Implementasi Dan Mitigasi *Phishing Attack* Menggunakan Metode *Human-Based* Pada Pt. Xyz

Pramudya Farmadika[1], Adityas Widjajarto[2], Muhammad Fathinuddi[3]
[1] Hubungan Masyarakat, Fakultas Komunikasi dan Ilmu Sosial, Universitas Telkom, Indonesia, pramudyafarmadika@student.telkomuniversity.ac.id
[2] Hubungan Masyarakat, Fakultas Komunikasi dan Ilmu Sosial, Universitas Telkom, Indonesia, adtwjrt@telkomuniversity.ac.id
[3] Hubungan Masyarakat, Fakultas Komunikasi dan Ilmu Sosial, Universitas Telkom, Indonesia, muhammadFathinuddin@telkomuniversity.ac.id

Abstrak
Phishing merupakan serangan di mana penyerang mencoba untuk mendapatkan informasi sensitif seperti data pribadi dengan menyamar sebagai entitas yang terpercaya. Keamanan informasi dapat diukur dari pengujian *phishing attack*. Penelitian ini bertujuan untuk melakukan mitigasi terhadap keamanan informasi berdasarkan hasil eksperimen *phishing attack*. Eksperimen menggunakan OSINT *tools* dan aktivitas *social engineering* dengan melakukan mitigasi berdasarkan metode *human-based*. *Phishing attack* yang dilakukan menggunakan teknik *spear phishing* dan *social media phishing*. *Spear phishing* digunakan untuk memanipulasi suatu bidang pada perusahaan dengan cara *website cloning* url perusahaan dengan menggunakan SEToolkit, *social media phishing* dengan *website cloning* media sosial, seperti Instagram dan Facebook menggunakan Zphisher, kepada pegawai perusahaan. OSINT *tools* yang paling dominan adalah Snov.io dengan mendapatkan data nama, *email*, dan pekerjaan sebanyak 81 data. Eksperimen OSINT, *social engineering*, dan *phishing attack* dijelaskan dalam bentuk DFD untuk menunjukkan alur dari serangan yang dilakukan. *Activity diagram* digunakan untuk merumuskan penggunaan konten *email*. Setelah mendapatkan data, dilakukan analisis perbandingan dari hasil eksperimen konten *email* untuk menyusun mitigasi agar dapat mencegah dampak serangan siber. Mitigasi yang digunakan menggunakan metode *human- based*, metode yang berfokus pada aspek *people*, yaitu aspek yang berfokus pada kesadaran dan perilaku manusia untuk mencegah ancaman serangan *phishing*. Dengan memberikan edukasi kepada pegawai secara rutin, setidaknya sebulan sekali melalui pelatihan, simulasi, dan pengujian, perusahaan dapat mencegah kemungkinan terjadinya insiden keamanan yang disebabkan oleh kelalaian atau kurangnya pengetahuan pegawai.

Kata kunci—phishing, osint, social engineering, human- based, mitigasi

I. PENDAHULUAN

Teknologi informasi dan komunikasi yang sudah sangat berkembang di era industri 4.0 yang pesat membuka banyak fasilitas yang tersedia. Perkembangan teknologi informasi, termasuk Internet, komputasi awan, dan perangkat seluler, telah menciptakan lebih banyak pintu masuk ke sistem, memperluas serangan yang mungkin, dan meningkatkan kerentanannya. Ancaman terhadap keamanan informasi dapat berasal dari berbagai pihak, termasuk peretas, penjahat siber, pesaing, dan bahkan pegawai yang tidak bermaksud baik. Keamanan siber mencakup segala sesuatu berhubungan dengan pengawasan komputer, *monitoring* sampai kontrol yang sangat ketat atau perjuangan untuk hak asasi fundamental. Dalam mencegah ancaman terhadap keamanan informasi suatu perusahaan, dapat dilakukan pengujian serangan *phishing* dengan menggunakan OSINT *tools* dan *social engineering* untuk menganalisis hasil dari pengujian agar dapat dilakukan mitigasi berdasarkan hasil analisis dari serangan *phishing* tersebut. Teknik yang dapat dipakai dalam pengujian serangan *phishing* tersebut, yaitu *spear phishing* dan *social media phishing*. *Spear phishing* untuk melakukan serangan dengan menargetkan suatu individu dan *social media phishing* untuk melakukan serangan menggunakan*website* media sosial yang sering dipakai target.

