Dampak Serangan Social Engineering Studi Kasus Data Breach di Indonesia

(Impact of Social Engineering Attacks Case Study of Data Breach in Indonesia)

Oleh:

Yogi Kristiyanto[1*]; Dwi Ismiyana[2]; Johan Mohammad Palah[3]; Muhamad Maulana Rachman[4]

Universitas IPWIJA[1]; Universitas Bina Insani[2]; Universitas IPWIJA[3]; Universitas IPWIJA[4]
yogi.kristiyanto@gmail.com[1]; dwiismiyana@binainsani.ac.id[2]; johanpalah03@gmail.com[3]; muhamadmaulanarachman@gmail.com[4]
*Corresponding Author

Submit: 23 Jul 2024 Accept: 27 Jul 2024 Publish: 31 Agt 2024

ABSTRAK

Social engineering telah menjadi ancaman keamanan siber yang signifikan di Indonesia, menyebabkan kerugian finansial, pencurian identitas, kerusakan reputasi, dan gangguan operasional. Studi ini mengevaluasi dampak social engineering dalam konteks kebocoran data di Indonesia dan mengidentifikasi faktor-faktor yang berkontribusi pada kerentanan terhadap serangan tersebut. Melalui analisis kasus terhadap insiden kebocoran data, penelitian ini mengungkapkan bahwa kurangnya kesadaran keamanan informasi dan pelatihan, ditambah dengan rendahnya literasi digital, merupakan faktor utama yang meningkatkan risiko serangan social engineering. Teknik-teknik seperti phishing, pretexting, dan baiting seringkali digunakan untuk mengeksploitasi kelemahan manusia dan mendapatkan akses ke informasi sensitif. Temuan ini menyoroti perlunya upaya bersama untuk meningkatkan keamanan informasi di Indonesia. Kampanye kesadaran, simulasi serangan, program pelatihan berkelanjutan, dan peningkatan literasi digital nasional merupakan langkah-langkah penting untuk mengurangi risiko serangan social engineering dan melindungi individu serta organisasi dari dampak negatifnya.

Kata kunci:
cybersecurity; darknet exposure; data breach; digital literacy; information security; social engineering

ABSTRACT

Social engineering has become a significant cybersecurity threat in Indonesia, causing financial losses, identity theft, reputational damage, and operational disruptions. This study evaluates the impact of social engineering in the context of data breaches in Indonesia and identifies factors that contribute to vulnerability to such attacks. Through case analysis of data breach incidents, the study reveals that lack of information security awareness and training, coupled with low digital literacy, are key factors that increase the risk of social engineering attacks. Techniques such as phishing, pretexting, and baiting are often used to exploit human weaknesses and gain access to sensitive information. These findings highlight the need for a concerted effort to improve information security in Indonesia. Awareness campaigns, attack simulations, ongoing training programs, and increasing national digital literacy are important steps to reduce the risk of social engineering attacks and protect individuals and organizations from their negative impacts.

Keywords:

cybersecurity; darknet exposure; data breach; digital literacy; information security; social engineering

Pendahuluan

Dampak social engineering saat ini telah menjadi perhatian serius dalam dunia cybersecurity. Social engineering adalah teknik manipulasi psikologis [3] yang digunakan oleh penyerang untuk mengelabui individu agar memberikan informasi rahasia atau melakukan tindakan tertentu yang dapat mengakibatkan kebocoran data atau data breach. Di Indonesia, beberapa kasus kebocoran data yang besar telah mengindikasikan betapa rentannya masyarakat terhadap teknik social engineering ini.

