MUSYTARI
ISSN : 3025-9495
Neraca Akuntansi Manajemen, Ekonomi
Vol 17 No 6 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

MEMBANGUN STRATEGI PREVENTIF PROAKTIF UNTUK MENANGKAL PENCURIAN IDENTITAS DI ERA SIBER

Novan Nabil Muthohar[1], Adeela Khairina Alfian[2], Erlangga Putra Kosasih[3], Keryn Gracielle Cheerly[4]
Akuntansi, Universitas Pendidikan Indonesia, Bandung, Indonesia
sigma@upi.edu, adeela.khairina6@upi.edu, erlanggaptra@upi.edu, keryn.cheerly7@upi.edu

Abstract

This article aims to develop effective strategies to address the issue of personal data theft. Referring to the identity theft cycle as outlined in previous studies, it proposes a more comprehensive prevention approach through a combination of technological strategies, legal policies, and consumer awareness to minimize the risks and impacts of data theft. The study employs a qualitative approach through literature reviews, conceptual analysis, and case study evaluations. Secondary data is collected from academic sources, policy reports, and case studies highlighting data theft patterns to construct a comprehensive framework for data theft prevention. The unit of analysis includes individuals as identity theft victims, organizations as service providers and data owners, and regulators responsible for data protection and digital security policies. Preliminary findings indicate that implementing integrated security strategies—such as cyber awareness education and training, the use of encryption technologies and multi-factor authentication, and cross-sector collaboration—can significantly reduce the likelihood and impact of data theft. This study contributes to knowledge-building by integrating findings from literature and real-world cases and by developing a strategic framework that serves as a reference for cybersecurity researchers and practitioners. This framework can support the formulation of policies and technological innovations that are more adaptive to the evolving threats of data theft in the digital era. However, challenges remain in quantitatively measuring the effectiveness of these strategies, as the variability of conditions and the dynamics of data theft attacks require long-term evaluation to assess their global impact on reducing identity theft rates

Keywords: Cybersecurity, Data theft, Cybercrime, Data security

Abstrak

Artikel ini bertujuan mengembangkan strategi efektif dalam mengatasi permasalahan pencurian data pribadi. Mengacu pada siklus pencurian identitas sebagaimana diuraikan dalam penelitian sebelumnya, artikel ini mengembangkan pendekatan pencegahan yang lebih komprehensif dengan kombinasi strategi teknologi, kebijakan hukum, dan kesadaran konsumen untuk meminimalkan risiko dan dampak pencurian data. Penelitian ini menggunakan pendekatan kualitatif melalui studi literatur, analisis konseptual, dan evaluasi studi kasus. Data sekunder dikumpulkan dari sumber akademis, laporan kebijakan, serta studi kasus

Article history
Received: Mei 2025
Reviewed: Mei 2025
Published: Mei 2025

Plagirism checker no 80
Doi : prefix doi : 10.8734/musytari.v1i2.365
Copyright : author
Publish by : musytari

MUSYTARI
ISSN : 3025-9495
Neraca Akuntansi Manajemen, Ekonomi
Vol 17 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

yang menyoroti pola pencurian untuk menyusun kerangka strategi pencegahan pencurian data yang komprehensif. Unit analisis dalam penelitian ini mencakup individu sebagai korban pencurian identitas, organisasi sebagai penyedia layanan dan pemilik data konsumen, serta regulator yang bertanggung jawab dalam perlindungan data dan kebijakan keamanan digital. Hasil penelitian awal menunjukkan bahwa implementasi strategi keamanan terintegrasi, seperti edukasi dan pelatihan kesadaran siber, penerapan teknologi enkripsi dan autentikasi ganda, serta kerjasama lintas sektor, secara signifikan dapat mengurangi potensi dan dampak pencurian data. Penelitian ini berkontribusi dalam membangun pengetahuan dengan menyatukan berbagai temuan dari studi literatur dan kasus nyata, serta mengembangkan kerangka kerja strategis sebagai referensi bagi peneliti dan praktisi keamanan siber. Kerangka ini dapat digunakan untuk merumuskan kebijakan dan inovasi teknologi yang lebih adaptif terhadap perkembangan ancaman pencurian data di era digital. Sayangnya, terdapat tantangan dalam mengukur efektivitas strategi secara kuantitatif, sebab variabilitas kondisi dan dinamika serangan pencurian data serta efektivitas strategi yang diusulkan memerlukan evaluasi lebih lanjut dalam jangka panjang untuk mengukur dampaknya terhadap pengurangan tingkat pencurian identitas secara global.
Kata Kunci: **Keamanan siber, Pencurian data, Kriminal siber, Keamanan data**

