 Juni, setelah BEM UI mengkritik Presiden Joko Widodo dengan sebutan 'The King of Lip Service'[1]. Peretasan ini menyasar beberapa anggota BEM UI yang terlibat dalam aksi tersebut.

Selain itu, kita dapat melihat contoh lain dari serangan *hacking* yang terjadi pada Juli 2020. Pada 15 Juli 2020, antara pukul 20:00 dan 22:00 UTC, terjadi serangan hacking yang menargetkan sejumlah akun Twitter terkenal. Dalam insiden tersebut, para peretas berhasil mengakses dan mengendalikan setidaknya 130 akun yang dimiliki oleh tokoh-tokoh publik terkenal seperti Elon Musk, Barack Obama, Joe Biden, serta perusahaan-perusahaan besar seperti Apple dan Uber[6]. Para pelaku memanfaatkan akses ini untuk memposting pesan-pesan penipuan yang menyebarluaskan skema Bitcoin palsu. Mereka menyebarkan informasi yang menipu dengan menjanjikan pengembalian dua kali lipat dari bitcoin yang dikirim ke dompet tertentu. Taktik yang digunakan oleh para peretas termasuk teknik rekayasa sosial yang canggih untuk memperoleh akses ke alat administratif Twitter. Mereka menargetkan karyawan Twitter dengan cara memperoleh informasi pribadi mereka melalui LinkedIn dan sumber lainnya. Dengan menggunakan informasi ini, para peretas berpura-pura menjadi staf Twitter dan menipu karyawan untuk memberikan kredensial serta kode autentikasi dua faktor (2FA) yang diperlukan. Hal ini memungkinkan mereka untuk mengakses dan mengendalikan sistem internal Twitter[7]. Dengan memperoleh akses ke alat administratif Twitter, para peretas kemudian dapat mereset kata sandi dan memposting tweet dari akun-akun profil

tinggi tersebut. Akibat dari tindakan ini, lebih dari $110.000 dalam bentuk bitcoin berhasil dicuri sebelum Twitter berhasil menghapus pesan-pesan scam tersebut. Selain dampak finansial langsung, insiden ini juga menyebabkan penangguhan kemampuan *tweeting* untuk beberapa pengguna dan memengaruhi layanan penting seperti pengiriman peringatan cuaca oleh National Weather Service. Akibat keseluruhan dari peretasan ini juga memengaruhi harga saham Twitter, yang mengalami penurunan sebesar 4% setelah kejadian tersebut.

Dari contoh-contoh yang telah dijabarkan diatas, kita dapat melihat bahwa *hacking* melalui platform sosial media memiliki berbagai macam dampak yang signifikan. *Hacker* sering memanfaatkan kerentanan pada platform ini untuk mengakses data pengguna, seperti nama, alamat email, dan pesan pribadi. Data ini kemudian dapat dijual di pasar gelap atau digunakan untuk melancarkan serangan lebih lanjut. Contoh spesifik dari cara *hacking* dapat mengkompromikan informasi meliputi serangan *phishing*, di mana *hacker* mengirim pesan yang mengaku berasal dari perusahaan sah seperti bank atau lembaga pemerintah, berisi tautan ke situs web palsu. Jika pengguna memasukkan detail login mereka di situs palsu tersebut, *hacker* dapat mencuri informasi mereka. Serangan *malware* juga menjadi ancaman serius, di mana *hacker* membagikan tautan atau file yang mengandung *malware*. Mengklik tautan atau membuka file tersebut dapat menginfeksi perangkat pengguna dan mencuri informasi pribadi. Selain itu, serangan *watering hole* melibatkan penyisipan *malware* pada situs web populer untuk menargetkan kelompok orang tertentu. Ketika pengguna mengunjungi situs tersebut, *malware* dapat kemudian menginfeksi perangkat mereka dan menyebabkan kerusakan yang parah pada sistem[8].

