MAKALAH

UNAUTHORIZED ACCESS TO COMPUTER SYSTEM

(Disusun untuk memenuhi tugas etika dan profesi)

Dosen Pengampu :

Ikbal Jamaludin, M.KOM.

Disusun Oleh :

Yopi Pebrianti (21110380)

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER MARDIRA INDONESIA

Jl. Soekarno-Hatta No. 211, Leuwipanjang, Situsaeur, Bojongloa Kidul, Kota Bandung, 40233

Tlp: (022) 5230382, Email:info@stmik-mi.ac.id.

2024

KATA PENGANTAR

Puji syukur kami haturkan kehadirat Allah Swt. yang telah melimpahkan rahmat dan hidayah-Nya sehingga kami bisa menyelesaikan karya ilmiah tentang "*Unithorized access to computer system*".

Makalah ini disusun untuk memenuhi tugas mata kuliah “Etika dan Profesi” , Kami juga ingin menyampaikan apresiasi kepada para pembaca yang telah meluangkan waktu untuk membaca penulisan ini. Semoga penulisan ini dapat memberikan manfaat dan pemahaman yang lebih dalam terkait dengan topik yang dibahas.

Saya menyadari bahwa makalah ini masih banyak kekurangan. Sebagai penulis, saya berharap pembaca bisa memberikan kritik agar tulisan selanjutnya jauh lebih baik. Di sisi lain, saya berharap pembaca menemukan pengetahuan baru dari laporan penelitian ini. Walaupun tulisan ini tidak sepenuhnya bagus, saya berharap ada manfaat yang bisa diperoleh oleh pembaca. Demikian sepatah dua patah kata dari saya. Terima kasih.

Hormat kami

YOPI PEBRIANTI

DAFAR ISI

BAB I
PENDAHULUAN

I.I Latar Belakang Masalah

Semakin berkembangnya teknologi informasi dan komunikasi, akses ke sistem komputer menjadi semakin mudah. Namun, hal ini juga membawa risiko terhadap keamanan data dan informasi yang disimpan dalam sistem komputer.

Tindakan *Unauthorized Access To Computer System* merujuk pada kegiatan yang dilakukan oleh seseorang atau kelompok yang tidak memiliki izin atau hak untuk mengakses sistem komputer tersebut. Tindakan ini dapat dilakukan dengan berbagai cara, seperti mencuri kata sandi, menggunakan software atau teknik hacking, atau memanfaatkan celah keamanan yang ada dalam sistem.

Ada berbagai motif di balik serangan akses tidak sah ke sistem komputer. Beberapa pelaku mungkin mencari keuntungan finansial dengan mencuri informasi sensitif seperti data kartu kredit atau informasi pribadi. Sementara itu, yang lain mungkin melakukan serangan untuk tujuan politik, ideologis, atau bahkan hanya untuk mencari tantangan teknis. Sehingga dalam kejahatan computer dimungkinkan adanya delik formil dan delik materil. Delik formil adalah perbuatan seseorang yang memasuki Komputer orang lain tanpa ijin, sedangkan delik materil adalah perbuatan yang menimbulkan akibat kerugian bagi orang lain. Adanya cyber crime telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet dan intranet.

Akibat dari *Unauthorized Access To Computer System* dapat sangat merugikan, mulai dari pencurian data pribadi atau rahasia, perusakan sistem, hingga pencurian informasi penting yang dapat digunakan untuk kepentingan pribadi atau kejahatan lainnya. Oleh karena itu, perlindungan terhadap sistem komputer sangat penting untuk mencegah tindakan yang tidak diinginkan dan melindungi data dan informasi yang disimpan di dalamnya.

