AUDITING & *POLICY* UNTUK MITIGASI *SOCIAL ENGINEERING* DAN *PHISHING ATTACK* PADA KEAMANAN DATA PT. XYZ

1st Putri Alviona Hadist
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
putrialviona@student.telkomuniversity.ac.id

2nd Adityas Widjajarto
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
adtwjrt@telkomuniversity.ac.id

3rd Muhammad Fathinuddin, S.SI., M.T.
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
muhammadFathinuddin@telkomuniversity.ac.id

Abstrak— Keamanan data merupakan aspek penting dari kemajuan teknologi informasi di era digital ini. Meskipun upaya keamanan data terus meningkat, kebocoran data tetap menjadi ancaman signifikan. Penggunaan OSINT menjadi alat yang sangat berguna untuk membantu dalam mitigasi risiko *phishing attack* menggunakan metode *auditing and policy based* dengan melakukan aktivitas *Social Engineering* dan eksperimen menggunakan teknik *spear phishing* pada konten *email*. Hal ini dapat digunakan untuk mengidentifikasi celah keamanan yang mungkin perlu diperbaiki. Dengan menerapkan teknik tersebut, dapat memperoleh gambaran yang lebih jelas mengenai potensi titik lemah pada sistem yang digunakan. Penelitian ini melakukan implementasi eksperimen menggunakan OSINT *tools*, aktivitas *social engineering*, dan konten *email*. Eksperimen OSINT dan *phishing attack* disajikan dalam bentuk *Data Flow Diagram* untuk menunjukkan alur dari serangan yang dilakukan. Pada eksperimen konten *email* dirumuskan menggunakan *Activity Diagram* yang digunakan untuk memvisualisasikan langkah-langkah mitigasi menggunakan metode *auditing and policy based*. Metode ini mencakup penerapan *continuous auditing* dan kebijakan seperti UU PDP dan rancangan SOP yang tepat dalam menjaga keamanan data dalam menghadapi serangan *phishing*. Dengan mengintegrasikan *auditing and policy* memungkinkan penerapan strategi mitigasi yang lebih terstruktur dan berorientasi pada hasil yang efektif untuk melindungi data dari potensi kebocoran dan memperkuat sistem keamanan secara menyeluruh.

Kata kunci*— OSINT, *Phishing, Social Engineering, Auditing and Policy based

I. PENDAHULUAN

Perkembangan teknologi internet yang semakin cepat telah memberikan dampak yang sangat signifikan bagi masyarakat global. Perkembangan tersebut telah mengubah berbagai aspek kehidupan menjadi lebih modern, mencakup bidang sosial, budaya, ekonomi, militer, administrasi, dan lainnya [1]. Adanya perkembangan teknologi internet dan kemudahan akses informasi juga membuka peluang kejahatan yang dapat mengancam keamanan data dan informasi. Keamanan informasi merupakan aspek penting dari kemajuan teknologi informasi di era digital ini. Perlindungan data dan keamanan informasi juga merupakan kebutuhan untuk memastikan integritas, keamanan, dan ketersediaan informasi dalam suatu perusahaan.

Namun, meskipun upaya perlindungan data terus meningkat, kebocoran data tetap menjadi ancaman signifikan. Penggunaan OSINT dalam hal ini dapat membantu dalam menganalisis kebocoran data pada PT. XYZ dan mengidentifikasi celah keamanan yang mungkin perlu diperbaiki. OSINT dapat digunakan untuk melakukan aktivitas *social engineering* yaitu mengumpulkan informasi dari sumber publik dan situs *web* perusahaan.

Untuk menghadapi serangan *phishing*, dapat menerapkan mitigasi risiko yang efektif yaitu menggunakan metode *auditing and policy-based* untuk memastikan bahwa perusahaan dapat memperkuat pertahanan dan mengurangi serangan *phishing*. Mitigasi ini tidak hanya bergantung pada teknologi, tetapi juga melibatkan *auditing* yang sistematis serta kebijakan yang tepat untuk menjaga keamanan data dalam menghadapi serangan *phishing*.

II. KAJIAN TEORI

A. OSINT

OSINT adalah informasi intelijen yang diperoleh dari sumber yang tersedia untuk umum. Informasi ini dikumpulkan, dianalisis, dan disebarluaskan secara tepat waktu kepada audiens yang tepat, dengan tujuan memenuhi kebutuhan infomasi spesifik dan mendukung proses pengambilan keputusan [2].