Kemudian, berdasarkan suatu jurnal, terdapat pula beberapa teknik *hacking* lainnya yang juga umum digunakan oleh peretas untuk mencuri informasi atau mengakses sistem. Teknik yang pertama adalah *Dictionary Attack*, di mana peretas menggunakan daftar kata atau pola kata untuk mencoba menebak kata sandi[2]. Metode ini dapat lebih canggih dengan menggunakan pola tertentu (*pattern-based*) atau dilakukan secara *offline* untuk menyerang kartu pintar. Untuk mencegah serangan ini, dapat dilakukan pemilihan kata sandi dan nama pengguna yang sulit ditebak, dengan pola yang kompleks, mengandung karakter khusus, serta panjang minimal tujuh karakter. Selain itu, strategi pertahanan berupa pemblokiran sementara akun setelah beberapa kali gagal login juga dapat diterapkan. Sistem karakter tree juga digunakan untuk memastikan kata sandi bukan merupakan kata yang mudah ditebak[2]. Teknik lainnya adalah *Web-Based Attack*, yang menyasar aplikasi web melalui serangan seperti *Inspect Element* untuk memodifikasi kode sumber, *SQL Injection* untuk menyisipkan kode berbahaya ke dalam query database, serta *Cross-Site Scripting (XSS)* yang memanfaatkan kelemahan input pada aplikasi untuk mengirim skrip berbahaya kepada pengguna[2]. Selain itu, serangan *Buffer Overflow* terjadi ketika data yang dimasukkan melebihi kapasitas buffer, menyebabkan crash atau kerentanan sistem. Untuk mencegah serangan web berbasis seperti SQL injection, dilakukan validasi input dan penggunaan parameter SQL yang aman. Penting juga untuk tidak mengasumsikan ukuran, tipe, atau konten data yang diterima, serta melakukan penolakan terhadap nilai biner dan karakter komentar. Sementara itu, untuk mencegah cross-site scripting, semua karakter spesial harus difilter dan textboxes dibuat non-eksekusi. Teknik sandboxing digunakan untuk melindungi aplikasi dari serangan buffer overflow[2]. Selanjutnya terdapat teknik *Phishing* yang merupakan teknik di mana peretas memanipulasi korban agar memberikan informasi rahasia, misalnya melalui email palsu atau situs web tiruan[2]. Ada beberapa cara untuk melakukannya, seperti menggunakan layanan hosting gratis, hosting berbayar, atau membajak perangkat untuk mengontrol server web. Pencegahan *phishing attack* dilakukan dengan memeriksa tautan secara teliti, memperhatikan browser, toolbars, dan URL. Pengguna juga harus selalu waspada terhadap email yang meminta informasi pribadi dan menggunakan antivirus yang selalu diperbarui. Selain itu, penting untuk menghindari iklan dan popup yang mencurigakan[2]. Selain itu, *Wireless Hacking* memanfaatkan jaringan nirkabel yang tidak aman untuk mengakses data perangkat lain, sering kali menggunakan alat seperti AirSnort untuk memecahkan kunci enkripsi[2]. Dalam mencegah serangan jaringan nirkabel, hindari terhubung ke jaringan terbuka yang tidak terpercaya. Nama jaringan (SSID) sebaiknya tidak disiarkan, login router harus diubah dari pengaturan default, dan enkripsi yang lebih kuat seperti WPA/WPA2 harus digunakan. Perangkat router juga harus sering diperbarui, dan dimatikan saat tidak digunakan[2]. Metode lainnya adalah *Directory Harvesting Attack*, di mana peretas mengumpulkan alamat email dengan menguji berbagai kombinasi untuk menemukan yang valid[2]. Pencegahan directory harvesting attack dapat dilakukan melalui perlindungan berbasis host yang menyaring lalu lintas dari penyerang berdasarkan laporan kesalahan. Selain itu, perlindungan berbasis jaringan melibatkan kerja sama dengan pihak lain, di mana server yang diserang melaporkan alamat IP penyerang ke server pusat untuk mendapatkan perlindungan yang lebih luas[2]. Terakhir, *Keylogger* adalah perangkat lunak atau perangkat keras yang merekam ketukan tombol pengguna untuk mencuri informasi penting, yang dapat diklasifikasikan sebagai perangkat keras, akustik, nirkabel, atau berbasis perangkat lunak[2]. Untuk mencegah keylogger, pengguna dapat mengubah tata letak keyboard menjadi bahasa palsu yang unik, sehingga log file yang dihasilkan oleh keylogger menjadi tidak dapat digunakan oleh penyerang[2].