PENDAHULUAN

Identitas adalah suatu entitas yang berharga bagi setiap individu yang memilikinya. Menurut (Irshad & Soomro, 2018) kejahatan dalam hal mencuri identitas tidak hanya menjadi pusat perhatian umum, tetapi juga merupakan masalah umum sebelum adanya teknologi informasi internet. Menurut (The Council of Australian Governments, 2007, p. 3) Pencurian identitas terjadi ketika seseorang mengambil atau menggunakan identitas yang telah ada, baik sebagian maupun secara keseluruhan, dengan atau tanpa persetujuan. Tindakan ini dapat menimpa individu yang masih hidup maupun yang sudah meninggal. Dalam era teknologi yang semakin mudah diakses serta meningkatnya permintaan akan informasi, pencurian identitas telah menjadi kejahatan yang semakin marak. Kemudahan dalam memperoleh data pribadi membuat pelaku lebih berani karena risiko tertangkap atau mendapatkan sanksi hukum semakin kecil. Dengan berkembangnya teknologi, kejahatan ini menjadi lebih sulit dideteksi dan semakin sering terjadi, terutama karena banyaknya informasi pribadi yang tersebar di dunia digital. Sebagai akibat dari adanya internet, peningkatan teknologi, dan akses yang mudah ke data pribadi individu seperti, informasi nomor rekening bank dan kartu kredit, nomor jaminan sosial, nomor kartu telepon, dan informasi berharga lainnya dapat digunakan oleh orang lain untuk mendapatkan

MUSYTARI
ISSN : 3025-9495
Neraca Akuntansi Manajemen, Ekonomi
Vol 17 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

keuntungan dengan mengorbankan konsumen (Berghel, 2000). Di Amerika terdapat lima kerugian finansial tertinggi yang dianalisis di ITAP yaitu magnetic stripe sebesar $28,909,617, ATM PIN sebesar $24,223,291, fake ID card information sebesar $15,177,824, financial information sebesar $13,722,781 dan age information $11,977,044 (The University of Texas at Austin, 2017). Banyak organisasi beroperasi secara reaktif dalam menangani masalah. Kami menyarankan pendekatan yang lebih proaktif, seperti "pertahanan preventif". Konsep ini menekankan perlunya fokus pada strategi pencegahan dibandingkan reaksi setelah kejadian terjadi. Dengan pendekatan ini, jumlah kasus pencurian identitas dapat dikurangi sebelum situasi semakin memburuk. Strategi pencegahan yang proaktif ini berfungsi layaknya "pertahanan preventif," karena dalam kasus penipuan, langkah terbaik untuk mengatasi pencurian identitas adalah mencegahnya sejak awal. Jika pencurian identitas sudah terjadi, proses penyelidikan dan penyelesaiannya akan menjadi sulit, mahal, dan memakan banyak waktu.

Di era teknologi saat ini, data pribadi sangat penting untuk dilindungi karena merupakan aset yang sangat berharga. Berbagai metode canggih memungkinkan peretas dengan mudah menyalahgunakan data yang tidak terlindungi. Peretas adalah seseorang yang menggunakan kecerdasan teknis untuk mendapatkan akses tidak sah ke data guna memodifikasi, menghapus, atau menjualnya dengan cara apa pun (Pal dan Anand 2018). Hal ini membawa resiko kehilangan uang, kehormatan, dan pelanggaran privasi.

Maka dari itu, penting untuk menyusun strategi pencegahan agar peretas tidak dapat mencuri data penting konsumen. Strategi ini dimaksudkan untuk meningkatkan sistem keamanan digital dan meminimalkan celah yang dapat dimanfaatkan oleh peretas melalui penggabungan teknologi terbaru, kebijakan hukum, dan prinsip moral. Dengan tindakan preventif yang tepat, harapannya dapat menciptakan ekosistem digital yang aman dan bertanggung jawab.

METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif melalui studi literatur, analisis konseptual, dan evaluasi studi kasus. Data sekunder dikumpulkan dari berbagai sumber akademis, laporan kebijakan, serta studi kasus yang menyoroti pola-pola pencurian untuk menyusun kerangka strategi pencegahan pencurian data yang komprehensif.

HASIL DAN PEMBAHASAN

1. Metode Meretas

Di dunia bisnis saat ini semakin terhubung secara digital, yang mengakibatkan tingginya ancaman dari serangan siber. Pihak yang berniat jahat dengan cerdik dapat menggunakan berbagai teknik untuk memperoleh keuntungan pribadi dan merugikan pengguna internet. Berikut ini adalah 6 metode meretas yang umumnya terjadi dalam peretasan di bisnis:

1) Clickjacking

Clickjacking adalah teknik peretasan di mana penyerang menyembunyikan elemen berbahaya di balik tampilan yang tampak aman, seperti halaman web berbahaya kemudian menempatkan lapisan elemen interaktif di atasnya. Akibatnya, saat pengguna mencoba mengklik elemen yang

MUSYTARI
ISSN : 3025-9495
Neraca Akuntansi Manajemen, Ekonomi
Vol 17 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

mereka anggap aman, mereka sebenarnya mengklik elemen tersembunyi yang menjalankan perintah berbahaya, seperti mengunduh malware, mengubah pengaturan akun, atau mengirimkan data pribadi ke server peretas.