B. Kali Linux

Kali Linux adalah sistem distribusi Linux yang dirancang dengan fokus pada tugas pengujian penetrasi. Kali Linux dirancang untuk meningkatkan keamanan jaringan dan sistem komputer. Hal ini membantu meminimalkan risiko serangan dan kemungkinan pelanggaran keamanan [3].

C. Phishing

Phishing adalah serangan rekayasa sosial di mana penyerang menyamar sebagai sumber yang terpercaya dalam upaya untuk meyakinkan pengguna agar mengungkapkan informasi pribadi. Penyerang biasanya menggunakan *email* palsu, pesan teks, atau situs *web* palsu yang tampak sah untuk memancing target agar memberikan informasi yang berharga [4].

D. *Social Engineering*

Social engineering adalah serangan yang menggunakan teknik manipulasi psikologis untuk memanfaatkan kelemahan dan kesalahan manusia, dengan tujuan untuk memperoleh informasi yang sensitif atau rahasia. Serangan yang didasarkan pada manipulasi psikologis dilakukan dengan menganalisis pola pikir target, sehingga dapat mempengaruhi target secara efektif [5].

E. *Flowchart*

Flowchart merupakan penggambaran secara grafik dari langkah-langkah dan urutan prosedur dalam sebuah program. Penggambaran ini mempengaruhi penyelesaian masalah, terutama yang perlu dipelajari dan dievaluasi lebih lanjut, karena memberikan pandangan yang jelas tentang bagaimana setiap langkah saling berhubungan dan berkontribusi terhadap tujuan akhir [6].

F. *Activity Diagram*

Activity diagram adalah representasi aliran kerja atau aktivitas dalam sebuah sistem, proses bisnis, atau menu dalam perangkat lunak. Diagram ini memvisualisasikan aktivitas yang terjadi di dalam sistem, bukan tindakan yang dilakukan oleh aktor [7].

G. Data Flow Diagram

Data Flow Diagram (DFD) adalah model logika data atau proses yang dirancang untuk menggambarkan asal usul data, tujuan data yang keluar dari sistem, lokasi penyimpanan data, proses yang menghasilkan data tersebut, serta interaksi antara data yang disimpan dan proses yang diterapkan pada data tersebut [8].

H. *Spear Phishing*

Spear Phishing adalah teknik *email phishing* di mana pelaku telah memiliki informasi pribadi korban, seperti nama dan alamat, dan berusaha untuk memperoleh informasi pribadi tambahan dari korban. Tindakan ini sering kali dilakukan dengan mengirimkan pesan yang tampak sangat relevan dan meyakinkan, sehingga korban merasa lebih cenderung untuk membagikan data sensitif atau melakukan tindakan yang diminta oleh pelaku [9].

I. Mitigasi

Mitigasi adalah pendekatan untuk mengelola risiko dengan cara mengurangi probabilitas terjadinya risiko, dan atau mengurangi dampak negatif yang timbul bila risiko tersebut terjadi, melalui pembuatan prosedur dan pengawasan juga pelatihan [10].

J. *Auditing and Policy Based*

Audit dianggap sebagai pendekatan tambahan terhadap metode berbasis kebijakan, yang terutama digunakan untuk menilai atau memeriksa proses atau sistem guna memastikan kepatuhan terhadap persyaratan. Kebijakan adalah aturan yang ditetapkan untuk membimbing *staff* dalam mendeteksi dan mencegah serangan rekayasa sosial, termasuk *phishing* [11].

K. *Continuous Auditing*

Continuous auditing adalah metode yang digunakan oleh auditor internal untuk melakukan pengauditan, pengawasan, dan penilaian risiko secara berkelanjutan. Dengan melakukan *continuous auditing*, dapat melakukan perbaikan dan evaluasi untuk memitigasi masalah yang dapat terjadi secara berulang dengan lebih cepat [12].

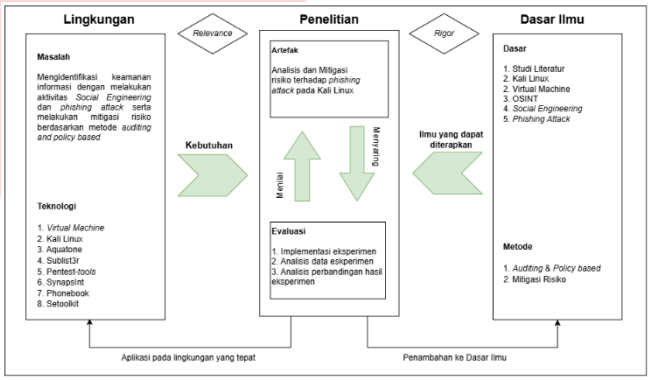
L. SOP

Standard Operating Procedure (SOP) adalah serangkaian prosedur operasional standar yang berfungsi sebagai panduan dalam perusahaan untuk memastikan bahwa setiap langkah kerja anggota dilakukan secara efektif dan konsisten, serta sesuai dengan standar dan sistematika yang telah ditetapkan [13].