Paragraf sebelumnya membahas bagaimana cara mencegah adanya peretasan alias *hacking* berdasarkan teknik-teknik *hacking*. Pencegahan tersebut berfokus pada bagaimana cara media sosial atau platform-platform lain untuk menghindari terjadinya peretasan pada sistem mereka. Sebenarnya pengguna pun dapat melakukan pencegahan peretasan ini, tidak hanya bergantung pada sistem keamanan platform. Bagi pengguna aktif media sosial, penting untuk mengetahui langkah-langkah pencegahan guna meminimalkan risiko dan melindungi akun dari peretasan. Berikut adalah beberapa cara yang bisa dilakukan: Pertama, gunakan kata sandi yang kuat dengan kombinasi angka dan huruf, serta pastikan setiap akun memiliki kata sandi yang berbeda. Mengubah kata sandi secara berkala juga penting. Kedua, aktifkan autentikasi dua faktor (2FA) untuk menambah lapisan keamanan, karena metode ini meminta verifikasi identitas dua kali. Ketiga, aktifkan peringatan masuk perangkat baru agar mendapat notifikasi jika ada upaya akses dari perangkat yang tidak dikenali. Jika notifikasi tersebut muncul, segera ganti detail login. Keempat, hindari mengklik tautan yang mencurigakan, karena phishing sering digunakan untuk mencuri informasi login. Terakhir, buat alamat email khusus untuk media sosial agar data pribadi tetap aman jika akun media sosial diretas[3].

Terkadang pengguna media sosial tidak menyadari bahwa media sosial mereka sedang diretas. Beberapa hal yang menandakan bahwa media sosial diretas antara lain: adanya postingan yang tidak pernah dibuat oleh pengguna, teman atau pengikut pengguna menerima pesan pribadi yang tidak wajar dari akun pengguna, menerima email notifikasi terkait perubahan pada akun yang tidak pernah pengguna lakukan, serta munculnya aktivitas lain yang tidak pengguna lakukan, seperti menyukai postingan, mengirim permintaan pertemanan, berhenti mengikuti, atau memblokir akun lain tanpa sepengetahuan pengguna. Tentu saja pengguna harus melakukan hal-hal untuk mengatasi peretasan akun media sosial mereka. Langkah pertama yang perlu dilakukan adalah segera mengubah kata sandi akun tersebut, terutama jika masih memiliki akses. Selanjutnya, pengguna perlu mengaktifkan autentikasi dua faktor (2FA) untuk meningkatkan keamanan. Pengguna dapat melaporkan peretasan kepada platform media sosial terkait agar pihak media sosial tersebut dapat membantu mengamankan akun pengguna. Selain itu, pengguna dapat memeriksa dan menghapus perangkat atau aplikasi yang mencurigakan yang terhubung ke akun. Jika akun sudah diretas dan konten berubah, pengguna dapat melaporkan kejadian kepada kontak yang relevan serta berhati-hati terhadap tautan atau pesan mencurigakan[4]. Setiap media sosial memiliki cara pelaporan kasus yang berbeda-beda, maka setiap pengguna harus mengetahui bagaimana cara melapor pada setiap media sosial yang mereka miliki.