Seperti pada kasus yang ada di PT. XYZ yang terjadi kebocoran data. Berdasarkan kasus tersebut dapat dilakukan pengujian untuk menganalisis keamanan informasi dengan melakukan *phishing attack* menggunakan *Open Source Intelligence* (OSINT) dan *Social Engineering*. OSINT sendiri berguna sebagai tempat pengumpulan data yang digunakan untuk menganalisis sumber informasi terbuka dan *social engineering* merupakan teknik untuk

memanipulasi target agar dapat memberikan informasi pribadi.

Dari hasil pengujian serangan tersebut dapat dilakukan mitigasi untuk mencegah atau mengurangi dampak terkena serangan siber yang akan merugikan perusahaan dengan meningkatkan pemahaman terhadap bahaya serangan siber. Mitigasi pada penelitian ini menggunakan metode *human- based*. Metode *human-based* ini merupakan pendekatan yang memprioritaskan pengetahuan, sikap, dan tindakan yang dilakukan oleh manusia dalam upaya pengembangan sistem atau aplikasi.

II. KAJIAN TEORI

A. *Open Source Intelligence (OSINT)*

Open Source Intelligence (OSINT) adalah intelijen yang dihasilkan dari informasi yang tersedia untuk umum dan dikumpulkan, dieksploitasi, dan disebarluaskan secara tepat kepada audiens dengan tujuan untuk memenuhi persyaratan kebutuhan intelijen tertentu [1].

B. Kali Linux

Kali Linux adalah distribusi Linux berbasis Debian yang berfokus pada pengujian penetrasi tingkat lanjut dan peretasan etis. Linux sendiri berisikan beberapa alat yang ditujukan untuk berbagai macam tugas keamanan informasi, seperti pengujian penetrasi, pemeriksaan keamanan, komputer forensik, dan rekayasa terbalik [2].

C. *Social engineering*

Social engineering adalah teknik memanipulasi psikologis target dengan memanfaatkan kelemahan dan kesalahan manusia, yang bertujuan untuk memdapatkan informasi data pribadi atau sensitif. *Social engineering* biasanya dilakukan oleh pihak luar yang menggunakan berbagai trik psikologis untuk membuat pengguna komputer memberikan informasi yang mereka butuhkan untuk mengakses komputer atau jaringan . (Peltier, Thommas, 2006.).

D. *Phishing attack*

Phishing attack adalah jenis serangan jaringan khusus, di mana penyerang membuat replika halaman *web* yang sudah ada untuk mengelabui pengguna agar mengirimkan data pribadi, keuangan, transaksi, atau kata sandi ke situs *web* yang mereka anggap sebagai situs *web* penyedia layanan mereka [4].

E. *Spear phishing*

Spear phishing adalah teknik serangan *phishing* yang lebih terarah lewat *email phishing* dan menggunakan informasi pribadi tentang korban yang dituju agar tampak autentik dan meningkatkan kemungkinan target menanggapi serangan. Oleh karena itu, serangan ini sangat sulit dideteksi oleh pengguna dan menimbulkan masalah keamanan yang semakin meningkat bagi pengguna daring. [5].

F. *Social media phishing*

Phishing media sosial adalah bentuk serangan siber dengan cara menipu pengguna agar mengungkapkan informasi pribadi atau sensitif melalui *platform* media sosial. Media sosial menjadi sasaran utama *hacker* untuk menjalankan aksinya karena media sosial memiliki banyak pengguna dan sangat bebas tanpa adanya suatu *filter.* [6].

G. Mitigasi

Mitigasi TI menekankan pada tindakan awal dalam suatu proyek untuk mencegah terjadinya kejadian yang tidak diinginkan atau mengurangi konsekuensi dari kejadian tersebut . [7].

H. *Human-Based*

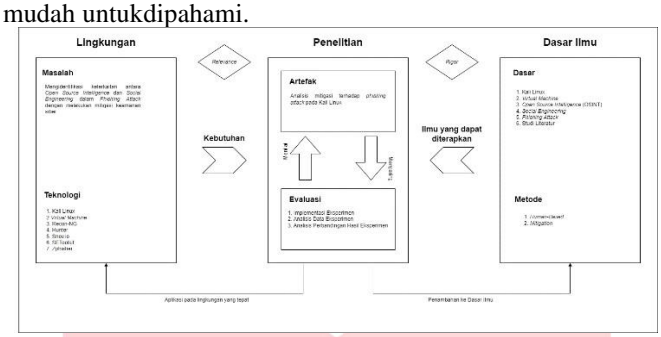
Metode *human-based* digunakan karena melibatkan manusia sebagai pengguna dari segi kebutuhan dan tingkah laku. Pendekatan ini menekankan pentingnya memahami bagaimana manusia berinteraksi dengan sistem, serta bagaimana kebutuhan dan preferensi mereka dapat dipenuhi secara efektif. [8].