Social engineering telah menjadi ancaman yang semakin meningkat di Indonesia, dengan dampak yang signifikan pada berbagai sektor. Beberapa contoh kasus yang menggarisbawahi dampak ini antara lain pada tahun 2020, Tokopedia, salah satu platform e-commerce terbesar di Indonesia, mengalami kebocoran data yang melibatkan 91 juta pengguna. Meskipun tidak dikonfirmasi secara eksplisit, serangan social engineering seperti phishing diduga menjadi salah satu faktor yang berkontribusi pada insiden ini. Pada tahun 2023, Polri melaporkan peningkatan kasus penipuan online yang melibatkan social engineering, dengan modus undian berhadiah palsu yang menargetkan pengguna media sosial. Korban tertipu untuk memberikan informasi pribadi atau melakukan transfer uang dengan harapan mendapatkan hadiah. Bank-bank di Indonesia juga menjadi target serangan social engineering, seperti vishing (phishing melalui telepon) dan smishing (phishing melalui SMS). Penipu berpura-pura menjadi petugas bank untuk mendapatkan informasi sensitif seperti nomor kartu kredit dan PIN.

Kajian penelitian sebelumnya mendefenisikan social engineering merupakan istilah yang diasosiasikan oleh komunitas peretas dengan proses penggunaan interaksi sosial untuk mendapatkan informasi tentang sistem komputer "korban". Terlebih lagi, social engineering memberikan jalan pintas yang efisien bagi peretas, dan dalam banyak kasus memfasilitasi serangan yang tidak mungkin dilakukan melalui cara lain [1]. Dampak social engineering di Indonesia tidak hanya terbatas pada kerugian finansial, tetapi juga mencakup kerugian non-finansial yang signifikan.

(1) Kerugian Finansial, menurut laporan dari BSSN, kerugian finansial akibat serangan siber di Indonesia pada tahun 2022 mencapai Rp 56 triliun. Serangan social engineering berkontribusi besar pada angka ini, terutama melalui penipuan online dan pencurian data finansial. (2) Kerusakan Reputasi, organisasi yang menjadi korban serangan social engineering dapat mengalami kerusakan reputasi yang parah. Kehilangan kepercayaan dari pelanggan dan mitra bisnis dapat berdampak jangka panjang pada keberhasilan bisnis. (3) Gangguan Operasional, serangan social engineering dapat mengganggu operasional bisnis, menyebabkan downtime, kehilangan produktivitas, dan kerugian finansial tambahan. (4) Dampak Psikologis, korban serangan social engineering seringkali mengalami dampak psikologis seperti stres, kecemasan, dan depresi. Hal ini dapat mempengaruhi kualitas hidup mereka secara keseluruhan.

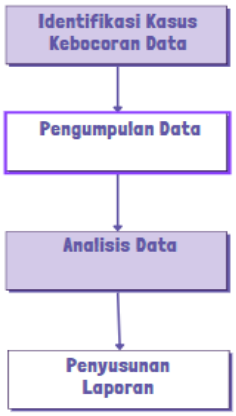
Mengingat dampak yang serius dari social engineering, penting untuk meningkatkan kesadaran masyarakat tentang ancaman ini dan mengambil langkah-langkah proaktif untuk melindungi diri mereka sendiri dan organisasi mereka. Social engineering menggunakan berbagai strategi untuk memanfaatkan kelemahan setiap orang untuk mendapatkan akses ke sistem pribadi, data rahasia, atau uang. Salah satu titik terlemah dalam pertahanan suatu sistem adalah penggunanya. Apa yang disebut distorsi kognitif adalah penyebab ketidaksempurnaan otak manusia. Penyerang menggunakan distorsi ini, kadang-kadang

disebut "kesalahan dalam pemikiran manusia" dalam berbagai cara untuk mengembangkan strategi serangan mereka. Peretas memeriksa kelemahan seseorang atau sekelompok individu yang memiliki akses terhadap data yang diperlukan. Kemudian, mereka menggunakan "kelemahan" yang ditemukan untuk mendapatkan data sensitif atau data yang diinginkan [2].