2) Trojan

Menurut Symantec (2018), Trojan adalah jenis malware yang menyamar sebagai program atau file yang tampak sah, namun sebenarnya berisi kode jahat yang memungkinkan peretas mengakses sistem korban tanpa diketahui. Trojan bekerja dengan menipu pengguna agar mengunduh dan menjalankan aplikasi yang terlihat normal, sehingga membuka celah pada komputer korban. Dengan demikian, peretas dapat mencuri data sensitif, mengendalikan sistem, atau bahkan menginstal malware tambahan secara tersembunyi. Untuk mendeteksi Trojan, pengguna dapat menerapkan beberapa pendekatan berikut:

- Deteksi Berbasis Tanda Tangan (Signature-based Detection). Pendekatan ini mencari pola kode yang sudah diketahui dari Trojan di dalam file atau program.
- Analisis Perilaku (Behavior-based Detection). Pendekatan ini memantau aktivitas sistem secara real-time untuk mendeteksi perilaku mencurigakan, seperti akses tidak sah, koneksi ke server yang tidak dikenal, atau perubahan pada sistem file.
- Pendekatan Machine Learning, yaitu dengan menggunakan dataset yang mencakup perilaku normal dan anomali akibat serangan Trojan, contohnya dengan teknik seperti klasifikasi, clustering, dan anomaly detection, model dapat mengenali pola-pola yang khas dari Trojan.

3) Phishing

Menurut Rajalakshmi Shenbaga Moorthy et al. (2020), "Phising adalah kejahatan siber rekayasa sosial yang berbahaya yang bertujuan mencuri informasi pribadi pengguna dengan mengirimkan email yang dipalsukan". Phishing dapat dilakukan dengan cara mengirimkan email, pesan teks, atau bahkan panggilan telepon yang tampak seolah-olah berasal dari sumber yang terpercaya, seperti bank atau layanan online populer. Pesan-pesan tersebut biasanya mengandung tautan yang mengarah ke situs web palsu yang menyerupai situs asli. Begitu korban mengklik tautan tersebut, mereka diminta untuk memasukkan informasi pribadi seperti username, password, atau data keuangan. Serangan phishing tidak hanya dilakukan melalui email biasa, tetapi juga melalui metode seperti spear phishing, yang menargetkan individu atau organisasi tertentu dengan memanfaatkan data yang telah dikumpulkan sebelumnya, dan clone phishing, yaitu dengan memodifikasi email asli yang sah sehingga mengarahkan korban ke situs web palsu. Dua pendekatan dalam mendeteksi serangan phising, yaitu:

- Pendekatan Host-Based: Menggunakan teknik seperti pencocokan pola (pattern matching) dan heuristik untuk mendeteksi malware pada sistem.
- Pendekatan Network-Based: Melibatkan pemantauan informasi status jaringan untuk mengidentifikasi adanya aktivitas mencurigakan atau serangan.

4) Ransomware

Merujuk pada laporan European Union Agency for Cybersecurity (2023) dan Europol (2024), ransomware adalah jenis kejahatan siber di mana file, data, atau perangkat korban dienkripsi oleh peretas, lalu tebusan diminta agar akses dapat dipulihkan.

MUSYTARI
ISSN : 3025-9495
Neraca Akuntansi Manajemen, Ekonomi
Vol 17 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

5) SQL Injection

SQL Injection (SQLi) adalah salah satu serangan siber paling berbahaya yang menargetkan kelemahan sistem database dalam aplikasi web. OWASP mencatat bahwa SQLi termasuk dalam tiga besar ancaman keamanan web pada 2017 dan 2021, karena memungkinkan penyerang untuk menyisipkan kode SQL berbahaya ke dalam input aplikasi sehingga dapat mengakses, mengubah, atau menghapus data tanpa izin. Untuk mendeteksi SQLi, berbagai pendekatan dapat digunakan, mulai dari framework AMNESIA (Analysis and Monitoring for NEutralizing SQL Injection Attacks) yang menganalisis kode secara statis dan dinamis. Paul et al. (2024) menemukan bahwa pendekatan ini meningkatkan akurasi deteksi hingga 97%, menjadikannya lebih efektif dibanding metode tradisional.

6) Spyware

Spyware didefinisikan sebagai malware yang diam-diam memata-matai aktivitas pengguna, mulai dari mencuri informasi login, pesan, hingga file pribadi, serta sering disamarkan dalam aplikasi yang menawarkan fungsi berguna.

2. Simulasi Kebocoran Data

Pada umumnya peretasan yang terjadi dalam bisnis terdapat 3 tipe berdasarkan tujuan yang ingin dicapai oleh peretas (Mahmud, 2019).