III. METODE

A. Model Konseptual

Model konseptual merupakan susunan struktur logis berupa sistem konsep dan kerangka untuk menjelaskan variabel penelitian yang ditinjau dari sudut pandang pengetahuan. Model ini juga dapat digunakan sebagai alat yang digunakan untuk mendeskripsikan dan mewakili berbagai jenis sistem atau kejadian agar lebih mudah dipahami. Berikut merupakan model konseptual untuk membantu penelitian serta mengidentifikasi faktor dari permasalahan penelitian.



Gambar 1 Model Konseptual

B. Sistematika Penulisan

1. Tahap Awal

Tahap Awal dalam penelitian ini yaitu dengan memahami pemahaman mengenai *phishing attack* yang mengacu pada studi literatur. Studi literatur berguna untuk memperdalam teori melalui jurnal dan buku yang juga berkaitan dengan *phishing attack*, Fungsi OSINT, dan *Social Engineering.*

2. Tahap Hipotesa

Tahap kedua yaitu tahap hipotesa. Pada tahapan ini menggunakan OSINT *tools* yang dijalankan pada terminal Kali Linux untuk mengidentifikasi keamanan informasi melalui aktivitas *social engineering* untuk mengumpulkan data terkait perusahaan dan selanjutnya dapat menyusun mitigasi.

3. Tahap Eksperimen

Tahap ketiga melakukan implementasi eksperimen menggunakan tiga kategori utama untuk menguji kemampuan untuk mengidentifikasi keamanan pada perusahaan. Berikut adalah rincian dari tahap implementasi eksperimen ini:

1. Implementasi Eksperimen menggunakan OSINT *tools*
2. Implementasi Eksperimen menggunakan Aktivitas *Social Engineering*
3. Implementasi Eksperimen menggunakan Konten *Email Phishing*

Pada implementasi eksperimen menggunakan konten *email phishing* dilakukan pembuatan skenario dan menjalankannya menggunakan teknik *spear phishing*. Setelah implementasi eksperimen dilakukan, akan menghasilkan data eksperimen berupa data *input* dan *output* dari setiap kategori.

4. Tahap Analisis

Tahap keempat yaitu melakukan analisis. Setelah implementasi eksperimen, hasil *input* dan *output* dari kategori utama akan dilakukan analisis untuk mengevaluasi kemampuan keamanan data pada perusahaan. Berikut adalah langkah-langkah dalam tahap analisis:

1. Analisis perbandingan terhadap konten *email phishing.*
2. Analisis mitigasi risiko *phishing attack* berdasarkan metode *auditing and policy based.*
    a. Mitigasi dengan metode *auditing*, mencakup *continuous auditing.*
    b. Mitigasi dengan metode *policy*, mencakup UU PDP dan rancangan SOP.

Hasil analisis mitigasi berdasarkan metode *auditing and policy* digunakan untuk memaksimalkan pencegahan serangan *phishing* pada perusahaan.

5. Tahap Pelaporan

Tahap kelima yaitu tahap pelaporan. Tahap ini berupa penyusun laporan hasil penelitian serta menyusun kesimpulan dan saran yang diperoleh dari OSINT, aktivitas *social engineering* dan mitigasi.

IV. HASIL DAN PEMBAHASAN

Bagian ini menjelaskan proses eksperimen yang dilakukan untuk memperoleh data, meliputi spesifikasi perangkat yang digunakan, skenario eksperimen *phishing attack*, analisis mitigasi menggunakan metode *auditing and policy based* untuk mengambil langkah pencegahan yang tepat.

1. Spesifikasi Perangkat Lunak

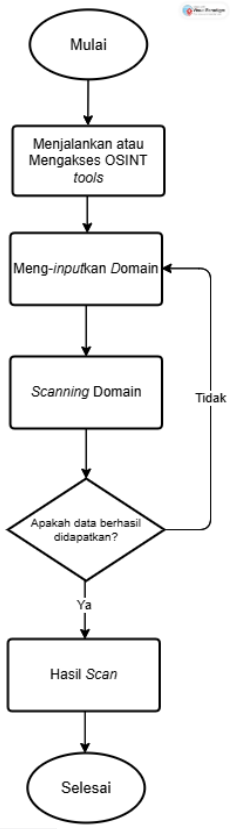
Tipe	Software	Versi
Operating System	Kali Linux	2022.1 Kali-rolling
OSINT *Tools*	Aquatone	1.7.0
	Sublist3r	*Tools* digunakan tahun 2024
	Pentest-*tools*	*Tools* digunakan tahun 2024
	SynapsInt	*Tools* digunakan tahun 2024
	PhoneBook	*Tools* digunakan tahun 2024
Phishing Tools	Social Engineering Toolkit (Setoolkit)	8.0.3

