

LAPORAN ANALISA KEAMANAN SIBER

IF 673: KEAMANAN SIBER: KONFIGURASI DAN MANAJEMEN FIREWALL

Analisis Serangan Phishing pada Kasus Pelanggaran Data Dropbox



KELOMPOK: Rasta Giting Bersama (RGB) ANGGOTA:

- 1. Muhammad Zaidan Fiqri – 00000060117**
- 2. Ananta Viryadiva – 00000055173**
- 3. Luthfil Razak Putra Septiyanagara - 00000061384**
- 4. Jovansha Cancerio - 00000055387**
- 5. Ikbar Muhammad Mumtaz - 00000061296**

**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2023**

Judul Laporan Analisa:
Analisis Serangan Phishing Pada Kasus Data Breach Dropbox

1. Abstrak / Ringkasan Eksekutif

Pada 14 Oktober 2020, Dropbox, perusahaan layanan penyimpanan awan, mengalami insiden pelanggaran data yang disebabkan oleh serangan phishing yang menargetkan para karyawannya. Penyerang berpura-pura menjadi CircleCI, sebuah platform integrasi dan pengiriman kode, untuk menipu karyawan Dropbox agar memberikan login dan kode autentikasi mereka. Dengan informasi yang berhasil dicuri tersebut, pelaku mendapatkan akses ke akun Dropbox di GitHub, sebuah platform repositori kode. Melalui metode ini, penyerang berhasil mengakses beberapa kode yang disimpan oleh Dropbox di GitHub, termasuk kunci API yang digunakan oleh pengembang Dropbox.

Pelanggaran ini terungkap ketika GitHub memberi tahu Dropbox tentang aktivitas mencurigakan yang terdeteksi di akun mereka. Setelah penyelidikan, ditemukan bahwa peretas telah berhasil mengakses dan menyalin kode dari 130 repositori milik Dropbox. Sebagai respons terhadap insiden ini, Dropbox segera menghubungi semua pihak yang terdampak dan memberikan jaminan kepada pengguna bahwa informasi sensitif seperti konten akun Dropbox, kata sandi, atau informasi pembayaran tidak berhasil diakses oleh pelaku serangan.

Dropbox juga mengambil langkah-langkah untuk memperkuat keamanan mereka guna mencegah insiden serupa di masa depan. Mereka terus memantau aktivitas yang mencurigakan dan memberikan edukasi kepada karyawan tentang cara mengenali dan melaporkan potensi serangan phishing. Langkah-langkah tambahan ini penting untuk memastikan bahwa sistem keamanan Dropbox tetap kuat dan dapat menghadapi ancaman yang semakin canggih.[1].

2. Kasus Serangan Siber

2.1. Jenis dan Teknik Serangan

Jenis Serangan: Phishing attack, hacking attack, or malware attack.

Serangan dilakukan oleh penjahat yang menyamar sebagai CircleCI untuk mendapatkan kredensial login dan kode otentikasi dari karyawan. Mereka kemudian menggunakan informasi tersebut untuk mengakses akun Dropbox yang terhubung dengan GitHub, melalui sebuah situs phishing. Situs tersebut mengalihkan kode otentikasi dua faktor berbasis waktu (TOTP) langsung kepada penyerang, memungkinkannya untuk mengakses akun yang dilindungi oleh otentikasi dua faktor TOTP. Akun yang menggunakan kunci keamanan perangkat keras tidak terpengaruh oleh serangan ini. [2].

2.2. Penyebab Korban Terkena Serangan

Korban bisa menjadi sasaran serangan karena berbagai faktor. Misalnya, langkah keamanan yang tidak memadai, seperti penggunaan kata sandi yang lemah atau perangkat lunak yang tidak diperbarui, dapat menciptakan celah yang dimanfaatkan oleh penyerang. Selain itu, kurangnya kesadaran tentang ancaman seperti phishing atau teknik rekayasa sosial dapat membuat individu lebih mudah diserang. Perlindungan yang kurang terhadap malware, termasuk virus, ransomware, dan perangkat lunak berbahaya lainnya, juga meningkatkan risiko serangan. Oleh karena itu, penting bagi individu dan organisasi untuk menempatkan keamanan siber sebagai prioritas utama, dengan cara memperbarui perangkat lunak secara rutin, menggunakan kata sandi yang kuat, dan terus mengedukasi diri tentang ancaman yang ada, guna mengurangi risiko menjadi korban serangan siber.