III. METODE

A. Model Konseptual

Model dapat diartikan sebagai suatu kerangka konseptual yang berguna sebagai pedoman dalam melakukan

aktivitas atau kegiatan. Model ini juga dapat dipahami sebagai: (1) Suatu tipe atau desain; (2) Deskripsi atau gambaran yang dapat digunakan untuk membantu proses evaluasi yang tidak dapat diamati secara langsung; (3) Suatu sistem yang bisa diasumsikan, dan juga dapat berupa data-data yang dipakai untuk menggambarkan suatu obyek atau aktivitas; (4) Suatu desain yang telah disederhanakan dari suatu sistem kerja; (5) Penyajian yang diperkecil agar dapat lebih mudah untukdipahami.



Gambar 1 Model Konseptual

Model konseptual pada Gambar III.1 Model konseptual dijelaskan secara detail sebagai berikut:

1. Pada bagian lingkungan terdiri dari dua elemen, yaitu Masalah dan Teknologi. Pada Masalah, Mengidentifikasi keterkaitan antara OSINT dan *social engineering* dan melakukan mitigasi keamanan siber. Kemudian Teknologi yang dipakai pada penelitian ini, yaitu Kali Linux, Virtual Machine, Recon-NG, Hunter, Snov.io, SEToolkit,dan Zphisher.
2. Pada bagian penelitian terdiri dari dua elemen, yaitu Artefak dan Evaluasi. Bagian artefak penelitian ini menghasilkan analisis mitigasi terhadap *phishing attack* pada Kali Linux, sedangkan pada bagian Evaluasi sendiri terdiri dari implementasi eksperimen, analisis data eksperimen, dan analisis perbandingan hasil eksperimen.
3. Pada bagian dasar ilmu terdiri dari dua elemen, yaitu dasar dan metode. Bagian dasar terdiri dari Kali Linux, Virtual Machine, *Open Source Intelligence*, Social engineering, *Phishing Attack*, dan Studi Literatur. Pada bagian metode terdiri dari *Human- Based* dan *Mitigation*.

B. Sistematika Penyelesaian Masalah

1. Tahap Awal

Tahap awal dalam penelitian ini diawali dengan memahami *phishing attack*, bagaimana mengimplementasikan *phishing attack*, teknik yang digunakan dalam *phishing attack*, dan mitigasi yang dapat dilakukan untuk menyusun mitigasi terhadap *phishing attack* dengan mengacu pada studi literatur. Studi literatur berfungsi untuk memperdalam dan meningkatkan pemahaman teori mengenai keamanan informasi. Selanjutnya, mengetahui fungsi OSINT dan *socialengineering*.

2. Tahap Hipotesa

Pada tahap ke-dua yaitu tahap hipotesa. Pada tahap ini melakukan hipotesa dengan penggunaan OSINT *tools* dan social engineering untuk menyusun mitigasi berdasarkan *phishing attack*.

3. Tahap Eksperimen

Pada tahap ke-tiga yaitu tahap eksperimen, yaitu dengan melakukan implementasi eksperimen yang dibagi menjadi tiga tahap, yaitu:

a. Implementasi Eksperimen menggunakan OSINT *tools*.
b. Implementasi Eksperimen menggunakan aktivitas *social engineering*.
c. Implementasi Eksperimen menggunakan konten *email phishing*.

Pada implementasi eksperimen dengan OSINT dan social engineering ini menghasilkan data *input* dan data *output*. Selanjutnya, pada konten *email phishing* akan membuat skenario konten *email phishing*. Kemudian, menjalankan skenario konten *email phishing* menggunakan teknik *spear phishing* dan *social media phishing*.

4. Tahap Analisis

Pada tahap ke-empat yaitu melakukan analisis. Proses analisis ini dilakukan dengan menganalisa data eksperimen berupa data *input* dan *output* dari OSINT *tools* dan aktivitas *social engineering* dan menganalisis perbandingan konten *email phishing* berdasarkan teknik *spear phishing* dan *social media phishing*. Dilanjutkan dengan menganilisis mitigasi *phishing attack* berdasarkan metode *human-based*.

5. Tahap Pelaporan

Pada tahap akhir ini, berisi penyusunan kesimpulan dan sarandari hasil analisa eksperimen dan mitigasi.