Tabel 1 Spesifikasi Perangkat Lunak

2. Spesifikasi Perangkat Keras

Spesifikasi perangkat keras yang digunakan adalah laptop dengan prosesor Intel Core i7, 8GB RAM, 512 SSD. Perangkat lainnya yang digunakan adalah *Virtual Machine* untuk virtualisasi dalam eksperimen ini.

3. Skenario Implementasi Aktivitas *Social Engineering*

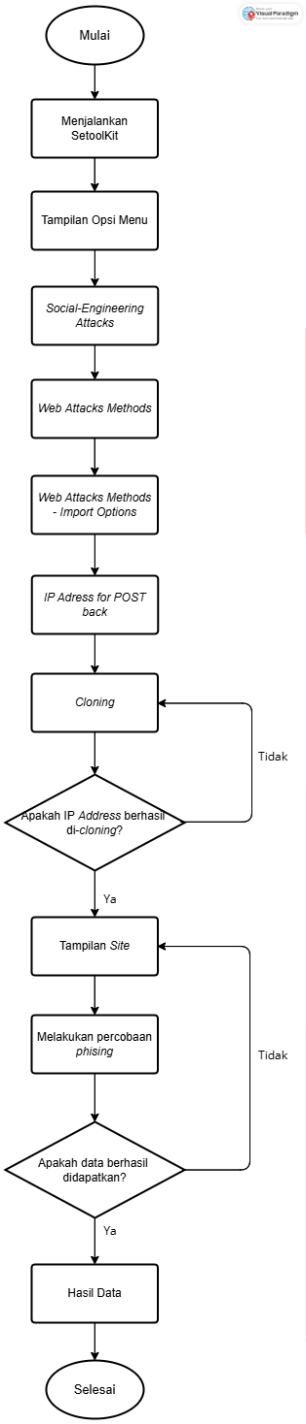


Gambar 2 Skenario Aktivitas *Social Engineering*

Gambar diatas merupakan skenario aktivitas *social engineering* menggunakan OSINT *tools* hingga berhasil mendapatkan data yang melibatkan beberapa langkah diantaranya:

1. Memulai dengan mengakses OSINT *tools*
2. Meng-*input*kan *domain* yang dituju
3. Melakukan *scanning domain*, apakah data berhasil didapatkan, jika tidak akan kembali pada tahap sebelumnya.
4. Mendapatkan hasil *scan*, dan proses selesai.

4. Skenario Eksperimen *Phishing Attack*

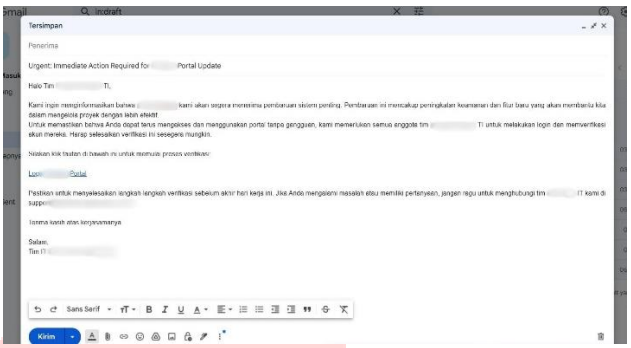


Gambar 3 Skenario Eksperimen *Phishing Attack*

Gambar diatas merupakan skenario eksperimen *phishing attack* yang dijalankan pada terminal Kali Linux menggunakan *tools* Setoolkit. Pada eksperimen ini dilakukan percobaan *cloning* pada *website* perusahaan yang ditemukan melalui aktivitas *social engineering*. Apabila proses *cloning* berhasil, maka akan ditampilkan *website* yang dihasilkan untuk dilanjutkan *phishing attack* untuk mendapatkan informasi sensitif target. Selanjutnya, data ditampilkan pada Setoolkit melalui terminal Kali Linux.

