Pemanfaatan Infrastruktur Seluler untuk Pencegahan Pengambilalihan Akun Mobile Banking PT Bank XYZ = Cellular Infrastructure Utilization for Mobile Banking Account Takeover Prevention in Bank XYZ

Aldiansah Prayogi, author

Abstrak

Pandemik Covid 19 dan pemberlakuan pembatasan kegiatan masyarakat di Indonesia telah dilalui juga dengan terjadinya peningkatan 71% transaksi mobile banking. Bank XYZ merupakan salah satu Bank milik BUMN dan sebagian sahamnya juga dimiliki oleh publik ikut berdampak dengan delapan kali lipat pengguna dan lima kali lipat transaksi mobile banking hingga 2022. Melihat peningkatan pengguna dan transaksi mobile banking ini juga menjadi perhatian penjahat siber untuk mengambil kesempatan. Hal ini ditunjukkan dengan ditangkapnya 13 pelaku pengambilalihan 493 akun nasabah mobile banking dengan kerugian 12 milyar Rupiah melalui social engineering, phishing, dan file .apk palsu untuk mengakses inbox SMS OTP atau Magic Link. Bank XYZ pun terkena serangan tersebut dengan didapatkannya 1008 akun impersonasi Bank XYZ di Whatsapp dan 500 kasus pengambilalihan akun serta pencurian uang nasabah mobile banking sejak 2022 dengan kerugian milyaran Rupiah. Akar masalah telah dianalisis dari sisi People, Process, dan Technology serta telah ditentukan sisi Technology untuk diberikan solusi untuk pencegahannya. Tinjauan literatur digunakan untuk mencari penelitian sebelumnya dan referensi pendukung penelitian ini dengan 3C+2S serta membentuk kerangka teoretis. Desain dan tahapan penelitian ini dibuat, mulai dari identifikasi masalah, tinjauan literatur, penggunaan kerangka kerja NIST CSF dan COBIT untuk menerapkan teknologi pencegahan pengambilalihan akun mobile banking, dan validasi rancangannya dengan manajemen PT Bank XYZ. Teknologi yang disarankan untuk menjadi solusi pencegahan pengambilalihan akun mobile banking adalah pengembangan atau pengganti SMS OTP atau Magic Link dengan memanfaatkan infrastruktur seluler. Verifikasi dilakukan pada jaringan inti seluler (MME, SGW, dan GGSN/PGW) dengan membandingkan kesesuaian nomor telepon yang terdaftar di aplikasi dengan nomor telepon yang sedang digunakan di smartphone atau tablet menggunakan Header Enrichment. Dengan demikian, penjahat siber yang memiliki kredensial korban, tidak bisa mengambilalih akun dan mencuri uang nasabah di mobile banking, karena penjahat siber tidak memiliki nomor telepon yang terpasang di smartphone atau tablet-nya. Pengetesan dilakukan dengan API yang disediakan salah satu operator seluler dengan mengintegrasikan ke aplikasi prototype yang dibuat. Hasil yang diperoleh dari beberapa skenario pengetesan, pengambilalihan akun tidak dapat terjadi, rancangan desain aksi penerapan teknologi autentikasi sudah tervalidasi, dan dapat dijadikan acuan.

.....The Corona virus 19 pandemic and the gathering activity restrictions in Indonesia have been passed with an increase of 71% in mobile banking transactions. Bank XYZ is a state-owned bank and which part of its shares are also owned by the public has had an impact too with eight times more users and five times more transactions of mobile banking until 2022. Seeing the increase in mobile banking users and transactions, it is also a concern for cybercriminals to take advantage. This was shown by the arrest of 13 threat actors who have taken over 493 mobile banking customer accounts with a loss of 12 billion Rupiah through social engineering, phishing, and fake .apk files to access OTP SMS inboxes or Magic Link. The attack also hit

Bank XYZ by obtaining 1008 Bank XYZ impersonation accounts on Whatsapp and 500 cases of account takeover and theft of mobile banking customer money since 2022 with losses about billions of Rupiah. The root cause problem has been analyzed from the People, Process, and Technology side, then a Technology side has been determined to provide a solution for its prevention. The Literature review is used to find previous research and references to support this research with 3C + 2S also build a theoretical framework. The design and stages of this research were made, starting from identifying the problem, reviewing the literature, using the NIST CSF and COBIT frameworks for technology implementation to prevent takeover of mobile banking accounts, and validating the design with management of Bank XYZ. The recommended technology to be a solution to prevent takeover of mobile banking accounts is the development or replacement of SMS OTP or Magic Link by utilizing cellular infrastructure. Verification is carried out on the cellular core network (MME, SGW, and GGSN/PGW) to do comparison between the suitability of the phone number registered in the application with the phone number being used on a smartphone or tablet using Header Enrichment. Thus, cyber criminals who have the victim's credentials cannot take over accounts and steal customer money in mobile banking, because cyber criminals do not have a phone number installed on their smartphone or tablet. The test was carried out using an API provided by one of the mobile operators with a prototype application that has been built. The results obtained from several test scenarios, account takeover cannot occur, the action plan for implementing authentication technology has been validated and can be used as a guide or reference.