2.3. Teknik dan Metode Penanganan

Teknik pencegahan terbaik terhadap serangan phishing seperti ini meliputi:

- Pendidikan dan pelatihan karyawan tentang cara mengidentifikasi dan melaporkan potensi serangan phishing.
- Implementasi otentikasi multi-faktor untuk mencegah akses tanpa izin.
- Memantau aktivitas pengguna untuk aktivitas mencurigakan.
- Mengimplementasikan kebijakan hak akses paling sedikit (least privilege) untuk hak akses.
- Memastikan perangkat lunak selalu diperbarui dan di-patch secara berkala.

Sebagai respons terhadap serangan, Dropbox telah mengambil langkah-langkah untuk memastikan bahwa pelaku tidak lagi bisa mengakses akunnya di GitHub.

Perusahaan juga telah menghubungi semua yang terpengaruh oleh pelanggaran ini dan memastikan kepada pengguna bahwa pelaku ancaman tidak berhasil mengakses isi dari akun Dropbox, kata sandi, atau informasi pembayaran. Untuk mencegah serangan serupa di masa depan, Dropbox telah menerapkan langkah-langkah keamanan tambahan dan secara aktif memantau segala aktivitas yang mencurigakan. Selain itu, perusahaan terus memberikan edukasi kepada karyawannya tentang pentingnya mengidentifikasi dan melaporkan potensi serangan phishing [3].

3. Usulan Teknik dan Metode Keamanan Siber

Salah satu metode untuk mencegah terjadinya phishing ataupun mencegah dampak negatif dari phishing adalah dengan melakukan analisis link atau website. Di arsitektur firewall Palo Alto, analisis ini dapat dilakukan dengan fitur WildFire.

3.1. Teori

Menurut Wibowo dan Fatimah (2017), phishing adalah tindakan penipuan yang dirancang untuk menjebak korban agar memberikan informasi yang diinginkan oleh pelaku. Metode yang sering digunakan oleh pelaku adalah dengan menyamar melalui email atau situs web palsu yang dibuat dengan konten persuasif. Konten ini dirancang sedemikian rupa agar korban merasa terdorong untuk memasukkan data pribadi mereka, seperti informasi login, detail kartu kredit, atau informasi sensitif lainnya, yang kemudian dikumpulkan oleh pelaku untuk tujuan yang merugikan korban.

Phishing memanfaatkan kelemahan psikologis manusia, seperti kepercayaan dan kepanikan, untuk menipu korban. Contohnya, pelaku dapat mengirim email yang tampak resmi dari bank atau layanan online populer, dengan pesan yang mendesak pengguna untuk memperbarui informasi akun mereka untuk menghindari penangguhan atau denda. Karena email ini terlihat asli dan mendesak, banyak korban yang tanpa sadar memberikan informasi mereka kepada pelaku.

Teknik phishing juga semakin canggih dengan adanya teknik spear-phishing, di mana pelaku menargetkan individu atau organisasi tertentu dengan pesan

yang lebih personal dan relevan. Hal ini membuat korban lebih mudah tertipu karena pesan tersebut tampak sangat sesuai dengan konteks mereka.

Untuk melindungi diri dari serangan phishing, pengguna harus selalu waspada dan skeptis terhadap email atau situs web yang meminta informasi pribadi atau sensitif. Penggunaan alat keamanan, seperti filter email spam dan perangkat lunak antivirus, juga dapat membantu mendeteksi dan mencegah serangan phishing. Selain itu, pendidikan dan kesadaran tentang teknik-teknik phishing dan bagaimana mengidentifikasinya adalah langkah penting untuk mengurangi risiko menjadi korban serangan ini. Dengan pemahaman yang lebih baik tentang bagaimana phishing bekerja, pengguna dapat lebih berhati-hati dan mengambil langkah-langkah pencegahan yang diperlukan untuk melindungi informasi pribadi mereka. [4]

Salah satu metode untuk mengurangi dampak negatif dari phishing adalah dengan menghindari mengklik tautan atau membuka lampiran email yang mencurigakan. Namun, pengguna juga bisa menjadi korban phishing melalui email yang tampak seolah-olah berasal dari individu atau perusahaan yang dikenal dan dipercaya. Oleh karena itu, diperlukan cara yang memungkinkan pengguna untuk memastikan apakah tautan atau lampiran dalam suatu email aman atau tidak. Salah satu metode yang efektif adalah dengan melakukan analisis file secara otomatis, di mana tautan atau lampiran dikirim ke sistem komputer untuk dianalisis, dan hasilnya akan dikembalikan kepada pengguna untuk menentukan apakah tautan atau lampiran tersebut aman.