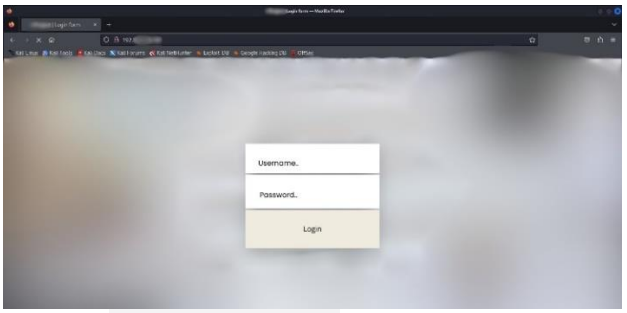
5. Skenario Eksperimen *Phishing Attack* menggunakan konten *email*

a. Konten *email* terhadap *website* 1 (*website*1.zzz.xx.aa)



Gambar 4 Eksperimen terhadap konten *email*

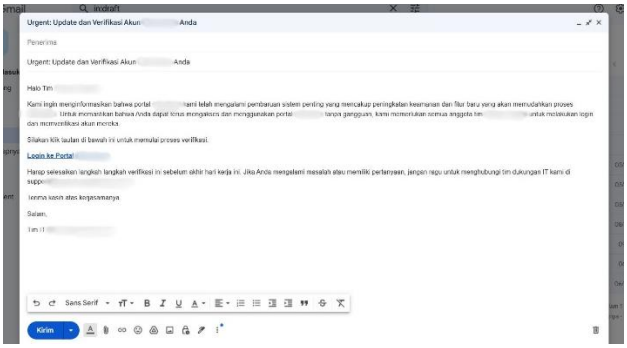
Gambar 4 menunjukkan contoh *email phishing* yang dibuat untuk mendapatkan informasi *login* dari target dengan menyamar sebagai *email* resmi dari Tim IT PT. XYZ terhadap Divisi PT.XYZ. Hal ini merupakan bagian dari eksperimen untuk memahami metode serangan *phishing* dan bagaimana cara agar dapat terhindar dari *email* serupa lainnya.



Gambar 5 Hasil Eksperimen terhadap konten *email*

Gambar 5 menujukkan tampilan dari URL serupa yang menyerupai situs *web* resmi yang terdapat pada pesan *email* yang dikirimkan kepada target. Apabila target berhasil mengakses URL tersebut dan memasukkan data pribadi, maka Setoolkit akan menampilkan data tersebut. Hal ini menunjukkan bahwa serangan *phishing* telah berhasil. Dapat disimpulkan, bahwa *website* 1 dapat di-*cloning*, menandakan *website* tersebut mebamiliki celah keamanan yang *minimum* dan dapat membahayakan perusahaan karena akan mudah terjadinya pencurian data.

b. Konten *email* terhadap *website* 2 (*website*2.zzz.xx.aa)



Gambar 6 Eksperimen terhadap konten *email*

Gambar 6 menunjukkan contoh *email phishing* yang dibuat untuk mendapatkan informasi *login* dari target dengan menyamar sebagai *email* resmi dari Tim IT PT.XYZ terhadap Divisi PT. XYZ. Hal ini merupakan bagian dari eksperimen untuk memahami metode serangan *phishing* dan bagaimana cara agar dapat terhindar dari *email* serupa lainnya.

Gambar 7 Eksperimen terhadap konten *email*

Gambar 7 menunjukkan tampilan URL yang dibagikan kepada target. Tampilan tersebut merupakan hasil *cloning* yang tidak berhasil dari *website* 2. Dapat dilihat bahwa *website* 2 tersebut memiliki kekuatan dan memiliki tingkat keamanan yang tinggi dan dapat dibuktikan dalam serangan *phishing* ini.

6. Analisis Mitigasi Phishing Attack berdasarkan metode *Auditing and Policy Based*

Mitigasi dalam *social engineering* berarti mengambil langkah-langkah untuk mencegah, mendeteksi, dan menanggapi serangan yang memanfaatkan manipulasi psikologis untuk mendapatkan akses ke informasi atau sistem yang sensitif [14].

Social engineering mencakup berbagai teknik, salah satunya adalah *spear phishing*. Teknik ini melibatkan dengan melakukan riset mengenai target, pemalsuan identitas pengirim *email* dan menciptakan skenario agar tampak seolah-olah berasal dari sumber tepercaya. Apabila target menerima *email* tersebut, selanjutnya akan diarahkan ke situs web *phishing* yang menyerupai *web* asli dan mencuri informasi kredensial *login* melalui URL yang dibagikan.

Dengan mengetahui teknik tersebut, perusahaan harus lebih memahami dan mewaspadai dengan menerapkan metode *auditing and policy-based* yang lebih tepat dan melibatkan serangkaian langkah dan prosedur untuk memastikan bahwa kebijakan keamanan diimplementasikan dengan benar.

