JURNAL TEKNOINFO
Volume 18, Nomor 2, Juli 2024, Page 434-441
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

PROTECTION SECOND LAYER MENGGUNAKAN MULTI FACTOR AUTHENTICATOR UNTUK MEMVERFIKASI KEABSAHAN ACCOUNT EMAIL DI DALAM ACTIVE DIRECTORY

Kotim Subandi[1*)], Dinar Munggaran Ahmad[2)], Victor Ilyas Sugara[3)], Adriana Sari Aryani[4)], Hermawan[5)]

[1,2,3,4,5]Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Pakuan
[1,2,3,4,5]Jl. Pakuan, RT.02/RW.06, Tegallega, Kecamatan Bogor Tengah, Kota Bogor, Indonesia

Email: [1]kotim.subandi@unpak.ac.id, [2]dinar.munggaran@unpak.ac.id, [3]victorilyassugara@unpak.ac.id, [4]adriana.sari@unpak.ac.id, [5]hermawani@unpak.ac.id

Abstract

The problem that often occurs is that many users use unsafe devices to carry out the login process, for example using laptops, mobile phones and other devices in public spaces such as terminals, airport stations, public libraries, cafes and even internet cafes. One of the important steps in the security and authentication process. This verification ensures that the account owner has access to the email address used to register or log in to a service. Multi-Factor Authentication (MFA) is a security method that requires users to provide more than one form of authentication to access a system or application. Research focuses on evaluating the security of MFA, using appropriate metrics (such as authentication success rate, successful attack rate, or discovered vulnerabilities) to assess the effectiveness of MFA. Implementing MFA on email accounts is not only a wise security measure, but also a recommended practice to protect personal information and reduce online security risks

Keywords: *Protection, Email Account*, *Multi-Factor Authentication, Active Directory*

.

Abstrak

Masalah sering yang terjadi adalah banyak pengguna yang memakai perangkat yang tidak aman dalam melakukan proses *login*, contohnya pemakaian Laptop,Mobile Phone dan perangkat lain di ruang publik seperti terminal, stasiun bandara, perpustakaan umum, café bahkan warnet. Salah satu langkah penting dalam proses keamanan dan otentikasi. Verifikasi ini memastikan bahwa pemilik akun memiliki akses ke alamat email yang digunakan untuk mendaftar atau masuk ke suatu layanan. *Multi-Factor Authentication* (MFA) adalah metode keamanan yang mengharuskan pengguna memberikan lebih dari satu bentuk otentikasi untuk mengakses sistem atau aplikasi. Penelitian berfokus pada evaluasi keamanan MFA, gunakan metrik yang sesuai (seperti tingkat keberhasilan otentikasi, tingkat serangan yang berhasil, atau kerentanan yang ditemukan) untuk menilai efektivitas MFA. Penerapan MFA pada akun email bukan hanya merupakan tindakan keamanan yang bijaksana, tetapi juga merupakan praktik yang direkomendasikan untuk melindungi informasi pribadi dan mengurangi risiko keamanan online

Kata Kunci: Proteksi, Akun Emal, *Multi Factor Authencation.Active Directory*

1. PENDAHULUAN

Dalam era digital keamanan informasi menjadi semakin penting karena semakin banyak data yang disimpan secara online. Ancaman seperti peretasan data, pencurian identitas, dan serangan siber semakin umum dan canggih.Penggunaan kata sandi tunggal sebagai satu-satunya lapisan keamanan tidak lagi cukup untuk melindungi akun dan data. Kata sandi dapat mudah diretas atau dicuri oleh peretas yang menggunakan teknik-teknik seperti *phishing* atau *brute force attacks*. [1]

Organisasi dan individu membutuhkan tingkat keamanan yang lebih tinggi untuk melindungi informasi sensitif, seperti data keuangan, medis, dan pribadi seperti email. MFA memberikan lapisan tambahan dalam perlindungan data. Banyak negara dan industri mengatur persyaratan keamanan data yang ketat. Sebagai contoh, Regulasi Umum Perlindungan Data (GDPR) di Uni Eropa mengharuskan perusahaan untuk melindungi data pribadi dengan lebih cermat. MFA membantu meme-nuhi persyaratan ini.Teknologi terus berkem-bang, memungkinkan implementasi MFA yang lebih