1) Financial identity theft

Di mana seseorang ingin mendapatkan keuntungan finansial atas nama orang lain, ini disebut penipuan identitas keuangan. Biasanya pelaku melakukan ini untuk mendapatkan barang dan jasa dengan kredit, pinjaman, dana, atau dana lainnya. Intinya, pencurian identitas finansial untuk mendapatkan keuntungan materi dari identitas orang yang dicuri. Langkahnya sebagai berikut,

- Pelaku melakukan transaksi atau penarikan
- Pelaku menggunakan identitas palsu, seperti kartu kredit atau identitas lainnya
- Korban menerima tagihan atau pemberitahuan
- Pelaku menikmati hasil

Contoh kasus, spamming dan carding di jawa timur yang merugikan Rp 500 juta, pelaku mencuri data kartu kredit milik orang lain yang kemudian digunakan untuk membeli barang melalui online dengan kartu tersebut. Mereka masuk dengan akun palsu di Apple dan Paypal dari akun tersebut, mereka mencuri data berupa nomor kartu kredit dan tanggal expired.

2) Medical identity theft

Peneliti privasi Pam Dixon, pendiri World Privacy Forum, dirilis pertama kali pada tahun 2006. pencurian identitas medis terjadi ketika seseorang mencari penanganan medis dengan memakai identitas orang lain. Pencurian asuransi juga sangat sering terjadi, jika pencuri memiliki informasi asuransi korban dan atau kartu asuransi, maka mereka dapat mencari penanganan medis seolah-olah seperti korban yang memiliki asuransi itu sendiri. Berikut ini adalah keterangan dari simulasi medical identity theft :

- Pelaku melakukan klaim kesehatan

MUSYTARI
ISSN : 3025-9495
Neraca Akuntansi Manajemen, Ekonomi
Vol 17 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

- Pelaku menggunakan identitas palsu (nama, tanggal lahir, nomor kebijakan, kode diagnosis, nomor jaminan sosial)
- Tagihan dan diagnosis dikirim ke korban
- Pelaku tidak terkena tagihan

Contoh kasus, pencurian data Healthcare setengah penduduk Norwegia, seorang hacker berhasil melanggar sistem Health South East Health Authority (RHF) dan dilaporkan mencuri data pribadi dan catatan kesehatan sekitar 2,9 juta orang norwegia dari total 5,2 juta penduduk negara tersebut.

3) Criminal identity theft

Penipuan identitas kriminal terjadi ketika seorang pelaku pelanggaran hukum mengaku dirinya sebagai orang lain kepada polisi atau petugas. Penjahat sebelumnya sering menggunakan kredensial yang dicuri dari orang lain atau hanya menunjukkan identitas palsu untuk mendapatkan dokumen identitas negara. Di sini, korban dapat menghadapi masalah yang signifikan.

- Pelaku melakukan tindakan kriminal dengan menggunakan identitas palsu dan berpura-pura sebagai korban.
- Korban terkena dakwaan, dan pelaku tidak terkena pelanggaran apa pun. Contoh kasus, pencurian dan penggunaan identitas palsu dari Lee Harvey Oswald dalam kasus pembunuhan presiden amerika serikat ke-53 Jhon F kennedy, Jim Garrison sebagai Jaksa Distrik Orleans Parish, Mencurigai bahwa pembunuhan Jhon F Kennedy adalah pembunuhan yang melibatkan lebih dari satu orang. Dan setelah pengusutan diketahui bahwa beberapa dokumen tersangka utama lee Harvey Oswald telah dipalsukan oleh seseorang yang memakai identitasnya. Jadi seolah-olah dia ini adalah pembunuh tunggal dari John F Kennedy.

3. Bagaimana Peretas Mengubah Informasi Pribadi Menjadi Keuntungan Finansial

Dengan memanfaatkan data korban untuk melakukan transaksi atau kegiatan ilegal, peretas mengubah informasi pribadi menjadi keuntungan finansial. Tidak hanya itu, mereka juga dapat merusak identitas korban, yang berdampak buruk dalam jangka panjang. Berikut bagaimana peretas mengubah informasi pribadi menjadi keuntungan finansial:

1) Pembelian barang mahal, dimana penetas menggunakan data korban untuk membuat kartu kredit atau debit palsu dan membeli barang mahal seperti komputer atau televisi. Kemudian, mereka menjual barang-barang ini di pasar gelap untuk mendapatkan uang tunai dengan cepat.

2) Pengajuan pinjaman dan kredit, dimana peretas menggunakan identitas korban untuk mengajukan pinjaman, seperti kredit mobil atau rumah, dan setelah disetujui, barang yang dibeli dijual segera, membuat mereka sulit dilacak.

3) Pembuatan akun layanan telepon yaitu pembuatan akun telepon atau internet atas nama korban dan menggunakan akun ini untuk melakukan kegiatan penipuan lainnya, seperti telemarketing atau transaksi ilegal, serta membangun kredibilitas palsu.