I.2 Keberadaan Unauthorized system

Unauthorized access sering diartikan sebagai upaya masuk atau mengakses suatu sistem atau informasi tanpa izin resmi dari pemiliknya. Istilah ini sering dikaitkan dengan hacking, pencurian data, dan peretasan sistem. Dalam konteks perusahaan, unauthorized access dapat membuka pintu bagi kebocoran informasi yang bernilai tinggi atau bahkan menghancurkan reputasi perusahaan. Saat ini, entitas baik kecil maupun besar semakin rentan terhadap risiko unauthorized access. Pengelolaan akses data yang kompleks, termasuk pengaturan izin dan enkripsi, tidak selalu cukup untuk melindungi sistem. Pelaku unauthorized access, yang seringkali memiliki kemampuan setara dengan peretas profesional, memanfaatkan kelemahan sistem atau celah keamanan untuk mencapai tujuan mereka.

BAB II
LANDASAN TEORI

2.1 Cybercrime

Kejahatan cyber atau kerap dikenal dengan cyber crime merupakan tindak perilaku kejahatan berbasis komputer dan jaringan internet. Pelaku dari kejahatan siber biasanya akan meretas sistem untuk memperoleh data korban yang bersifat privasi. Terdapat berbagai jenis tindak kejahatan siber. Berikut empat jenis tindak kejahatan siber:

Menurut brenda nawawi (2001) kejahatan cyber merupakan bentuk fenomena baru dalam tindak kejahatan sebagai dampak langsung dari perkembangan teknologi informasi beberapa sebutan diberikan pada jenis kejahatan baru ini di dalam berbagai tulisan, antara lain: sebagai " kejahatan dunia maya" (cyberspace/virtual-space offence), dimensi baru dari "hi-tech crime", dimensi baru dari "transnational crime", dan dimensi baru dari "white collar crime".

2.2 Peretasan

Peretasan merupakan upaya menyusup kepada sistem komputer tanpa izin. Beberapa hal yang biasa dilakukan para peretas yaitu membobol sistem, mencuri data pribadi, dan data keuangan.

2.3 unauthorized access

Kejahatan dengan cara menyusup ke dalam sistem komputer tanpa izin dan tanpa sepengetahuan pemilik sistem. Dengan cara ini, pelaku dapat mencuri data-data pemilik sistem sehingga dapat melakukan pembajakan dan perusakan sistem (hacking dan cracking).

BAB III
PEMBAHASAN

3.1.1 Metode dan Teknik *Unauthorized Access To Computer System*

Motif pelaku *unauthorized access* dapat bervariasi dari tujuan ekonomi hingga ideologis, di bawa ini beberapa yang dilakukan oleh pelaku *unauthorized access*.

1. Hacking

   Individu atau kelompok mendapatkan akses tidak sah ke sistem komputer melalui berbagai cara, seperti memanfaatkan kerentanan perangkat lunak atau menggunakan teknik rekayasa sosial untuk menipu pengguna agar mengungkapkan kredensial mereka.

2. Malware

   Perangkat lunak berbahaya, seperti virus, worm, Trojan, dan ransomware, dapat menginfeksi komputer dan memberikan akses tidak sah kepada penyerang, memungkinkan mereka untuk mencuri data, memantau aktivitas, atau mengendalikan sistem yang terinfeksi secara remote.

3. Ancaman dari Dalam

   Karyawan, kontraktor, atau individu tepercaya lainnya dengan akses yang sah dapat menyalahgunakan hak istimewa mereka untuk mendapatkan akses tidak sah ke informasi atau sistem sensitif untuk keuntungan pribadi, balas dendam, atau spionase.

4. Brute force

   Metode serangan yang mencoba semua kemungkinan kombinasi password atau kunci enkripsi untuk mendapatkan akses ke sistem atau data yang dilindungi.

3.1.2 Dampak *Unauthorized Access*

1. Bocornya informasi perusahaan dan data pribadi pelanggan.
2. Perusahaan bisa dituntut karena merugikan pelanggan.
3. Reputasi perusahaan rusak karena masyarakat jadi tidak percaya bahwa mereka aman.