IV. HASIL DAN PEMBAHASAN

A. Spesifikasi Perangkat Keras

Tabel 1 adalah tabel yang menjelaskan perangkas keras selama proses pengujian dan penelitian. Berikut ini adalah rincian perangkat keras yang digunakan:

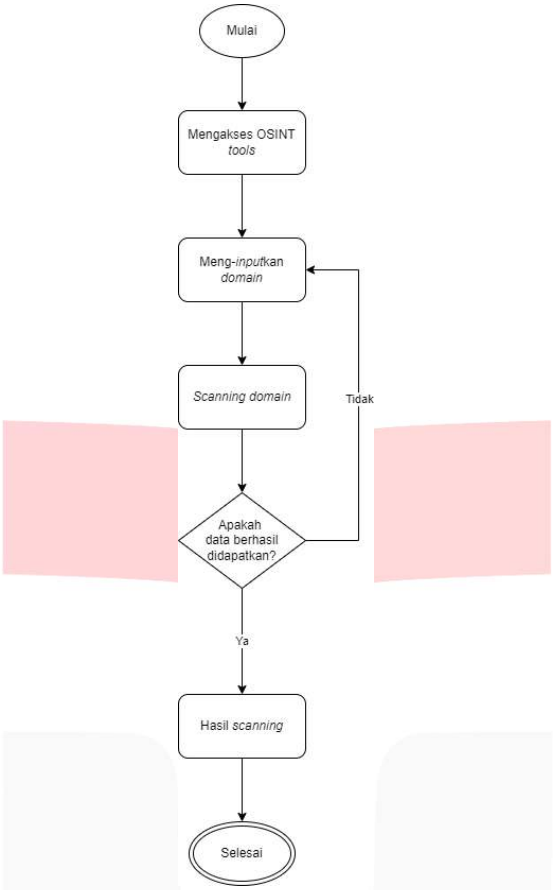
Tabel 1 Spesifikasi Perangkat Keras

Komponen	**Informasi**	
Core Hardware Specification	*Processor*	Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
	Memory	8192MB RAM
	Disk	SSD 512GB, HDD 1TB
	Operating System	Windows 11 Home Single Language 64-bit (10.0, Build 22631)
Virtual Machine Specification	*Processor*	Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz (12 CPUs), ~2.6GHz
	Memory	6048MB
	Disk	20 GB HDD
	Operating System	Kali Linux 2023.1 kali-rolling

B. Spesifikasi Perangkat Lunak

Pada penelitian ini spesifikasi perangkat lunak menggunakan *operating system* Kali Linux, *tools* OSINT Recon-NG, Hunter, Get Prospect, Snov.io dan untuk *phishingtools* yaitu Zphisher dan SEToolkit.

C. Skenario Implementasi Aktivitas *Social Engineering*

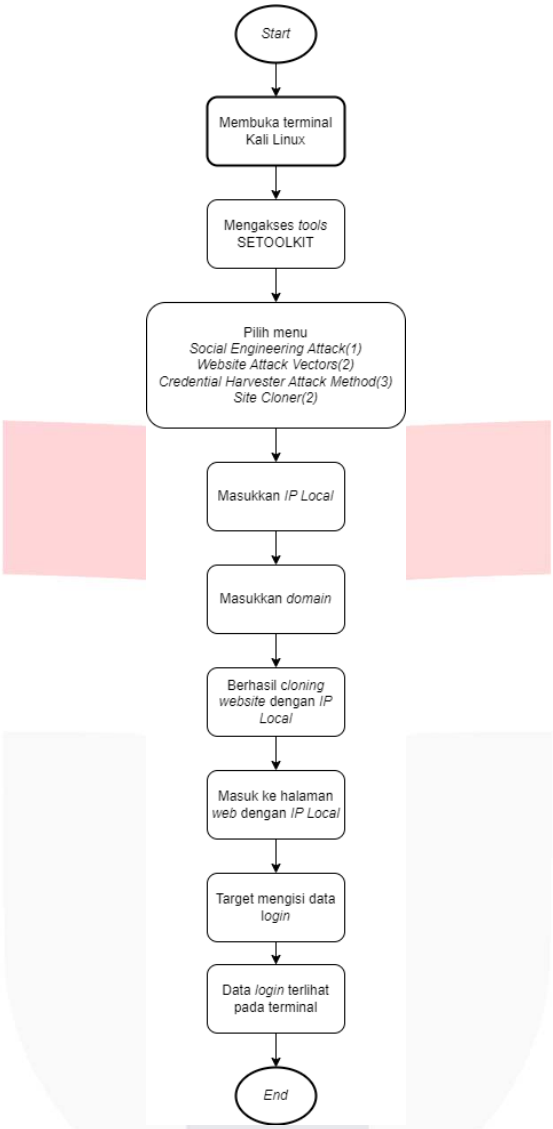


Gambar 2 Skenario Aktivitas *Social Engineering*

Gambar diatas merupakan skenario aktivitas *social engineering* menggunakan OSINT *tools* sampai berhasil mendapatkan data yang melibatkan beberapa langkah, yaitu:

a. Memulai mengakses OSINT *tools*
b. Meng-*input*kan *domain* yang dituju
c. Melakukan *scanning domain*, apakah data berhasil didapatkan, jika tidak maka kembali ke tahap sebelumnya.
d. Mendapatkan hasil *scanning*, dan proses selesai

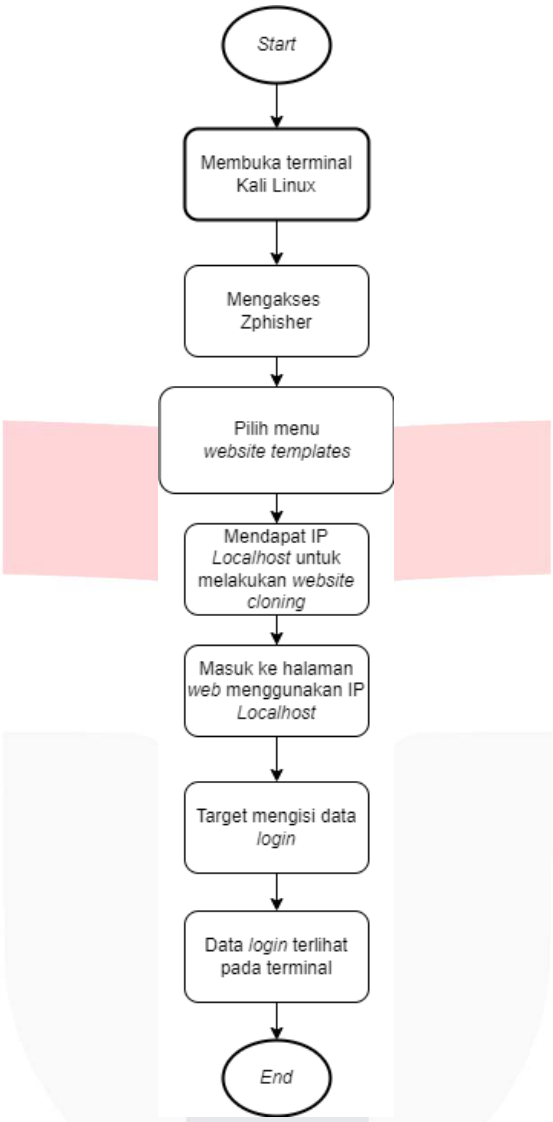
D. Skenario Eksperimen *Phishing Attack* MenggunakanSEToolkit



Gambar 3 Skenario Eksperimen *Phishing Attack* MenggunakanSEToolkit

Gambar diatas merupakan skenario eksperimen phishing attack yang dijalankan pada terminal Kali Linux menggunakan SEToolkit. Pada eksperimen ini dilakukan percobaan *cloning* pada *website* perusahaan yang ditemukan lewat aktivitas *social engineering*. Jika proses *cloning* berhasil, maka akan ditampilkan alamat *website* yang telah di-*cloning* yang akan dilanjutkan dengan proses *phishing attack* untuk mendapatkan informasi sensitif dari target. Setelah target mengisi halaman *website cloning* tersebut, data akan otomatis terlihat pada terminal Kali Linux.

