Kenapa Ya Androidku Kena Hack?

Christian Yudistira Hermawan

2306241676

Muda ini, mobilisasi digital merupakan salah satu hal yang bertumbuh dengan sangat pesat. Hal ini didukung oleh perkembangan media platform yang juga terus berkembang seiring zaman. Selaras dengan dua faktor ini, akses sarana dan pra sarana media turut berkembang, terlebih di dunia mobile dengan basis platform berbentuk android maupun IOS mobile yang dapat lebih diintegrasikan dengan mobilitas manusia. Eksistensi dari platform mobile ini memberikan kemudahan dalam mengakses dan menyalurkan berbagai informasi dengan cepat dan efisien, namun di tengah maraknya perkembangan ini, masih ada *concern* yang sangatlah penting untuk diperhatikan.

Pepatah mengatakan “semakin besar suatu sistem, semakin besar pula resikonya”, hal ini sangat menggambarkan situasi dunia digital sekarang. Pengguna platform mobile seringkali menjadi sasaran empuk *cybercriminal* karena tingkat keamanan siber yang sangat rentan. Saya sendiri sebagai pengguna platform mobile berbasis Android merasakan bahwa keamanan data di sistem ini kurang memadai apabila dijalankan tanpa *supervise* yang benar. Meskipun belum pernah mengalaminya, saya sering melihat secara langsung bagaimana platform ini disalahgunakan para oknum yang tidak bertanggung jawab. Hal yang menjadi pertanyaannya ialah, kenapa harus platform Android? Apakah ada keunikan di platform Android?

Dalam memahami permasalahan ini, kita harus paham betul bahwa ada 3 struktur dasar yang menopang pertumbuhan akses digital dalam segala aspek. Struktur tersebut ialah software (perangkat lunak), hardware (perangkat keras), dan brainware (perangkat manusia/pengoperasi). Eksistensi dari ketiga aspek ini saling berkesinambungan dan mendukung berdirinya sebuah platform digital, ketiga hal

ini harus ada dan juga memiliki kontribusi yang sesuai porsinya demi menciptakan keamanan siber yang memadai. Hilangnya kekuatan pada 3 faktor penopang ini akan berakibat fatal dan menurut saya hal ini menjadi pemicu dari rentannya keamanan siber.

Android merupakan platfom yang sangat popular dan menjadi platform mobile paling banyak digunakan di dunia. Basis platform Android dapat digolongkan sebagai sektor *software*.

"*Firstly, the open nature of the Android platform allows for greater flexibility and customisation, making it easier for malicious actors to create and distribute fake app stores or unauthorised apps*,"

berdasarkan pernyataan yang dikatakan oleh Mr Steven Scheurmann selaku ketua *cybersecurity* ASEAN dari Palo Alto Networks, Android dikatakan sangat fleksibel terhadap kostomisasi. Fleksibilitas ini menjadi pisau bermata dua karena dapat juga digunakan oknum untuk membuat aplikasi yang berbahaya. Selain itu, keterbukaan google play sebagai pengakses aplikasi utama pada android juga memiliki kesulitan dalam meregulasi dan memonitor aplikasinya. Hal ini mengakibatkan adanya *fraud* yang seringkali lolos publikasi di platform ini. Dari segi software, dapat disimpulkan bahwa fleksibilitas Android merupakan kelebihan serta kekurangan utamanya.

Fleksibilitas mungkin masih menjanjikan ketika kita mampu mengatur variable kontrol dalam penggunaan Android (selektif dalam menginstall ataupun penggunaan secara general), namun ketika membahas tentang hardware yang menjadi komponen dasar berjalannya platform, hal ini cenderung lebih sulit untuk diatasi. Android seringkali dikaitkan dengan afordabilitas harganya yang disebabkan oleh keragaman produsen dan komponen perangkatnya. Saya sendiri merupakan pengguna Android, berbasis Mi UI (kostomisasi Xiaomi) pada perangkat Poco F5. Harga yang ditawarkan memang fantastis, namun apakah ada *tradeoff*nya? Jawabannya ada, ada banyak kasus data bocor di penggunaan perangkat Xiaomi meskipun perangkat ini *midrange priced*. Dapat dibayangkan

apabila perangkat terus ditekan harganya demi memenuhi kebutuhan khalayak ramai, pasti ada hal lain yang dikorbankan.

Manufaktur yang menggunakan berbagai macam komponen mungkin mampu menekan harga perangkat, namun juga dapat memperbesar potensi adanya celah keamanan. Beberapa komponen seperti chipset atau modul lainnya pasti memiliki kelemahan, dan kelemahan ini cenderung semakin besar, berbanding terbalik dengan harga perangkat (semakin murah perangkat semakin rentan juga perangkat tersebut). Maka sebagai pengguna, kita harus selektif dalam memilih *daily driver* kita. Sedikit tambahan, masalah hardware ini mungkin dapat diatasi dengan perbaruan berkala driver. Manufaktur yang kredibel pasti akan terus meng-*update* driver hardware mereka, namun hal ini tidak dapat menjadi acuan dikarenakan variable ini tidak dapat dikontrol oleh pengguna.