Tujuan dari studi ini adalah untuk mengevaluasi dampak social engineering dalam konteks kebocoran data di Indonesia, serta mengidentifikasi faktor-faktor yang berkontribusi terhadap rentannya terhadap serangan tersebut. Metode yang digunakan dalam penelitian ini adalah analisis kasus terhadap beberapa insiden kebocoran data yang terjadi di Indonesia. Hasil menunjukkan bahwa kurangnya kesadaran keamanan informasi dan pelatihan menjadi faktor utama yang meningkatkan risiko serangan social engineering. Kesimpulan dari studi ini mengindikasikan perlunya upaya lebih lanjut dalam pendidikan dan pelatihan keamanan untuk mengurangi dampak social engineering.

Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus untuk menganalisis dampak serangan social engineering dalam konteks kebocoran data di Indonesia. Pemilihan metode ini didasarkan pada tujuan penelitian untuk memperoleh pemahaman mendalam mengenai bagaimana social engineering digunakan dalam serangan terhadap berbagai entitas di Indonesia dan untuk mengidentifikasi faktor-faktor yang mempengaruhi tingkat kerentanannya.



Gambar 1. Diagram Tahapan Penelitian

Tahapan Penelitian

Identifikasi Kasus Kebocoran Data

Beberapa insiden kebocoran data di Indonesia yang terjadi dalam lima tahun terakhir dipilih berdasarkan signifikansi dan relevansinya dengan social engineering. Kasus-kasus ini mencakup sektor pemerintahan, pendidikan, dan masyarakat umum. Data diperoleh dari laporan publik, data statistik dari instansi pemerintah, serta laporan investigasi oleh penyedia layanan keamanan siber.

Pengumpulan Data

Mengumpulkan literatur yang relevan, termasuk jurnal ilmiah, laporan industri, dan buku teks, yang membahas teknik social engineering, dampaknya, serta mitigasi risiko. Fokus pada literatur yang berkaitan dengan konteks Indonesia untuk mendapatkan pandangan lokal yang lebih jelas.

Analisis Data

Data dianalisis menggunakan analisis tematik untuk mengidentifikasi pola dan teknik social engineering yang digunakan dalam setiap insiden. Analisis ini juga mencakup identifikasi faktor-faktor yang mempengaruhi rentannya korban, seperti kurangnya kesadaran dan pelatihan keamanan informasi. Kasus-kasus diorganisir ke dalam kategori berdasarkan jenis teknik social engineering yang digunakan (misalnya, phishing, pretexting, baiting) dan sektor yang terkena dampak (misalnya, pemerintahan, pendidikan, masyarakat umum).

Interpretasi Hasil

Menilai dampak dari serangan social engineering terhadap organisasi dan individu yang menjadi korban. Penelitian ini juga mengevaluasi bagaimana tingkat literasi digital dan kesadaran keamanan informasi mempengaruhi keberhasilan serangan. Membandingkan temuan dengan studi terdahulu untuk menilai kesamaan, perbedaan, dan menemukan gap dalam pengetahuan yang ada.

Penyusunan Laporan

Laporan penelitian disusun untuk menyajikan temuan utama, diskusi tentang dampak social engineering, serta rekomendasi untuk meningkatkan kesadaran dan mitigasi risiko di Indonesia.

Penelitian sebelumnya yang berfokus pada social engineering telah banyak membahas teknik-teknik seperti phishing dan pretexting dalam konteks global. Namun, penelitian di Indonesia masih relatif terbatas, terutama yang berfokus pada bagaimana serangan ini mempengaruhi sektor-sektor spesifik di Indonesia seperti pemerintahan dan pendidikan.