Auditing and policy merupakan komponen krusial dalam mitigasi risiko serangan *phishing* di perusahaan. Pentingnya *auditing*, terletak pada kemampuannya untuk secara aktif memantau dan menilai aktivitas sistem serta mengidentifikasi kerentanan yang dapat dimanfaatkan oleh pelaku *phishing*. *Policy*, di sisi lain, memberikan panduan yang jelas bagi staff mengenai cara menghadapi ancaman *phishing* dan menetapkan prosedur untuk pelaporan serta *respons* terhadap serangan.

Dalam *auditing*, frekuensi audit dapat bervariasi tergantung pada jenis audit yang dilakukan dan kebijakan perusahaan. Berikut adalah beberapa jenis audit dan frekuensinya:

1. Audit Internal

Frekuensi audit internal dapat bervariasi, mulai dari mingguan, bulanan, triwulanan, semesteran, hingga tahunan berdasarkan kebutuhan spesifik dari area yang diaudit.

2. Audit Eskternal

Dalam audit eksternal dilakukan untuk laporan keuangan dilakukan setahun sekali. Ini adalah standar umum untuk audit tahunan yang diwajibkan oleh regulasi keuangan dan pasar modal untuk memverifikasi laporan keuangan perusahaan.

3. Audit Kepatuhan

Audit ini dilakukan tergantung pada regulasi yang berlaku dan kebijakan internal, audit kepatuhan bisa dilakukan lebih dari sekali dalam setahun.

4. Audit IT (Teknologi Perusahaan)

Frekuensi audit IT juga tergantung pada risiko yang terkait dengan sistem IT dan kebijakan perusahaan. Audit IT bisa dilakukan setahun sekali atau lebih sering, terutama jika ada perubahan besar pada infrastruktur IT atau setelah terjadi insiden keamanan.

5. Audit Sertifikasi

Dalam sertifikasi, audit pengawasan dilakukan setiap tahun, dengan audit sertifikasi ulang biasanya dilakukan setiap tiga tahun.

Dengan frekuensi tersebut, dapat memaksimalkan *auditing* pada perusahaan dalam membantu mitigasi serangan *phishing*. Perusahaan dapat menerapkan metode *continuous auditing* untuk memantau aktivitas secara *real-time* dan memberikan peringatan dini apabila terjadi penyimpangan atau aktivitas mencurigakan.

A. *Continuous Auditing*

Continuous auditing adalah proses audit elektronik yang komprehensif yang memungkinkan auditor memberikan jaminan berkelanjutan terhadap informasi secara simultan dan segera setelah informasi tersebut diungkapkan [15].

Continuous auditing juga berarti auditor mengumpulkan bukti audit dari sistem dan transaksi yang terjadi secara berkelanjutan selama satu periode, sehingga membangun bukti audit serta meningkatkan pengetahuan auditor [16].

Continuous auditing memiliki keunggulan dalam memudahkan auditor mendapatkan informasi, sehingga dapat mengurangi waktu yang dibutuhkan untuk pengujian dalam audit. Metode ini dapat digunakan untuk mempercepat proses audit, yang awalnya memerlukan waktu tiga hari, hingga kurang dari satu hari.

Secara umum, audit berkelanjutan memiliki *key steps process* untuk memantau proses *auditing* agar lebih optimal untuk memberikan rekomendasi perbaikannya, jika diperlukan. Langkah-langkah ini meliputi:

1. *Establishing Priority Areas*

Dalam mitigasi risiko serangan *phishing*, *establishing priority areas* atau penetapan area prioritas untuk audit berkelanjutan sangat relevan, seperti area prioritas dapat mencakup pemeriksaan sistem *email* perusahaan dan kebijakan keamanan yang terkait.

2. *Identifying monitoring and continuous audit rules.*

Dalam melakukan *monitoring and continous audit rules* atau aturan monitor dan audit berkelanjutan, perusahaan dapat menentukan aturan untuk memandu aktivitas audit. Aturan ini mencakup konfigurasi ulang yang harus sering diperbarui dan disesuaikan dengan ancaman *phishing* terbaru.

3. *Determining the process' frequency.*

Dalam menentukan frekuensi proses atau *determining the process' frequency* untuk mitigasi serangan *phishing*, perusahaan perlu mempertimbangkan ritme dari proses yang dilakukan *auditing*, seperti sistem *email* dan pelatihan keamanan. Ketersediaan staff perusahaan yang berpengalaman dalam deteksi dan pemcegahan phishing juga penting. Meskipun pengujian yang lebih sering, seperti pemantauan *email* dan analisis ancaman secara rutin, dapat memberikan manfaat signifikan dalam mendeteksi dan mencegah serangan *phishing*, biaya terkait dengan pengolahan dan tindak lanjut hasil pengujian juga harus dipertimbangkan.