MUSYTARI
ISSN : 3025-9495
Neraca Akuntansi Manajemen, Ekonomi
Vol 17 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

4) Penyalahgunaan rekening bank, dimana peretas dapat mengambil uang dari rekening korban dengan menyalahgunakan rekening bank melalui cek atau kartu debit palsu. Mereka juga dapat membuka rekening baru dengan data korban, kemudian menggunakan rekening tersebut untuk menulis cek palsu, menyebabkan kerugian uang.

5) Manipulasi data identitas, yang dilakukan dengan mengubah mengubah alamat pengiriman akun kredit korban atau bahkan mengajukan kebangkrutan atas nama korban. Karena tindakan ini merusak reputasi dan skor kredit korban, sulit untuk menemukan dan memulihkan kerugian segera.

4. Solusi dan Strategi Pencegahan untuk Meminimalisir Resiko

1) Strategi untuk Konsumen atau Masyarakat

Meningkatnya pelanggaran siber mendorong perlunya melindungi informasi rahasia dan media penyimpanan dari ancaman. Ancaman siber menjadi lebih kompleks seiring meningkatnya jumlah pengguna internet secara global. Hingga Juni 2014, lebih dari tiga miliar orang di seluruh dunia menggunakan internet, khususnya mereka yang berusia 12-19 tahun, merupakan kelompok yang paling aktif menggunakan internet. Studi menunjukkan bahwa mereka lebih rentan terhadap kejahatan siber, seperti pencurian identitas dan pelanggaran privasi. Oleh karena itu, kesadaran keamanan siber sangat penting bagi mereka sebagai strategi pencegahan (Atkinson et al,2009)

Menurut Zahwani, S. T., & Nasution, M. I. P. (2023) dalam artikel yang berjudul "Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital" menyatakan hal-hal berikut:

Cara Melindungi Data Pribadi

1. Gunakan kata sandi yang kuat dan unik untuk setiap akun.
2. Aktifkan autentikasi dua faktor (2FA) untuk keamanan tambahan.
3. Waspada terhadap tautan dan email mencurigakan.
4. Jangan membagikan informasi pribadi secara sembarangan di media sosial.
5. Selalu perbarui perangkat lunak dan aplikasi untuk menghindari celah keamanan.

Mengenali dan Menanggapi Serangan Siber

1. Jika menerima email atau pesan mencurigakan, jangan klik tautan atau unduh lampiran.
2. Laporkan aktivitas mencurigakan kepada penyedia layanan atau pihak berwenang.
3. Jika akun diretas, segera ubah kata sandi dan periksa aktivitas terbaru.

Keamanan siber bukan hanya tanggung jawab pemerintah atau perusahaan, tetapi juga individu. Dengan meningkatkan kesadaran dan menerapkan langkah-langkah perlindungan, kita dapat mengurangi risiko menjadi korban kejahatan siber.

Keamanan siber menjadi aspek krusial bagi perusahaan dalam menghadapi ancaman hacker dan serangan siber. Salah satu tantangan utama adalah memastikan sistem tetap aman dari berbagai upaya eksploitasi yang terus berkembang. Oleh karena itu, diperlukan strategi yang efektif untuk mengelola risiko dan memperkuat pertahanan sistem.

MUSYTARI
ISSN : 3025-9495
Neraca Akuntansi Manajemen, Ekonomi
Vol 17 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

2) Strategi untuk Bisnis

Terdapat tiga strategi utama yang dapat diterapkan perusahaan, yaitu pertanyaan sebagai kunci sistem tetap aman untuk mengidentifikasi potensi celah keamanan, *Security Incident Event Management* (SIEM) untuk mendeteksi dan merespons ancaman secara *real-time*, serta *bug bounty* sebagai metode proaktif dalam menemukan dan menutup kerentanan sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab.

1. Kunci Pertanyaan agar Sistem Tetap Aman

Menurut Lahcen, R. A. M., Caulkins, B., Mohapatra, R., & Kumar, M. (2020), beberapa pertanyaan strategis harus dijawab secara berkala untuk menjaga keamanan sistem, seperti:

- Apakah attack surface sudah terdefinisi? Ini mencakup semua titik lemah yang bisa dimanfaatkan oleh peretas.
- Apa aset paling kritis atau paling rentan? Perusahaan perlu memahami data atau sistem mana yang paling berisiko jika dieksploitasi.
- Bagaimana akses ke sistem dilindungi? Ini termasuk kontrol akses terhadap data penting atau crown jewels.
- Apakah inventaris perangkat yang digunakan sudah diketahui? Termasuk perangkat yang diizinkan dan tidak diizinkan di jaringan.
- Apakah sistem operasi dikonfigurasi dengan baik dan selalu diperbarui? Pembaruan sangat penting untuk menutup celah keamanan.
- Bagaimana sistem mendeteksi kredensial yang dicuri atau akun yang dikompromikan?
- Seberapa efektif pertahanan terhadap malware? Perusahaan perlu memastikan sistem keamanan mereka dapat mengenali dan mencegah serangan malware.
- Apakah karyawan mendapat pelatihan tentang ancaman siber dan risiko media sosial? Kesadaran karyawan tentang keamanan siber dapat mencegah serangan berbasis rekayasa sosial.
- Bagaimana lingkungan kerja karyawan? Faktor ini berpengaruh terhadap risiko ancaman dari orang dalam.
- Seberapa efektif sistem deteksi intrusi? Sistem ini harus mampu mengenali dan merespons ancaman dengan cepat.
- Apakah sistem pelaporan ancaman sudah jelas? Karyawan harus tahu bagaimana melaporkan potensi ancaman atau pelanggaran keamanan.
- Apakah ada rencana untuk menghadapi ancaman dari orang dalam? Ancaman ini sering kali lebih sulit dideteksi dibandingkan serangan eksternal.