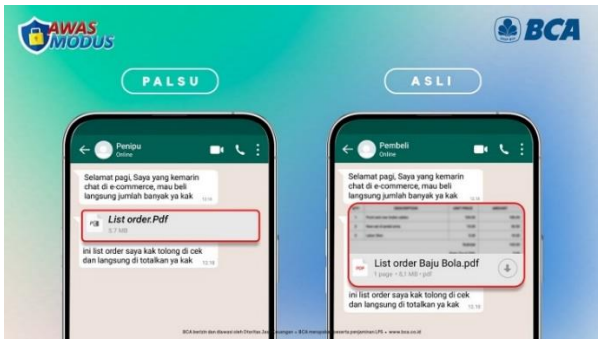
Artikel ini merujuk pada beberapa penelitian terdahulu: (1) Mendefinisikan social engineering dan menyoroti efisiensi serta potensinya dalam memfasilitasi serangan yang sulit dilakukan dengan cara lain. (2) Menjelaskan bagaimana social engineering mengeksploitasi kelemahan manusia dan distorsi kognitif untuk mendapatkan akses ke data sensitif. (3) Menggarisbawahi bahwa social engineering adalah teknik manipulasi psikologis yang digunakan untuk mengelabui individu. (4) Mengidentifikasi phishing, pretexting, dan baiting sebagai teknik social engineering yang paling umum.

Meskipun artikel ini memberikan wawasan berharga tentang dampak social engineering di Indonesia, ada beberapa gap penelitian yang dapat diidentifikasi. (1) Fokus pada kasus: Penelitian ini berfokus pada analisis kasus, yang mungkin membatasi generalisasi temuan ke konteks yang lebih luas. Penelitian kuantitatif dengan sampel yang lebih besar dapat memberikan bukti yang lebih kuat. (2) Kurangnya eksplorasi mendalam tentang faktor kerentanan: Artikel ini mengidentifikasi kurangnya kesadaran dan pelatihan sebagai faktor utama, tetapi tidak menggali lebih dalam faktor-faktor lain seperti budaya, norma sosial, atau faktor teknologi yang mungkin berperan. (3) Tidak adanya solusi konkret: Artikel ini menyarankan perlunya peningkatan kesadaran dan pelatihan, tetapi tidak memberikan solusi konkret atau intervensi spesifik yang dapat diterapkan untuk mengurangi kerentanan terhadap social engineering. (4) Evaluasi dampak jangka panjang: Penelitian ini berfokus pada dampak langsung dari social engineering, tetapi tidak mengevaluasi dampak jangka panjang pada individu atau organisasi, seperti kerugian finansial, kerusakan reputasi, atau dampak psikologis.

Dengan mengatasi gap-gap ini, penelitian selanjutnya dapat memberikan pemahaman yang lebih komprehensif tentang social engineering dan dampaknya di Indonesia, serta mengembangkan strategi yang lebih efektif untuk mengurangi risiko dan melindungi individu serta organisasi dari serangan semacam itu.

Hasil Penelitian

Teknik social engineering yang paling sering digunakan adalah phishing, pretexting, dan baiting [4]. Phishing, teknik ini melibatkan pengiriman email atau pesan palsu yang dirancang untuk menipu penerima agar mengungkapkan informasi pribadi seperti kata sandi atau nomor kartu kredit. Pretexting, penyerang membuat skenario palsu untuk memperoleh informasi dari korban, seperti berpura-pura menjadi teknisi IT yang memerlukan akses ke akun tertentu. Baiting, melibatkan penempatan perangkat yang terinfeksi malware atau menawarkan sesuatu yang menarik untuk menarik perhatian korban agar men-download malware.



Gambar 2. Contoh Phising Menggunakan Chat Messenger WhatsApp [12]

Jumlah laporan phishing yang diterima oleh IDADX dalam kuartal keempat 2023 sebanyak 8.161 laporan dan selama kurun waktu 5 tahun dari tahun 2018 dengan total 106.806 laporan [5]. Contoh kasus data breach pada keamanan informasi di segmen pemerintahan, terdapat 17.585 data kredensial untuk akses ke situs djponline.pajak.go.id yang bocor. Bukan hanya di situs itu saja, kebocoran data milik wajib pajak juga terjadi di situs ereg.pajak.go.id[6],