4. *Following up.*

Pada langkah-langkah sebelumnya dijelaskan cara penanganan dan *phishing* yang terdeteksi. Namun, pada tahap *following up* atau proses tindak lanjut berfokus terhadap respon siapa yang menerima ketika serangan *phishing* terdeteksi. Respon tersebut dapat berupa notifikasi berupa alarm ketika *phishing* terdeteksi.

5. *Communicating results*

Dalam mitigasi risiko *phishing*, *communicating results* atau mengkomunikasikan hasil audit berkelanjutan memegang peranan penting yang dapat disampaikan secara konsisten untuk memastikan bahwa tidak terdistorsi oleh faktor *internal* atau eksternal. Hal ini penting untuk menjaga akurasi informasi serangan *phishing* tepat dan berdasarkan data yang valid.

Dari *key steps process* diatas, dapat diterapkan pada perusahaan menggunakan kebijakan yang dapat memaksimalkan proses audit berkelanjutan untuk mitigasi risiko *phishing*.

B. Kebijakan atau Policy dalam Undang-Undang Perlindungan Data (UU PDP)

UU PDP adalah Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi merupakan instrumen hukum yang melindungi data pribadi masyarakat Indonesia dari penyalahgunaan, termasuk praktik *phishing*. UU ini memberikan perlindungan data pribadi seseorang dan menetapkan *sanksi* tegas bagi pelaku kejahatan siber, termasuk pelaku *phishing* [17].

Dalam Pasal 1 Ayat 1 UU PDP dijelaskan bahwa data pribadi adalah data perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau kombinasi dengan informasi lainnya baik secara langusng maupun tidak langsung melalui sistem elektronik atau nonelektronik.

Kebijakan data pribadi menurut UU PDP memberikan perlindungan menyeluruh bagi data pribadi seseorang yang mencakup semua informasi yang dapat digunakan untuk mengidentifikasi individu, baik secara langsung maupun melalui kombinasi informasi lain serta memberikan *sanksi* tegas bagi pelaku kejahatan pencurian data, termasuk pelaku *phishing*.

C. Kebijakan atau Policy *Standard Operating Procedure* (SOP)

Kebijakan atau Policy berikut berupa rancangan *Standard Operating Procedure* (SOP) pada perusahaan, yaitu:

A. Kebijakan atau Policy *Standard Operating Procedure* (SOP) Kontrol Keamanan dalam Penggunaan *Email*

Dengan SOP ini, perusahaan dapat memastikan bahwa penggunaan email dilakukan secara efisien dan aman, serta meminimalkan risiko penyalahgunaan atau pelanggaran kebijakan, sehingga menjamin keamanan dan perlindungan sistem email di perusahaan.

B. Kebijakan atau *Policy Standard Operating Procedure* (SOP) Terhadap Penggunaan *Website Internal* Perusahaan

Dengan SOP ini, dapat menjadi pedoman atau prosedur standar yang ditetapkan untuk mengatur penggunaan dan keamanan *website* yang digunakan dalam lingkungan *internal* perusahaan. SOP ini bertujuan untuk memastikan bahwa semua kegiatan terkait *website internal* dilakukan secara konsisten, aman, dan sesuai dengan kebijakan perusahaan.

C. Kebijakan atau *Policy Standard Operating Procedure* (SOP) Terhadap Penggunaan Media Sosial untuk *Staff* atau Karyawan Dalam Pembuatan Konten Perusahaan

Dengan SOP ini, perusahaan dapat memastikan bahwa terdapat kebijakan dan pedoman yang dirancang untuk mengatur bagaimana karyawan menggunakan platform media sosial dalam pembuatan konten perusahaan. Kebijakan ini bertujuan untuk melindungi reputasi perusahaan, memastikan bahwa informasi yang dibagikan adalah akurat dan sesuai, serta menjaga privasi dan kepatuhan terhadap peraturan.