JURNAL TEKNOINFO
Volume 18, Nomor 2, Juli 2024, Page 434-441
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

mudah dan efisien. [2]

Teknologi seperti otentikasi berbasis token, otentikasi berbasis biometrik, dan otentikasi dua faktor (2FA) telah menjadi lebih tersedia dan terjangkau. Semakin banyak orang mengakses akun mereka melalui perangkat mobile, yang sering memi-liki berbagai opsi otentikasi, seperti sidik jari, pemindaian wajah, atau otentikasi dua faktor melalui aplikasi [3]

Multi-Factor Authentication (MFA) adalah metode keamanan yang meng-haruskan pengguna memberikan lebih dari satu bentuk otentikasi untuk mengakses sistem atau aplikasi. Secara topologis, MFA tidak berarti menggambarkan suatu jaringan fisik atau konfigurasi perangkat keras tertentu seperti yang dilakukan dalam topologi jaringan komputer. Alih-alih, MFA lebih merupakan konsep keamanan yang dapat diterapkan dalam berbagai konteks jaringan. Ini tidak menggambarkan struktur fisik atau konfigurasi jaringan, tetapi cara sistem otentikasi berinteraksi dengan peng-guna layangan jaringan publik. [4]

Salah satu langkah penting dalam proses keamanan dan otentikasi. Verifikasi ini memastikan bahwa pemilik akun memiliki akses ke alamat email yang digunakan untuk mendaftar atau masuk ke suatu layanan, Kemudian memasukkan alamat email saat mendaftar, situs web atau layanan akan mengirimkan email verifikasi ke alamat tersebut. Email ini berisi tautan atau kode verifikasi yang harus konfirmasikan. Penting untuk memverifikasi akun email karena ini membantu melindungi akun email dari penggunaan yang tidak sah. Ini juga dapat membantu mendapatkan akses kembali ke akun jika terjadi lupa kata sandi atau mengalami masalah dengan akun email. [5]

Masalah sering yang terjadi adalah banyak pengguna yang memakai perangkat yang tidak aman dalam melakukan proses *login*, contohnya pemakaian Laptop,Mobile Phone dan perangkat lain di ruang publik seperti terminal, stasiun bandara, perpus-takaan umum, café bahkan warnet. Mes-kipun telah memanfaatkan jaringan yang aman sekalipun, apabila *password* akan dapat terbaca oleh komputer lain yang telah terpasang perangkat lunak atau perangkat keras yang dirancang untuk merekam setiap tombol yang ditekan oleh pengguna pada keyboard komputer atau perangkat mobile. [6]

Dalam penelitian ini penulis memilih MFA telah sebagai salah satu langkah yang paling efektif untuk meningkatkan keamanan dalam dunia digital. Ini memberikan perlin-dungan tambahan dengan menggabungkan dua atau lebih metode otentikasi yang berbeda.MFA menjadi standar dalam melin-dungi akun email, keabsahan *user Active directory* dan data *Confidential* dalam lingkungan yang semakin kompleks dan terhubung jaringan internet. [7]

2. METODE PENELITIAN

Metode penelitian yang digunakan mengenai *Multi-Factor Authentication* (MFA) dengan melakukan pendekatan untuk memahami, mengembangkan, atau meng-evaluasi sistem keamanan informasi dan komunikasi. MFA adalah sebuah metode yang digunakan untuk meningkatkan keamanan akses sistem dengan meminta lebih dari satu bentuk otentikasi dari pengguna sebelum memberikan akses ke data atau sumber daya yang dilindungi. Berikut adalah langkah-langkah digunakan peneliti dalam mene-rapkan MFA sebagai proteksi keamanan akun email [8]

1.Studi Literatur

Dalam studi literatur ini sangat penting untuk memahami konsep MFA, berbagai jenis MFA (seperti penggunaan kata sandi, token, sidik jari, atau pengenalan wajah), dan teknologi yang terlibat.