Serangan social engineering telah menyebabkan kerugian signifikan di Indonesia, baik bagi individu maupun organisasi. Beberapa dampak yang telah tercatat meliputi: (1) Kerugian Finansial, Menurut laporan dari BSSN (Badan Siber dan Sandi Negara), kerugian finansial akibat serangan siber di Indonesia pada tahun 2022 mencapai Rp 56 triliun. Sebagian besar dari kerugian ini disebabkan oleh serangan social engineering seperti phishing dan penipuan online. (2) Pencurian Identitas, Data pribadi yang dicuri melalui serangan social engineering dapat digunakan untuk melakukan pencurian identitas, yang dapat berdampak serius pada korban, seperti pembukaan rekening bank ilegal, pengajuan pinjaman, atau bahkan tindakan kriminal lainnya. (3) Kerusakan Reputasi, Organisasi yang mengalami data breach akibat serangan social engineering dapat mengalami kerusakan reputasi yang signifikan. Kepercayaan pelanggan dan mitra bisnis dapat terganggu, yang dapat berdampak pada pendapatan dan pertumbuhan bisnis. (4) Gangguan Operasional, Serangan social engineering juga dapat mengganggu operasional bisnis, terutama jika penyerang berhasil mendapatkan akses ke sistem penting atau data sensitif. Hal ini dapat menyebabkan downtime, kehilangan produktivitas, dan kerugian finansial.

Data breach adalah insiden keamanan di mana informasi yang sensitif, rahasia, atau terproteksi diakses atau diungkapkan oleh pihak yang tidak berwenang. Ini dapat mencakup data pribadi, informasi keuangan, rahasia bisnis, dan data lain yang seharusnya dilindungi dari akses publik atau tidak sah. Data breach dapat terjadi akibat berbagai faktor, termasuk kesalahan manusia, kerentanan teknis, atau serangan cyber yang dilakukan oleh peretas.

Contoh Kasus di Indonesia, pada tahun 2021, terjadi kebocoran data BPJS Kesehatan yang melibatkan 279 juta data penduduk Indonesia. Data yang bocor meliputi nama, nomor identitas, alamat, nomor telepon, dan informasi kesehatan. Meskipun belum diketahui secara pasti apakah kebocoran ini disebabkan oleh serangan social engineering, insiden ini

menunjukkan betapa rentannya data pribadi di Indonesia. Kemudian adanya penipuan online yang memanfaatkan social engineering, seperti penipuan investasi bodong atau penipuan undian berhadiah, semakin marak di Indonesia. Banyak korban yang tertipu karena kurangnya kesadaran akan risiko keamanan siber dan mudah percaya pada tawaran yang terlalu bagus untuk menjadi kenyataan.

Oleh karena itu, penting untuk meningkatkan kesadaran masyarakat tentang pentingnya keamanan informasi salah satunya dengan meningkatkan Literasi Digital, yaitu sebagai kemampuan untuk mengakses, mengelola, memahami, mengintegrasikan, mengkomunikasikan, mengevaluasi dan menciptakan informasi dengan aman dan tepat melalui teknologi digital [7]. Indeks Literasi Digital Nasional mendapatkan skor 3,54 di tahun 2022, pilar Digital Culture secara umum merupakan pilar dengan skor indeks tertinggi (3,84), sedangkan pilar Digital Safety mendapatkan skor indeks terendah (3,12) [8]. Digital safety, atau keamanan digital, adalah upaya untuk melindungi informasi dan perangkat digital dari ancaman online seperti peretas, malware, virus, dan aktivitas berbahaya lainnya. Ini mencakup berbagai praktik, alat, dan kebijakan yang dirancang untuk menjaga kerahasiaan, integritas, dan ketersediaan data serta melindungi privasi individu saat menggunakan teknologi digital.