Beberapa perusahaan enggan mengutamakan pencegahan karena dianggap meningkatkan biaya dan menurunkan produktivitas. Hal ini disebabkan oleh perlunya pengelolaan izin akses, autentikasi ulang, dan pemantauan keamanan yang terus-menerus (Donaldson et al., 2015). Namun, perusahaan perlu mempertimbangkan strategi yang paling sesuai, apakah lebih fokus pada pencegahan, reaksi terhadap insiden, atau kombinasi keduanya.

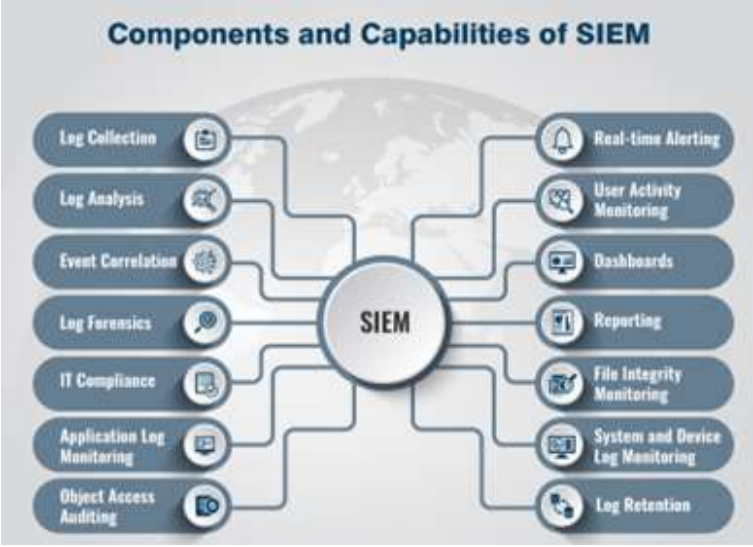
2. *Security Incident Event Management* (SIEM)

Dalam menghadapi ancaman siber yang semakin canggih, organisasi perlu menerapkan strategi keamanan yang komprehensif untuk melindungi sistem informasi mereka. Salah satu

MUSYTARI
ISSN : 3025-9495
Neraca Akuntansi Manajemen, Ekonomi
Vol 17 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

pendekatan yang banyak digunakan adalah Security Incident Event Management (SIEM). Menurut Pham (2018), SIEM merupakan sebuah sistem yang memungkinkan analis keamanan untuk memahami berbagai ancaman yang menyerang proses TI suatu perusahaan dengan cara mengumpulkan, menginterpretasikan, serta mengasosiasikan data dari berbagai sumber log dalam jaringan. Dengan cara ini, organisasi dapat mendeteksi potensi serangan dengan tingkat akurasi yang lebih tinggi dan tingkat kesalahan positif yang lebih rendah.
Gambar berikut menunjukkan komponen dari sistem SIEM, yang terdiri dari beberapa elemen utama, seperti pengumpulan log, normalisasi data, analisis ancaman, serta respons insiden:

Gambar 1. Components of SIEM System (Sumber: Fakiha, 2021)



Sumber: Fakiha, 2021

Selain itu, Pham (2018) menegaskan bahwa penting bagi analis keamanan untuk mengidentifikasi komponen sistem yang paling rentan di setiap departemen dalam organisasi. Hal ini dilakukan agar ancaman dapat diprioritaskan dan direspons berdasarkan tingkat risikonya. SIEM juga mempermudah proses investigasi serangan dengan memberikan korelasi antara berbagai kejadian keamanan dalam jaringan, sehingga tim keamanan dapat mengantisipasi serangan sebelum terjadi atau meresponsnya dengan lebih cepat.
Di sisi lain, Intrusion Detection System (IDS) juga menjadi alat keamanan penting dalam melindungi komunikasi dan sistem informasi. Menurut Singh et al. (2016), IDS merupakan sistem yang berfungsi sebagai pemantau aktivitas jaringan yang dapat mendeteksi pelanggaran kebijakan atau indikasi serangan berbahaya. Jika sistem mendeteksi suatu anomali, IDS akan segera mengirimkan peringatan kepada tim keamanan. Meski teknologi IDS masih dalam tahap pengembangan lebih lanjut, penelitian dari Azodolmolky et al. (2020) menegaskan bahwa IDS memainkan peran krusial dalam arsitektur keamanan informasi modern.
Singh et al. (2016) juga menyoroti bahwa dalam mengamankan sistem digital, organisasi perlu menggabungkan beberapa solusi keamanan, seperti firewall, sistem deteksi intrusi (IDS), antivirus yang andal, serta teknologi SIEM. Dengan kombinasi perlindungan ini, perusahaan dapat mengelola ancaman siber secara lebih efektif dan mengurangi risiko kebocoran data atau serangan siber yang dapat merugikan operasional bisnis.