2. Identifikasi Masalah

Diifokuskan dengan cara mencoba dan membandingkan efektivitas berbagai metode MFA atau mengidentifikasi tantangan yang dihadapi dalam penerapan MFA.

3. Desain Penelitian

Pilih desain penelitian yang sesuai dengan tujuan Anda, seperti eksperimen, studi kasus, survei, atau analisis doku-mentasi.

4. Pengumpulan Data

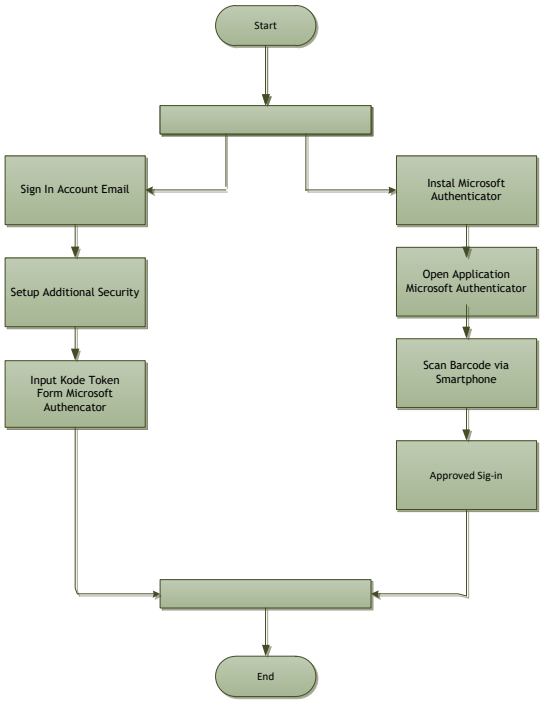
Kumpulkan data yang diperlukan untuk penelitian Anda. Ini dapat mencakup informasi tentang implementasi MFA, metode pengujian, atau hasil dari survei

5. Analisa Data

Lakukan analisis data untuk menjawab pertanyaan penelitian Anda. Ini mungkin melibatkan perbandingan antara berbagai metode MFA, evaluasi keamanan sistem yang menggunakan MFA, atau analisis tren dalam penggunaan MFA. [9]

JURNAL TEKNOINFO
Volume 18, Nomor 2, Juli 2024, Page 434-441
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

6. Evaluasi Keamanan
Penelitian berfokus pada evaluasi keamanan MFA, gunakan metrik yang sesuai (seperti tingkat keberhasilan otentikasi, tingkat serangan yang berhasil, atau kerentanan yang ditemukan) untuk menilai efektivitas MFA. [10]



Gambar 1 Flowchart MFA Setup

Sebagai langkah awal bahwa akun email terproteksi dari tindakan kejahatan dalam dunia maya dan memastikan bahwa sistem yang sudah diterapkan dapat berjalan dengan baik, maka perlu dipersiapkan beberapa tahapan sebelum melakukan aktifitas email, Gambar 1 Flowchart MFA Setup.

1. *User login* terlebih dengan menggunakan password yang sudah di verifikasi dalam *Active Directory* ,jika pengguna tidak sah
output yang diharapkan gagal login

2. User harus menjalankan setup *Additional Security* untuk pemilihan kode verifikasi token akan di kirim via SMS atau Applikasi Microsoft Authenticator

3. Pengguna harus mengiputkan kode token yang di generate via Applikasi *Microsoft Authenticator* sebelum akun email akan gunakan untuk berkomunikasi

4. Instal Microsoft Authenticator, user peng-guna akun email dapat membuktikan iden-titas mereka dengan lebih aman. Setelah memasukkan kata sandi, pengguna harus memberikan persetujuan atau kode yang dihasilkan oleh aplikasi Authenticator sebagai bentuk verifikasi tambahan.