Dalam konteks arsitektur firewall Palo Alto, terdapat alat yang dirancang untuk melakukan analisis otomatis ini, yaitu WildFire. WildFire adalah sistem berbasis cloud yang menggunakan teknologi pembelajaran mesin untuk menilai tingkat keamanan suatu file atau situs web. Sistem ini mampu menganalisis tautan dan lampiran email tanpa perlu membuka isi dari email tersebut. Ketika pengguna menerima email, tautan atau lampiran dalam email tersebut dikirim ke cloud WildFire untuk dianalisis. Setelah analisis selesai, hasilnya dicatat di log firewall pengguna, sehingga pengguna dapat mengetahui apakah tautan atau lampiran tersebut berbahaya atau tidak.

WildFire memungkinkan pengguna untuk menjaga keamanan data mereka dengan memanfaatkan teknologi analisis berbasis cloud yang canggih. Sistem ini tidak hanya mendeteksi ancaman secara real-time tetapi juga meminimalkan risiko dengan memastikan bahwa file atau tautan yang diterima melalui email diperiksa sebelum dibuka. Dengan demikian, pengguna dapat lebih percaya diri dan aman dari ancaman phishing yang semakin canggih dan beragam.

WildFire menggunakan pembelajaran mesin untuk meningkatkan kemampuan deteksinya seiring waktu, dengan mempelajari pola dan tanda-tanda serangan phishing baru. Sistem ini juga terintegrasi dengan firewall Palo Alto, memberikan lapisan tambahan perlindungan bagi pengguna. Implementasi WildFire dalam lingkungan jaringan perusahaan tidak hanya meningkatkan keamanan tetapi juga efisiensi dalam mengelola potensi ancaman, karena proses analisis dan deteksi dilakukan secara otomatis dan cepat. [5] Ketika user mendapatkan email, link atau attachment dalam email tersebut langsung dikirim ke cloud WildFire untuk dianalisis, dan ketika selesai, maka hasil dari analisis dicatat di log firewall user agar user tahu apakah attachment atau link dalam suatu email itu berbahaya atau tidak.

3.2. Simulasi Penerapan

Untuk dapat melakukan analisis file di WildFire, pertama user firewall Palo Alto perlu mendapatkan lisensi WildFire terlebih dahulu. Jika sudah, cara untuk melakukan konfigurasi WildFire tidaklah sulit. Cukup dengan melakukan konfigurasi WildFire Analysis Profile dan memasukkannya ke sebuah Security Policy Rule atau profile Group, file yang didapatkan dari email akan langsung dikirim ke WildFire untuk analisis.

Konfigurasi WildFire Analysis Profile dapat dilakukan di menu Objects > Security Profiles > WildFire Analysis. Klik Add untuk menambahkan WildFire Analysis Profile baru, dan beri nama, deskripsi, dan daftar file yang akan dikirim ke WildFire untuk analisis. Untuk contoh ini, hanya akan mengirim file PE, sehingga konfigurasinya adalah sebagai berikut:

- Applications : pastikan any dicentang
- File Types : klik Add dan pilih pe dari dropdown list
- Direction : pastikan both dicentang
- Analysis : pastikan public-cloud dicentang

WildFire Analysis Profile

Name: WildFire_Eliezer

Description: Wildfire_Eliezer

	NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
<input checked="" type="checkbox"/>	pc	any	any	both	public-cloud