Peretasan sosial media ini biasanya berkaitan erat dengan kebocoran data pengguna. Bila peretasan sudah terjadi, kebocoran data ini perlu segera diatasi. Untuk mengatasi kebocoran data, diperlukan peran aktif dari pemerintah, perusahaan, dan masing-masing individu pengguna. Pemerintah harus segera menetapkan undang-undang yang jelas seperti RUU Perlindungan Data Pribadi (PDP) untuk memberikan landasan hukum yang kuat dalam melindungi data masyarakat. Perusahaan baik itu sosial media maupun instansi-instansi lain perlu memperkuat sistem keamanan digital dengan meningkatkan arsitektur data serta merekrut pekerja profesional yang kompeten dalam mengelola basis data sehingga tidak mudah diretas. Selain itu, masing-masing individu juga harus meningkatkan literasi keamanan digital dengan menggunakan kata sandi berbeda untuk setiap akun, bijak dalam membagikan data pribadi, serta berhati-hati terhadap situs atau aplikasi yang mencurigakan. Upaya bersama ini akan membantu mengurangi risiko kebocoran data dan menjaga keamanan digital secara lebih efektif[5].

Dengan demikian, dapat disimpulkan bahwa *hacking* merupakan suatu ancaman serius yang memiliki dampak luas dan beragam, terutama dalam lingkup media sosial. Media sosial sering menjadi sasaran peretas karena kerentanannya yang dapat menyebabkan kebocoran data pribadi dan dampak psikologis bagi seorang individu maupun perusahaan. Kasus peretasan yang menargetkan tokoh masyarakat, organisasi, dan perusahaan menunjukkan betapa signifikan dan luasnya masalah ini. Serangan *hacking*, seperti *phishing*, *malware*, dan teknik rekayasa sosial, menyoroti pentingnya pencegahan dan perlindungan yang memadai. Untuk mengatasi peretasan, diperlukan upaya bersama antara pemerintah, perusahaan, dan individu. Pemerintah harus menetapkan regulasi yang ketat, perusahaan harus memperkuat keamanan sistem, dan individu harus menerapkan langkah-langkah pencegahan yang proaktif, seperti menggunakan kata sandi yang kuat dan autentikasi dua faktor (2FA). Kesadaran dan tindakan preventif ini penting untuk melindungi data dan mengurangi risiko peretasan di media sosial.

Denise Felicia Tiowanni (K1 - 13522013)
Erdianti Wiga Putri Andini (K1 - 13522053

Referensi

[1] https://www.facebook.com/CNNIndonesia. (2022, April 23). 7 kasus peretasan akun medsos aktivis pengkritik pemerintah. *Nasional*. https://www.cnnindonesia.com/nasional/20220423122302-20-788688/7-kasus-peretasan-akun-medsos-aktivis-pengkritik-pemerintah

[2] Staff, I. (2017). *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*.

[3] Yudha, T. (2022, October 1). 5 Cara Melindungi Akun Media Sosial Pribadi dari Hacker. *SINDOnews Tekno*. https://tekno.sindonews.com/read/900617/207/5-cara-melindungi-akun-media-sosial-pribadi-dari-hacker-1664619032#:~:text=A%20A%20A%201%201.%20Pilih%20kata%20sandi,5.%20Buatlah%20email%20khusus%20untuk%20media%20sosial.%20

[4] *Sosmed Kena Hack? Ikuti Langkah Cepat Ini untuk Mengatasinya*. (n.d.). Wwwallianzcoid. https://www.allianz.co.id/explore/sosmed-kena-hack-tenang-ikuti-langkahlangkah-cepat-ini-untuk-mengatasinya.html

[5] Itsojt. (2022, November 2). *Menyikapi Kasus Kebocoran Data Pribadi di Era Digital - ITS News*. ITS News. https://www.its.ac.id/news/2022/11/02/menyikapi-kasus-kebocoran-data-pribadi-di-era-digital/

[6] CNN. (2020, July 15). Twitter Hack: Elon Musk, Bill Gates, and Others Targeted in Massive Attack. Diakses dari https://edition.cnn.com/2020/07/15/tech/twitter-hack-elon-musk-bill-gates/index.html

[7] Wiggins, T. (2020, July 15). Twitter Hack: How the Attackers Took Over High-Profile Accounts. TechCrunch. Diakses dari https://techcrunch.com/2020/07/15/twitter-hacker-admin-scam/

[8] InterplayIT. (n.d.). The effects of social media on cybersecurity. Retrieved from https://www.interplayit.com/blog/the-effects-of-social-media-on-cybersecurity/

)