5. *Authenticator* menghasilkan token waktu yang berubah secara berkala sebagai bagian dari proses autentikasi. Token ini biasanya valid hanya untuk jangka waktu yang singkat, meningkatkan keamanan dengan mengurangi risiko penggunaan kembali kode otentikasi

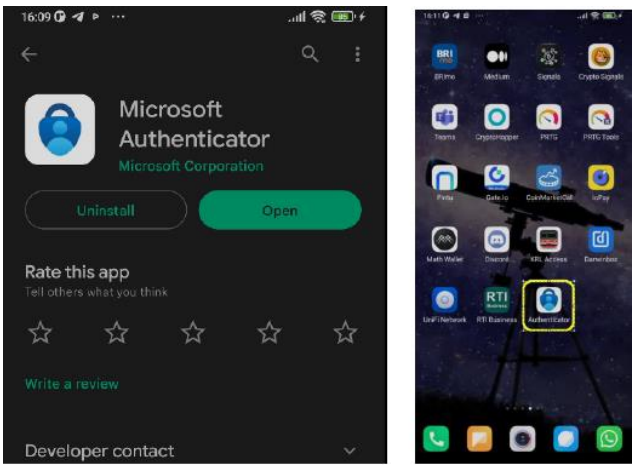
6. Untuk menambahkan akun ke Authenticator, pengguna dapat memindai kode QR yang diberikan oleh layanan atau memasukkan kunci yang disediakan. Ini mem-permudah proses konfigurasi. Arahkan kamera perangkat Anda ke kode QR yang disediakan oleh layanan atau situs web yang akan ditambahkan ke *Authenticator*, pastikan agar kamera fokus pada seluruh kode QR. Setelah berhasil memindai kode QR, aplikasi Authenticator akan menam-pilkan informasi akun email yang akan digunakan.

JURNAL TEKNOINFO
Volume 18, Nomor 2, Juli 2024, Page 434-441
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

7. Pada tahapan *Approved Sign-In* pada Microsoft Authenticator merujuk pada proses di mana pengguna memberikan persetujuan atau menyetujui permintaan masuk ke akun email yang akan digunakan untuk berko-munikasi melalui notifikasi push dari aplikasi *Authenticator.* Fungsi ini sangat relevan dalam konteks autentikasi dua faktor (2FA) dan digunakan untuk meningkatkan kea-manan akun email. Dengan menyetujui masuk melalui notifikasi *push*, pengguna dapat memastikan bahwa mereka memiliki kendali penuh atas akses ke akun mereka. Ini membantu melindungi akun dari akses yang tidak sah

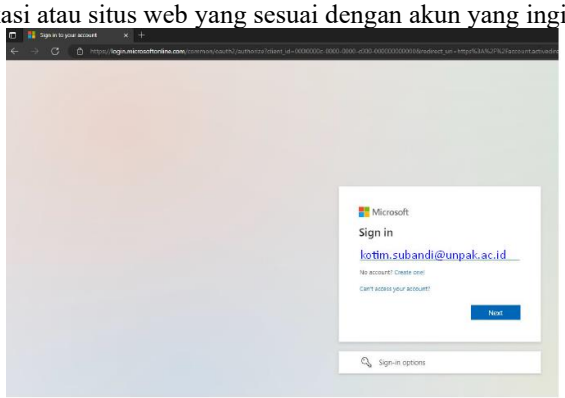
3. HASIL DAN PEMBAHASAN

Sebelum dapat menggunakan *Multi-Factor Authentication* (MFA) ke dalam sistem email, ada beberapa syarat yang perlu dipenuhi. namun, perlu diingat bahwa persyaratan ini dapat bervariasi tergantung pada penyedia layanan email yang Anda gunakan.pastikan applikasi dari *Microsoft Authenticator* sudah di install di *Mobile Phone* yang akan digunakan untuk mendapatkan kode token MFA ,seperti pada gambar 2