+ Add - Delete

OK Cancel

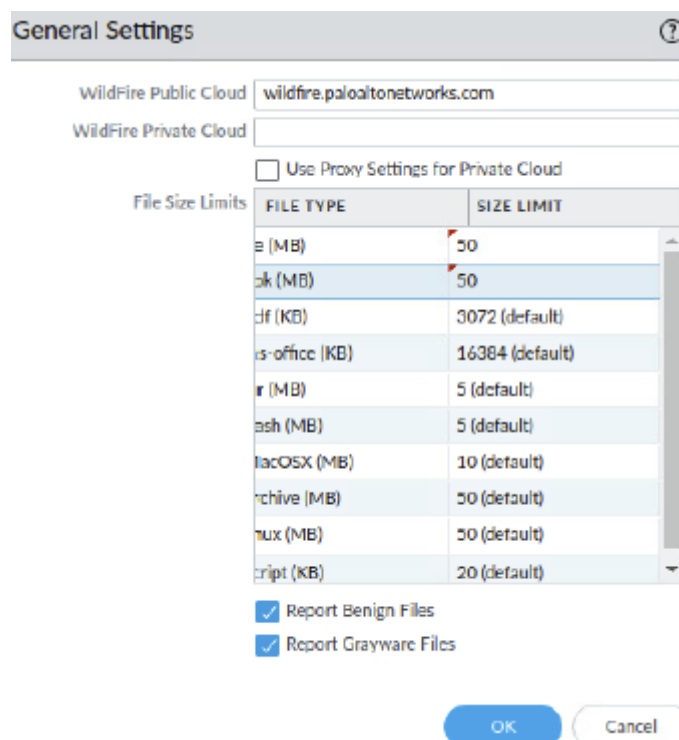
Ketika selesai, WildFire Analysis Profile ini dapat ditambahkan langsung ke Security Policy Rule, ataupun ke sebuah Security Profile Group yang dapat diberikan ke Security Policy Rule. Selain itu, hal-hal tentang analisis WildFire lainnya juga dapat dikonfigurasi di Device > Setup > WildFire. Pengaturan yang ada di sini mencakup lokasi public dan private cloud untuk WildFire, perubahan ukuran file maksimum yang dapat di-upload ke WildFire, serta apakah WildFire akan melakukan log terhadap file dengan verdict benign atau grayware.

3.3. Pengujian Teknik atau Metode Keamanan Siber

Metode simulasi untuk attack bersifat phishing dapat dilakukan dengan 2 email: email pelaku dan email korban. Pelaku mengirim file, misalnya file Test PE dari Palo Alto Networks ke korban, dan ketika korban menerima email, korban dapat melakukan cek terhadap status upload file tersebut ke WildFire menggunakan Putty dan status keamanan file yang terkirim

melalui log di firewall.

Untuk melakukan pengetesan terhadap WildFire Analysis Profile, langkah pertama adalah mendownload attack file dari link Palo Alto (<http://wildfire.paloaltonetworks.com/publicapi/test/pe>) yang menghasilkan file dengan signature yang unik. Pastikan untuk hanya mengunduh file tanpa membukanya. Selanjutnya, buka PuTTY dan double-click firewall-management, lalu masukkan login profile dan password pada prompt. Setelah berhasil login, jalankan perintah `admin@firewall-a> debug wildfire upload-log show`. Output ini akan memverifikasi bahwa file telah diunggah ke public cloud WildFire. Setelah itu, tutup PuTTY.



General Settings

WildFire Public Cloud:

WildFire Private Cloud:

☐ Use Proxy Settings for Private Cloud

File Size Limits

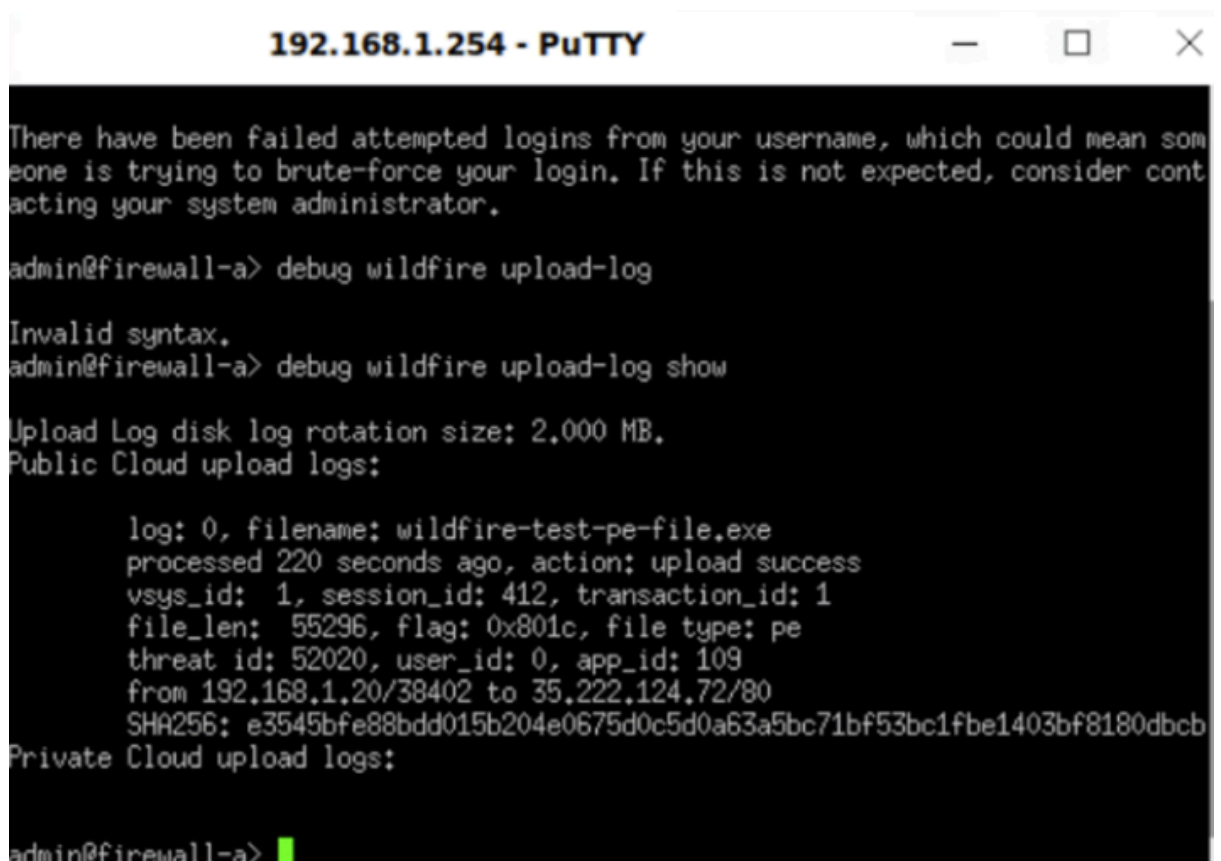
FILE TYPE	SIZE LIMIT
exe (MB)	50
apk (MB)	50
pdf (KB)	3072 (default)
ms-office (KB)	16384 (default)
rar (MB)	5 (default)
bash (MB)	5 (default)
macOSX (MB)	10 (default)
archive (MB)	50 (default)
linux (MB)	50 (default)
script (KB)	20 (default)

☒ Report Benign Files

☒ Report Grayware Files

OK Cancel

Untuk memastikan bahwa WildFire Analysis Profile berfungsi dengan baik, periksa hasilnya di Monitor > Logs > WildFire Submissions pada situs web PaloAlto. Di sana, akan diberikan penjelasan yang lebih rinci terkait threat yang berhasil diblokir oleh WildFire, yang dapat digunakan untuk studi lebih lanjut dan meningkatkan keamanan jaringan.



```
192.168.1.254 - PuTTY

There have been failed attempted logins from your username, which could mean som
eone is trying to brute-force your login. If this is not expected, consider cont
acting your system administrator.

admin@firewall-a> debug wildfire upload-log

Invalid syntax.
admin@firewall-a> debug wildfire upload-log show

Upload Log disk log rotation size: 2,000 MB.
Public Cloud upload logs:

    log: 0, filename: wildfire-test-pe-file.exe
    processed 220 seconds ago, action: upload success
    vsys_id: 1, session_id: 412, transaction_id: 1
    file_len: 55296, flag: 0x801c, file type: pe
    threat id: 52020, user_id: 0, app_id: 109
    from 192.168.1.20/38402 to 35.222.124.72/80
    SHA256: e3545bfe88bdd015b204e0675d0c5d0a63a5bc71bf53bc1fbe1403bf8180dbcb
Private Cloud upload logs:

admin@firewall-a>
```