Dalam mengontrol dua variable di atas, menurut saya user adalah kunci utamanya dan perlu diketahui bahwa user ialah brainware yang menjadi operator sebuah platform. Brainware/pengguna/penikmat merupakan terdampak bahkan berpotensi menjadi korban/calon korban dari serangan siber di platform manapun. Secanggih apapun teknologi dalam mendeteksi serangan siber, tetap manusia lah yang membuat keputusan penting, sebuah brainware selalu menjadi akhir ataupun awal dari serangan siber. Oleh karena itu, dibutuhkan **pengetahuan digital yang baik** oleh pengguna dalam penggunaan suatu platform.

Kembali ke pertanyaan awal, mengapa Android? Secara statistika, platform Android merupakan platform *mobile* terbanyak pertama di dunia dalam hal penggunaan. Data demografi juga memaparkan fakta bahwa platform Android cenderung lebih banyak digunakan di negara berkembang seperti di Asia Tenggara termasuk Indonesia. Populasi manusia pada seluruh negara berkembang cenderung lebih banyak disbanding negara maju dan data juga menyatakan bahwa negara ini memiliki jumlah dan tingkat pendidikan yang jauh lebih rendah dibanding negara maju. Penarikan benang merah saya menyimpulkan satu hal, kurangnya Pendidikan mempengaruhi tingkat literasi digital, dan tingkat literasi digital yang rendah akan menghasilkan brainware/pengguna yang kurang mampu me *manage risk*

penggunaan perangkat mereka. Pada poin ini, bukan platform Android penyebabnya, namun pengguna lah yang bertanggung jawab untuk memahami dan meningkatkan literasi digital mereka.

Karena brainware menjadi pusat keputusan, brainwarelah yang biasanya menjadi celah paling rentan untuk sebuah perangkat mengalami serangan siber. Maka dari itu perlu adanya kesadaran pengguna tentang potensi ancaman seperti phising, malware, dan lainnya. Apabila pengguna memahami dan sadar akan *threats* ini kemungkinan pengguna terkena serangan siber akan semakin kecil begitupun sebaliknya. Secara tidak langsung hal ini menekankan bahwa tingkat pendidikan akan menunjang pentingnya literasi digital dan demografi pengguna pada daerah sangat berperan penting dalam keamanan siber.

Dengan mengkonsiderasikan tiga faktor ini, saya melihat bahwa langkah nyata haruslah diterapkan. Sebagai pengguna android saya selalu melakukan beberapa hal untuk memastikan bahwa saya tidak akan menjadi korban serangan siber. Saya selalu melakukan perbaruan software rutin, dan sebelum membeli atau memilih perangkat saya selalu melihat kredibilitas manufaktur hardware dari perangkat ini. Untuk penggunaan aplikasi, saya juga menggunakan autentikasi dua faktor (2FA) yang memberikan saya keamanan ekstra dengan mengakomodir password yang lebih kompleks. Selain permasalahan teknis, seperti yang sudah dibahas brainware lah yang terpenting, maka sebagai mahasiswa Ilmu Komputer saya juga terus menambah ilmu terkait keamanan siber dasar yang mampu menjadi bekal saya untuk melindungi diri saya sendiri dari celah celah yang ada.

Hal – hal yang bisa dikontrol dari brainware sangat mempengaruhi proteksi dari serangan siber, namun ada baiknya kita juga harus memberikan *backup* demi mengatasi hal – hal tidak terduga. Hal ini saya lakukan dengan mengenkripsi data penting saya dan selalu menggunakan VPN dalam mengakses wifi publik. Begitupun dengan membackup secara rutin data di cloud agar terdapat akses lebih baik apabila suatu saat ada serangan siber yang menghilangkan data saya. Terakhir, *awareness* juga merupakan hal yang krusial, maka sebagai brainware yang bijak kit

aharus mematau segala aktivitas akun secara berkala dan langsung menindak langsung apabila ada hal yang mencurigakan.

Berdasarkan seluruh pembahasan ini, dapat disimpulkan bahwa Android merupakan sebuah platform yang ditopang oleh *software, hardware,* dan *brainware* sama halnya dengan platform lain. Akar permasalahan ini sebenarnya ialah literasi digital dan selektifitas sang pengguna terhadap resiko penggunaan media di platform apapun. Pada akhirnya, sebagai user kita harus lebih memahami bagaimana ketiga hal fundamental ini bekerja, berkorelasi dan berkesinambungan untuk menciptakan keamanan siber yang kuat di platform manapun.

DAFTAR PUSTAKA

Channel News Asia. (2024, September 3). *Android malware scams: Why cybercriminals target Google's operating system over Apple's iOS.* Channel News Asia. Diakses dari https://www.channelnewsasia.com/singapore/android-malware-scams-google-apple-operating-systems-cybersecurity-cna-explains-3661566

AppMySite. (2023, Maret 8). *Android vs iOS: Mobile operating system market share & statistics you must know.* AppMySite. Diakses dari https://www.appmysite.com/blog/android-vs-ios-mobile-operating-system-market-share-statistics-you-must-know/

The Economic Times. (2024, September 2). *Beware Android users: This new malware can steal your phone data and misuse bank details - Know how to stay safe.* The Economic Times. Diakses dari https://economictimes.indiatimes.com/news/international/us/beware-android-users-this-new-malware-can-steal-your-phone-data-and-misuse-bank-details-know-how-to-stay-safe/articleshow/110711941.cms?from=mdr

Kaspersky. (2023, September 1). *How to avoid threats from budget Android devices.* Kaspersky. Diakses dari https://www.kaspersky.com/blog/how-to-avoid-threats-from-budget-android-devices/49565/