Gambar 2 Applikasi Microsoft Authenticator

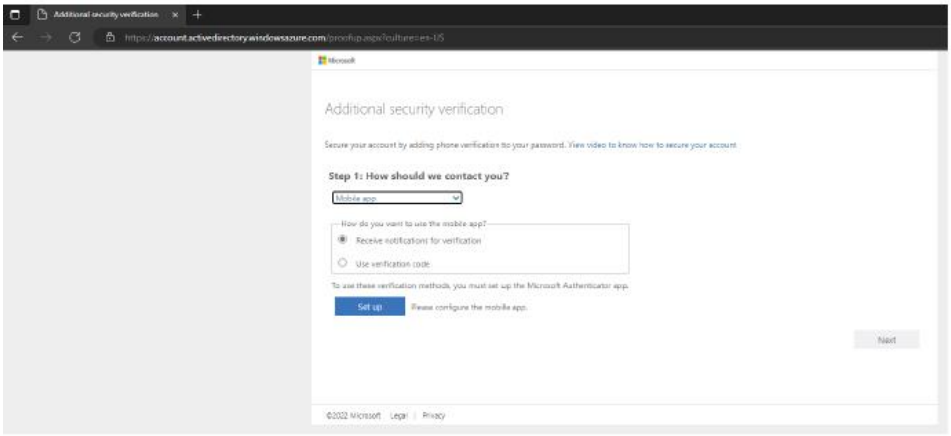
Dalam menerapkan aktivasi MFA (*Multi-Factor Authentication*) melibatkan beberapa langkah untuk menambahkan lapisan keamanan tambahan pada akun Anda. Langkah-langkah yang tepat dapat bervariasi tergantung pada platform atau layanan yang Anda gunakan, tetapi umumnya melibatkan langkah-langkah berikut Masuk terlebih dahulu ke menu akun yang akan di terapkan, buka aplikasi atau situs web yang sesuai dengan akun yang ingin Anda lindungi dengan MFA



Gambar 3 Akun Email dari Web

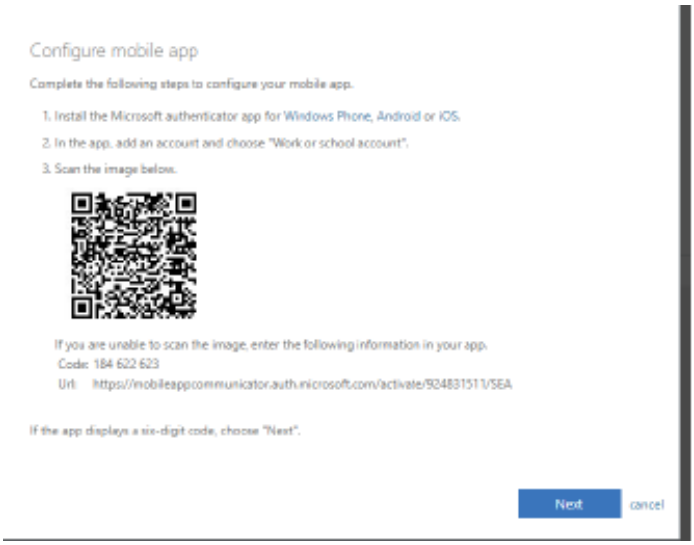
Setelah masuk ke akun email cari opsi keamanan atau akun dalam pengaturan. Ini bisa disebut Keamanan Privasi, Pengaturan Akun", atau hal serupa

JURNAL TEKNOINFO
Volume 18, Nomor 2, Juli 2024, Page 434-441
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index



Gambar 4 Security Verification

Pilihan tambahan yang diambil untuk meningkatkan keamanan suatu system, dengan cara verifikasi identitas, seperti kata sandi dan kode yang dikirim melalui SMS atau aplikasi autentikasi *Microsoft Authenticato*r, Memastikan bahwa pengguna hanya memiliki hak akses yang diperlukan untuk melak-sanakan kegiatan berkomunikasi dengan email. Hal penting untuk selalu memperbarui dan meninjau kebijakan keamanan sesuai dengan perkembangan teknologi dan ancaman keamanan terkini