Tabel 1. Skor Digital Safety pada Segmen Masyarakat Umum, Pemerintahan, dan Pendidikan (Kominfo, 2022).[9]

Segmen	Indeks Literasi Digital Secure	Sasaran
Masyarakat Umum	3,04	Kelompok Masyarakat di luar sektor lainnya
Pemerintahan	3,46	Tenaga Kerja ASN non tenaga pendidik, TNI, dan Polri
Pendidikan	3,49	Tenaga Pendidik, Siswa dan Mahasiswa

Dari tabel 1 dan data statistik Literasi Digital Nasional dari Kominfo, dapat disimpulkan ada beberapa faktor yang dapat memengaruhi tingkat kesadaran keamanan informasi di Indonesia, antara lain pertama tingkat pendidikan, masyarakat dengan tingkat pendidikan yang lebih tinggi umumnya memiliki tingkat kesadaran keamanan informasi yang lebih tinggi. Kedua, pekerjaan yaitu orang-orang yang bekerja di sektor yang rentan terhadap serangan siber, seperti sektor keuangan dan teknologi, umumnya memiliki tingkat kesadaran keamanan informasi yang lebih tinggi. Ketiga usia, generasi muda umumnya lebih melek teknologi dan lebih sadar akan risiko keamanan siber dibandingkan dengan generasi yang lebih tua. Terakhir akses informasi, masyarakat yang memiliki akses mudah ke informasi tentang keamanan siber umumnya memiliki tingkat kesadaran keamanan informasi yang lebih tinggi.

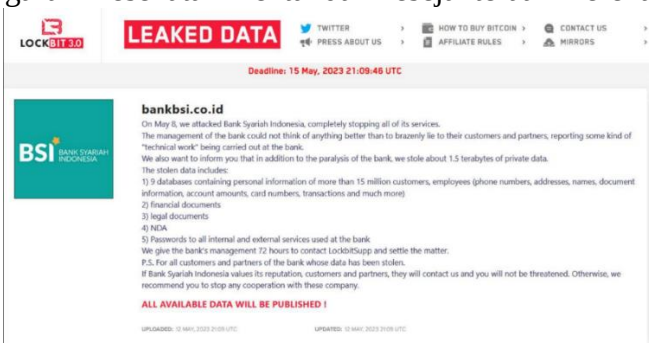
Pembahasan

Hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan informasi di indonesia masih rendah. Hal ini sejalan dengan data statistik Literasi Digital Nasional [8] yang menyatakan bahwa kurangnya kesadaran keamanan informasi merupakan faktor utama yang membuat individu rentan terhadap serangan social engineering. Faktor-faktor penyebab kerentanan yang diidentifikasi dalam penjelasan sebelumnya, merupakan minimnya literasi digital akan kesadaran keamanan informasi di ketiga segmen yaitu masyarakat umum, pemerintah dan pendidikan, menunjukkan bahwa masih banyak yang harus dilakukan untuk meningkatkan keamanan informasi di Indonesia.

Dampak dari kebocoran data yang diakibatkan oleh serangan social engineering yang mengakibatkan data breach dapat membawa ke kondisi darknet exposure, merupakan kondisi

ketika terdapat data/informasi kredensial akun pada suatu instansi/organisasi tertentu yang terekspos di darknet, baik itu pada forum jual beli data, forum diskusi hacker, maupun pada instant messaging, sehingga berpotensi dapat disalahgunakan oleh pihak yang tidak berkepentingan [10].

Selain kerugian finansial yang telah disebutkan sebelumnya, serangan social engineering juga memiliki dampak nyata lainnya di Indonesia. (1) Penipuan Berbasis Social Engineering, pada tahun 2023, Polri mencatat peningkatan kasus penipuan online sebesar 35% dibandingkan tahun sebelumnya. Banyak dari kasus ini melibatkan penggunaan teknik social engineering seperti phishing dan pretexting untuk menipu korban. (2) Serangan terhadap Infrastruktur Kritis, pada tahun 2022, beberapa rumah sakit di Indonesia menjadi target serangan ransomware, yang seringkali dimulai dengan serangan phishing atau social engineering lainnya. Serangan ini mengganggu layanan kesehatan dan membahayakan nyawa pasien. (3) Eksploitasi Data di Dark Web, data pribadi yang dicuri melalui social engineering seringkali dijual di dark web, pasar gelap online yang sulit diakses oleh penegak hukum. Data ini dapat digunakan untuk berbagai tujuan jahat, termasuk penipuan finansial, pemerasan, dan bahkan spionase. (4) Dampak Psikologis pada Korban, korban serangan social engineering seringkali mengalami dampak psikologis yang serius, seperti rasa malu, bersalah, dan cemas. Hal ini dapat mempengaruhi kesehatan mental dan kesejahteraan mereka secara keseluruhan.