D. Skenario Eksperimen *Phishing Attack* Menggunakan Zphisher

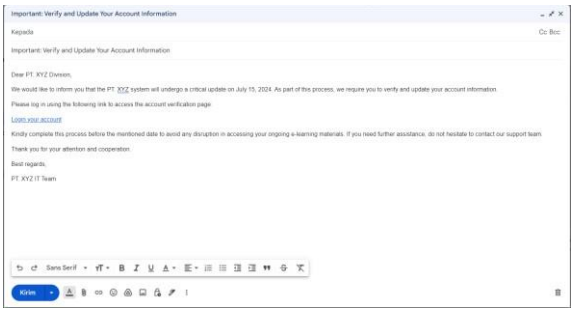


Gambar 4 Skenario Eksperimen *Phishing Attack* MenggunakanZphisher

Gambar diatas merupakan skenario eksperimen phishing attack yang dijalankan pada terminal Kali Linux menggunakan *tools* Zphisher. Pada eksperimen ini dilakukanpercobaan *cloning* pada *website* media sosial. *Tools* akan menyediakan *website templates* yang bisa dipakai, sebagai contoh disini memakai *template* Instagram untuk di-*cloning*.Jika proses *cloning* berhasil, maka akan ditampilkan alamat *website* yang telah di-*cloning* yang akan dilanjutkan dengan proses *phishing attack* untuk mendapatkan informasi sensitifdari target. Setelah target mengisi halaman *website cloning* tersebut, data akan otomatis terlihat pada terminal Kali Linux.

E. Skenario Eksperimen *Phishing Attack* dengan Menggunakan Konten *Email*

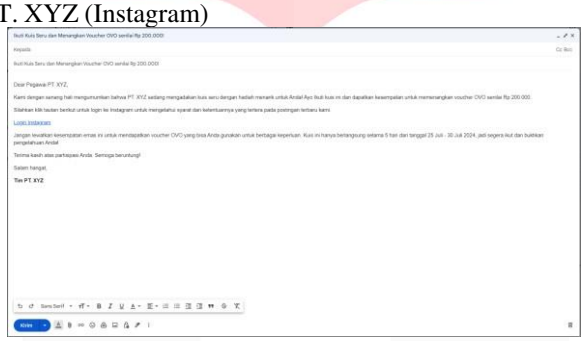
1. Skenario Eksperimen *Phishing Attack* dengan SEToolkit Menggunakan Konten *Email* terhadap *website* 1 (website1.zzz.xx.aa)



Gambar 5 Eksperimen Konten *Email* Menggunakan SEToolkit

Gambar 5 merupakan Eksperimen menggunakan Gmail untuk membuat konten *email* yang akan dikirimkan kepada target. *User* menggunakan alamat *website* dari PT. XYZ yaitu website1.zzz.xx.aa dan membuat konten *email* untuk Divisi PT. XYZ. Konten berisi pesan tentang sistem yang sedang mengalami pembaruan yang mengharuskan pengguna untuk memverikasi dan memperbarui akun dengan masuk ke url yang tertera pada pesan tersebut dan mengisi data *login*.

2. Skenario Eksperimen Zphisher Menggunakan Konten *Email* terhadap Pegawai PT. XYZ (Instagram)



Gambar 6 Eksperimen Konten *Email* Menggunakan Zphisher

Gambar 6 merupakan Eksperimen menggunakan Gmail untuk membuat konten *email* yang akan dikirimkan kepada target. *User* menggunakan alamat *website* dari Instagram dan membuat konten *email* untuk Pegawai PT. XYZ. Konten berisi pesan untuk mengikuti kuis berhadiah yang diselenggarakan oleh PT. XYZ yang mengharuskan pegawai untuk *login* ke Instagram dengan url yang telah disediakan dan melihat syarat dan ketentuannya pada postingan terbaru PT. XYZ.

F. Analisis perbandingan terhadap Konten *Email*

Tabel 2 Perbandingan konten *email*

No	URL PT. XYZ (Internal)	URL Media Sosial (Publik)
	website1.zzz.xx.aa	www.instagram.com
1	Akses Terbatas	Visibilitas Tinggi
2	Target *domain email* Pegawai PT. XYZ	Target identitas Pegawai PT. XYZ
3	Konten Terfokus	Konten Variatif

Tabel V.2 merupakan perbandingan antara kedua alamat *email* yang telah berhasil di-*cloning* dan dijadikan

konten*email phishing*.