3.1.3 Strategi dan Taktik Pencegahan *Unauthorized Access To Computer System*

1. Penggunaan Firewall

   Firewall adalah sebuah sistem keamanan yang digunakan untuk melindungi jaringan komputer dari serangan dan akses yang tidak sah. Penggunaan firewall sangat penting untuk menjaga keamanan dan privasi data di dalam jaringan.

Di bawah ini cara penggunaan firewall:

a. Mengatur kebijakan akses
b. Memonitor lalu lintas jaringan
c. Mendeteksi dan mencegah serangan
d. Melindungi data sensitive
e. Mengoptimalkan kinerja jaringan

2. Enkripsi

   Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa di mengerti menjadi sebuah kode yang tidak dapat di mengerti. Pada dasarnya enkripsi mempunyai 2 model dasar yang sangat penting enkripsi dengan kunci pribadi *(private key)* dan enkripsi public model *(Public Key).*

3. Pelatihan Kesadaran Keamanan

   Mendidik karyawan dan pengguna tentang praktik keamanan cyber terbaik, seperti menghindari penipuan phishing, menggunakan kata sandi yang kuat, dan melaporkan aktivitas mencurigakan, dapat membantu mencegah akses tidak sah yang disebabkan oleh kesalahan atau kelalaian manusia.

IV
KESIMPULAN

4.1 KESIMPULAN

Dalam era perkembangan teknologi informasi dan komunikasi yang semakin maju, akses ke sistem komputer menjadi lebih mudah. Namun, bersamaan dengan kemudahan tersebut, muncul pula risiko terhadap keamanan data dan informasi yang disimpan dalam sistem komputer. Tindakan Unauthorized Access To Computer System, yang merujuk pada kegiatan yang dilakukan oleh seseorang atau kelompok tanpa izin atau hak untuk mengakses sistem komputer, dapat membawa dampak yang serius bagi individu, perusahaan, dan masyarakat secara keseluruhan.

Pelaku unauthorized access dapat memiliki berbagai motif, mulai dari keuntungan finansial hingga tujuan politik atau ideologis. Metode dan teknik yang digunakan pun bervariasi, seperti hacking, penggunaan malware, ancaman dari dalam, dan serangan brute force. Dampak dari tindakan unauthorized access juga dapat beragam, termasuk bocornya informasi perusahaan dan data pribadi pelanggan, tuntutan hukum, kerusakan reputasi perusahaan, dan kerugian finansial.

Untuk mencegah tindakan unauthorized access, diperlukan strategi dan taktik yang efektif. Penggunaan firewall, enkripsi data, dan pelatihan kesadaran keamanan menjadi langkah-langkah yang penting untuk melindungi sistem komputer dari serangan. Dengan demikian, perlindungan terhadap sistem komputer tidak hanya penting untuk mencegah tindakan yang tidak diinginkan, tetapi juga untuk menjaga keamanan dan privasi data yang disimpan di dalamnya.

DAFTAR PUSTAKA

Budiartio Hary (2014). *Membangun Cyber community memajukan perekonomian nasional dalam rangka ketahanan nasional.*

Ilham, Bintang (2023), *Pembahasan, Analisis Kasus dan Landasan Teori Tentang Unauthorized Access to Computer Systems,* diakses pada 20 maret 2024. https://www.anandanesia.com/unauthorized-access-to-computer-systems/

Mukhtar Harun (2022). *Kriptografi untuk keamanan data*.

Reageadies, Jessy M dan Apriliani, N (2020), *MAKALAH UNAUTHORIZED ACCESS TO COMPUTER SYSTEM AND SERVICE EPTIK PERTEMUAN 9 UBSI*, Di akses pada 18 maret 2024. https://thismineok.wordpress.com/2020/05/22/unauthorized-access-to-computer-system-and-service/

Rini, Pertiwi (2024), *Kejahatan cybercrime*, diakases pada 18 maret 2024. https://kominfo.kotabogor.go.id/index.php/post/single/740