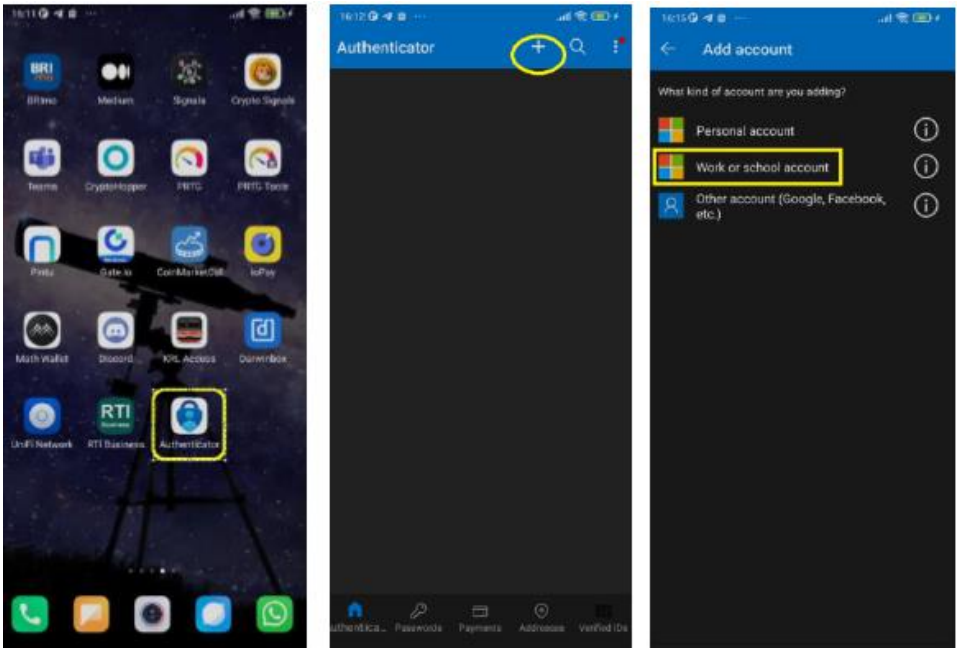


Gambar 5 Barcode MFA

Penggunaan scan barcode dalam konteks *Multi-Factor Authentication* (MFA) biasanya terkait dengan metode otentikasi dua faktor (2FA) menggunakan aplikasi autentikasi pada perangkat seluler. Selama proses ini, sistem akan menyediakan barcode QR unik yang terkait dengan akun email pengguna. kemudian dengan menggunakan aplikasi autentikasi yang sesuai seperti *Google Authenticator* atau *Authy* untuk memindai barcode tersebut dengan menggunakan ka-mera perangkat seluler aplikasi autentikasi akan mulai menghasilkan kode-kode waktu yang berubah secara dinamis.

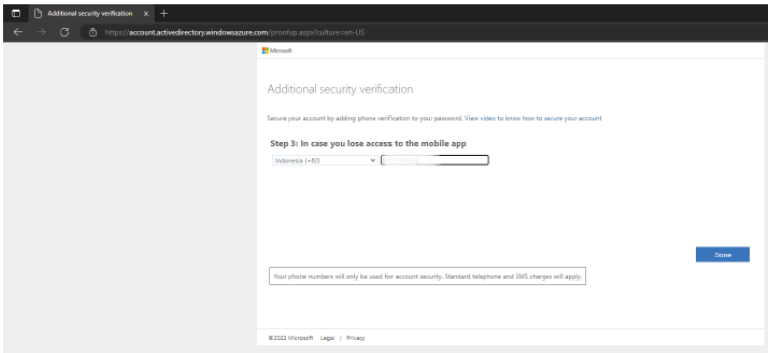
Kode ini berubah secara periodik biasanya setiap 30 detik, dan hanya dapat diakses oleh pengguna yang memiliki perangkat seluler yang telah terdaftar dengan benar dengan sistem MFA,seperti pada gambar 5 *Barcode MFA*

JURNAL TEKNOINFO
Volume 18, Nomor 2, Juli 2024, Page 434-441
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index