MUSYTARI
ISSN : 3025-9495
Neraca Akuntansi Manajemen, Ekonomi
Vol 17 No 2 Tahun 2025
Prefix DOI : 10.8734/mnmae.v1i2.359

Seiring meningkatnya ancaman siber secara global, diperlukan pula kerangka hukum yang jelas dan konsisten untuk menangani serangan siber yang semakin kompleks. Oleh karena itu, organisasi harus terus memperbarui sistem keamanan mereka dengan mengadopsi metode yang lebih canggih serta meningkatkan kesadaran akan pentingnya keamanan siber di antara karyawan dan pengguna sistem.

3. Bug Bounty

Bug bounty programs telah menjadi strategi efektif dalam memperkuat keamanan siber dengan melibatkan white hat hackers untuk menemukan dan memperbaiki celah keamanan sebelum dieksploitasi oleh black hat hackers. Program ini memberikan insentif berupa kompensasi finansial serta pengakuan kepada para hacker yang melaporkan celah keamanan dalam sistem perusahaan atau organisasi (Conger, 2017).

Salah satu contoh sukses dari *bug bounty* adalah kerja sama Angkatan Darat AS dengan HackerOne pada November 2016 dalam program "Hack the Army". Program ini mengungkap berbagai celah keamanan yang sebelumnya tidak diketahui, termasuk akses tanpa kredensial ke jaringan internal Departemen Pertahanan (DOD) melalui situs perekrutan publik mereka. Tanpa laporan dari hacker etis, celah ini mungkin tidak akan terdeteksi, yang berpotensi membahayakan keamanan nasional (Conger, 2017). Keberhasilan ini berlanjut dengan program lain seperti "Hack the Pentagon" dan "Hack the Air Force", yang masing-masing menemukan lebih banyak celah keamanan dari program sebelumnya (Uchill, 2017).

Bug bounty bukanlah konsep baru. Bahkan sebelum era digital, perusahaan seperti Hunter and Ready telah menggunakannya pada tahun 1983 untuk menguji sistem operasi real-time mereka dengan hadiah berupa mobil Volkswagen Beetle bagi mereka yang menemukan celah dalam sistem VRTX. Perusahaan otomotif lain, seperti Fiat Chrysler dan Tesla, juga menerapkan *bug bounty* guna meningkatkan keamanan sistem kendaraan mereka (Greenberg, 2016; Fox-Brewster, 2015).

Meskipun terbukti efektif, *bug bounty* memiliki keterbatasan. Program ini hanya mengidentifikasi dan memperbaiki celah keamanan saat bounty sedang berlangsung, sehingga untuk menjaga keamanan secara berkelanjutan, organisasi perlu mengadakan program ini secara terus-menerus, yang bisa sangat mahal. Sebagai contoh, "Hack the Air Force" menghabiskan lebih dari $130.000 hanya untuk hadiah kepada hacker (Uchill, 2017). Selain itu, antusiasme peserta cenderung menurun seiring waktu, membuat program ini kurang efektif dalam jangka panjang.

Karena biaya yang tinggi, *bug bounty* lebih banyak dimanfaatkan oleh perusahaan besar dibanding individu. Namun, individu tetap bisa meningkatkan keamanan siber dengan langkah sederhana seperti rutin memperbarui perangkat lunak dan sistem operasi untuk menutup celah yang bisa dimanfaatkan oleh malware. Semakin lama pembaruan ditunda, semakin besar risiko serangan (Greenberg, 2016).

Lebih jauh, penerapan keamanan siber harus dimulai sejak tahap awal pengembangan sistem, terutama dalam teknologi yang sulit diperbarui setelah digunakan, seperti perangkat medis dan sistem kontrol lalu lintas udara. Beberapa perusahaan memiliki departemen IT untuk menangani tugas dasar seperti pemeliharaan sistem dan pencadangan data, namun akan lebih ideal jika memiliki tim khusus keamanan siber yang fokus mengatasi ancaman siber. Alternatif lain adalah

bekerja sama dengan perusahaan keamanan siber eksternal yang dapat membantu mengevaluasi sistem, memberikan solusi perlindungan, dan melatih tim internal dalam menjaga keamanan data.