1. Akses Terbatas, yaitu url yang hanya dapat diakses oleh pegawai PT. XYZ. Pada tabel tersebut url PT. XYZ yang berhasil di-*cloning* adalah website1.zzz.xx.aa. Url tersebut dikirim sesuai kebutuhan divisi tersebut.
2. Visibilitas Tinggi, yaitu url yang dapat diakses oleh publik. Pada tabel tersebut menggunakan url dari media sosial yang berhasil di-*cloning* yaitu www.instagram.com. Url tersebut dikirim kepada seluruh pegawai PT. XYZ.
3. Target *domain email* PT. XYZ, dari parameter ini menjelaskan tentang incaran dari serangan yang dilakukan yaitu untuk mendapatkan data internal seperti *domain email* PT. XYZ pegawai dari Divisi yang ditargetkan.
4. Target identitas Pegawai PT. XYZ, dari parameter ini menjelaskan tentang incaran dari serangan yang dilakukan yaitu untuk mendapatkan data identitas dari pegawai PT. XYZ.
5. Konten Terfokus, menggunakan isi konten *email* terkait informasi internal dari Divisi yang ditargetkan untuk memanipulasi pegawai dari Divisitersebut agar membuka url yang dikirim lewat *email*
6. Konten Variatif, menggunakan isi konten *email* yang lebih bervariasi seperti pemberitahuan *like* dan *share* postingan, kuis, berita, kampanye promosi. Upaya tersebut dilakukan untuk memanipulasi target agar membuka url yang dikirim lewat *email*.

G. Mitigasi *Phishing Attack* Berdasarkan Metode *Human-Based*

Mitigasi *phishing attack* dan *social engineering* dapat diimplementasikan menggunakan metode *human-based* dengan melibatkan strategi yang berfokus pada kesadaran dan perilaku manusia untuk mencegah risiko serangan *phishing*. Metode *human-based* merupakan pendekatan yang memprioritaskan pengetahuan, sikap, dan tindakan yang dilakukan oleh manusia dalam upaya pengembangan sistem atau aplikasi. Fungsi dari metode ini dalam mitigasi *phishing* adalah untuk melakukan penanganan terhadap individu atau manusia agar mempunyai kesadaran tentang keamanan informasi dan juga untuk mencegah risiko terkena serangan *phishing*.

Berikut merupakan contoh mitigasi *phishing attack* dari metode *Human-Based*. Dapat dijelaskan dalam tabel "*What, Why, Who, How*" sebagai berikut.

Tabel 3 Implementasi Mitigasi dari *Phishing Attack* berdasarkan Metode *Human-Based* (*What, Why, Who,How*)

No	***What***	***Why***	***Who***	***How***
1	Pelatihan dan simulasi	Meningkatkan kesadaran dan pelatihan tentang sistem TI yang terkait dengan keamanan siber.	Seluruh pegawai, terutama yang sering mengakses *email*.	Memberi materi atau pelatihan khusus kepada pegawai untuk meningkatkan pemahaman tentang adanya ancaman keamanan siber

2	Kebijakan jejaring sosial	Mencegah pegawai agar tidak mudah menyebarkan informasi pribadi atau sensitif.	Seluruh pegawai, terutama yang mengelola informasi sensitif.	Menerapkan kebijakan atau sosialisasi mengenai penggunaan jejaringsosial yangaman

Tabel 3 berisi informasi terkait contoh implementasi mitigasi dari *phishing attack* berdasarkan metode *human-based* yang memuat dua poin, berikut penjelasan terkait poin-poin diatas:

1. Pelatihan dan simulasi, untuk meningkatkan kesadaran dan pelatihan tentang sistem TI yang terkait dengan keamanan siber
   Contoh: Memberikan materi atau pelatihan khusus kepada pegawai untuk meningkatkan pemahaman tentang adanya ancaman keamanan siber agar mengurangi risiko terkena serangan *phishing*.

2. Kebijakan jejaring sosial, Menerapkan kebijakan atau sosialisasi mengenai penggunaan jejaring sosial yang aman, termasuk menghimbau pegawai agar tidak mudah menyebarkan informasi pribadi atau sensitif, terkhusus informasi terkait pekerjaan dan perusahaan. Contoh:
   a. Menyaring informasi yang ingin disebarkan hanya untuk tujuan tertentu, Seperti informasi seputar pekerjaan hanya di-*upload* pada *platform* media sosial yang berfokus dibidang tersebut, seperti LinkedIn. Upaya tersebut dilakukan agar meminimalisir dampak aktivitas *social engineering* yang bisa berakibatkan terkena *phishing attack*.
   b. Pegawai harus menjaga privasi dengan mengatur pengaturan akun sosial media. Untuk membatasi akses hanya kepada orang yang dikenal dan tepercaya. Disarankan untuk menghindari mengunggah informasi pribadi yang dapat digunakan untuk tujuan jahat.
   c. Pegawai diwajibkan untuk tidak membagikan informasi sensitif, rahasia perusahaan, atau data pribadi orang lain di jejaring sosial tanpa izin yang sah. Ini termasuk, namun tidak terbatas pada, informasi keuangan, strategi bisnis, dan data pelanggan.