Gambar 6 Add Account

Penerapan *Microsoft Authenticator* sebagai aplikasi otentikasi dua faktor (2FA) yang dikembangkan oleh Microsoft untuk meningkatkan keamanan akun pengguna. Pengguna dapat menerima notifikasi push pada perangkat mereka ketika mencoba melakukan login. Mereka hanya perlu menyetujui atau menolak notifikasi untuk mengkonfirmasi identitas mereka. *Microsoft Authenticator* dapat dikonfigurasi untuk menggunakan metode otentikasi berbasis biometrik seperti pemindaian sidik jari atau pengenalan wajah atau PIN sebagai lapisan tambahan keamanan. Informasi otentikasi dan kunci rahasia disimpan secara aman di perangkat pengguna. Ini membantu melin-dungi data otentikasi dari akses yang tidak sah



Gambar 7 *No HP Recovery*

Pemulihan nomor telepon harus dikon-figurasi dengan baik untuk menghindari potensi penyalahgunaan atau akses yang tidak sah ke akun pengguna Jika perangkat pengguna hilang atau dicuri, *Microsoft Authenticator* memungkinkan untuk mela-kukan penghapusan akun jarak jauh untuk mencegah akses yang tidak sah. *Microsoft Authenticator* mendukung opsi pemulihan akun, sehingga pengguna dapat mengakses kembali akun mereka jika mereka kehilangan akses ke perangkat autentikasi. Gambar 7 *No HP recovery*

JURNAL TEKNOINFO
Volume 18, Nomor 2, Juli 2024, Page 434-441
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

Gambar 8 Approve Account Email

Metode ini memungkinkan pengguna untuk mengonfirmasi atau menyetujui proses masuk ke akun mereka dengan cara yang lebih mudah dan cepat. Fungsi utama dan kegunaan dari "Approve Sign-In" melibatkan notifikasi push yang diterima oleh pengguna di perangkat seluler mereka ketika mereka mencoba untuk masuk ke akun tertentu. Ketika pengguna mencoba masuk ke akun mereka (seperti akun Microsoft, Office 365, atau layanan lain yang mendukung MFA), mereka akan menerima notifikasi push di perangkat seluler mereka melalui aplikasi *Microsoft Authenticator*.

Dengan menggunakan notifikasi push, *"Approve Sign-In*" memberikan perlindungan yang baik terhadap akses tidak sah atau percobaan masuk yang tidak diinginkan. Jika pengguna tidak mengenali atau tidak menyetujui permintaan masuk, mereka dapat segera menolaknya, Gambar 8 *Approve Account Email*.

4. KESIMPULAN

Perlu diingat bahwa Langkah-langkah dalam proses otentikasi MFA dapat bervariasi tergantung pada metode MFA yang digunakan, seperti penggunaan aplikasi otentikasi, pesan teks, atau perangkat keras token. Selain itu, beberapa sistem MFA mungkin memiliki langkah-langkah tam-bahan, seperti verifikasi biometrik, ergantung pada tingkat keamanan yang diinginkan. Ketika pengguna memahami risiko yang terlibat dan tindakan yang harus mereka ambil untuk mengamankan perangkat mereka, keamanan secara keseluruhan dapat ditingkatkan. Dukungan teknis dan edukasi adalah kunci dalam mengatasi masalah pengguna yang menggunakan perangkat yang tidak aman.Keamanan MFA bergantung juga pada pengguna melindungi perangkat seluler mereka dengan baik, karena akses ke aplikasi autentikasi juga bisa menjadi pintu masuk ke akun yang dilindungi oleh MFA. Selain itu, proses ini menunjukkan betapa pentingnya pengguna untuk mengelola dan melindungi perangkat yang digunakan untuk MFA. Penerapan MFA pada akun email bukan hanya merupakan tindakan keamanan yang bijaksana, tetapi juga merupakan praktik yang direkomendasikan untuk melindungi informasi pribadi dan mengurangi risiko keamanan online. Beberapa sistem MFA memberikan kontrol yang lebih baik terhadap perangkat yang diizinkan untuk mengakses akun. Pengguna dapat mengelola perangkat yang terkait dengan akun mereka, membantu mencegah akses yang tidak sah dari perangkat yang tidak dikenal

UCAPAN TERIMAKASIH

Penulis mengucapkan banyak terima kasih kepada Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Universitas

Pakuan yang telah menyediakan fasilitas demi kelancaran penelitian ini.