4. Simpulan dan Saran

4.1. Simpulan

Berdasarkan analisis yang telah dilakukan, serangan phishing merupakan ancaman umum yang selalu ada. Meskipun terdapat berbagai teknik pencegahan yang dapat digunakan untuk melindungi diri dari serangan tersebut, para penyerang tetap dapat menemukan cara untuk melewati perlindungan ini dan mendapatkan akses ke akun. Oleh karena itu, sangat penting untuk memiliki sistem keamanan yang kuat yang diterapkan dan dipantau secara teratur serta diperbarui secara berkala. Selain itu, program pelatihan karyawan yang efektif juga sangat diperlukan untuk memastikan bahwa karyawan menyadari risiko serangan phishing dan mampu mengidentifikasi serta melaporkannya.

Serangan phishing menjadi ancaman berkelanjutan karena penyerang terus mengembangkan metode baru untuk mengelabui pengguna. Mereka memanfaatkan kelemahan manusia, seperti kepercayaan dan ketidakwaspadaan, serta celah keamanan dalam sistem teknologi. Oleh karena itu, pendekatan multi-layer diperlukan

untuk melindungi dari ancaman ini. Salah satu lapisan penting adalah sistem keamanan yang kuat, termasuk penggunaan firewall, perangkat lunak antivirus, dan solusi berbasis cloud seperti WildFire yang dapat menganalisis dan mendeteksi ancaman secara real-time.

Namun, teknologi saja tidak cukup. Karyawan juga harus dilatih untuk mengenali tanda-tanda serangan phishing. Program pelatihan harus mencakup simulasi serangan phishing, sehingga karyawan dapat berlatih dalam situasi yang realistis dan belajar bagaimana menanggapi dengan tepat. Pelatihan ini harus berkelanjutan dan diperbarui secara berkala untuk mengatasi metode serangan terbaru.

Selain itu, penting untuk membangun budaya keamanan di tempat kerja di mana karyawan merasa nyaman melaporkan email yang mencurigakan tanpa takut akan dampak negatif. Proses pelaporan yang sederhana dan dukungan dari manajemen akan meningkatkan respons terhadap ancaman phishing.

Secara keseluruhan, kombinasi dari sistem keamanan teknologi yang canggih dan program pelatihan karyawan yang efektif akan meningkatkan kemampuan organisasi untuk melindungi diri dari serangan phishing. Dengan pendekatan yang komprehensif ini, risiko serangan dapat diminimalkan, dan kerentanan terhadap ancaman yang selalu berubah ini dapat dikurangi secara signifikan.

Detailed Log View													
Log Info WildFire Analysis Report													
General				Source				Destination					
Session ID 412				Source User				Destination User					
Action allow				Source 192.168.1.20				Destination 35.222.124.72					
Application web-browsing				Source DAG				Destination DAG					
Rule egress-outside-content-id				Port 38402				Port 80					
Rule UUID 6090f2f7-d3ac-4f6e-8fac-0af4b83513da				Zone inside				Zone outside					
Verdict malicious				Interface ethernet1/2				Interface ethernet1/1					
Device SN 015351000086611				NAT IP				NAT IP					
				NAT Port 22844				NAT Port 80					
PCAP	RECEIVE TIME	TYPE	APPLICAT...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG... LIST	VERDI...	URL	FILE NAME
	2023/12/20 15:15:30	end	web-browsing	allow	egress-outside-content-id	6090f2f7-d3ac-4f6e-8fac-0af4b83513da ...							
	2023/12/20 15:18:56	wildfire	web-browsing	allow	egress-outside-content-id	6090f...		high			malicio...		wildfir...