Gambar 3. Serangan Ransomware pada Bank BSI [13]

Data-data ini menunjukkan bahwa social engineering merupakan ancaman serius di Indonesia. Untuk mengatasi masalah ini, diperlukan tindakan konkret dari berbagai pihak. (1) Peningkatan Literasi Digital, pemerintah, sektor swasta, dan lembaga pendidikan harus bekerja sama untuk meningkatkan literasi digital masyarakat, terutama dalam hal keamanan siber dan kesadaran akan risiko social engineering. (2) Penguatan Regulasi dan Penegakan Hukum, pemerintah perlu memperkuat regulasi terkait perlindungan data pribadi dan meningkatkan penegakan hukum terhadap pelaku kejahatan siber, termasuk yang menggunakan social engineering. (3) Pengembangan Teknologi Keamanan, organisasi harus terus mengembangkan dan menerapkan teknologi keamanan terbaru untuk melindungi data mereka dari serangan siber, termasuk social engineering. (4) Kolaborasi Lintas Sektor, semua pihak terkait, termasuk pemerintah, sektor swasta, akademisi, dan masyarakat, harus bekerja sama untuk mengatasi ancaman social engineering secara efektif.

Untuk mengatasi masalah ini, diperlukan upaya bersama antara pemerintah, masyarakat umum, dan pendidikan untuk meningkatkan kesadaran dan pelatihan keamanan informasi[11]. Langkah-langkah seperti kampanye kesadaran, simulasi serangan, dan program pelatihan berkelanjutan dapat membantu mengurangi risiko serangan social engineering dan dampak negatif yang ditimbulkannya melalui literasi digital nasional.

Kesimpulan

Phising, pretexting, dan baiting adalah teknik social engineering yang paling sering digunakan dalam insiden kebocoran data di Indonesia. Teknik-teknik ini memanfaatkan kelemahan manusia melalui manipulasi psikologis, menunjukkan bahwa aspek manusia dalam keamanan informasi merupakan titik lemah yang signifikan. Serangan social engineering berdampak serius pada segmen masyarakat umum, pemerintah dan pendidikan dapat menyebabkan data breach ke kondisi darknet exposure. Hasil penelitian menunjukkan bahwa kurangnya kesadaran dan pelatihan keamanan informasi adalah faktor utama yang membuat rentan terhadap serangan. Dampak nyata social engineering di Indonesia: (1) Kerugian Finansial yang Signifikan, studi dari BSSN menunjukkan bahwa kerugian finansial akibat serangan siber, termasuk social engineering, mencapai Rp 56 triliun pada tahun 2022, menunjukkan dampak ekonomi yang besar. (2) Pelanggaran Data Skala Besar, kasus seperti kebocoran data Tokopedia yang melibatkan 91 juta pengguna menunjukkan potensi kerusakan yang luas dari serangan social engineering. (3) Ancaman terhadap Infrastruktur Kritis, serangan ransomware terhadap rumah sakit, yang seringkali dimulai dengan social engineering, menunjukkan bagaimana serangan ini dapat membahayakan nyawa dan mengganggu layanan penting. (4) Eksploitasi Data di Dark Web, data pribadi yang dicuri melalui social engineering seringkali dijual di dark web, menciptakan pasar gelap untuk informasi sensitif yang dapat digunakan untuk berbagai tujuan jahat. Kesimpulan ini menegaskan perlunya tindakan segera dan kolaboratif untuk mengatasi ancaman social engineering di Indonesia. Peningkatan literasi digital, penguatan regulasi, pengembangan teknologi keamanan, dan kolaborasi lintas sektor adalah kunci untuk mengurangi risiko dan melindungi individu serta organisasi dari dampak merugikan serangan ini.