V. KESIMPULAN

Spear Phishing dan aktivitas *social engineering* efektif untuk mengidentifikasi keamanan informasi dengan menyerang target menggunakan *email* yang tampak sah dan identitas palsu, seringkali berisi URL *phishing* untuk mencuri kredensial *login*. Kemudian, OSINT *tools* dan aktivitas *social engineering* terkait dalam mengumpulkan data keamanan informasi menggunakan alat seperti Aquatone, Pentest-*tools* Sublist3r, dan SynapsInt, dan Phonebook yang menghasilkan data seperti IP *Address*, *Subdomain*, dan *Email Addresses*, kemudian digunakan untuk menyerang target secara spesifik. Selanjutnya, mitigasi risiko *phishing email* memerlukan metode *auditing* berkelanjutan dan kebijakan yang jelas sesuai dengan Undang-Undang Perlindungan Data Pribadi. Kebijakan ini

mencakup SOP untuk keamanan *email*, *website*, dan media sosial yang digunakan untuk melindungi data sensitif dan menjaga reputasi perusahaan.

REFERENSI

[1] H. S. Wahyudi and M. P. Sukmasari, "Teknologi Dan Kehidupan Masyarakat," *J. Anal. Sosiol.*, vol. 3, no. 1, 2018, doi: 10.20961/jas.v3i1.17444.

[2] S. Kelleher and S. S.Analyst, "No Title," *OSINT Common Tools How to use them Safely,"*, 2018.

[3] S. A. Lee Allen, Tedi Heriyanto, "No Title," *Kali Linux–Assuring Secur. by penetration testing.*, 2014, [Online]. Available: https://books.google.co.id/books?hl=en&lr=&id=QcBGAwAAQBAJ&oi=fnd&pg=PT2&dq=Assuring++Security+by+++Penetration+Testing.+Network+Security&ots=s81T_eXi_d&sig=AL9hxicQeLYfpuRc-5aPVWE-RY0&redir_esc=y#v=onepage&q=Assuring Security by Penetration Testing. N

[4] T. . Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "No Title," *Soc. phishing. Commun. ACM*, pp. 94–100, 2007.

[5] S. Wahyuni, I. M. Raazi, and I. Dwitawati, "Analisis Teknik Penyerangan Phishing Pada Social Engineering Terhadap Keamanan Informasi di Media Sosial Profesional Menggunakan Kombinasi Black Eye dan Setoolkit," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 5, no. 1, pp. 49–55, 2022, doi: 10.32672/jnkti.v5i1.3962.

[6] Indrajani, "No Title," *Peranc. Basis Data Dalam all 1*, 2011.

[7] M. A. Musthofa, Nurul; Adiguna, "Perancangan Aplikasi E-Commerce Spare-Part Komputer Berbasis Web Menggunakan CodeIgniter Pada Dhamar Putra Ccomputer Kota Tangerang," *J. Ilmu Komput. dan Sci.*, vol. 1, no. 03, pp. 199–207, 2002.

[8] D. B. Paillin and Y. Widiatmoko, "Rancangan Aplikasi Monitoring Online Untuk Meningkatkan Pemeliharaan Prediktif Pada PLTD," *J. Sist. Inf. Bisnis*, vol. 11, no. 1, pp. 9–17, 2021, doi: 10.21456/vol11iss1pp9-17.

[9] P. Sari and T. Sutabri, "Analisis kejahatan online phising pada institusi pemerintah/pendidik sehari-hari," *J. Digit. Teknol. Inf.*, vol. 6, no. 1, p. 29, 2023, doi: 10.32502/digital.v6i1.5620.

[10] Hery, *Manajemen Risiko Bisnis*. PT Grasindo Jakarta, 2015.

[11] S. Buchyk, "Deteksi Serangan Phishing," pp. 193–209, 2022.

[12] T. Maulidiastuti, Suratno, and M. Yusuf, "Analisis peran akuntansi forensik, data mining, continuous auditing, terhadap pendeteksian fraud serta dampaknya pada pencegahan fraud," *J. EKOBISMAN*, vol. 3, no. 2, pp. 104–121, 2018.

[13] R. M and Tambunan, *Standard Operating Procedures (SOP) Edisi 2*. Jakarta: Maeistas Publishing, 2013.

[14] S. R. Wicaksono, *Social Engineering : Konsep Dasar dan Perkembangan*, no. January. 2024. doi: 10.5281/zenodo.10466386.

[15] Z. Rezaee, P. Ahmad Sharbatoghlie, R. Elam, and P. Peter L. McMickle, "No Title," *A J. Pract. theory. Contin. Audit. Build. Autom. Audit. Capab. 21(1)*, pp. 147–163, 2002.

[16] Hiererra S and M. Sarayar, "Continuous_Audit_Implementasi_dan_Pengendalian_Ber," pp. 763–774, 2014.

[17] J. F. Mariani, "Cracker," *Encycl. Am. Food Drink*, vol. 3, pp. 176–176, 2020, doi: 10.5040/9781635577068-0537.