4.2.Saran

Beberapa hal yang dapat dilakukan untuk meningkatkan keamanan online terkait serangan phishing:

- 1) Kesadaran dan Pendidikan Pengguna: Penting untuk meningkatkan kesadaran pengguna terhadap teknik phishing dan cara mengidentifikasi serangan tersebut. Pelatihan rutin dan pendidikan mengenai praktik keamanan digital perlu diperkuat di seluruh organisasi.
- 2) Penggunaan Kunci Keamanan Perangkat Keras: Implementasi kunci keamanan perangkat keras seperti YubiKey atau perangkat serupa dapat memberikan lapisan perlindungan tambahan terhadap serangan phishing. Penggunaan kunci keamanan perangkat keras mempersulit upaya penyerang untuk mencuri kredensial login dan informasi otentikasi.
- 3) Implementasi Tindakan Keamanan Berlapis: Organisasi harus mengadopsi pendekatan keamanan berlapis yang mencakup penggunaan otentikasi dua faktor, deteksi ancaman real-time, enkripsi data, dan pemantauan keamanan yang terus-menerus. Dengan menggabungkan berbagai tindakan keamanan, organisasi dapat meningkatkan ketahanan mereka terhadap serangan phishing dan pelanggaran data.

- 4) Tinjauan Regulasi dan Kebijakan Keamanan: Organisasi perlu secara teratur meninjau kebijakan keamanan mereka untuk memastikan bahwa mereka sesuai dengan regulasi yang berlaku dan mengadopsi praktik terbaik dalam melindungi data sensitif. Tinjauan ini harus mencakup kebijakan terkait manajemen akses, retensi data, dan pemulihan bencana.

Dengan menerapkan saran-saran di atas, organisasi dapat memperkuat pertahanan mereka terhadap serangan phishing dan mengurangi risiko pelanggaran data seperti yang terjadi pada kasus Dropbox.

- Kesadaran dan Edukasi: Tingkatkan pemahaman masyarakat tentang cara mengidentifikasi phishing dan pesan mencurigakan.
- Pelatihan Karyawan: Lakukan pelatihan keamanan siber rutin bagi karyawan untuk mengenali dan mencegah serangan.
- Pembaruan Rutin: Pastikan perangkat lunak dan keamanan selalu diperbarui untuk mendapatkan perlindungan terkini.
- Kata Sandi Kuat: Gunakan kata sandi unik dan kuat untuk setiap akun online.
- Verifikasi Identitas: Selalu verifikasi identitas sebelum memberikan informasi pribadi.
- Pemeriksaan Akun Rutin: Periksa secara berkala aktivitas akun untuk mendeteksi tindakan mencurigakan.
- Keamanan Perangkat: Lindungi perangkat dengan perangkat lunak keamanan dan aktifkan fitur keamanan.
- Laporan Serangan: Laporkan segera kepada pihak berwenang atau penyedia layanan jika menjadi korban serangan.

Dengan melakukan tindakan-tindakan tersebut, kita dapat meningkatkan keamanan online dan mengurangi resiko menjadi korban serangan siber.

5. Daftar Pustaka

1. C. Mayo, "Learning From the Dropbox Data Breach," www.doppler.com.
<https://www.doppler.com/blog/learning-dropbox-data-breach>
2. O. Powell, "Dropbox suffers data breach following phishing attack," Cyber Security Hub, Nov. 02, 2022.
<https://www.cshub.com/attacks/news/dropbox-suffers-data-breach-following-phishing-attack>
3. E. Kovacs, "Hackers Stole Source Code, Personal Data From Dropbox Following Phishing Attack," SecurityWeek, Nov. 02, 2022.
<https://www.securityweek.com/hackers-stole-source-code-personal-data-dropbox-following-phishing-attack/>
4. M. H. Wibowo & N. Fatimah, "Ancaman Phishing terhadap Pengguna Sosial Media dalam Dunia Cyber Crime," JOEICT (Journal of Education and Information Communication Technology, vol. 1, no. 1, pp. 1-5, 2017.
<https://core.ac.uk/download/pdf/328198623.pdf>
5. Palo Alto Networks, "WildFire at a Glance," www.westconcomstor.com.
<https://www.westconcomstor.com/content/dam/wcgcom/Global/CorpSite/pdfs/Palo-Alto-Networks-WildFire-at-a-glance-EN.pdf>

6. Lampiran

URL Slide Presentation:

https://www.canva.com/design/DAFTQp04GCw/FoOASbLWh54eyD7eWnhS9Q/edit?utm_content=DAFTQp04GCw&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton

URL video presentation:

<https://drive.google.com/file/d/1CEG7JOy7AQMUIEhSMc9m3GKJQfi0Ys8A/view?usp=sharing>