Daftar Pustaka

Zuoguang Wang, Limin sun, And Hongsong Zhu, 2020, Defining Social Engineering in Cybersecurity, IEEE Access Vol. 8 - 202, 85094-85115.

António Lopes, Henrique S. Mamede, Leonilde Reis, Arnaldo Santos, 2024, Common Techniques, Success Attack Factors and Obstacles to Social Engineering: A Systematic Literature Review, Emerging Science Journal Vol. 8, No. 2 - April, 2024, 761-794, ISSN: 2610-9182.

Devi Nurjanah dan Senie Destya, 2022, Pengukuran Tingkat Kesadaran Keamanan Informasi Mahasiswa pada Pembelajaran Online, Jurnal Sistem dan Teknologi Informasi Vol. 10, No. 1 - Januari 2022, 81-85, e-ISSN : 2620-8989.

Muhamad Baihaqi Mohd Azhar, Wan Nurfitri Athirah Wan A.Azlan, Wan Nursyaza Ainaa Wan Mazri, Salliza Md Radzi, 2023, SOCIAL ENGINEERING AND CYBER THREATS: EXPLORING TECHNIQUES, IMPACTS AND STRATEGIES, International Journal of Accounting, Finance and Business (IJAFB) Volume: 8 Issues: 50 - September, 2023, 13 – 25, eISSN: 0128-1844.

IDADX, 2023, LAPORAN AKTIVITAS PHISHING DOMAIN ~.ID Periode Q4 2023 , Indonesia Anti-Phishing Data Exchange Phishing Activity Report, 4th Quarter 2023, 1-8.

Mahmud Ashari (2022, 22 Maret). Belajar Dari Kebocoran Data Kredensial: Data Yang Paling Berharga adalah Data Pribadi. Diakses pada 31 Juni 2024, dari https://www.djkn.kemenkeu.go.id/kpknl-kisaran/baca-artikel/14838/Belajar-Dari-Kebocoran-Data-Kredensial-Data-Yang-Paling-Berharga-adalah-Data-Pribadi.html.

UNESCO (2024, 17 July). What you need to know about literacy. Diakses pada 20 Juli 2024, dari https://www.unesco.org/en/literacy/need-know.

KOMINFO, 2022, Status Literasi Digital Di Indonesia 2022, KOMINFO Katadata Insight Center - 2022, 1 – 78.

KOMINFO (2022). Indeks Literasi Digital. Diakses pada 31 Juni 2024, dari https://survei.literasidigital.id/akses-dan-penggunaan-teknologi-digital.

BSSN, 2023, LANSKAP KEAMANAN SIBER INDONESIA 2023, BSSN – 2023, 1 – 105.

Neetu Bansla, Swati Kunwar And Khushboo Gupta, 2019, Social Engineering: A Technique for Managing Human Behavior, Journal of Information Technology and Sciences Volume 5 Issue 1 – 2019, 18 – 22.

BCA (2023). Waspada Modus Penipuan File PDF Palsu. Diakses pada 31 Juni 2024, dari https://www.bca.co.id/id/informasi/awas-modus/2023/07/07/02/24/waspada-modus-penipuan-file-pdf-palsu.

Agus Ramadhan (2023). Ransomware LockBit Sebut BSI Tidak Transparan: Mereka Berani Berbohong dengan Alasan Maintenance. Diakses pada 31 Juni 2024, dari https://aceh.tribunnews.com/2023/05/13/ransomware-lockbit-sebut-bsi-tidak-transparan-mereka-berani-berbohong-dengan-alasan-maintenance?page=3.