Pendekatan terbaik dalam mengatasi ancaman siber adalah bersikap proaktif dibanding reaktif. Jika hanya bertindak setelah serangan terjadi, dampaknya bisa meluas ke sistem lain dan lebih sulit dikendalikan. Sebaliknya, strategi proaktif dengan mengantisipasi potensi ancaman dan menerapkan langkah-langkah pencegahan sejak awal akan jauh lebih efektif dalam menjaga keamanan jaringan dan sistem organisasi.

KESIMPULAN

Pencurian identitas merupakan ancaman serius di era digital, dengan implikasi finansial dan pribadi yang signifikan. Kemudahan akses informasi pribadi di dunia maya telah memicu peningkatan kejahatan ini, yang semakin sulit dideteksi dan diatasi. Kerugian finansial yang besar, seperti yang tercatat di ITAP, menegaskan urgensi untuk mengambil tindakan pencegahan yang lebih efektif.

Organisasi dan individu perlu beralih dari pendekatan reaktif ke pendekatan proaktif dalam menangani pencurian identitas. Strategi "pertahanan preventif" harus diutamakan, dengan fokus pada pencegahan sejak awal. Langkah-langkah seperti peningkatan keamanan data pribadi, edukasi pengguna tentang praktik keamanan digital, dan penerapan teknologi deteksi dini dapat membantu mengurangi risiko pencurian identitas. Penerapan strategi pencegahan yang efektif akan mengurangi jumlah kasus pencurian identitas, meminimalkan kerugian finansial, dan melindungi reputasi individu serta organisasi. Investasi dalam teknologi keamanan dan peningkatan kesadaran akan menjadi kunci dalam membangun lingkungan digital yang lebih aman. Selain itu, diperlukan kerjasama antara pemerintah, lembaga keuangan, dan penyedia layanan digital untuk menciptakan kerangka kerja yang kuat dalam memerangi kejahatan ini.

DAFTAR PUSTAKA

Fakiha, B. (2021). Business organization Security Strategies to Cyber Security Threats. International Journal of Safety and Security Engineering, 11(1), 101–104. https://doi.org/10.18280/ijsse.110111

N. H. A., Hamid, S., Kiah, L. M., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. Kybernetes, 44(4), 606-622. https://doi.org/10.1108/K-12-2014-0283

Moorthy, R. S., & Pabitha, P. (2020). Optimal detection of phishing attack using SCA-based K NN. Procedia Computer Science, 171, 1716–1725. Elsevier https://doi.org/10.1016/j.procs.2020.04.184

Wang, X., Wen, Q., Li, C., & Guo, J. (2024). Studying subthreshold resonance using the Trojan horse method. Physics Letters B, 854, 138745. https://doi.org/10.1016/j.physletb.2024.138745

Paul, A., Sharma, V., & Olukoya, O. (2024). SQL injection attack: Detection, prioritization &

prevention. Journal of Information Security and Applications, 85, 103871. https://doi.org/10.1016/j.jisa.2024.103871

Kaur, P., & Sharma, S. (2015). Spyware detection in Android using hybridization of description analysis, permission mapping and interface analysis. Procedia Computer Science, 46, 794– 803. https://doi.org/10.1016/j.procs.2015.02.148

Mahmud, R. (2019). Pencurian Identitas: Kategori & Kasus. CyberSecurity dan Forensik Digital, 2(1), 38-42. https://doi.org/10.14421/csecurity.2019.2.1.1421

Uchill, J. (2017), "'Hack the Air Force' challenge most successful military bug bounty yet", The Hill, 10 August, available at: https://thehill.com/policy/cybersecurity/346016-hack-the airforce-challenge-most-successful-military-bug-bounty-yet/

Lahcen, R. a. M., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. Cybersecurity, 3(1). https://doi.org/10.1186/s42400-020-00050-w

Zahwani, S. T., & Nasution, M. I. P. (2024). Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital. Zahwani | Journal of Sharia Economics Scholar (JoSES). https://doi.org/10.5281/zenodo.12608751

Hasan, M. S., Rahman, R. A., Abdillah, S. F. H. B. T., & Omar, N. (2015). Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia. Journal of Social Sciences, 11(4), 395–404. https://doi.org/10.3844/jssp.2015.395.404

Conger, K. (2017), "Hacking the Army", TechCrunch, 19 January, available at: https://techcrunch.com/2017/01/19/hacking-the-army/

Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2015). Enterprise Cybersecurity. In Apress eBooks. https://doi.org/10.1007/978-1-4302-6083-7

Pham, Lan. (2018). A Review of key paradigms: positivism, interpretivism and critical inquiry. http://dx.doi.org/10.13140/RG.2.2.13995.54569

Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2015). Twenty Security Considerations for Cloud-Supported Internet of Things. IEEE Internet of Things Journal, 3(3), 269–284. https://doi.org/10.1109/jiot.2015.2460333