DAFTAR PUSTAKA

[1] Anon., n.d. F5, "K51213246: BIG-IP APM AD authentication vulnerability CVE-2021-23008,"28 April 2021.. pp. [Online]. Available:https://support.f5.com/csp/article/K51213246,diakses 04 Desember 2023.

[2] C. Z. Acemyan, P. K. J. X. a. D. S. W., 2022. 2FA might be secure, but it's not usable: A summative usability assessment of Google's two-factor authentication (2FA) methods. Proc. Hum. Factors Ergon. Soc, 2(doi: 10.1177/1541931218621262), p. 1141–1145.

[3] D. E. Kurniawan, M. I. J. F. F. H. a. R. D. P., 2021. Login Security Using One Time Password (OTP) Application with Encryption Algorithm Performance. J. Phys. Conf. Ser, 1783 no 1(doi: 10.1088/1742-6596/1783/1/012041)

[4] Elanda, A. L. B., 2020. Analisis Sistem Keamanan Sistem Informasi Berbasis Webiste Dengan Metode Open Web Application Security Project (OWASP) Versi 4: Systematic Review. Journal of Computer Engineering System and Science, Volume 5 (2), pp. 185-191.

[5] F. Ayankoya and B. Ohwo, 2019. Brute-Force Attack Prevention in Cloud Computing Using One-Time Password and Cryptographic Hash Function,. Int. J. Comput. Sci. Inf. Secur., , 12(Available: https://www.academia.edu/38523734/Brute-Force_Attack_Prevention_in_Cloud_Computing_Using_One-Time_Password_and_Cryptographic_Hash_Function), pp. 7-19.

[6] H. Khalid, S. J. H. S. M. S. A. F. H. a. M. A. C., 2020. New and Simple Offline Authentication Approach using Time-based One-time Password with Biometric for Car Sharing Vehicles,". 2020 IEEE Asia-Pacific Conf. Comput. Sci. Data Eng. CSDE 2020, Issue doi: 10.1109/CSDE50874.2020.9411569, p. 110.

[7] Kurniawan, A., 2020. Penerapan Framework OWASP dan Network Forensics untuk Analisis, Deteksi, dan Pencegahan Serangan Injeksi di Sisi Host-Based. Telematika, Volume 1 (14), pp. 9-18..

[8] M. K. Sharma and M. J. Nene, 2022. Two-factor authentication using biometric based quantum operations. Secur. Priv, 3 No 3(doi: 10.1002/spy2.102.), p. 102.

[9] Maxim, R. S. P. a. B. R., 2020. Software Engineering A PRACTITIONER'S APPROACH, s.l.: McGraw-Hill.

[10] Mayasari, R. A. R. A. J. D. A. B. K., 2020. Analisis Vulnerability pada Website Universitas Singaperbangsa Karawang menggunakan Acunetix Vulnerability. SYSTEMATICS, Volume 2 (1), pp. 33-38..

[11] Nigel Cunong, D. S. M. P. W., 2020. Analisis Resiko Keamanan Terhadap Website Dinas Penanaman Modan dan Pelayanan Terpadu Satu Pintu Pemerintahan XYZYZ Menggunakan Standar Penetration Testing Execution Standard (PTES. -, e-Proceeding of Engineering.

.

[12] Pusat Operasi Keamanan Siber Nasional, L. T. 2., 2020. (Monitoring Keamanan Siber). , Jakarta: Badan Siber Dan Sandi Negara,.

[13] Rafsanjani, H. T. a. M. K., 2020. A survey on security challenges in cloud computing: issues, threats, and solutions. A survey on security challenges in cloud computing, Issue threats, and solutions.

[14] Yudiana., E. A. L. B. R., 2021. Analisis Kualitas Keamanan Sistem Informasi EOffice Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP TOP 10. Journal of Computer Engineering System and Science, Volume 2, pp. 185-191