Mitigasi *phishing attack* dan *social engineering* berdasarkan metode *human-based* ini diharapkan menjadi langkah proaktif yang efektif dalam melindungi perusahaan dari ancaman keamanan siber. Dengan mengedukasi pegawai secara terus-menerus melalui pelatihan, simulasi, dan pengujian rutin, perusahaan dapat mencegah kemungkinan terjadinya insiden keamanan yang disebabkan oleh kelalaianatau kurangnya pengetahuan pegawai.

V. KESIMPULAN

Teknik *spear phishing* dan *social media phishing* memiliki keterkaitan dalam penggunaan OSINT *tools* dan aktivitas *social engineering*. *Spear phishing* melibatkan serangan yang terarah, penyerang menggunakan informasi detail yang telah dikumpulkan melalui OSINT untuk mengirimkan pesan yang dirancang khusus untuk satu atau beberapa individu. DFD, OSINT, dan *social engineering* memiliki keterhubungan dalam implementasi *phishing attack*. DFD membantu dalam memahami bagaimana data dan proses terkait, sedangkan OSINT memberikan informasi tambahan tentang individu dan entitas yang terlibat, dalam penggunaan OSINT *tools*, Snov.io merupakan *tools* yang paling dominan dengan mendapatkan data nama, *email address*, dan pekerjaan sebanyak 81 data. *Social engineering* menggabungkan informasi ini untuk melakukan serangan yang memanipulasi target dengan cara yang sangat spesifik dan berdasarkan pada pengetahuan yang diperoleh. Secara keseluruhan, DFD, OSINT, dan *social engineering* saling terkait dalam memahami danmengeksploitasi sistem informasi dengan lebih terstruktur danefektif.

Metode *human-based* untuk melakukan mitigasi, metode ini berfokus pada aspek *people*, yaitu aspek yang berfokus pada kesadaran dan perilaku manusia untuk mencegah serangan *phishing*. Dengan memberikan edukasi kepada pegawai secara rutin sebulan sekali melalui pelatihan, simulasi, dan pengujian, perusahaan dapat melakukan tindakan pencegahan terjadinya insiden keamanan yang disebabkan oleh kelalaian atau kurangnya pengetahuan pegawai. Pendekatan ini tidak hanya meningkatkan kesadaran pegawai terhadap ancaman yang ada, tetapi juga

membangun budaya keamanan siber yang kuat di seluruh organisasi, sehingga setiap individu merasa bertanggung jawab untuk menjaga keamanan informasi dan aset perusahaan.

REFERENSI

[1] D. V Lande and E. V Shnurko-Tabakova, "OSINT as a part of cyber defense system." [Online]. Available: http://netcraft.com

[2] P. Cisar and R. Pinter, "Journal of Applied Technical and Educational Sciences jATES Some ethical hacking possibilities in Kali Linux environment,"vol. 9, no. 4, pp. 129–149, 2019, doi: 10.24368/jates.v9i4.139.

[3] "6535856a33b27389b0f070f8a841c1bd".

[4] . IEEE Staff, *2012 IEEE International Conference onIntelligence and Security Informatics*. IEEE, 2012.

[5] T. Halevi, N. Memon, and O. Nov, "Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-efficacy and Vulnerability to Spear-Phishing Attacks." [Online]. Available: http://ssrn.com/abstract=2544742https://ssrn.com/abstract=2544742Electroniccopyavailableat:https://ssrn.com/abstract=2544742Electroniccopyavailableat:http://ssrn.com/abstract=2544742

[6] I. Kadek Odie Kharisma Putra, I. Made Adi Darmawan, I. Putu Gede Juliana, K. Kunci, and C. Crime, "TINDAKAN KEJAHATAN PADA DUNIA DIGITAL DALAM BENTUK PHISING CRIMINAL ACTS IN THE DIGITAL WORLD WITH A FORM OF PHISHING," 2022.

[7] N. ChePa, B. Anthony Jn, R. Nor Haizan, and M. Azrifah Az, "A Review on Risk Mitigation of IT Governance," *Information Technology Journal*, vol. 14, no. 1, pp. 1–9, Dec. 2014, doi: 10.3923/itj.2015.1.9.

[8] V. K. Sampurno, R. S. Sianturi, and A. P. Kharisma, "Penggunaan Metode Human-Centered Design dalam Perancangan Pengalaman Pengguna Aplikasi Sistem Informasi UMKM Kelurahan Cacaban Kota Magelang," 2023. [Online]. Available: http://j- ptiik.ub.ac.id